AfricanFalls (Cyberdefenders)

Background: John Doe was accused of doing illegal activities. A disk image of his laptop was taken. Your task is analyzing the image and understanding what happened under the hood.

SHA1SUM	475b5c8c679ef034541edbd761faad5b5441656e	Tools that can be used
Published	June 15, 2021	• FTK Imager • Autopsy • rifiuti2 • Browsing History View • WinPrefetchView • ShellBagsExplorer • mimikatz • Metdata Extractor • Online Hash Crack • NTLM Hash
Author	DFIRScience	
Size	672 MB	

Link: https://cyberdefenders.org/blueteam-ctf-challenges/66

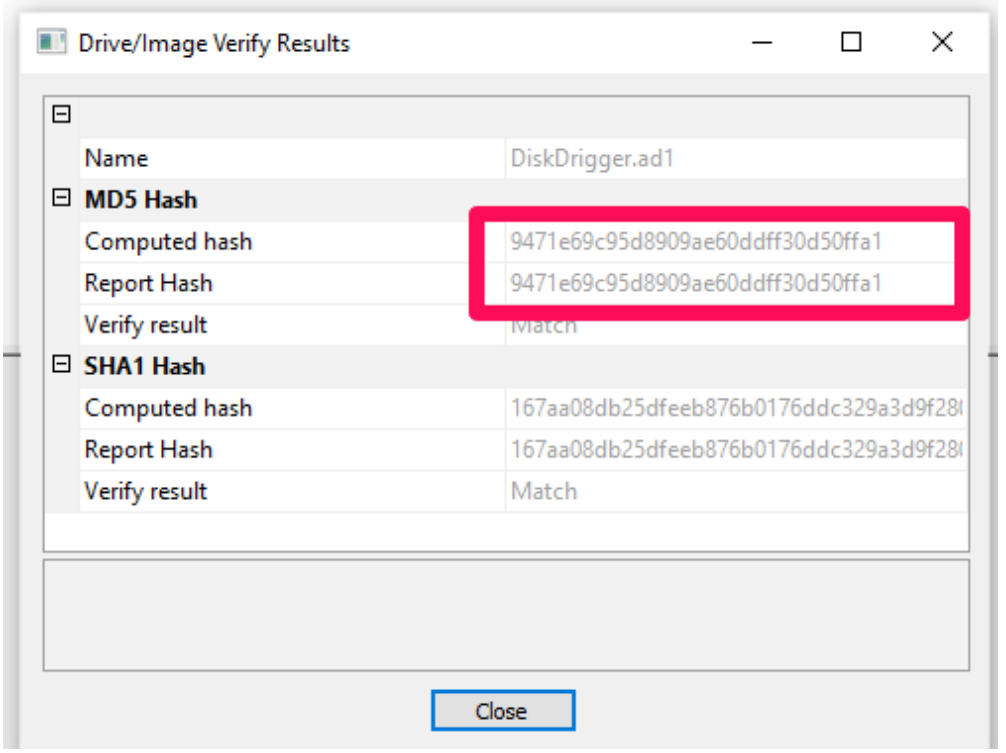
Tools used

- FTK imager
- Autopsy
- PEcmd.exe

Question

#1 What is the MD5 hash value of the suspect disk? Answer: (9471e69c95d8909ae60ddff30d50ffa1)

