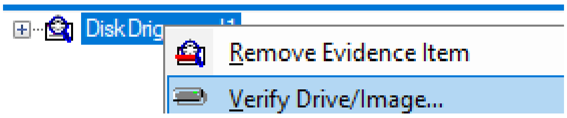
CyberDefenders: AfricanFalls Lab

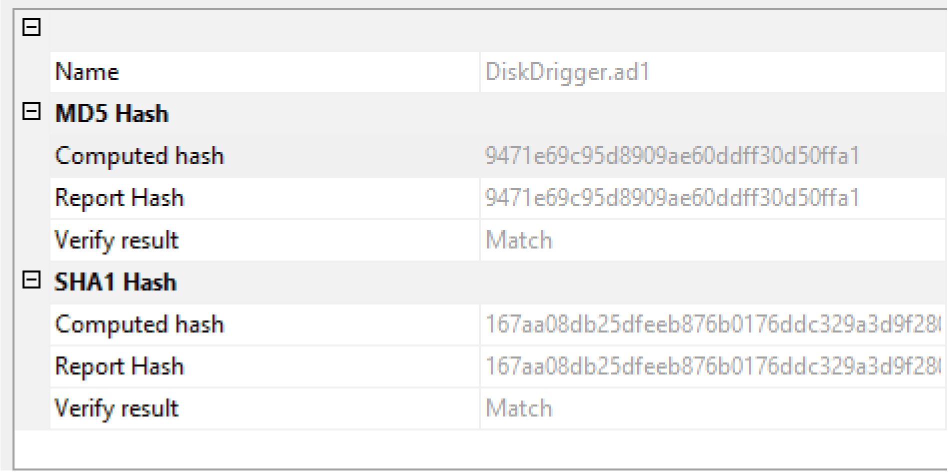
The following writeup is for AfricanFalls Lab on CyberDefenders, it involves investigating a disk image from a suspect's laptop using a series of tools, including FTK Imager, rifiuti2, BrowserHistoryView, PECmd, ShellBags Explorer, and more.

Scenario: 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.

What is the MD5 hash value of the suspect disk?

We can easily generate the MD5 hash of the disk image by loading it into FTK Imager, right-clicking the disk image and selecting Verify Drive/Image:



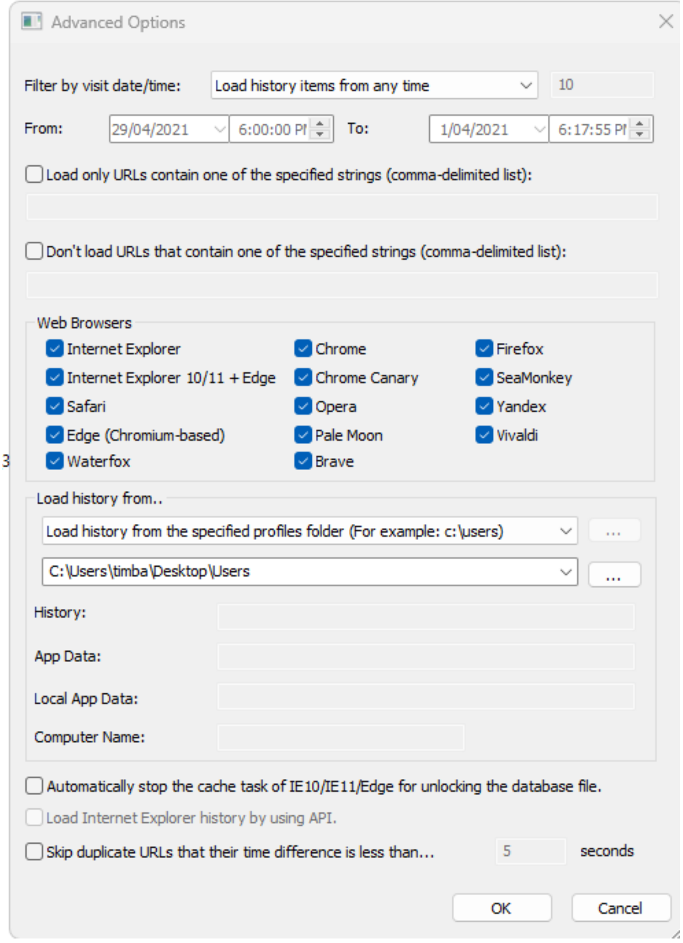


Name	DiskDrigger.ad1
MD5 Hash	
Computed hash	9471e69c95d8909ae60ddff30d50ffa1
Report Hash	9471e69c95d8909ae60ddff30d50ffa1
Verify result	Match
SHA1 Hash	
Computed hash	167aa08db25dfeeb876b0176ddc329a3d9f28
Report Hash	167aa08db25dfeeb876b0176ddc329a3d9f28
Verify result	Match

