Windows Forensics 2

Task 2 The FAT file systems

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

What is the maximum file size supported by the FAT32 file system? (In GB)

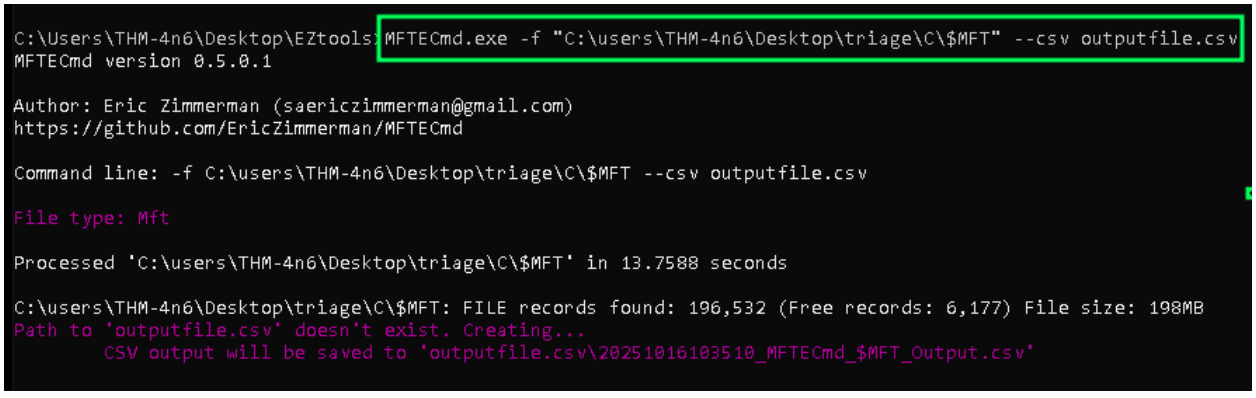
4

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

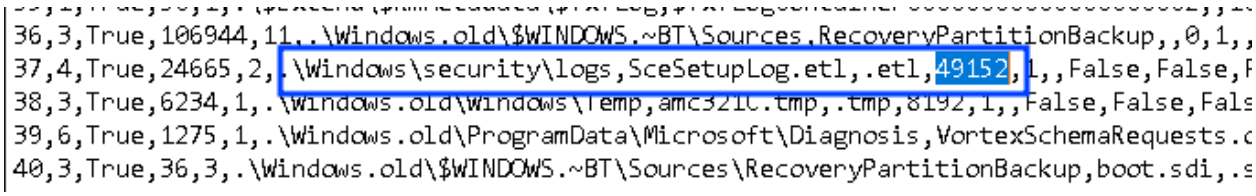
Task 3 The NTFS File System

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`

Run the command prompt as administrator move to folder C:\Users\THM-4n6\Desktop\Eztools
Run the command MFTECmd.exe -f "C:\users\THM-4n6\Desktop\triage\C\$MFT" --csv outputfile.csv



Open the file in notepad , search for the file SceSetupLog.etl



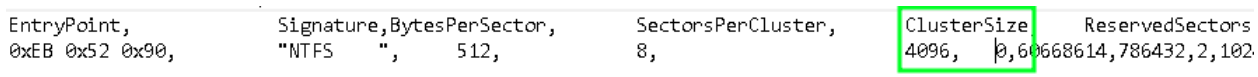
49152

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

Now use the $Boot file

MFTECmd.exe -f "C:\users\THM-4n6\Desktop\triage\C\$Boot" --csv output2.csv

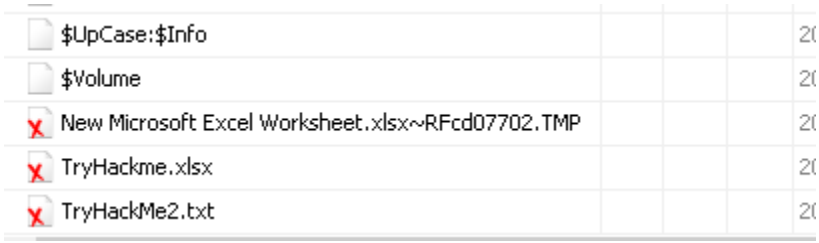
After that open the file



4096

Task 4 Recovering deleted files

There is another xlsx file that was deleted. What is the full name of that file?
Open the file in the autopsy



TryHackme.xlsx

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

TryHackMe2.txt

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

Right click on the file TryHackMe2.txt -> extract -> select the location where to save the file -> open the recovered file

