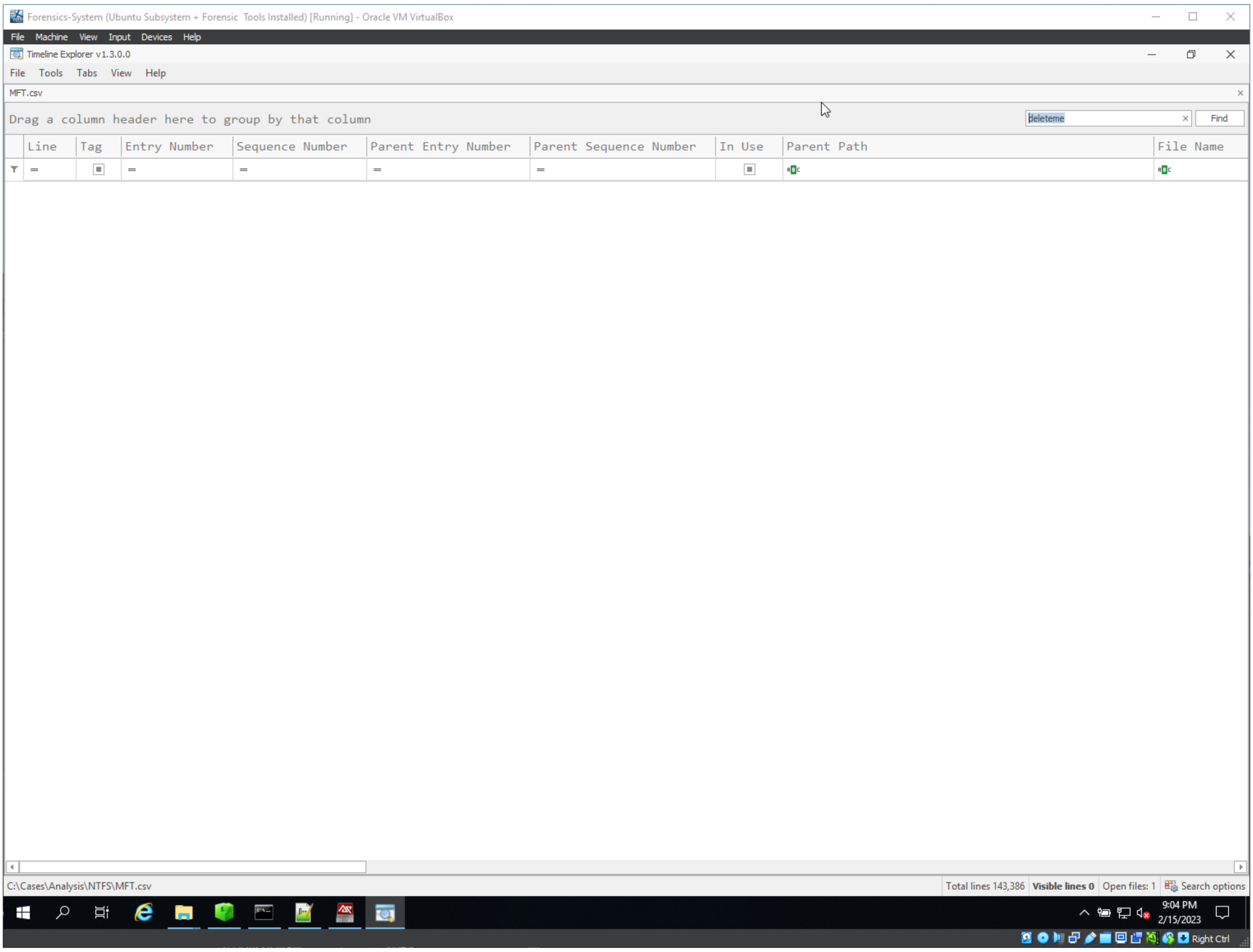
Recovering Deleted Files:

- Evidence of deleted files
- USN Journal

- Find :
  - Creation and deletion of “deleteme_T1551.004”
  - Entry number of the above file and the existence of it in the MFT

Evidence of deleted files

- Search in the MFT.csv, evidence of deleteme file.


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
MFT.csv
Drag a column header here to group by that column
Find
Right Ctrl

deleteme

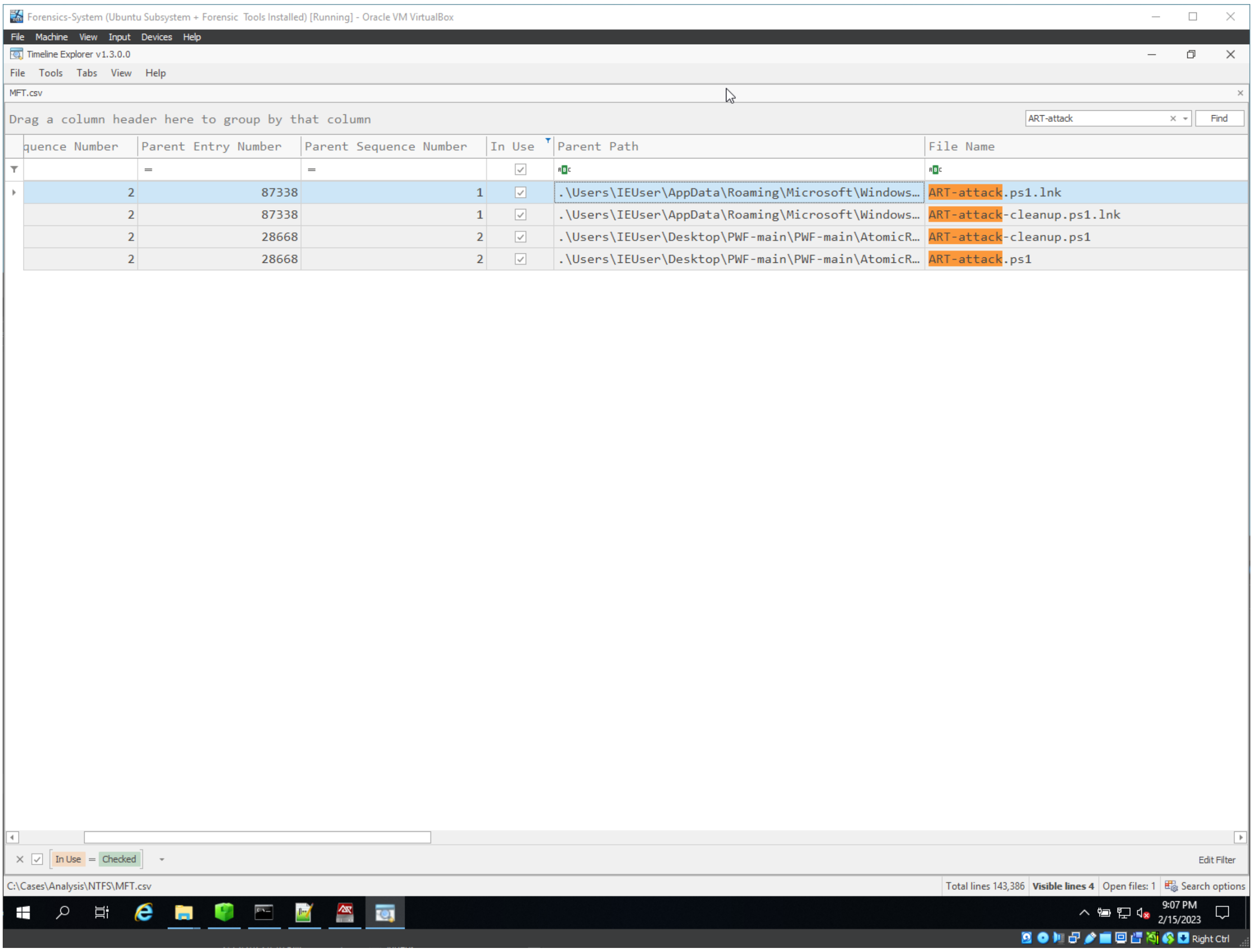
Line	Tag	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name

C:\Cases\Analysis\NTFS\MFT.csv

Total lines 143,386 **Visible lines 0** Open files: 1 Search options

9:04 PM
2/15/2023

- Let’s try with ART-attack:
- Based on In Use checked box, the partition area where is located is protected.



Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox

Timeline Explorer v1.3.0.0

MFT.csv

Drag a column header here to group by that column

ART-attack

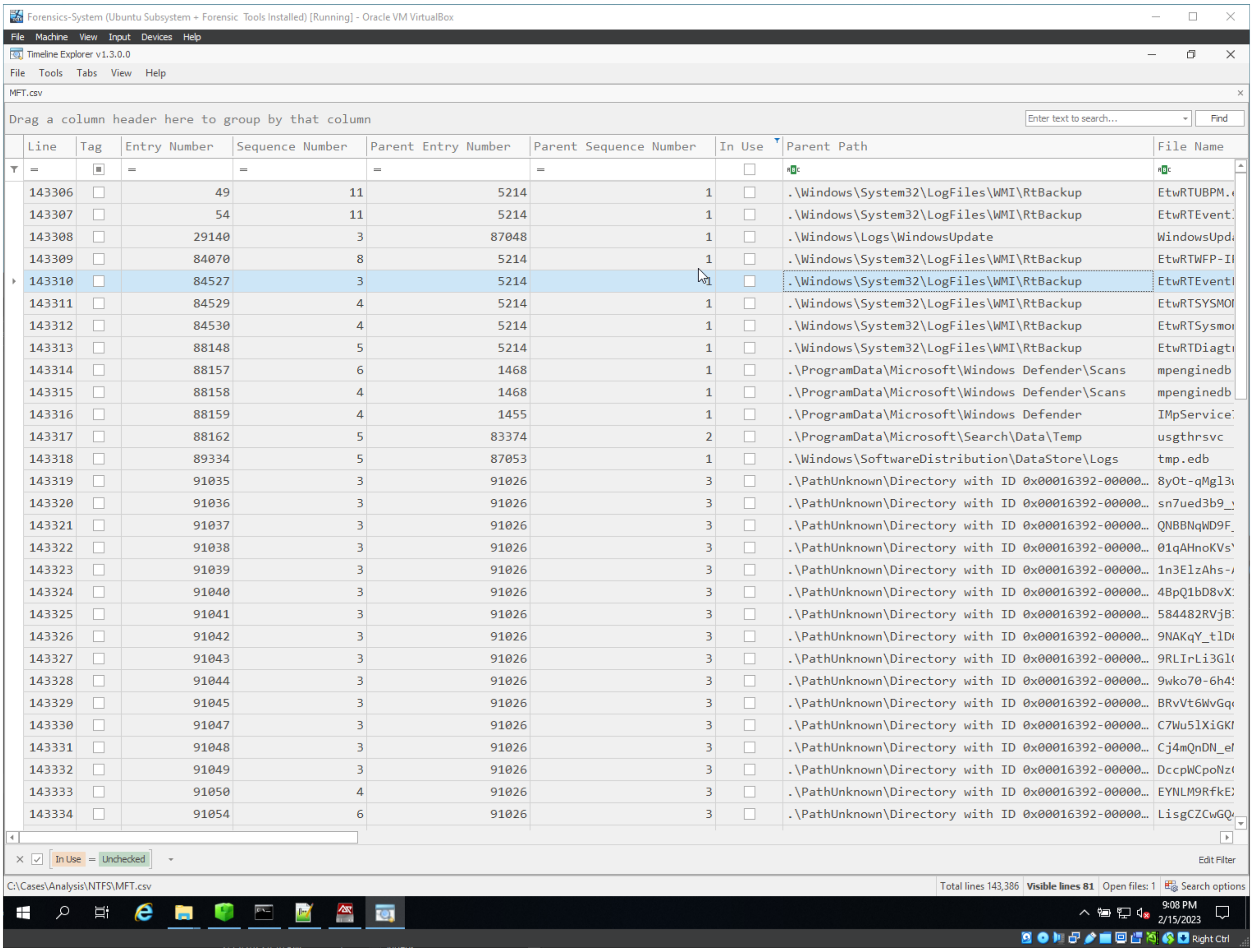
quence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name
2	87338	1	☑	.\Users\IEUser\AppData\Roaming\Microsoft\Windows…	ART-attack.ps1.lnk
2	87338	1	☑	.\Users\IEUser\AppData\Roaming\Microsoft\Windows…	ART-attack-cleanup.ps1.lnk
2	28668	2	☑	.\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR…	ART-attack-cleanup.ps1
2	28668	2	☑	.\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR…	ART-attack.ps1

In Use = Checked

C:\Cases\Analysis\NTFS\MFT.csv

Total lines 143,386 Visible lines 4 Open files: 1

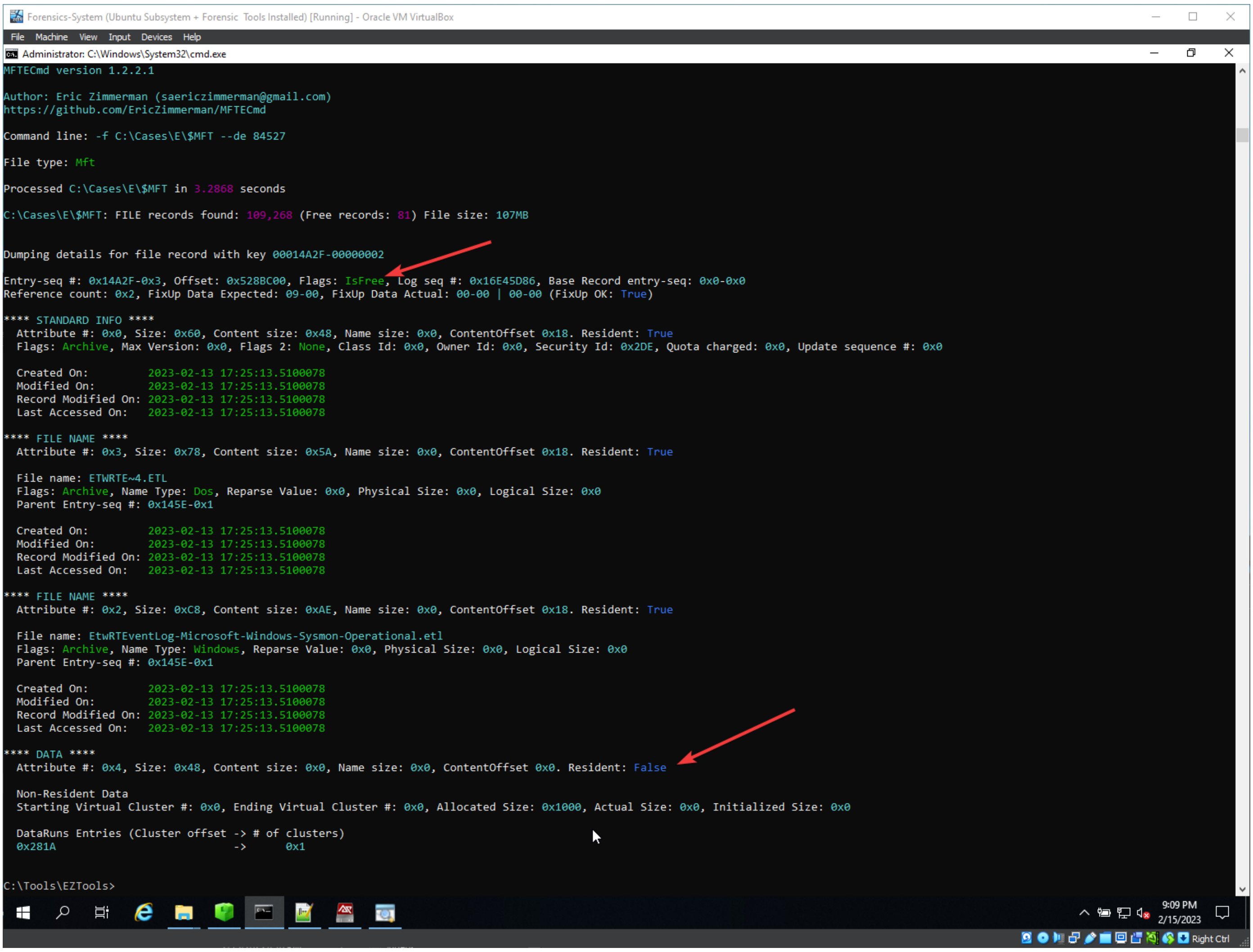
- Let s see a file that is no longer in use , take Entry Number and let s query it in the MFT cmd tool .


