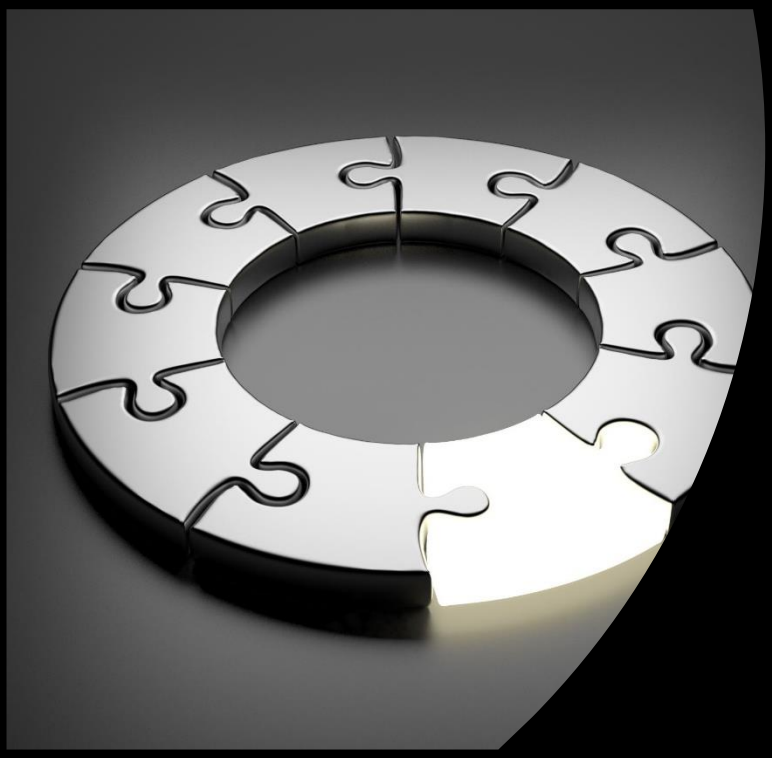
{Digital Forensics Fundamentals}



AusCERT

10 May 2022

Table of Contents

MUS2019 DFIR CTF

MUS2019 DFIR CTF

The Magnet User Summit 2019 DFIR CTF Challenge was released to the public. This CTF was created by David Cowen, Matthew Seyer and Jessica Hyde. We'll use this evidence and questions to demonstrate the fundamentals of digital forensics.

In order to play along you will need to download the artefacts.

List of Questions

1. (Acquisition/Verification) What is the SHA1 hash of the desktop post's forensic image?
2. (Acquisition/Verification) Who acquired the forensic image of the desk?
3. (Acquisition/Verification) What is the serial number of the OS volume of the desktop station?
4. (File System) What is the name of the file associated with MFT entry number 102698?
5. (File System) What is the file name that represented MFT entry 60725 with a sequence number of 10?
6. (File System) Which file name represents the USN record where the USN number is 546416480?
7. (File System) What is the MFT sequence number associated with the file "\Users\Administrator\Desktop\FTK_Imager_Lite_3.1.1\FTK Imager.exe"?
8. (Registry) What was the timezone offset at the time of imaging?
9. (Registry) What is the timezone of the desktop station?
10. (Registry) When was the Windows OS installed?
11. (Registry) What is the IP address of the Desktop?
12. (Event Logs) Which User Shutdown Windows on February 25th 2019?
13. (User Activity) Which user installed TeamViewer?
14. (User Activity) At least how many times did the teamviewer_desktop.exe run?
15. (User Activity) After looking at the TEAMVIEWER_DESKTOP.EXE prefetch file, which path was the executable in at the time of execution?

1.What is the SHA1 hash of the desktop image?

- This is one of the most critical parts of computer forensics, validating the evidence. The weakest point in any investigation is the integrity of the data, so validation is essential.
- Validating digital evidence requires using a hashing algorithm utility which is design to create a binary or hexadecimal number that represents the uniqueness of the data set. Because hash values are unique, if two files have the same hash values, they are identical. (Collisions are out of scope of this course).
- MD5 and SHA1 are the two most popular hashing algorithms used today to verify the integrity of a given piece of evidence.
- There are several tools that can be used to calculate the digital footprint of the evidence file.

FTK Imager

1. Open FTK Imager
2. Go to File > Add Evidence Item
3. Choose “Image File” then Next
4. Browse and find the E01 evidence file then Next
5. Right click on the item under the Evidence Tree and select “Verify Drive/Image”
6. The process will begin.

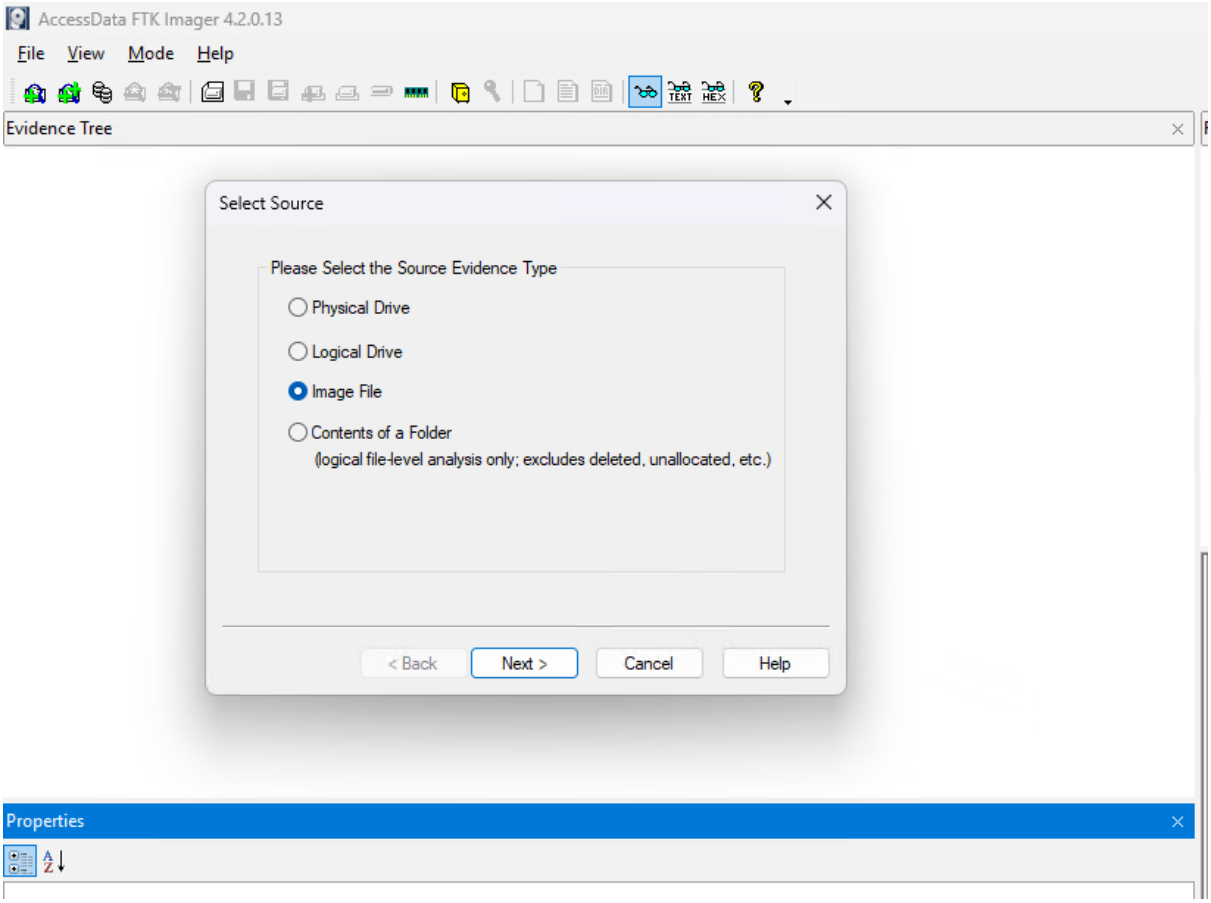


Figure 1: FTK Imager Image Verification

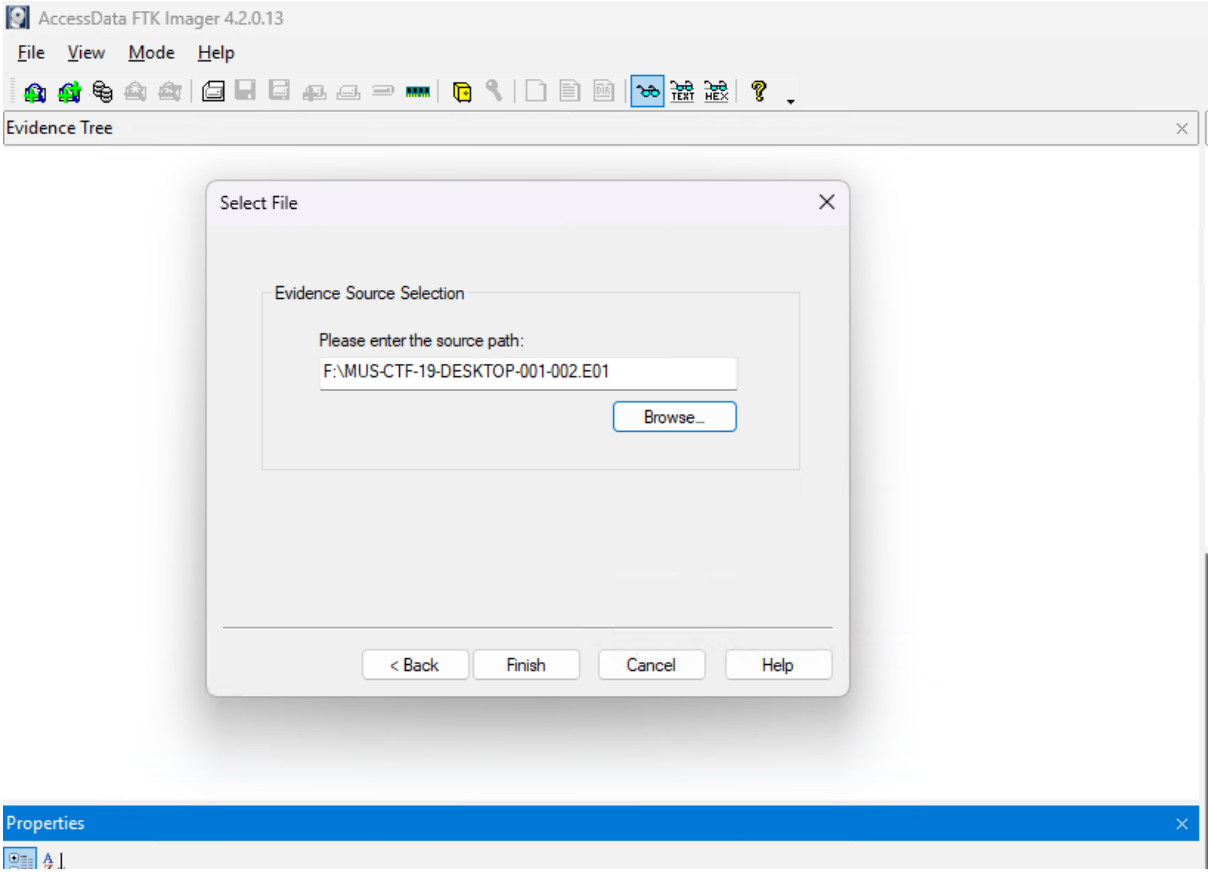


Figure 2: FTK Imager Image Verification

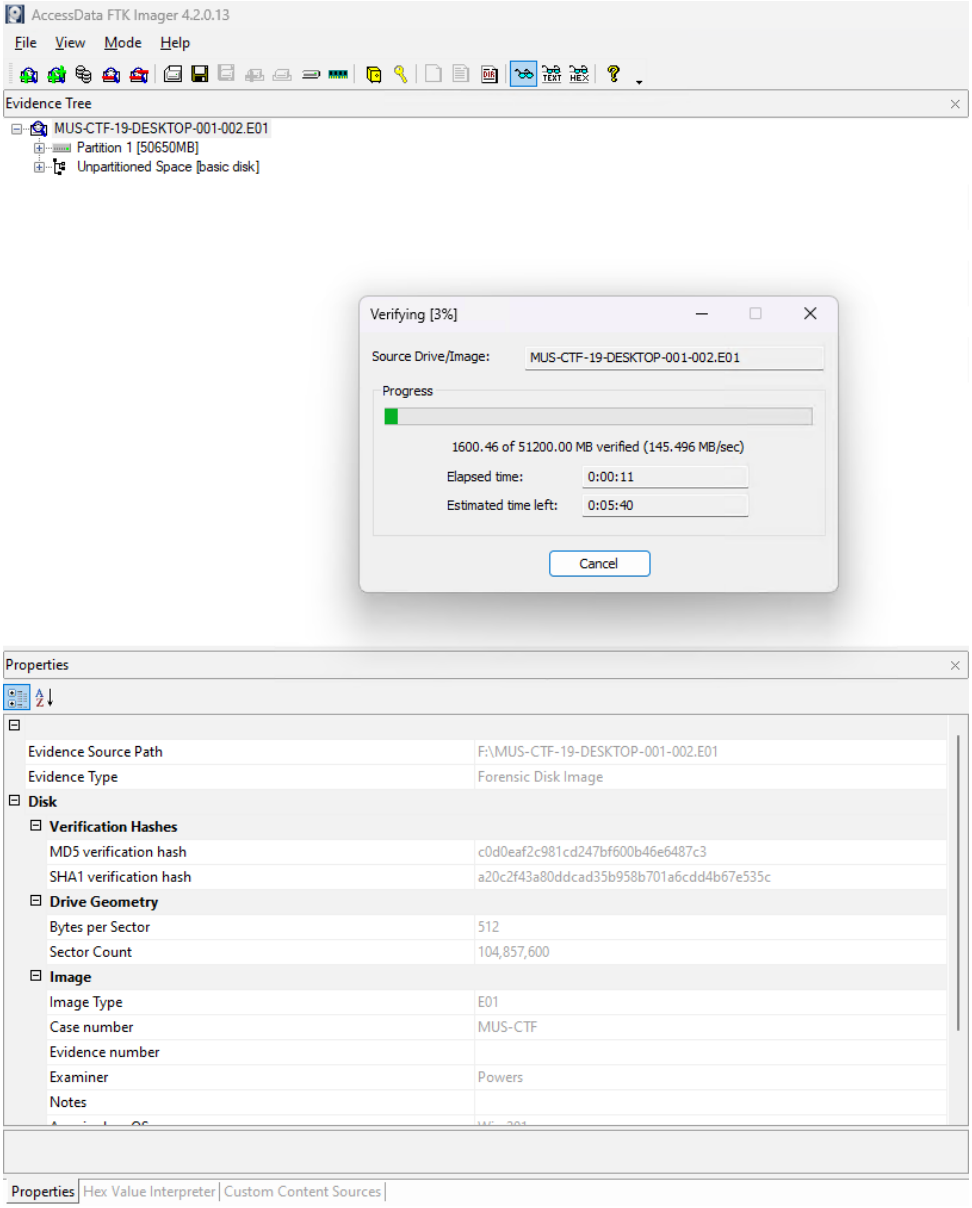


Figure 3: FTK Imager Image Verification

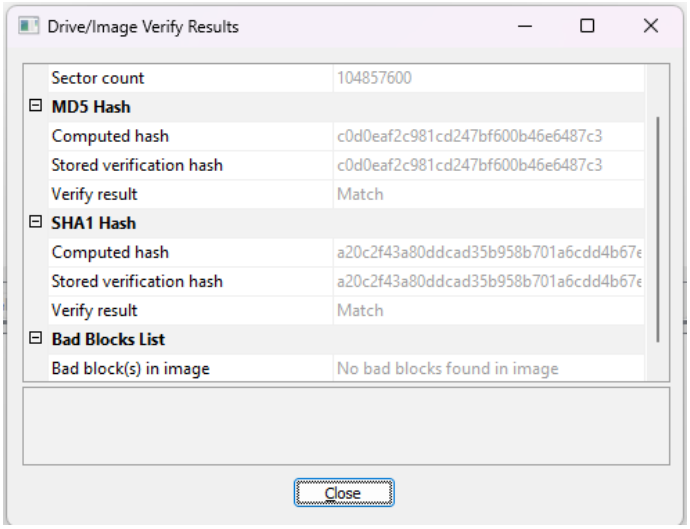


Figure 4: FTK Imager Image Verification

MUS-CTF-19-DESKTOP-001.E01.txt

This text file was included with the evidence and contains the metadata that is embedded into the E01 file. This file contains the Image information and checksums as well as the verification results.

MUS-CTF-19-DESKTOP-001.E01.txt - Notepad

File Edit View

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: MUS-CTF
Evidence Number:
Unique description: Desktop
Examiner: Powers
Notes:

--------------------------------------------------------------

Information for Z:\Image\MUS-CTF-19\MUS-CTF-19-DESKTOP-001:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 6,527
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 104,857,600
[Physical Drive Information]
 Drive Model: Red Hat VirtIO SCSI Disk Device
 Drive Interface Type: SCSI
 Removable drive: False
 Source data size: 51200 MB
 Sector count:    104857600
[Computed Hashes]
 MD5 checksum:    c0d0eaf2c981cd247bf600b46e6487c3
 SHA1 checksum:   a20c2f43a80ddcad35b958b701a6cdd4b67e535c

Image Information:
 Acquisition started:   Wed Mar 20 14:29:33 2019
 Acquisition finished:  Wed Mar 20 15:42:50 2019
 Segment list:
  Z:\Image\MUS-CTF-19\MUS-CTF-19-DESKTOP-001.E01

Image Verification Results:
 Verification started:  Wed Mar 20 12:06:24 2019
 Verification finished: Wed Mar 20 12:10:28 2019
 MD5 checksum:    c0d0eaf2c981cd247bf600b46e6487c3 : verified
 SHA1 checksum:   a20c2f43a80ddcad35b958b701a6cdd4b67e535c : verified
```

Ln 32, Col 59 | 100% | Windows (CRLF) | UTF-8 with BOM

Figure 5: MUS-CTF-19-DESKTOP-001.E01.txt

PowerShell

The Get-FileHash cmdlet computes the hash value for a file by using a specified hash algorithm.

7. Open a PowerShell command prompt.
8. Browse to the location of the E01 file on your system.
9. Run the following command.

```
Get-FileHash MUS-CTF-19-DESKTOP-001-002.E01 -Algorithm SHA1 | Format-List
```

Review the output which should match the output below.

