Table of Contents

Intro

In this Sherlock, you will become acquainted with MFT (Master File Table) forensics. You will be introduced to well-known tools and methodologies for analyzing MFT artifacts to identify malicious activity. During our analysis, you will utilize the MFTECmd tool to parse the provided MFT file, TimeLine Explorer to open and analyze the results from the parsed MFT, and a Hex editor to recover file contents from the MFT.

Ok so for this sherlock we are noticed that we need 3 different tools.

The MFTECmd and TimeLine Explorer tools, can obtained from ericzimmerman site:

https://ericzimmerman.github.io/#!index.md

ericzimmerman.github.io/#!index.md

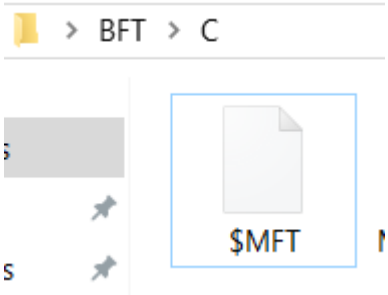
Eric Zimmerman's tools | Documentation | Benchmarks | ChangeLog | Theme

LECmd	1.5.0.0 | 1.5.0.0	Parse lnk files
MFTECmd	1.2.2.0 | 1.2.2.0	$MFT, $Boot, $J, $SDS, $I30, and $LogFile (coming soon) parser. Handles locked files
MFTExplorer	- | 2.0.0.0	Graphical $MFT viewer
PECmd	1.5.0.0 | 1.5.0.0	Prefetch parser
RBCmd	1.5.0.0 | 1.5.0.0	Recycle Bin artifact (INFO2/$I) parser
RecentFileCacheParser	1.5.0.0 | 1.5.0.0	RecentFileCache parser
RECmd	1.6.0.0 | 2.0.0.0	Powerful command line Registry tool searching, multi-hive support, plugins, and more
Registry Explorer	- | 2.0.0.0	Registry viewer with searching, multi-hive support, plugins, and more. Handles locked files
RLA	2.0.0.0 | 2.0.0.0	Replay transaction logs and update Registry hives so they are no longer dirty. Useful when tools do not know how to handle transaction logs
SDB Explorer	- | 2.0.0.0	Shim database GUI
SBECmd	2.0.0.0 | 2.0.0.0	ShellBags Explorer, command line edition, for exporting shellbag data
ShellBags Explorer	- | 2.0.0.0	GUI for browsing shellbags data. Handles locked files
SQLECmd	1.0.0.0 | 1.0.0.0	Find and process SQLite files according to your needs with maps!
SrumECmd	0.5.1.0 | 0.5.1.0	Process SRUDB.dat and (optionally) SOFTWARE hive for network, process, and energy info!
SumECmd	0.5.2.0 | 0.5.2.0	Process Microsoft User Access Logs found under 'C:\Windows\System32\LogFiles\SUM'
Timeline Explorer	- | 2.0.0.0	View CSV and Excel files, filter, group, sort, etc. with ease
VSCMount	1.5.0.0 | 1.5.0.0	Mount all VSCs on a drive letter to a given mount point

The third tool is any Hex editor but im using in the sherlock MFTExplorer, this tool is not must have, but it will make it all simple here. This tool available in ericzimmerman site too.

MFTExplorer	- | 2.0.0.0	Graphical $MFT viewer

We are getting a zip file that inside him there is a directory **c** that inside her there is $MFT file after we unzip all.



Task 1:

Simon Stark was targeted by attackers on February 13. He downloaded a ZIP file from a link received in an email. What was the name of the ZIP file he downloaded from the link?

