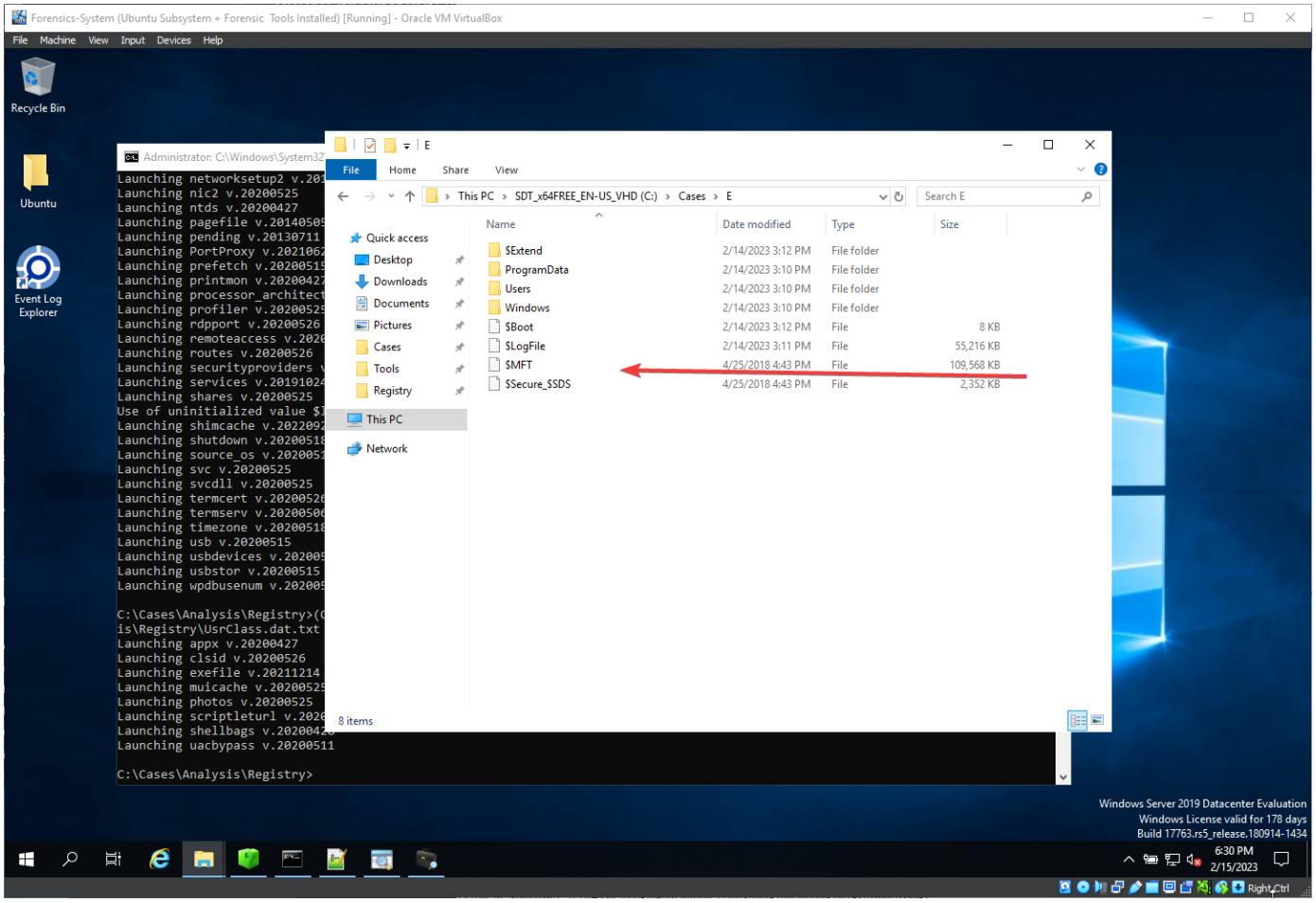
Master File Table (MFT):

- Overview
- MFT Records
- MFT parsing and analysis
- File timestamps (MACB)
- File stomping

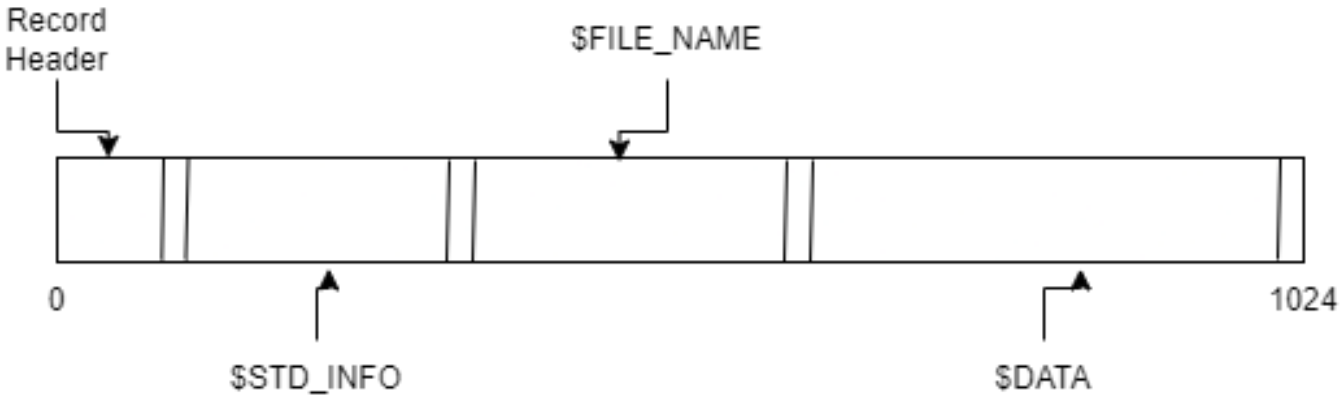
Overview

- Location:



- Any file that is created, read, stored, modified or deleted on the file system , the operating system lets NTFS handle these operations using the $MFT file, to create entries for each file or folder.

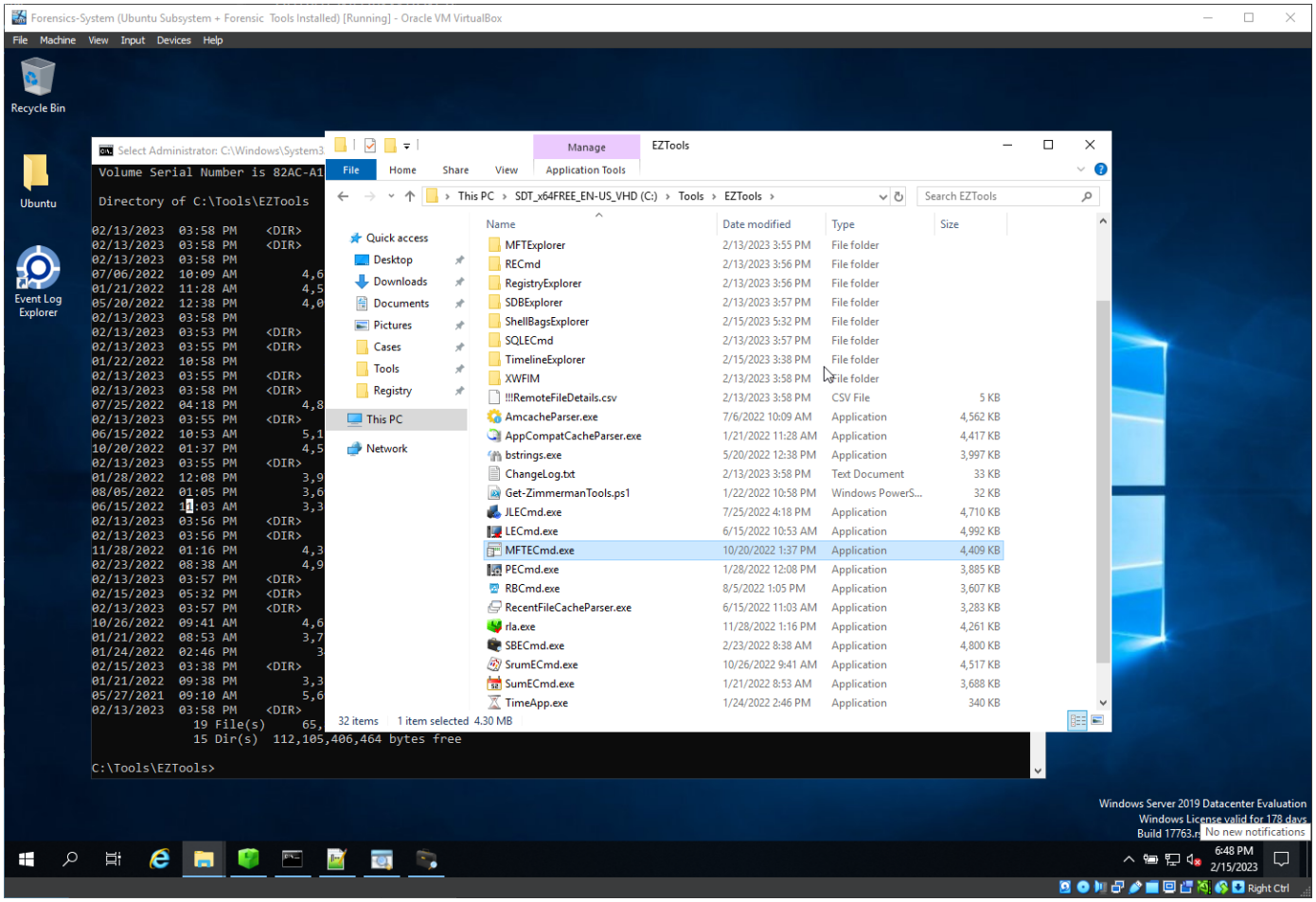
- Master File Table Structure:



- A record is 1024 B.
- Record Header contains information about unique entry number of files. After that, it has a flag InUse that remembers if a file is marked as deleted or not by the operating system, the record of that file will not be deleted, will just be marked as in use or not .
- Important to know, if we parse the MFT , we could come across files that does not exist anymore.
- $STD_INFO : we get timestamps (Could be changed)
- $FILE_NAME : stores a filename, and also contains four (Cannot be changed) different types of timestamps
- $DATA : stores the data of a file , if it is small enough, it will be contained there , if not , it will contain pointers to allocated space on the disk for the file system to know where to find that particular file from the file record of MFT
- Between $DATA and the final of the entry, there exists a Slack Space , that might contain data from a previous record .

