

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

```
[Computed Hashes]
MD5 checksum: 9471e69c95d8909ae60ddff30d50ffa1
SHA1 checksum: 167aa08db25df0eb876b0176ddc329a3d9f2803a
```

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.



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

https://www.google.com/search?q=hackerbackground&ibis=ch&source=1&icsts=1&lr=93388787650H5W52CZY1EYK5G3H2V52C_&ret=1&uq=a14_ktthwHd50XxwKd3VnAe-3Q4a-X4vD-ZahKt4w16_68pH4MhDCKN5Y2YhKQ0068AgMA&ibi=11478bH-730HnrcyYcG4MhD_ghnHacker+background+-+Google+Search

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

```
<?xml version="1.0" encoding="UTF-8">
<FileZilla>
  <version>"0.53.1" platform="windows">
    <InsecureHosts>
      <Host Parm="01">149.168.1.20</Host>
    </InsecureHosts>
  </FileZilla>
</?xml>
```

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 "rifiut2" 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 - "rifuti-vista.exe "E:\001Win10.e01_Partition 2 [50647MB]_NONAME [NTFS]\root\\$\Recycle.Bin\S-1-5-21-3061953532-2461696977-1363062292-1001\SIW98J2Z.txt"

[illegible]

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

Show Hint 1

Extract and analyze the list of run programs from the system. Look for entries specific to Tor Browser.

Show Hint 2

Check `root\winlogs\prefetch` files related to Tor Browser in the program execution logs. Use `WinPrefetchView.exe` to analyze prefetch files. The user ran the Tor installer, but did not run the browser itself.

Answer : 0

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

Same like task 2

https://mail.protonmail.com/inbox/bny65frcz38Bv_sl_lHwGx1Cb0Bxt5wZ6Gx8lVedpUcy3e57f4k1Cb1gWd3SU3qspMA6bjyQkLA==Inbox | dreammaker8@protonmail.com | ProtonMail

Answer: dreammaker82@protonmail.com

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

I checked the PSReadLine

```
bettercap --check-updates
bettercap -S
bettercap -X --no-spoofing
bettercap --status
bettercap -eval '*caplets.updater: ui.updater: q*'
bettercap --caplet http-s1
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
delete
ipconfig
ipconfig /renew
ipconfig /flushdns
exit
delete
exit
ipconfig /flushdns
ping dfir.science
nmap dfir.science
dir
cd .\Documents\
dir
delete .\account@um
delete .\account@um.rsp
exit
cd K:\FTK Imager Lite_3.1.1
s *.\\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

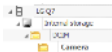
Answer: Zambia

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 UserClass.dat with ShellBags Explorer and I assumed the picture as come from LG Q7 - DCIM - Camera



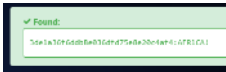
Answer: Camera

Task 10:

A Windows password hashes for an account are below. What is the user's password?

Anon:1001aad3b435d51404eeadd3b43b51404ee:3DE1A36FD08B036DFD75EB20C4AF4:::

I used <https://hashes.com/en/decrypt/hash> and pasted the NTLM hash
3DE1A36FD08B036DFD75EB20C4AF4



Answer: AFRICA!

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.x01_Partition 2 [50647MB]_NONAME [NTFS]\(root)\Windows\System32\config\SYSTEM" /sam:"E:\001Win10.x01_Partition 2 [50647MB]_NONAME [NTFS]\(root)\Windows\System32\config\SAM"

```
NTLMDump (1001)
User : John Doe
Hash NTLM: ecf53750b76cc9a62057ca85ff4c850e

Supplemental Credentials:
* Primary:NTLH-Strong-NTLM *
  Random Value : 7844854d845112afaa30823b3ffcedfc

* Primary:Kerberos-Newer-Keys *
  Default Salt : DESKTOP-03358C23John Doe
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : f81bc409150d41445b:28dc002eb8dffe695e23c13d4070a94c62fc3249da4ad
    aes128_hmac (4096) : b88a45d7cb7af324781526956391875
    des_cbc_md5 (4096) : b3d691e6dc7a9e73
  Oldest Credentials
    aes256_hmac (4096) : f81bc409150d41445b:28dc002eb8dffe695e23c13d4070a94c62fc3249da4ad
    aes128_hmac (4096) : b88a45d7cb7af324781526956391875
    des_cbc_md5 (4096) : b3d691e6dc7a9e73

* Packages *
  NTLH-Strong-NTLM

* Primary:Kerberos *
  Default Salt : DESKTOP-03358C23John Doe
  Credentials
    des_cbc_md5 : b3d691e6dc7a9e73
  Oldest Credentials
    des_cbc_md5 : b3d691e6dc7a9e73
```

NTLM hash - ecf53750b76cc9a62057ca85ff4c850e

Then I used John The Ripper to crack the NTLM

john hashes.txt --format=nt

```

(bobbie@kali) ~/Desktop
$ john hashes.txt --format=nt

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:00:39 3/3 0g/s 15626Kp/s 15626Kc/s 8lp-jl..8lp-73
0g 0:00:00:45 3/3 0g/s 15287Kp/s 15287Kc/s 15287Kc/s rk1j7..rks7.
0g 0:00:00:50 3/3 0g/s 17195Kp/s 17195Kc/s 17195Kc/s 519eai..519gtz
0g 0:00:00:51 3/3 0g/s 17225Kp/s 17225Kc/s 17225Kc/s 13athd00..13athy02
0g 0:00:02:09 3/3 0g/s 24356Kp/s 24356Kc/s 24356Kc/s bcpt_c5..bcpt_bf
0g 0:00:02:10 3/3 0g/s 24214Kp/s 24214Kc/s 24214Kc/s lp1558r..lp1553d
ctf2021 (?)
1g 0:00:02:55 DONE 3/3 (2024-09-17 16:49) 0.005709g/s 22762Kp/s 22762Kc/s 22762Kc/s ctfcd3l..ctf202k
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

```

Answer: ctf2021