First of all I took the MFTECmd.exe and moved it to the $MFT file. I look at the help menu to understand the right syntax for us:

```
C:\Users\user\Desktop\BFT\C>MFTECmd.exe -h
Description:
  MFTECmd version 1.2.2.1

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

  Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv
            MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out"
            MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\jsonout"
            MFTECmd.exe -f "C:\Temp\SomeMFT" --body "c:\temp\bout" --bdl c
            MFTECmd.exe -f "C:\Temp\SomeMFT" --de 5-5
            MFTECmd.exe -f "c:\temp\SomeJ" --csv c:\temp
            MFTECmd.exe -f "c:\temp\SomeBoot"
            MFTECmd.exe -f "c:\temp\SomeSecure_SDS" --csv c:\temp
            MFTECmd.exe -f "c:\temp\SomeI30" --csv c:\temp
            Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  MFTECmd [options]

Options:
  -f <f>           File to process ($MFT | $J | $Boot | $SDS | $I30). Required
```

Then I started to parse the tool according to that:

```
C:\Users\user\Desktop\BFT\C>MFTECmd.exe -f ".\$MFT" --csv "." --csvf mft.csv
MFTECmd version 1.2.2.1

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

Command line: -f .\$MFT --csv . --csvf mft.csv

Warning: Administrator privileges not found!

File type: Mft

Processed .\$MFT in 29.3698 seconds

.\$MFT: FILE records found: 171,927 (Free records: 142,905) File size: 307.5MB
        CSV output will be saved to .\mft.csv
```

I saved the output "mft.csv" then I opened the tool Timeline Explorer and loaded him the file we got, mft.csv.

As we know, according to the question we are looking for a zip file, so we will look at the tab "Extension" we will write "zip" and press enter:

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

mft.csv

Enter text to search... Find

Line	Parent Path	Extension	File Name
=		zip	
97524	.\Users\simon.stark\Downloads	.zip	Stage-20240213T093324Z-001.zip
113338	.\Users\simon.stark\Downloads	.zip	KAPE.zip
114706	.\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2211.24012.0_x64__8wekyb3d8bbwe\Assets	.zip	Archive.zip
115404	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	.zip	invoice.zip
115412	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	.zip	invoices.zip

As we can see got 5 zip files here.

See that I hid some tabs and I want to see the tab "Created0x10" next to the files. We want to do that to observe which zip is connected to 13 in February.

Parent Path	Extension	File Name	Created0x10
	zip		=
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	.zip	invoice.zip	1980-01-01 08:00:00
.\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2211.24012.0_x64_…	.zip	Archive.zip	2023-07-07 15:25:20
.\Users\simon.stark\Downloads	.zip	Stage-20240213T093324Z-001.zip	2024-02-13 16:34:40
.\Users\simon.stark\Downloads	.zip	KAPE.zip	2024-02-13 16:39:06
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	.zip	invoices.zip	2024-02-13 17:25:52

Based on the Parent Path and the date we got two suspicious files. Stage-20240213T093324Z-001.zip and KAPE.zip.

KAPE is a software for digital forensic (based on google search) so I thought more likely its not that, so I chose the other zip file and that's the answer for the malicious.

Answer:

Stage-20240213T093324Z-001.zip

Task 2 :

Examine the Zone Identifier contents for the initially downloaded ZIP file. This field reveals the HostUrl from where the file was downloaded, serving as a valuable Indicator of Compromise (IOC) in our investigation/analysis. What is the full Host URL from where this ZIP file was downloaded?

For that I removed the ".zip" Extension and I searched the name of our file and I saw the zone identifier:

Stage-20240213T093324Z-001.zip | Find

Line	Parent Path	Extension	File Name	Created0x10
97524	.\Users\simon.stark\Downloads	.zip	Stage-20240213T093324Z-001.zip	2024-02-13 16:34:40
97525	.\Users\simon.stark\Downloads	.Identifier	Stage-20240213T093324Z-001.zip:Zone.Identifier	2024-02-13 16:34:40

If we are running on " Stage-20240213T093324Z-001.zip:Zone.Identifier" file and finding the tab of "Zone Id Contents" we can see the answer where are the URL host:

Last Access0x30	Zone Id Contents	Reparse Target	Reference Count
2024-02-13 16:34:40			1
2024-02-13 16:34:40	[ZoneTransfer] ZoneId=3 HostUrl=https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser		1

Cell contents

```
[ZoneTransfer]
ZoneId=3
HostUrl=https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser
```

Answer:

https://storage.googleapis.com/drive-bulk-export-anonymous/20240213T093324.039Z/4133399871716478688/a40aecd0-1cf3-4f88-b55a-e188d5c1c04f/1/c277a8b4-afa9-4d34-b8ca-e1eb5e5f983c?authuser

Task 3:

What is the full path and name of the malicious file that executed malicious code and connected to a C2 server?

