TryHackMe Windows Forensics 2 Write-Up

Toumo · Follow

7 min read · Aug 7, 2023

Listen Share More

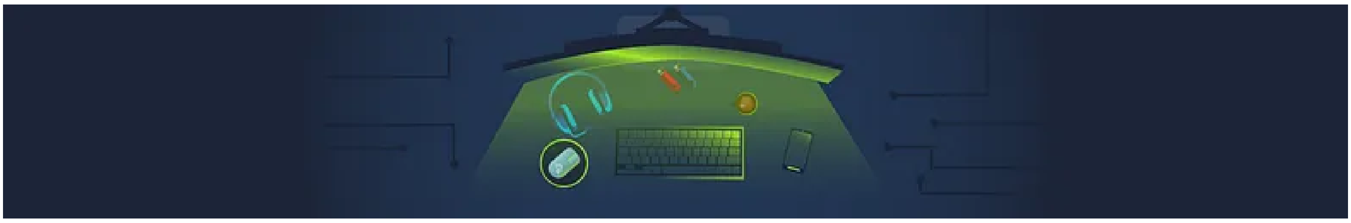


Image from tryhackme.comF

This is the second part of Windows Forensics. The write-up I did for the first part can be found here. I enjoyed the difficulty last time and I hope this time will be the same. Looks like we're not going tob e focused on the registry but also on the file system this time. Let's get started!

Task 2 The FAT file systems

1: How many addressable bits are there in the FAT32 file system?

This can be found in the reading.

Answer: 28 bits

2: What is the maximum file size supported by the FAT32 file system?

This can be found in the reading. Just note that while FAT32 can hold up to 2TB, a **single** file can only be a maximum of 4GB.

Answer: 4GB

3: Which file system is used by digital cameras and SD cards?

This can be found in the reading.

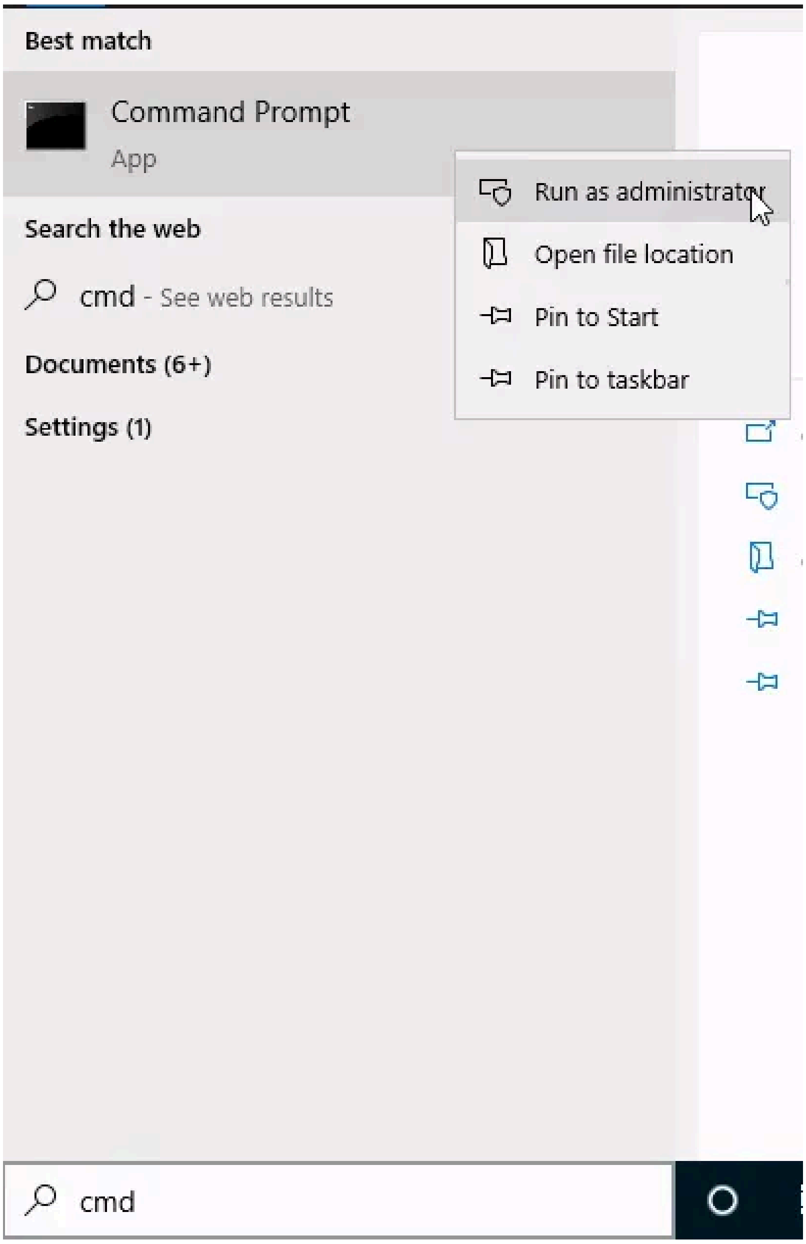
Answer: exFAT

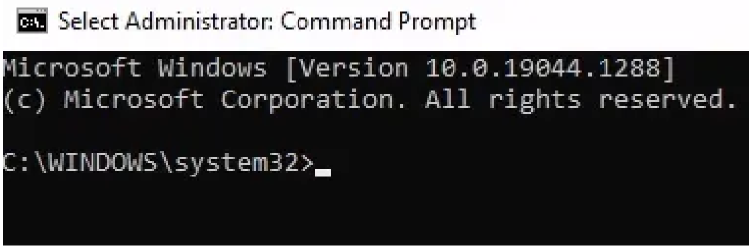
Task 3 The NTFS File System

I will be RDPing into the machine. I wrote a guide here. Please check it out!

1: Parse the $MFT file placed in `C:\users\THM-4n6\Desktop\triage\C\` and analyze it. What is the Size of the file located at `.\Windows\Security\logs\SceSetupLog.etl`

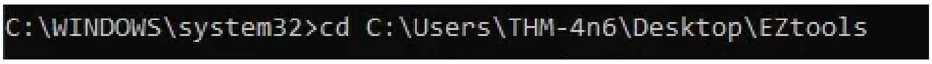
First, we will open the command prompt and run it as an administrator. Go to the search bar next to the start menu and type in cmd. Right click command prompt and run it as administrator. If you did it correctly, it should show C:\WINDOWS\system32 like below.