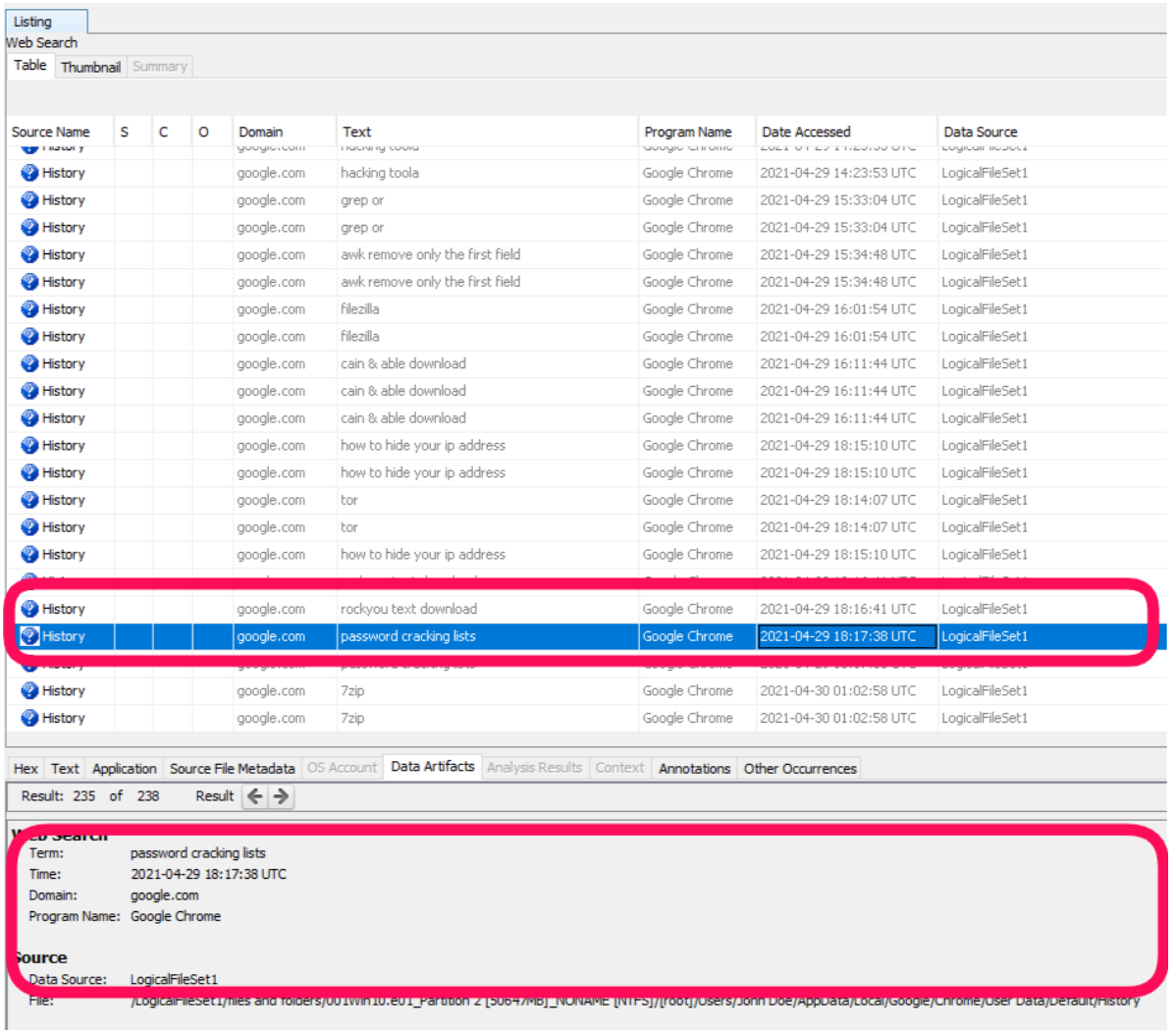
Go to FTK imager and click on the select source select the image file, go to the source location and attach the image file. Then right-click on the attached file and click on verify the Drive/Image. you will get the hash of the attached file.



#2 What phrase did the suspect search for on 2021-04-29 18:17:38 UTC? (three words, two spaces in between) Answer: (password cracking lists)