```
PS F:\> Get-FileHash MUS-CTF-19-DESKTOP-001-002.E01 -Algorithm SHA1 |
Format-List

Algorithm : SHA1

Hash      : CCB80231AC0E748C14070BC472E5F08053360C08

Path      : F:\MUS-CTF-19-DESKTOP-001-002.E01
```

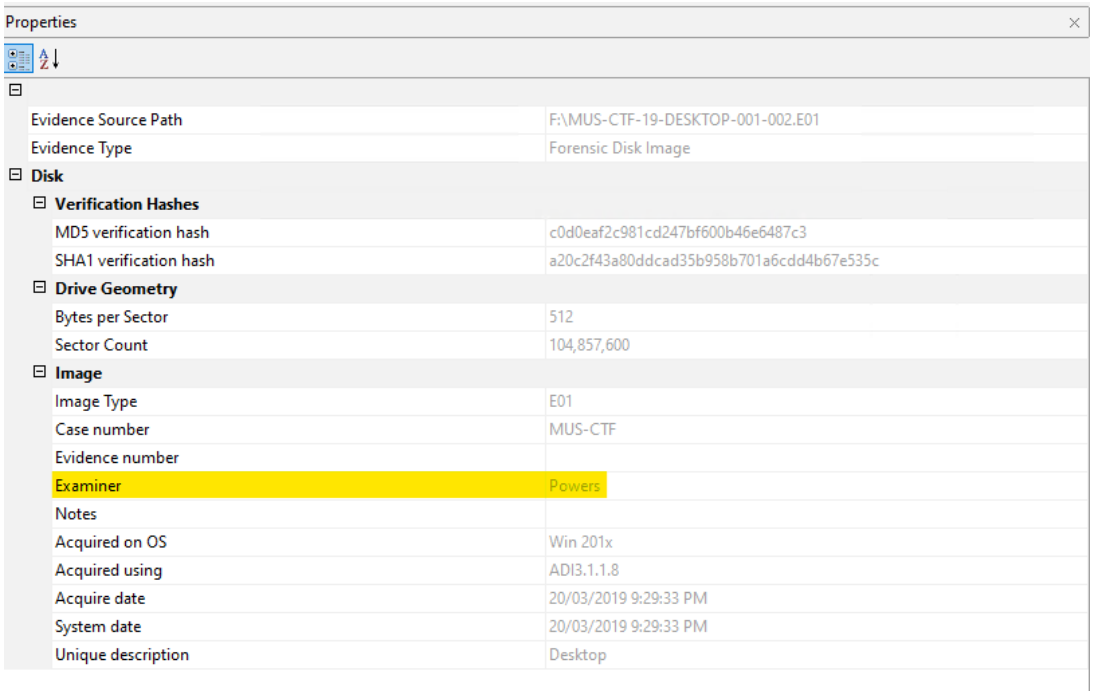
Question: Why doesn't this match what we found in FTK Imager?

Flag	a20c2f43a80ddcad35b958b701a6cdd4b67e535c

2. Who acquired the forensic image of the desk?

FTK Imager

You may have already noticed the pane on the bottom left called “Properties” in FTK Imager. This displays the contents of the evidence acquisition process. The Examiner who acquired the forensic image called themselves “Powers”.

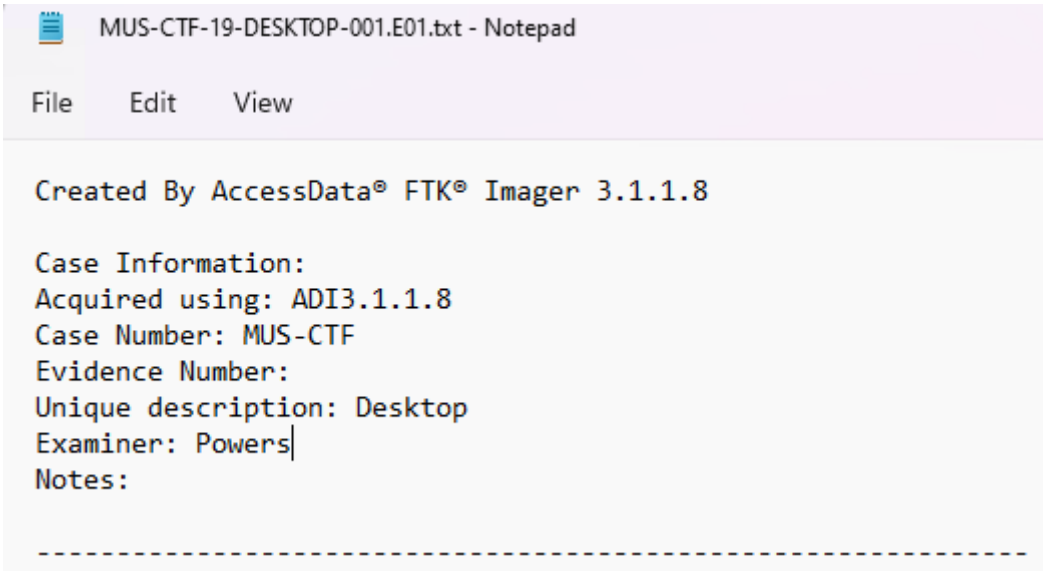


Properties

Evidence Source Path	F:\MUS-CTF-19-DESKTOP-001-002.E01
Evidence Type	Forensic Disk Image
Disk	
Verification Hashes	
MD5 verification hash	c0d0eaf2c981cd247bf600b46e6487c3
SHA1 verification hash	a20c2f43a80ddcad35b958b701a6cdd4b67e535c
Drive Geometry	
Bytes per Sector	512
Sector Count	104,857,600
Image	
Image Type	E01
Case number	MUS-CTF
Evidence number	
Examiner	Powers
Notes	
Acquired on OS	Win 201x
Acquired using	ADI3.1.1.8
Acquire date	20/03/2019 9:29:33 PM
System date	20/03/2019 9:29:33 PM
Unique description	Desktop

Figure 6: Who acquired the forensic image of the disk

MUS-CTF-19-DESKTOP-001.E01.txt



MUS-CTF-19-DESKTOP-001.E01.txt - Notepad

File Edit View

```
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: MUS-CTF
Evidence Number:
Unique description: Desktop
Examiner: Powers
Notes:

--------------------------------------------------------------
```

Flag	Powers

3. What is the serial number of the OS volume of the desktop station?

- The volume serial number is stored in the disk parameter block part of the volume boot record.
- A volume serial number is a serial number assigned to a disk volume or tape volume. In FAT and NTFS file systems, a volume serial number is a feature used to determine if a disk is present in a drive or not, and to detect if it was exchanged with another one.
- When a USB device is examined in forensic software, the volume serial number of the device can be seen. If a link file for a deleted file is located on a computer hard drive and the volume serial number matches that of a USB device that is in evidence, a clear connection can be made between the USB device and the file that once existed on the hard drive, even if the file is no longer present on the USB device or the hard drive.

FTK Imager

You may have already noticed the pane on the bottom left called "Properties" in FTK Imager. If we select the partition we want to view the properties for we can see the Volume Serial Number under the File System Information pane.

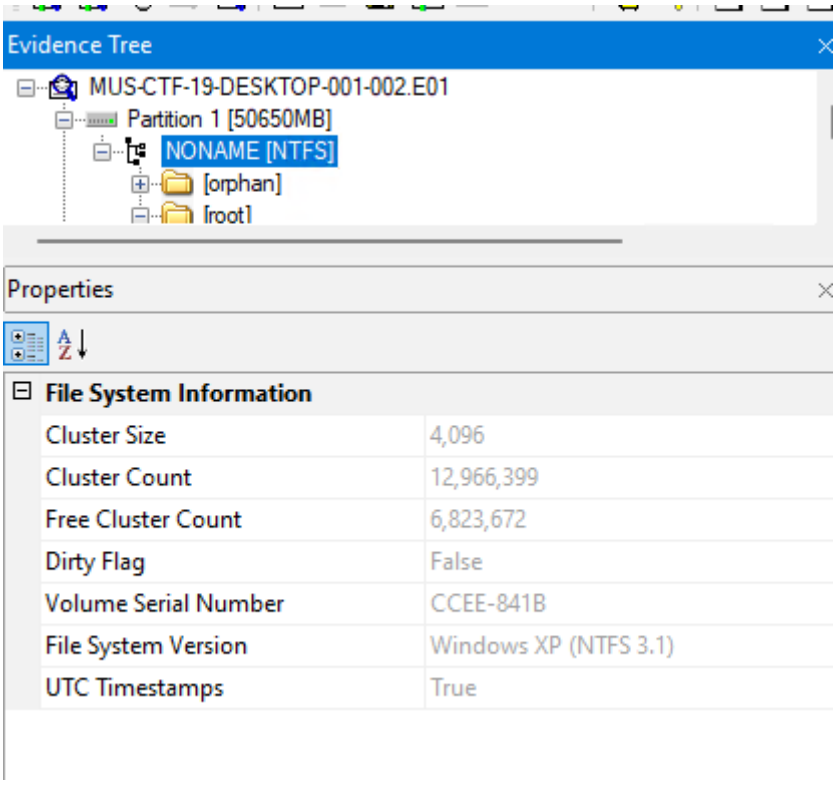


Figure 7: Volume Serial Number in FTK Imager

Flag	CCEE-841B

File System Forensics – the MFT

Obtaining the MFT

FTK Imager

1. As before, open FTK Imager and add your evidence item.
2. Click on the expand + symbol to the left of the evidence item. Do this again until you see the root directory and its contents.

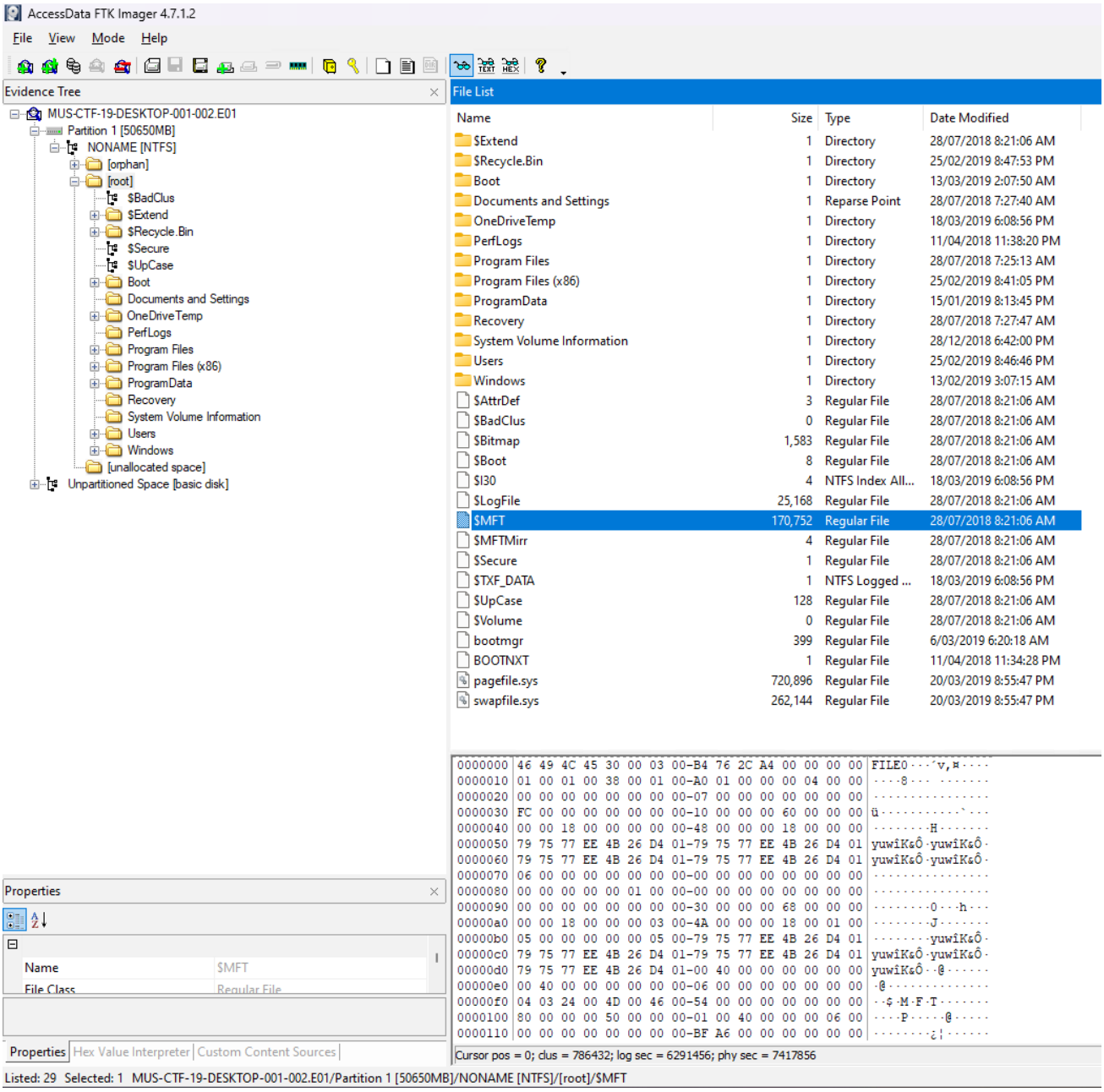
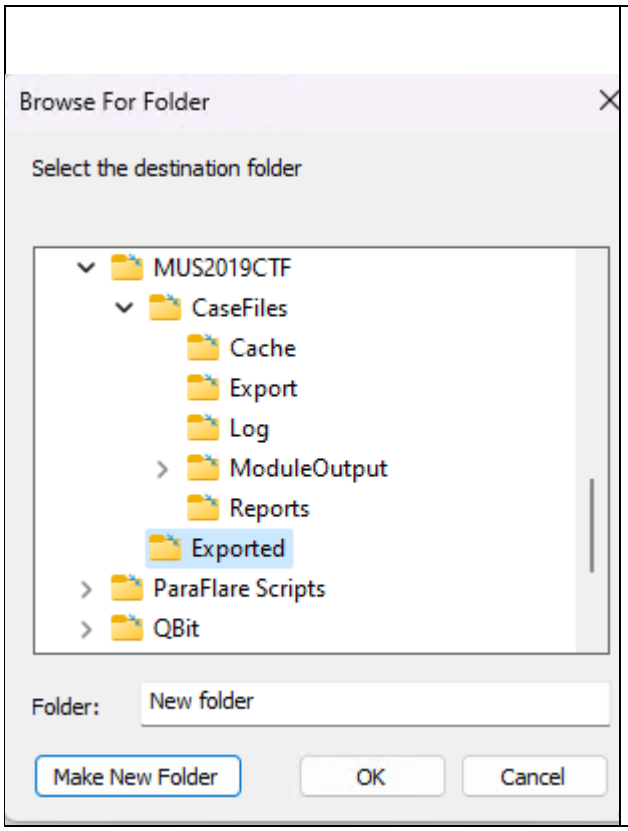
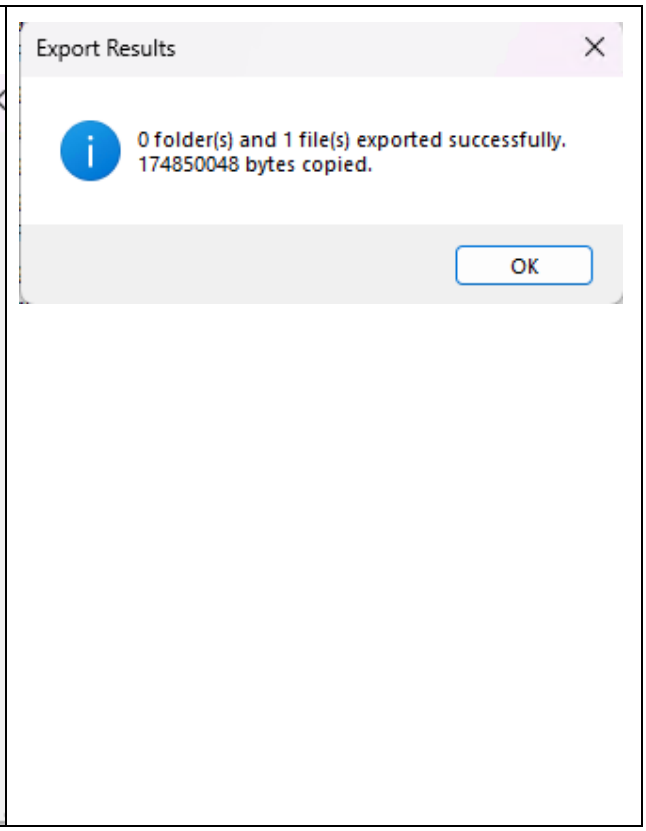


Figure 8: Obtaining the MFT with FTK Imager





🖫 Parsing the MFT with EZTools

1. Open a PowerShell window as an Administrator
2. Cd to <x>:\EZTools\Get-ZimmermanTools\ (or the location you downloaded them to).
3. We will use the tool called "MFTECmd.exe" to parse the MFT and create a csv of the output we can read.

```
PS F:\EZTools\Get-ZimmermanTools> .\MFTECmd.exe -f "D:\`$MFT" --csv
F:\MUS2019CTF\Exported\ --csvf MUS-CTF-19-DESKTOP-001-002.csv
```

- The command will also work the same on the exported file.