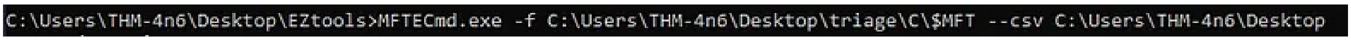
```
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Let’s navigate to where EZtools is at with `cd C:\Users\THM-4n6\Desktop\EZtools`



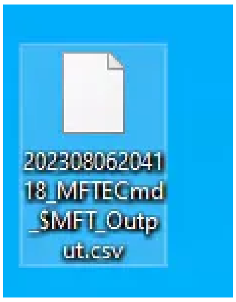
```
C:\WINDOWS\system32>cd C:\Users\THM-4n6\Desktop\EZtools
```

Now we will run the following command to parse the $MFT file and save it to a new location with `MFTECmd.exe -f C:\Users\THM-4n6\Desktop\triage\C\$MFT -csv C:\Users\THM-4n6\Desktop` . I got the command from the reading.



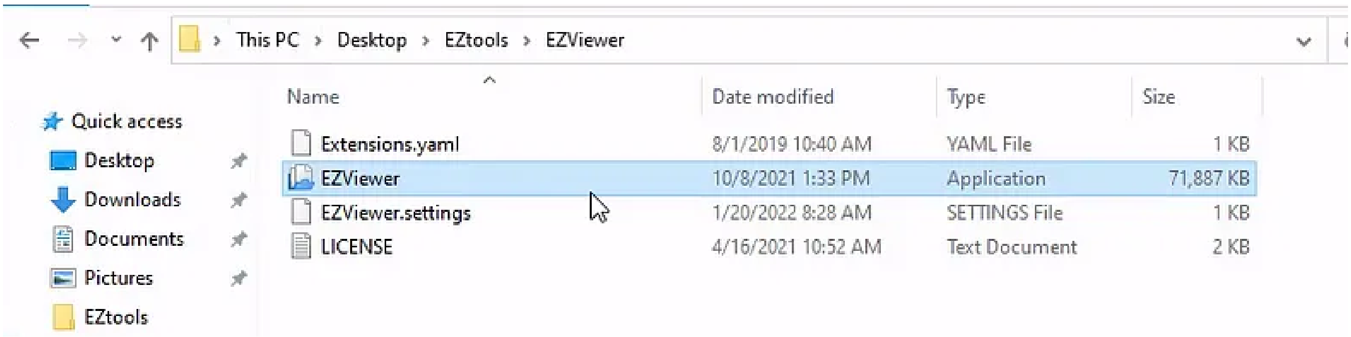
```
C:\Users\THM-4n6\Desktop\EZtools>MFTECmd.exe -f C:\Users\THM-4n6\Desktop\triage\C\$MFT --csv C:\Users\THM-4n6\Desktop
```

It may take a while to process. The new file will appear in the desktop.



20230806204118_MFTECmd_$MFT_Output.csv

Now lets open EZViewer. It can be found in your Desktop folder -> EZtools -> EZViewer.

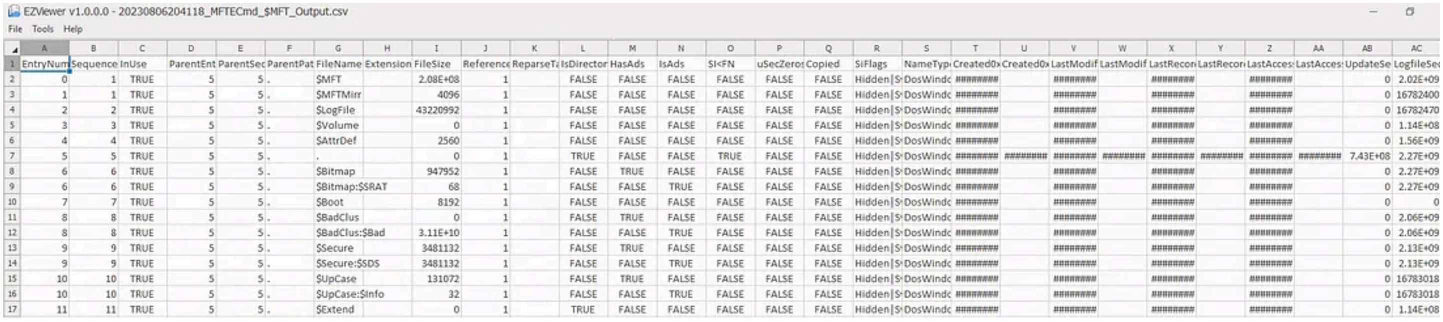


This PC › Desktop › EZtools › EZViewer

Name	Date modified	Type	Size
Extensions.yaml	8/1/2019 10:40 AM	YAML File	1 KB
EZViewer	10/8/2021 1:33 PM	Application	71,887 KB
EZViewer.settings	1/20/2022 8:28 AM	SETTINGS File	1 KB
LICENSE	4/16/2021 10:52 AM	Text Document	2 KB

Once EZViewer loads, I dragged our output file into EZViewer.

If done correctly, it should load the file and it'll look like an excel spreadsheet.

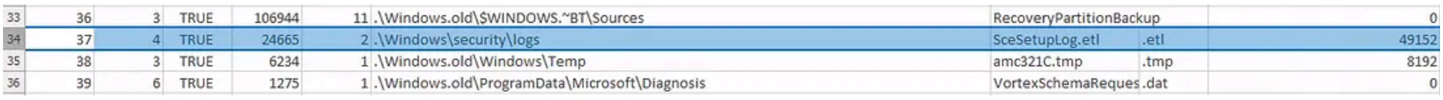


EZViewer v1.0.0.0 - 20230806204118_MFTECmd_$MFT_Output.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	EntryNum	Sequence	InUse	ParentEnt	ParentSec	ParentPat	FileName	Extension	FileSize	Reference	ReparseT	IsDirector	HasAds	IsAds	SI<FN
2	0	1	TRUE	5	5	.	$MFT		2.08E+08	1		FALSE	FALSE	FALSE	FALSE
3	1	1	TRUE	5	5	.	$MFTMirr		4096	1		FALSE	FALSE	FALSE	FALSE
4	2	2	TRUE	5	5	.	$LogFile		43220992	1		FALSE	FALSE	FALSE	FALSE
5	3	3	TRUE	5	5	.	$Volume		0	1		FALSE	FALSE	FALSE	FALSE
6	4	4	TRUE	5	5	.	$AttrDef		2560	1		FALSE	FALSE	FALSE	FALSE
7	5	5	TRUE	5	5	.	.		0	1		TRUE	FALSE	FALSE	TRUE
8	6	6	TRUE	5	5	.	$Bitmap		947952	1		FALSE	TRUE	FALSE	FALSE
9	6	6	TRUE	5	5	.	$Bitmap:$SRAT		68	1		FALSE	FALSE	TRUE	FALSE
10	7	7	TRUE	5	5	.	$Boot		8192	1		FALSE	FALSE	FALSE	FALSE
11	8	8	TRUE	5	5	.	$BadClus		0	1		FALSE	TRUE	FALSE	FALSE
12	8	8	TRUE	5	5	.	$BadClus:$Bad		3.11E+10	1		FALSE	FALSE	TRUE	FALSE
13	9	9	TRUE	5	5	.	$Secure		3481132	1		FALSE	TRUE	FALSE	FALSE
14	9	9	TRUE	5	5	.	$Secure:$SDS		3481132	1		FALSE	FALSE	TRUE	FALSE
15	10	10	TRUE	5	5	.	$UpCase		131072	1		FALSE	TRUE	FALSE	FALSE
16	10	10	TRUE	5	5	.	$UpCase:$Info		32	1		FALSE	FALSE	TRUE	FALSE
17	11	11	TRUE	5	5	.	$Extend		0	1		TRUE	FALSE	FALSE	FALSE

	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	uSecZeros	Copied	SiFlags	NameTyp	Created0x	Created0x	LastModif	LastModif	LastRecor	LastRecor	LastAcces	LastAcces	UpdateSe	LogfileSe
2	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.02E+09
3	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	16782400
4	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	16782470
5	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	1.14E+08
6	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	1.56E+09
7	FALSE	FALSE	Hidden|S	DosWindc	########	########	########	########	########	########	########	########	7.43E+08	2.27E+09
8	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.27E+09
9	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.27E+09
10	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	0
11	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.06E+09
12	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.06E+09
13	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.13E+09
14	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	2.13E+09
15	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	16783018
16	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	16783018
17	FALSE	FALSE	Hidden|S	DosWindc	########		########		########		########		0	1.14E+08

The next step took me about 10 minutes. I did CTRL+F to help find my results and pasted `.\Windows\Security\logs\SceSetupLog.etl` but I kept getting no results. I ended up trying out `.\Windows\Se` to see if this works. I ended up finding what I need!



33	36	3	TRUE	106944	11	.\Windows.old\$WINDOWS.~BT\Sources		RecoveryPartitionBackup			0
34	37	4	TRUE	24665	2	.\Windows\security\logs		SceSetupLog.etl	.etl		49152
35	38	3	TRUE	6234	1	.\Windows.old\Windows\Temp		amc321C.tmp	.tmp		8192
36	39	6	TRUE	1275	1	.\Windows.old\ProgramData\Microsoft\Diagnosis		VortexSchemaReques	.dat		0

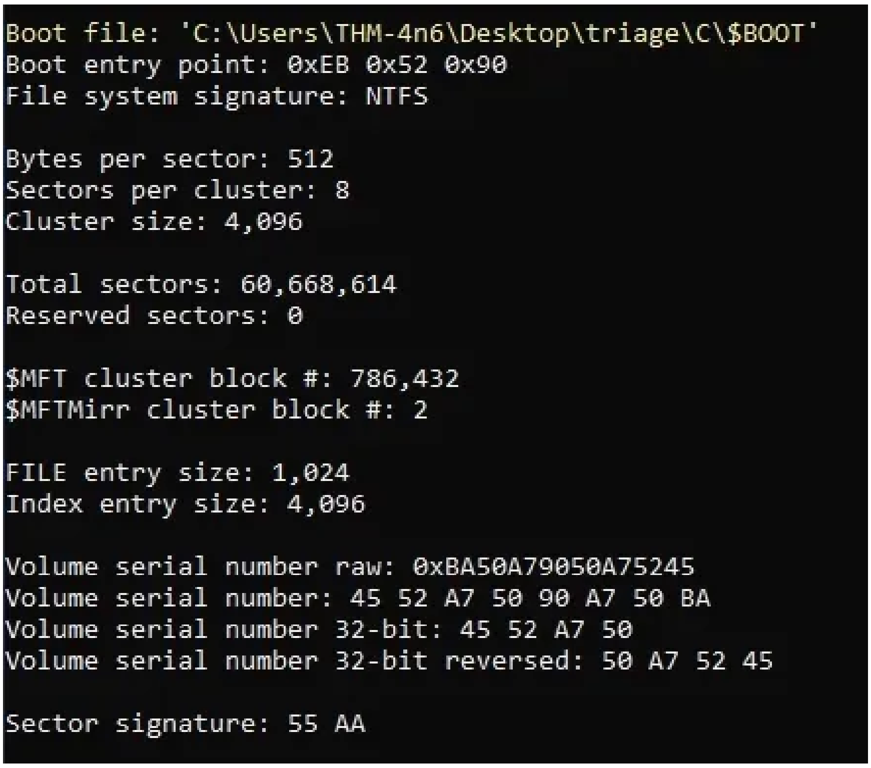
I extended a few column headers to see what the columns were displaying.

Answer: 49152

2: What is the size of the cluster for the volume from which this triage was taken?

I had to look at the hint for this. Looks like we need to parse the $BOOT file this time. The command I used is `MFTECmd.exe -f C:\Users\THM-4n6\Desktop\triage\C\$BOOT` . Remember that your command prompt has to be in administrator mode, and it has to be in the EZTool folder.

The output should be like this.



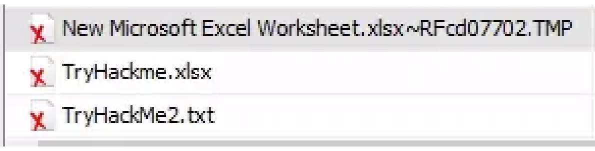
```
Boot file: 'C:\Users\THM-4n6\Desktop\triage\C\$BOOT'
Boot entry point: 0xEB 0x52 0x90
File system signature: NTFS