MFT Records

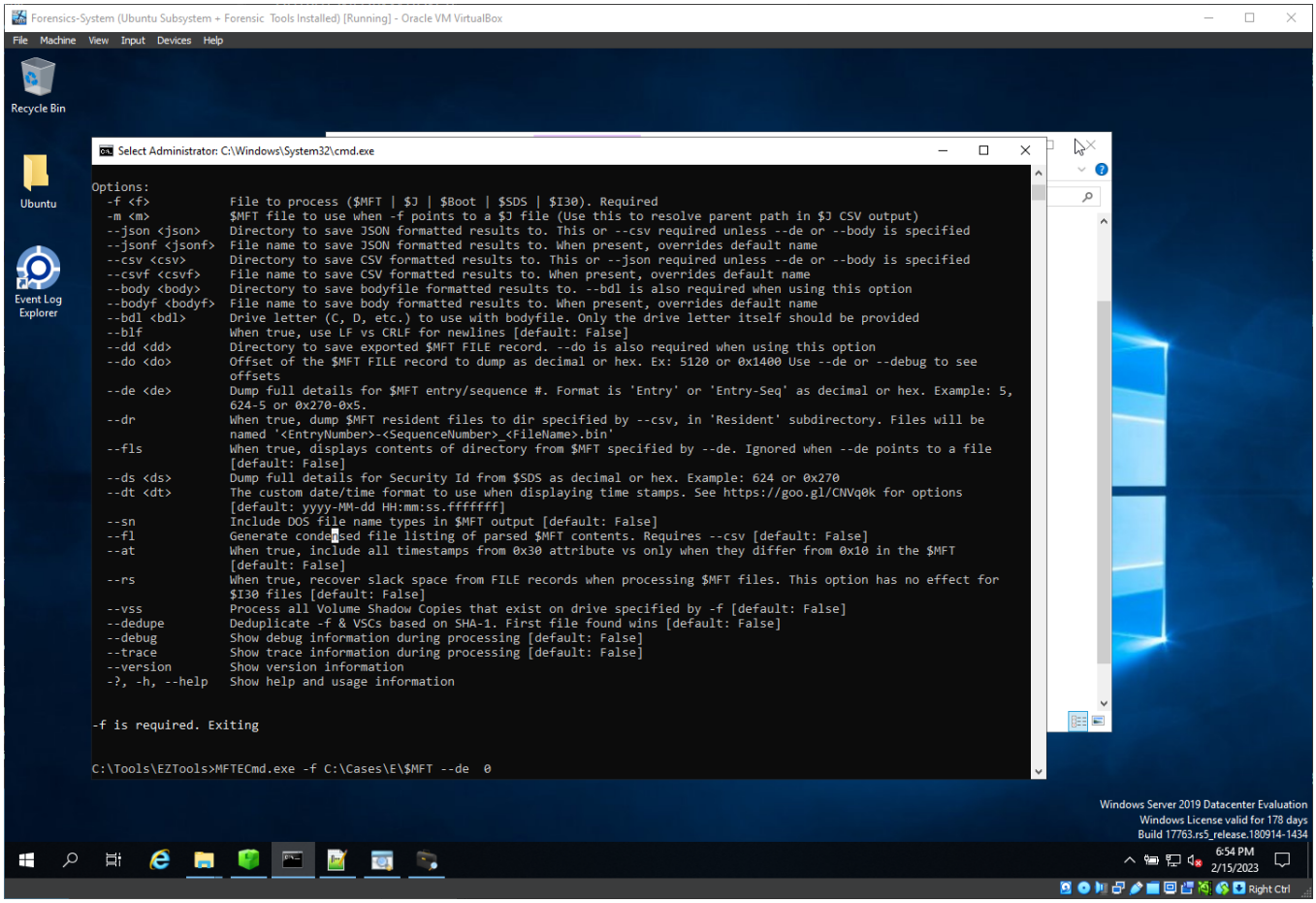
- We will use an application called MFTECmd.exe from EZTools:

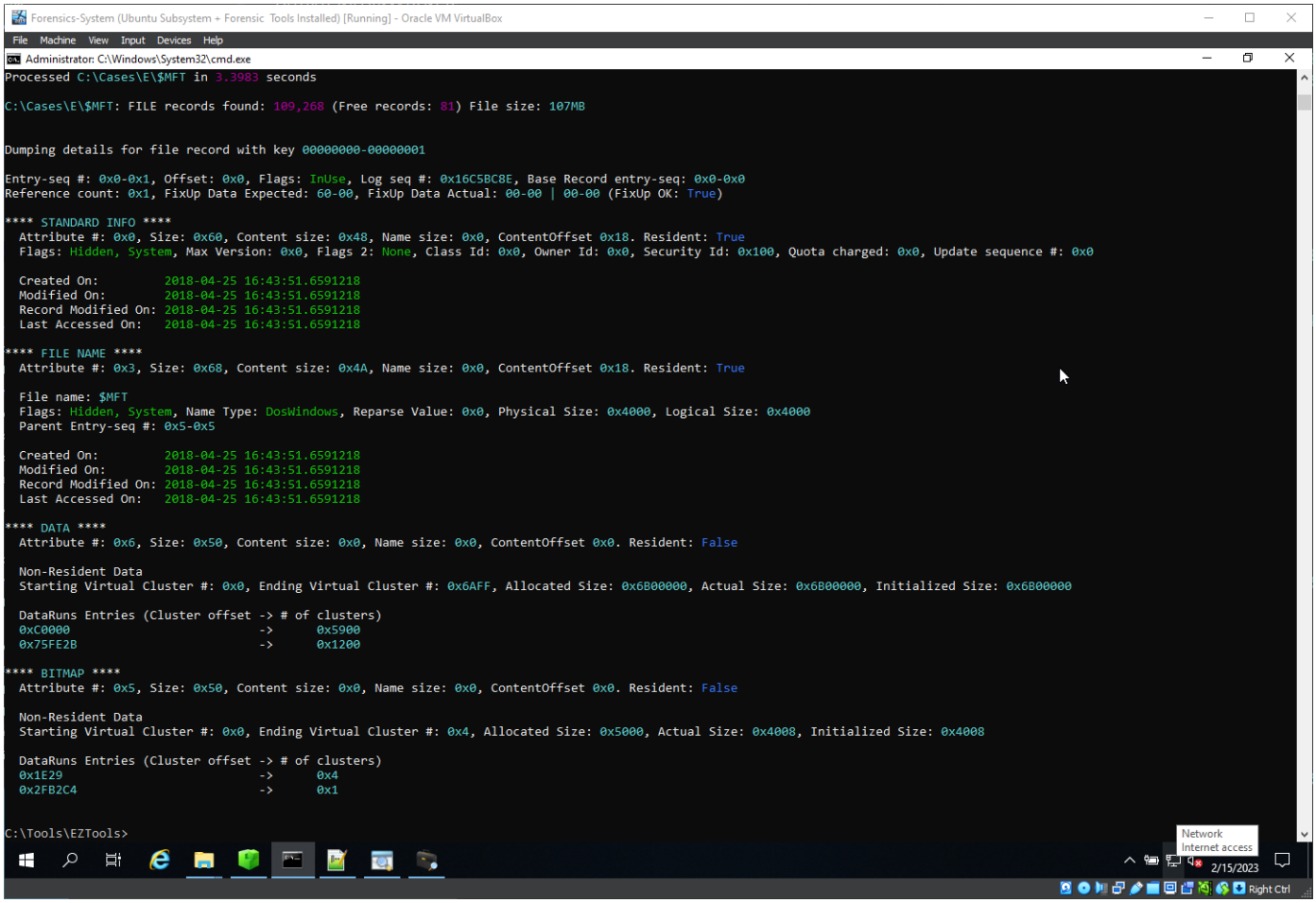


- Based on : https://www.ntfs.com/ntfs-system-files.htm , these below are examples of metadata , before the actual data is stored.

