AfricanFalls Lab (Cyber Defenders) - Walkthrough

Monday, September 16, 2024 1:16 PM

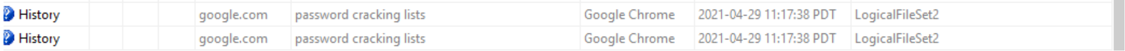
Story:
John Doe was accused of doing illegal activities. A disk image of his laptop was taken. Your task as a soc analyst is to analyze the image and understand what happened under the hood.

Q1: What is the MD5 hash value of the suspect disk?

- The MD5 hash is written in the TXT file you received along with the disk image.

Q2:What phrase did the suspect search for on 2021-04-29 18:17:38 UTC? (three words, two spaces in between)

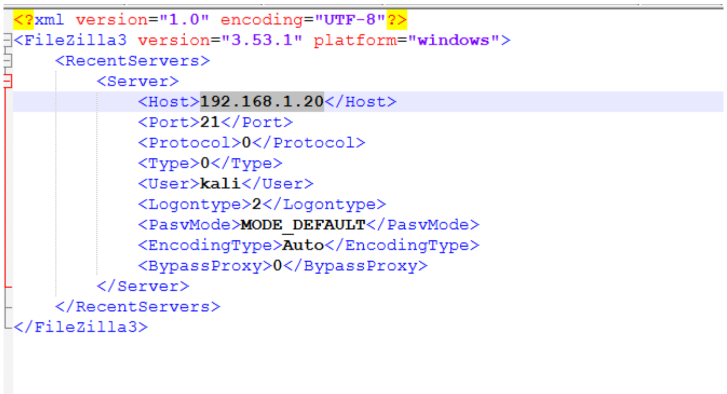
- To address this question, I parsed the data using 'Autopsy' and navigated to the 'Web Search' section. During the specified timeframe, I found the phrase 'Password Cracking Lists.'



History				google.com	password cracking lists	Google Chrome	2021-04-29 11:17:38 PDT	LogicalFileSet2
History				google.com	password cracking lists	Google Chrome	2021-04-29 11:17:38 PDT	LogicalFileSet2

Q3: What is the IPv4 address of the FTP server the suspect connected to?

- I accessed the FileZilla directory in AppData at 'C:\Users\John Doe\AppData\Roaming\FileZilla' and found the file 'RecentServers.xml', which contains the recently logged-in server.



```
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.53.1" platform="windows">
    <RecentServers>
        <Server>
            <Host>192.168.1.20</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>kali</User>
            <Logontype>2</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
        </Server>
    </RecentServers>
</FileZilla3>
```

Q4: What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)

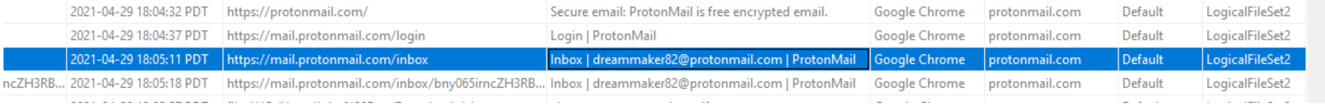
- To address this question, I parsed the data using 'Autopsy' and navigated to the 'Recycle Bin' section.
  I found that the list was deleted on '2021-04-29 11:22:17 PDT', which converts to '2021-04-29 18:22:17 UTC'.

Q5:How many times was Tor Browser ran on the suspect's computer? (number only)

- I accessed to the 'Shell Bags' artifacts via Autopsy, Shellbags are artifacts that are created when a user interacts with the shell.
  I don't see any indication of an execution of 'TOR', which indicates the answer is **0.**

Q6: What is the suspect's email address?