Bytes per sector: 512
Sectors per cluster: 8
Cluster size: 4,096

Total sectors: 60,668,614
Reserved sectors: 0

$MFT cluster block #: 786,432
$MFTMirr cluster block #: 2

FILE entry size: 1,024
Index entry size: 4,096

Volume serial number raw: 0xBA50A79050A75245
Volume serial number: 45 52 A7 50 90 A7 50 BA
Volume serial number 32-bit: 45 52 A7 50
Volume serial number 32-bit reversed: 50 A7 52 45

Sector signature: 55 AA
```

Answer: 4096

Task 4 Recovering deleted files

1: There is another xlsx file that was deleted. What is the full name of that file?

I followed the instructions per the reading to set up Autopsy. There are a few deleted files I can see. Deleted files has an X mark on their icon. The first one, “New Microsoft Excel Worksheet.xlsx” was part of the Autopsy set up demonstration. The second one is the answer.



New Microsoft Excel Worksheet.xlsx~RFcd07702.TMP
TryHackme.xlsx
TryHackMe2.txt

Answer: TryHackme.xlsx

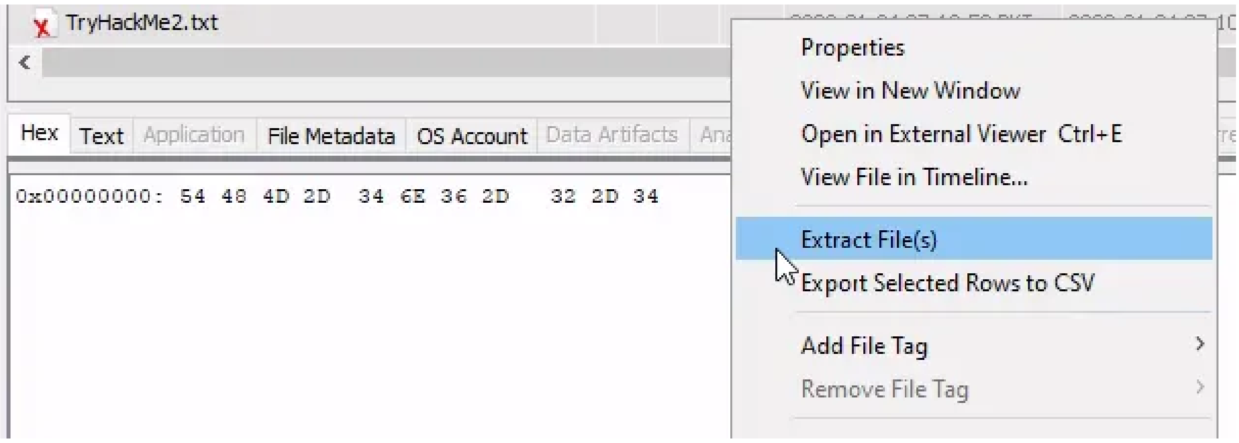
2: What is the name of the TXT file that was deleted from the disk?

From the above screenshot, we can see another deleted file, this time a .txt. This is what we need.

Answer: TryHackMe2.txt

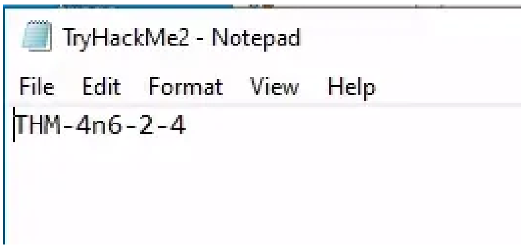
3: Recover the TXT file from Question #2. What was written in this txt file?

Right click the file and then select Extra File(s). Remember where you saved it!



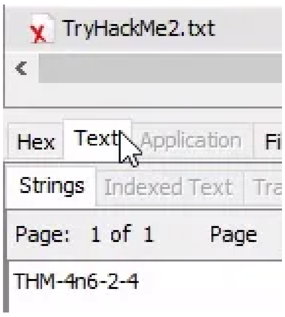
```
0x00000000: 54 48 4D 2D  34 6E 36 2D   32 2D 34
```

After that, it’s a matter of opening that file to view contents.



THM-4n6-2-4

Alternatively, you can view text file directly from Autopsy by selecting the Text tab at the bottom.


TryHackMe2.txt

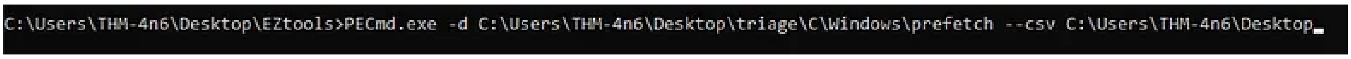
THM-4n6-2-4

Answer: THM-4n6–2–4

Task 5 Evidence of Execution

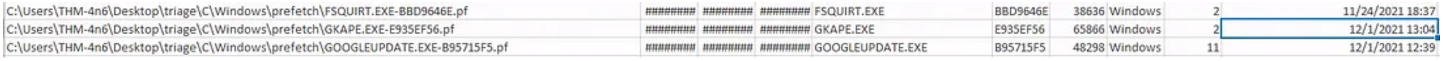
1: How many times was gkape.exe executed?

Looks like we will be parsing files quite a bit in this section. Since we are checking how many times a certain file was executed, we will be using Prefetch Parser. The command is that I used is `PECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch -csv C:\Users\THM-4n6\Desktop` . I modified the example command given from the reading. The location of the prefetch directory we need to parse is at `C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch` .



