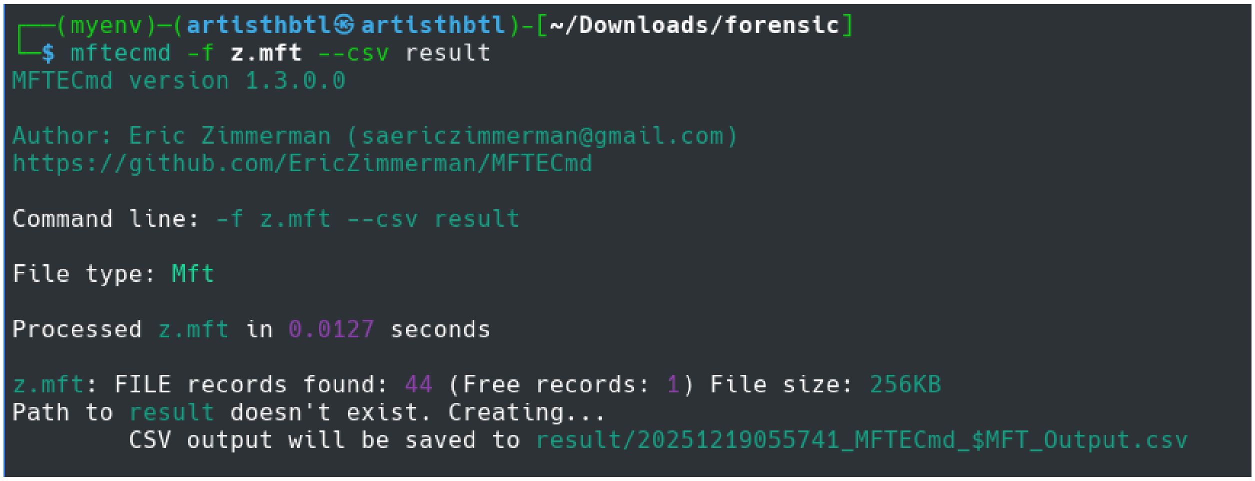
HTB - Pursue The Track (Easy) - Windows Artifacts

Marcello - 2702276140

Challenge Description

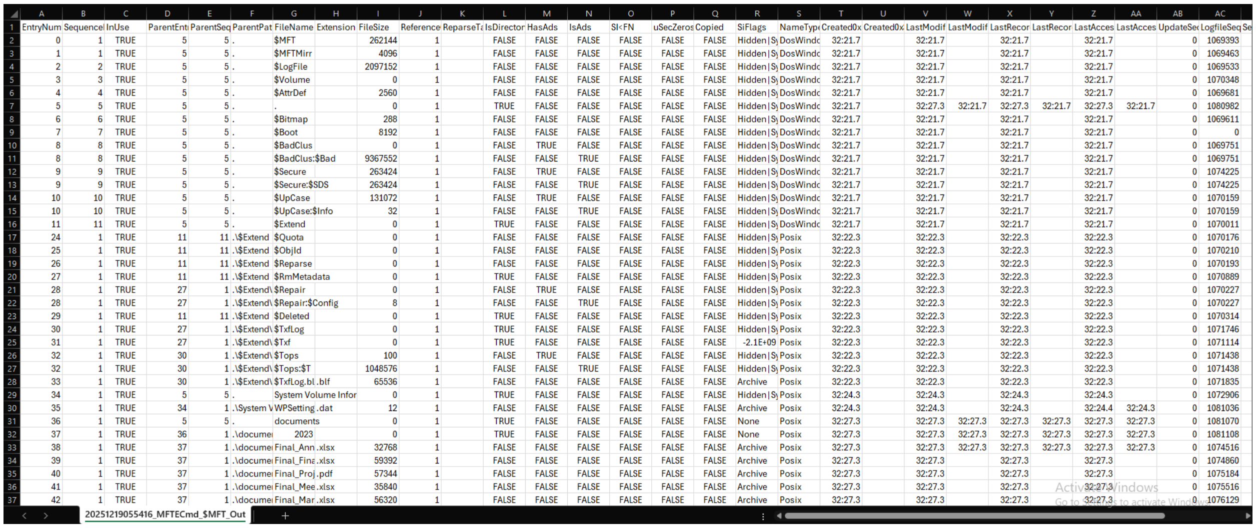
Luxx, leader of The Phreaks, immerses himself in the depths of his computer, tirelessly pursuing the secrets of a file he obtained accessing an opposing faction member's workstation. With unwavering determination, he scours through data, putting together fragments of information trying to take some advantage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

Saat kita download file challengenya, kita akan mendapat suatu file bernama z.mft, Master File Table atau file MFT adalah database untuk NTFS Windows, dimana file itu menyimpan data data yang berhubungan dengan file system seperti nama file / directory, kapan file dibuat, kapan terakhir kali file di write, dan sebagainya. Jadi untuk menganalisis file mft kita harus menggunakan tool, toolnya bisa macem-macem, yang terkenal ada analyzeMFT, MFTECmd, atau MFTExplorer, nah karena disini saya sudah install yang MFTECmd, kita akan menggunakan MFTECmd.



```
┌──(myenv)─(artisthbtl㉿artisthbtl)-[~/Downloads/forensic]
└─$ mftecmd -f z.mft --csv result
MFTECmd version 1.3.0.0

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

Command line: -f z.mft --csv result

File type: Mft

Processed z.mft in 0.0127 seconds

z.mft: FILE records found: 44 (Free records: 1) File size: 256KB
Path to result doesn't exist. Creating...
        CSV output will be saved to result/20251219055741_MFTECmd_$MFT_Output.csv
```

Oke dengan command di atas, kita berhasil extract file MFTnya menjadi suatu directory yang di dalemnya ada file csv, jadi kita bisa analisis file csv itu di excel.