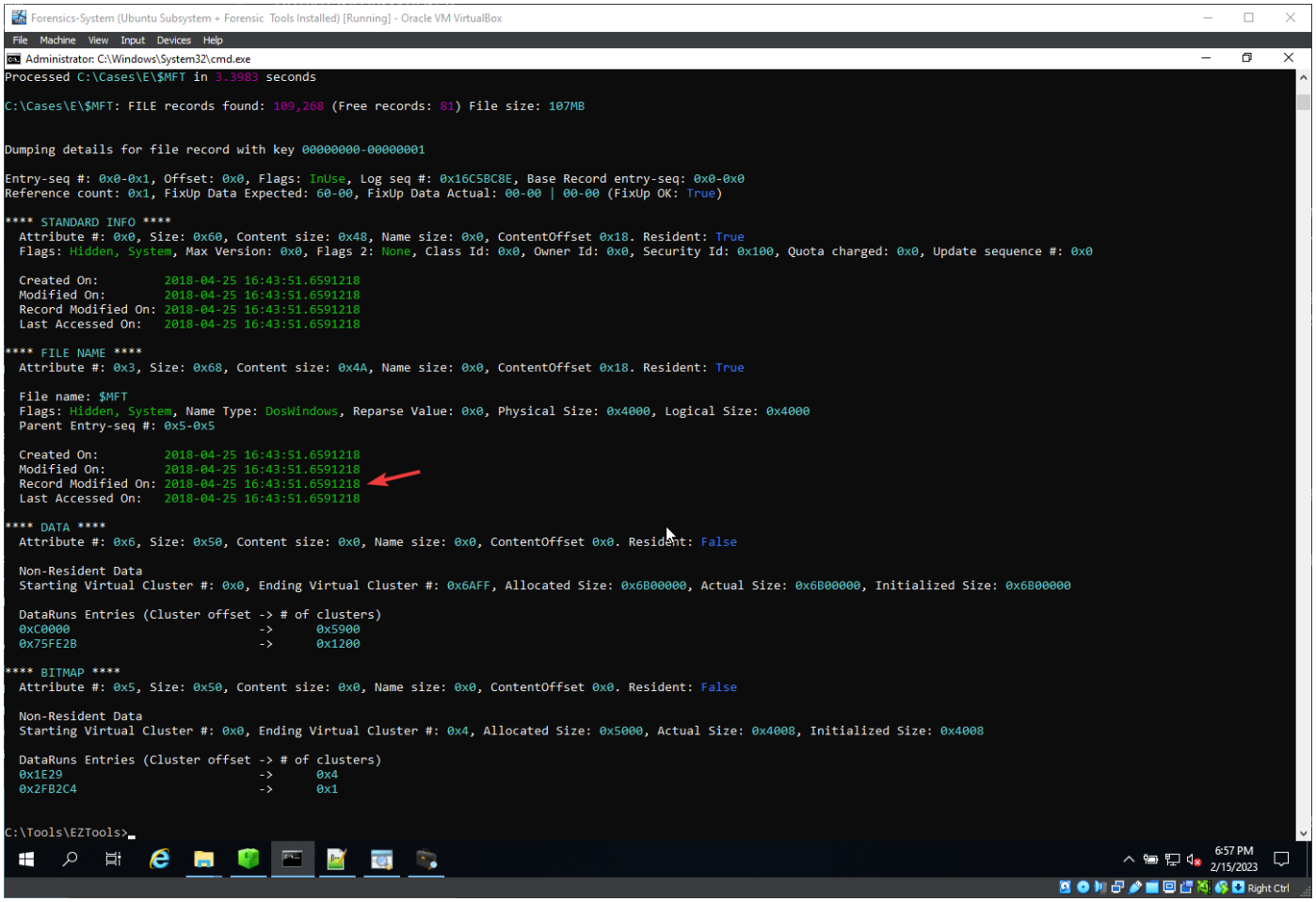
System File	File Name	MFT Record	Purpose of the File
Master file table	$Mft	0	Contains one base file record for each file and folder on an NTFS volume. If the allocation information for a file or folder is too large to fit within a single record, other file records are allocated as well.
Master file table 2	$MftMirr	1	A duplicate image of the first four records of the MFT. This file guarantees access to the MFT in case of a single-sector failure.
Log file	$LogFile	2	Contains a list of transaction steps used for NTFS recoverability. Log file size depends on the volume size and can be as large as 4 MB. It is used by Windows NT/2000 to restore consistency to NTFS after a system failure.

- The following command will parse the $MFT and query us the first entry

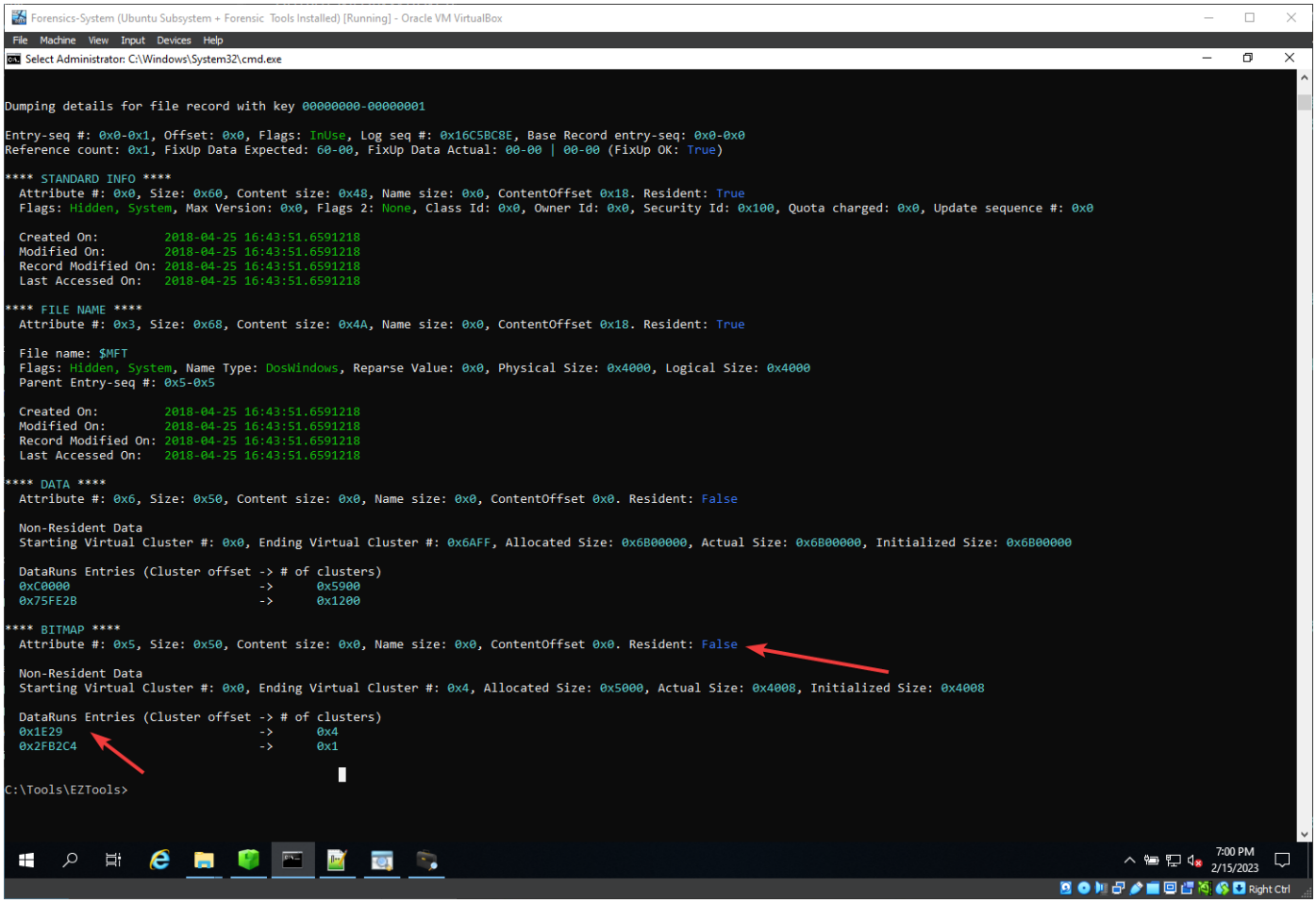

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Event Log Explorer
Select Administrator: C:\Windows\System32\cmd.exe
Options:
-f <f> File to process ($MFT | $J | $Boot | $SDS | $I30). Required
-m <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]
--version Show version information
-?, -h, --help Show help and usage information
-f is required. Exiting
C:\Tools\EZTools>MFTECmd.exe -f C:\Cases\E\$MFT --de 0
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
6:54 PM
2/15/2023
Right Ctrl



- InUse – it is not deleted.
- Resident: The information is stored in the record itself, if it s true, if it is not , the data is somewhere on the disk and we would see a pointer , below



- Record Modified On: means when the MFT Record Table it is being modified. For example, if the name of the record is changed , Record Modified will be changed, in relation with the MFT
-
- Example of Resident: False