Answer: 9471e69c95d8909ae60ddff30d50ffa1

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

Due to the wording of the question, I'm assuming this is asking what the suspected searched for using a browser. To find this, we can dump the Users directory and use BrowserHistoryView:



Filter by visit date/time: Load history items from any time 10

From: 29/04/2021 6:00:00 PM To: 1/04/2021 6:17:55 PM

☐ Load only URLs contain one of the specified strings (comma-delimited list):

☐ Don't load URLs that contain one of the specified strings (comma-delimited list):

Web Browsers

☑ Internet Explorer ☑ Chrome ☑ Firefox
☑ Internet Explorer 10/11 + Edge ☑ Chrome Canary ☑ SeaMonkey
☑ Safari ☑ Opera ☑ Yandex
☑ Edge (Chromium-based) ☑ Pale Moon ☑ Vivaldi
☑ Waterfox ☑ Brave

Load history from..

Load history from the specified profiles folder (For example: c:\users)

C:\Users\timba\Desktop\Users

History:

App Data:

Local App Data:

Computer Name:

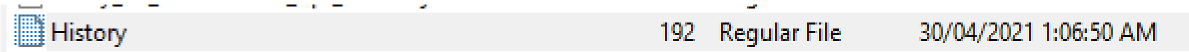
☐ Automatically stop the cache task of IE10/IE11/Edge for unlocking the database file.

☐ Load Internet Explorer history by using API.

☐ Skip duplicate URLs that their time difference is less than... 5 seconds

password cracking lists - Google Search
password cracking lists - Google Search

Alternatively, we can dump the history file located at root\Users\John Doe\Local\Google\User Data\Default:



History 192 Regular File 30/04/2021 1:06:50 AM

You can then open up this database file using a tool like DB Browser for SQLite:

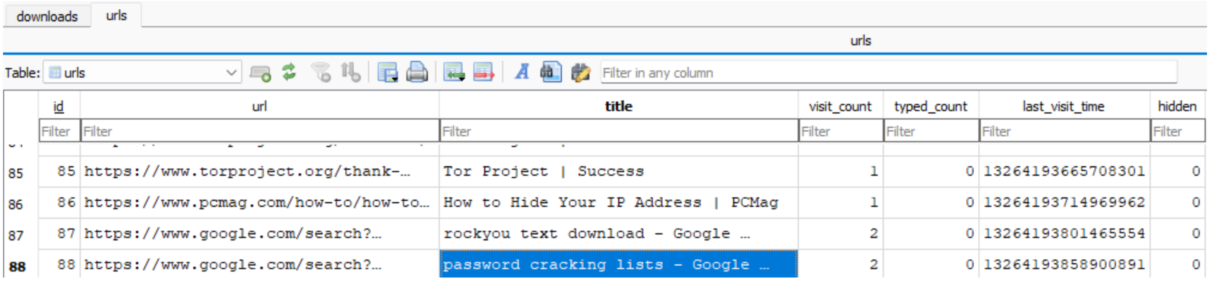


Table: urls

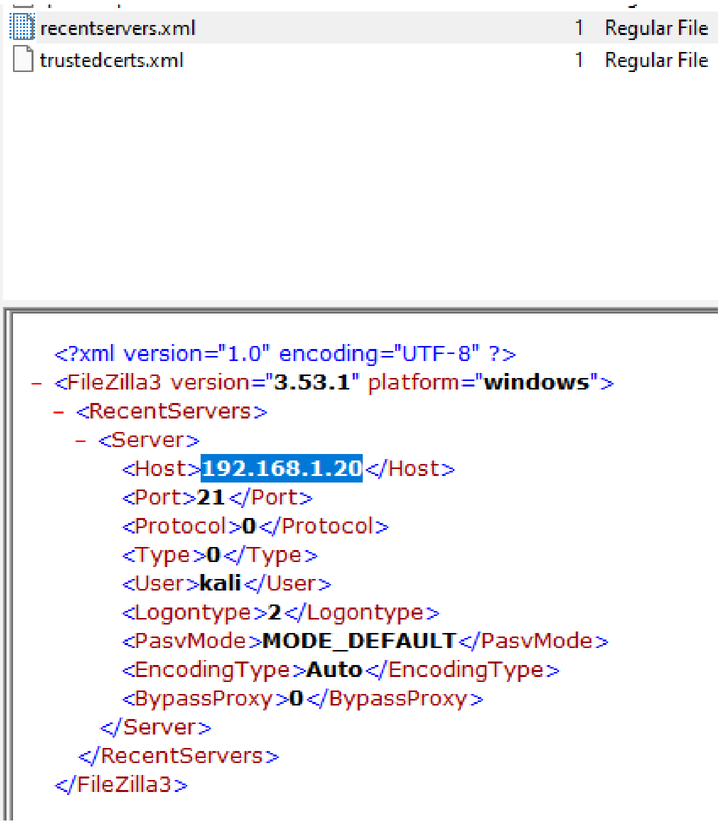
	id	url	title	visit_count	typed_count	last_visit_time	hidden
85	85	https://www.torproject.org/thank-...	Tor Project | Success	1	0	13264193665708301	0
86	86	https://www.pcmag.com/how-to/how-to...	How to Hide Your IP Address | PCMag	1	0	13264193714969962	0
87	87	https://www.google.com/search?...	rockyou text download - Google ...	2	0	13264193801465554	0
88	88	https://www.google.com/search?...	password cracking lists - Google ...	2	0	13264193858900891	0

As you can see, the last_visit_time is in a weird format, we can use a tool like DCode to encode the given timestamp and search for it.

Answer: password cracking lists

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

FileZilla is a popular FTP solution used for both legitimate and malicious use cases. Threat actors often use it to exfiltrate data. If you take a look at John Doe’s Roaming directory, we can see that FileZilla is present. Within the FileZilla directory is a recentservers.xml file that contains the FTP server the suspect connected to:



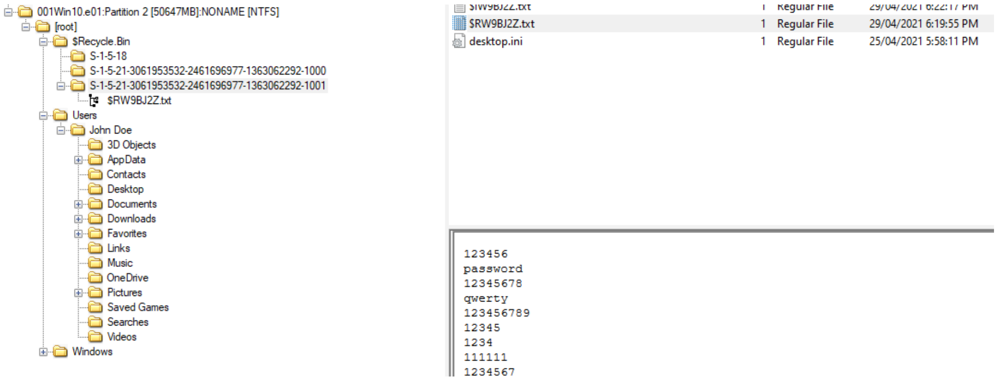
```
recentservers.xml        1   Regular File
trustedcerts.xml         1   Regular File
```

```
  <?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>
```

Answer: 192.168.1.20

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

In order to find the date and time a password list was deleted, we can take a look at the Recycle Bin:

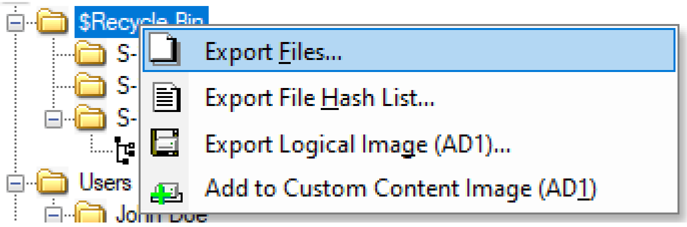


```
001Win10.e01:Partition 2 [50647MB]:NONAME [NTFS]
  [root]
    $Recycle.Bin
      S-1-5-18
      S-1-5-21-3061953532-2461696977-1363062292-1000
      S-1-5-21-3061953532-2461696977-1363062292-1001
        $RW9BJ2Z.txt
    Users
      John Doe
        3D Objects
        AppData
        Contacts
        Desktop
        Documents
        Downloads
        Favorites
        Links
        Music
        OneDrive
        Pictures
        Saved Games
        Searches
        Videos
    Windows
```