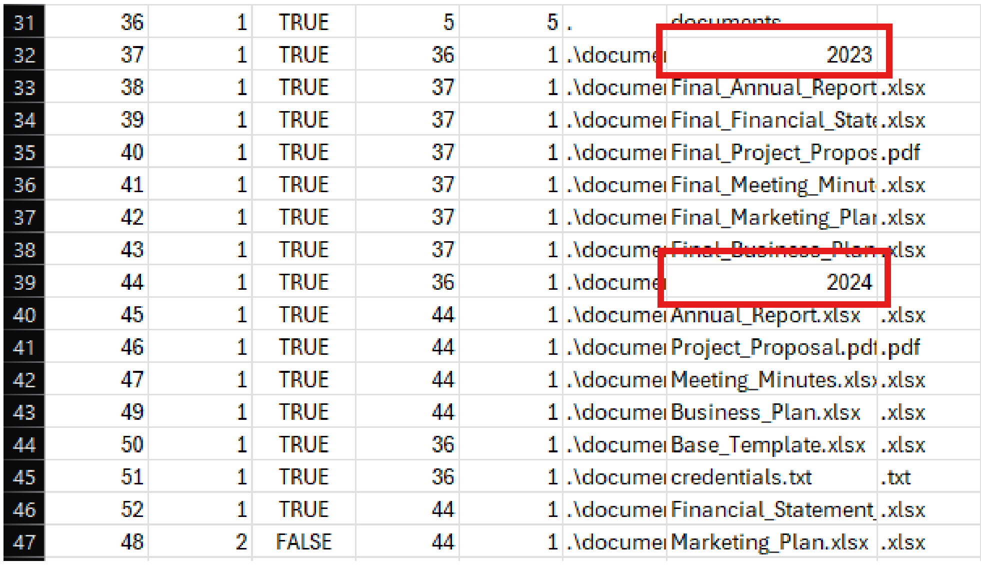


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	EntryNum	Sequence	InUse	ParentEnt	ParentSeq	ParentPat	FileName	Extension	FileSize	Reference	ReparseTa	IsDirector	HasAds	IsAds	SI<FN	uSecZeros	Copied	SiFlags	NameType	Created0x	Created0x	LastModif	LastModif	LastRecor	LastRecor	LastAcces	LastAcces	UpdateSe	LogfileSeq
2	0	1	TRUE	5	5	.	$MFT		262144	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069393
3	1	1	TRUE	5	5	.	$MFTMirr		4096	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069463
4	2	2	TRUE	5	5	.	$LogFile		2097152	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069533
5	3	3	TRUE	5	5	.	$Volume		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1070348
6	4	4	TRUE	5	5	.	$AttrDef		2560	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069681
7	5	5	TRUE	5	5	.	.		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:27.3	32:21.7	32:27.3	32:21.7	32:27.3	32:21.7	0	1080982
8	6	6	TRUE	5	5	.	$Bitmap		288	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069611
9	7	7	TRUE	5	5	.	$Boot		8192	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	0
10	8	8	TRUE	5	5	.	$BadClus		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069751
11	8	8	TRUE	5	5	.	$BadClus:$Bad		9367552	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1069751
12	9	9	TRUE	5	5	.	$Secure		263424	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1074225
13	9	9	TRUE	5	5	.	$Secure:$SDS		263424	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1074225
14	10	10	TRUE	5	5	.	$UpCase		131072	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1070159
15	10	10	TRUE	5	5	.	$UpCase:$Info		32	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1070159
16	11	11	TRUE	5	5	.	$Extend		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	DosWindc	32:21.7		32:21.7		32:21.7		32:21.7		0	1070011
17	24	1	TRUE	11	11	.\$Extend	$Quota		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070176
18	25	1	TRUE	11	11	.\$Extend	$ObjId		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070210
19	26	1	TRUE	11	11	.\$Extend	$Reparse		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070193
20	27	1	TRUE	11	11	.\$Extend	$RmMetadata		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070889
21	28	1	TRUE	27	1	.\$Extend\	$Repair		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070227
22	28	1	TRUE	27	1	.\$Extend\	$Repair:$Config		8	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070227
23	29	1	TRUE	11	11	.\$Extend	$Deleted		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1070314
24	30	1	TRUE	27	1	.\$Extend\	$TxfLog		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1071746
25	31	1	TRUE	27	1	.\$Extend\	$Txf		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	-2.1E+09	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1071114
26	32	1	TRUE	30	1	.\$Extend\	$Tops		100	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1071438
27	32	1	TRUE	30	1	.\$Extend\	$Tops:$T		1048576	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1071438
28	33	1	TRUE	30	1	.\$Extend\	$TxfLog.bl	.blf	65536	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:22.3		32:22.3		32:22.3		32:22.3		0	1071835
29	34	1	TRUE	5	5	.	System Volume Infor		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|Sy	Posix	32:24.3		32:24.3		32:24.3		32:24.3		0	1072906
30	35	1	TRUE	34	1	.\System V	WPSetting	.dat	12	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:24.3		32:24.3		32:24.3		32:24.4	32:24.3	0	1081036
31	36	1	TRUE	5	5	.	documents		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	None	Posix	32:27.3		32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	0	1081070
32	37	1	TRUE	36	1	.\documei	2023		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	None	Posix	32:27.3		32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	0	1081108
33	38	1	TRUE	37	1	.\documei	Final_Ann	.xlsx	32768	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:27.3		32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	32:27.3	0	1074516
34	39	1	TRUE	37	1	.\documei	Final_Fina	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:27.3		32:27.3		32:27.3		32:27.3		0	1074860
35	40	1	TRUE	37	1	.\documei	Final_Proj	.pdf	57344	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:27.3		32:27.3		32:27.3		32:27.3		0	1075184
36	41	1	TRUE	37	1	.\documei	Final_Mee	.xlsx	35840	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:27.3		32:27.3		32:27.3		32:27.3		0	1075516
37	42	1	TRUE	37	1	.\documei	Final_Mar	.xlsx	56320	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Posix	32:27.3		32:27.3		32:27.3		32:27.3		0	1076129

20251219055416_MFTECmd_$MFT_Out

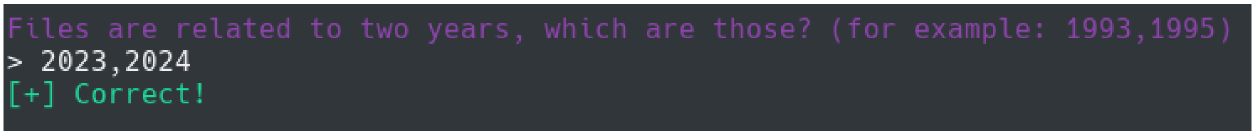
Sebelum menganalisa, kita coba connect ke netcatnya, dan ternyata, sepertinya challenge ini mengharuskan kita menjawab beberapa soal untuk mendapatkan file yang berkaitan dengan file MFT itu.

Question 1: Files are related to two years, which are those? (for example: 1993,1995)



31	36	1	TRUE	5	5	.	documents	
32	37	1	TRUE	36	1	.\docume	2023	
33	38	1	TRUE	37	1	.\documei	Final_Annual_Report	.xlsx
34	39	1	TRUE	37	1	.\documei	Final_Financial_State	.xlsx
35	40	1	TRUE	37	1	.\documei	Final_Project_Propos	.pdf
36	41	1	TRUE	37	1	.\documei	Final_Meeting_Minut	.xlsx
37	42	1	TRUE	37	1	.\documei	Final_Marketing_Plar	.xlsx
38	43	1	TRUE	37	1	.\docume	Final_Business_Plan	.xlsx
39	44	1	TRUE	36	1	.\docume	2024	
40	45	1	TRUE	44	1	.\documei	Annual_Report.xlsx	.xlsx
41	46	1	TRUE	44	1	.\documei	Project_Proposal.pdf	.pdf
42	47	1	TRUE	44	1	.\documei	Meeting_Minutes.xlsx	.xlsx
43	49	1	TRUE	44	1	.\documei	Business_Plan.xlsx	.xlsx
44	50	1	TRUE	36	1	.\documei	Base_Template.xlsx	.xlsx
45	51	1	TRUE	36	1	.\documei	credentials.txt	.txt
46	52	1	TRUE	44	1	.\documei	Financial_Statement	.xlsx
47	48	2	FALSE	44	1	.\documei	Marketing_Plan.xlsx	.xlsx

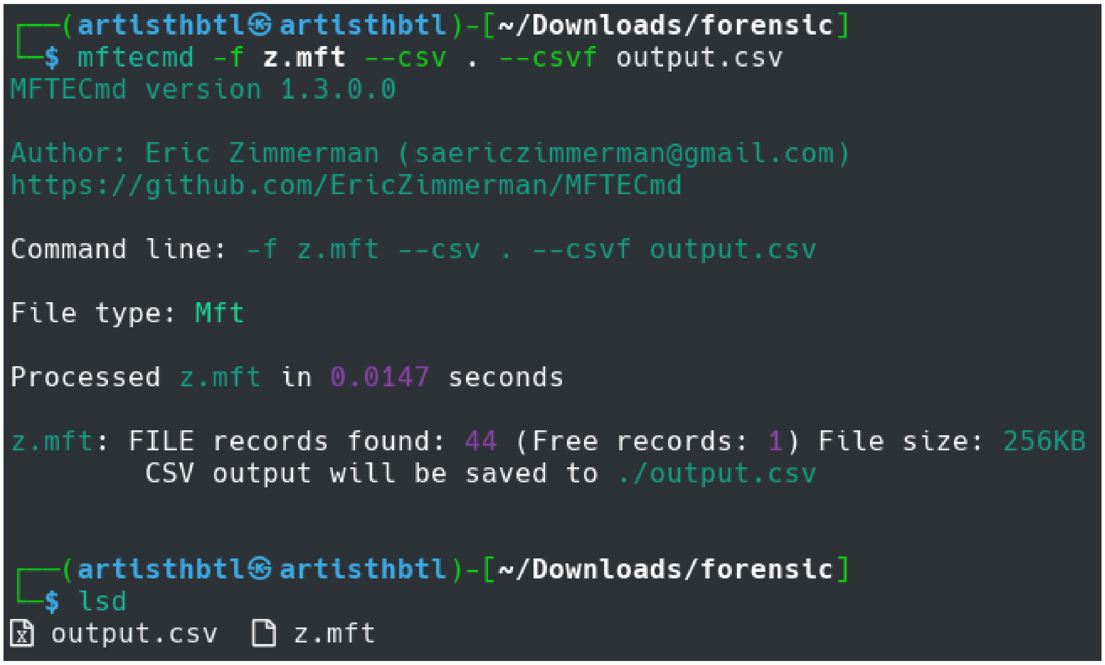
Kita bisa liat di gambar di atas, kalo file structure di file z.mft kurang lebih kayak ada folder documents, di dalamnya ada folder 2023, dan 2024, di setiap folder ada file yang berhubungan sama suatu bisnis. Nah, karena kita udah tau ada folder yang berhubungan di tahun 2023 dan 2024, jadi jawaban Q1 adalah 2023, 2024.



```
Files are related to two years, which are those? (for example: 1993,1995)
> 2023,2024
[+] Correct!
```

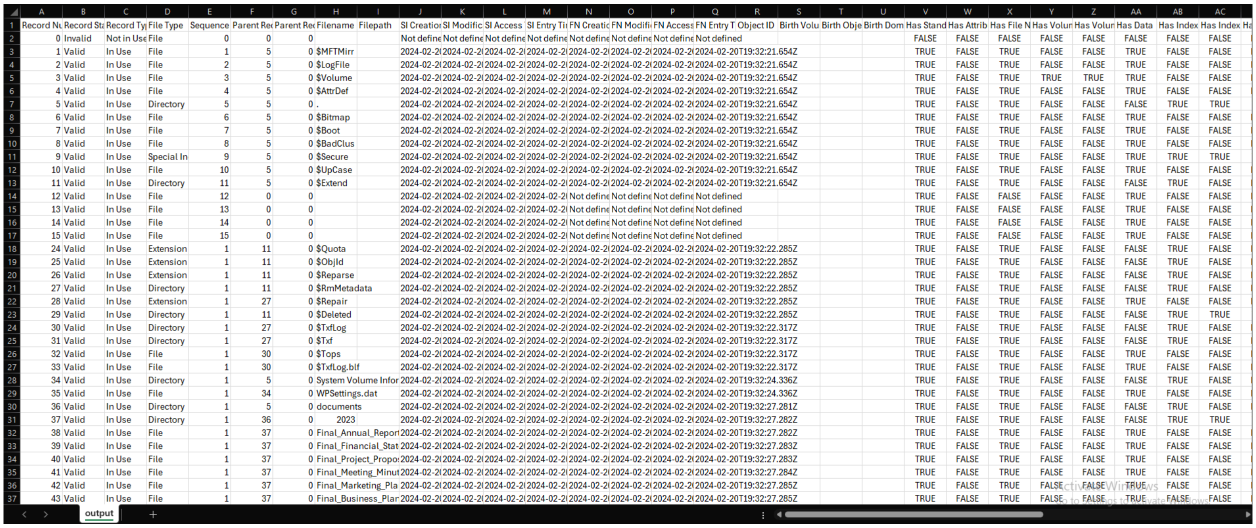
Question 2: There are some documents, which is the name of the first file written? (for example: randomname.pdf)

Nah disini saya kesulitan untuk jawab soal ini, karena timestampnya dari file csv itu rada kurang bagus, jadi saya liat-liat help MFTECmd dan coba-coba pake flag –csvf pas extract z.mft:



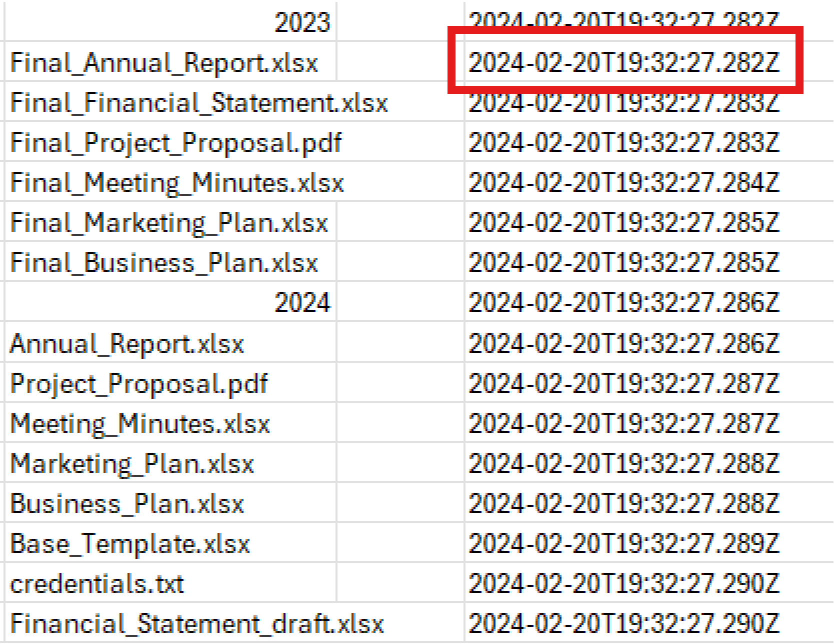
```
┌──(artisthbtl㉿artisthbtl)-[~/Downloads/forensic]
└─$ mftecmd -f z.mft --csv . --csvf output.csv
MFTECmd version 1.3.0.0

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

Command line: -f z.mft --csv . --csvf output.csv

File type: Mft

Processed z.mft in 0.0147 seconds

z.mft: FILE records found: 44 (Free records: 1) File size: 256KB
        CSV output will be saved to ./output.csv


┌──(artisthbtl㉿artisthbtl)-[~/Downloads/forensic]
└─$ lsd
 output.csv    z.mft
```

Nah kita dapet file csv dengan timestamp yang lebih lengkap.



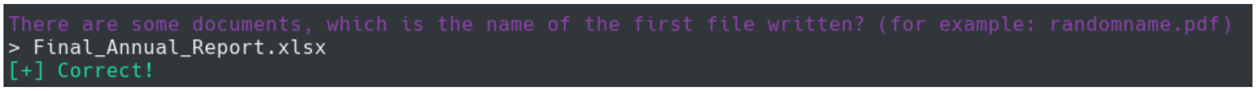
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	Record Nu	Record Sta	Record Ty	File Type	Sequence	Parent Re	Parent Re	Filename	Filepath	SI Creatior	SI Modific	SI Access	SI Entry Tir	FN Creatic	FN Modifi	FN Access	FN Entry T	Object ID	Birth Volu	Birth Obje	Birth Dom	Has Stand	Has Attrib	Has File N	Has Volun	Has Volun	Has Data	Has Index	Has Index
2	0	Invalid	Not in Use	File	0	0	0			Not define	Not define	Not define	Not define	Not define	Not define	Not define	Not defined					FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
3	1	Valid	In Use	File	1	5	0	$MFTMirr		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
4	2	Valid	In Use	File	2	5	0	$LogFile		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
5	3	Valid	In Use	File	3	5	0	$Volume		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE
6	4	Valid	In Use	File	4	5	0	$AttrDef		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
7	5	Valid	In Use	Directory	5	5	0	.		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
8	6	Valid	In Use	File	6	5	0	$Bitmap		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
9	7	Valid	In Use	File	7	5	0	$Boot		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
10	8	Valid	In Use	File	8	5	0	$BadClus		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
11	9	Valid	In Use	Special In	9	5	0	$Secure		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE
12	10	Valid	In Use	File	10	5	0	$UpCase		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
13	11	Valid	In Use	Directory	11	5	0	$Extend		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:21.654Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
14	12	Valid	In Use	File	12	0	0			2024-02-2	2024-02-2	2024-02-2	2024-02-2	Not define	Not define	Not define	Not defined					TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
15	13	Valid	In Use	File	13	0	0			2024-02-2	2024-02-2	2024-02-2	2024-02-2	Not define	Not define	Not define	Not defined					TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
16	14	Valid	In Use	File	14	0	0			2024-02-2	2024-02-2	2024-02-2	2024-02-2	Not define	Not define	Not define	Not defined					TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
17	15	Valid	In Use	File	15	0	0			2024-02-2	2024-02-2	2024-02-2	2024-02-2	Not define	Not define	Not define	Not defined					TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
18	24	Valid	In Use	Extension	1	11	0	$Quota		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
19	25	Valid	In Use	Extension	1	11	0	$ObjId		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
20	26	Valid	In Use	Extension	1	11	0	$Reparse		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
21	27	Valid	In Use	Directory	1	11	0	$RmMetadata		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
22	28	Valid	In Use	Extension	1	27	0	$Repair		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
23	29	Valid	In Use	Directory	1	11	0	$Deleted		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
24	30	Valid	In Use	Directory	1	27	0	$TxfLog		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.317Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
25	31	Valid	In Use	Directory	1	27	0	$Txf		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.317Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
26	32	Valid	In Use	File	1	30	0	$Tops		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.317Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
27	33	Valid	In Use	File	1	30	0	$TxfLog.blf		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:22.317Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
28	34	Valid	In Use	Directory	1	5	0	System Volume Infor		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:24.336Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
29	35	Valid	In Use	File	1	34	0	WPSettings.dat		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:24.336Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
30	36	Valid	In Use	Directory	1	5	0	documents		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.281Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE
31	37	Valid	In Use	Directory	1	36	0	2023		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.282Z					TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE
32	38	Valid	In Use	File	1	37	0	Final_Annual_Report		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.282Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
33	39	Valid	In Use	File	1	37	0	Final_Financial_Stat		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.283Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
34	40	Valid	In Use	File	1	37	0	Final_Project_Propo		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.283Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
35	41	Valid	In Use	File	1	37	0	Final_Meeting_Minut		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.284Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
36	42	Valid	In Use	File	1	37	0	Final_Marketing_Pla		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
37	43	Valid	In Use	File	1	37	0	Final_Business_Plar		2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-2	2024-02-20T19:32:27.285Z					TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE

Kita bisa liat di kolom SI Creation Time, atau Standard Information Creation Time, dimana berisi timstamp kapan file ini dibuat, karena file creation itu termasuk write privilege di directory + biasanya kita write suatu file baru save as / create filenya.



2023	2024-02-20T19:32:27.282Z
Final_Annual_Report.xlsx	2024-02-20T19:32:27.282Z
Final_Financial_Statement.xlsx	2024-02-20T19:32:27.283Z
Final_Project_Proposal.pdf	2024-02-20T19:32:27.283Z
Final_Meeting_Minutes.xlsx	2024-02-20T19:32:27.284Z
Final_Marketing_Plan.xlsx	2024-02-20T19:32:27.285Z
Final_Business_Plan.xlsx	2024-02-20T19:32:27.285Z
2024	2024-02-20T19:32:27.286Z
Annual_Report.xlsx	2024-02-20T19:32:27.286Z
Project_Proposal.pdf	2024-02-20T19:32:27.287Z
Meeting_Minutes.xlsx	2024-02-20T19:32:27.287Z
Marketing_Plan.xlsx	2024-02-20T19:32:27.288Z
Business_Plan.xlsx	2024-02-20T19:32:27.288Z
Base_Template.xlsx	2024-02-20T19:32:27.289Z
credentials.txt	2024-02-20T19:32:27.290Z
Financial_Statement_draft.xlsx	2024-02-20T19:32:27.290Z