```
C:\Users\THM-4n6\Desktop\EZtools>PECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch --csv C:\Users\THM-4n6\Desktop_
```

Two output files should appear. I opened the PECmd_Output.csv file (not timeline) with EZViewer. To search for the file, I did CTRL+F and typed in gkape.exe. There may be two results. The first result didn't really give me the path that I needed. The second one sent me to the path I need. I then scrolled up to look at the column headers and saw it was ran twice.



C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch\FSQUIRT.EXE-BBD9646E.pf	########	########	########	FSQUIRT.EXE	BBD9646E	38636	Windows	2	11/24/2021 18:37
C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch\GKAPE.EXE-E935EF56.pf	########	########	########	GKAPE.EXE	E935EF56	65866	Windows	2	12/1/2021 13:04
C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch\GOOGLEUPDATE.EXE-B95715F5.pf	########	########	########	GOOGLEUPDATE.EXE	B95715F5	48298	Windows	11	12/1/2021 12:39

Answer: 2

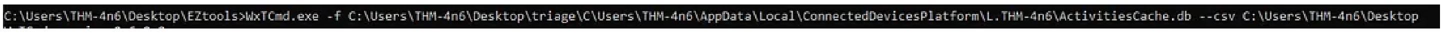
2: What is the last execution time of gkape.exe

The above screenshot also shows the last time it was executed. Also note that THM wants the answer in a MM/**DD**/YYYY HH:MM format. I was wondering why 12/1/2012 13:04 didn't work for a bit.

Answer: 12/01/2021 13:04

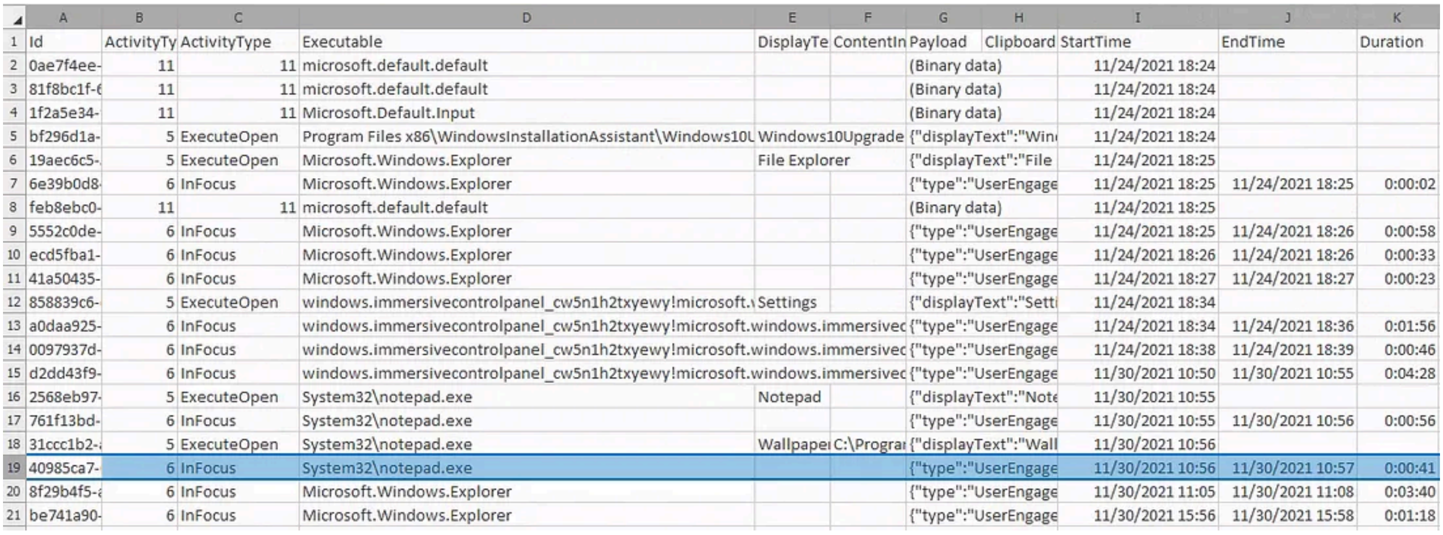
3: When Notepad.exe was opened on 11/30/2021 at 10:56, how long did it remain in focus?

Since we are going to see how long a certain application has been in focus, we will need to parse using Windows 10 Timeline. I used the following command on the command line. `WxTCmd.exe -f C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Local\ConnectedDevicesPlatform\L.THM-4n6\ActivitiesCache.db — csv C:\Users\THM-4n6\Desktop` .



