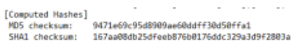
AfricanFalls Challenge

John Doe was accused of doing illegal activities. A disk image of his laptop was taken. Your task as a soc analyst is to analyze the image and understand what happened under the hood.

Task 1:
What is the MD5 hash value of the suspect disk?

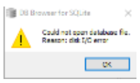
I checked the DiskDrigger.ad1.txt file



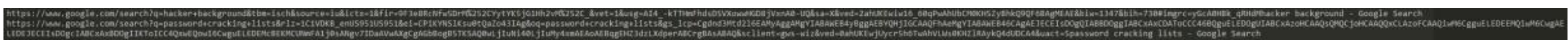
Answer: 9471e69c95d8909ae60ddff30d50ffa1

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

First I thought about going to the Registry keys like TypedPaths and WordWheelQuery but no there is no NTUSER.DAT in the user files.
Then I tried to check the History of the Chrome browser with SQL DB Browser but it didn't worked



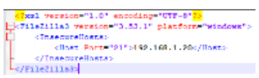
So I used Strings on the History and analyzed it until I found some search which was look like the answer format



Answer: password cracking lists
(After checking the hint, the History file should work with DB SQL Browser)

Task 3:
What is the IPv4 address of the FTP server the suspect connected to?

I checked the trustedcerts.xml inside the FileZilla folder and noticed the port21 with an IP

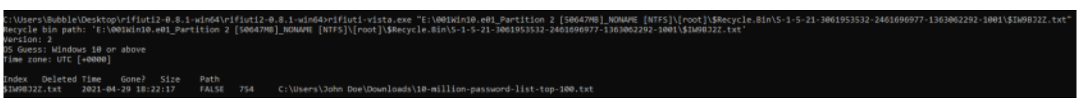


Answer: 192.168.1.20

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

First I tried to find the USN Journal which shows such things but this artifact is not in the image so I checked the recommended tools for this challenge and saw the "rifiuti2" which is forensic tool used to analyze the Recycle Bin on Windows systems.

I asked the ChatGPT how to work with this tool.
I used the command - "rifiuti-vista.exe "E:\001Win10.e01_Partition 2 [50647MB]_NONAME [NTFS]\[root]\$Recycle.Bin\S-1-5-21-3061953532-2461696977-1363062292-1001\$IW9BJ2Z.txt"

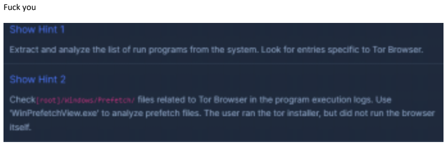


Answer: 2021-04-29 18:22:17 UTC

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

I tried to check in Prefetch and didn't find anything besides the installer
After some time I checked the hint and they said there not execution of Tor browser

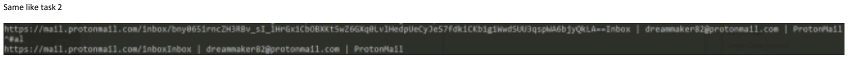
Fuck you



Answer : 0

Task 6:
What is the suspect's email address?

Same like task 2



Answer: dreammaker82@protonmail.com

Task 7:
What is the FQDN did the suspect port scan?

I checked the PSReadLine

```
bettercap
bettercap --check-updates
bettercap -S
bettercap -X --no-spoofing
bettercap -version
bettercap -eval "caplets.update; ui.update; q"
bettercap -caplet http-ui
ipconfig
nmap -Sp 10.0.2.15
nmap -Sp 10.0.2.1-254
nmap -sP 10.0.2.1-254
ping 10.0.2.2.
ping 10.0.2.2
exit
sdelete
ipconfig
ipconfig /cleardns
ipconfig /flushdns
exit
sdelete
exit
ipconfig /flushdns
ping dfir.science
nmap dfir.science
dir
cd .\Documents\
dir
sdelete .\accountNum
sdelete .\accountNum.zip
exit
cd E:\FTK_Imager_Lite_3.1.1
& '.\FTK Imager.exe'
exit
```

Answer: dfir.science

Task 8:
What country was picture "20210429_152043.jpg" allegedly taken in?

I used the website https://exif.tools/ which can be also used in Kali by the command: exiftool "filepath"

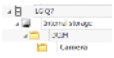
Create Date	2021:04:29 15:20:43.367153
Date/Time Original	2021:04:29 15:20:43.367153
Modify Date	2021:04:29 15:33:32.367153
Thumbnail Image	(Binary data 9000 bytes, use -b option to extract)
GPS Latitude	16° 0' 0.00" S
GPS Longitude	23° 0' 0.00" E
Focal Length	3.7 mm
GPS Position	16° 0' 0.00" S, 23° 0' 0.00" E

I copied everything from Create Date to GPS Position and asked the ChatGPT and asked them where is the location

Answer: Zambia

Task 9:
What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?

I checked the ShellBags first with Registry Explorer but I didn't find anything.
Then I opened the UsrClass.dat with ShellBags Explorer and I assumed the picture as come from LG Q7 - DCIM -Camera



Answer: Camera

Task 10:
A Windows password hashes for an account are below. What is the user's password?
Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::

I used https://hashes.com/en/decrypt/hash and pasted the NTLM hash 3DE1A36F6DDB8E036DFD75E8E20C4AF4

Answer: AFR1CA!

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

I used Mimikatz on the SYSTEM and SAM Hives

sekurlsa::logonPasswords

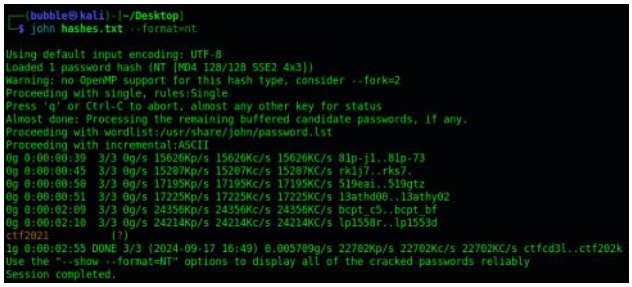
token::elevate

lsadump::sam /system:"E:\001Win10.e01_Partition 2 [50647MB]_NONAME [NTFS]\[root]\Windows\System32\config\SYSTEM" /sam:"E:\001Win10.e01_Partition 2 [50647MB]_NONAME [NTFS]\[root]\Windows\System32\config\SAM"

NTLM hash - ecf53750b76cc9a62057ca85ff4c850e

Then I used John The Ripper to crack the NTLM

john hashes.txt --format=nt



Answer: ctf2021