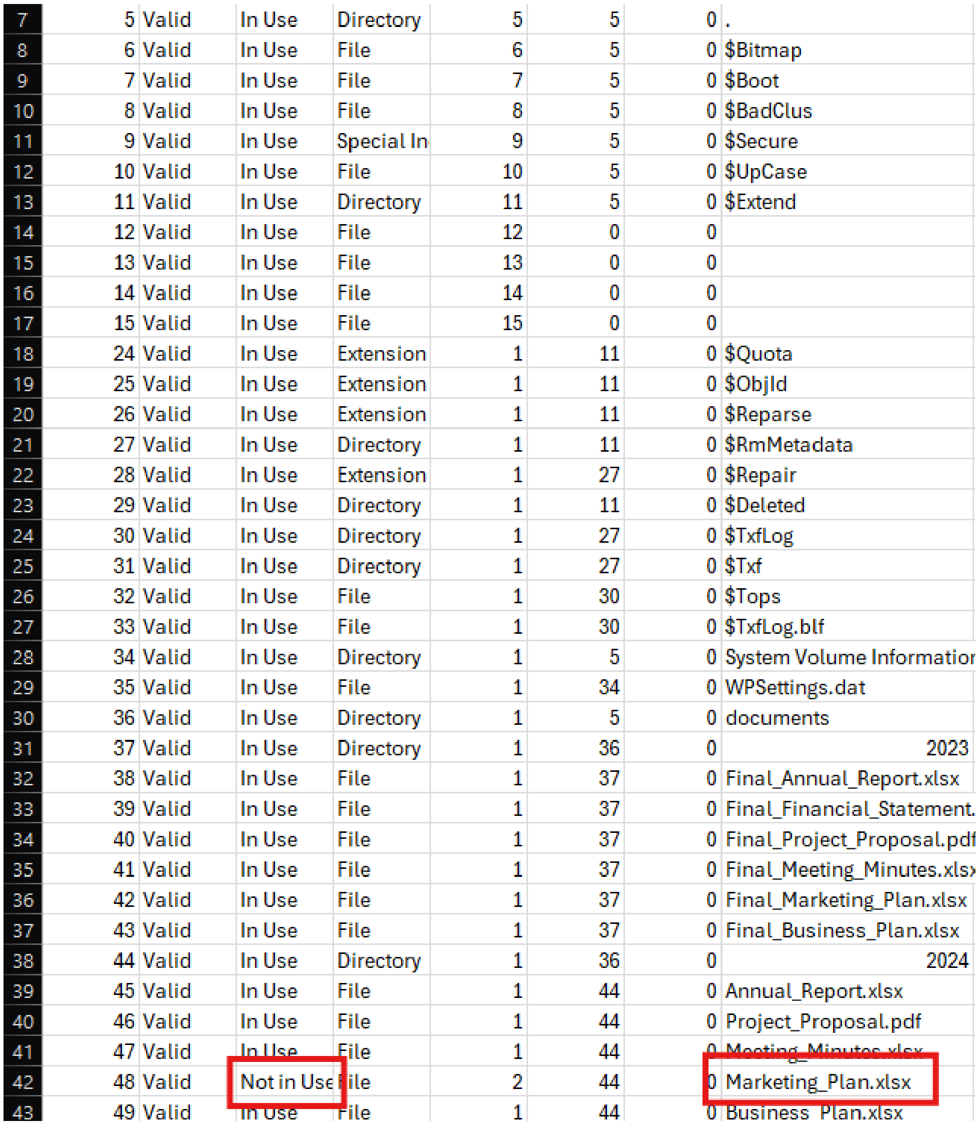
Kita bisa liat kalau file yang paling awal dibuat adalah suatu file xlsx bernama Final_Annual_Report.xlsx.



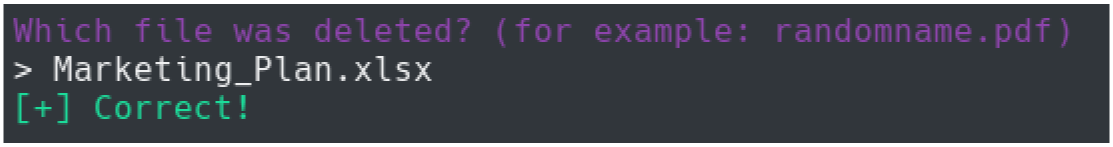
```
There are some documents, which is the name of the first file written? (for example: randomname.pdf)
> Final_Annual_Report.xlsx
[+] Correct!
```

Question 3: Which file was deleted? (for example: randomname.pdf)

Question ini cukup straightforward, kita bisa liat ke kolom Record Type dan kalau value cellnya Not In Use, berarti file itu udah di delete



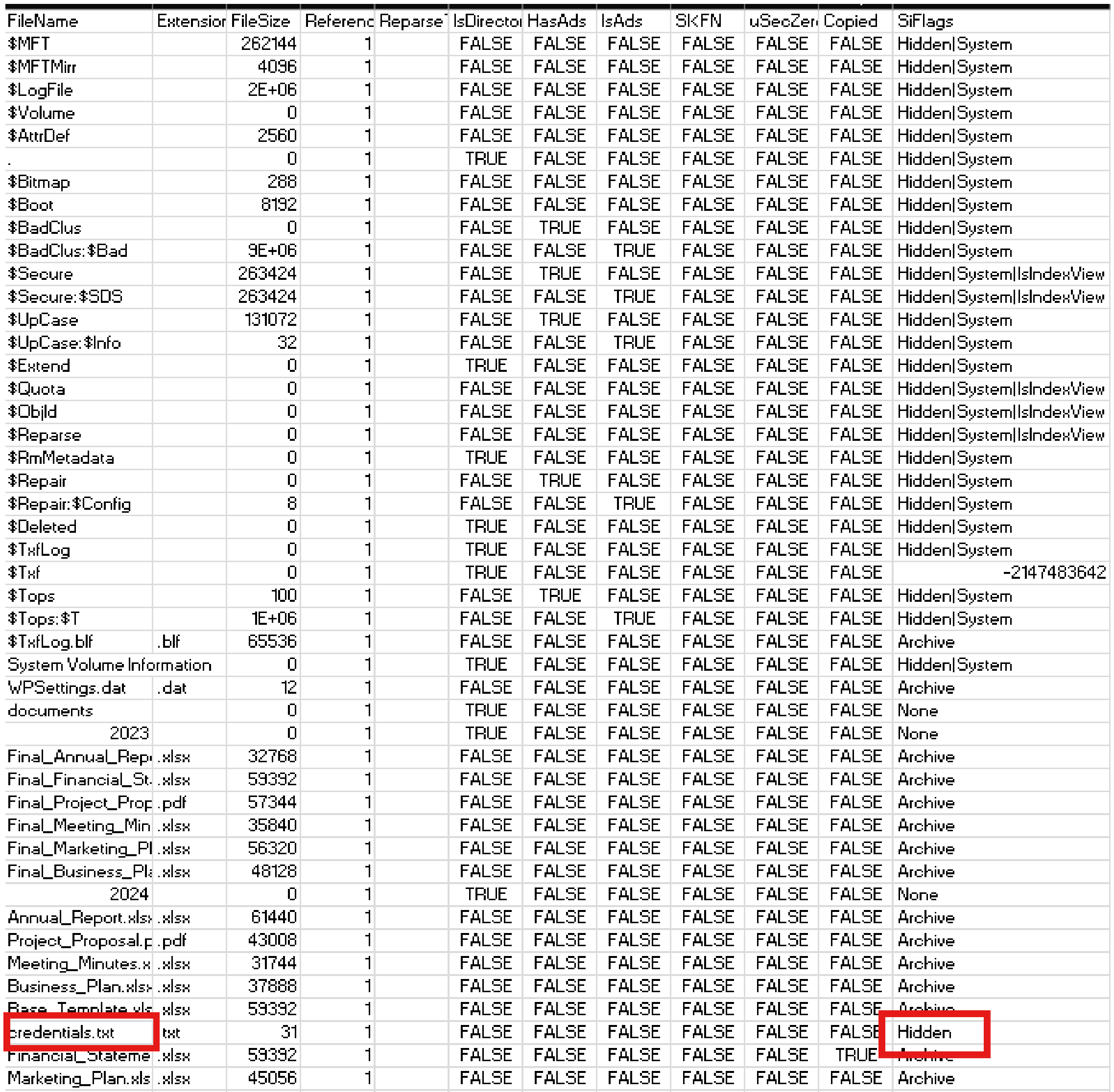
7	5	Valid	In Use	Directory	5	5	0	.
8	6	Valid	In Use	File	6	5	0	$Bitmap
9	7	Valid	In Use	File	7	5	0	$Boot
10	8	Valid	In Use	File	8	5	0	$BadClus
11	9	Valid	In Use	Special In	9	5	0	$Secure
12	10	Valid	In Use	File	10	5	0	$UpCase
13	11	Valid	In Use	Directory	11	5	0	$Extend
14	12	Valid	In Use	File	12	0	0	
15	13	Valid	In Use	File	13	0	0	
16	14	Valid	In Use	File	14	0	0	
17	15	Valid	In Use	File	15	0	0	
18	24	Valid	In Use	Extension	1	11	0	$Quota
19	25	Valid	In Use	Extension	1	11	0	$ObjId
20	26	Valid	In Use	Extension	1	11	0	$Reparse
21	27	Valid	In Use	Directory	1	11	0	$RmMetadata
22	28	Valid	In Use	Extension	1	27	0	$Repair
23	29	Valid	In Use	Directory	1	11	0	$Deleted
24	30	Valid	In Use	Directory	1	27	0	$TxfLog
25	31	Valid	In Use	Directory	1	27	0	$Txf
26	32	Valid	In Use	File	1	30	0	$Tops
27	33	Valid	In Use	File	1	30	0	$TxfLog.blf
28	34	Valid	In Use	Directory	1	5	0	System Volume Informatior
29	35	Valid	In Use	File	1	34	0	WPSettings.dat
30	36	Valid	In Use	Directory	1	5	0	documents
31	37	Valid	In Use	Directory	1	36	0	2023
32	38	Valid	In Use	File	1	37	0	Final_Annual_Report.xlsx
33	39	Valid	In Use	File	1	37	0	Final_Financial_Statement.
34	40	Valid	In Use	File	1	37	0	Final_Project_Proposal.pdf
35	41	Valid	In Use	File	1	37	0	Final_Meeting_Minutes.xlsx
36	42	Valid	In Use	File	1	37	0	Final_Marketing_Plan.xlsx
37	43	Valid	In Use	File	1	37	0	Final_Business_Plan.xlsx
38	44	Valid	In Use	Directory	1	36	0	2024
39	45	Valid	In Use	File	1	44	0	Annual_Report.xlsx
40	46	Valid	In Use	File	1	44	0	Project_Proposal.pdf
41	47	Valid	In Use	File	1	44	0	Meeting_Minutes.xlsx
42	48	Valid	Not in Use	File	2	44	0	Marketing_Plan.xlsx
43	49	Valid	In Use	File	1	44	0	Business_Plan.xlsx



```
Which file was deleted? (for example: randomname.pdf)
> Marketing_Plan.xlsx
[+] Correct!
```

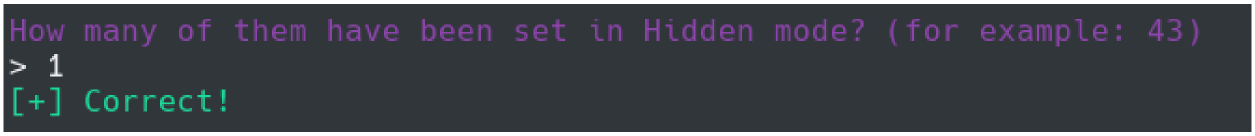
Question 4: How many of them have been set in Hidden mode? (for example: 43)

Nah untuk jawab file ini kita balik ke file csv yang awal, karena dari file csv yang kedua, gaada info buat tau apakah suatu file / dir di hidden atau ngga, tapi di file csv awal ada kolom SiFlags atau Security Identification Flags yang berisi informasi security settings apa aja yang di file ke dir / file, salah satunya hidden atau ngga.