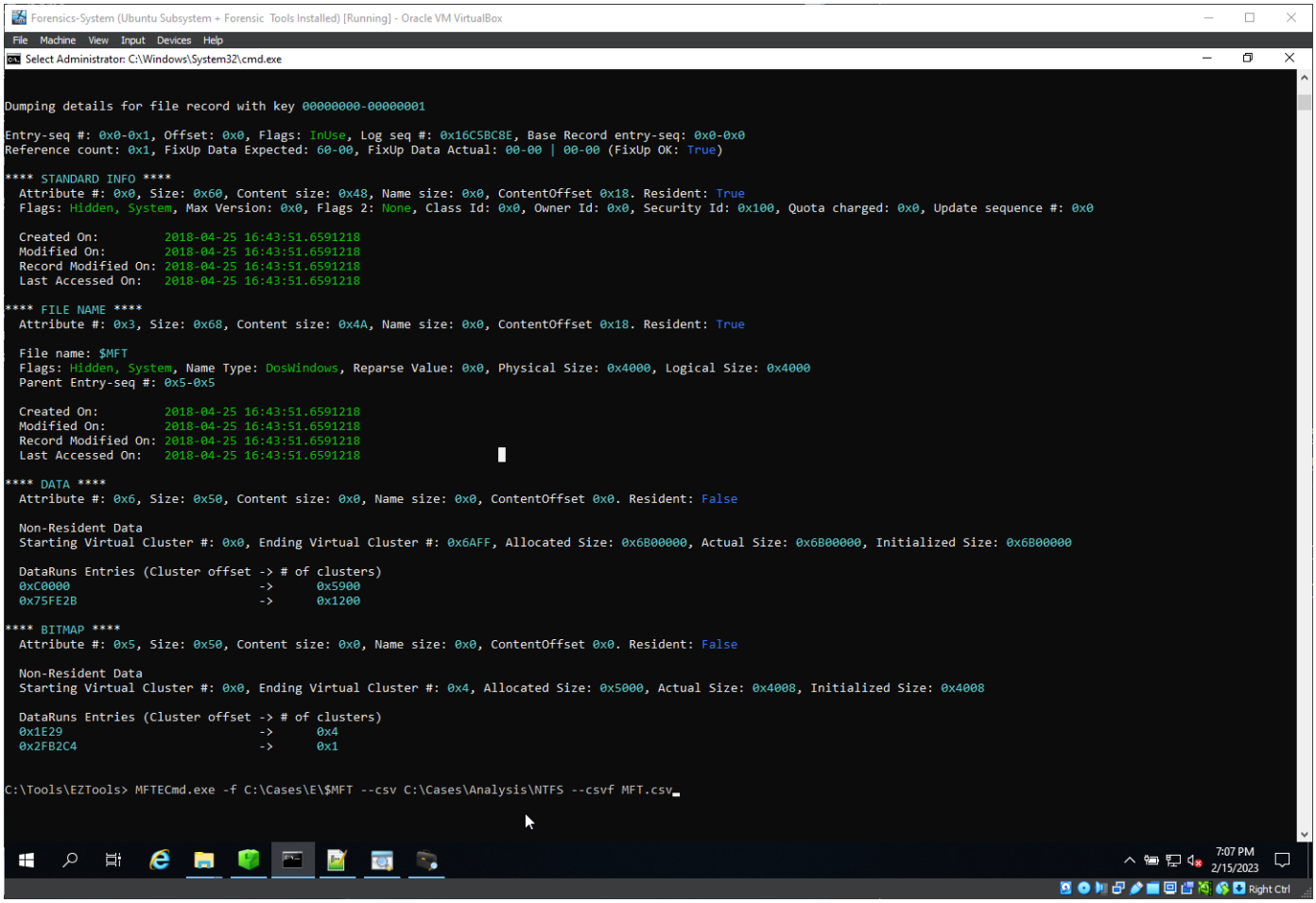


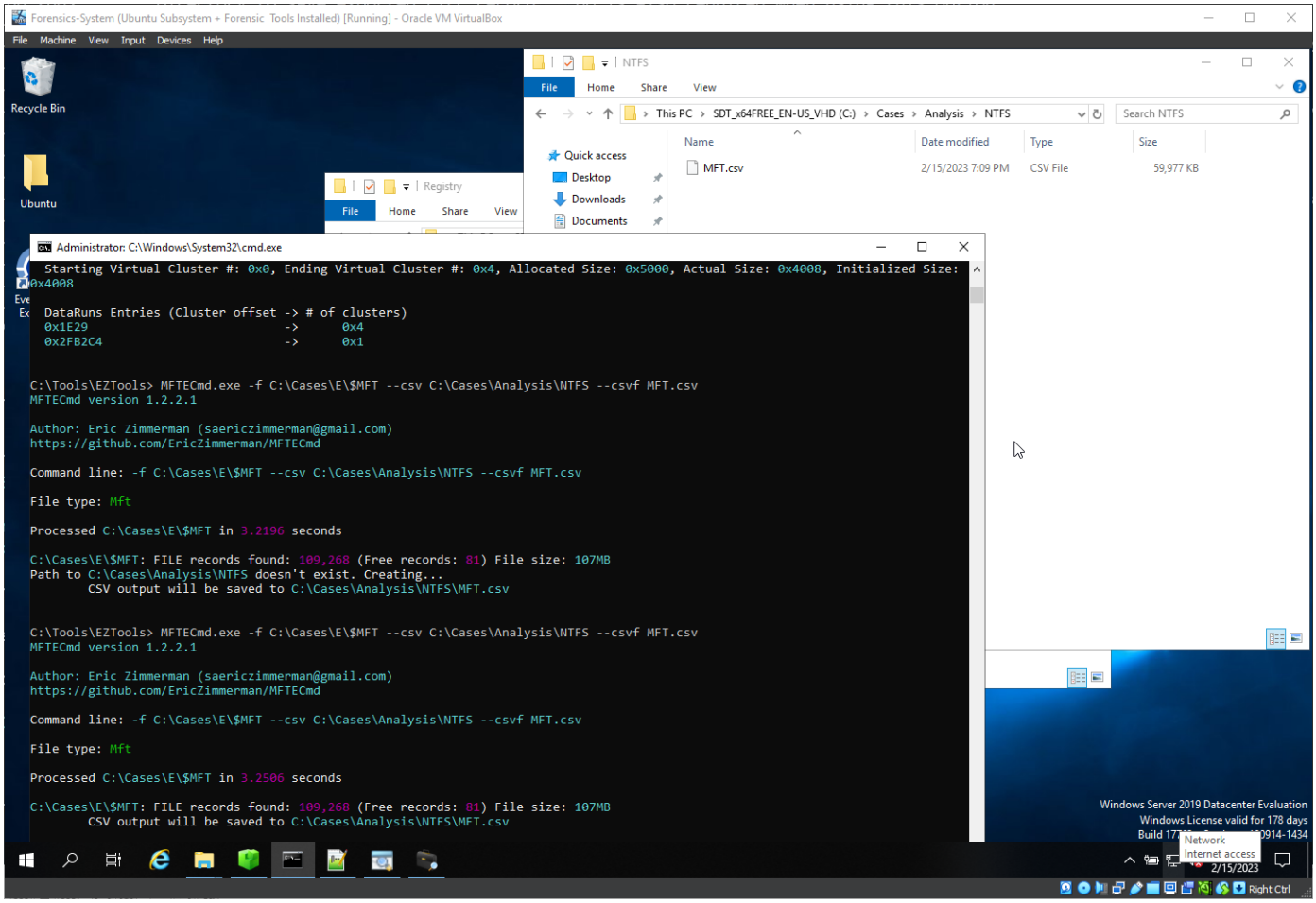
- UserAssist – applications opened
- UserAssist – applications opened

MFT parsing and analysis

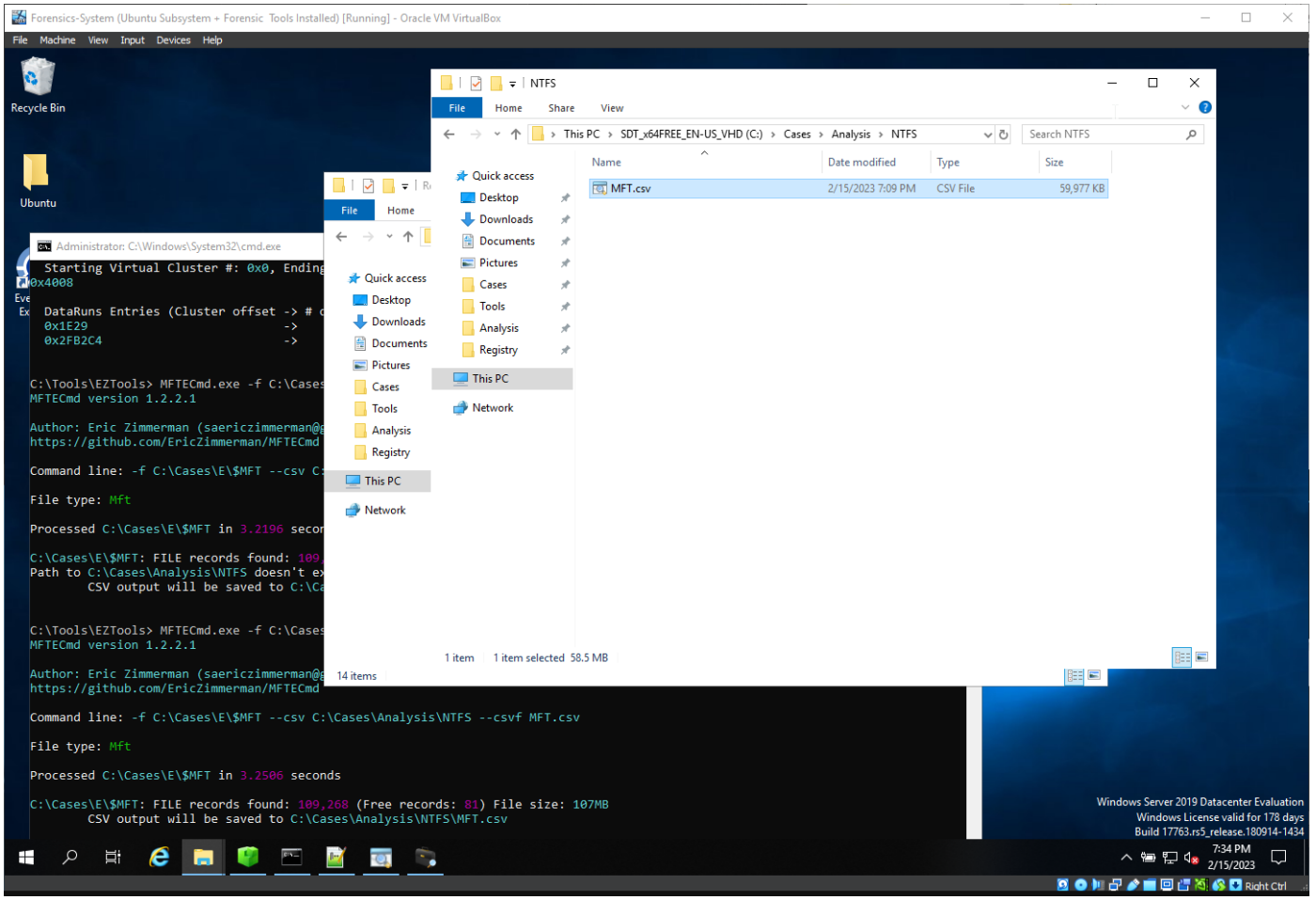
- Find :
  - Files located in My Computer\CLSID_Desktop\PWF-main\PWF-main\AtomicRedTeam
  - MFT Entry Number for “ART-attack.ps1”
  - MACB timestamps for the above file
  - Was the same file , timestomped?