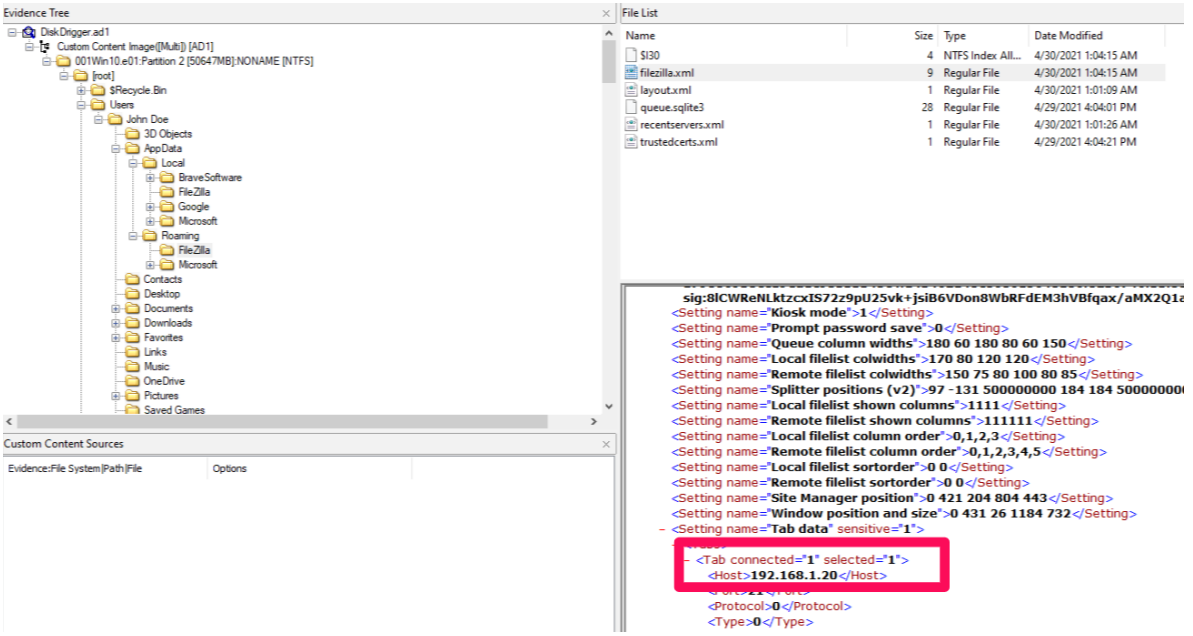
As I prefer using Autopsy to dig deep. I extracted all the files and folders from the image using an FTK imager and added these extracted files and folders as the data source for the autopsy.

I changed the timezone to UTC and checked the Web search using the provided time frame .



#3 What is the IPv4 address of the FTP server the suspect connected to? Answer: (192.168.1.20) (check in the set-up config file of that particular application)

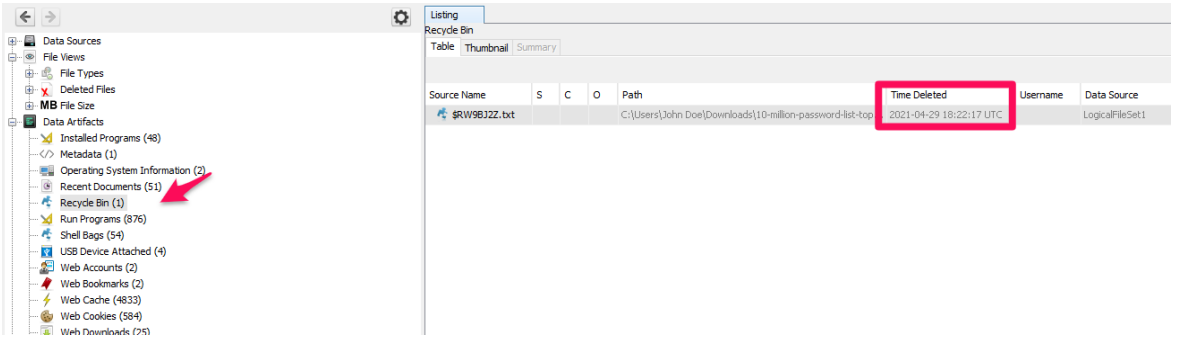
To host an FTP server you need to configure the server on the device. There should be a configuration file for that. Usually, configuration files are present in users/appdata/roaming.



#4 What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)

Answer: (2021-04-29 18:22:17 UTC)

To identify the date and time of the password list am using Autopsy for quicker analysis. There is a Data Artifact name Recycle Bin in the Autopsy where the deleted file's date and time are shown.