FileName	Extensior	FileSize	Referenc	Reparse	IsDirector	HasAds	IsAds	SKFN	uSecZer	Copied	SiFlags
$MFT		262144	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$MFTMirr		4096	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$LogFile		2E+06	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Volume		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$AttrDef		2560	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
.		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Bitmap		288	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Boot		8192	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$BadClus		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$BadClus:$Bad		9E+06	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|System
$Secure		263424	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|System|IsIndexView
$Secure:$SDS		263424	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|System|IsIndexView
$UpCase		131072	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$UpCase:$Info		32	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|System
$Extend		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Quota		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System|IsIndexView
$ObjId		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System|IsIndexView
$Reparse		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System|IsIndexView
$RmMetadata		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Repair		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Repair:$Config		8	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|System
$Deleted		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$TxfLog		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Txf		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	-2147483642
$Tops		100	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	Hidden|System
$Tops:$T		1E+06	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	Hidden|System
$TxfLog.blf	.blf	65536	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
System Volume Information		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden|System
WPSettings.dat	.dat	12	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
documents		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	None
2023		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	None
Final_Annual_Rep	.xlsx	32768	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Final_Financial_St	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Final_Project_Prop	.pdf	57344	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Final_Meeting_Min	.xlsx	35840	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Final_Marketing_Pl	.xlsx	56320	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Final_Business_Pl	.xlsx	48128	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
2024		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	None
Annual_Report.xls	.xlsx	61440	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Project_Proposal.p	.pdf	43008	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Meeting_Minutes.x	.xlsx	31744	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Business_Plan.xls	.xlsx	37888	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
Base_Template.xls	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive
credentials.txt	.txt	31	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Hidden
Financial_Stateme	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	Archive
Marketing_Plan.xls	.xlsx	45056	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive

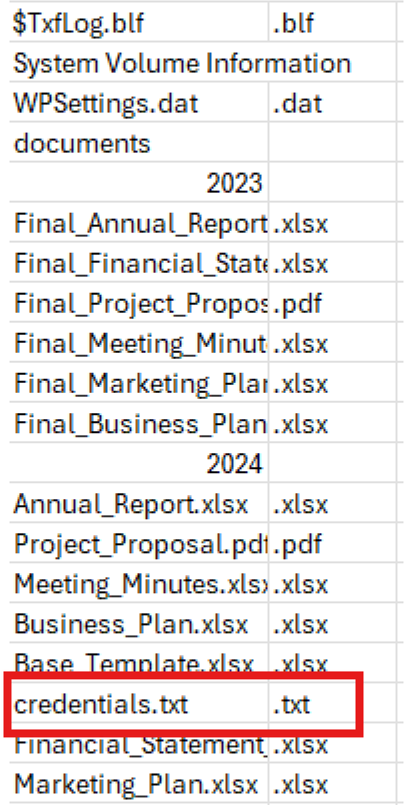
Sebenernya ada beberapa file yang di set to hidden, tapi pas aku jawab 27 disini gabisa, nah karena cuma ada 1 file yang bukan System yang di set hidden, yaitu credentials.txt, jadi disini jawabannya 1.



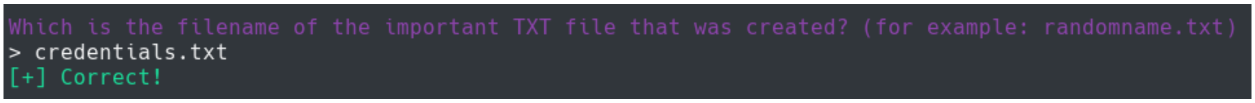
```
How many of them have been set in Hidden mode? (for example: 43)
> 1
[+] Correct!
```

Question 5: Which is the filename of the important TXT file that was created? (for example: randomname.txt)

Nah disini cukup simple, satu satunya file txt yang ada disini adalah credentials.txt, dan itu keliatan important



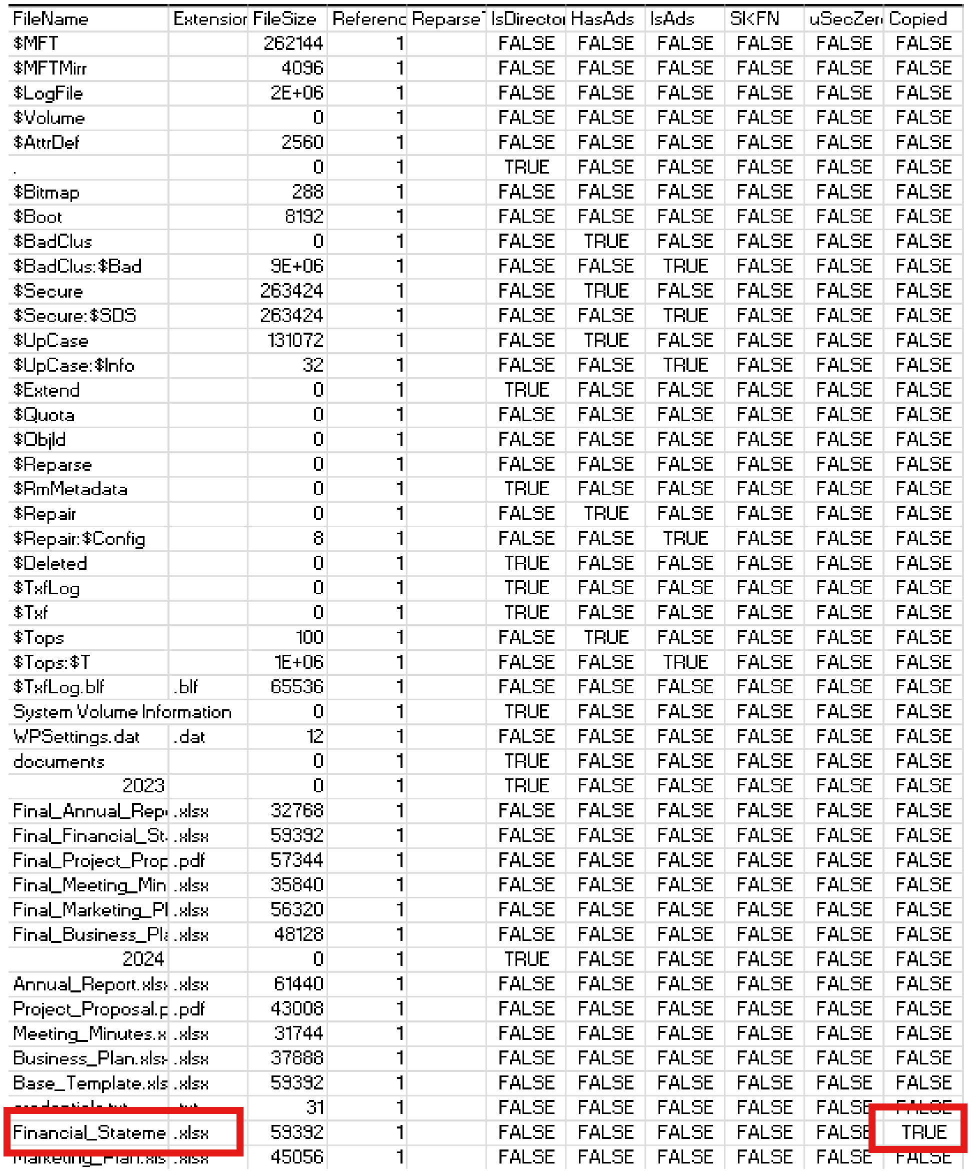
$TxfLog.blf	.blf
System Volume Information	
WPSettings.dat	.dat
documents	
2023	
Final_Annual_Report	.xlsx
Final_Financial_State	.xlsx
Final_Project_Propos	.pdf
Final_Meeting_Minut	.xlsx
Final_Marketing_Plar	.xlsx
Final_Business_Plan	.xlsx
2024	
Annual_Report.xlsx	.xlsx
Project_Proposal.pdf	.pdf
Meeting_Minutes.xls	.xlsx
Business_Plan.xlsx	.xlsx
Base_Template.xlsx	.xlsx
credentials.txt	.txt
Financial_Statement	.xlsx
Marketing_Plan.xlsx	.xlsx



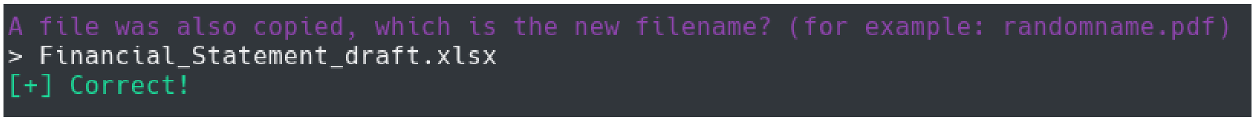
```
Which is the filename of the important TXT file that was created? (for example: randomname.txt)
> credentials.txt
[+] Correct!
```