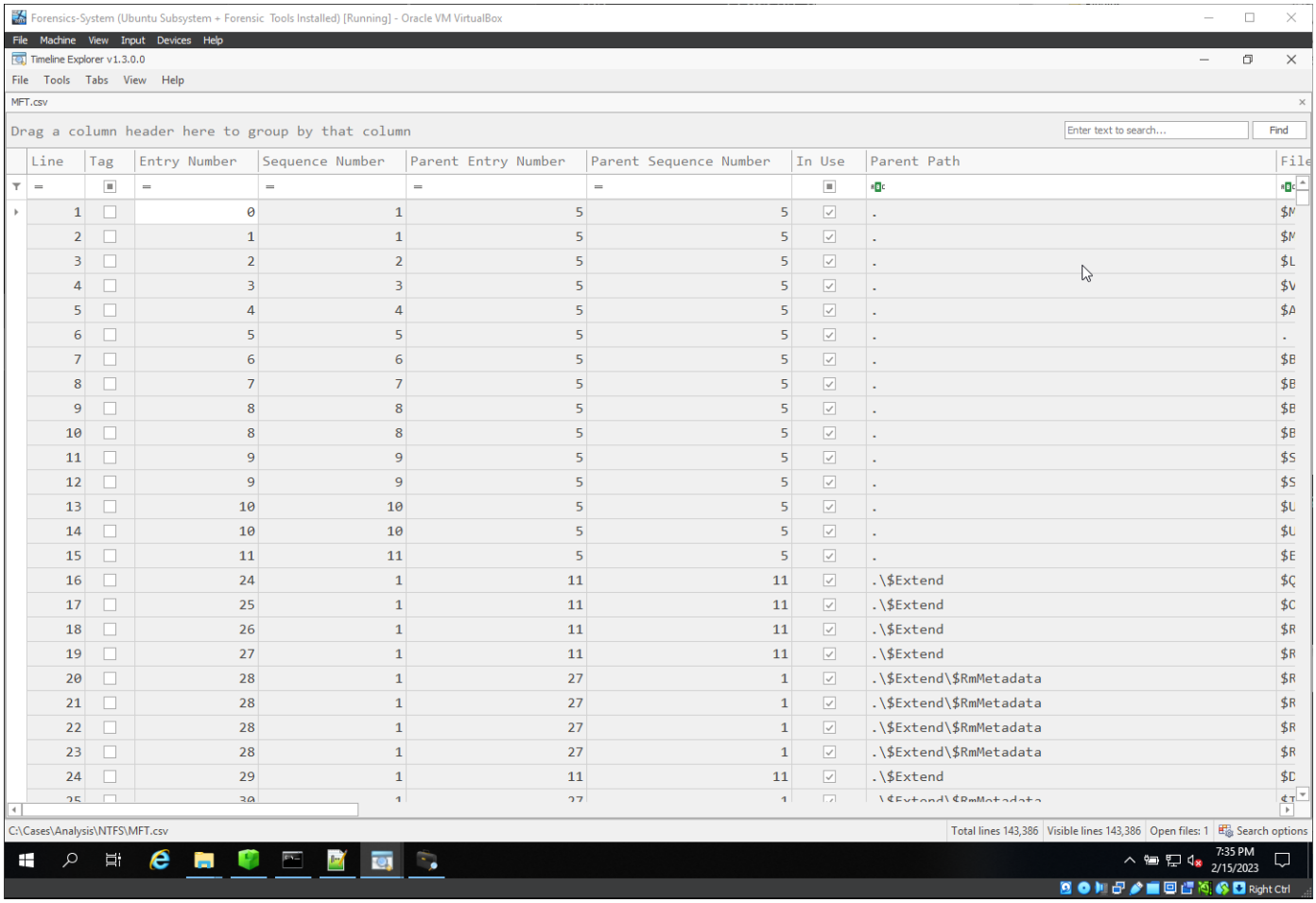
- Convert the file to csv:

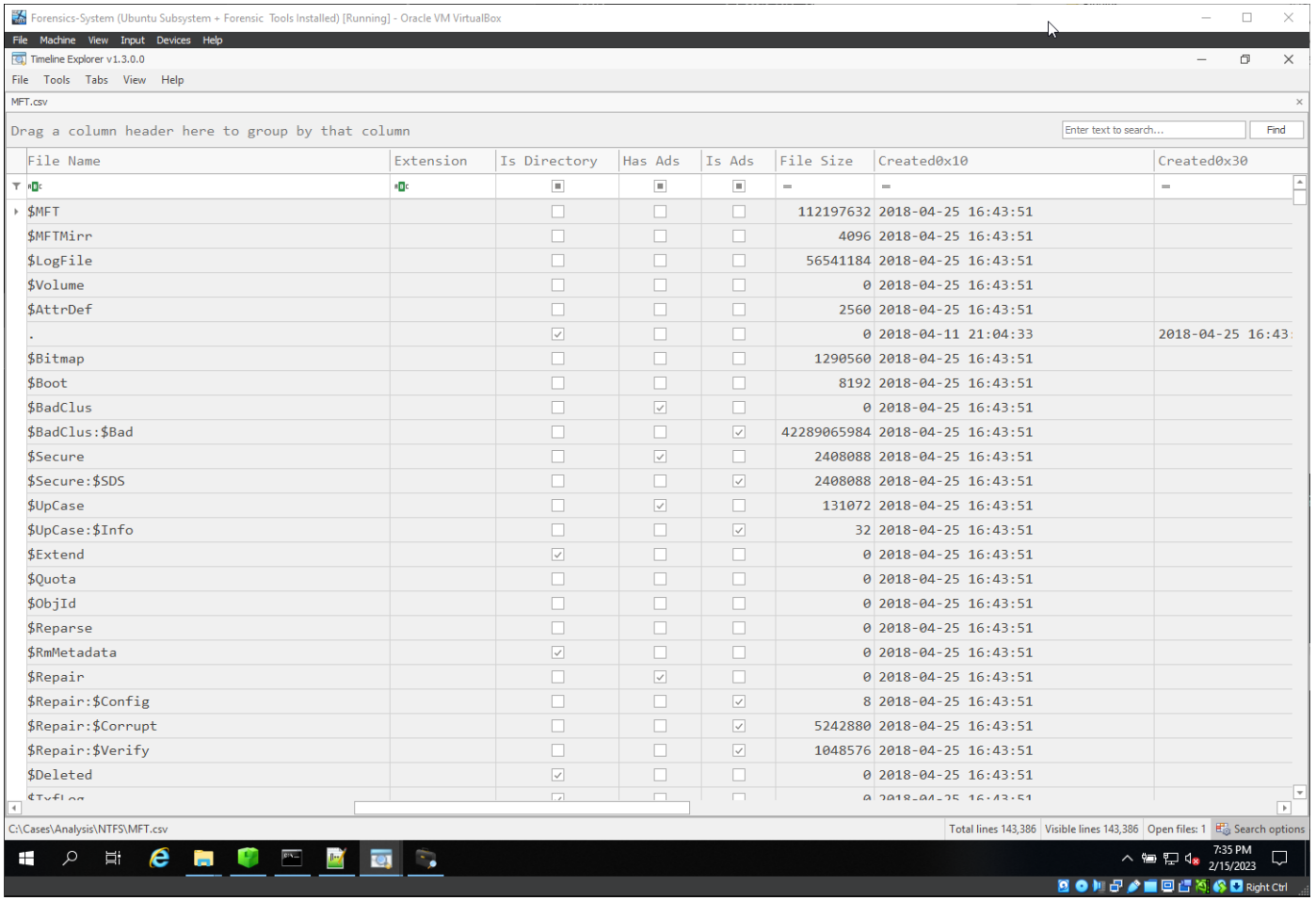

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Administrator: C:\Windows\System32\cmd.exe
Dumping details for file record with key 00000000-00000001
Entry-seq #: 0x0-0x1, Offset: 0x0, Flags: InUse, Log seq #: 0x16C5BC8E, Base Record entry-seq: 0x0-0x0
Reference count: 0x1, FixUp Data Expected: 60-00, FixUp Data Actual: 00-00 | 00-00 (FixUp OK: True)
**** STANDARD INFO ****
Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, ContentOffset 0x18. Resident: True
Flags: Hidden, System, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x100, Quota charged: 0x0, Update sequence #: 0x0
Created On: 2018-04-25 16:43:51.6591218
Modified On: 2018-04-25 16:43:51.6591218
Record Modified On: 2018-04-25 16:43:51.6591218
Last Accessed On: 2018-04-25 16:43:51.6591218
**** 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: 2018-04-25 16:43:51.6591218
Modified On: 2018-04-25 16:43:51.6591218
Record Modified On: 2018-04-25 16:43:51.6591218
Last Accessed On: 2018-04-25 16:43:51.6591218
**** 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 #: 0x6AFF, Allocated Size: 0x6B00000, Actual Size: 0x6B00000, Initialized Size: 0x6B00000
DataRuns Entries (Cluster offset -> # of clusters)
0xC0000 -> 0x5900
0x75FE2B -> 0x1200
**** BITMAP ****
Attribute #: 0x5, Size: 0x50, 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)
0x1E29 -> 0x4
0x2FB2C4 -> 0x1
C:\Tools\EZTools> MFTECmd.exe -f C:\Cases\E\$MFT --csv C:\Cases\Analysis\NTFS --csvf MFT.csv
7:07 PM
2/15/2023
Right Ctrl