#5 How many times was Tor Browser ran on the suspect's computer? (number only)

Answer: (0)

To identify how many times the browser is ran on the device, I check Prefetch files. I Prefer using PECmd.exe to extract the prefetch files in CSV format.

Prefetch files are located at C:Windows\Prefetch.

we can observe the output of the prefetch TORBROWSER output where the RUNCount is 1, but we can observe there are no date/time entry in PreviousRun0. Therefore I can say that this application was only installed but never ran on the device.

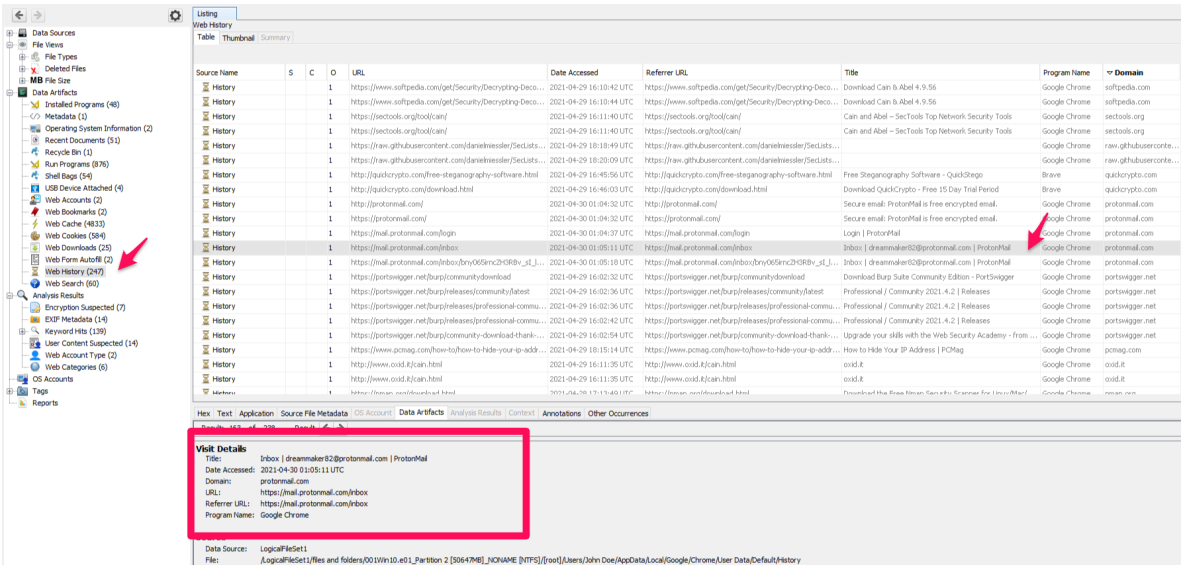
```
D:\Tools for forensic>PECmd.exe -d "D:\CTFs big game\ctf details\Windows\Prefetch" --csv "D:\CTFs big game\ctf details\Windows"
```

SourceFilename	ExecutableName	Hash	Size	Version	RunCount	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4	PreviousRun5	PreviousRun6	Volume0Name	Volume0Serial	Volume0Created	Volume1Name	Volume1Serial	Volume1Created

