Mission Name

LibrarianTest

Background

Claire and Ethan are at ACADEMIUM (PARIS), locating to THE LIBRARIAN. THE LIBRARIAN has answers about code snippets.

Technical High-Level Overview

The Librarian is going to make a special test to Claire, in order to get the Librarian Card. For completing the test, Claire will be provided two forensic artifacts to check if Claire is able get the name of the program which deleted a file related to the Librarian.

Short Mission Description

You´re going to analyse two forensic artifacts provide from The Librarian. Your goal is to identify which is the name of a file, right after it has been deleted by a secure delete program. Keep in mind, the deletion was in 2049 and the file is related to The Librarian.

Mission Description

The Librarian is going to make a special test to Claire, in order to get the Librarian Card. You´re going to analyse two forensic artifacts provide from The Librarian. Your goal is to identify which is the name of a file, right after it has been deleted by a secure delete program. Keep in mind, the deletion was in 2049 and the file is related to The Librarian.

Location

FRANCE, PARIS | THE ACADEMIUM

Tools

- https://github.com/msuhanov/dfir_ntfs

Questions

Which is the parent MFT reference number of the file located?

- 1407374883553285

For you, what is the deletion date?

- 2049-04-19 20:43:56.926028

Hints

1. Use ntfs_parser tool to analyse $J y $MFT
2. Use Timeline explorer to analyse CSV file and locate BCWipe prefetch file
3. Look at around the prefetch file and check file: libraryID8564213261.txt

Write Up

Player must use dfir_ntfs to analyse $MFT and $J (usnjrnl), launching the following command:

Install from https://github.com/msuhanov/dfir_ntfs

```
mma@demowindows:~/NTFS/dfir_ntfs$ ntfs_parser --usn /mnt/c/Thratia_2/C2-M4/Medium/Evidencias/\$MFT /mnt/c/Thratia_2/C2-
M4/Medium/Evidencias/\$J /mnt/c/Thratia_2/C2-M4/Medium/salida_musoft.csv
mma@demowindows:~/NTFS/dfir_ntfs$
```

Figure 1

Then open CSV file to start the investigation:

Timeline Explorer v1.1.0.0

File Tools Tabs Help

salida_musoft.csv

Arrastre una columna aquí para agrupar por dicha columna

USN value	Source	Reason
393706352		USN_REASON_FILE_CREATE
393706456		USN_REASON_FILE_CREATE | 0x1000000
393706584		USN_REASON_FILE_CREATE | USN_REASON_CLOSE
393706688		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000
393706816		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_SECURITY_CHAN…
393706944		USN_REASON_FILE_CREATE | 0x1000000
393707072		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000
393707200		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_SECURITY_CHAN…
393707328		USN_REASON_FILE_CREATE | 0x1000000
393707520		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000
393707648		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_SECURITY_CHAN…
393707776		USN_REASON_FILE_CREATE | 0x1000000
393707904		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000
393708032		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_SECURITY_CHAN…
393708160		USN_REASON_FILE_CREATE | 0x1000000
393708288		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000
393708416		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_SECURITY_CHAN…
393708544		USN_REASON_FILE_CREATE | 0x1000000
393708672		USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | 0x1000000

Figure 2

The key would be firstly locate a file related to the librarian or library

Parent MFT reference number	Timestamp	File name
		librar
281474976725640	2021-04-19 20:25:22.866484	WmsAdminUILibrary.Resources.dll
281474976725640	2021-04-19 20:25:22.866484	WmsAdminUILibrary.Resources.dll
281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
281474976714017	2021-04-19 20:26:17.429024	Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856a…
281474976714017	2021-04-19 20:26:17.429024	Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856a…
281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
844424930220228	2021-04-19 20:26:45.585202	Microsoft.Practices.EnterpriseLibrary.Common.dll
844424930220228	2021-04-19 20:26:45.585202	Microsoft.Practices.EnterpriseLibrary.Common.dll