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
MFT.csv
Drag a column header here to group by that column
Enter text to search...
Find
In Use = Unchecked
Edit Filter
9:08 PM
2/15/2023
Right Ctrl

Line	Tag	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name
143306	☐	49	11	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTUBPM.
143307	☐	54	11	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTEvent
143308	☐	29140	3	87048	1	☐	.\Windows\Logs\WindowsUpdate	WindowsUpd
143309	☐	84070	8	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTWFP-I
143310	☐	84527	3	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTEvent
143311	☐	84529	4	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTSYSMO
143312	☐	84530	4	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTSysmo
143313	☐	88148	5	5214	1	☐	.\Windows\System32\LogFiles\WMI\RtBackup	EtwRTDiagt
143314	☐	88157	6	1468	1	☐	.\ProgramData\Microsoft\Windows Defender\Scans	mpenginedb
143315	☐	88158	4	1468	1	☐	.\ProgramData\Microsoft\Windows Defender\Scans	mpenginedb
143316	☐	88159	4	1455	1	☐	.\ProgramData\Microsoft\Windows Defender	IMpService
143317	☐	88162	5	83374	2	☐	.\ProgramData\Microsoft\Search\Data\Temp	usgthrsvc
143318	☐	89334	5	87053	1	☐	.\Windows\SoftwareDistribution\DataStore\Logs	tmp.edb
143319	☐	91035	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	8yOt-qMgl3
143320	☐	91036	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	sn7ued3b9_
143321	☐	91037	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	QNBBNqWD9F_
143322	☐	91038	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	01qAHnoKVs
143323	☐	91039	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	1n3ElzAhs-
143324	☐	91040	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	4BpQ1bD8vX
143325	☐	91041	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	584482RVjB
143326	☐	91042	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	9NAKqY_tlD
143327	☐	91043	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	9RLIrLi3Gl
143328	☐	91044	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	9wko70-6h4
143329	☐	91045	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	BRvVt6WvGq
143330	☐	91047	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	C7Wu5lXiGK
143331	☐	91048	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	Cj4mQnDN_e
143332	☐	91049	3	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	DccpWCpoNz
143333	☐	91050	4	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	EYNLM9RfkE
143334	☐	91054	6	91026	3	☐	.\PathUnknown\Directory with ID 0x00016392-00000…	LisgCZCwGQ

C:\Cases\Analysis\NTFS\MFT.csv Total lines 143,386 **Visible lines 81** Open files: 1 Search options

- IsFree flag says that this file can be overwritten, the entry of MFT can be overwritten aswell as the data



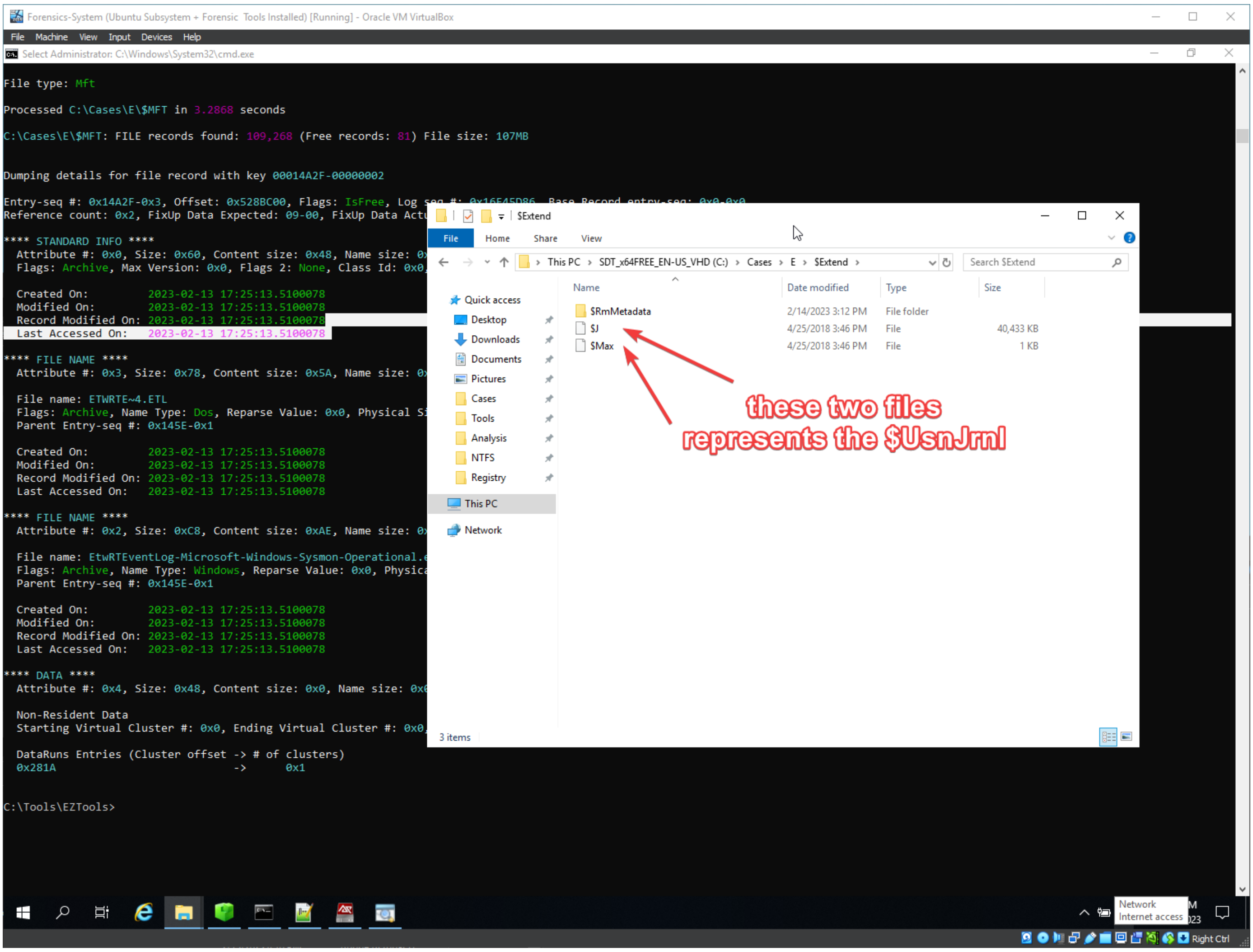
Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: C:\Windows\System32\cmd.exe

```
MFTECmd version 1.2.2.1

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

Command line: -f C:\Cases\E\$MFT --de 84527

File type: Mft

Processed C:\Cases\E\$MFT in 3.2868 seconds

C:\Cases\E\$MFT: FILE records found: 109,268 (Free records: 81) File size: 107MB


Dumping details for file record with key 00014A2F-00000002

Entry-seq #: 0x14A2F-0x3, Offset: 0x528BC00, Flags: IsFree, Log seq #: 0x16E45D86, Base Record entry-seq: 0x0-0x0
Reference count: 0x2, FixUp Data Expected: 09-00, 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: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x2DE, Quota charged: 0x0, Update sequence #: 0x0

  Created On:         2023-02-13 17:25:13.5100078
  Modified On:        2023-02-13 17:25:13.5100078
  Record Modified On: 2023-02-13 17:25:13.5100078
  Last Accessed On:   2023-02-13 17:25:13.5100078

**** FILE NAME ****
  Attribute #: 0x3, Size: 0x78, Content size: 0x5A, Name size: 0x0, ContentOffset 0x18. Resident: True

  File name: ETWRTE~4.ETL
  Flags: Archive, Name Type: Dos, Reparse Value: 0x0, Physical Size: 0x0, Logical Size: 0x0
  Parent Entry-seq #: 0x145E-0x1

  Created On:         2023-02-13 17:25:13.5100078
  Modified On:        2023-02-13 17:25:13.5100078
  Record Modified On: 2023-02-13 17:25:13.5100078
  Last Accessed On:   2023-02-13 17:25:13.5100078

**** FILE NAME ****
  Attribute #: 0x2, Size: 0xC8, Content size: 0xAE, Name size: 0x0, ContentOffset 0x18. Resident: True

  File name: EtwRTEventLog-Microsoft-Windows-Sysmon-Operational.etl
  Flags: Archive, Name Type: Windows, Reparse Value: 0x0, Physical Size: 0x0, Logical Size: 0x0
  Parent Entry-seq #: 0x145E-0x1

  Created On:         2023-02-13 17:25:13.5100078
  Modified On:        2023-02-13 17:25:13.5100078
  Record Modified On: 2023-02-13 17:25:13.5100078
  Last Accessed On:   2023-02-13 17:25:13.5100078

**** DATA ****
  Attribute #: 0x4, Size: 0x48, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

  Non-Resident Data
  Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x0, Allocated Size: 0x1000, Actual Size: 0x0, Initialized Size: 0x0

  DataRuns Entries (Cluster offset -> # of clusters)
  0x281A                         ->      0x1


C:\Tools\EZTools>
```