```
C:\Users\THM-4n6\Desktop\EZtools>WxTCmd.exe -f C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Local\ConnectedDevicesPlatform\L.THM-4n6\ActivitiesCache.db --csv C:\Users\THM-4n6\Desktop
```

Two files should be outputted. I opened Activity.csv (not Activity Package ID) with EZViewer. I used CTRL+F again and looked for notepad.exe. There are 4 results. Make sure you check the correct notepad.exe! I definitely didn't make that mistake and entered 0:00:56 twice! Then look at the duration.

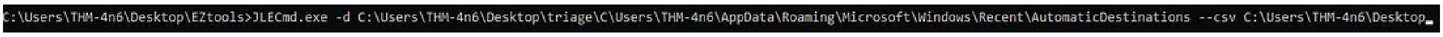


	A	B	C	D	E	F	G	H	I	J	K
1	Id	ActivityTy	ActivityType	Executable	DisplayTe	ContentIn	Payload	Clipboard	StartTime	EndTime	Duration
2	0ae7f4ee-	11	11	microsoft.default.default			(Binary data)		11/24/2021 18:24		
3	81f8bc1f-6	11	11	microsoft.default.default			(Binary data)		11/24/2021 18:24		
4	1f2a5e34-	11	11	Microsoft.Default.Input			(Binary data)		11/24/2021 18:24		
5	bf296d1a-	5	ExecuteOpen	Program Files x86\WindowsInstallationAssistant\Windows10U	Windows10Upgrade		{"displayText":"Win		11/24/2021 18:24		
6	19aec6c5-	5	ExecuteOpen	Microsoft.Windows.Explorer	File Explorer		{"displayText":"File		11/24/2021 18:25		
7	6e39b0d8-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/24/2021 18:25	11/24/2021 18:25	0:00:02
8	feb8ebc0-	11	11	microsoft.default.default			(Binary data)		11/24/2021 18:25		
9	5552c0de-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/24/2021 18:25	11/24/2021 18:26	0:00:58
10	ecd5fba1-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/24/2021 18:26	11/24/2021 18:26	0:00:33
11	41a50435-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/24/2021 18:27	11/24/2021 18:27	0:00:23
12	858839c6-	5	ExecuteOpen	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.\	Settings		{"displayText":"Setti		11/24/2021 18:34		
13	a0daa925-	6	InFocus	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivec			{"type":"UserEngage		11/24/2021 18:34	11/24/2021 18:36	0:01:56
14	0097937d-	6	InFocus	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivec			{"type":"UserEngage		11/24/2021 18:38	11/24/2021 18:39	0:00:46
15	d2dd43f9-	6	InFocus	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivec			{"type":"UserEngage		11/30/2021 10:50	11/30/2021 10:55	0:04:28
16	2568eb97-	5	ExecuteOpen	System32\notepad.exe	Notepad		{"displayText":"Note		11/30/2021 10:55		
17	761f13bd-	6	InFocus	System32\notepad.exe			{"type":"UserEngage		11/30/2021 10:55	11/30/2021 10:56	0:00:56
18	31ccc1b2-	5	ExecuteOpen	System32\notepad.exe	Wallpaper	C:\Progra	{"displayText":"Wall		11/30/2021 10:56		
19	40985ca7-	6	InFocus	System32\notepad.exe			{"type":"UserEngage		11/30/2021 10:56	11/30/2021 10:57	0:00:41
20	8f29b4f5-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/30/2021 11:05	11/30/2021 11:08	0:03:40
21	be741a90-	6	InFocus	Microsoft.Windows.Explorer			{"type":"UserEngage		11/30/2021 15:56	11/30/2021 15:58	0:01:18

Answer: 00:00:41

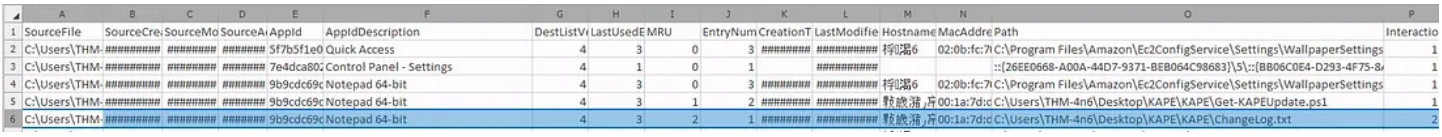
4: What program was used to open C:\Users\THM-4n6\Desktop\KAPE\KAPE\ChangeLog.txt?

Back to the terminal again! This time we will be parsing the Jump Lists. I typed in `JLECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations — csv C:\Users\THM-4n6\Desktop` in the terminal. Again, I modified the example command that was given in the reading.



```
C:\Users\THM-4n6\Desktop\EZtools>JLECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations --csv C:\Users\THM-4n6\Desktop_
```

I opened the output file, AutomaticDestinations.csv, with EZViewer. I used CTRL+F to find KAPE\KAPE and found few results. I'm not entirely sure but I looked at AppIdDescription and saw notepad, so my guess was the user used notepad.



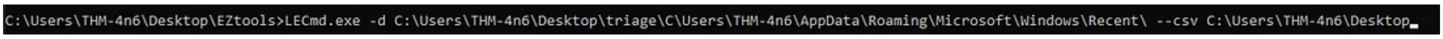
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	SourceFile	SourceCre	SourceMo	SourceA	AppId	AppIdDescription	DestListV	LastUsedE	MRU	EntryNum	CreationT	LastModifie	Hostname	MacAddre	Path	Interactio
2	C:\Users\THM-	#########	########	#######	5f7b5f1e0	Quick Access	4	3	0	3	########	##########	桔ⵍ渴6	02:0b:fc:7	C:\Program Files\Amazon\Ec2ConfigService\Settings\WallpaperSettings	1
3	C:\Users\THM-	#########	########	#######	7e4dca80	Control Panel - Settings	4	1	0	1		##########			::{26EE0668-A00A-44D7-9371-BEB064C98683}\5\::{BB06C0E4-D293-4F75-8	1
4	C:\Users\THM-	#########	########	#######	9b9cdc69c	Notepad 64-bit	4	3	0	3	########	##########	桔ⵍ渴6	02:0b:fc:7	C:\Program Files\Amazon\Ec2ConfigService\Settings\WallpaperSettings	1
5	C:\Users\THM-	#########	########	#######	9b9cdc69c	Notepad 64-bit	4	3	1	2	########	##########	敷歲漪,斥	00:1a:7d:c	C:\Users\THM-4n6\Desktop\KAPE\KAPE\Get-KAPEUpdate.ps1	1
6	C:\Users\THM-	#########	########	#######	9b9cdc69c	Notepad 64-bit	4	3	2	1	########	##########	敷歲漪,斥	00:1a:7d:c	C:\Users\THM-4n6\Desktop\KAPE\KAPE\ChangeLog.txt	2

Answer: Notepad.exe

Task 6 File/folder knowledge

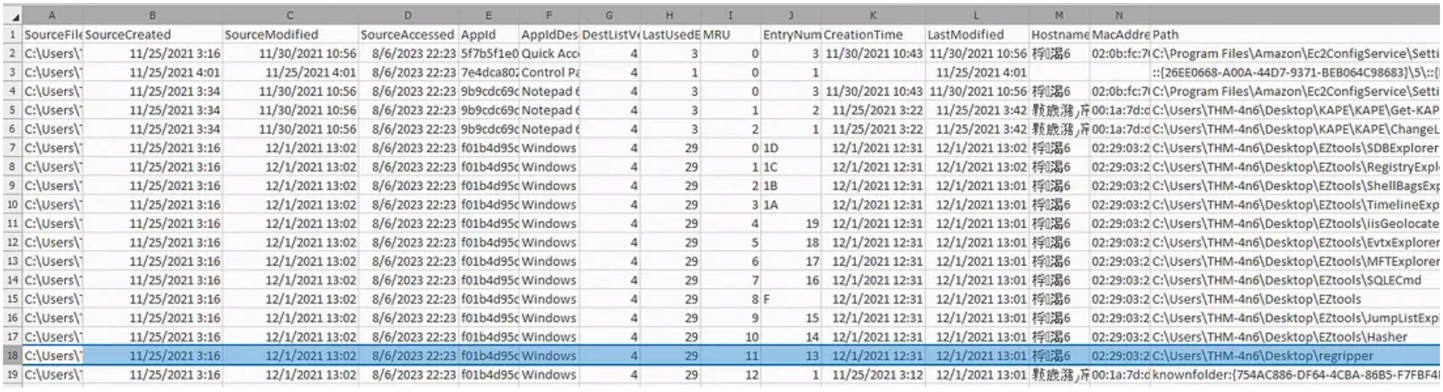
1: When was the folder C:\Users\THM-4n6\Desktop\regripper last opened?

I used the following command `LECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\ — csv C:\Users\THM-4n6\Desktop` . I modified the example given in the reading.