ParsingError
D:\CTFs big game\ctf details\Windows\Pref-

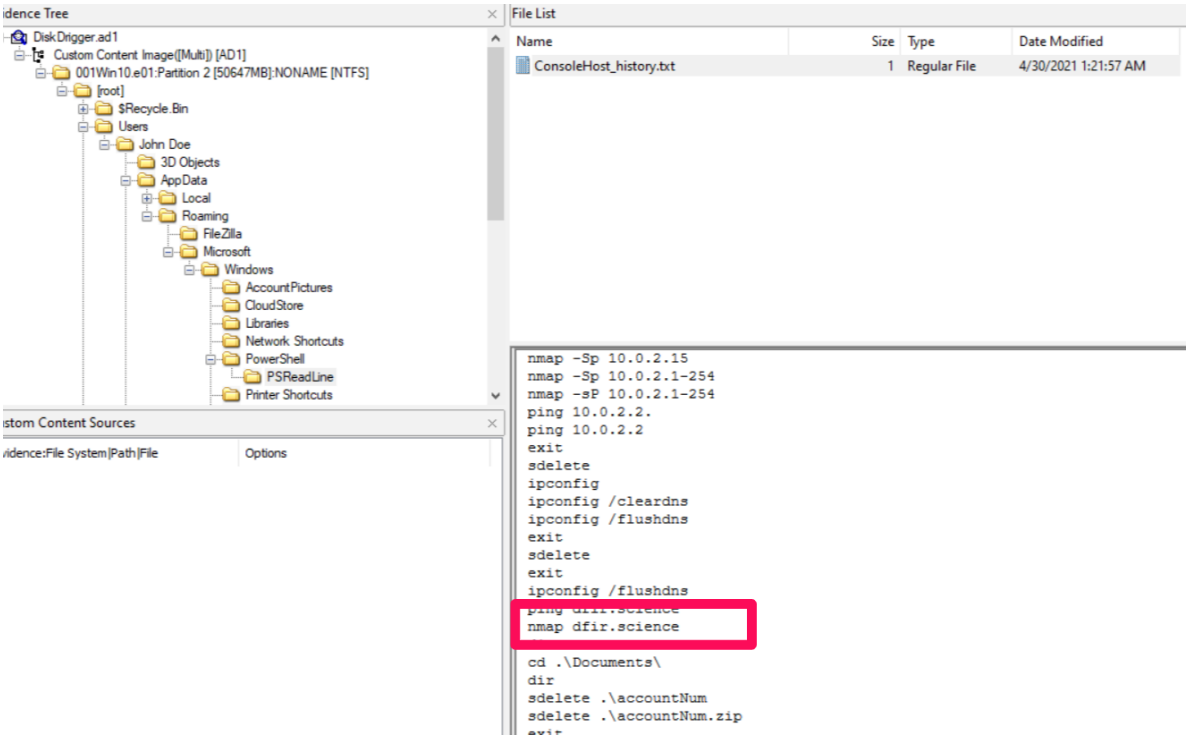
etch \TORBROWSER-INSTALL-WIN64-10.0-F3C4DF19.	TORBROWSER-INSTALL-WIN64-10.0	F3C4DF19	139504	Windows10orWindows11	1	2021-04-29 18:22:32								\VOLUME{01d73a10b8b64f80-92b8d553}	92B8D553	2021-04-25 20:22:32					

#6 What is the suspect's email address? Answer: (dreammaker82@protonmail.com)
Using Autopsy checked Web History, filter domain you can identify the email address in the bottom box in view details.