Hint:

Identify any suspicious file related to the initially downloaded ZIP file. Look for MFT records with suspicious extensions and timestamps around the ZIP download time.

Ok so we are understanding that the zip file " Stage-20240213T093324Z-001.zip" he is the source for the malicious file. I tried to search about this file without his extension to find another files that connected to him:

\Stage-20240213T093324Z-001 Find

Line	Parent Path	File Name	Extension	Created0x10	Cre
24584	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat:Zone.Identifier	.Identifier	2024-02-13 17:23:16	202
24583	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat	.bat	2024-02-13 17:23:16	202
115414	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices		2024-02-13 16:35:39	
115413	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices.zip:Zone.Identifier	.Identifier	2024-02-13 17:25:52	202
115412	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices.zip	.zip	2024-02-13 17:25:52	202
115411	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	invoice		2024-02-13 16:35:26	
115405	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	invoice.zip:Zone.Identifier	.Identifier	1980-01-01 08:00:00	202
115404	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage	invoice.zip	.zip	1980-01-01 08:00:00	202
115403	.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001	Stage		2024-02-13 16:35:15	

As we can see we find that the file "invoice.bat" is inside some files inside " Stage-20240213T093324Z-001.zip" . ".bat" files known as can be malicious. We can see that "invoice.bat" inside ".\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices" so his real path is:

.\Users\simon.stark\Downloads\Stage-20240213T093324Z-\.
001\Stage\invoice\invoices\invoice.bat

I tried this, but this is not the answer. I scrolled right in the software, and I saw in the tab "Zone Id Contents" that the files there, got fixed path:

Zone Id Contents

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices.zip
```

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice.zip
```

When I saw that I realized that the path is starting with "C:" so I fixed the real path for the invoice.bat, and this is the answer

C:\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices\invoice.bat

Task 4:

Analyze the $Created0x30 timestamp for the previously identified file. When was this file created on disk?

ok so quick look at the file invoice.bat file under the Created0x30 gives us the answer:

Parent Path	File Name	Extension	Crea…	Created0x30
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat:Zone.Identifier	.Identifier	2024…	2024-02-13 16:38:39
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice\invoices	invoice.bat	.bat	2024…	2024-02-13 16:38:39
.\Users\simon.stark\Downloads\Stage-20240213T093324Z-001\Stage\invoice	invoices		2024…	

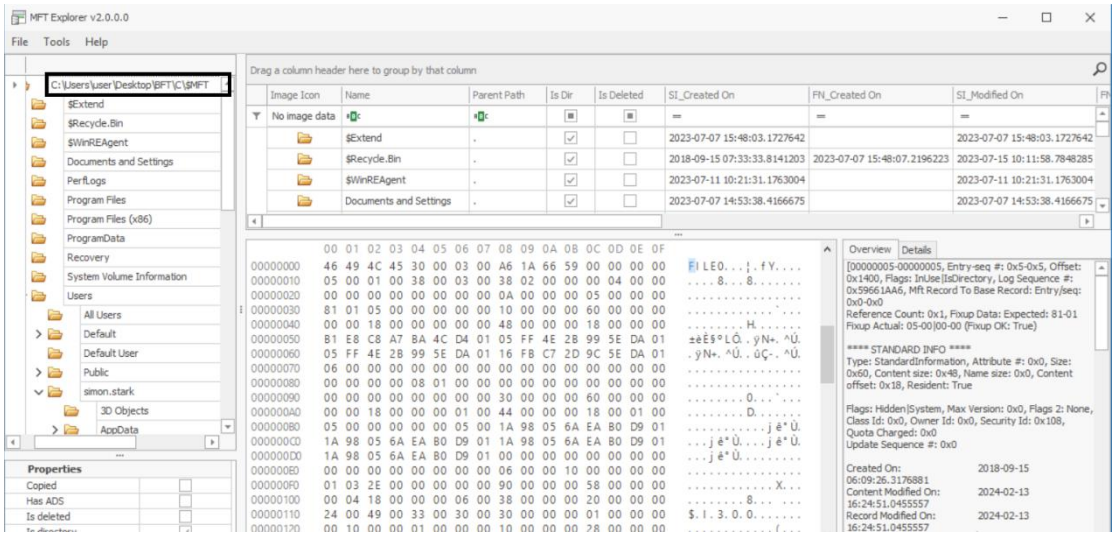
Answer:

2024-02-13 16:38:39

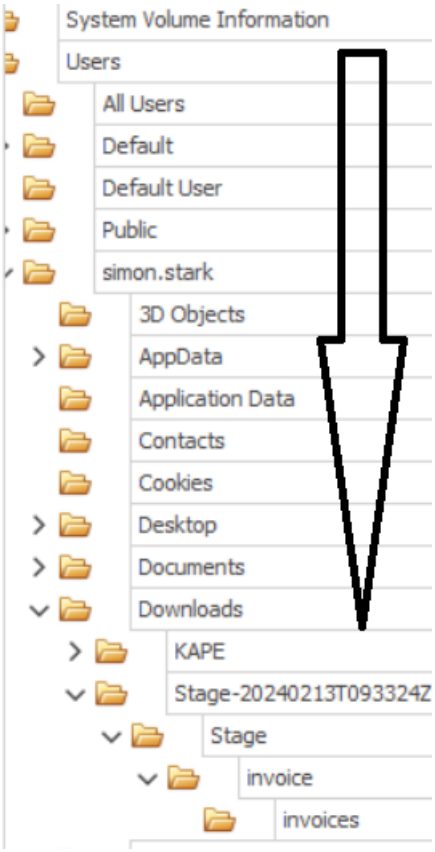
Task 5:

Finding the hex offset of an MFT record is beneficial in many investigative scenarios. Find the hex offset of the stager file from Question 3.

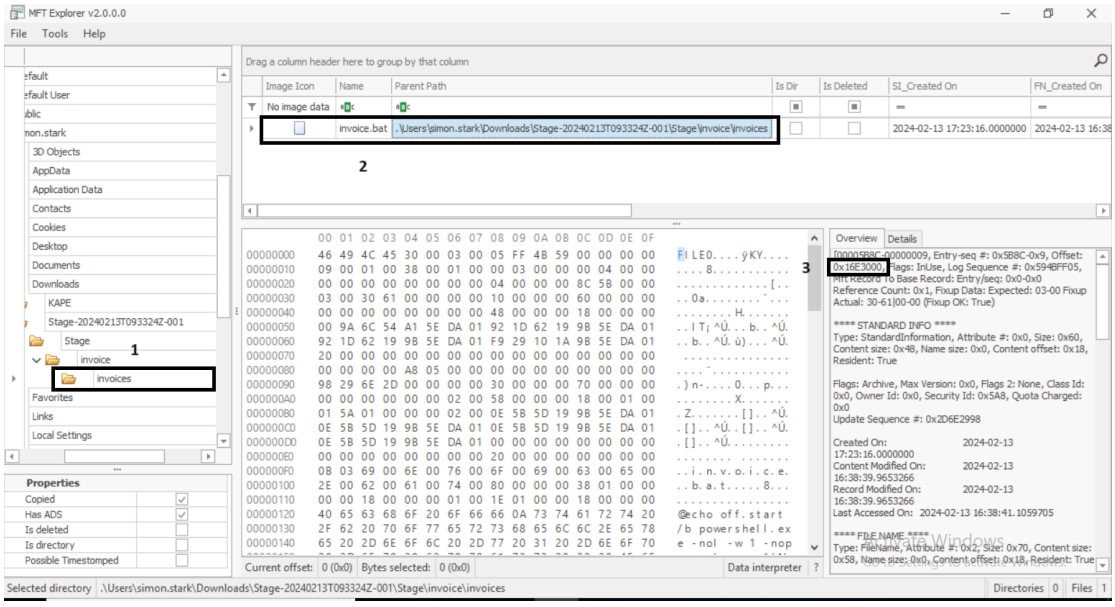
ok for this question I used MFTExplorer I loaded the $MFT file into him.