```
PS F:\EZTools\Get-ZimmermanTools> .\MFTECmd.exe -f
"F:\MUS2019CTF\Exported\`$MFT" --csv F:\MUS2019CTF\Exported\ --csvf
MUS-CTF-19-DESKTOP-001-002.csv
```

- You should now have a csv file ready for review.

Do you notice anything in that above command the file paths?

🖫 Tip

- You are going to get a lot of excel files, I tend to find its easier to create an xlsx file now and name it according to the system being analysed and then combining all artefact parse output into the one excel spreadsheet.
- To set up my sheet I do the following:
    a. View > Freeze Panes > Freeze Top Row
    b. With the top row still selected – Data > Filter
    c. Select columns T through AA
        i. Right click > format cells
        ii. Custom > Replace the words in General with
        iii. yyyy-mm-dd hh:mm:ss.000
            1. NOTE: ensuring that you have the milliseconds represented will stop any rounding which will change your answers.
    d. Save

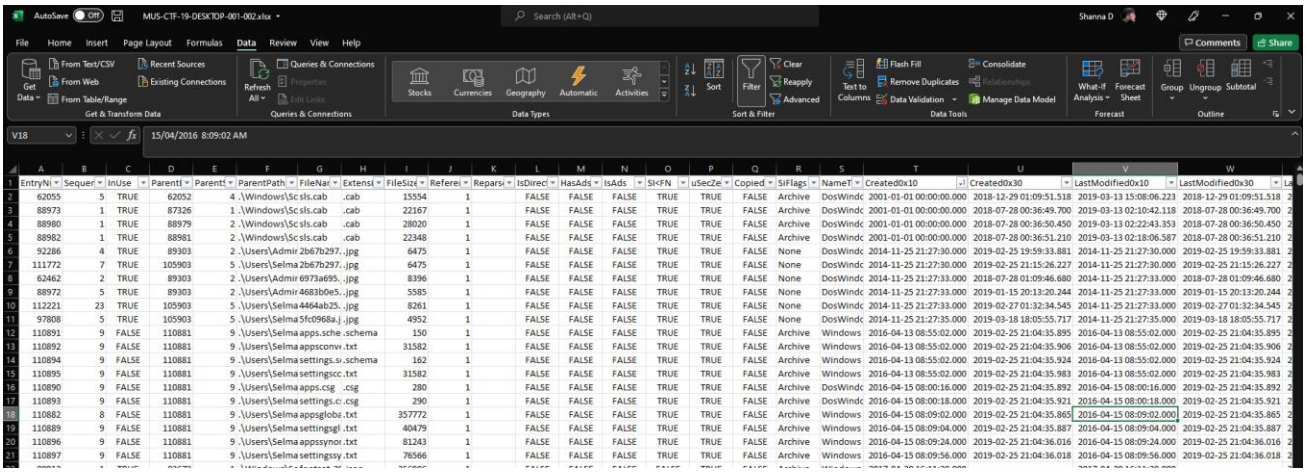
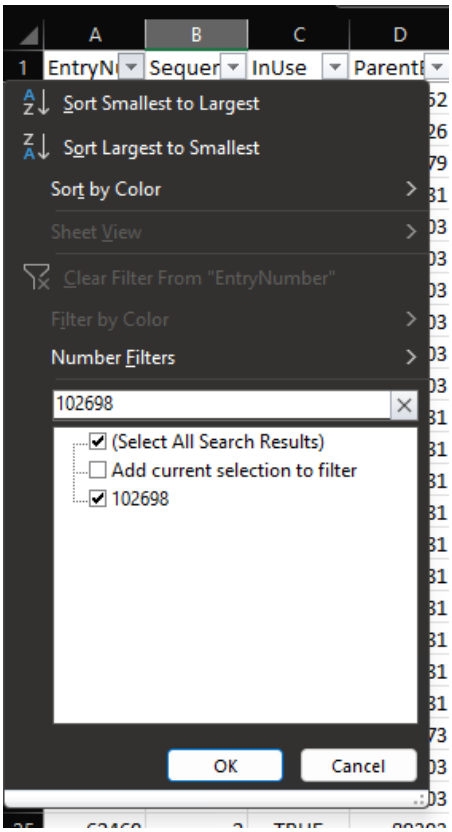
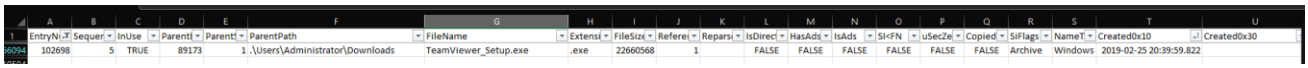


Figure 9: Excel Spreadsheet with MFT Output

4. What is the name of the file associated with MFT entry number 102698?

1. Column A of your spreadsheet should have the header “EntryNumber”.
2. Select the down arrow for the filter menu.
3. Type in 102698 and click OK.
4. The one line left will be the file you are after - TeamViewer_Setup.exe





EntryN	Sequer	InUse	Parent	Parent	ParentPath	FileName	Extens	FileSiz	Referei	Repars	IsDirec	HasAds	IsAds	SI<FN	uSec2e	Copied	SiFlags	NameT	Created0x10	Created0x30
102698	5	TRUE	89173	1	.\Users\Administrator\Downloads	TeamViewer_Setup.exe	.exe	22660568	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Windows	2019-02-25 20:39:59.822	

There is a column called Created0x10 and another called Created0x30. You will notice that there is two dates for LastModified, LastRecordChange and LastAccess as well. Why is that?

Flag	TeamViewer_Setup.exe

5. What is the MFT sequence number associated with the file "\Users\Administrator\Desktop\FTK_Imager_Lite_3.1.1\FTK Imager.exe"?

1. Clear the filter from the EntryNumber column.
2. Filter on Column G for the filename.
3. We'll see the SequenceNumber is 4.

Flag	4

Question	If you filter on "FTK Imager.exe", two files will be left. What is the other file in relation to?

6. What is the file name that represented MFT entry 60725 with a sequence number of 10?

1. Clear the filter from EntryNumber
2. Now when we filter on 60725 we get the SequenceNumber 15. But we want 10.

🖫 Autopsy

We can parse the USNJrnl in Autopsy. This usually takes quite a long to complete. You'll firstly need to ensure that you have downloaded and copied the Python parsers for Autopsy locally.

1. In Autopsy go to the Tools menu and select Run Ingest Modules and choose the evidence file.
2. Ingest Profile Selection > click next
3. Deselect All then scroll to find USN Parser.
4. The select finish.
5. Walk away and do something else.

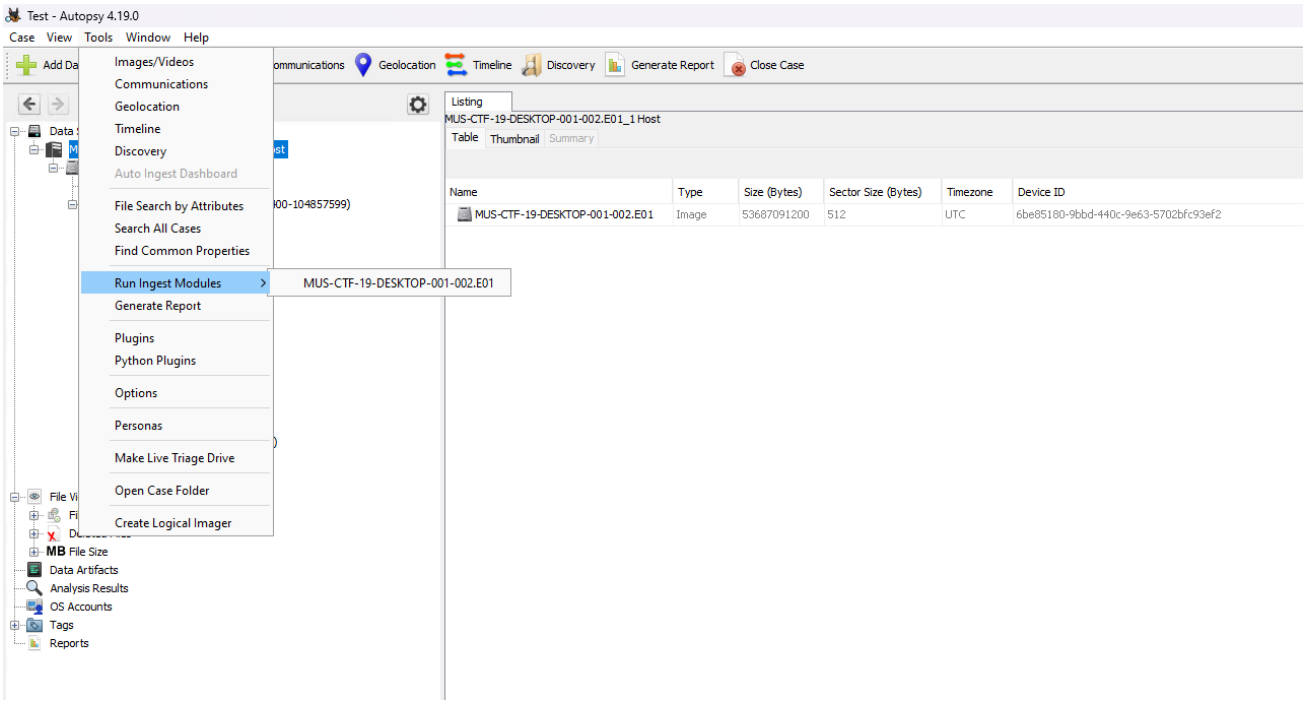
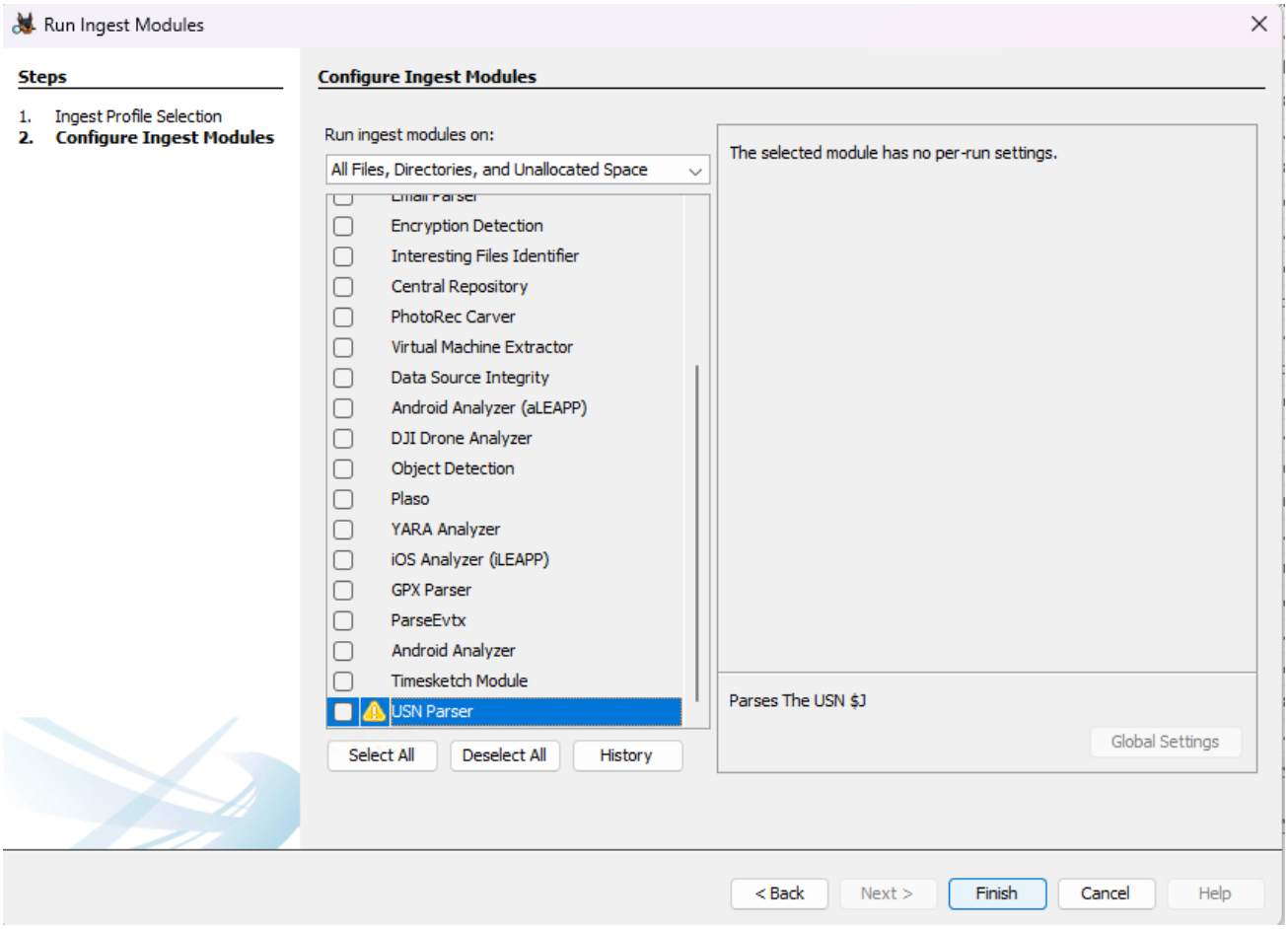


Figure 10: Use the USN Parser in Autopsy



While for this specific question I only need to run the USN Parser module, for nearly every image or files I add to Autopsy, the Recent Activity module comes in extremely handy.

- Recent Activity (should be relatively quick)
- USN Parser (may take some time to run)

As the parsers run, you will start to see the "Data Artifacts" tree on the left pane of Autopsy filling up with information and artefact names.

Figure 11: Ingest module progress in Autopsy

When it's done, under the Data Artifacts Tree there should be "NTFS UsrJrnl entries. Click on that, wait some more.

- We'll want to start by sorting my "MFT_Reference" and look for 60725, we'll then have each of the files and the sequence numbers.
- Find the file associated with the sequence number 10.

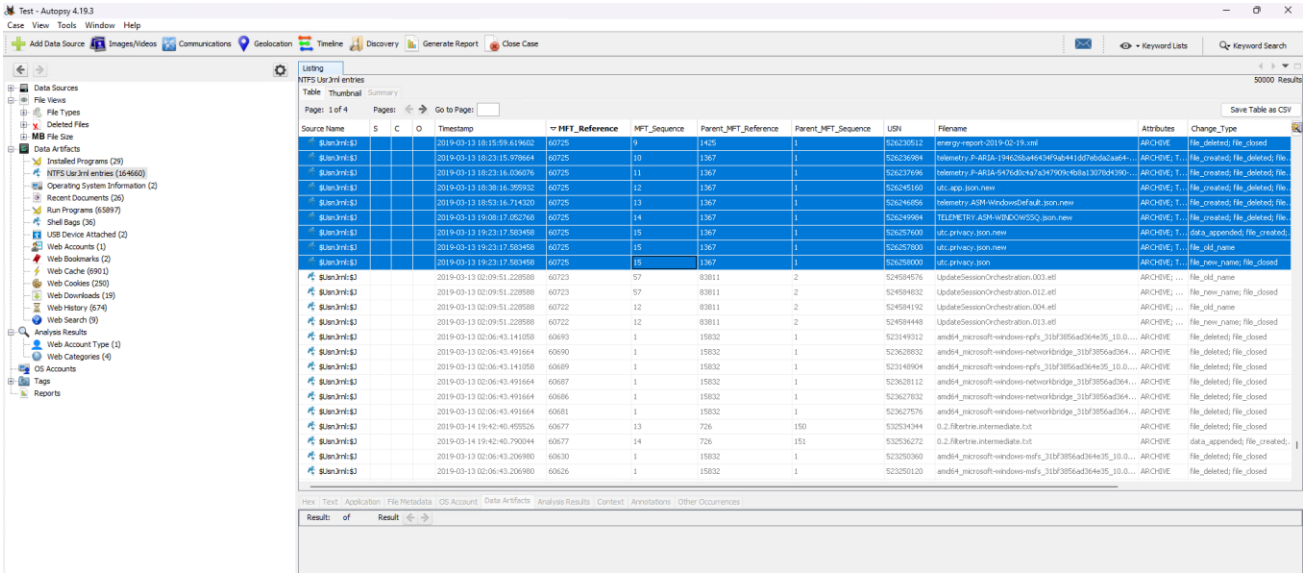


Figure 12: Find the MFT_Reference number 60725

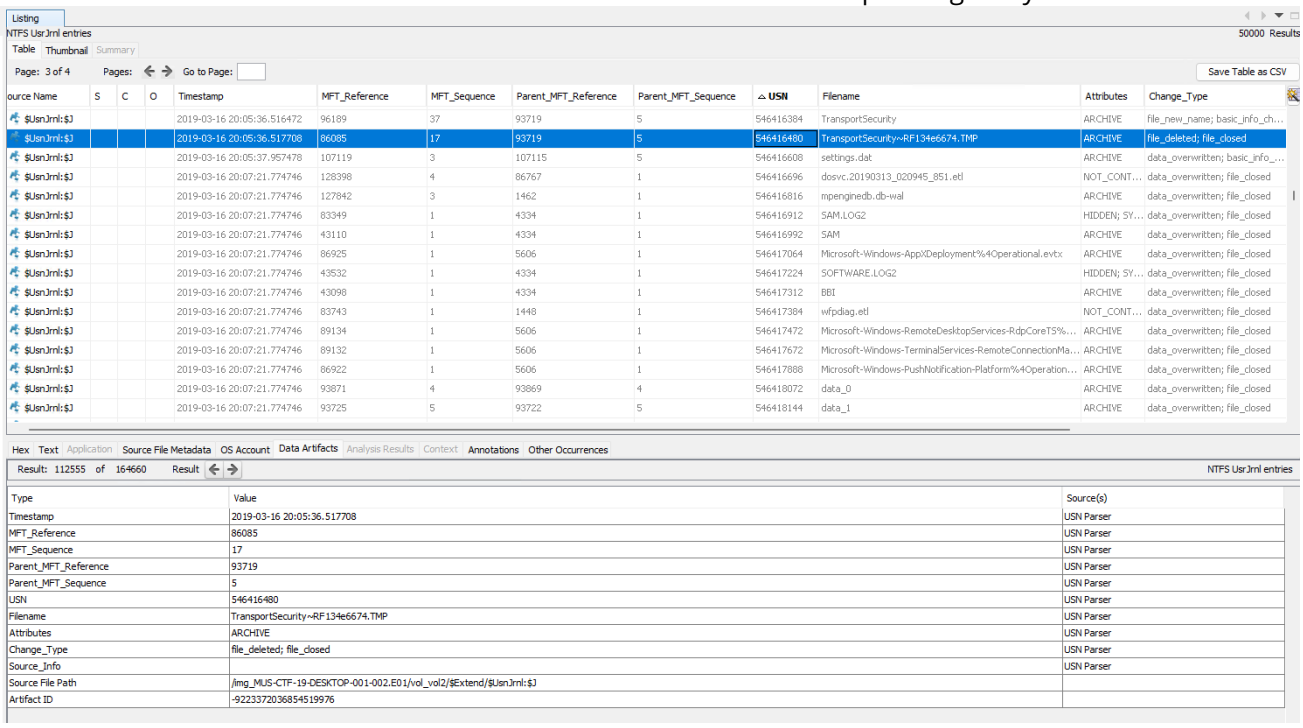
Type	Value
Timestamp	2019-03-13 18:23:15.978664
MFT_Reference	60725
MFT_Sequence	10
Parent_MFT_Reference	1367
Parent_MFT_Sequence	1
USN	526236984
Filename	telemetry.P-ARIA-194626ba46434f9ab441dd7ebda2aa64-5f64bebb-ac28-4cc7-bd52-570c8fe077c9-7717.json.new
Attributes	ARCHIVE; TEMPORARY
Change_Type	file_created; file_deleted; file_closed
Source_Info	
Source File Path	/img_MUS-CTF-19-DESKTOP-001-002.E01/vol_vol2/$Extend/$UsnJrnl:$J
Artifact ID	-9223372036854610616

Figure 13: MFT_Reference 60725 and sequence number 10

Flag	telemetry.P-ARIA-194626ba46434f9ab441dd7ebda2aa64-5f64bebb-ac28-4cc7-bd52-570c8fe077c9-7717.json.new

7. Which file name represents the USN record where the USN number is 546416480?

- Now we'll want to sort on the USN column and find the corresponding entry.



ource Name	S	C	O	Timestamp	MFT_Reference	MFT_Sequence	Parent_MFT_Reference	Parent_MFT_Sequence	USN	Filename	Attributes	Change_Type
$UsnJrnl:$J				2019-03-16 20:05:36.516472	96189	37	93719	5	546416384	TransportSecurity	ARCHIVE	file_new_name; basic_info_ch...
$UsnJrnl:$J				2019-03-16 20:05:36.517708	86085	17	93719	5	546416480	TransportSecurity~RF134e6674.TMP	ARCHIVE	file_deleted; file_closed
$UsnJrnl:$J				2019-03-16 20:05:37.957478	107119	3	107115	5	546416608	settings.dat	ARCHIVE	data_overwritten; basic_info_...
$UsnJrnl:$J				2019-03-16 20:07:21.774746	128398	4	86767	1	546416696	dosvc.20190313_020945_851.etl	NOT_CONT...	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	127842	3	1462	1	546416816	mpenginedb.db-wal	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	83349	1	4334	1	546416912	SAM.LOG2	HIDDEN; SY...	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	43110	1	4334	1	546416992	SAM	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	86925	1	5606	1	546417064	Microsoft-Windows-AppXDeployment%4Operational.evtx	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	43532	1	4334	1	546417224	SOFTWARE.LOG2	HIDDEN; SY...	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	43098	1	4334	1	546417312	BBI	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	83743	1	1448	1	546417384	wfpdiag.etl	NOT_CONT...	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	89134	1	5606	1	546417472	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%...	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	89132	1	5606	1	546417672	Microsoft-Windows-TerminalServices-RemoteConnectionMa...	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	86922	1	5606	1	546417888	Microsoft-Windows-PushNotification-Platform%4Operation...	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	93871	4	93869	4	546418072	data_0	ARCHIVE	data_overwritten; file_closed
$UsnJrnl:$J				2019-03-16 20:07:21.774746	93725	5	93722	5	546418144	data_1	ARCHIVE	data_overwritten; file_closed

Type	Value	Source(s)
Timestamp	2019-03-16 20:05:36.517708	USN Parser
MFT_Reference	86085	USN Parser
MFT_Sequence	17	USN Parser
Parent_MFT_Reference	93719	USN Parser
Parent_MFT_Sequence	5	USN Parser
USN	546416480	USN Parser
Filename	TransportSecurity~RF134e6674.TMP	USN Parser
Attributes	ARCHIVE	USN Parser
Change_Type	file_deleted; file_closed	USN Parser
Source_Info		USN Parser
Source File Path	/img_MUS-CTF-19-DESKTOP-001-002.E01/vol_vol2/$Extend/$UsnJrnl:$J	
Artifact ID	-9223372036854519976	

Figure 14: USN 546416480

Flag	TransportSecurity~RF134e6674.TMP

Registry Forensics

Obtaining and parsing registry files

🖫 Extracting the registry files with FTK Imager

Similarly, as with the MFT, the registry files can be extracted with FTK Imager, or with Arsenal Image Mounter.