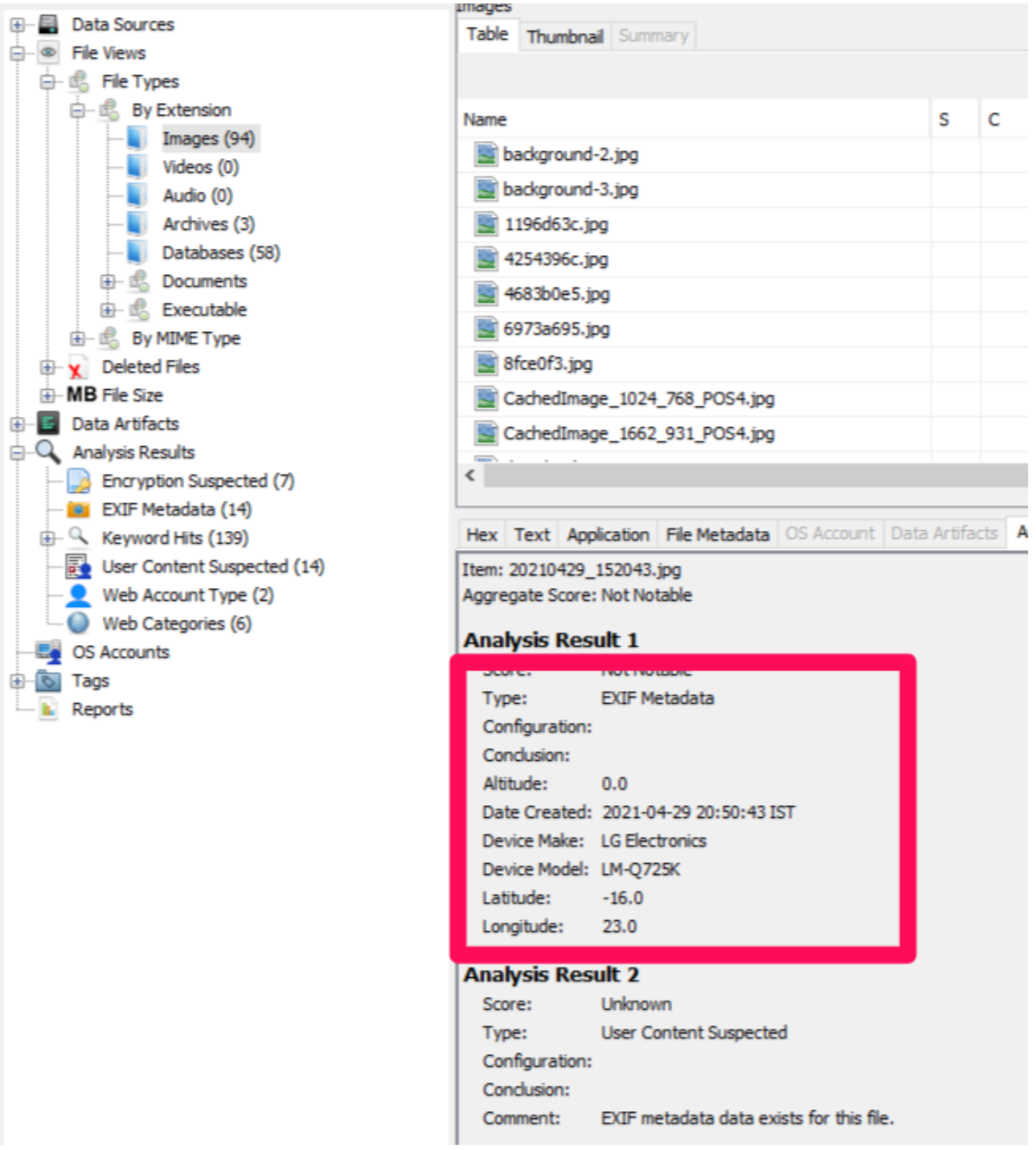
#7 What is the FQDN did the suspect port scan? Answer: (dfir.science)
The suspect port scan could have run a cmd in PowerShell. I am about to check the PowerShell Console history. The location of the console history file is

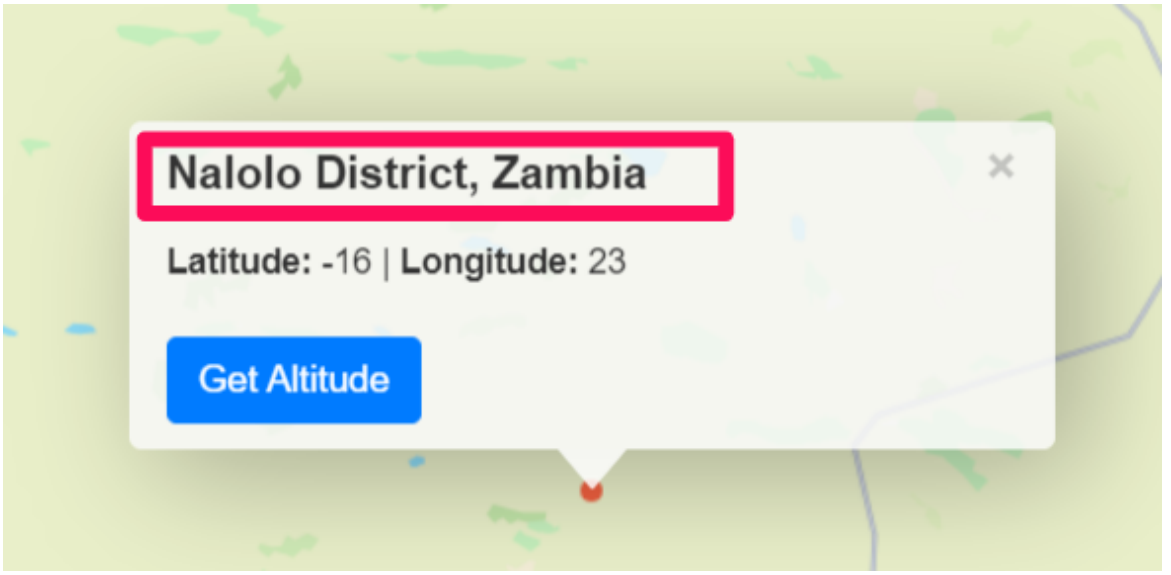
(user/appdata/roaming/microsoft/windows/powershell/PSReadLine/ConsoleHost_history.txt)