- In the DATA attribute, it is called Unallocated space but it is not empty

USN Journal

- Journaling is an NTFS specific feature and ensures file system integrity in event of a crash. There are lgo files that are storing operations executed on particular files or on MFT specific entries. In the case of system crashing , the NTFS will use that in order to restore some operations such as: if a file was created , modified, read, renamed, deleted.



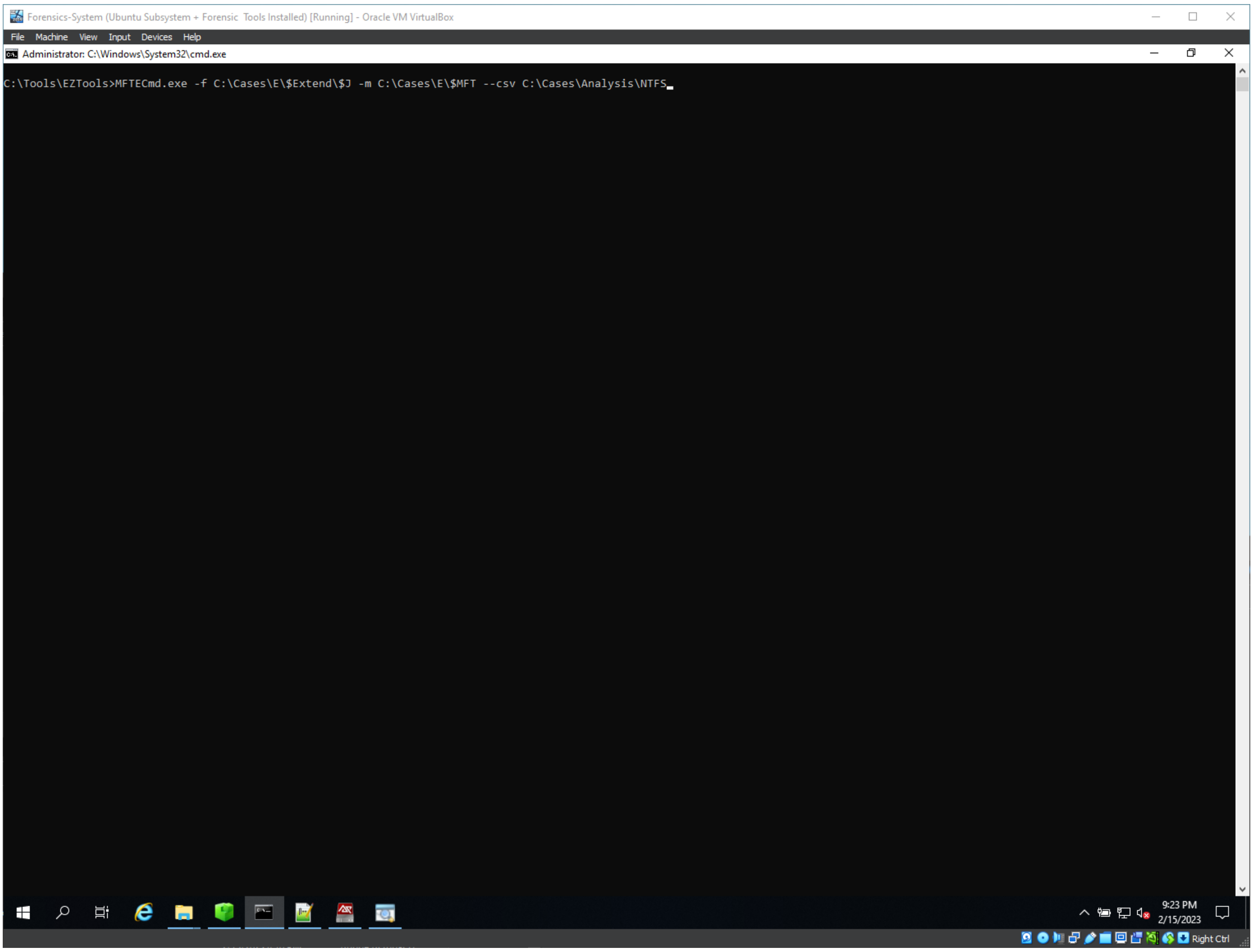
Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Administrator: C:\Windows\System32\cmd.exe
$Extend
File Home Share View
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › E › $Extend ›
Search $Extend
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
Analysis
NTFS
Registry
This PC
Network
3 items

```
File type: Mft

Processed C:\Cases\E\$MFT in 3.2868 seconds

C:\Cases\E\$MFT: FILE records found: 109,268 (Free records: 81) File size: 107MB


Dumping details for file record with key 00014A2F-00000002

Entry-seq #: 0x14A2F-0x3, Offset: 0x528BC00, Flags: IsFree, Log seq #: 0x16F45D86, Base Record entry-seq: 0x0-0x0
Reference count: 0x2, FixUp Data Expected: 09-00, FixUp Data Actu

**** STANDARD INFO ****
  Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x
  Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0,

  Created On:          2023-02-13 17:25:13.5100078
  Modified On:         2023-02-13 17:25:13.5100078
  Record Modified On:  2023-02-13 17:25:13.5100078
  Last Accessed On:    2023-02-13 17:25:13.5100078

**** FILE NAME ****
  Attribute #: 0x3, Size: 0x78, Content size: 0x5A, Name size: 0x

  File name: ETWRTE~4.ETL
  Flags: Archive, Name Type: Dos, Reparse Value: 0x0, Physical Si
  Parent Entry-seq #: 0x145E-0x1

  Created On:          2023-02-13 17:25:13.5100078
  Modified On:         2023-02-13 17:25:13.5100078
  Record Modified On:  2023-02-13 17:25:13.5100078
  Last Accessed On:    2023-02-13 17:25:13.5100078

**** FILE NAME ****
  Attribute #: 0x2, Size: 0xC8, Content size: 0xAE, Name size: 0x

  File name: EtwRTEventLog-Microsoft-Windows-Sysmon-Operational.e
  Flags: Archive, Name Type: Windows, Reparse Value: 0x0, Physica
  Parent Entry-seq #: 0x145E-0x1

  Created On:          2023-02-13 17:25:13.5100078
  Modified On:         2023-02-13 17:25:13.5100078
  Record Modified On:  2023-02-13 17:25:13.5100078
  Last Accessed On:    2023-02-13 17:25:13.5100078

**** DATA ****
  Attribute #: 0x4, Size: 0x48, Content size: 0x0, Name size: 0x0

  Non-Resident Data
  Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x0,

  DataRuns Entries (Cluster offset -> # of clusters)
  0x281A                           ->      0x1


C:\Tools\EZTools>
```