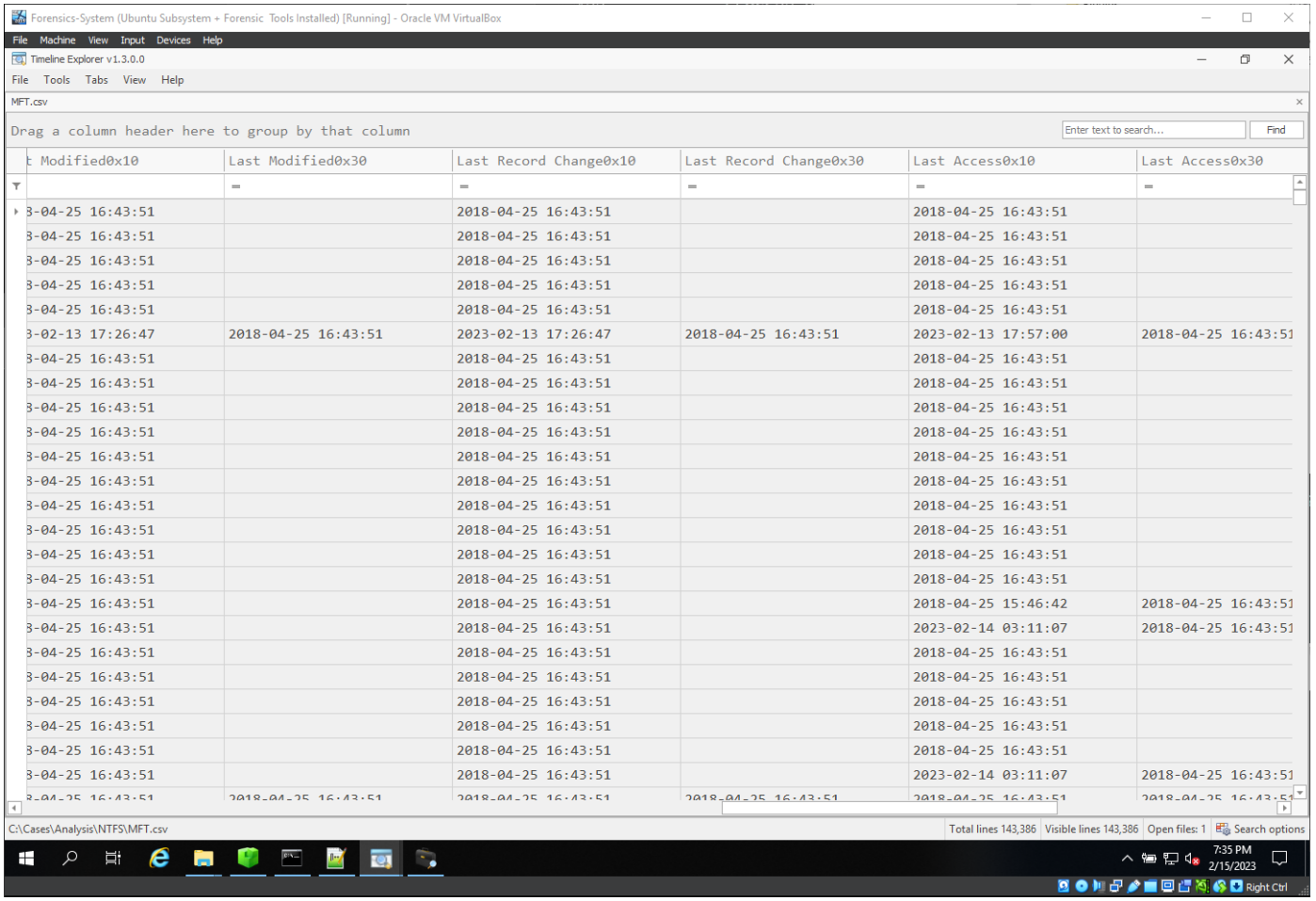


- Open with TimeLineExplorer:


Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Ubuntu
Administrator: C:\Windows\System32\cmd.exe
Starting Virtual Cluster #: 0x0, Ending
0x4008
DataRuns Entries (Cluster offset -> # c
0x1E29 ->
0x2FB2C4 ->
C:\Tools\EZTools> MFTECmd.exe -f C:\Cases
MFTECmd version 1.2.2.1
Author: Eric Zimmerman (saericzimmerman@g
https://github.com/EricZimmerman/MFTECmd
Command line: -f C:\Cases\E\$MFT --csv C:
File type: Mft
Processed C:\Cases\E\$MFT in 3.2196 secon
C:\Cases\E\$MFT: FILE records found: 109,
Path to C:\Cases\Analysis\NTFS doesn't ex
CSV output will be saved to C:\Ca
C:\Tools\EZTools> MFTECmd.exe -f C:\Cases
MFTECmd version 1.2.2.1
Author: Eric Zimmerman (saericzimmerman@g
https://github.com/EricZimmerman/MFTECmd
Command line: -f C:\Cases\E\$MFT --csv C:\Cases\Analysis\NTFS --csvf MFT.csv
File type: Mft
Processed C:\Cases\E\$MFT in 3.2506 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\MFT.csv
NTFS
File Home Share View
This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > NTFS
Search NTFS
Quick access
Desktop
Downloads
Documents
Pictures
Cases
Tools
Analysis
Registry
This PC
Network
Name
Date modified
Type
Size
MFT.csv
2/15/2023 7:09 PM
CSV File
59,977 KB
1 item
1 item selected 58.5 MB
14 items
Windows Server 2019 Datacenter Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
7:34 PM
2/15/2023
Right Ctrl


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
Line | Tag | Entry Number | Sequence Number | Parent Entry Number | Parent Sequence Number | In Use | Parent Path | File
1 | 0 | 1 | 5 | 5 | . | $M
2 | 1 | 1 | 5 | 5 | . | $M
3 | 2 | 2 | 5 | 5 | . | $L
4 | 3 | 3 | 5 | 5 | . | $V
5 | 4 | 4 | 5 | 5 | . | $A
6 | 5 | 5 | 5 | 5 | . | .
7 | 6 | 6 | 5 | 5 | . | $B
8 | 7 | 7 | 5 | 5 | . | $B
9 | 8 | 8 | 5 | 5 | . | $B
10 | 8 | 8 | 5 | 5 | . | $B
11 | 9 | 9 | 5 | 5 | . | $S
12 | 9 | 9 | 5 | 5 | . | $S
13 | 10 | 10 | 5 | 5 | . | $U
14 | 10 | 10 | 5 | 5 | . | $U
15 | 11 | 11 | 5 | 5 | . | $E
16 | 24 | 1 | 11 | 11 | .\$Extend | $Q
17 | 25 | 1 | 11 | 11 | .\$Extend | $C
18 | 26 | 1 | 11 | 11 | .\$Extend | $R
19 | 27 | 1 | 11 | 11 | .\$Extend | $R
20 | 28 | 1 | 27 | 1 | .\$Extend\$RmMetadata | $R
21 | 28 | 1 | 27 | 1 | .\$Extend\$RmMetadata | $R
22 | 28 | 1 | 27 | 1 | .\$Extend\$RmMetadata | $R
23 | 28 | 1 | 27 | 1 | .\$Extend\$RmMetadata | $R
24 | 29 | 1 | 11 | 11 | .\$Extend | $D
C:\Cases\Analysis\NTFS\MFT.csv
Total lines 143,386 | Visible lines 143,386 | Open files: 1 | Search options
7:35 PM
2/15/2023
Right Ctrl