Windows NT systems store the registry in a binary file format which can be exported[1], loaded and unloaded by the Registry Editor in these operating systems. The following system registry files are stored in %SystemRoot%\System32\Config\:

- Sam – HKEY_LOCAL_MACHINE\SAM
- Security – HKEY_LOCAL_MACHINE\SECURITY
- Software – HKEY_LOCAL_MACHINE\SOFTWARE
- System – HKEY_LOCAL_MACHINE\SYSTEM
- Default – HKEY_USERS\.DEFAULT
- The following file is stored in each user's profile folder:
    a. %USERPROFILE%\Ntuser.dat
    b. %USERPROFILE%\AppData\Local\Microsoft\Windows\Usrclass.dat

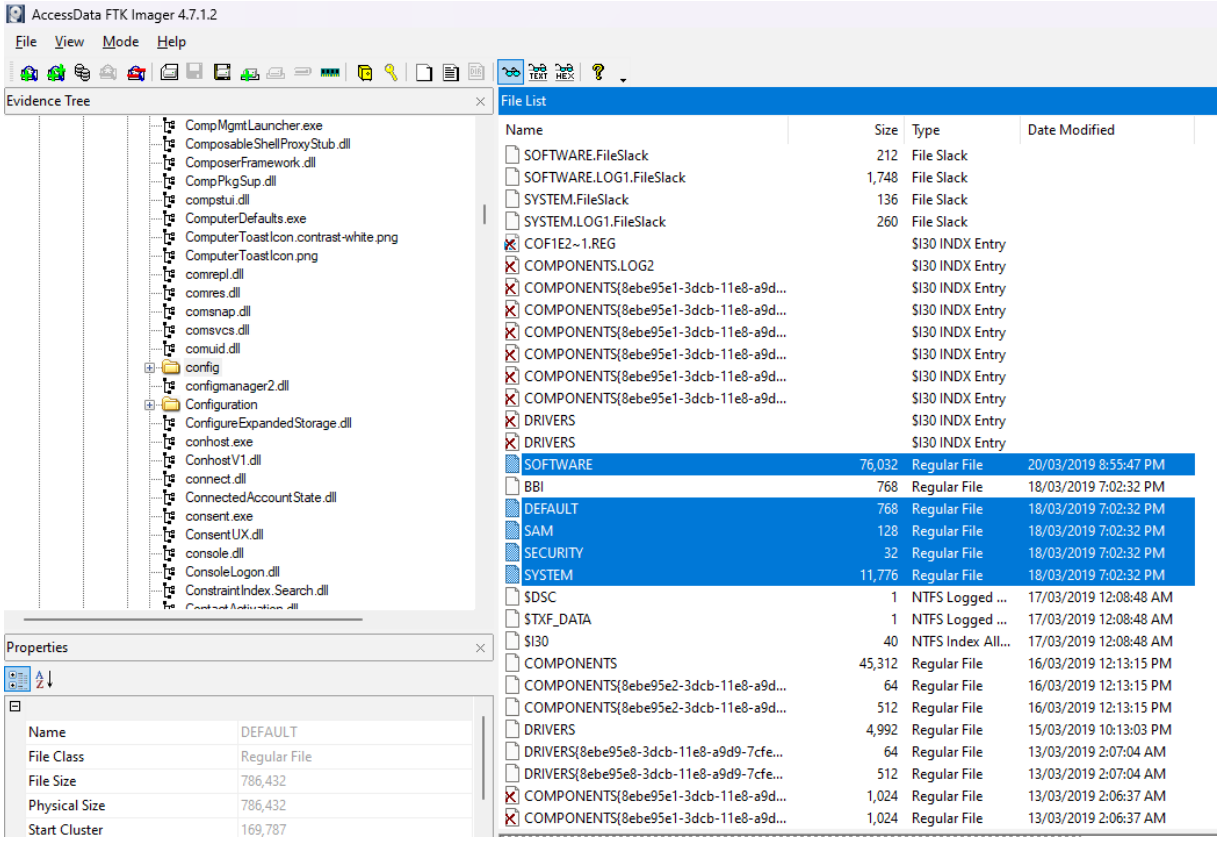
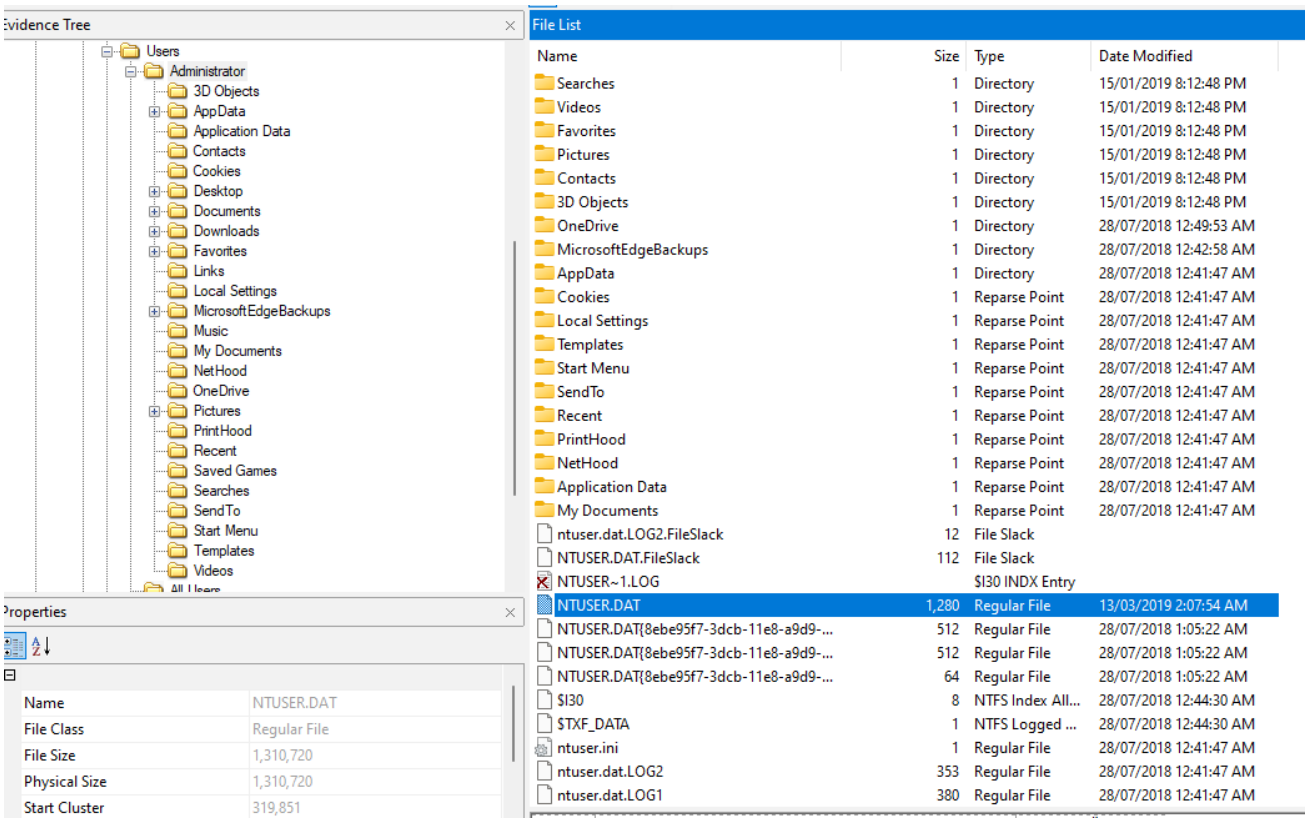
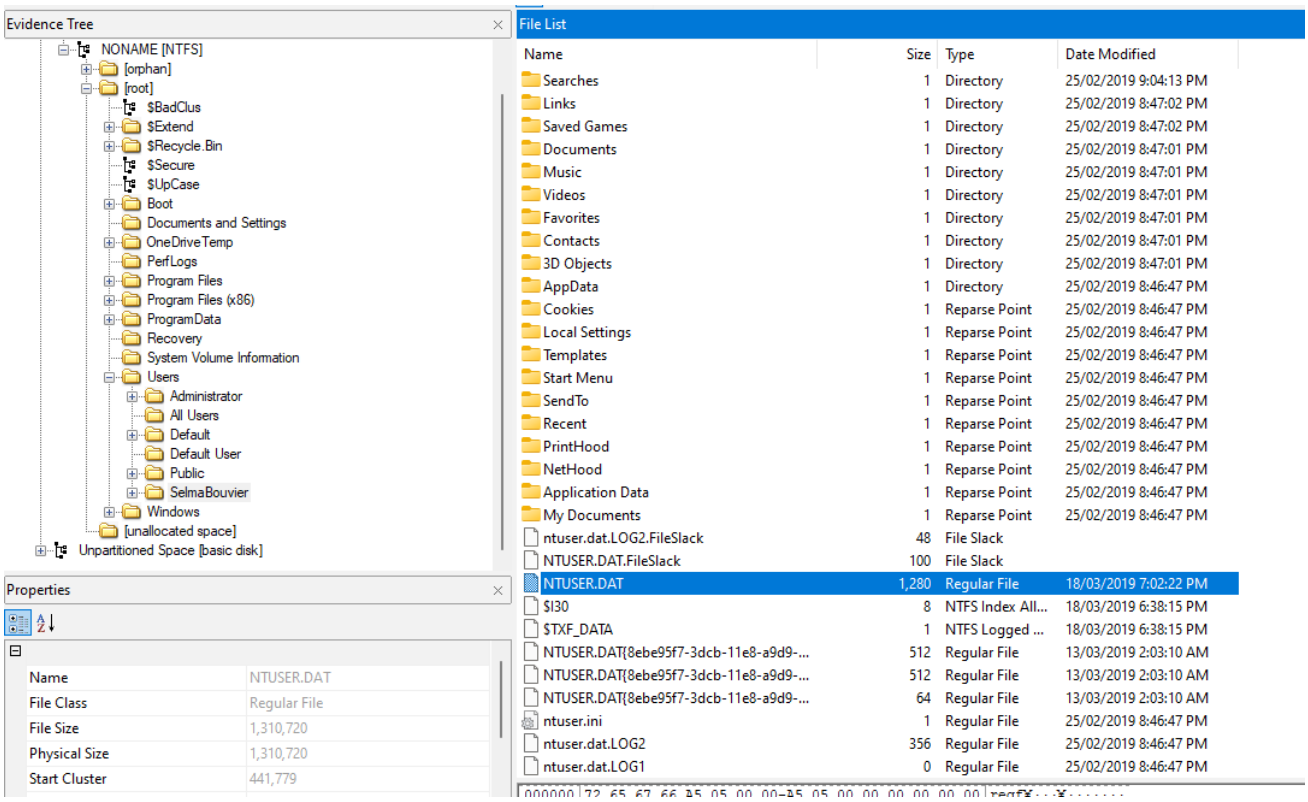
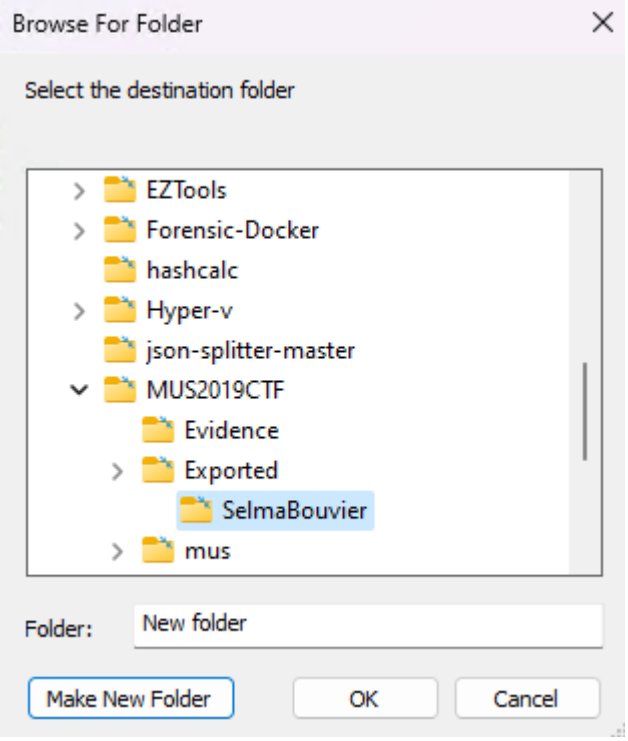


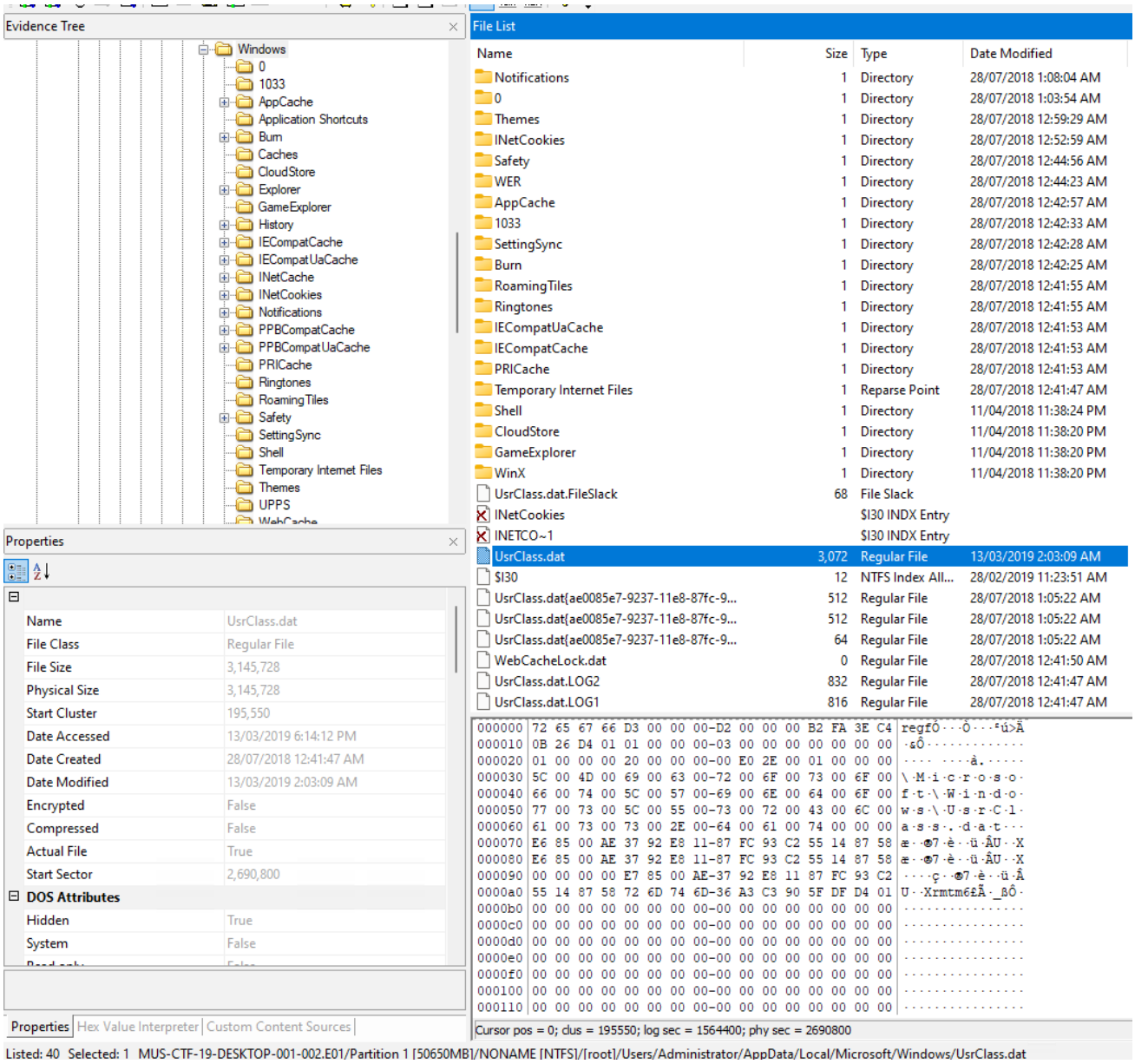
Figure 15: Select the 5 registry files from the image to export

1 https://en.wikipedia.org/wiki/Windows_Registry#:~:text=The%20location%20for%20system%20registry,hive%20is%20stored%20in%20Ntuser.


Evidence Tree
Users
Administrator
3D Objects
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Links
Local Settings
MicrosoftEdgeBackups
Music
My Documents
NetHood
OneDrive
Pictures
PrintHood
Recent
Saved Games
Searches
SendTo
Start Menu
Templates
Videos
Properties
Name NTUSER.DAT
File Class Regular File
File Size 1,310,720
Physical Size 1,310,720
Start Cluster 319,851
File List
Name Size Type Date Modified
Searches 1 Directory 15/01/2019 8:12:48 PM
Videos 1 Directory 15/01/2019 8:12:48 PM
Favorites 1 Directory 15/01/2019 8:12:48 PM
Pictures 1 Directory 15/01/2019 8:12:48 PM
Contacts 1 Directory 15/01/2019 8:12:48 PM
3D Objects 1 Directory 15/01/2019 8:12:48 PM
OneDrive 1 Directory 28/07/2018 12:49:53 AM
MicrosoftEdgeBackups 1 Directory 28/07/2018 12:42:58 AM
AppData 1 Directory 28/07/2018 12:41:47 AM
Cookies 1 Reparse Point 28/07/2018 12:41:47 AM
Local Settings 1 Reparse Point 28/07/2018 12:41:47 AM
Templates 1 Reparse Point 28/07/2018 12:41:47 AM
Start Menu 1 Reparse Point 28/07/2018 12:41:47 AM
SendTo 1 Reparse Point 28/07/2018 12:41:47 AM
Recent 1 Reparse Point 28/07/2018 12:41:47 AM
PrintHood 1 Reparse Point 28/07/2018 12:41:47 AM
NetHood 1 Reparse Point 28/07/2018 12:41:47 AM
Application Data 1 Reparse Point 28/07/2018 12:41:47 AM
My Documents 1 Reparse Point 28/07/2018 12:41:47 AM
ntuser.dat.LOG2.FileSlack 12 File Slack
NTUSER.DAT.FileSlack 112 File Slack
NTUSER~1.LOG $I30 INDX Entry
NTUSER.DAT 1,280 Regular File 13/03/2019 2:07:54 AM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 512 Regular File 28/07/2018 1:05:22 AM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 512 Regular File 28/07/2018 1:05:22 AM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 64 Regular File 28/07/2018 1:05:22 AM
$I30 8 NTFS Index All... 28/07/2018 12:44:30 AM
$TXF_DATA 1 NTFS Logged ... 28/07/2018 12:44:30 AM
ntuser.ini 1 Regular File 28/07/2018 12:41:47 AM
ntuser.dat.LOG2 353 Regular File 28/07/2018 12:41:47 AM
ntuser.dat.LOG1 380 Regular File 28/07/2018 12:41:47 AM


Evidence Tree
NONAME [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Recycle.Bin
$Secure
$UpCase
Boot
Documents and Settings
OneDriveTemp
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
System Volume Information
Users
Administrator
All Users
Default
Default User
Public
SelmaBouvier
Windows
[unallocated space]
Unpartitioned Space [basic disk]
Properties
Name NTUSER.DAT
File Class Regular File
File Size 1,310,720
Physical Size 1,310,720
Start Cluster 441,779
File List
Name Size Type Date Modified
Searches 1 Directory 25/02/2019 9:04:13 PM
Links 1 Directory 25/02/2019 8:47:02 PM
Saved Games 1 Directory 25/02/2019 8:47:02 PM
Documents 1 Directory 25/02/2019 8:47:01 PM
Music 1 Directory 25/02/2019 8:47:01 PM
Videos 1 Directory 25/02/2019 8:47:01 PM
Favorites 1 Directory 25/02/2019 8:47:01 PM
Contacts 1 Directory 25/02/2019 8:47:01 PM
3D Objects 1 Directory 25/02/2019 8:47:01 PM
AppData 1 Directory 25/02/2019 8:46:47 PM
Cookies 1 Reparse Point 25/02/2019 8:46:47 PM
Local Settings 1 Reparse Point 25/02/2019 8:46:47 PM
Templates 1 Reparse Point 25/02/2019 8:46:47 PM
Start Menu 1 Reparse Point 25/02/2019 8:46:47 PM
SendTo 1 Reparse Point 25/02/2019 8:46:47 PM
Recent 1 Reparse Point 25/02/2019 8:46:47 PM
PrintHood 1 Reparse Point 25/02/2019 8:46:47 PM
NetHood 1 Reparse Point 25/02/2019 8:46:47 PM
Application Data 1 Reparse Point 25/02/2019 8:46:47 PM
My Documents 1 Reparse Point 25/02/2019 8:46:47 PM
ntuser.dat.LOG2.FileSlack 48 File Slack
NTUSER.DAT.FileSlack 100 File Slack
NTUSER.DAT 1,280 Regular File 18/03/2019 7:02:22 PM
$I30 8 NTFS Index All... 18/03/2019 6:38:15 PM
$TXF_DATA 1 NTFS Logged ... 18/03/2019 6:38:15 PM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 512 Regular File 13/03/2019 2:03:10 AM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 512 Regular File 13/03/2019 2:03:10 AM
NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-... 64 Regular File 13/03/2019 2:03:10 AM
ntuser.ini 1 Regular File 25/02/2019 8:46:47 PM
ntuser.dat.LOG2 356 Regular File 25/02/2019 8:46:47 PM
ntuser.dat.LOG1 0 Regular File 25/02/2019 8:46:47 PM


Browse For Folder
Select the destination folder
EZTools
Forensic-Docker
hashcalc
Hyper-v
json-splitter-master
MUS2019CTF
Evidence
Exported
SelmaBouvier
mus
Folder:
New folder
Make New Folder
OK
Cancel


Evidence Tree
Windows
0
1033
AppCache
Application Shortcuts
Burn
Caches
CloudStore
Explorer
GameExplorer
History
IECompatCache
IECompatUaCache
INetCache
INetCookies
Notifications
PPBCompatCache
PPBCompatUaCache
PRICache
Ringtones
RoamingTiles
Safety
SettingSync
Shell
Temporary Internet Files
Themes
UPPS
File List
Name Size Type Date Modified
Notifications 1 Directory 28/07/2018 1:08:04 AM
0 1 Directory 28/07/2018 1:03:54 AM
Themes 1 Directory 28/07/2018 12:59:29 AM
INetCookies 1 Directory 28/07/2018 12:52:59 AM
Safety 1 Directory 28/07/2018 12:44:56 AM
WER 1 Directory 28/07/2018 12:44:23 AM
AppCache 1 Directory 28/07/2018 12:42:57 AM
1033 1 Directory 28/07/2018 12:42:33 AM
SettingSync 1 Directory 28/07/2018 12:42:28 AM
Burn 1 Directory 28/07/2018 12:42:25 AM
RoamingTiles 1 Directory 28/07/2018 12:41:55 AM
Ringtones 1 Directory 28/07/2018 12:41:55 AM
IECompatUaCache 1 Directory 28/07/2018 12:41:53 AM
IECompatCache 1 Directory 28/07/2018 12:41:53 AM
PRICache 1 Directory 28/07/2018 12:41:53 AM
Temporary Internet Files 1 Reparse Point 28/07/2018 12:41:47 AM
Shell 1 Directory 11/04/2018 11:38:24 PM
CloudStore 1 Directory 11/04/2018 11:38:20 PM
GameExplorer 1 Directory 11/04/2018 11:38:20 PM
WinX 1 Directory 11/04/2018 11:38:20 PM
UsrClass.dat.FileSlack 68 File Slack
INetCookies $I30 INDX Entry
INETCO~1 $I30 INDX Entry
UsrClass.dat 3,072 Regular File 13/03/2019 2:03:09 AM
$I30 12 NTFS Index All... 28/02/2019 11:23:51 AM
UsrClass.dat{ae0085e7-9237-11e8-87fc-9... 512 Regular File 28/07/2018 1:05:22 AM
UsrClass.dat{ae0085e7-9237-11e8-87fc-9... 512 Regular File 28/07/2018 1:05:22 AM
UsrClass.dat{ae0085e7-9237-11e8-87fc-9... 64 Regular File 28/07/2018 1:05:22 AM
WebCacheLock.dat 0 Regular File 28/07/2018 12:41:50 AM
UsrClass.dat.LOG2 832 Regular File 28/07/2018 12:41:47 AM
UsrClass.dat.LOG1 816 Regular File 28/07/2018 12:41:47 AM
Properties
Name UsrClass.dat
File Class Regular File
File Size 3,145,728
Physical Size 3,145,728
Start Cluster 195,550
Date Accessed 13/03/2019 6:14:12 PM
Date Created 28/07/2018 12:41:47 AM
Date Modified 13/03/2019 2:03:09 AM
Encrypted False
Compressed False
Actual File True
Start Sector 2,690,800
DOS Attributes
Hidden True
System False
Properties Hex Value Interpreter Custom Content Sources
Cursor pos = 0; clus = 195550; log sec = 1564400; phy sec = 2690800
Listed: 40 Selected: 1 MUS-CTF-19-DESKTOP-001-002.E01/Partition 1 [50650MB]/NONAME [NTFS]/[root]/Users/Administrator/AppData/Local/Microsoft/Windows/UsrClass.dat