Question 6: A file was also copied, which is the new filename? (for example: randomname.pdf)

Disini juga simple, kita bisa liat ke kolom Copied dan cari yang valuenya true



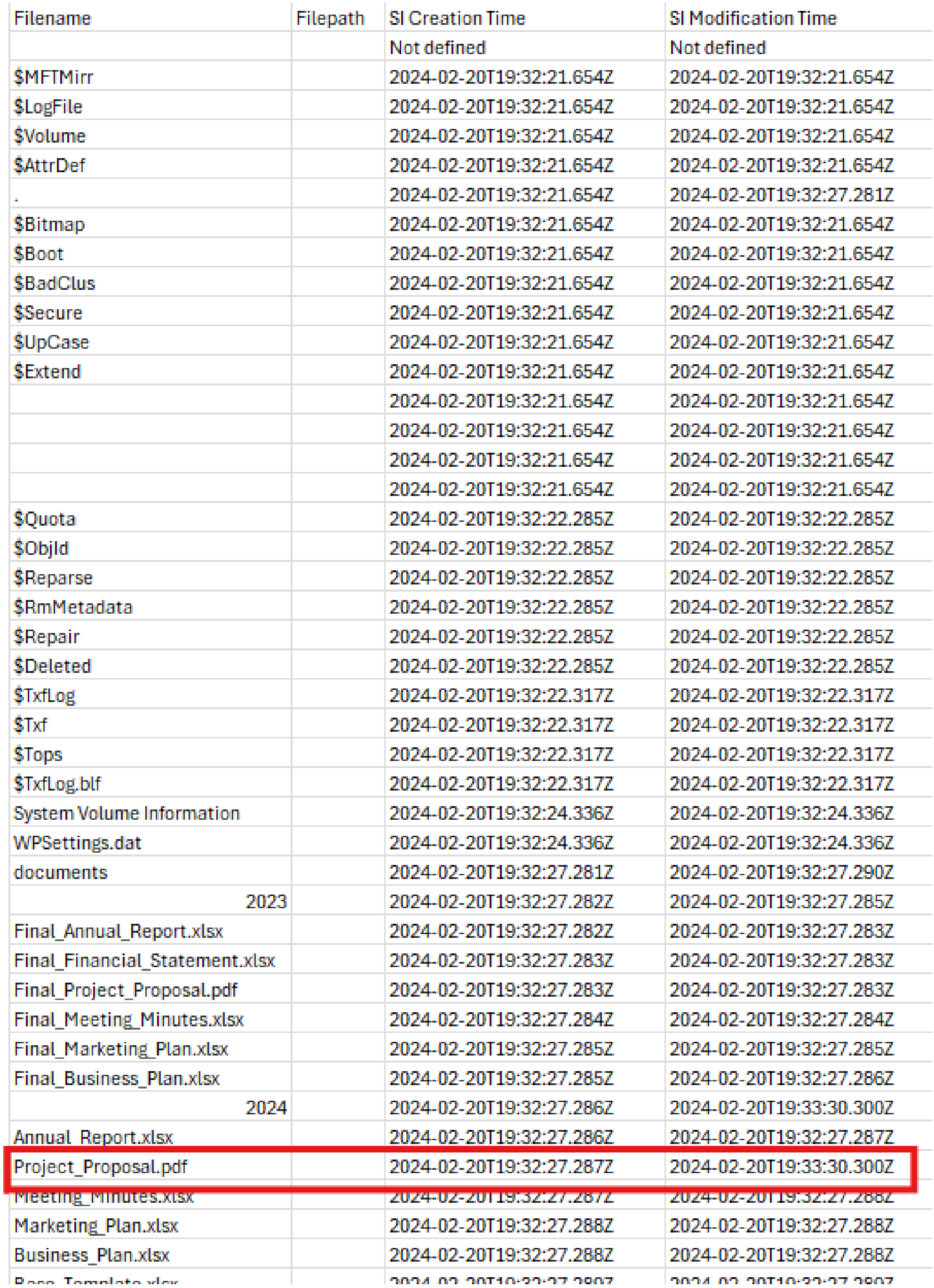
FileName	Extensior	FileSize	Referenc	Reparse	IsDirector	HasAds	IsAds	SI<FN	uSecZer	Copied
$MFT		262144	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$MFTMirr		4096	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$LogFile		2E+06	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$Volume		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$AttrDef		2560	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
.		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$Bitmap		288	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$Boot		8192	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$BadClus		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
$BadClus:$Bad		9E+06	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
$Secure		263424	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
$Secure:$SDS		263424	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
$UpCase		131072	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
$UpCase:$Info		32	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
$Extend		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$Quota		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$ObjId		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$Reparse		0	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
$RmMetadata		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$Repair		0	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
$Repair:$Config		8	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
$Deleted		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$TxfLog		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$Txf		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
$Tops		100	1		FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
$Tops:$T		1E+06	1		FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
$TxfLog.blf	.blf	65536	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
System Volume Information		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
WPSettings.dat	.dat	12	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
documents		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
2023		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Annual_Rep	.xlsx	32768	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Financial_St	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Project_Prop	.pdf	57344	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Meeting_Min	.xlsx	35840	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Marketing_Pl	.xlsx	56320	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Final_Business_Pl	.xlsx	48128	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2024		0	1		TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
Annual_Report.xls	.xlsx	61440	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Project_Proposal.p	.pdf	43008	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Meeting_Minutes.x	.xlsx	31744	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Business_Plan.xls	.xlsx	37888	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Base_Template.xls	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
credentials.txt	.txt	31	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
Financial_Stateme	.xlsx	59392	1		FALSE	FALSE	FALSE	FALSE	FALSE	TRUE
Marketing_Plan.xls	.xlsx	45056	1		FALSE	FALSE	FALSE	FALSE	FALSE	FALSE



```
A file was also copied, which is the new filename? (for example: randomname.pdf)
> Financial_Statement_draft.xlsx
[+] Correct!
```

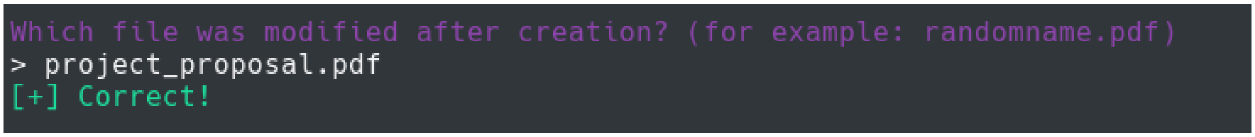
Question 7: Which file was modified after creation? (for example: randomname.pdf)

Nah, untuk jawab pertanyaan ini kita balik ke file csv kedua karena timestampnya lebih informative, kita liat ke SI Creation Time dan SI Modification Time.



Filename	Filepath	SI Creation Time	SI Modification Time
		Not defined	Not defined
$MFTMirr		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$LogFile		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$Volume		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$AttrDef		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
.		2024-02-20T19:32:21.654Z	2024-02-20T19:32:27.281Z
$Bitmap		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$Boot		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$BadClus		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$Secure		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$UpCase		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$Extend		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
		2024-02-20T19:32:21.654Z	2024-02-20T19:32:21.654Z
$Quota		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$ObjId		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$Reparse		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$RmMetadata		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$Repair		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$Deleted		2024-02-20T19:32:22.285Z	2024-02-20T19:32:22.285Z
$TxfLog		2024-02-20T19:32:22.317Z	2024-02-20T19:32:22.317Z
$Txf		2024-02-20T19:32:22.317Z	2024-02-20T19:32:22.317Z
$Tops		2024-02-20T19:32:22.317Z	2024-02-20T19:32:22.317Z
$TxfLog.blf		2024-02-20T19:32:22.317Z	2024-02-20T19:32:22.317Z
System Volume Information		2024-02-20T19:32:24.336Z	2024-02-20T19:32:24.336Z
WPSettings.dat		2024-02-20T19:32:24.336Z	2024-02-20T19:32:24.336Z
documents		2024-02-20T19:32:27.281Z	2024-02-20T19:32:27.290Z
2023		2024-02-20T19:32:27.282Z	2024-02-20T19:32:27.285Z
Final_Annual_Report.xlsx		2024-02-20T19:32:27.282Z	2024-02-20T19:32:27.283Z
Final_Financial_Statement.xlsx		2024-02-20T19:32:27.283Z	2024-02-20T19:32:27.283Z
Final_Project_Proposal.pdf		2024-02-20T19:32:27.283Z	2024-02-20T19:32:27.283Z
Final_Meeting_Minutes.xlsx		2024-02-20T19:32:27.284Z	2024-02-20T19:32:27.284Z
Final_Marketing_Plan.xlsx		2024-02-20T19:32:27.285Z	2024-02-20T19:32:27.285Z
Final_Business_Plan.xlsx		2024-02-20T19:32:27.285Z	2024-02-20T19:32:27.286Z
2024		2024-02-20T19:32:27.286Z	2024-02-20T19:33:30.300Z
Annual_Report.xlsx		2024-02-20T19:32:27.286Z	2024-02-20T19:32:27.287Z
Project_Proposal.pdf		2024-02-20T19:32:27.287Z	2024-02-20T19:33:30.300Z
Meeting_Minutes.xlsx		2024-02-20T19:32:27.287Z	2024-02-20T19:32:27.288Z
Marketing_Plan.xlsx		2024-02-20T19:32:27.288Z	2024-02-20T19:32:27.288Z
Business_Plan.xlsx		2024-02-20T19:32:27.288Z	2024-02-20T19:32:27.288Z
Base_Template.xlsx		2024-02-20T19:32:27.289Z	2024-02-20T19:32:27.289Z