Name	Date modified	Type	Size
$RmMetadata	2/14/2023 3:12 PM	File folder	
$J	4/25/2018 3:46 PM	File	40,433 KB
$Max	4/25/2018 3:46 PM	File	1 KB

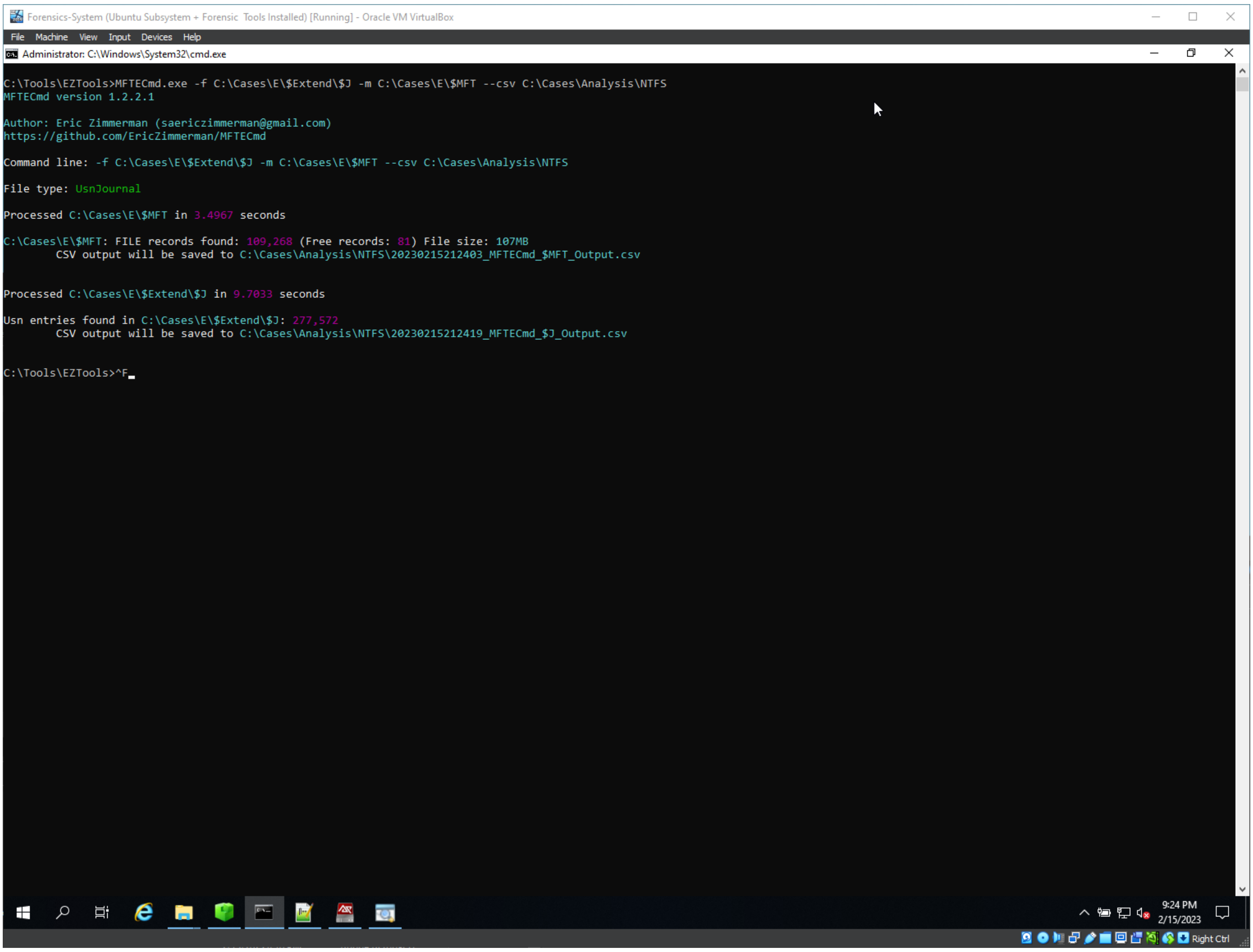
these two files represents the $UsnJrnl

- Kape ensured that $UsnJrnl becomes $J and $Max.
- We will use $J for our forensic analysis on deleted files.