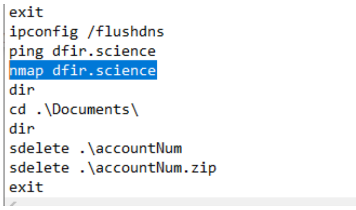
- When I navigated in the 'Web History' section I found the inbox of the user 'dreammaker82 @protonmail.com'



	2021-04-29 18:04:32 PDT	https://protonmail.com/	Secure email: ProtonMail is free encrypted email.	Google Chrome	protonmail.com	Default	LogicalFileSet2
	2021-04-29 18:04:37 PDT	https://mail.protonmail.com/login	Login | ProtonMail	Google Chrome	protonmail.com	Default	LogicalFileSet2
	2021-04-29 18:05:11 PDT	https://mail.protonmail.com/inbox	Inbox | dreammaker82@protonmail.com | ProtonMail	Google Chrome	protonmail.com	Default	LogicalFileSet2
ncZH3RB...	2021-04-29 18:05:18 PDT	https://mail.protonmail.com/inbox/bny065irncZH3RB...	Inbox | dreammaker82@protonmail.com | ProtonMail	Google Chrome	protonmail.com	Default	LogicalFileSet2

Q7:What is the FQDN did the suspect port scan?

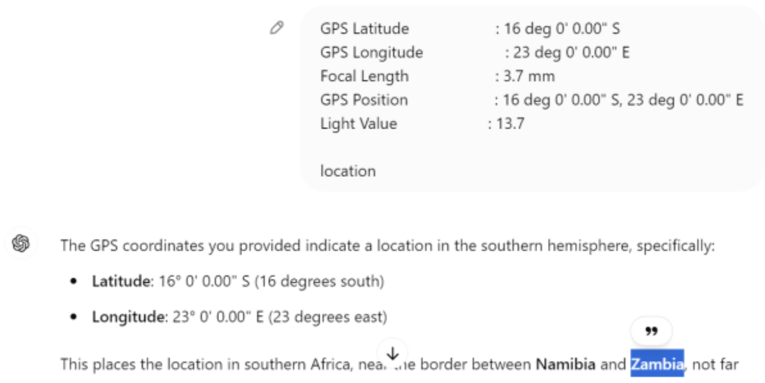
- During the investigation, I noticed the user downloaded 'Nmap' for Windows.
  To address the question, I checked the PowerShell history file which located at C:\Users\John Doe \AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine



```
exit
ipconfig /flushdns
ping dfir.science
nmap dfir.science
dir
cd .\Documents\
dir
sdelete .\accountNum
sdelete .\accountNum.zip
exit
```

Q8:What country was picture "20210429_152043.jpg" allegedly taken in?

- I searched the disk image for the photo by name, and after locating it, I used 'Exiftool' to examine the file's metadata.
   The metadata revealed the GPS coordinates of the image, which I then entered into ChatGPT to obtain the location."



```
GPS Latitude                : 16 deg 0' 0.00" S
GPS Longitude                 : 23 deg 0' 0.00" E
Focal Length                : 3.7 mm
GPS Position                : 16 deg 0' 0.00" S, 23 deg 0' 0.00" E
Light Value                : 13.7

location
```

The GPS coordinates you provided indicate a location in the southern hemisphere, specifically:

- **Latitude**: 16° 0' 0.00" S (16 degrees south)
- **Longitude**: 23° 0' 0.00" E (23 degrees east)

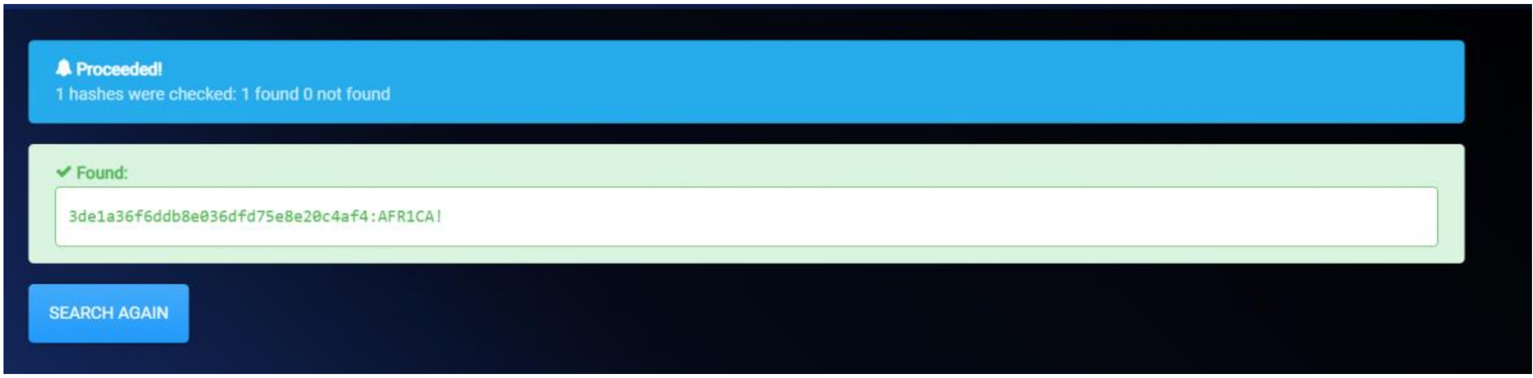
This places the location in southern Africa, near the border between **Namibia** and **Zambia**, not far

Q9:What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?