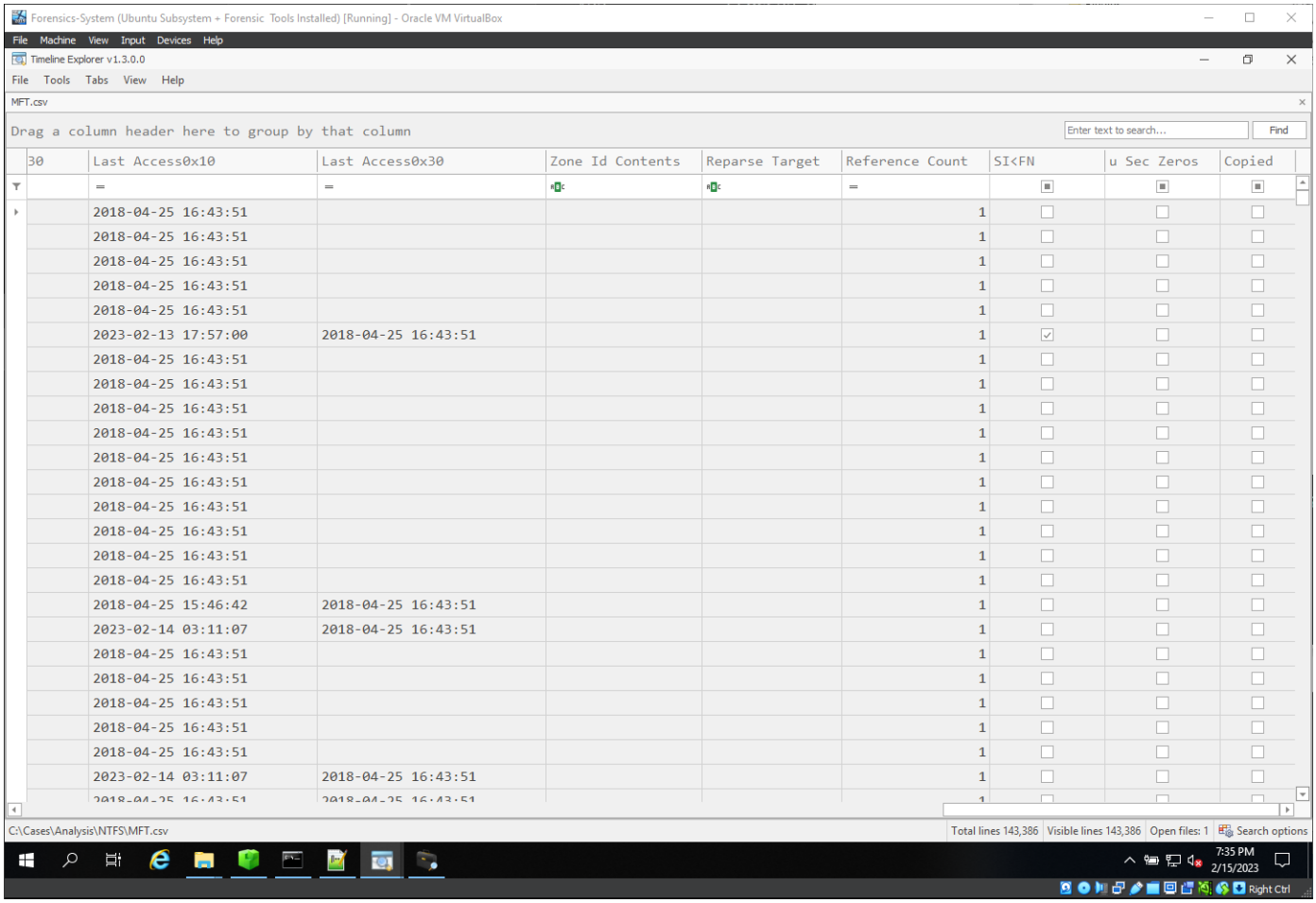

Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
MFT.csv
Drag a column header here to group by that column
Enter text to search...
Find
File Name | Extension | Is Directory | Has Ads | Is Ads | File Size | Created0x10 | Created0x30
$MFT 112197632 2018-04-25 16:43:51
$MFTMirr 4096 2018-04-25 16:43:51
$LogFile 56541184 2018-04-25 16:43:51
$Volume 0 2018-04-25 16:43:51
$AttrDef 2560 2018-04-25 16:43:51
. 0 2018-04-11 21:04:33 2018-04-25 16:43
$Bitmap 1290560 2018-04-25 16:43:51
$Boot 8192 2018-04-25 16:43:51
$BadClus 0 2018-04-25 16:43:51
$BadClus:$Bad 42289065984 2018-04-25 16:43:51
$Secure 2408088 2018-04-25 16:43:51
$Secure:$SDS 2408088 2018-04-25 16:43:51
$UpCase 131072 2018-04-25 16:43:51
$UpCase:$Info 32 2018-04-25 16:43:51
$Extend 0 2018-04-25 16:43:51
$Quota 0 2018-04-25 16:43:51
$ObjId 0 2018-04-25 16:43:51
$Reparse 0 2018-04-25 16:43:51
$RmMetadata 0 2018-04-25 16:43:51
$Repair 0 2018-04-25 16:43:51
$Repair:$Config 8 2018-04-25 16:43:51
$Repair:$Corrupt 5242880 2018-04-25 16:43:51
$Repair:$Verify 1048576 2018-04-25 16:43:51
$Deleted 0 2018-04-25 16:43:51
C:\Cases\Analysis\NTFS\MFT.csv
Total lines 143,386 Visible lines 143,386 Open files: 1 Search options
7:35 PM
2/15/2023
Right Ctrl



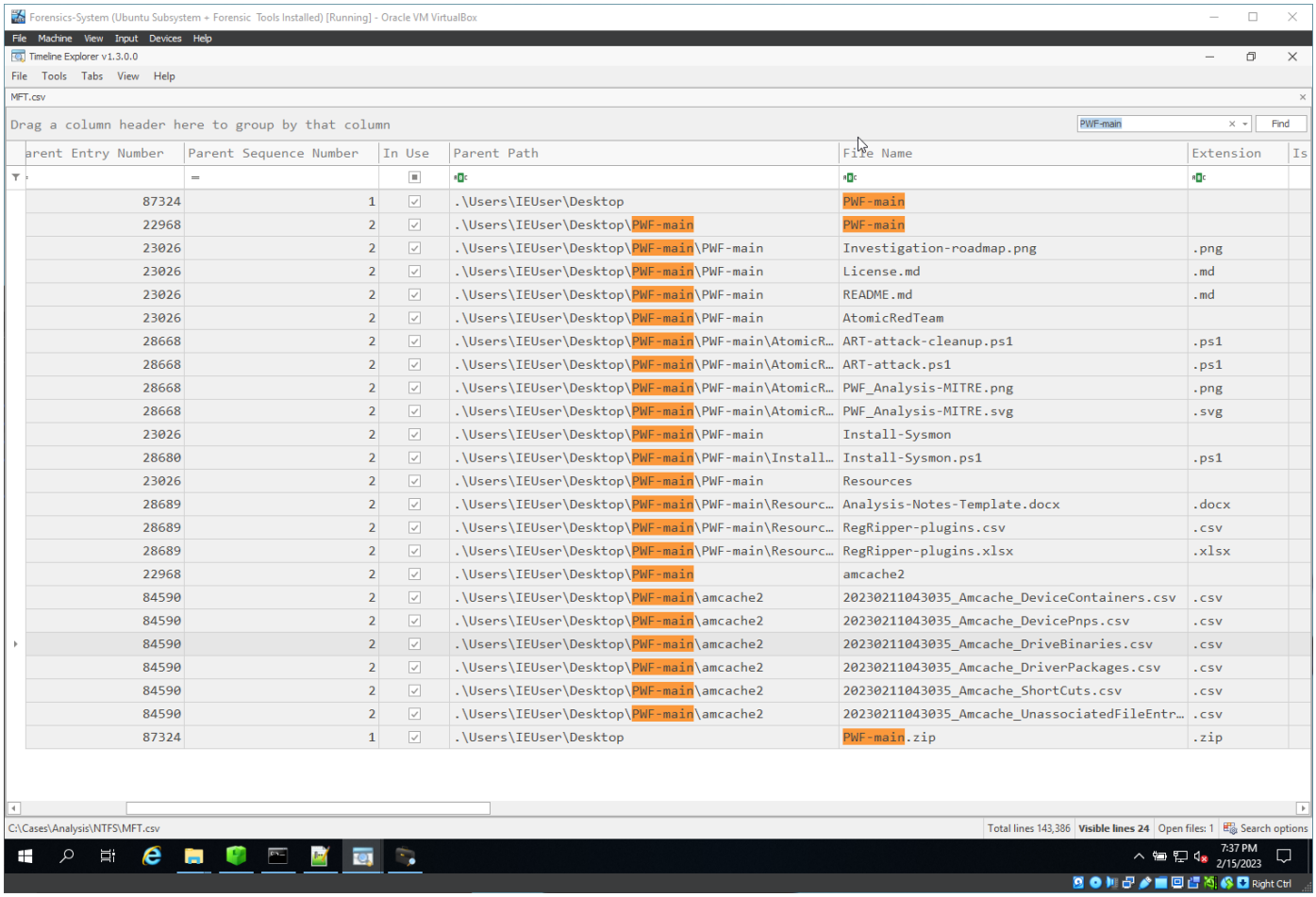
t Modified0x10	Last Modified0x30	Last Record Change0x10	Last Record Change0x30	Last Access0x10	Last Access0x30
=	=	=	=	=	=
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-02-13 17:26:47	2018-04-25 16:43:51	2023-02-13 17:26:47	2018-04-25 16:43:51	2023-02-13 17:57:00	2018-04-25 16:43:51
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 15:46:42	2018-04-25 16:43:51
3-04-25 16:43:51		2018-04-25 16:43:51		2023-02-14 03:11:07	2018-04-25 16:43:51
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2018-04-25 16:43:51	
3-04-25 16:43:51		2018-04-25 16:43:51		2023-02-14 03:11:07	2018-04-25 16:43:51
3-04-25 16:43:51	2018-04-25 16:43:51	2018-04-25 16:43:51	2018-04-25 16:43:51	2018-04-25 16:43:51	2018-04-25 16:43:51

C:\Cases\Analysis\NTFS\MFT.csv | Total lines 143,386 | Visible lines 143,386 | Open files: 1