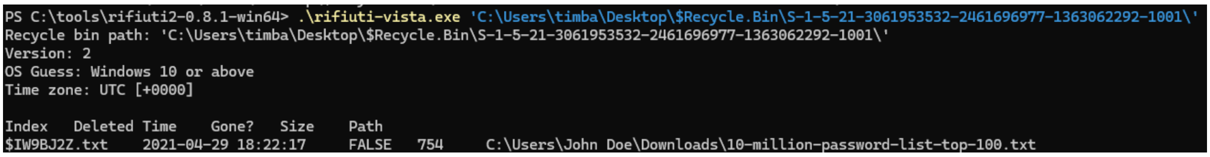
```
$IW9BJ2Z.txt      1   Regular File   29/04/2021 6:22:17 PM
$RW9BJ2Z.txt      1   Regular File   29/04/2021 6:19:55 PM
desktop.ini       1   Regular File   25/04/2021 5:58:11 PM
```

```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
```

To determine the deletion timestamp, we can use a tool called rifiuti, which analyses the metadata of the Windows Recycle Bin. To do so, first dump the Recycle Bin Directory like as follows:



You can then execute the rifiuti-vista.exe binary like as follows:



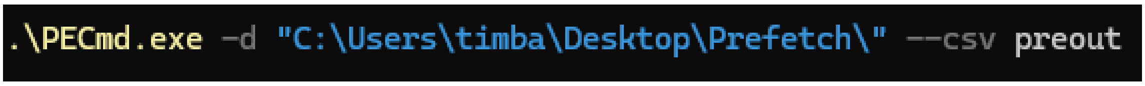
```
PS C:\tools\rifiuti2-0.8.1-win64> .\rifiuti-vista.exe 'C:\Users\timba\Desktop\$Recycle.Bin\S-1-5-21-3061953532-2461696977-1363062292-1001\'
Recycle bin path: 'C:\Users\timba\Desktop\$Recycle.Bin\S-1-5-21-3061953532-2461696977-1363062292-1001\'
Version: 2
OS Guess: Windows 10 or above
Time zone: UTC [+0000]

Index    Deleted Time     Gone?   Size    Path
$IW9BJ2Z.txt    2021-04-29 18:22:17     FALSE   754     C:\Users\John Doe\Downloads\10-million-password-list-top-100.txt
```

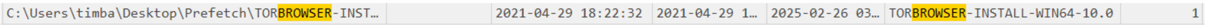
Answer: 2021-04-29 18:22:17 UTC

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

In order to determine how many times the Tor Browser ran, we can analyse the Prefetch files located at root\Windows\Prefetch. For context, Prefetch files server as evidence of execution. We can use PECmd.exe to parse the Prefetch files and examine the output using Timeline Explorer:



```
.\PECmd.exe -d "C:\Users\timba\Desktop\Prefetch\" --csv preout
```



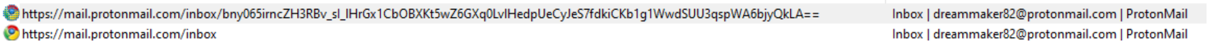
```
C:\Users\timba\Desktop\Prefetch\TORBROWSER-INST…        2021-04-29 18:22:32  2021-04-29 1…  2025-02-26 03…  TORBROWSER-INSTALL-WIN64-10.0        1
```

No Prefetch file exists for the Tor Browser executable itself, so we can conclude that Tor was never run.