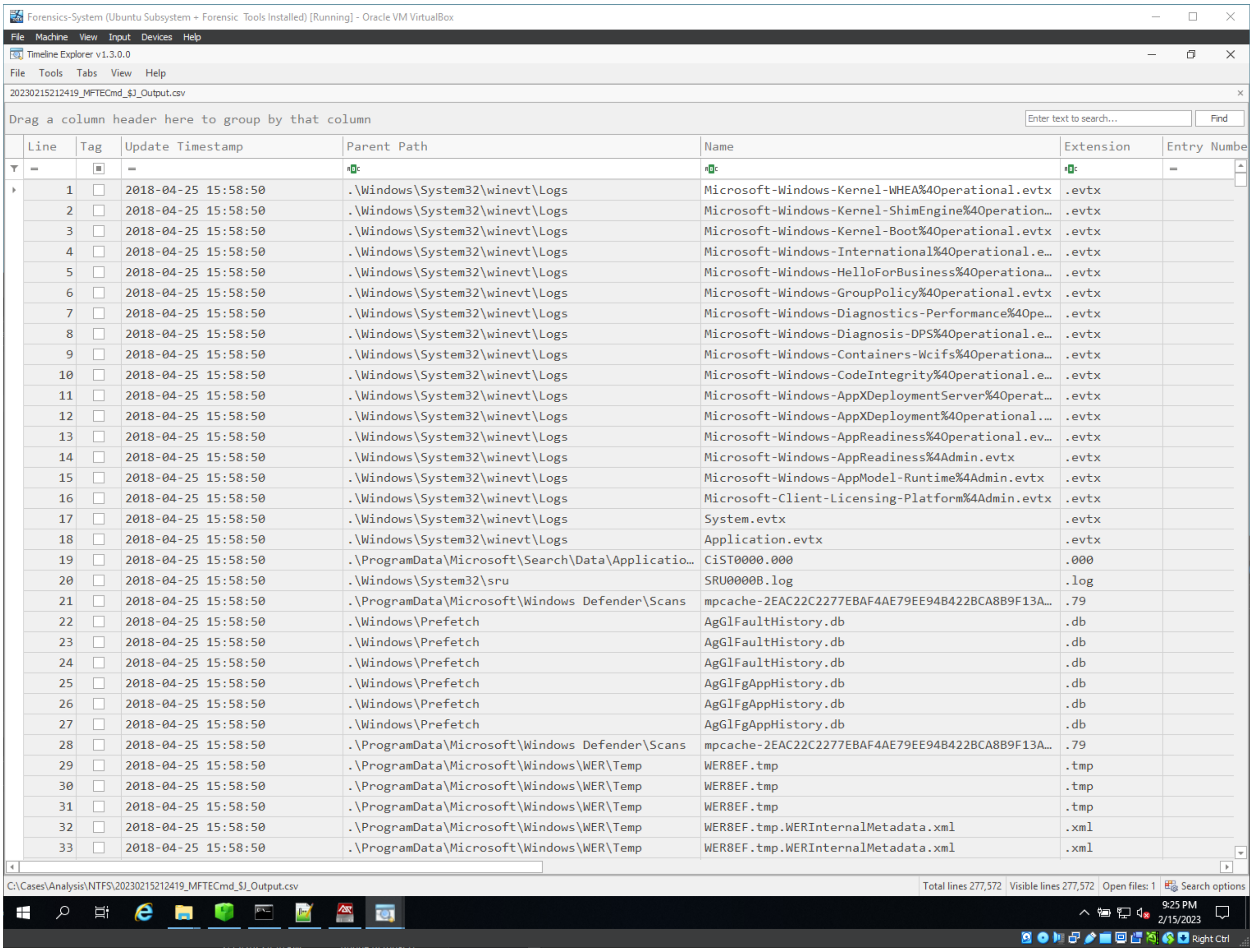
Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: C:\Windows\System32\cmd.exe
9:23 PM
2/15/2023
Right Ctrl

```
C:\Tools\EZTools>MFTECmd.exe -f C:\Cases\E\$Extend\$J -m C:\Cases\E\$MFT --csv C:\Cases\Analysis\NTFS
```


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: C:\Windows\System32\cmd.exe
9:24 PM
2/15/2023
Right Ctrl

```
C:\Tools\EZTools>MFTECmd.exe -f C:\Cases\E\$Extend\$J -m C:\Cases\E\$MFT --csv C:\Cases\Analysis\NTFS
MFTECmd version 1.2.2.1

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

Command line: -f C:\Cases\E\$Extend\$J -m C:\Cases\E\$MFT --csv C:\Cases\Analysis\NTFS

File type: UsnJournal

Processed C:\Cases\E\$MFT in 3.4967 seconds

C:\Cases\E\$MFT: FILE records found: 109,268 (Free records: 81) File size: 107MB
        CSV output will be saved to C:\Cases\Analysis\NTFS\20230215212403_MFTECmd_$MFT_Output.csv


Processed C:\Cases\E\$Extend\$J in 9.7033 seconds

Usn entries found in C:\Cases\E\$Extend\$J: 277,572
        CSV output will be saved to C:\Cases\Analysis\NTFS\20230215212419_MFTECmd_$J_Output.csv


C:\Tools\EZTools>^F
```

- $J file in csv format:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
Drag a column header here to group by that column
Enter text to search...
Find