```
C:\Users\THM-4n6\Desktop\EZtools>LECmd.exe -d C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\ --csv C:\Users\THM-4n6\Desktop_
```

I opened the output, LECmd_Output.csv, with EZViewer. I used CTRL+F and searched for regripper. I inputted quite a few dates before finding out that LastModified had the right answer.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
1	SourceFile	SourceCreated	SourceModified	SourceAccessed	AppId	AppIdDes	DestListV	LastUsedE	MRU	EntryNum	CreationTime	LastModified	Hostname	MacAddre	Path
2	C:\Users\T	11/25/2021 3:16	11/30/2021 10:56	8/6/2023 22:23	5f7b5f1e0	Quick Acc	4	3	0	3	11/30/2021 10:43	11/30/2021 10:56	桔ⵍ渴6	02:0b:fc:7	C:\Program Files\Amazon\Ec2ConfigService\Setti
3	C:\Users\T	11/25/2021 4:01	11/25/2021 4:01	8/6/2023 22:23	7e4dca80	Control Pa	4	1	0	1		11/25/2021 4:01			::{26EE0668-A00A-44D7-9371-BEB064C98683}\5\::{
4	C:\Users\T	11/25/2021 3:34	11/30/2021 10:56	8/6/2023 22:23	9b9cdc69c	Notepad 6	4	3	0	3	11/30/2021 10:43	11/30/2021 10:56	桔ⵍ渴6	02:0b:fc:7	C:\Program Files\Amazon\Ec2ConfigService\Setti
5	C:\Users\T	11/25/2021 3:34	11/30/2021 10:56	8/6/2023 22:23	9b9cdc69c	Notepad 6	4	3	1	2	11/25/2021 3:22	11/25/2021 3:42	敷歲漪,斥	00:1a:7d:c	C:\Users\THM-4n6\Desktop\KAPE\KAPE\Get-KAP
6	C:\Users\T	11/25/2021 3:34	11/30/2021 10:56	8/6/2023 22:23	9b9cdc69c	Notepad 6	4	3	2	1	11/25/2021 3:22	11/25/2021 3:42	敷歲漪,斥	00:1a:7d:c	C:\Users\THM-4n6\Desktop\KAPE\KAPE\ChangeL
7	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	0	1D	12/1/2021 12:31	12/1/2021 13:02	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\SDBExplorer
8	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	1	1C	12/1/2021 12:31	12/1/2021 13:02	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\RegistryExpl
9	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	2	1B	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\ShellBagsExp
10	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	3	1A	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\TimelineExp
11	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	4	19	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\iisGeolocate
12	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	5	18	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\EvtxExplorer
13	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	6	17	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\MFTExplorer
14	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	7	16	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\SQLECmd
15	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	8	F	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools
16	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	9	15	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\JumpListExp
17	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	10	14	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\EZtools\Hasher
18	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	11	13	12/1/2021 12:31	12/1/2021 13:01	桔ⵍ渴6	02:29:03:2	C:\Users\THM-4n6\Desktop\regripper
19	C:\Users\T	11/25/2021 3:16	12/1/2021 13:02	8/6/2023 22:23	f01b4d95c	Windows	4	29	12	1	11/25/2021 3:12	12/1/2021 13:01	敷歲漪,斥	00:1a:7d:c	knownfolder:{754AC886-DF64-4CBA-86B5-F7FBF4

Answer: 12/1/2021 13:01

2: When was the above-mentioned folder first opened?

From the above screenshot, this time we enter the date found in CreationTime.

Answer: 12/1/2021 12:31

Task 7 External Devices/USB device forensics

1: Which artifact will tell us the first and last connection times of a removable drive?

The answer can be found in the reading.

Answer: setupapi.dev.log

Thoughts:

I still enjoyed it as much as the first room. Definitely had a bit of setting up to do. I wished Autopsy was used more but I know there is a dedicated Autopsy room a bit later in this Digital Forensics room. I'm really enjoying, and seeing, the benefits of Eric Zimmerman's tools. It would be cool if there was a cheat sheet here too as there was just too much information to absorb. Can't wait for the Linux room!

Cybersecurity Tryhackme Digital Forensics Dfir Digital Forensic Tools

Follow

Written by Toumo

152 Followers · 1 Following

Responses (1)

What are your thoughts?

Respond

Samar
about 2 months ago

thanks

Reply

More from Toumo

Toumo

TryHackMe Redline Write-Up

We just finished the Autopsy room and now we will be learning how to use Redline. I've never used it, nor have I heard of it before, so...

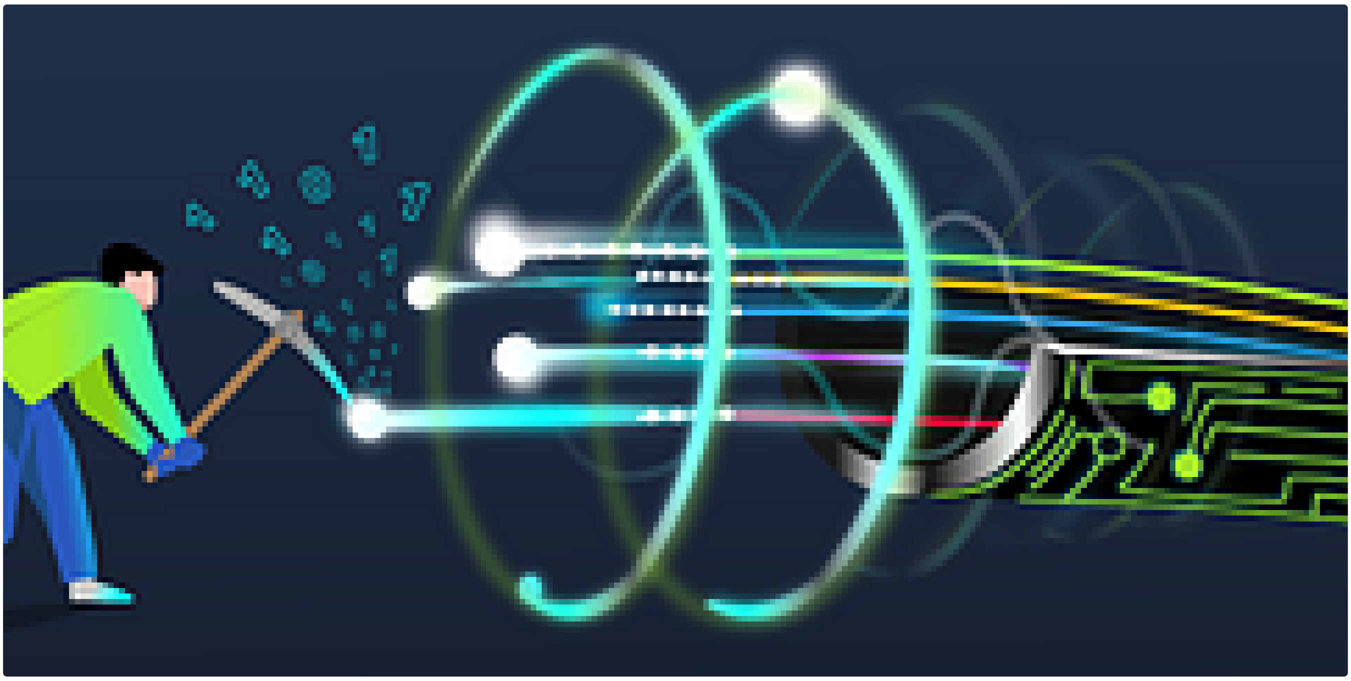
Aug 8, 2023 45 4

Toumo

TryHackMe Velociraptor Write-Up

We'll be learning about Velociraptor now. Another tool that I never heard of but I wonder how this will be different compared to the rest...

Aug 9, 2023 20 1

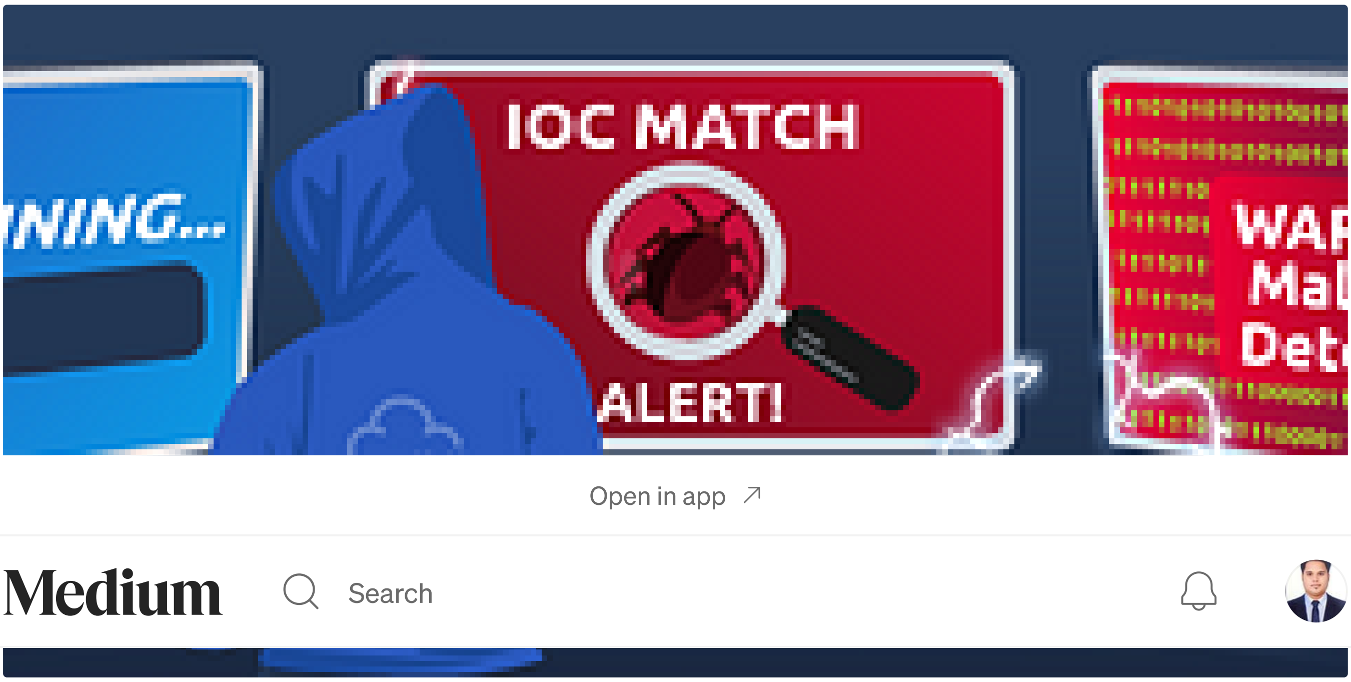


Toumo

TryHackMe NetworkMiner Write-Up

This time, we will be using a new tool called NetworkMiner. My assumption is that we're being exposed to many tools as we do not know what...

Jul 5, 2023 6 1



Open in app ↗

Medium Search

T Toumo

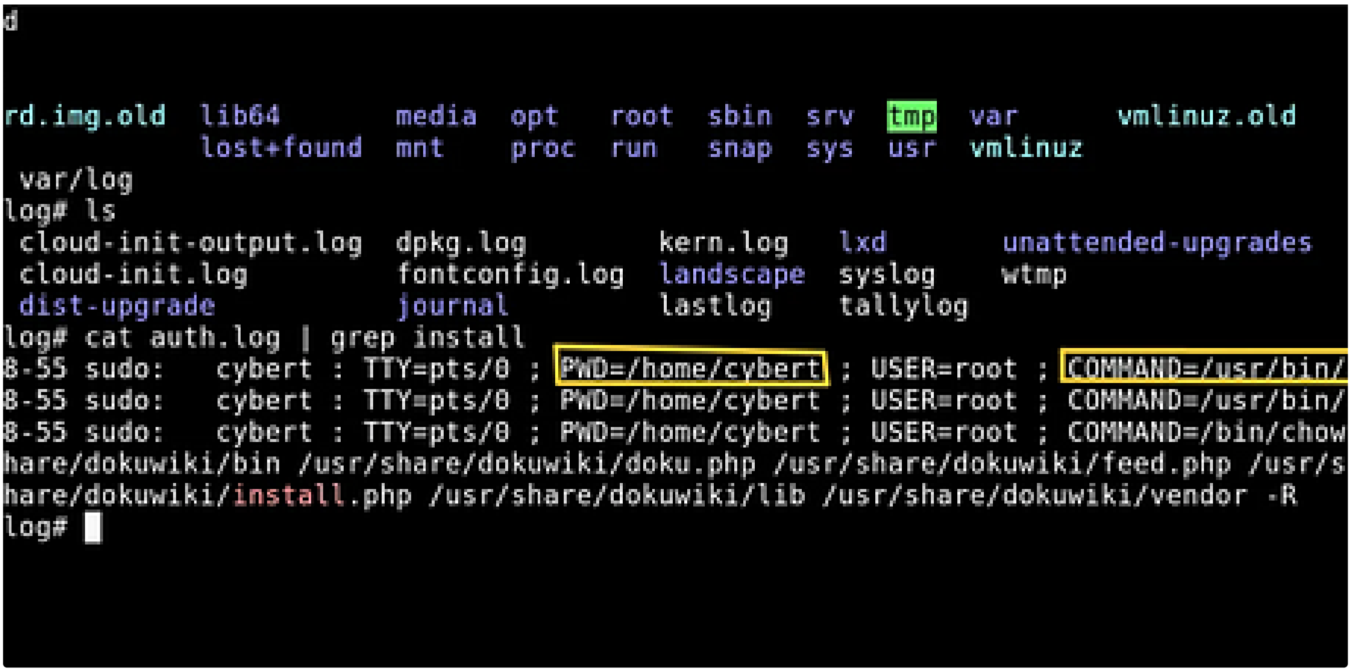
TryHackMe Sysmon Write-Up

We will be doing the Sysmon room this time. I don’t know about Sysmon too much except that it’s usually running in the background and helps...

Jul 31, 2023 6

See all from Toumo

Recommended from Medium



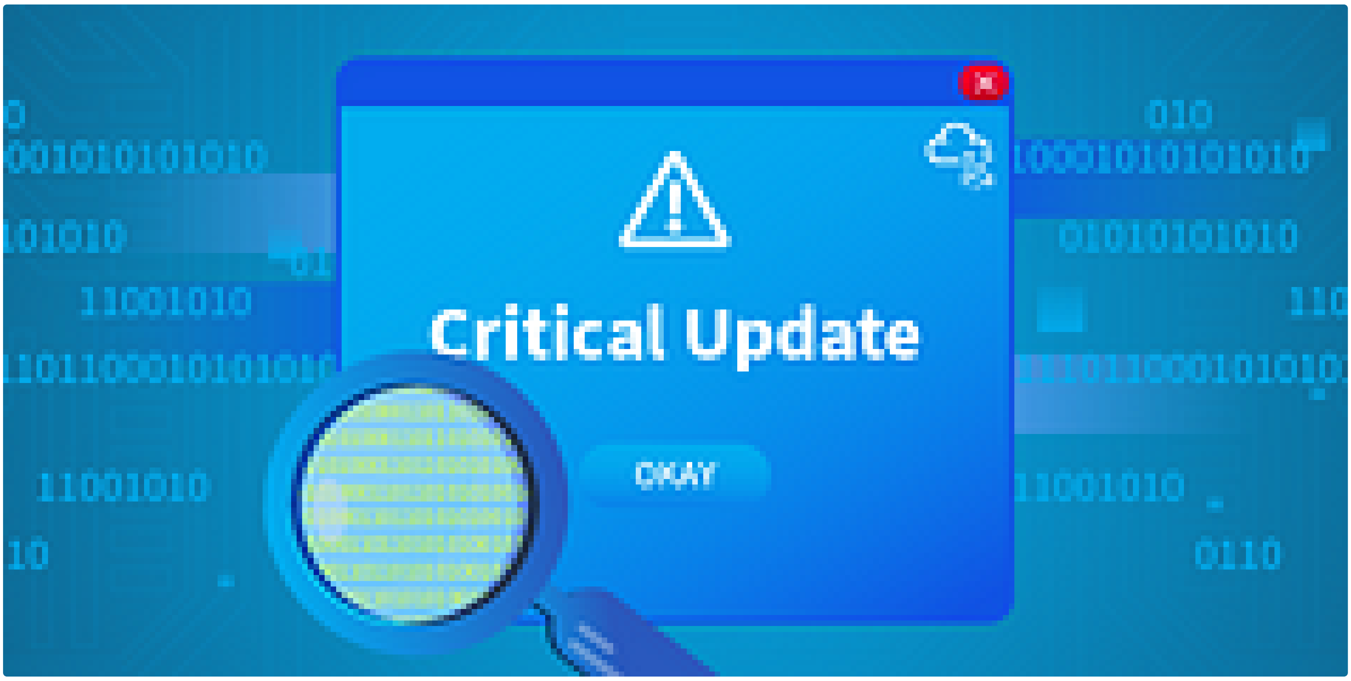
```
d