THM-4n6-2-4

Task 5Evidence of Execution

How many times was gkape.exe executed?
Run the command prompt as administrator and go to the directory
C:\Users\THM-4n6\Desktop\EZtools
Execute the PECmd.exe on the file
C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch\GKAPE.EXE-E935EF56.pf

PECmd.exe -f "C:\Users\THM-4n6\Desktop\triage\C\Windows\prefetch\GKAPE.EXE-E935EF56.pf" --csv GKAPE
It will create a files in the dir GKAPE , open the timeline file , two entries were present

```
RunTime,ExecutableName
2021-12-01 13:04:49,\VOLUME{01d7e1a9a74620d0-50a75245}\USERS\THM-4N6\DESKTOP\KAPE\GKAPE.EXE
2021-12-01 13:04:04,\VOLUME{01d7e1a9a74620d0-50a75245}\USERS\THM-4N6\DESKTOP\KAPE\GKAPE.EXE
```

2

What is the last execution time of gkape.exe

2021-12-01 13:04:49 but changer the format according to the question 12/01/2021 13:04

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

Use the file C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Local\ConnectedDevicesPlatform\L.THM-4n6\ActivitiesCache.db and tool WxTCmd.exe

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

After that open the file , search for the time given in the question in the same row after the start time end time is there then the duration is present

```
,,2021-11-30 10:56:19,2021-11-30 10:57:00,00:00:41,2021-11-30 :
```

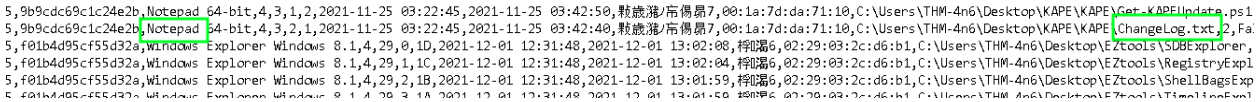
00:00:41

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

Now we are using the tool JLECmd.exe on the folder C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

JLECmd.exe -d "C:\Users\THM-4n6\Desktop\triage\C\Users\THM-4n6\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations" --csv JLECMD

Open the extracted file , search for ChangeLog.txt



notepad.exe

Task 6 File/folder knowledge

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

Open the lastly extracted file in EZViewer search for the regripper

EntryNum	CreationTime	LastModified	MacAddre	Path	I
3	11/30/2021 10:43	11/30/2021 10:56	02:0b:fc:70	C:\Program Files\Amazon\Ec2ConfigService\Settings\WallpaperSet	
1		11/25/2021 4:01		::{26EE0668-A00A-44D7-9371-BEB064C98683}\5\::{BB06C0E4-D293-4F	
3	11/30/2021 10:43	11/30/2021 10:56	02:0b:fc:70	C:\Program Files\Amazon\Ec2ConfigService\Settings\WallpaperSet	
2	11/25/2021 3:22	11/25/2021 3:42	00:1a:7d:d	C:\Users\THM-4n6\Desktop\KAPE\KAPE\Get-KAPEUpdate.ps1	
1	11/25/2021 3:22	11/25/2021 3:42	00:1a:7d:d	C:\Users\THM-4n6\Desktop\KAPE\KAPE\ChangeLog.txt	
1D	12/1/2021 12:31	12/1/2021 13:02	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\SDBExplorer	
1C	12/1/2021 12:31	12/1/2021 13:02	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\RegistryExplorer	
1B	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\ShellBagsExplorer	
1A	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\TimelineExplorer	
19	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\iisGeolocate	
18	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\EvtxExplorer	
17	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\MFTExplorer	
16	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\SQLECmd	
F	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools	
15	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\JumpListExplorer	
14	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\EZtools\Hasher	
13	12/1/2021 12:31	12/1/2021 13:01	02:29:03:2(	C:\Users\THM-4n6\Desktop\regripper	
1	11/25/2021 3:12	12/1/2021 13:01	00:1a:7d:d	knownfolder:{754AC886-DF64-4CBA-86B5-F7FBF4FBCEF5} ==> ThisP(	
12		12/1/2021 13:01		\\tsclient\D	

12/1/2021 13:01

When was the above-mentioned folder first opened?

12/1/2021 12:31

Task 7 External Devices/USB device forensics

Which artifact will tell us the first and last connection times of a removable drive?
Setupapi.dev.log