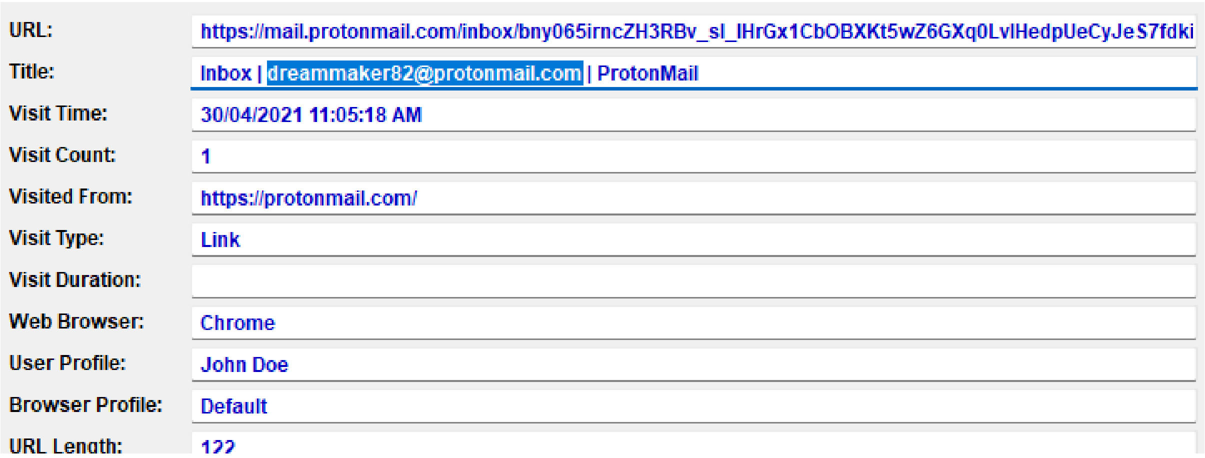
Answer: 0

What is the suspect's email address?

To find the suspect's email address, I started by looking for an OST file within the AppData\Local\Microsoft\Outlook\ directory, however, it seems as if Outlook is not used on the system. I then analysed the users browser history using BrowsingHistoryView, filtering for the string "mail" and found that the user used protonmail:



```
https://mail.protonmail.com/inbox/bny065irncZH3RBv_sl_IHrGx1CbOBXKt5wZ6GXq0LvlHedpUeCyJeS7fdkiCKb1g1WwdSUU3qspWA6bjyQkLA==    Inbox | dreammaker82@protonmail.com | ProtonMail
https://mail.protonmail.com/inbox                                                                                             Inbox | dreammaker82@protonmail.com | ProtonMail
```

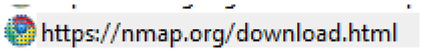


URL:	https://mail.protonmail.com/inbox/bny065irncZH3RBv_sl_IHrGx1CbOBXKt5wZ6GXq0LvlHedpUeCyJeS7fdki
Title:	Inbox | dreammaker82@protonmail.com | ProtonMail
Visit Time:	30/04/2021 11:05:18 AM
Visit Count:	1
Visited From:	https://protonmail.com/
Visit Type:	Link
Visit Duration:	
Web Browser:	Chrome
User Profile:	John Doe
Browser Profile:	Default
URL Length:	122