- We examined the ShellBags artifacts using ShellBagsExplorer.
  After uploading all the Usrdat.dat HIVE files to the tool, I identified a USB connection labeled 'LG Q7,' which is likely a phone.
  I then checked the suspect's documents and found a directory named **'Camera'.**

Q10: A Windows password hashes for an account are below. What is the user's password?
Anon:1001:aad3b435b51404eeaad3b435b51404ee:3DE1A36F6DDB8E036DFD75E8E20C4AF4:::

- To address this question, I took the NTLM hash (3DE1A36F6DDB8E036DFD75E8E20C4AF4) and searched it via Hashes.com and found the password.



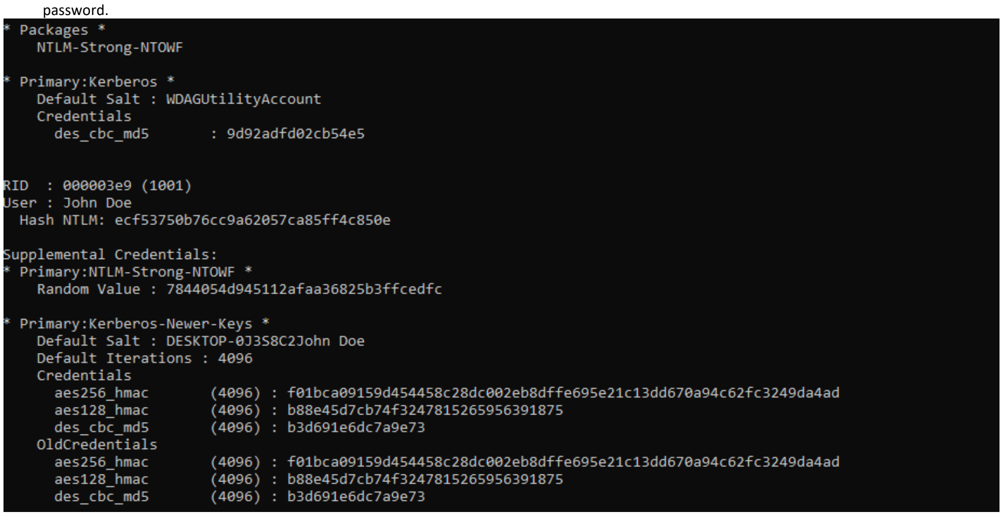
Proceeded!
1 hashes were checked: 1 found 0 not found

✔ Found:

```
3de1a36f6ddb8e036dfd75e8e20c4af4:AFR1CA!
```

Q11: What is the user "John Doe's" Windows login password?

- I used 'Mimikatz.exe' to extract the NTLM hash of the user and used 'Hashes.com' to decrypt the password.



```
* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 9d92adfd02cb54e5


RID  : 000003e9 (1001)
User : John Doe
  Hash NTLM: ecf53750b76cc9a62057ca85ff4c850e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 7844054d945112afaa36825b3ffcedfc

* Primary:Kerberos-Newer-Keys *
    Default Salt : DESKTOP-0J3S8C2John Doe
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : f01bca09159d454458c28dc002eb8dffe695e21c13dd670a94c62fc3249da4ad
      aes128_hmac       (4096) : b88e45d7cb74f3247815265956391875
      des_cbc_md5       (4096) : b3d691e6dc7a9e73
    OldCredentials
      aes256_hmac       (4096) : f01bca09159d454458c28dc002eb8dffe695e21c13dd670a94c62fc3249da4ad
      aes128_hmac       (4096) : b88e45d7cb74f3247815265956391875
      des_cbc_md5       (4096) : b3d691e6dc7a9e73
```