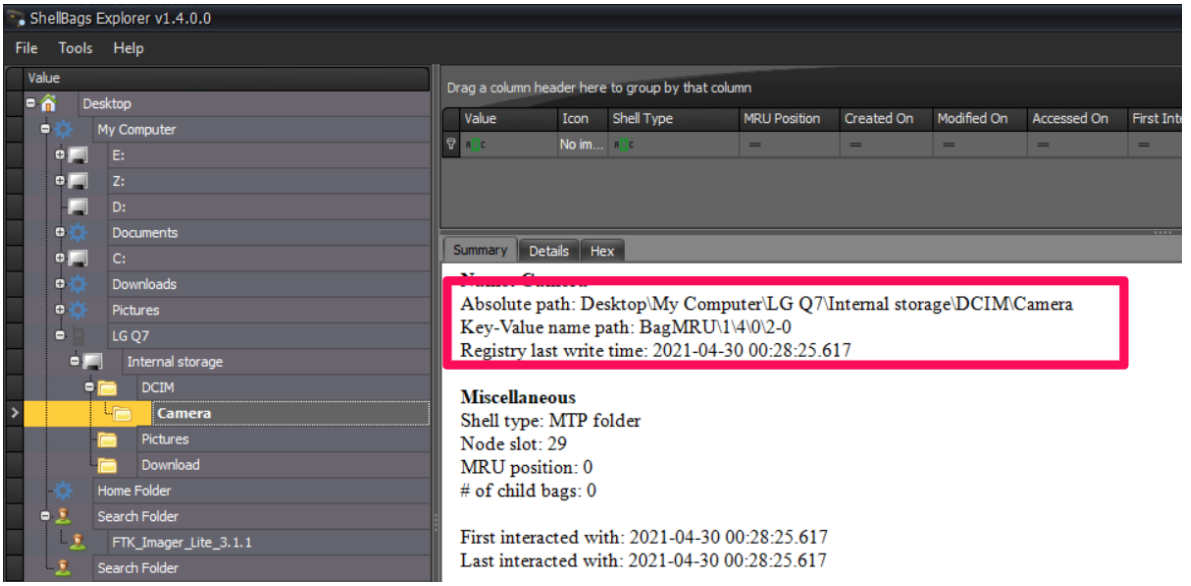
#8 What country was picture "20210429_152043.jpg" allegedly taken in? Answer: (Zambia)

(https://www.gps-coordinates.net/)



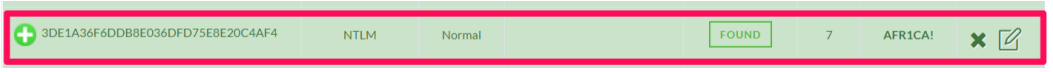


#9 What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop? Answer: (Camera)
To get details about the 20210429_151535.jpg picture, we need to check the shell bags .
shellbags are located in c:Users/App Data/Windows/ UsrClass.dat



#10 A Windows password hashes for an account are below. What is the user's password? (AFR1CA!)

Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::



#11 What is the user "John Doe's" Windows login password?

I tried to pull NTLM hash using samdump2 but I was getting invalid hash.