Answer: dreammaker82@protonmail.com

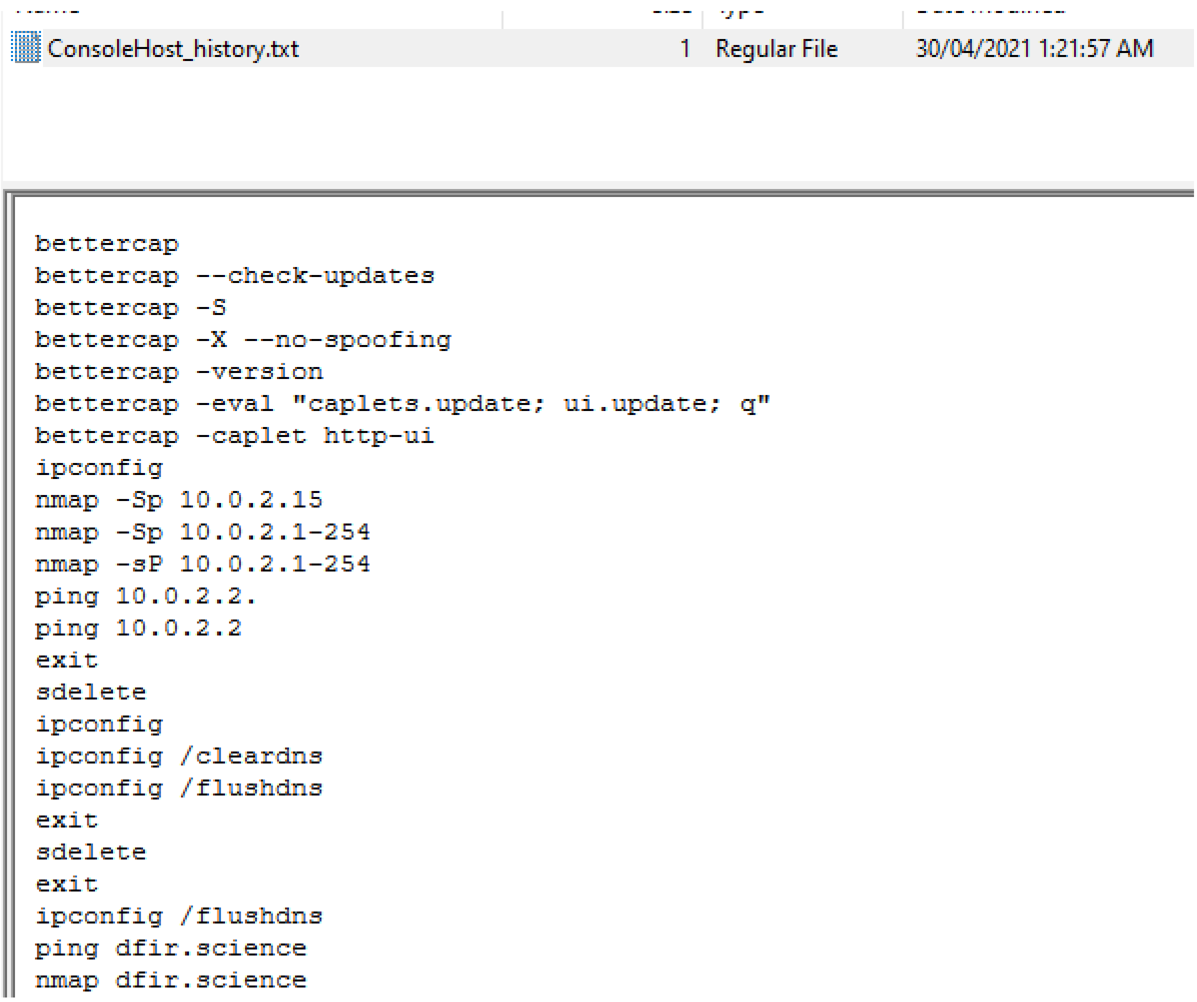
What is the FQDN did the suspect port scan?

If you investigate the user's browsing history, we can see that NMAP was downloaded:



https://nmap.org/download.html

Seeing as nmap is a command-line tool, we can start by investigating the PowerShell command history file located at AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.exe:



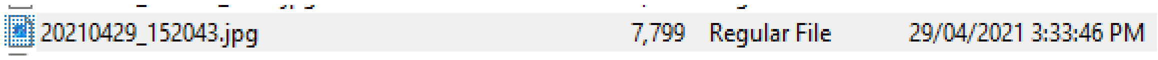
ConsoleHost_history.txt 1 Regular File 30/04/2021 1:21:57 AM

```
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
```

Answer: dfir.science

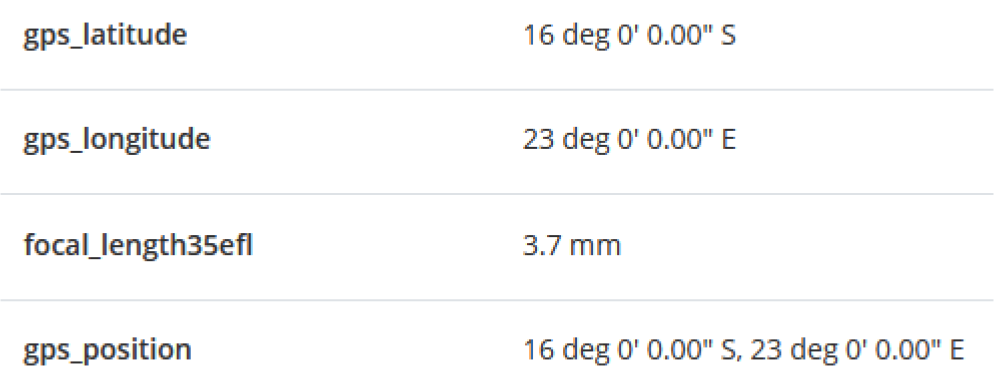
What country was picture "20210429_152043.jpg" allegedly taken in?

