

CHALLENGE DESCRIPTION

Luxx, leader of The Phreaks, immerses himself in the depths of his computer, tirelessly pursuing the secrets of a file he obtained accessing an opposing faction member's workstation. With unwavering determination, he scours through data, putting together fragments of information trying to take some advantage on other factions. To get the flag, you need to answer the questions from the docker instance.

The extracted file from the .zip is : “z.mft” , so its an mft(Master file table).

MFT is the master file table in the NTFS file system used by windows OS .

MFT stores information about all the files in the NTFS file system such as filename,size....

Let’s goo :

Literally, I tried all the tools that I know on kali linux to extract some information about the .mft file but all of the failed . after some google searching i found this tool “MFT explorer” I install it and I run it on windows and it works .

The screenshot displays the MFT Explorer v2.0.0.0 application. The left pane shows a file system tree with folders like \$Extend, \$Metadata, \$LogFile, documents, 2023, 2024, and System Volume Information. The main pane shows a table of file entries with columns: Image Icon, Name, Parent Path, Is Dir, Is Deleted, SI_Created On, FN_Created On, SI_Modified On, FN_Modified On, SI_Last Accessed, and FN_Last Accessed. The right pane shows the details of a selected file, including its type (Standard Information), flags, and creation/modification dates. The bottom pane shows a hex dump of the file's data.

Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created On	SI_Modified On	FN_Modified On	SI_Last Accessed	FN_Last Accessed
[Folder Icon]	\$Extend	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391	
[Folder Icon]	\$Metadata	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:27.2813759		2024-02-20 19:32:27.2813759		2024-02-20 19:32:27.2813759	
[Folder Icon]	\$LogFile	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:24.3362827		2024-02-20 19:32:24.3362827		2024-02-20 19:32:24.3362827	
[Folder Icon]	documents	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391	
[Folder Icon]	2023	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391	
[Folder Icon]	2024	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391	
[Folder Icon]	System Volume Information	.		<input checked="" type="checkbox"/>	2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391		2024-02-20 19:32:21.6546391	

So lets answer the question :

First question : Files are related to two years, which are those? (for example: 1993,1995) :



2023,2024

Next question : There are some documents, which is the name of the first file written? (for example: randomname.pdf) :

Just look at the creation date and chose the oldest one .

Final_Annual_Report.xlsx

Next question: Which file was deleted? (for example: randomname.pdf) :

	Financial_Statement_draft.xlsx	.\documents\2024	<input type="checkbox"/>	<input type="checkbox"/>	2024-02-20 19
	Marketing_Plan.xlsx	.\documents\2024	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2024-02-20 19

Marketing_plan.xlsx

Next question: How many of them have been set in Hidden mode? (for example: 43) :

<input type="checkbox"/>	credentials.txt	.\documents	<input type="checkbox"/>	<input type="checkbox"/>	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2901732
--------------------------	-----------------	-------------	--------------------------	--------------------------	-----------------------------	-----------------------------	-----------------------------

																Overview Details	
1000000	46	49	4C	45	30	00	03	00	8A	7D	10	00	00	00	00	[00000033-00000001, Entry-seq #: 0x33-0x1, Offset: 0xCC00, Flags: InUse, Log Sequence #: 0x107D8A, Mft Record To Base Record: Entry/seq: 0x0-0x0 Reference Count: 0x1, Fixup Data: Expected: 03-00 Fixup Actual: 00-00(00-00 (Fixup OK: True) **** STANDARD INFO **** Type: StandardInformation, Attribute #: 0x0, Size: 0x60, Content size: 0x48, Name size: 0x0, Content offset: 0x18, Resident: True Flags: Hidden, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x108, Quota Charged: 0x0 Update Sequence #: 0x0	
1000010	01	00	01	00	38	00	01	00	50	01	00	00	00	04	00		
1000020	00	00	00	00	00	00	00	00	03	00	00	00	33	00	00		
1000030	03	00	00	00	00	00	00	00	10	00	00	00	60	00	00		
1000040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00		
1000050	64	DE	71	89	33	64	DA	01	64	DE	71	89	33	64	DA		
1000060	C9	78	00	AF	33	64	DA	01	64	DE	71	89	33	64	DA		
1000070	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
1000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
1000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

There is one file that contains the word hidden in the Overview (flags)

1

Next question : Which is the filename of the important TXT file that was created? (for example: randomname.txt) :

The hidden file : credentials.txt

Next question: A file was also copied, which is the new filename?

	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record Changed	FN_Record Changed	Timestamped	Copied
	=	=	=	=	=	<input type="checkbox"/>	<input type="checkbox"/>
872119	2024-02-20 19:32:27.2862572	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2862572	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2862572	<input type="checkbox"/>	<input type="checkbox"/>
881770		2024-02-20 19:32:27.2881770		2024-02-20 19:32:27.2881770		<input type="checkbox"/>	<input type="checkbox"/>
891865	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2911603	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2891865	2024-02-20 19:32:27.2901732	<input type="checkbox"/>	<input checked="" type="checkbox"/>
881770		2024-02-20 19:32:27.2881770		2024-02-20 19:32:27.2881770		<input type="checkbox"/>	<input type="checkbox"/>
881770	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2881770	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2881770	2024-02-20 19:32:27.2872119	<input type="checkbox"/>	<input type="checkbox"/>
004361	2024-02-20 19:32:27.2872119	2024-02-20 19:33:30.3004361	2024-02-20 19:32:27.2872119	2024-02-20 19:33:30.3004361	2024-02-20 19:32:27.2872119	<input type="checkbox"/>	<input type="checkbox"/>

Financial_Statement_draft.xlsx

Next question: Which file was modified after creation?

Project_Proposal.pdf

Next question: What is the name of the file located at record number 45? (for example: randomname.pdf) :

45=0x2D

Overview	Details
[0000002D-00000001, Entry-seq #: 0x2D-0x1, Offset: 0xB400, Flags: InUse, Log Sequence #: 0x107034, Mft Record To Base Record: Entry/seq: 0x0-0x0	

its Annual_Report.xlsx

Next question : What is the size of the file located at record number 40? (for example: 1337)

40=0x28

The file name is Final_Project_Proposal.pdf

Non Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0xD, Allocated Size: 0xE000, Actual Size: 0xE000, Initialized Size 0x0

Non resident data: this means the file's content is not stored directly in the MFT entry but in clusters on the disk.

The file size is :0xE000 == 57344

And you get the flag .