rd.img.old  lib64        media  opt   root  sbin  srv  tmp  var      vmlinuz.old
            lost+found   mnt    proc  run   snap  sys  usr  vmlinuz
 var/log
log# ls
 cloud-init-output.log  dpkg.log        kern.log   lxd       unattended-upgrades
 cloud-init.log         fontconfig.log  landscape  syslog    wtmp
 dist-upgrade           journal         lastlog    tallylog
log# cat auth.log | grep install
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:   cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log# 
```

T Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here: https://tryhackme.com/room/disgruntled

Oct 22, 2024



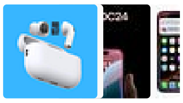
In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

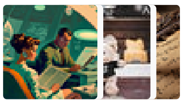
Jul 21, 2024 104

Lists



Tech & Tools

22 stories · 380 saves

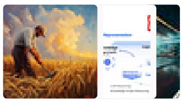


Medium's Huge List of Publications Accepting Submissions

377 stories · 4345 saves

Staff picks

796 stories · 1561 saves



Natural Language Processing

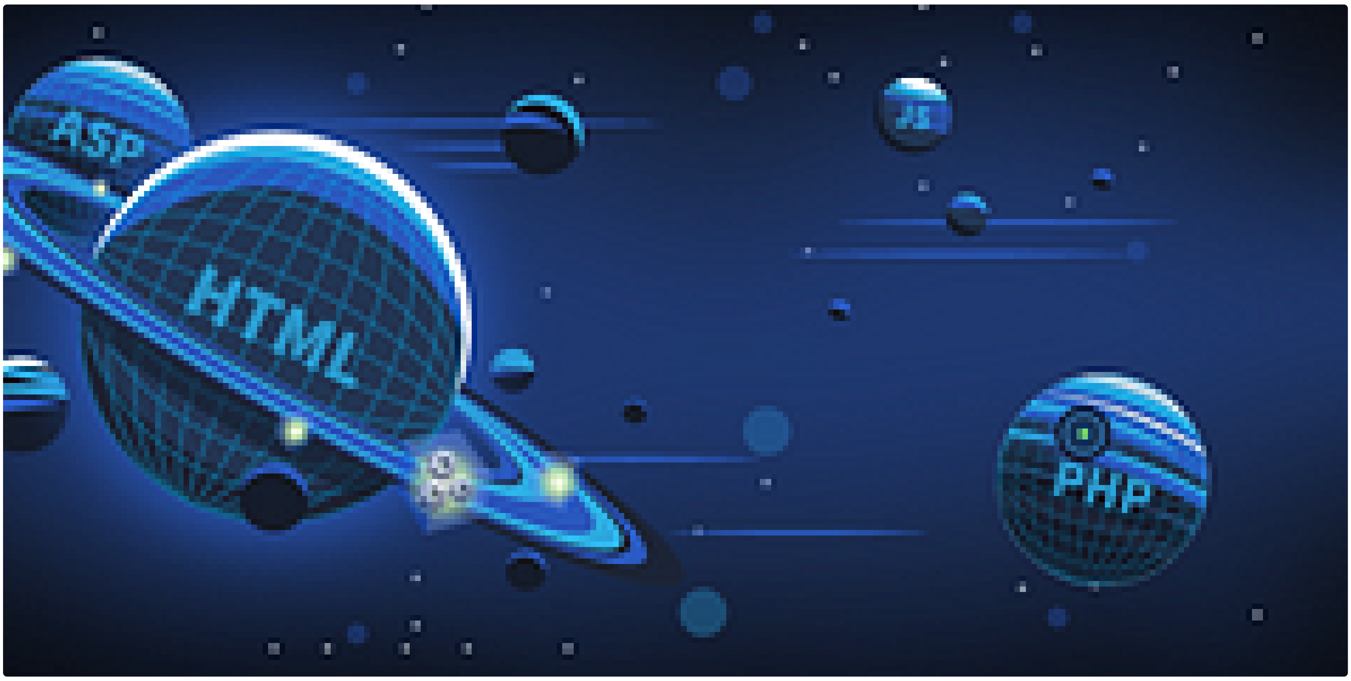
1884 stories · 1529 saves

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

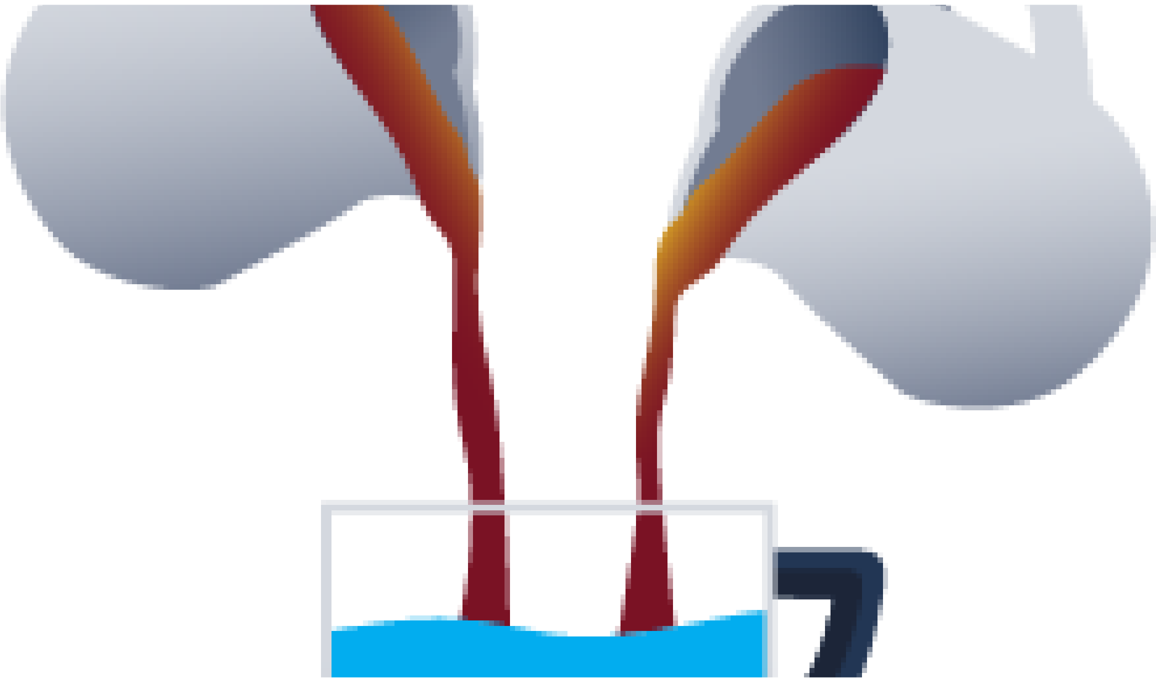
Oct 26, 2024 56

Fritzadriano

Retracted — TryHackMe WriteUp

IInvestigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

Sep 4, 2024 50



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

See more recommendations