```
.
├── ./$MFT
├── ./$MFT.copy0
├── ./Administrator
│   ├── ./Administrator/NTUSER.DAT
│   └── ./Administrator/UsrClass.dat
├── ./DEFAULT
├── ./MUS-CTF-19-DESKTOP-001-002.csv
├── ./MUS-CTF-19-DESKTOP-001-002.xlsx
├── ./SAM
├── ./SECURITY
├── ./SOFTWARE
├── ./SYSTEM
└── ./SelmaBouvier
    ├── ./SelmaBouvier/NTUSER.DAT
    └── ./SelmaBouvier/UsrClass.dat

2 directories, 13 files
```

🖫 Arsenal Image Mounter

Instead of exporting the file from the evidence image, we can “Read-Only” mount the evidence image and assign a drive letter that is accessible in Windows Explorer.

1. Start Arsenal Image Mounter and from the home page choose “Mount disk Image”.
2. Browse to the evidence image file and open.
3. Under Mount options, leave “Read only disk device” selected and click OK.
4. Clicking on the + symbol beside the mounted device will show you the drive information and Windows mount point.
5. You can then open windows explorer and you should see the files under that mount point letter.

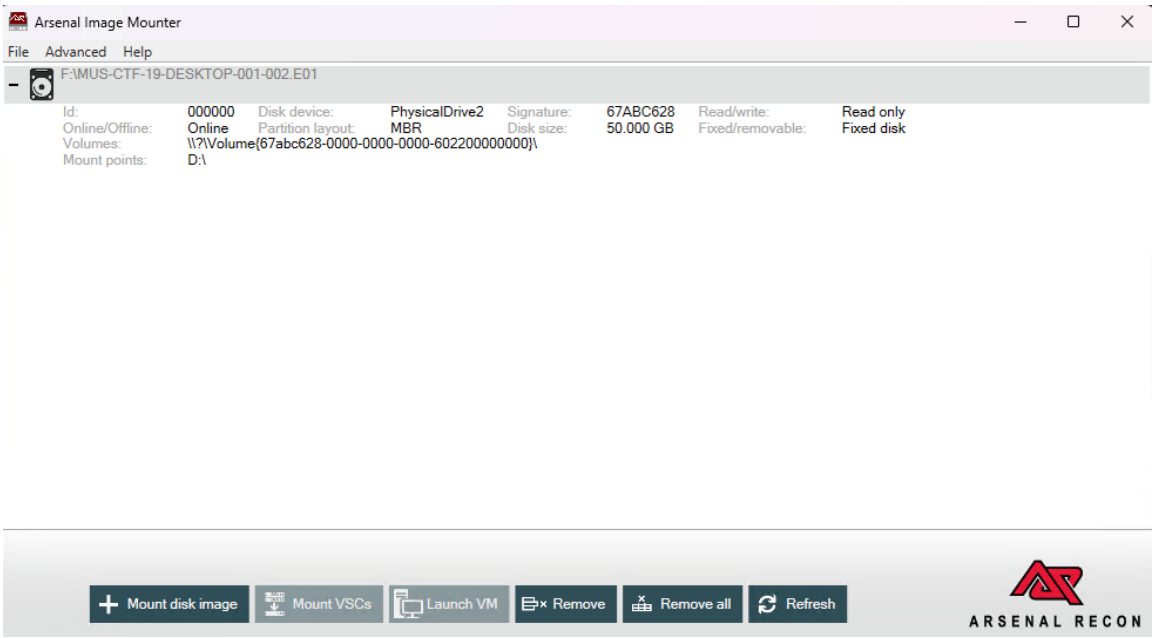


Figure 16: Arsenal Image Mounter

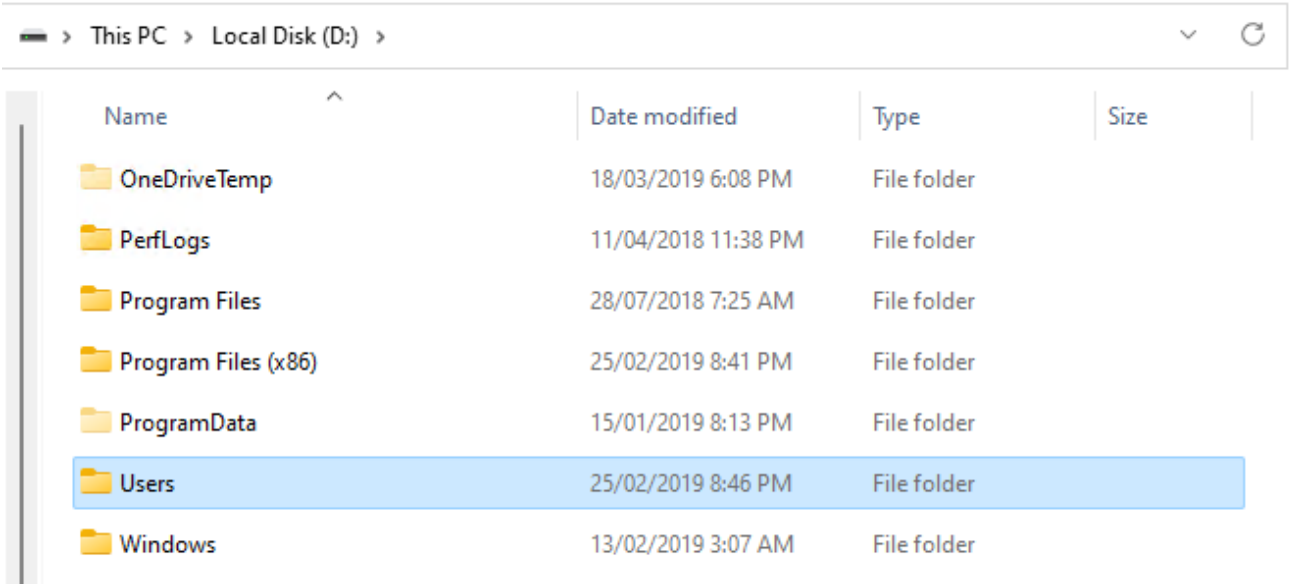


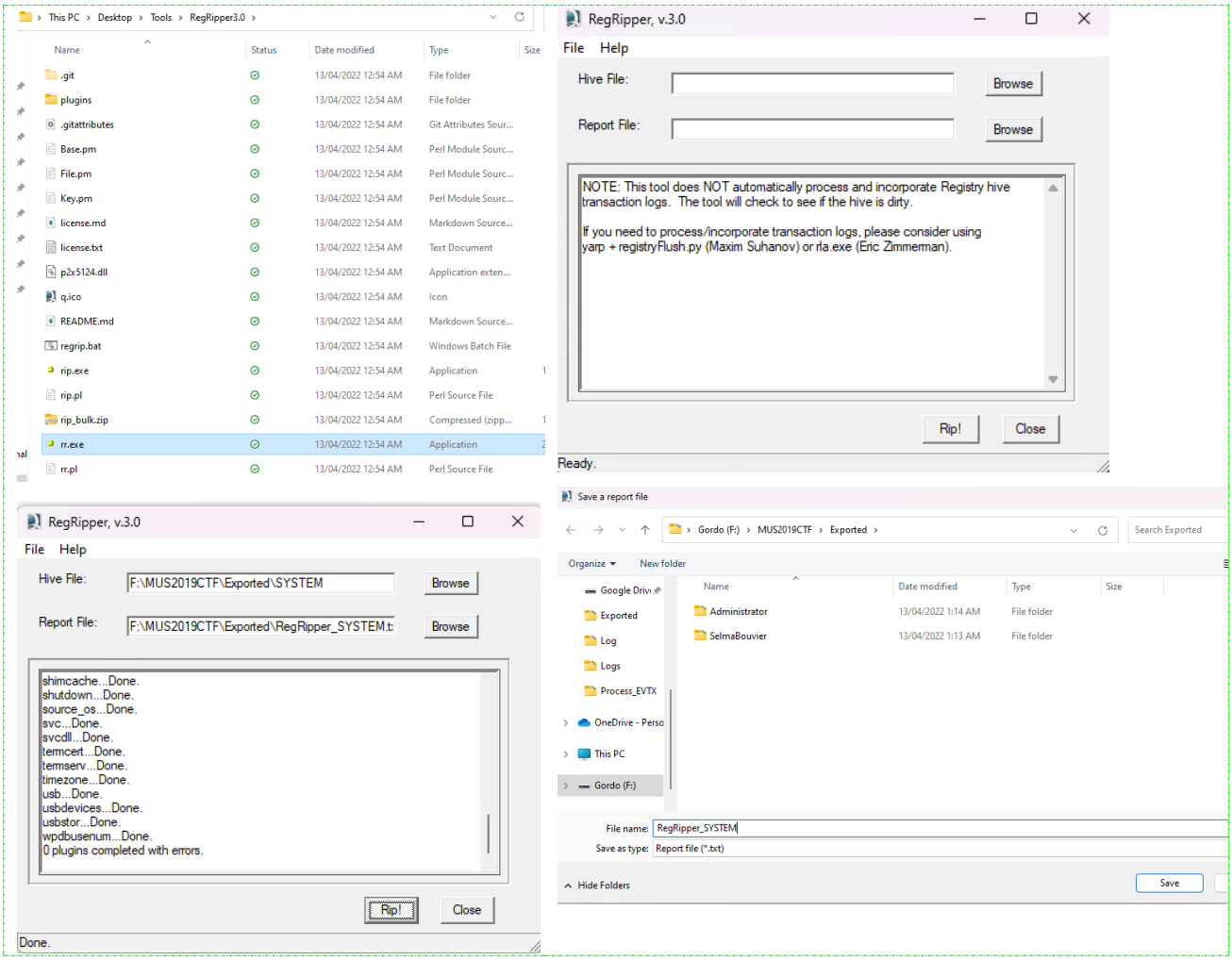
Figure 17: Windows Explorer Showing the Mounted Drive

NOW YOU HAVE THE FILES AVAILABLE AS EITHER A READ ONLY FILE MOUNTED IN WINDOWS EXPLORER (IN MY EXAMPLE D:\) OR THE FILES DOWNLOADED LOCALLY (F:\MUS2019CTF\EXPORTED)

RegRipper

Now we have our registry files it's time to make them human readable.

- Run rr.exe from the RegRipper3 folder to start the GUI.
- Select the hive file from either the read only mounted drive (D:\) or the locally downloaded copy.
- Choose where to save the report and give it a name.



- Do this for all the registry files to have them prepared to answer the questions. You'll end up with two files for each registry hive parsed (txt and log).

8. What was the timezone offset at the time of imaging?

I would not expect you to remember these things until you have done them several times, google is your friend, as are cheatsheets - https://www.13cubed.com/downloads/dfir_cheat_sheet.pdf

---

Miscellaneous Info:

HKLM\SYSTEM*CurrentControlSet*\Control\TimeZoneInformation
HKLM\SYSTEM*CurrentControlSet*\Control\ComputerName\ComputerName

---

HKLM\SYSTEM*CurrentControlSet*\services\LanmanServer\Shares

- Display all open shares on a system

HKLM\SYSTEM*CurrentControlSet*\Control\FileSystem

- Look for **NtfsDisableLastAccessUpdate**, which is set to 0x1 by default, which means that access time stamps are turned OFF by default

HKLM\SYSTEM*CurrentControlSet*\services\Tcpip\Parameters\Interfaces

- Display interfaces and their associated IP address configuration (record the interface GUID!)

Figure 18: Cheatsheet lets us know to check the SYSTEM hive

RegRipper

the registry key KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation where the field ActiveTimeBias will return the offset in minutes from GMT for the machine that you are running on. The answer we needed is in the hours.

```
7651  ----------------------------------------
7652  timezone v.20200518
7653  (System) Get TimeZoneInformation key contents
7654
7655  TimeZoneInformation key
7656  ControlSet001\Control\TimeZoneInformation
7657  LastWrite Time 2019-03-10 10:00:00Z
7658    DaylightName   -> @tzres.dll,-211
7659    StandardName   -> @tzres.dll,-212
7660    Bias           -> 480 (8 hours)
7661    ActiveTimeBias -> 420 (7 hours)
7662    TimeZoneKeyName-> Pacific Standard Time
7663  ----------------------------------------
```

Figure 19:: RegRipper output from RegRipper_SYSTEM.txt

Flag	7

9.What is the timezone of the desktop station?

The SYSTEM hive is where the version of the Windows OS is installed. We can simply search the RegRipper output to find the answer.

RegRipper

```
7651  ----------------------------------------
7652  timezone v.20200518
7653  (System) Get TimeZoneInformation key contents
7654
7655  TimeZoneInformation key
7656  ControlSet001\Control\TimeZoneInformation
7657  LastWrite Time 2019-03-10 10:00:00Z
7658    DaylightName   -> @tzres.dll,-211
7659    StandardName   -> @tzres.dll,-212
7660    Bias           -> 480 (8 hours)
7661    ActiveTimeBias -> 420 (7 hours)
7662    TimeZoneKeyName-> Pacific Standard Time
7663  ----------------------------------------
```

Figure 20: RegRipper output from RegRipper_SYSTEM.txt

Flag	Pacific Standard Time

10. What is the IP address of the Desktop?

Still looking at the SYSTEM hive output from RegRipper or Autopsy.