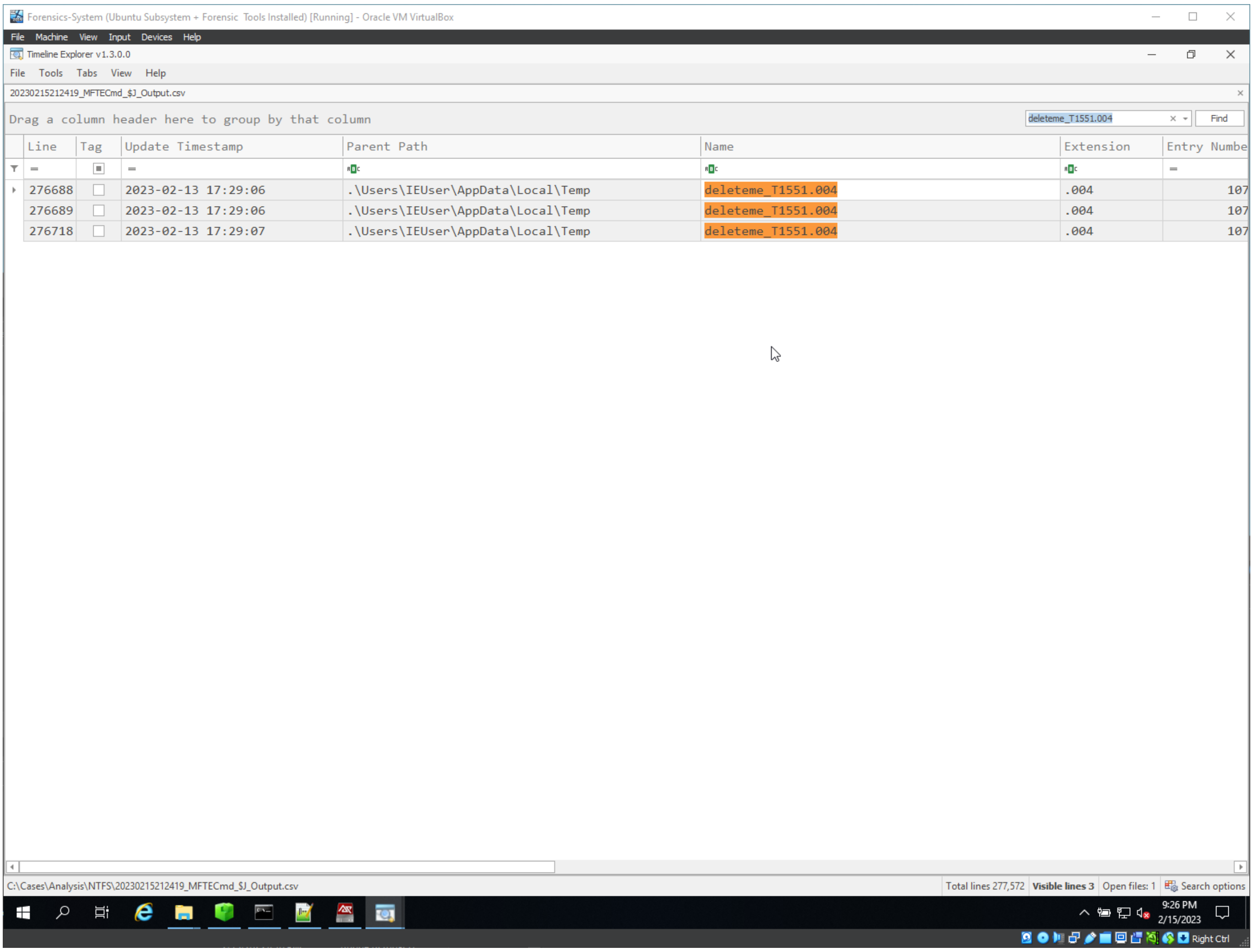
20230215212419_MFTECmd_$J_Output.csv

Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Numbe
1	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Kernel-WHEA%4Operational.evtx	.evtx	
2	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Kernel-ShimEngine%4Operation…	.evtx	
3	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Kernel-Boot%4Operational.evtx	.evtx	
4	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-International%4Operational.e…	.evtx	
5	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-HelloForBusiness%4Operationa…	.evtx	
6	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-GroupPolicy%4Operational.evtx	.evtx	
7	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Diagnostics-Performance%4Ope…	.evtx	
8	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Diagnosis-DPS%4Operational.e…	.evtx	
9	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-Containers-Wcifs%4Operationa…	.evtx	
10	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-CodeIntegrity%4Operational.e…	.evtx	
11	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-AppXDeploymentServer%4Operat…	.evtx	
12	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-AppXDeployment%4Operational.…	.evtx	
13	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-AppReadiness%4Operational.ev…	.evtx	
14	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-AppReadiness%4Admin.evtx	.evtx	
15	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Windows-AppModel-Runtime%4Admin.evtx	.evtx	
16	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Microsoft-Client-Licensing-Platform%4Admin.evtx	.evtx	
17	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	System.evtx	.evtx	
18	☐	2018-04-25 15:58:50	.\Windows\System32\winevt\Logs	Application.evtx	.evtx	
19	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Search\Data\Applicatio…	CiST0000.000	.000	
20	☐	2018-04-25 15:58:50	.\Windows\System32\sru	SRU0000B.log	.log	
21	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows Defender\Scans	mpcache-2EAC22C2277EBAF4AE79EE94B422BCA8B9F13A…	.79	
22	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFaultHistory.db	.db	
23	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFaultHistory.db	.db	
24	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFaultHistory.db	.db	
25	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFgAppHistory.db	.db	
26	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFgAppHistory.db	.db	
27	☐	2018-04-25 15:58:50	.\Windows\Prefetch	AgGlFgAppHistory.db	.db	
28	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows Defender\Scans	mpcache-2EAC22C2277EBAF4AE79EE94B422BCA8B9F13A…	.79	
29	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows\WER\Temp	WER8EF.tmp	.tmp	
30	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows\WER\Temp	WER8EF.tmp	.tmp	
31	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows\WER\Temp	WER8EF.tmp	.tmp	
32	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows\WER\Temp	WER8EF.tmp.WERInternalMetadata.xml	.xml	
33	☐	2018-04-25 15:58:50	.\ProgramData\Microsoft\Windows\WER\Temp	WER8EF.tmp.WERInternalMetadata.xml	.xml	

C:\Cases\Analysis\NTFS\20230215212419_MFTECmd_$J_Output.csv

Total lines 277,572 | Visible lines 277,572 | Open files: 1 | Search options

- Search for the deleteme_T1551.004:



Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230215212419_MFTECmd_$J_Output.csv

Drag a column header here to group by that column

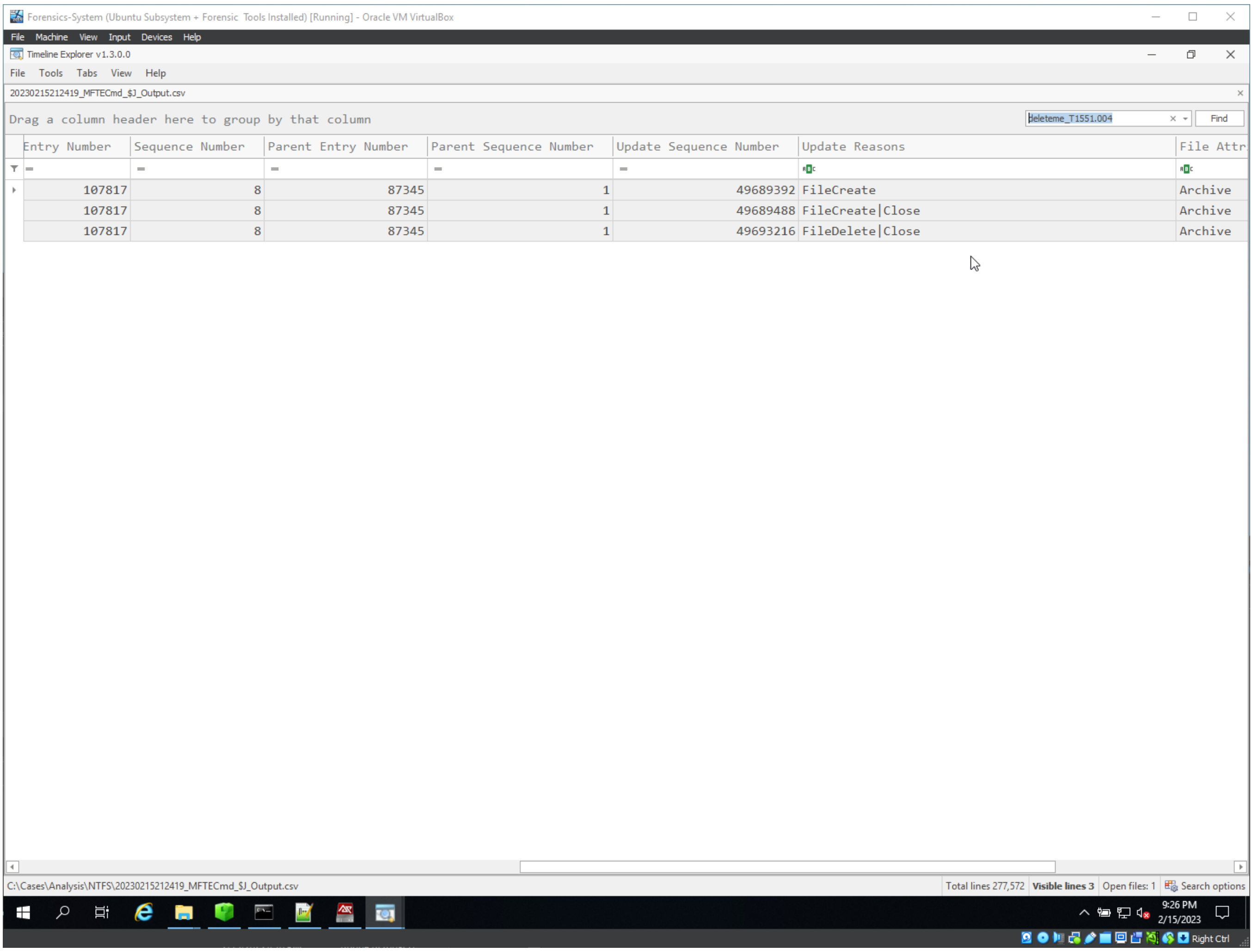
deleteme_T1551.004

Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Numbe
276688	□	2023-02-13 17:29:06	.\Users\IEUser\AppData\Local\Temp	deleteme_T1551.004	.004	107
276689	□	2023-02-13 17:29:06	.\Users\IEUser\AppData\Local\Temp	deleteme_T1551.004	.004	107
276718	□	2023-02-13 17:29:07	.\Users\IEUser\AppData\Local\Temp	deleteme_T1551.004	.004	107

C:\Cases\Analysis\NTFS\20230215212419_MFTECmd_$J_Output.csv

Total lines 277,572 **Visible lines 3** Open files: 1

9:26 PM
2/15/2023


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
20230215212419_MFTECmd_$J_Output.csv
Drag a column header here to group by that column
deleteme_T1551.004
Find
C:\Cases\Analysis\NTFS\20230215212419_MFTECmd_$J_Output.csv
Total lines 277,572
Visible lines 3
Open files: 1
Search options
9:26 PM
2/15/2023
Right Ctrl

Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	Update Sequence Number	Update Reasons	File Attr
107817	8	87345	1	49689392	FileCreate	Archive
107817	8	87345	1	49689488	FileCreate|Close	Archive
107817	8	87345	1	49693216	FileDelete|Close	Archive

Creation and deletion of “deleteme_T1551.004”

- 2023-02-13 17:29:06 - created

- 2023-02-13 17:29:07 - deleted

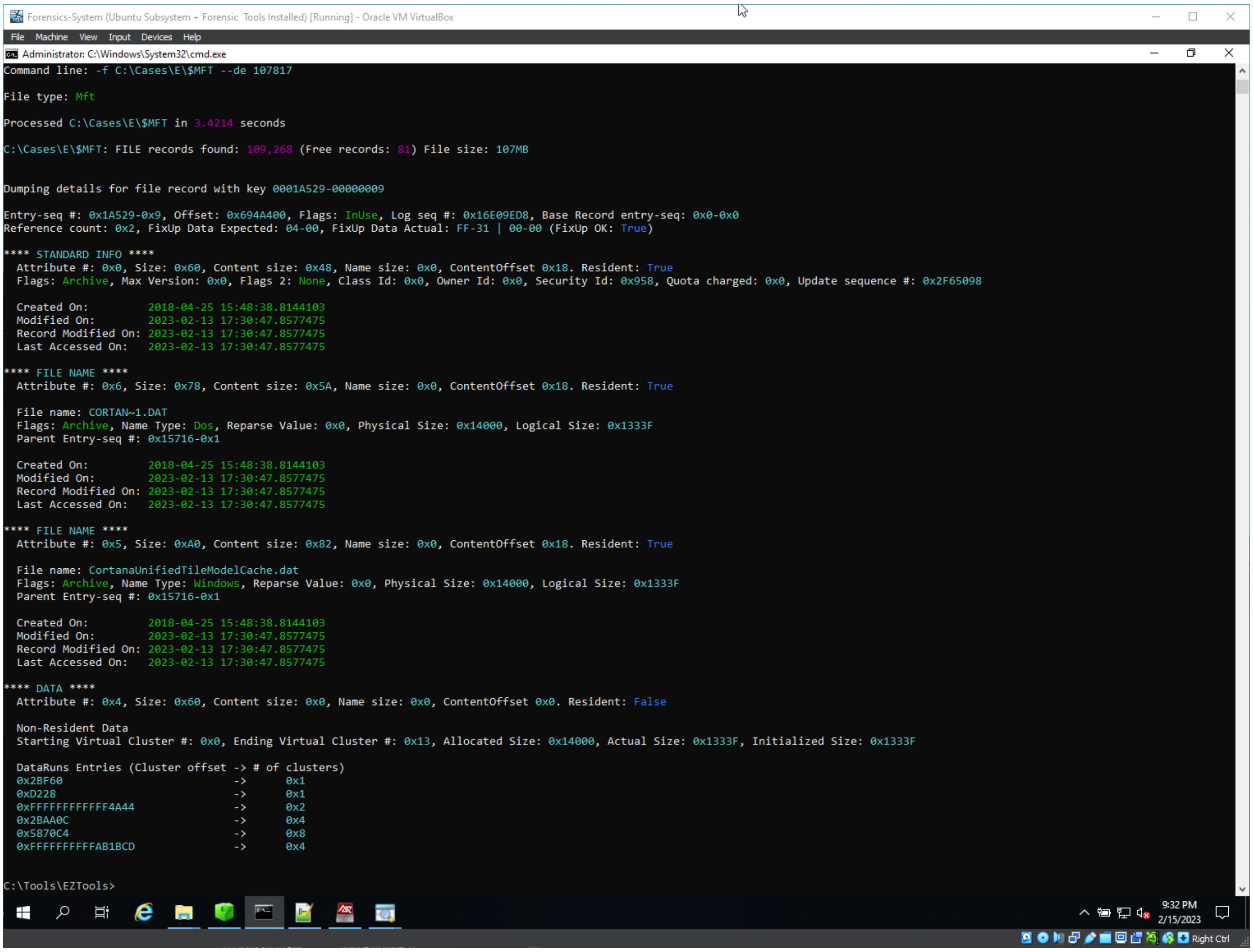
Entry number of the above file and the existence of it in the MFT

- **Entry Number**

  107817

- **It has been overwritten**

- Search for the entry number with MFTEcmd:



Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: C:\Windows\System32\cmd.exe
9:32 PM
2/15/2023
Right Ctrl

```
Command line: -f C:\Cases\E\$MFT --de 107817

File type: Mft

Processed C:\Cases\E\$MFT in 3.4214 seconds

C:\Cases\E\$MFT: FILE records found: 109,268 (Free records: 81) File size: 107MB


Dumping details for file record with key 0001A529-00000009

Entry-seq #: 0x1A529-0x9, Offset: 0x694A400, Flags: InUse, Log seq #: 0x16E09ED8, Base Record entry-seq: 0x0-0x0
Reference count: 0x2, FixUp Data Expected: 04-00, FixUp Data Actual: FF-31 | 00-00 (FixUp OK: True)

**** STANDARD INFO ****
  Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, ContentOffset 0x18. Resident: True
  Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x958, Quota charged: 0x0, Update sequence #: 0x2F65098

  Created On:         2018-04-25 15:48:38.8144103
  Modified On:        2023-02-13 17:30:47.8577475
  Record Modified On: 2023-02-13 17:30:47.8577475
  Last Accessed On:   2023-02-13 17:30:47.8577475

**** FILE NAME ****
  Attribute #: 0x6, Size: 0x78, Content size: 0x5A, Name size: 0x0, ContentOffset 0x18. Resident: True

  File name: CORTAN~1.DAT
  Flags: Archive, Name Type: Dos, Reparse Value: 0x0, Physical Size: 0x14000, Logical Size: 0x1333F
  Parent Entry-seq #: 0x15716-0x1

  Created On:         2018-04-25 15:48:38.8144103
  Modified On:        2023-02-13 17:30:47.8577475
  Record Modified On: 2023-02-13 17:30:47.8577475
  Last Accessed On:   2023-02-13 17:30:47.8577475

**** FILE NAME ****
  Attribute #: 0x5, Size: 0xA0, Content size: 0x82, Name size: 0x0, ContentOffset 0x18. Resident: True

  File name: CortanaUnifiedTileModelCache.dat
  Flags: Archive, Name Type: Windows, Reparse Value: 0x0, Physical Size: 0x14000, Logical Size: 0x1333F
  Parent Entry-seq #: 0x15716-0x1

  Created On:         2018-04-25 15:48:38.8144103
  Modified On:        2023-02-13 17:30:47.8577475
  Record Modified On: 2023-02-13 17:30:47.8577475
  Last Accessed On:   2023-02-13 17:30:47.8577475

**** DATA ****
  Attribute #: 0x4, Size: 0x60, Content size: 0x0, Name size: 0x0, ContentOffset 0x0. Resident: False

  Non-Resident Data
  Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x13, Allocated Size: 0x14000, Actual Size: 0x1333F, Initialized Size: 0x1333F

  DataRuns Entries (Cluster offset -> # of clusters)
  0x2BF60                         ->      0x1
  0xD228                          ->      0x1
  0xFFFFFFFFFFFF4A44              ->      0x2
  0x2BAA0C                        ->      0x4
  0x5870C4                        ->      0x8
  0xFFFFFFFFFFFAB1BCD             ->      0x4


C:\Tools\EZTools>
```

- The particular entry is in use, and it contains a file that has different timestamps.
- Another File name
- Another Long File name version.