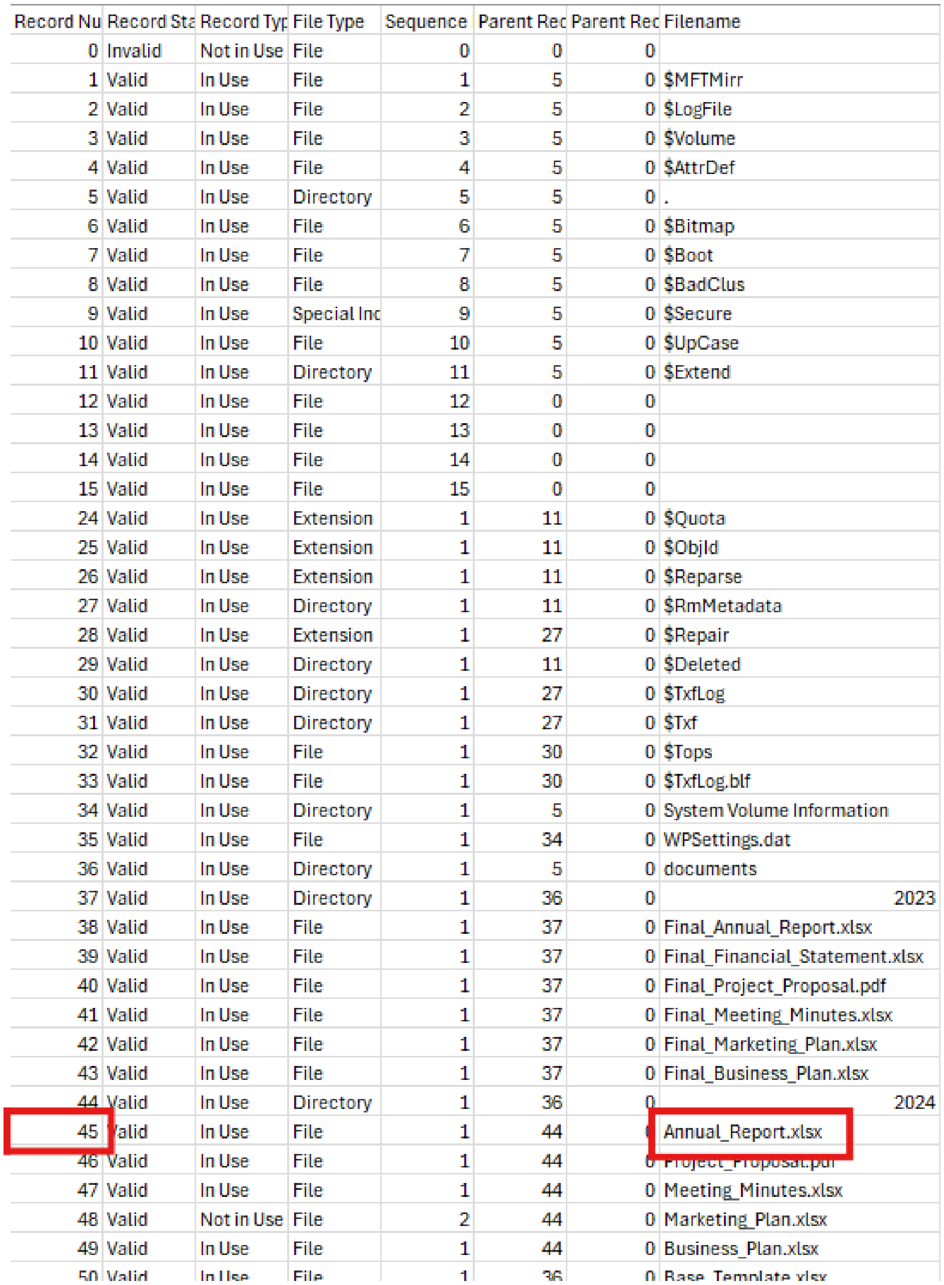
Walaupun ada beberapa file yang beda 0.001 ms, tapi Project_Proposal.pdf punya time difference paling jauh.



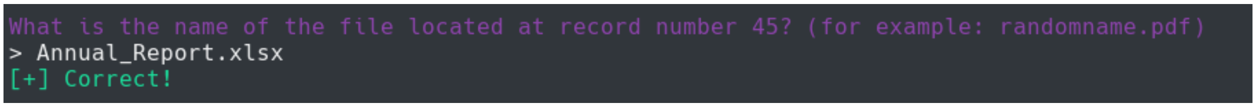
```
Which file was modified after creation? (for example: randomname.pdf)
> project_proposal.pdf
[+] Correct!
```

Question 8: What is the name of the file located at record number 45? (for example: randomname.pdf)

Ini juga cukup gampang, dari file csv kedua, kita liat record number ke 45, yaitu Annual_Report.xlsx



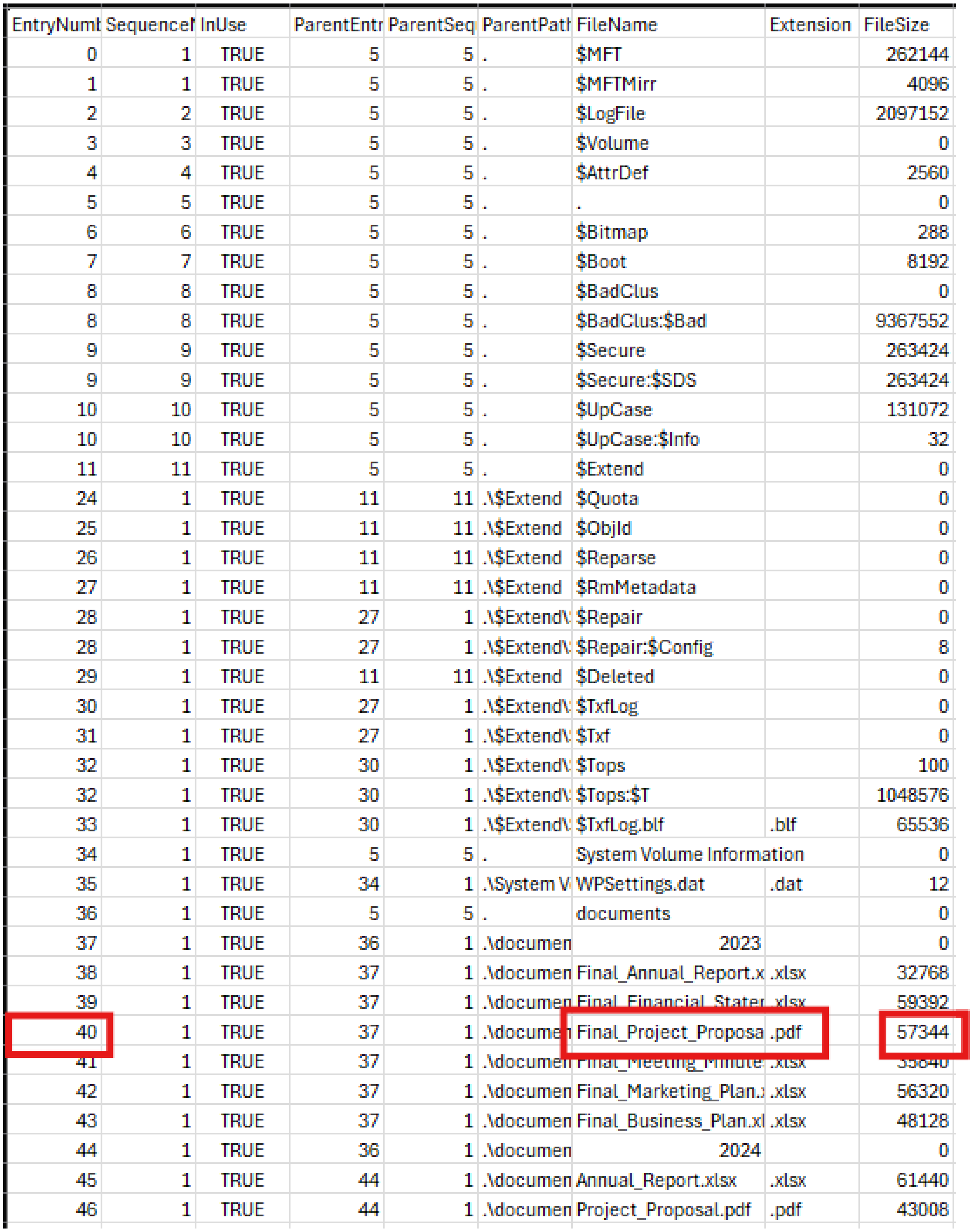
Record Nu	Record Sta	Record Typ	File Type	Sequence	Parent Rec	Parent Rec	Filename
0	Invalid	Not in Use	File	0	0	0	
1	Valid	In Use	File	1	5	0	$MFTMirr
2	Valid	In Use	File	2	5	0	$LogFile
3	Valid	In Use	File	3	5	0	$Volume
4	Valid	In Use	File	4	5	0	$AttrDef
5	Valid	In Use	Directory	5	5	0	.
6	Valid	In Use	File	6	5	0	$Bitmap
7	Valid	In Use	File	7	5	0	$Boot
8	Valid	In Use	File	8	5	0	$BadClus
9	Valid	In Use	Special Inc	9	5	0	$Secure
10	Valid	In Use	File	10	5	0	$UpCase
11	Valid	In Use	Directory	11	5	0	$Extend
12	Valid	In Use	File	12	0	0	
13	Valid	In Use	File	13	0	0	
14	Valid	In Use	File	14	0	0	
15	Valid	In Use	File	15	0	0	
24	Valid	In Use	Extension	1	11	0	$Quota
25	Valid	In Use	Extension	1	11	0	$ObjId
26	Valid	In Use	Extension	1	11	0	$Reparse
27	Valid	In Use	Directory	1	11	0	$RmMetadata
28	Valid	In Use	Extension	1	27	0	$Repair
29	Valid	In Use	Directory	1	11	0	$Deleted
30	Valid	In Use	Directory	1	27	0	$TxfLog
31	Valid	In Use	Directory	1	27	0	$Txf
32	Valid	In Use	File	1	30	0	$Tops
33	Valid	In Use	File	1	30	0	$TxfLog.blf
34	Valid	In Use	Directory	1	5	0	System Volume Information
35	Valid	In Use	File	1	34	0	WPSettings.dat
36	Valid	In Use	Directory	1	5	0	documents
37	Valid	In Use	Directory	1	36	0	2023
38	Valid	In Use	File	1	37	0	Final_Annual_Report.xlsx
39	Valid	In Use	File	1	37	0	Final_Financial_Statement.xlsx
40	Valid	In Use	File	1	37	0	Final_Project_Proposal.pdf
41	Valid	In Use	File	1	37	0	Final_Meeting_Minutes.xlsx
42	Valid	In Use	File	1	37	0	Final_Marketing_Plan.xlsx
43	Valid	In Use	File	1	37	0	Final_Business_Plan.xlsx
44	Valid	In Use	Directory	1	36	0	2024
45	Valid	In Use	File	1	44	0	Annual_Report.xlsx
46	Valid	In Use	File	1	44	0	Project_Proposal.pdf
47	Valid	In Use	File	1	44	0	Meeting_Minutes.xlsx
48	Valid	Not in Use	File	2	44	0	Marketing_Plan.xlsx
49	Valid	In Use	File	1	44	0	Business_Plan.xlsx
50	Valid	In Use	File	1	36	0	Base_Template.xlsx



```
What is the name of the file located at record number 45? (for example: randomname.pdf)
> Annual_Report.xlsx
[+] Correct!
```