If you export the provided image file found in the User's Pictures directory, we can start to examine its EXIF data that may contain GPS coordinates:



20210429_152043.jpg 7,799 Regular File 29/04/2021 3:33:46 PM

I personally use a web-based tool called metadata2go.com:



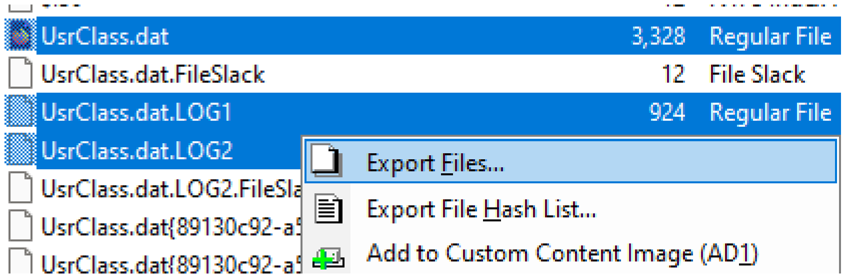
gps_latitude	16 deg 0' 0.00" S
gps_longitude	23 deg 0' 0.00" E
focal_length35efl	3.7 mm
gps_position	16 deg 0' 0.00" S, 23 deg 0' 0.00" E

If you search these coordinates, you will find yourself in Zambia.

Answer: Zambia

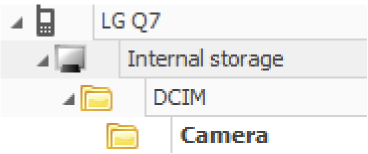
What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop?

To track the original storage location of the image, we can utilise a tool called ShellBags Explorer. ShellBags are an amazing forensic artifact that tracks user interactions with folders. To do so, we first need to export the UsrClass.dat file located at \Users\John Doe\AppData\Local\Microsoft\Windows\UserClass.dat:



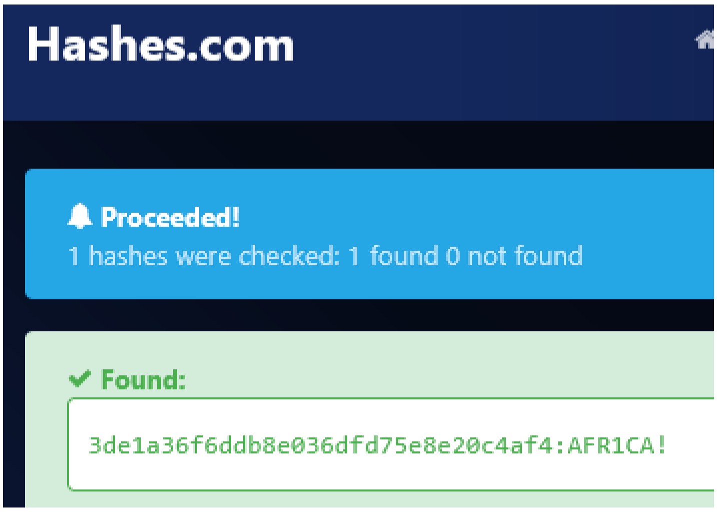
UsrClass.dat	3,328	Regular File
UsrClass.dat.FileSlack	12	File Slack
UsrClass.dat.LOG1	924	Regular File
UsrClass.dat.LOG2		
UsrClass.dat.LOG2.FileSla		
UsrClass.dat{89130c92-a		
UsrClass.dat{89130c92-a		

You can then load this hive using ShellBags explorer. If you look through drives the user has accessed, we can see that an LG Q7 device was connected to the device. The default photo storage directory in this instance is DCIM\Camera:



Answer: Camera

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


Hashes.com

Proceeded!

1 hashes were checked: 1 found 0 not found

✓ Found:

```
3de1a36f6ddb8e036dfd75e8e20c4af4:AFR1CA!
```

Answer: AFR1CA!

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

ctf2021