```
918  ----------------------------------------
919  ips v.20200518
920  (System) Get IP Addresses and domains (DHCP,static)
921
922  IPAddress            Domain
923  64.44.141.76
924  ----------------------------------------
```

Figure 21: IP Configuration in the SYSTEM hive

Flag	64.44.141.76

11. When was the Windows OS installed?

The SOFTWARE hive is where the version of the Windows OS is installed. We can simply search the RegRipper output to find the answer.

RegRipper

```
41216   ----------------------------------------
41217   winver v.20200525
41218   (Software) Get Windows version & build info
41219
41220   ProductName             Windows 10 Enterprise
41221   ReleaseID               1803
41222   BuildLab                17134.rs4_release.180410-1804
41223   BuildLabEx              17134.1.amd64fre.rs4_release.180410-1804
41224   CompositionEditionID    Enterprise
41225   RegisteredOrganization
41226   RegisteredOwner         User
41227   InstallDate             2018-07-28 07:27:53Z
41228   InstallTime             2018-07-28 07:27:53Z
41229   ----------------------------------------
```

Figure 22: RegRipper_Software.txt output showing windows OS version

Autopsy

If you ran the Recent Activity Ingest Module in Autopsy then RegRipper will have been run for you. You can access the output via the reports, then selecting the hive report, right click and open report.

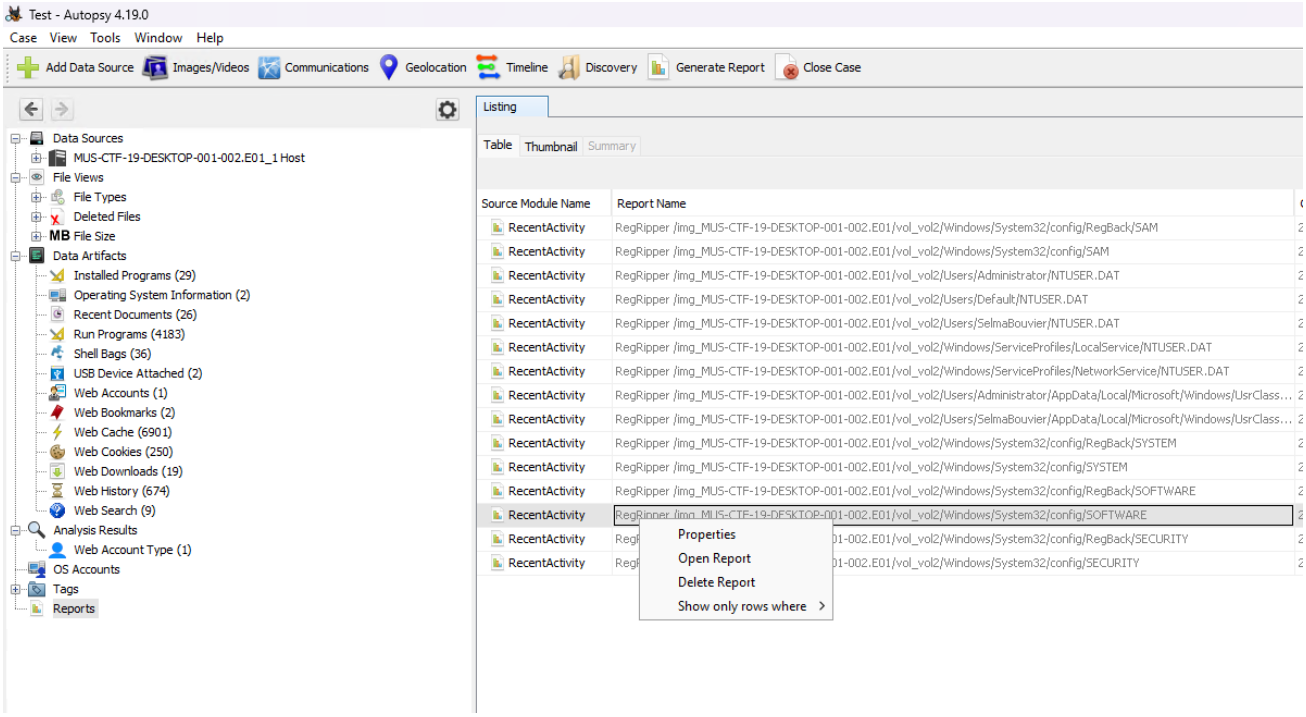


Figure 23: Autopsy Reports Window

```
----------------------------------------
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Enterprise
InstallDate = Sat Jul 28 07:27:53 2018
----------------------------------------
```

Figure 24: RegRipper SOFTWARE report from Autopsy

- You might notice there is a difference in the output of the two versions of RegRipper. The older version in Autopsy 4.19.0 contains less detail that the most up to date version.

Flag	2018-07-28 07:27:53 (GMT, Z, +00:00)

12. Which User Shutdown Windows on February 25th 2019?

- Event ID 1074: Logged when an app (such as Windows Update) causes the system to restart, or when a user initiates a restart or shutdown.
- We'll find that EventID in the SYSTEM eventlog.

🖫 Obtain the EventLog Files &/or Directory with FTK Imager

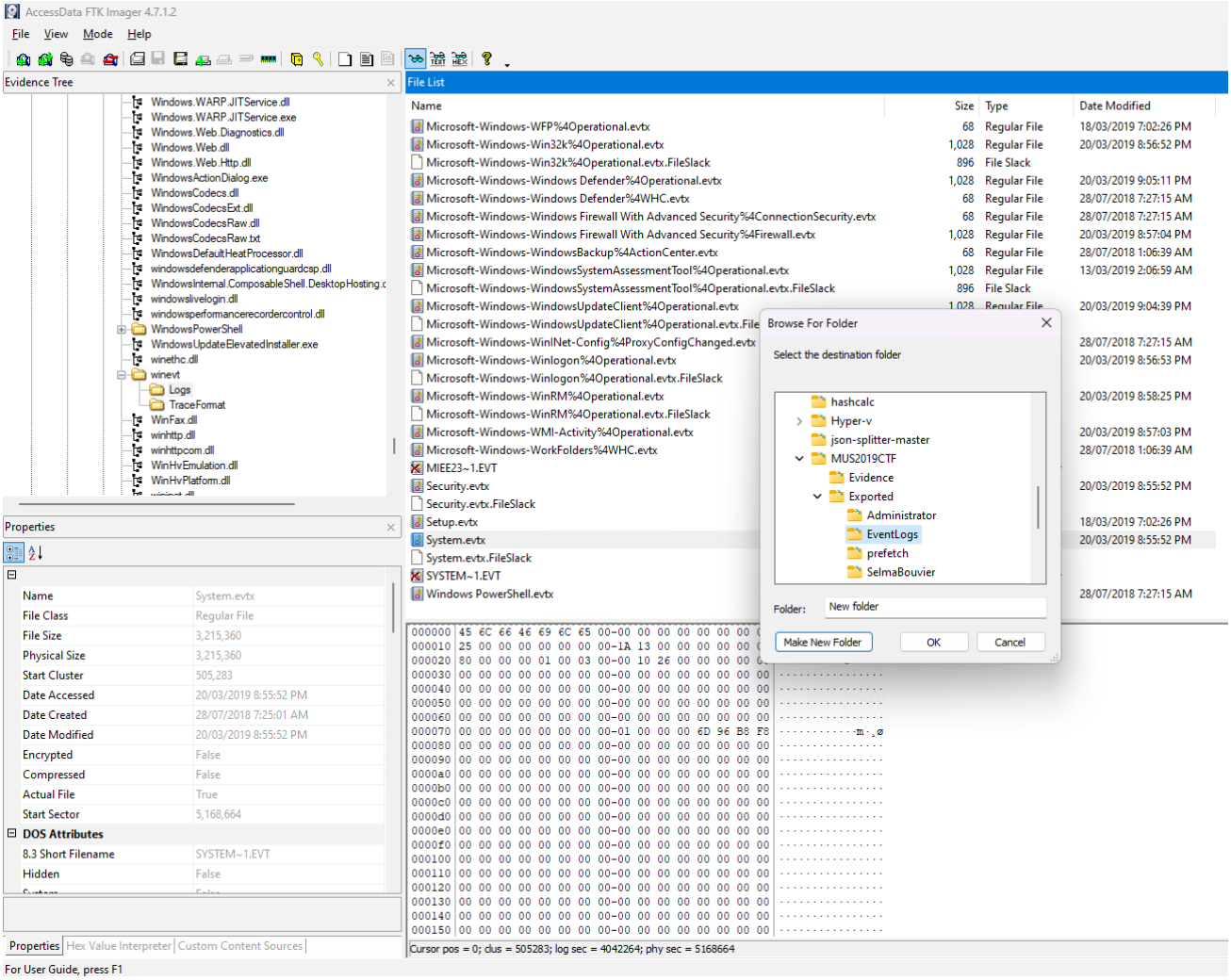


Figure 25: Exporting eventlogs with FTK Imager

🖫 EZTools – EvtxECmd.exe

- I'm going to create the csv file with EZTools and then import the data into my xlsx spreadsheet.

```
PS F:\EZTools\Get-ZimmermanTools\EvtxECmd> .\EvtxECmd.exe -f
F:\MUS2019CTF\Exported\EventLogs\System.evtx --csv "F:\MUS2019CTF\" -
-csvf system_evtlogs.csv
```

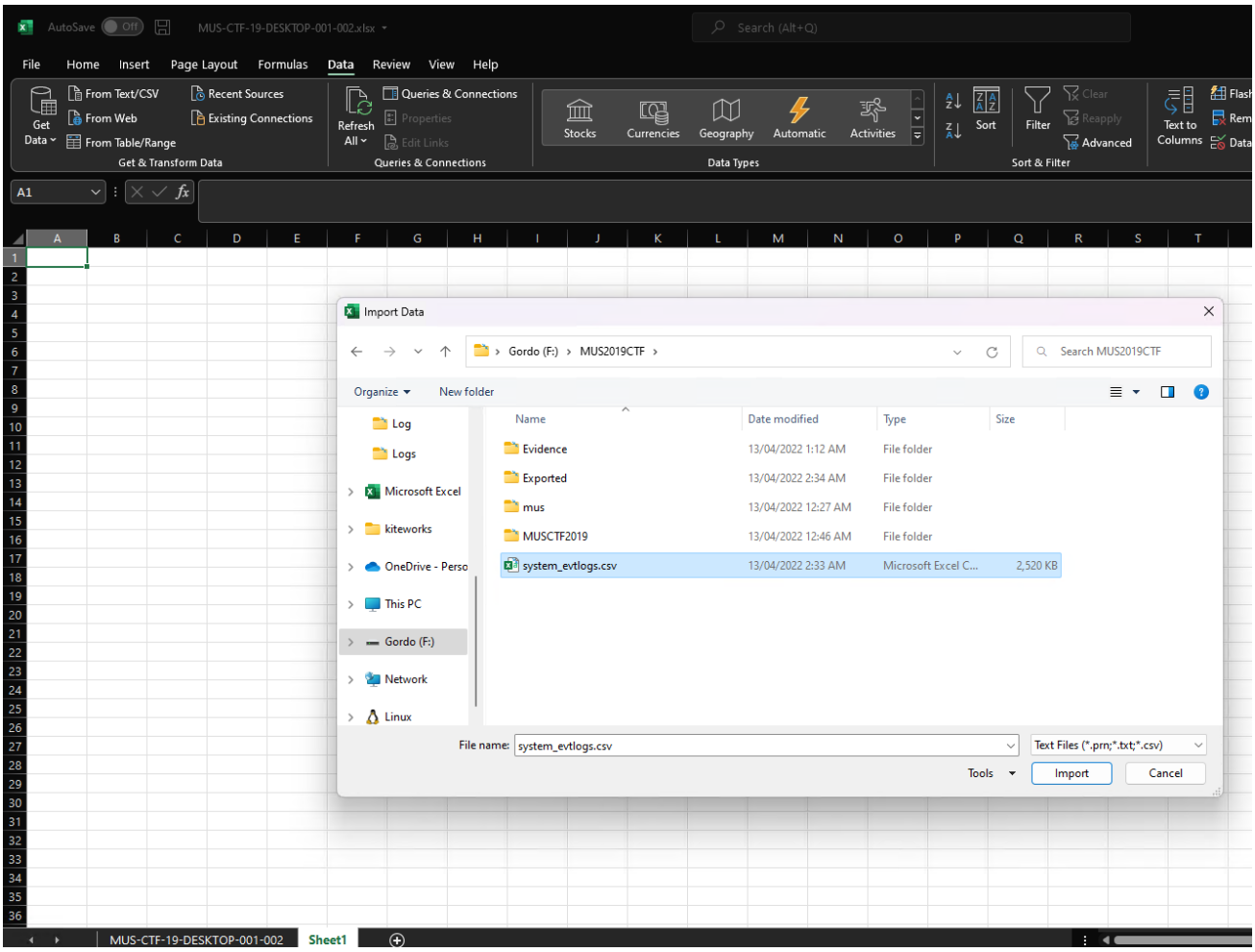
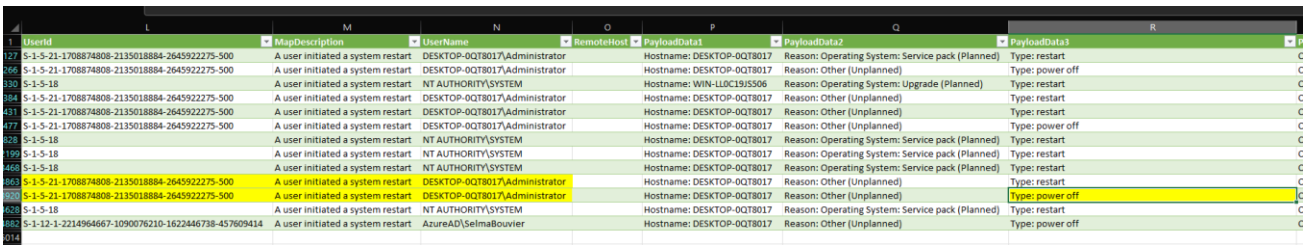


Figure 26: Import the csv data as a new sheet

- Filter on 1074 event ID and payloadData3 column for “Type: power off”

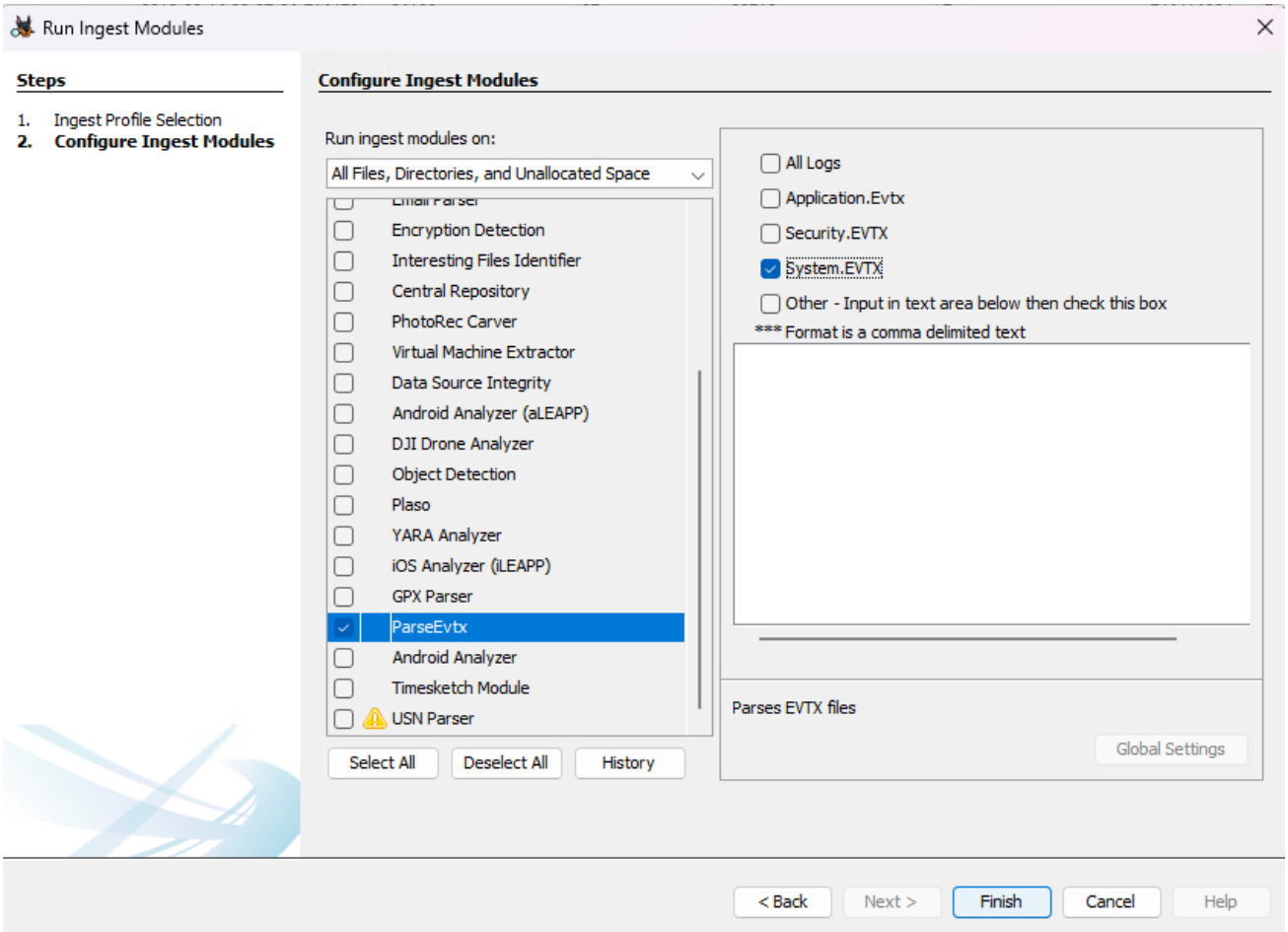


UserId	MapDescription	UserName	RemoteHost	PayloadData1	PayloadData2	PayloadData3
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Operating System: Service pack (Planned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: power off
S-1-5-18	A user initiated a system restart	NT AUTHORITY\SYSTEM		Hostname: WIN-LL0C19JS506	Reason: Operating System: Upgrade (Planned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: power off
S-1-5-18	A user initiated a system restart	NT AUTHORITY\SYSTEM		Hostname: DESKTOP-0QT8017	Reason: Operating System: Service pack (Planned)	Type: restart
S-1-5-18	A user initiated a system restart	NT AUTHORITY\SYSTEM		Hostname: DESKTOP-0QT8017	Reason: Operating System: Service pack (Planned)	Type: restart
S-1-5-18	A user initiated a system restart	NT AUTHORITY\SYSTEM		Hostname: DESKTOP-0QT8017	Reason: Operating System: Service pack (Planned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: restart
S-1-5-21-1708874808-2135018884-2645922275-500	A user initiated a system restart	DESKTOP-0QT8017\Administrator		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: power off
S-1-5-18	A user initiated a system restart	NT AUTHORITY\SYSTEM		Hostname: DESKTOP-0QT8017	Reason: Operating System: Service pack (Planned)	Type: restart
S-1-12-1-2214964667-1090076210-1622446738-457609414	A user initiated a system restart	AzureAD\SelmaBouvier		Hostname: DESKTOP-0QT8017	Reason: Other (Unplanned)	Type: power off

Figure 27: Finding the EventID in the csv data

Autopsy

- Go back to Autopsy and run another ingest module on the evidence.
- Deselect all and then choose “ParseEvtx”. Select SYSTEM from the right hand side.



- When the module has finished running the results will show under Data Artifacts > Windows Event Logs
- Sort by Event Identifier and find 1074

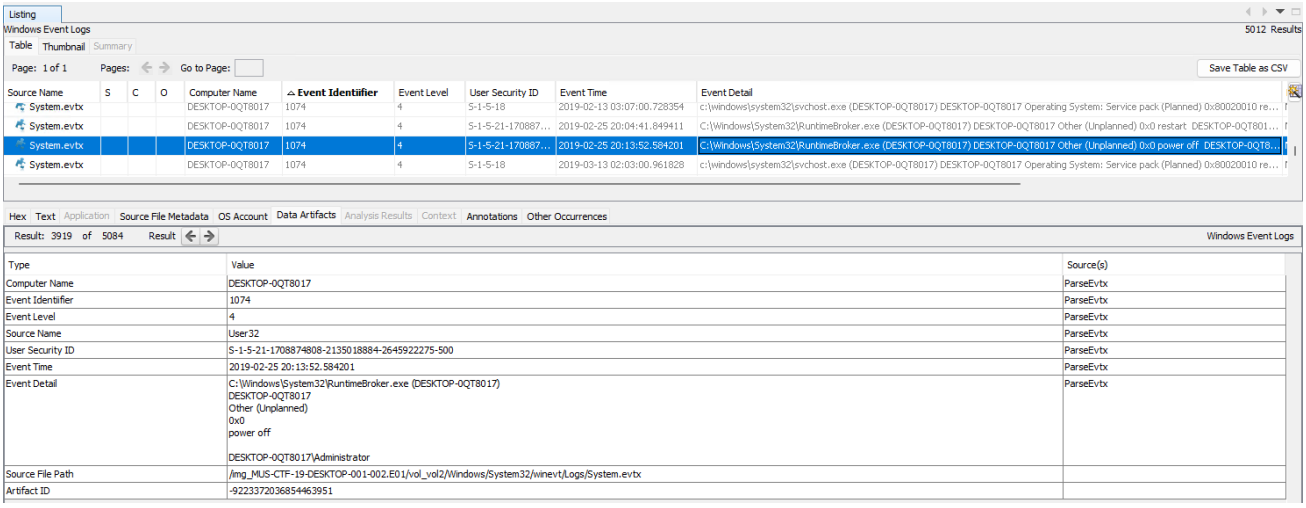


Figure 28:EventID 1074 and Powered Off Event Detail

Flag	Administrator

13. Which user installed TeamViewer?

- We saw in a previous question the Teamviewer setup file location in Users\Administrator\Downloads. But we don't want to assume they installed it.
- /img_MUS-CTF-19-DESKTOP-001-002.E01/vol_vol2/Users/Administrator/AppData/Local/Temp/TeamViewer/TV14Install.log confirms it.

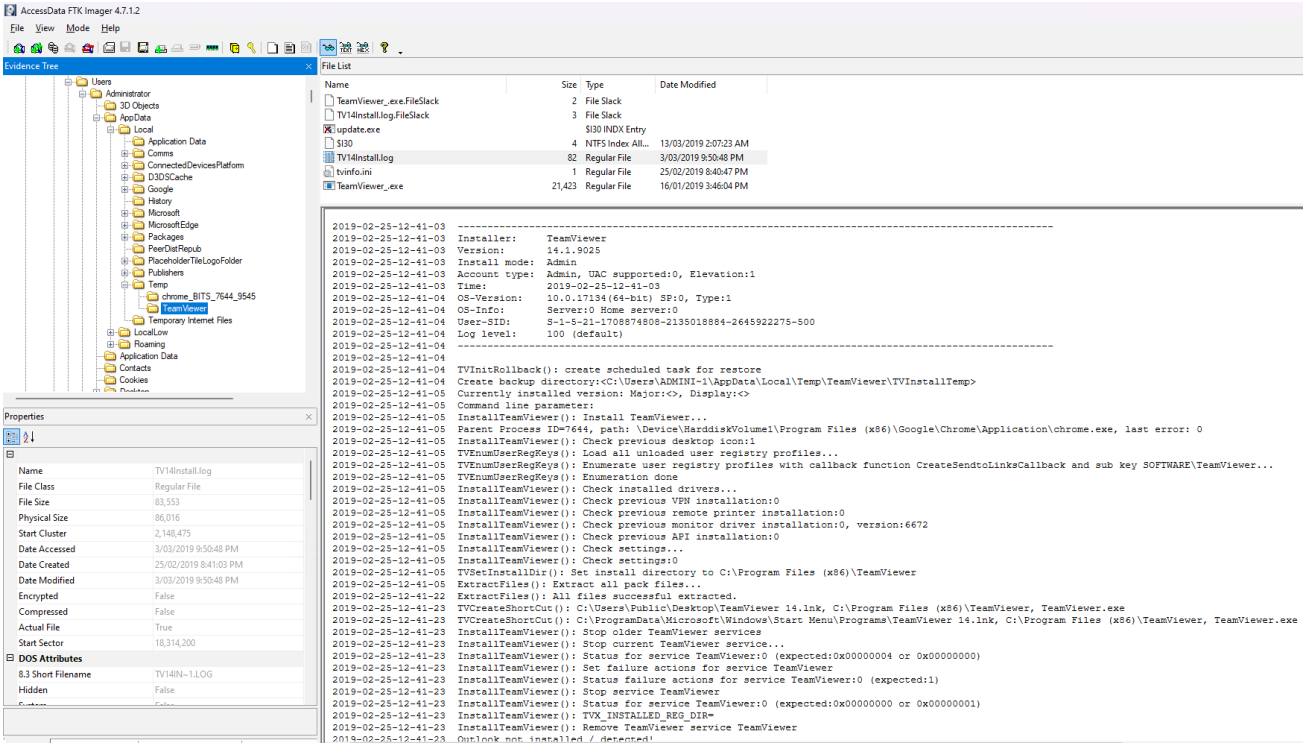


Figure 29: TeamViwer install log left on disk

Flag	Administrator

14. At least how many times did teamviewer_desktop.exe run?

- We'll need to obtain our prefetch files again.
  a. FTK Imager
  b. Mounted with Arsenal Image Mounter

EZTools – PECmd.exe

- You can run it across the whole directory of prefetch files or just specify one. IN this case we know the prefetch file we want to look at.