7:35 PM
2/15/2023



- Files located in My Computer\CLSID_Desktop\PWF-main\PWF-main\AtomicRedTeam



ART-attack-cleanup.ps1

ART-attack.ps1

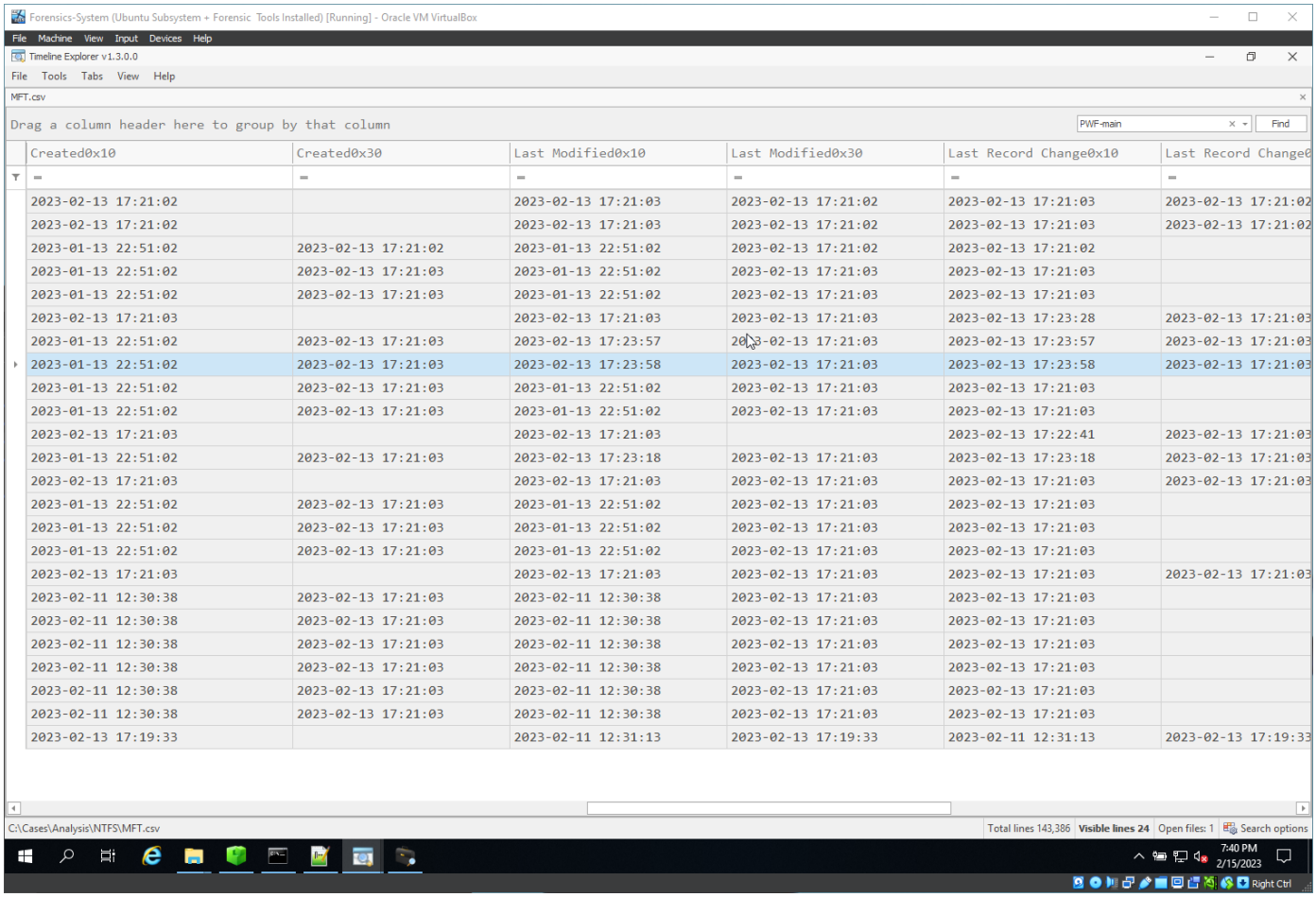
PWF_Analysis-MITRE.png

PWF_Analysis-MITRE.svg

- MFT Entry Number for “ART-attack.ps1”

Entry Number

28674



Created0x10	Created0x30	Last Modified0x10	Last Modified0x30	Last Record Change0x10	Last Record Change0
2023-02-13 17:21:02		2023-02-13 17:21:03	2023-02-13 17:21:02	2023-02-13 17:21:03	2023-02-13 17:21:02
2023-02-13 17:21:02		2023-02-13 17:21:03	2023-02-13 17:21:02	2023-02-13 17:21:03	2023-02-13 17:21:02
2023-01-13 22:51:02	2023-02-13 17:21:02	2023-01-13 22:51:02	2023-02-13 17:21:02	2023-02-13 17:21:02	
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-13 17:21:03		2023-02-13 17:21:03	2023-02-13 17:21:03	2023-02-13 17:23:28	2023-02-13 17:21:03
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:23:57	2023-02-13 17:21:03	2023-02-13 17:23:57	2023-02-13 17:21:03
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:23:58	2023-02-13 17:21:03	2023-02-13 17:23:58	2023-02-13 17:21:03
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-13 17:21:03		2023-02-13 17:21:03		2023-02-13 17:22:41	2023-02-13 17:21:03
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:23:18	2023-02-13 17:21:03	2023-02-13 17:23:18	2023-02-13 17:21:03
2023-02-13 17:21:03		2023-02-13 17:21:03	2023-02-13 17:21:03	2023-02-13 17:21:03	2023-02-13 17:21:03
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-01-13 22:51:02	2023-02-13 17:21:03	2023-01-13 22:51:02	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-13 17:21:03		2023-02-13 17:21:03	2023-02-13 17:21:03	2023-02-13 17:21:03	2023-02-13 17:21:03
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-11 12:30:38	2023-02-13 17:21:03	2023-02-13 17:21:03	
2023-02-13 17:19:33		2023-02-11 12:31:13	2023-02-13 17:19:33	2023-02-11 12:31:13	2023-02-13 17:19:33

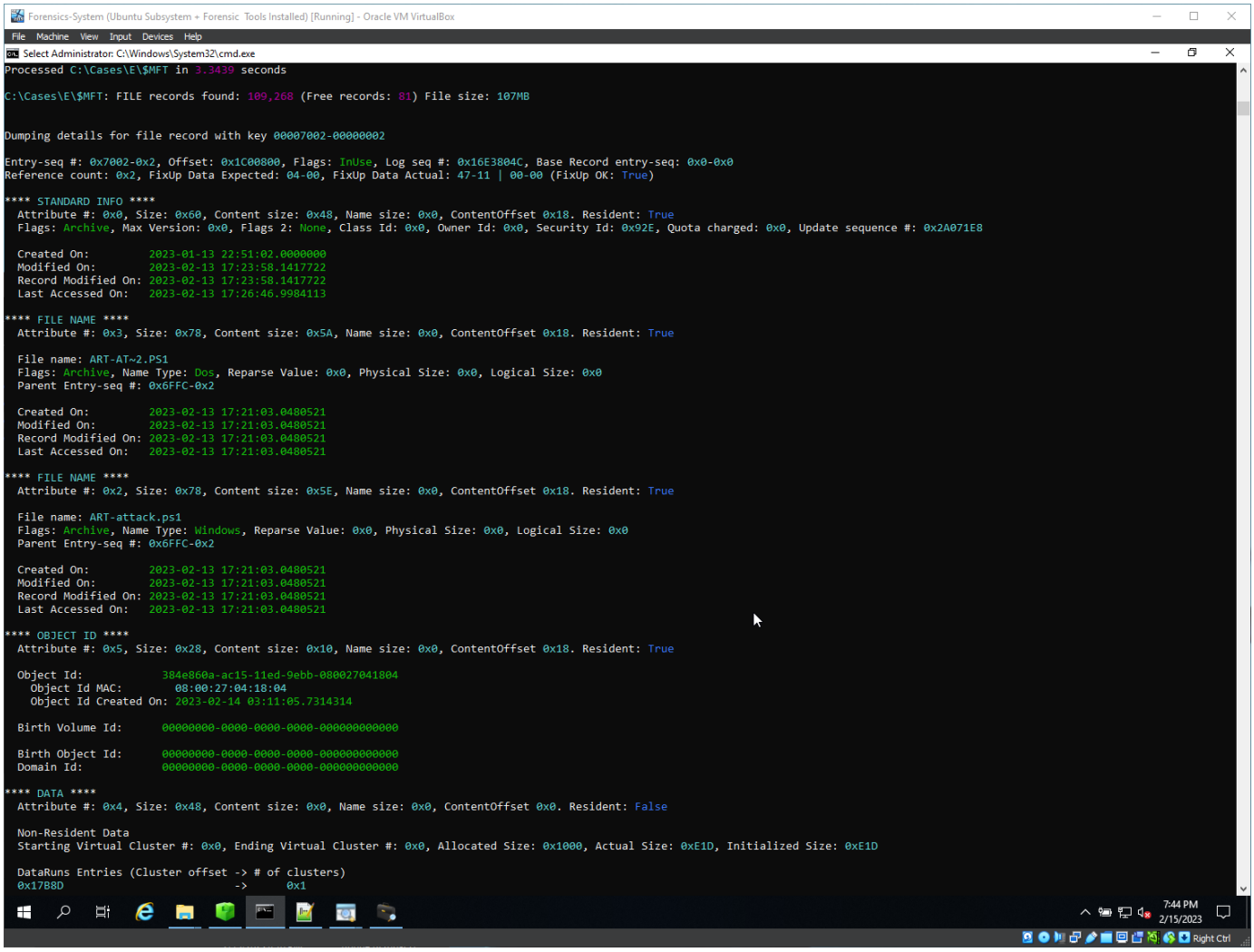
C:\Cases\Analysis\NTFS\MFT.csv

Total lines 143,386 | **Visible lines 24** | Open files: 1

- x10 is associated with $STD_INFO
- x30 is associated with $FILE_NAME

- Better viewing of timestamps:
-

```
C:\Tools\EZTools>MFTECmd.exe -f C:\Cases\E\$MFT --de 28674
```



SI(Standard info):

Information that inherited from ZIP file:

Created On: 2023-01-13 22:51:02.0000000

Modified On: 2023-02-13 17:23:58.1417722

When the file has been dropped on the disk:

Record Modified On: 2023-02-13 17:23:58.1417722

Last Accessed On: 2023-02-13 17:26:46.9984113

FN(File name):

Indicates the creation of the MFT record on the file system

Created On: 2023-02-13 17:21:03.0480521

Modified On: 2023-02-13 17:21:03.0480521

Record Modified On: 2023-02-13 17:21:03.0480521

Last Accessed On: 2023-02-13 17:21:03.0480521

File timestamps (MACB)

- The MACB format is a commonly undestood standard for timestamps and very used in the forensic industry

- MACB timestamps for the above file

Modified m... **2023-02-13 17:23:58.1417722**

Accessed .a.. **2023-02-13 17:26:46.9984113**

Changed ($MFT) ..c. **2023-02-13 17:23:58.1417722**

Birth ...b **2023-01-13 22:51:02.0000000**

File stomping

- File stomping reffers to manually modifying SI timestamps to make it dissapear from the attack timeframe, trying to hide it from the analysis. FN timestamps are created when the file

start to exist . If you move SI created on timestamp before FN timestamp , that means that is a possibility that the file has been timestomped .

- UserAssist – applications opened

  - Was the same file , timestomped?

Yes, because Birth ...b **2023-01-13 22:51:02.0000000**

> **FN Last Accessed On: 2023-02-13 17:21:03.0480521**