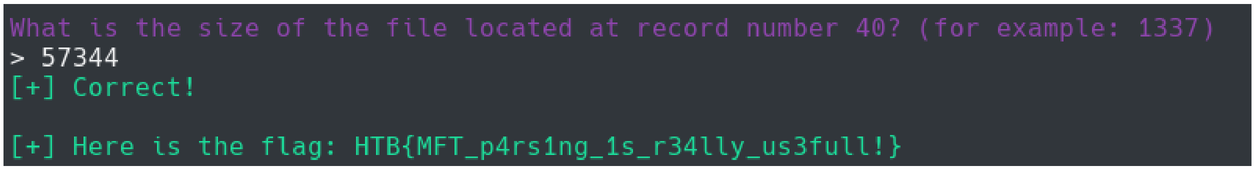
Question 8: What is the size of the file located at record number 40?? (for example: 1337)

Ini juga cukup gampang, tapi karena di file csv kedua gaada informasi buat file size kita pindah ke file pertama, dan ternyata kolom record number menjadi entry number



EntryNumb	SequenceN	InUse	ParentEntr	ParentSeq	ParentPath	FileName	Extension	FileSize
0	1	TRUE	5	5	.	$MFT		262144
1	1	TRUE	5	5	.	$MFTMirr		4096
2	2	TRUE	5	5	.	$LogFile		2097152
3	3	TRUE	5	5	.	$Volume		0
4	4	TRUE	5	5	.	$AttrDef		2560
5	5	TRUE	5	5	.	.		0
6	6	TRUE	5	5	.	$Bitmap		288
7	7	TRUE	5	5	.	$Boot		8192
8	8	TRUE	5	5	.	$BadClus		0
8	8	TRUE	5	5	.	$BadClus:$Bad		9367552
9	9	TRUE	5	5	.	$Secure		263424
9	9	TRUE	5	5	.	$Secure:$SDS		263424
10	10	TRUE	5	5	.	$UpCase		131072
10	10	TRUE	5	5	.	$UpCase:$Info		32
11	11	TRUE	5	5	.	$Extend		0
24	1	TRUE	11	11	.\$Extend	$Quota		0
25	1	TRUE	11	11	.\$Extend	$ObjId		0
26	1	TRUE	11	11	.\$Extend	$Reparse		0
27	1	TRUE	11	11	.\$Extend	$RmMetadata		0
28	1	TRUE	27	1	.\$Extend\	$Repair		0
28	1	TRUE	27	1	.\$Extend\	$Repair:$Config		8
29	1	TRUE	11	11	.\$Extend	$Deleted		0
30	1	TRUE	27	1	.\$Extend\	$TxfLog		0
31	1	TRUE	27	1	.\$Extend\	$Txf		0
32	1	TRUE	30	1	.\$Extend\	$Tops		100
32	1	TRUE	30	1	.\$Extend\	$Tops:$T		1048576
33	1	TRUE	30	1	.\$Extend\	$TxfLog.blf	.blf	65536
34	1	TRUE	5	5	.	System Volume Information		0
35	1	TRUE	34	1	.\System V	WPSettings.dat	.dat	12
36	1	TRUE	5	5	.	documents		0
37	1	TRUE	36	1	.\documen	2023		0
38	1	TRUE	37	1	.\documen	Final_Annual_Report.x	.xlsx	32768
39	1	TRUE	37	1	.\documen	Final_Financial_Stater	.xlsx	59392
40	1	TRUE	37	1	.\documen	Final_Project_Proposa	.pdf	57344
41	1	TRUE	37	1	.\documen	Final_Meeting_Minute:	.xlsx	35840
42	1	TRUE	37	1	.\documen	Final_Marketing_Plan.:	.xlsx	56320
43	1	TRUE	37	1	.\documen	Final_Business_Plan.xl	.xlsx	48128
44	1	TRUE	36	1	.\documen	2024		0
45	1	TRUE	44	1	.\documen	Annual_Report.xlsx	.xlsx	61440
46	1	TRUE	44	1	.\documen	Project_Proposal.pdf	.pdf	43008

Bisa kita liat file size Final_Project_Proposal.xlsx adalah 57344

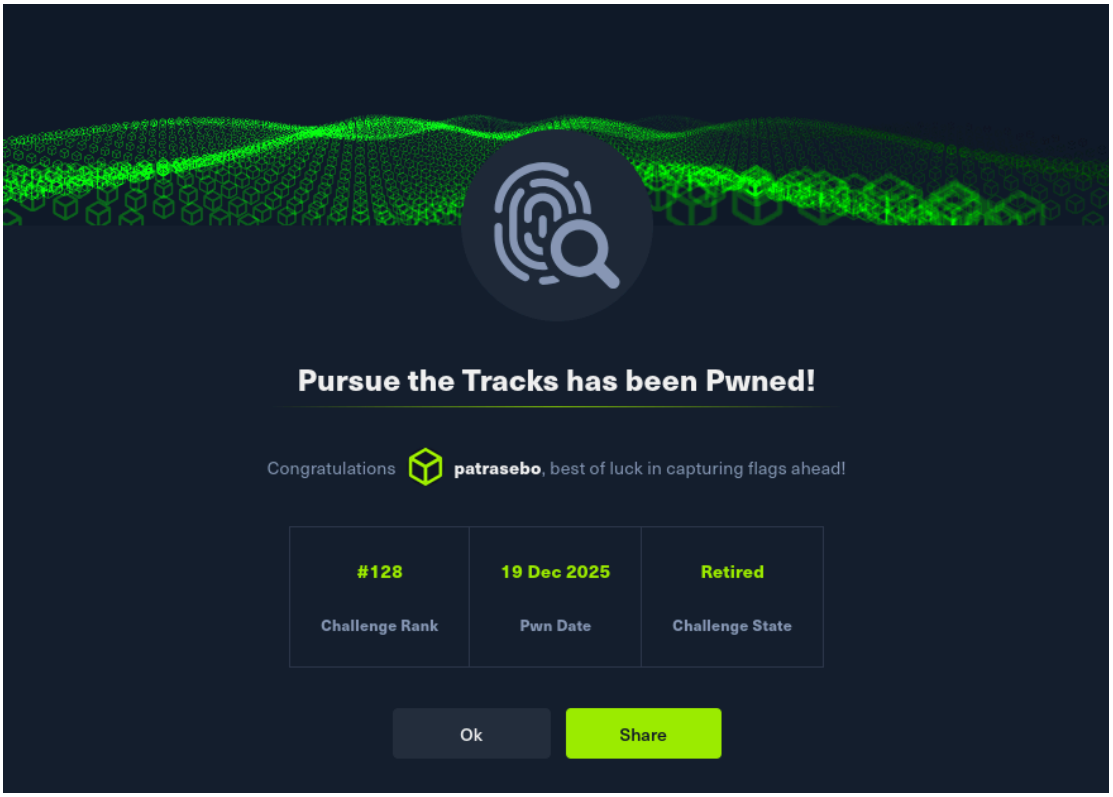


```
What is the size of the file located at record number 40? (for example: 1337)
> 57344
[+] Correct!

[+] Here is the flag: HTB{MFT_p4rs1ng_1s_r34lly_us3full!}
```

Dan setelah 9 pertanyaan, kita berhasil dapet flagnya.

Flag:

HTB{MFT_p4rs1ng_1s_r34lly_us3full!}



Pursue the Tracks has been Pwned!

Congratulations **patrasebo**, best of luck in capturing flags ahead!

#128	19 Dec 2025	Retired
Challenge Rank	Pwn Date	Challenge State