```
PS F:\EZTools\Get-ZimmermanTools> .\PECmd.exe -f
F:\MUS2019CTF\Exported\prefetch\TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf
```

- We'll then see the output on screen.

```
PS F:\EZTools\Get-ZimmermanTools> .\PECmd.exe -f F:\MUS2019CTF\Exported\prefetch\TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf
PECmd version 1.5.0.0

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

Command line: -f F:\MUS2019CTF\Exported\prefetch\TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf

Keywords: temp, tmp

Processing F:\MUS2019CTF\Exported\prefetch\TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf

Created on: 2019-03-18 17:59:30
Modified on: 2019-03-18 18:36:59
Last accessed on: 2022-04-13 02:18:25

Executable name: TEAMVIEWER_DESKTOP.EXE
Hash: 5B788ED3
File size (bytes): 81,350
Version: Windows 10 or Windows 11

Run count: 3
Last run: 2019-03-18 18:36:49
Other run times: 2019-03-18 18:34:19, 2019-03-18 17:59:20

Volume information:

#0: Name: \VOLUME{01d4264bee777579-ccee841b} Serial: CCEE841B Created: 2018-07-28 08:21:06 Directories: 13 File references: 108

Directories referenced: 13
```

Figure 30: Output of PERCmd.exe

Autopsy

- Go back to Autopsy and run another ingest module on the evidence.
- Deselect all and then choose "ParsePrefetchV41".
- Click Finish.

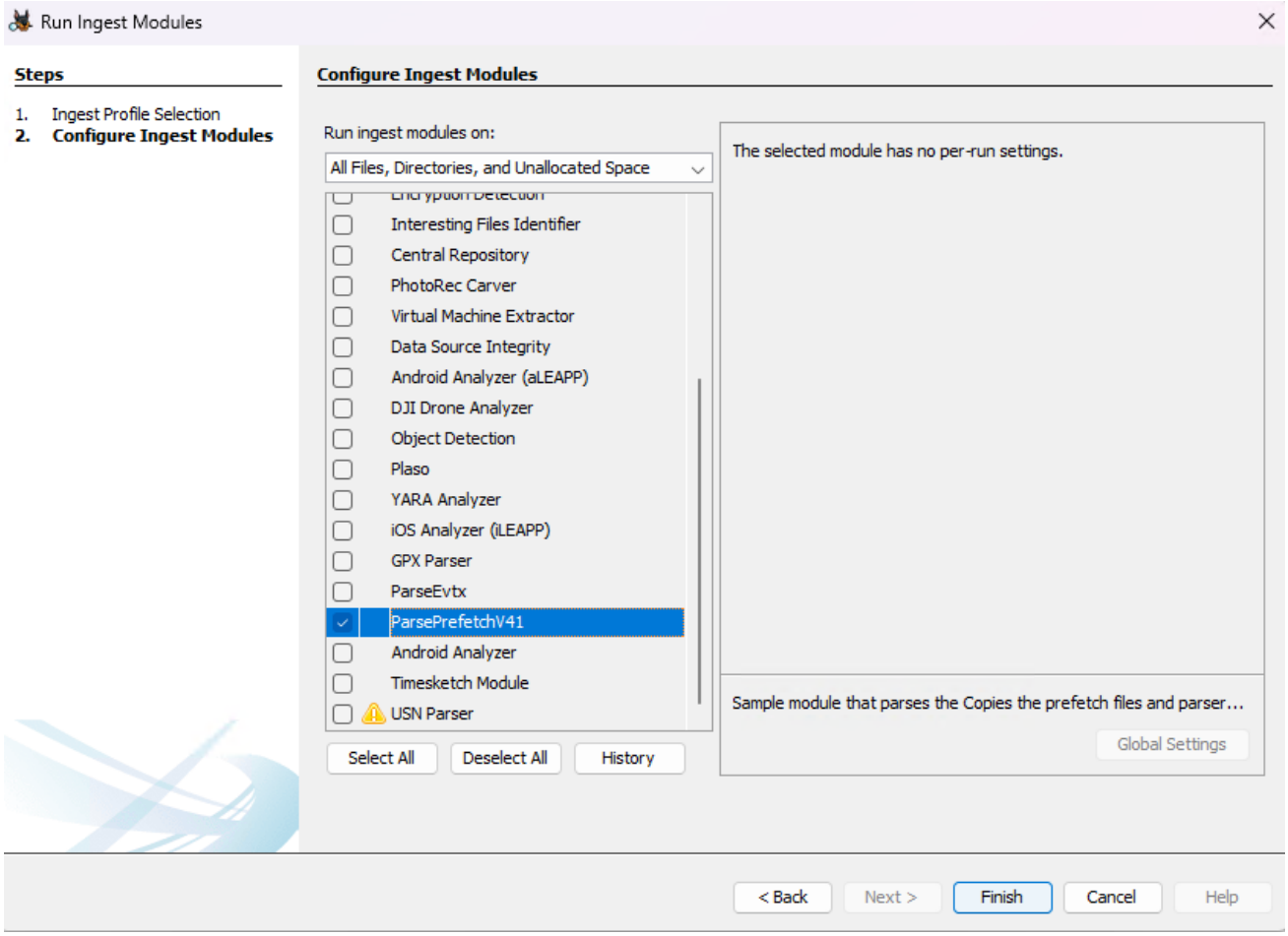


Figure 31: ParsePrefetchV41 Module

- The Data can be found under Data Artifacts > Run Programs and the Source Name will match the prefetch file.

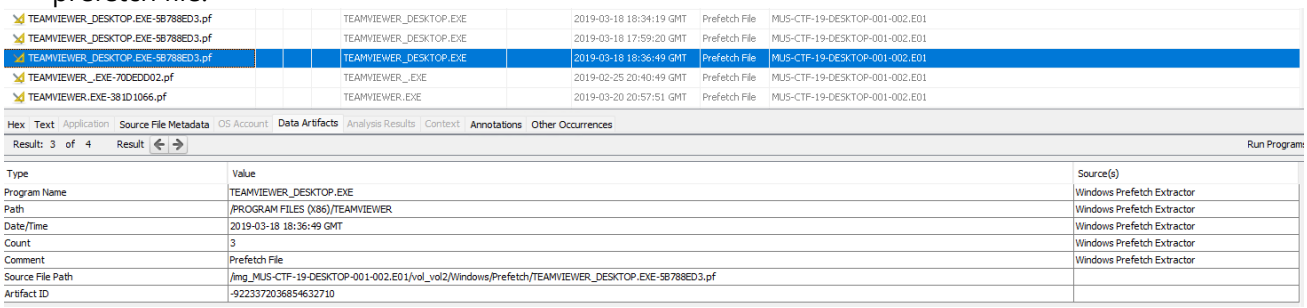


Figure 32: Parsing Prefetch with Autopsy

Flag	3

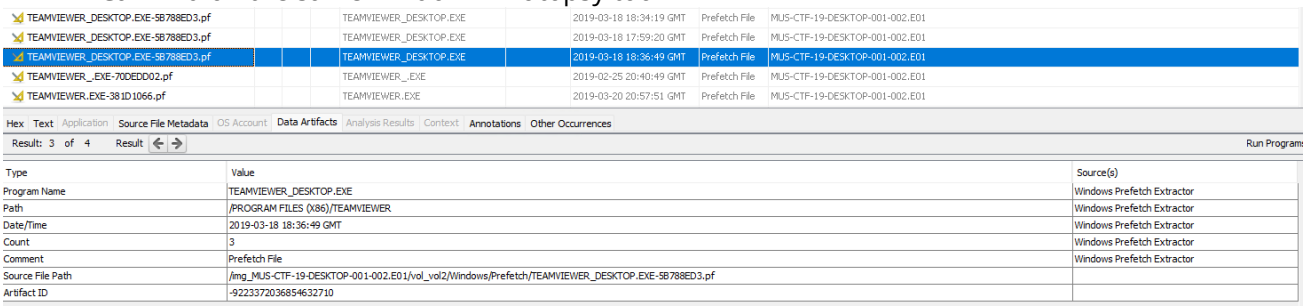
15. After looking at the TEAMVIEWER_DESKTOP.EXE prefetch file, which path was the executable in at the time of execution?

- Still on the same screen we'll find this answer too.

```
Files referenced: 80

00: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\WOW64.DLL
02: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\WOW64WIN.DLL
03: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\KERNEL32.DLL
04: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\KERNEL32.DLL
05: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\USER32.DLL
06: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\WOW64CPU.DLL
07: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\NTDLL.DLL
08: \VOLUME{01d4264bee777579-ccee841b}\PROGRAM FILES (X86)\TEAMVIEWER\TEAMVIEWER_DESKTOP.EXE (Executable: True)
09: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\KERNELBASE.DLL
10: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSTEM32\LOCALE.NLS
11: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\USER32.DLL
12: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\WIN32U.DLL
13: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\GDI32.DLL
14: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\GDI32FULL.DLL
15: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\MSVCP_WIN.DLL
16: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\UCRTBASE.DLL
17: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\IMM32.DLL
18: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\UXTHEME.DLL
19: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\MSVCRT.DLL
20: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\COMBASE.DLL
21: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\RPCRT4.DLL
22: \VOLUME{01d4264bee777579-ccee841b}\WINDOWS\SYSWOW64\SSPICLI.DLL
```

- Can find on the same window in Autopsy too



TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf	TEAMVIEWER_DESKTOP.EXE	2019-03-18 18:34:19 GMT	Prefetch File	MUS-CTF-19-DESKTOP-001-002.E01
TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf	TEAMVIEWER_DESKTOP.EXE	2019-03-18 17:59:20 GMT	Prefetch File	MUS-CTF-19-DESKTOP-001-002.E01
TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf	TEAMVIEWER_DESKTOP.EXE	2019-03-18 18:36:49 GMT	Prefetch File	MUS-CTF-19-DESKTOP-001-002.E01
TEAMVIEWER__.EXE-70DEDD02.pf	TEAMVIEWER_.EXE	2019-02-25 20:40:49 GMT	Prefetch File	MUS-CTF-19-DESKTOP-001-002.E01
TEAMVIEWER.EXE-381D1066.pf	TEAMVIEWER.EXE	2019-03-20 20:57:51 GMT	Prefetch File	MUS-CTF-19-DESKTOP-001-002.E01

Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 3 of 4 Result

Run Programs

Type	Value	Source(s)
Program Name	TEAMVIEWER_DESKTOP.EXE	Windows Prefetch Extractor
Path	/PROGRAM FILES (X86)/TEAMVIEWER	Windows Prefetch Extractor
Date/Time	2019-03-18 18:36:49 GMT	Windows Prefetch Extractor
Count	3	Windows Prefetch Extractor
Comment	Prefetch File	Windows Prefetch Extractor
Source File Path	/img_MUS-CTF-19-DESKTOP-001-002.E01/vol_vol2/Windows/Prefetch/TEAMVIEWER_DESKTOP.EXE-5B788ED3.pf	
Artifact ID	-9223372036854632710	

Flag	C:\Program Files (X86)\TeamViewer\

16. At 6:35PM on the 18th of March, Selma logged into her account on the Desktop. What method of did she use to access the Desktop?

MUS2019CTF > musctf-1 > Export > 70090-Connections_incoming.txt

```
1
2   136892318   ZBOOK   25-02-2019 20:43:35 27-02-2019 17:43:35 SelmaBouvier    RemoteControl   {52D6D8F5-36FF-47FA-9D62-2A9A9EF7D1BD}
3   1127661203  DESKTOP-B63488L 14-03-2019 19:40:13 14-03-2019 20:25:01 SelmaBouvier    RemoteControl   {0750C7DA-C452-410A-9751-99A4FC4D9AE8}
4   136892318   ZBOOK   18-03-2019 17:59:12 18-03-2019 18:14:54 SelmaBouvier    RemoteControl   {66628225-9782-49F3-A0CE-DA62F44F2AB9}
5   1222215886  JHYDE-SP    18-03-2019 18:34:18 18-03-2019 18:36:43 SelmaBouvier    RemoteControl   {9C67DA8F-EA96-4A5D-A4A4-E8693EACE7B3}
6   1222215886  JHYDE-SP    18-03-2019 18:36:48 18-03-2019 19:02:19 SelmaBouvier    RemoteControl   {B51BA739-ED49-4D23-9BD9-54576ABB5BF6}
```

Figure 33: Evidence of the connection in the TeamViewer Incoming Connections Log File

Flag	TeamViewer

17. What was the host name of the machine Selma used to remote into the Desktop at 6:35PM on the 18th of March?

```
MUS2019CTF > musctf-1 > Export > 70090-Connections_incoming.txt
1
2   136892318   ZBOOK   25-02-2019 20:43:35 27-02-2019 17:43:35 SelmaBouvier    RemoteControl   {52D6D8F5-36FF-47FA-9D62-2A9A9EF7D1BD}
3   1127661203  DESKTOP-B63488L 14-03-2019 19:40:13 14-03-2019 20:25:01 SelmaBouvier    RemoteControl   {0750C7DA-C452-410A-9751-99A4FC4D9AE8}
4   136892318   ZBOOK   18-03-2019 17:59:12 18-03-2019 18:14:54 SelmaBouvier    RemoteControl   {66628225-9782-49F3-A0CE-DA62F44F2AB9}
5   1222215886  JHYDE-SP    18-03-2019 18:34:18 18-03-2019 18:36:43 SelmaBouvier    RemoteControl   {9C67DA8F-EA96-4A5D-A4A4-E8693EACE7B3}
6   1222215886  JHYDE-SP    18-03-2019 18:36:48 18-03-2019 19:02:19 SelmaBouvier    RemoteControl   {B51BA739-ED49-4D23-9BD9-54576ABB5BF6}
```

Figure 34: Evidence of the connection in the TeamViewer Incoming Connections Log File

Flag	JHYDE-SP

18. How many unique machines accessed the Desktop via TeamViewer?

MUS2019CTF > musctf-1 > Export > 70090-Connections_incoming.txt

```
1
2   136892318   ZBOOK   25-02-2019 20:43:35 27-02-2019 17:43:35 SelmaBouvier    RemoteControl   {52D6D8F5-36FF-47FA-9D62-2A9A9EF7D1BD}
3   1127661203  DESKTOP-B63488L 14-03-2019 19:40:13 14-03-2019 20:25:01 SelmaBouvier    RemoteControl   {0750C7DA-C452-410A-9751-99A4FC4D9AE8}
4   136892318   ZBOOK   18-03-2019 17:59:12 18-03-2019 18:14:54 SelmaBouvier    RemoteControl   {66628225-9782-49F3-A0CE-DA62F44F2AB9}
5   1222215886  JHYDE-SP    18-03-2019 18:34:18 18-03-2019 18:36:43 SelmaBouvier    RemoteControl   {9C67DA8F-EA96-4A5D-A4A4-E8693EACE7B3}
6   1222215886  JHYDE-SP    18-03-2019 18:36:48 18-03-2019 19:02:19 SelmaBouvier    RemoteControl   {B51BA739-ED49-4D23-9BD9-54576ABB5BF6}
```

Figure 35: Evidence of the connection in the TeamViewer Incoming Connections Log File

Flag	3

19. How many bytes total were sent out on the network via the Team Viewer Service?

The SRUM (System Resource Usage Monitor) monitors desktop application programs, services, windows apps and network connections. It's saved in the file at C:\Windows\system32\sru\SRUDB.dat (using this tool to parse it by Mark Baggett). I just needed to export it and add up the bytes sent in excel.