Figure 3

Locate its MFTs reference number:

MFT reference number	Parent MFT reference number	Timestamp	File name
			librar
281474976787097	281474976725640	2021-04-19 20:25:22.866484	WmsAdminUILibrary.Resources.dll
281474976787097	281474976725640	2021-04-19 20:25:22.866484	WmsAdminUILibrary.Resources.dll
562949953648968	281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
281474976906472	281474976714017	2021-04-19 20:26:17.429024	Microsoft-Windows-Dedup-ChunkLibrary
281474976906472	281474976714017	2021-04-19 20:26:17.429024	Microsoft-Windows-Dedup-ChunkLibrary
562949953648968	281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt

Figure 4

MFT reference number is: 562949953648968. Once located filter by this mft reference number:

MFT reference number	Parent MFT reference number	Timestamp	File name
562949953648968			
562949953648968	281474976937487	2021-04-19 20:24:47.565648	New Text Document.txt
562949953648968	281474976937487	2021-04-19 20:24:47.565648	New Text Document.txt
562949953648968	281474976937487	2021-04-19 20:25:11.054056	New Text Document.txt
562949953648968	281474976937487	2021-04-19 20:25:11.054056	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:11.054056	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:11.116390	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:11.116390	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:25:45.337676	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:01.664486	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
562949953648968	281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
562949953648968	281474976937487	2049-04-19 20:43:56.910276	libraryID8564213261.txt
562949953648968	281474976937487	2049-04-19 20:43:56.910276	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy

Figure 5

Player would see that for the same MFT reference number, three names for the same file:

- New Text Document.txt
- libraryID8564213261.txt
- cwroqlapnlwhbphinkpfbfy

The would be again, when the file was deleted? In 2049..

562949953648968	281474976937487	2021-04-19 20:26:18.866876	libraryID8564213261.txt
562949953648968	281474976937487	2049-04-19 20:43:56.910276	libraryID8564213261.txt
562949953648968	281474976937487	2049-04-19 20:43:56.910276	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
562949953648968	281474976937487	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy

Figure 6

Player must check USN value, between the movement of file: libraryID8564213261.txt to cwroqlapnlwhbphinkpfbfy:

USN value	Source	Reason	Timestamp	File name
393706352		USN_REASON_FILE_CREATE	2021-04-19 20:24:47.565648	New Text Document.txt
393706584		USN_REASON_FILE_CREATE | USN_REASON_CLOSE	2021-04-19 20:24:47.565648	New Text Document.txt
395086752		USN_REASON_RENAME_OLD_NAME	2021-04-19 20:25:11.054056	New Text Document.txt
395086856		USN_REASON_RENAME_NEW_NAME	2021-04-19 20:25:11.054056	libraryID8564213261.txt
395086968		USN_REASON_RENAME_NEW_NAME | USN_REASON_CLOSE	2021-04-19 20:25:11.054056	libraryID8564213261.txt
395087368		USN_REASON_OBJECT_ID_CHANGE	2021-04-19 20:25:11.116390	libraryID8564213261.txt
395087480		USN_REASON_OBJECT_ID_CHANGE | USN_REASON_CLOSE	2021-04-19 20:25:11.116390	libraryID8564213261.txt
399921000		USN_REASON_DATA_EXTEND	2021-04-19 20:25:45.337676	libraryID8564213261.txt
399921152		USN_REASON_DATA_EXTEND | USN_REASON_CLOSE	2021-04-19 20:25:45.337676	libraryID8564213261.txt
400170720		USN_REASON_DATA_OVERWRITE	2021-04-19 20:26:01.664486	libraryID8564213261.txt
400170832		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_TRUNCATION	2021-04-19 20:26:01.664486	libraryID8564213261.txt
400171008		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_TRUNCATION | USN_...	2021-04-19 20:26:01.664486	libraryID8564213261.txt
401325904		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_EXTEND	2021-04-19 20:26:18.866876	libraryID8564213261.txt
401326080		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_EXTEND | USN_REAS...	2021-04-19 20:26:18.866876	libraryID8564213261.txt
419959008		USN_REASON_RENAME_OLD_NAME	2049-04-19 20:43:56.910276	libraryID8564213261.txt
419959120		USN_REASON_RENAME_NEW_NAME	2049-04-19 20:43:56.910276	cwroqlapnlwhbphinkpfbfy
419959232		USN_REASON_RENAME_NEW_NAME | USN_REASON_CLOSE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959344		USN_REASON_BASIC_INFO_CHANGE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959456		USN_REASON_BASIC_INFO_CHANGE | USN_REASON_CLOSE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959568		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_EXTEND	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959680		USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_EXTEND | USN_REAS...	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959792		USN_REASON_DATA_TRUNCATION	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959904		USN_REASON_DATA_TRUNCATION | USN_REASON_BASIC_INFO_CHANGE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy

Figure 7

And check files around the USN Value: 419959008

419958152	USN_REASON_DATA_EXTEND | USN_REASON_DATA_TRUNCATION | USN_REA...	2049-04-19 20:43:47.084834	SVCHOST.EXE-47F05ECE.pf
419958264	USN_REASON_DATA_TRUNCATION	2049-04-19 20:43:47.161824	BCWIPE.EXE-ABF741DC.pf
419958368	USN_REASON_DATA_EXTEND | USN_REASON_DATA_TRUNCATION	2049-04-19 20:43:47.161824	BCWIPE.EXE-ABF741DC.pf
419958472	USN_REASON_DATA_EXTEND | USN_REASON_DATA_TRUNCATION | USN_REA...	2049-04-19 20:43:47.161824	BCWIPE.EXE-ABF741DC.pf
419958576	USN_REASON_FILE_CREATE	2049-04-19 20:43:48.335744	WMIPRVSE.EXE-39F97B2D.pf
419958784	USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE	2049-04-19 20:43:48.335744	WMIPRVSE.EXE-39F97B2D.pf
419958896	USN_REASON_DATA_EXTEND | USN_REASON_FILE_CREATE | USN_REASON_...	2049-04-19 20:43:48.335744	WMIPRVSE.EXE-39F97B2D.pf
419959008	USN_REASON_RENAME_OLD_NAME	2049-04-19 20:43:56.910276	libraryID8564213261.txt
419959120	USN_REASON_RENAME_NEW_NAME	2049-04-19 20:43:56.910276	cwroqlapnlwhbphinkpfbfy
419959232	USN_REASON_RENAME_NEW_NAME | USN_REASON_CLOSE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959344	USN_REASON_BASIC_INFO_CHANGE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959456	USN_REASON_BASIC_INFO_CHANGE | USN_REASON_CLOSE	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy
419959568	USN_REASON_DATA_OVERWRITE | USN_REASON_DATA_EXTEND	2049-04-19 20:43:56.926028	cwroqlapnlwhbphinkpfbfy

Figure 8

Finally player will see:

- Prefetch file of BCWIPE.exe: this indicates that bcwiped was launched.
- libraryID8564213261.txt was renamed to cwroqlapnlwhbphinkpfbfy knowing both files are the same. The cause of this fact, is the same MFT reference number:

USN_REASON_RENAME_OLD_NAME	2049-04-19 20:43:56.910276	libraryID8564213261.txt	562949953648968
USN_REASON_RENAME_NEW_NAME	2049-04-19 20:43:56.910276	cwroqlapnlwhbphinkpfbfy	562949953648968

Figure 9

Finally player will able to get name of the file: cwroqlapnlwhbphinkpfbfy

Flag Information

flag{cwroqlapnlwhbphinkpfbfy}

Expected Time to Complete the Challenge

It depends on the player´s technical skills and capabilities, but one person with appropriated skills could complete this mission in 1h.