after that, I navigated to our malicious file:



Then I clicked by the order in the photo until I see the offset of the file, in the picture number 3:



This is the offset that the malicious file is starting inside the $MFT file. So this is the answer:

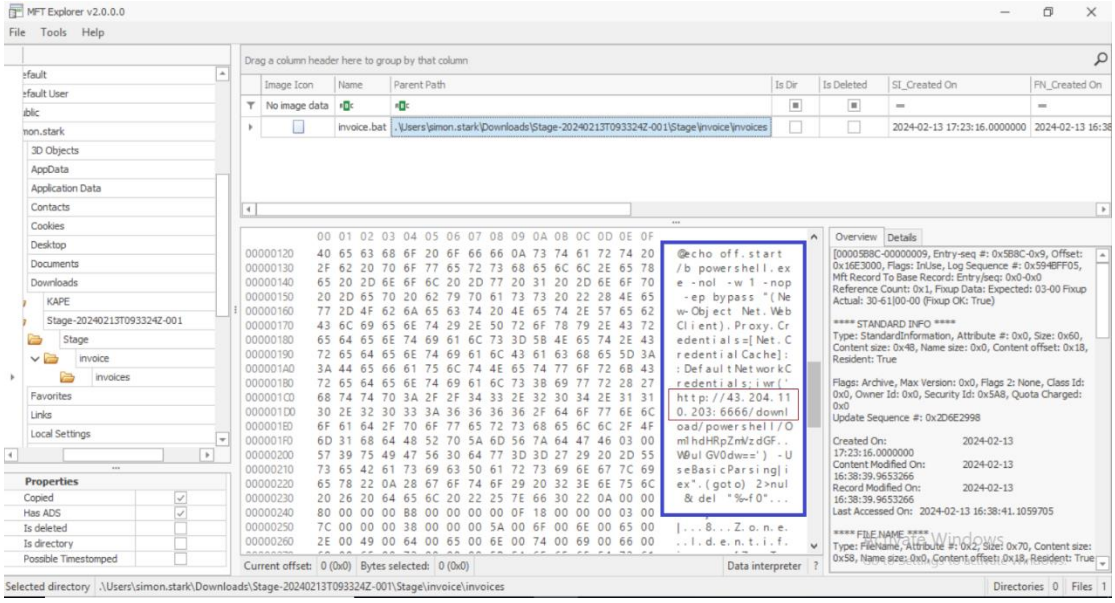
16E3000

Task 6:

Each MFT record is 1024 bytes in size. If a file on disk has smaller size than 1024 bytes, they can be stored directly on MFT File itself. These are called MFT Resident files. During Windows File system Investigation, its crucial to look for any malicious/suspicious files that may be resident in MFT. This way we can find contents of malicious files/scripts. Find the contents of The malicious stager identified in Question3 and answer with the C2 IP and port.

Hint: Open the MFT file in any hex editor tool of your choice. Then, either search for or jump to the offset identified in the previous question to find the stager file contents. For example, in the HxD (Hex editor) tool, go to the search tab and click the "go to" button, which opens up a prompt where you can input either hex or decimal offset to navigate to the relevant location.

Ok so for this question you can use any HxD editor and go for the offset 16E3000, but I didn't do that I saw it with MFTExplorer I scrolled down inside the details and I saw the malicious script:



As you can see there is a ip address with port inside the malicious file.

Answer:

43.204.110.203:6666