```
C:\Users\shanna\OneDrive\Desktop\Tools>git clone https://github.com/MarkBaggett/srum-dump
Cloning into 'srum-dump'...
remote: Enumerating objects: 239, done.
remote: Counting objects: 100% (55/55), done.
remote: Compressing objects: 100% (30/30), done. eceiving objects:  10% (24/239)
remote: Total 239 (delta 25), reused 48 (delta 25), pack-reused 184
Receiving objects: 100% (239/239), 72.09 MiB | 1.15 MiB/s, done.
Resolving deltas: 100% (123/123), done.
```

Figure 36: Clone SRUM-DUMP locally

```
 Directory of C:\Users\shanna\OneDrive\Desktop\Tools\srum-dump

09/05/2022  10:22 AM    <DIR>          .
09/05/2022  10:21 AM    <DIR>          ..
09/05/2022  10:22 AM             7,613 BLANK_TEMPLATE.xlsx
09/05/2022  10:22 AM           278,912 FGET.exe
09/05/2022  10:22 AM            35,859 LICENSE
09/05/2022  10:22 AM             6,061 README.md
09/05/2022  10:22 AM               380 release_notes.md
09/05/2022  10:22 AM               146 requirements.txt
09/05/2022  10:22 AM        11,204,274 srum_dump2.exe
09/05/2022  10:22 AM            52,960 srum_dump2.jpg
09/05/2022  10:22 AM            29,119 srum_dump2.py
09/05/2022  10:22 AM           116,707 srum_live_acquisition.jpg
09/05/2022  10:22 AM            31,774 SRUM_TEMPLATE2.xlsx
09/05/2022  10:22 AM           111,265 SRUM_TEMPLATE2_ORIG.xlsx
              12 File(s)     11,875,070 bytes
               2 Dir(s)  592,743,915,520 bytes free

C:\Users\shanna\OneDrive\Desktop\Tools\srum-dump>srum_dump2.exe
```

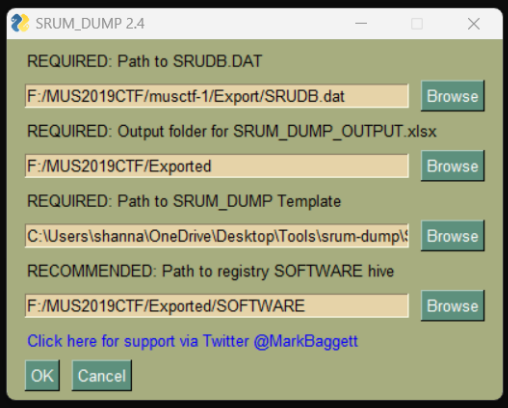
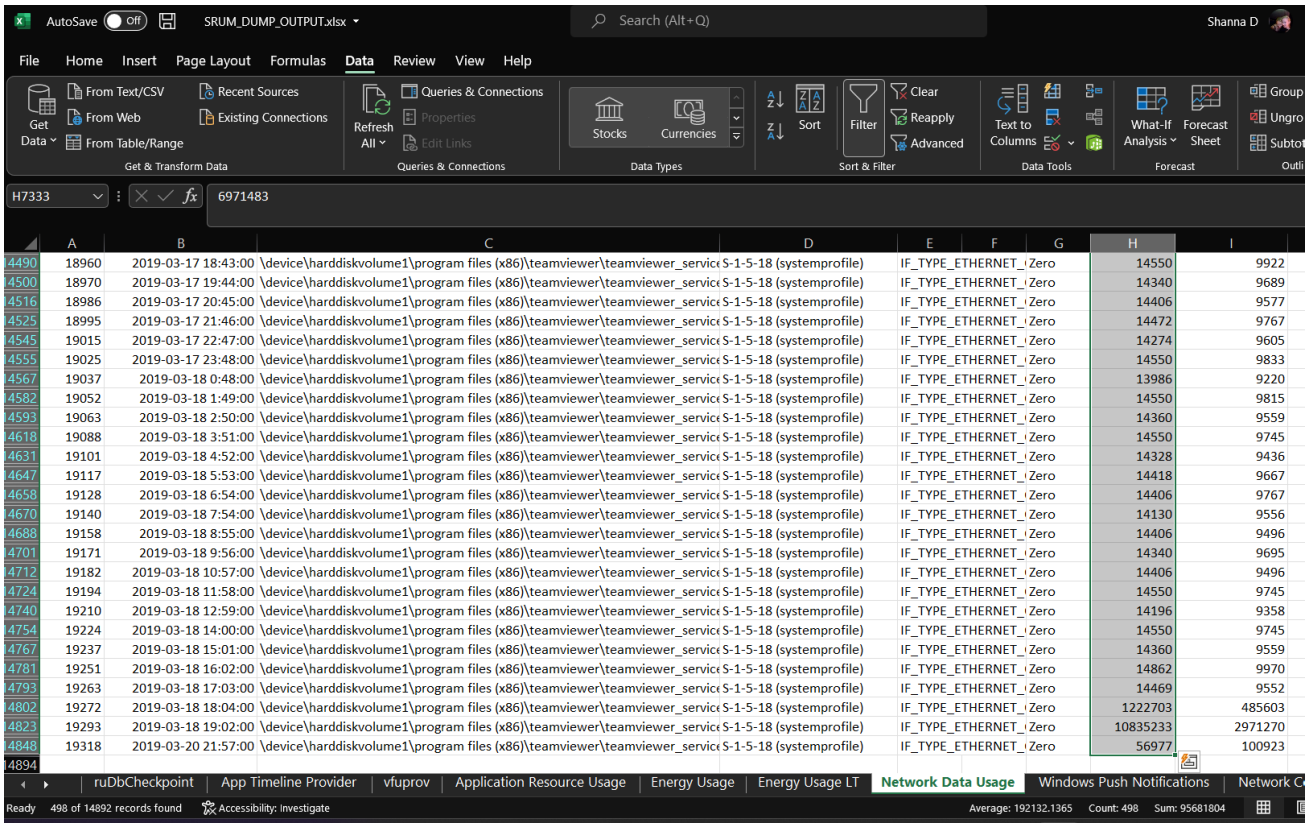


Figure 37: run srum-dump2.exe to start the GUI



	A	B	C	D	E	F	G	H	I
14490	18960	2019-03-17 18:43:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9922
14500	18970	2019-03-17 19:44:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14340	9689
14516	18986	2019-03-17 20:45:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14406	9577
14525	18995	2019-03-17 21:46:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14472	9767
14545	19015	2019-03-17 22:47:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14274	9605
14555	19025	2019-03-17 23:48:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9833
14567	19037	2019-03-18 0:48:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	13986	9220
14582	19052	2019-03-18 1:49:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9815
14593	19063	2019-03-18 2:50:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14360	9559
14618	19088	2019-03-18 3:51:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9745
14631	19101	2019-03-18 4:52:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14328	9436
14647	19117	2019-03-18 5:53:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14418	9667
14658	19128	2019-03-18 6:54:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14406	9767
14670	19140	2019-03-18 7:54:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14130	9556
14688	19158	2019-03-18 8:55:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14406	9496
14701	19171	2019-03-18 9:56:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14340	9695
14712	19182	2019-03-18 10:57:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14406	9496
14724	19194	2019-03-18 11:58:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9745
14740	19210	2019-03-18 12:59:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14196	9358
14754	19224	2019-03-18 14:00:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14550	9745
14767	19237	2019-03-18 15:01:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14360	9559
14781	19251	2019-03-18 16:02:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14862	9970
14793	19263	2019-03-18 17:03:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	14469	9552
14802	19272	2019-03-18 18:04:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	1222703	485603
14823	19293	2019-03-18 19:02:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	10835233	2971270
14848	19318	2019-03-20 21:57:00	\device\harddiskvolume1\program files (x86)\teamviewer\teamviewer_service	S-1-5-18 (systemprofile)	IF_TYPE_ETHERNET_		Zero	56977	100923

Figure 38: Analysing the spreadsheet

Flag	95681804

20. How many files were downloaded from the magnetic4nsics Sharepoint?

🖫 Autopsy

- When we ran the Recent Activity plugin, the web history was parsed and loaded under Data Artifacts for us.
- Under Web Downloads on the left we can see there is one file downloaded using Chrome.
    a. Path C:\Users\SelmaBouvier\Downloads\README

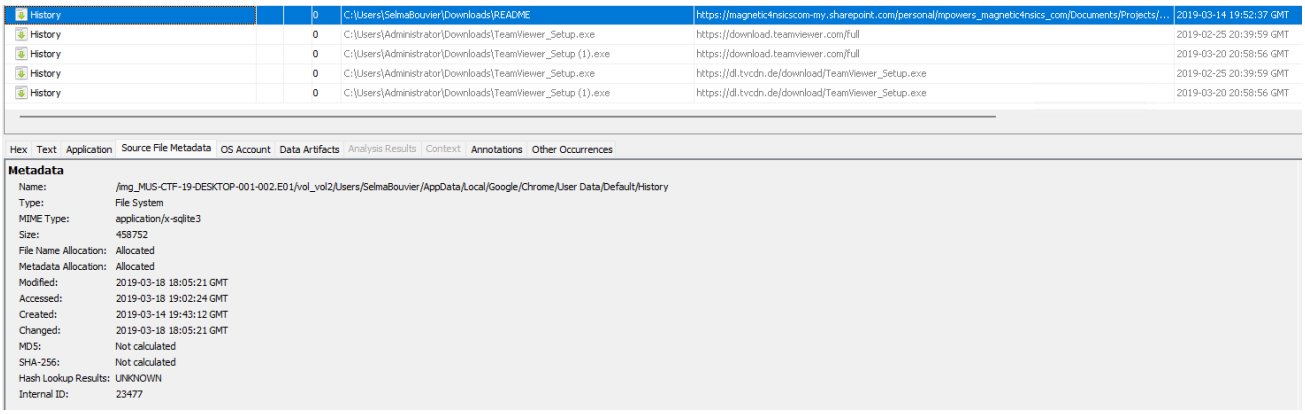


Figure 39: One file downloaded with Chrome

- Under Web History on the left we can see there is one file downloaded using Edge.
    a. Path D:\OneDrive_1_3-18-2019.zip

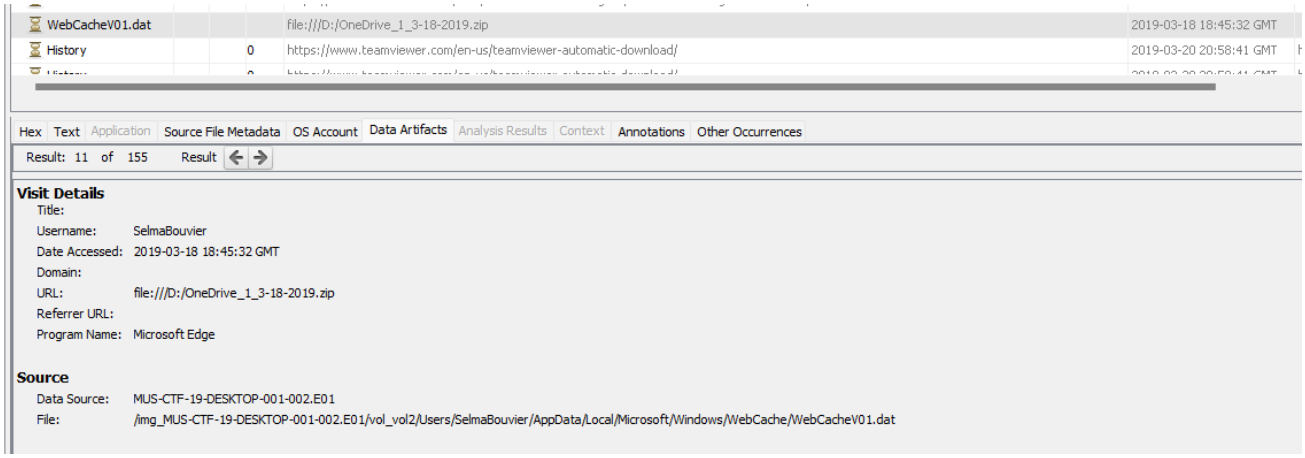


Figure 40: One file downloaded with Edge

🏳 Flag	2

It's a bit confusing having Web Downloads and Web History isn't it? How do you know? It's why we always double check our evidence, artefacts and findings.

21. On March 18th 2019 at 18:58:21 Selma saw a Windows popup notification. What type of notification was it?

- Some Googling tells me there is an event log for these pop up notifications - Microsoft-Windows-PushNotification-Platform%4Operational.evtx

🖫 Autopsy

- I'll use Autopsy to parse this event log for me
- Select ParseEvtx under Configure Ingest Modules and then paste in the Event Log name BEFORE checking the box next to other … this is important.

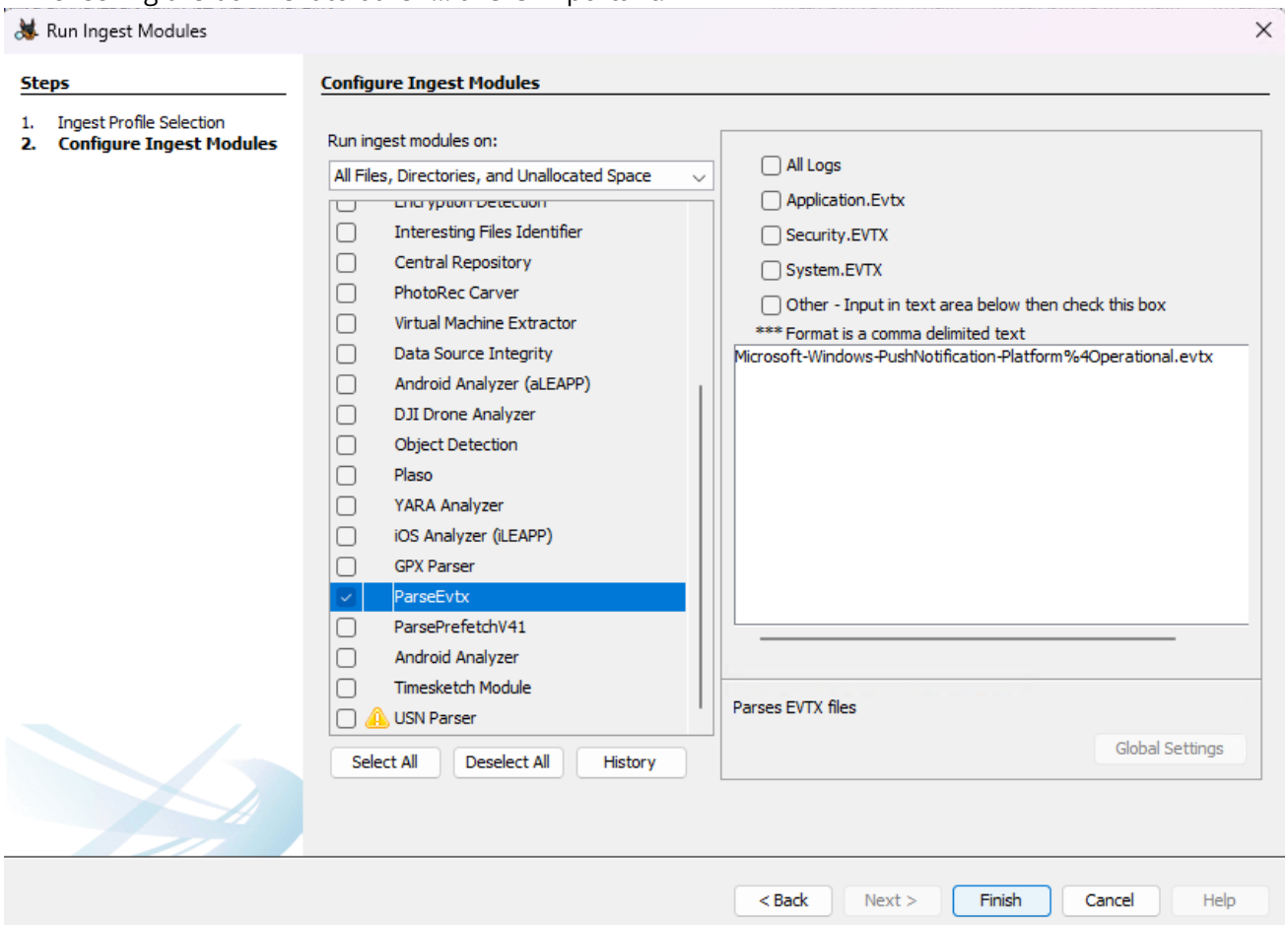


Figure 41: Paste the event log name before checking the box next to other

- You'll see that you don't get a huge amount of information

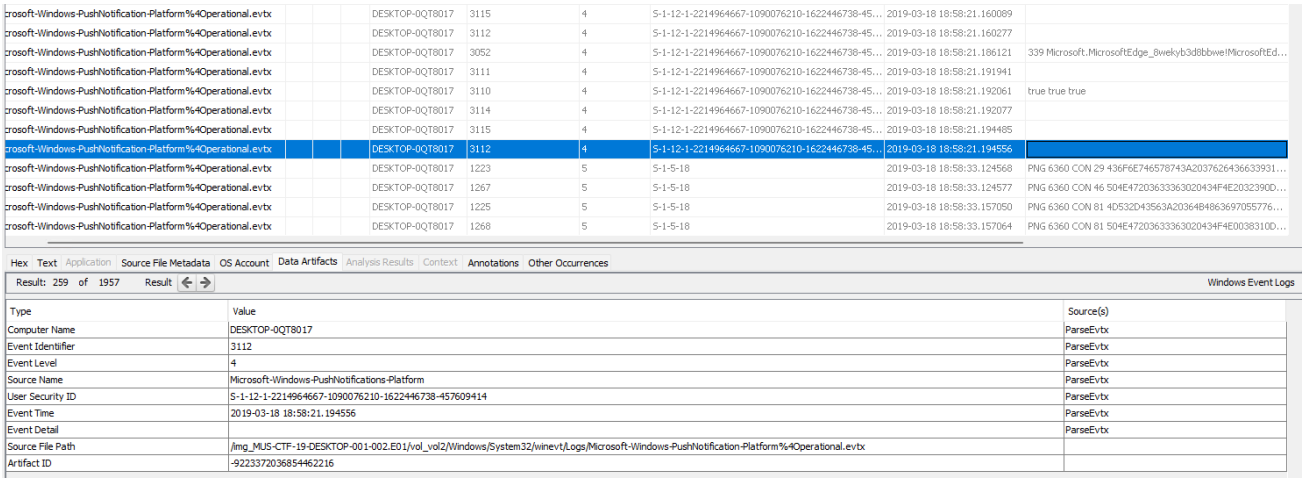
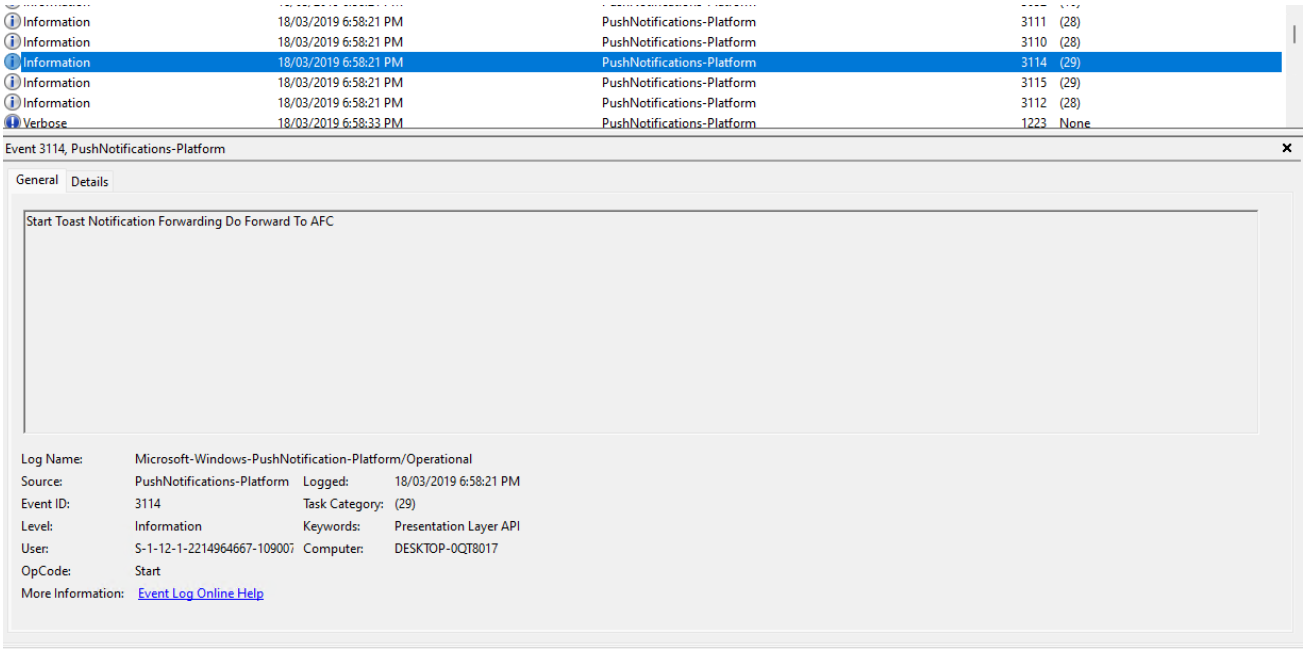


Figure 42: Parsing Push Notifications event log in Autopsy

Event Viewer

- Another easy way to find this is by finding the event log in Autopsy, right clicking and opening in external viewer. This will open the event log in your native windows event log viewer.
- A toast provides simple feedback about an operation in a small popup. It only fills the amount of space required for the message and the current activity remains visible and interactive. Toasts automatically disappear after a timeout.



Flag	Toast