

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 <ul style="list-style-type: none">• FTK Imager• Autopsy• rifiuti2• Browsing History View• WinPrefetchView• ShellBagsExplorer• mimikatz• Metdata Extractor• Online Hash Crack• NTLM Hash
Published	June 15, 2021	
Author	DFIRScience	
Size	672 MB	

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

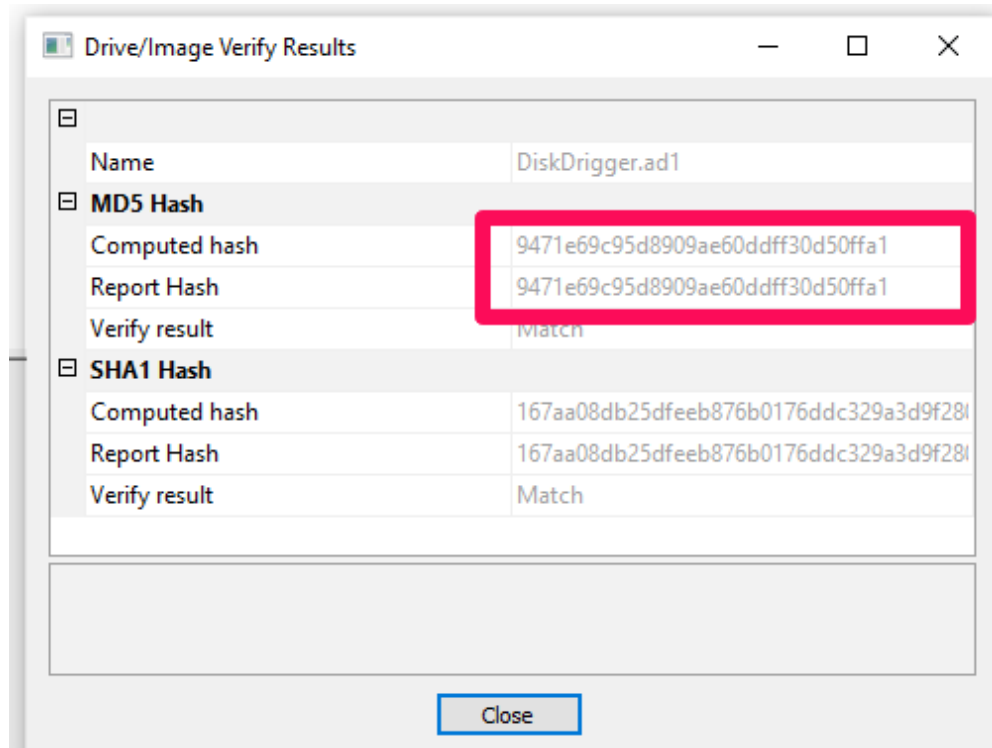
Tools used

- 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 .

Listing

Web Search

Table Thumbnail Summary

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	hacking tools	Google Chrome	2021-04-29 14:23:53 UTC	LogicalFileSet1
History				google.com	grep or	Google Chrome	2021-04-29 15:33:04 UTC	LogicalFileSet1
History				google.com	grep or	Google Chrome	2021-04-29 15:33:04 UTC	LogicalFileSet1
History				google.com	awk remove only the first field	Google Chrome	2021-04-29 15:34:48 UTC	LogicalFileSet1
History				google.com	awk remove only the first field	Google Chrome	2021-04-29 15:34:48 UTC	LogicalFileSet1
History				google.com	filezilla	Google Chrome	2021-04-29 16:01:54 UTC	LogicalFileSet1
History				google.com	filezilla	Google Chrome	2021-04-29 16:01:54 UTC	LogicalFileSet1
History				google.com	caia & able download	Google Chrome	2021-04-29 16:11:44 UTC	LogicalFileSet1
History				google.com	caia & able download	Google Chrome	2021-04-29 16:11:44 UTC	LogicalFileSet1
History				google.com	caia & able download	Google Chrome	2021-04-29 16:11:44 UTC	LogicalFileSet1
History				google.com	how to hide your ip address	Google Chrome	2021-04-29 18:15:10 UTC	LogicalFileSet1
History				google.com	how to hide your ip address	Google Chrome	2021-04-29 18:15:10 UTC	LogicalFileSet1
History				google.com	tor	Google Chrome	2021-04-29 18:14:07 UTC	LogicalFileSet1
History				google.com	tor	Google Chrome	2021-04-29 18:14:07 UTC	LogicalFileSet1
History				google.com	how to hide your ip address	Google Chrome	2021-04-29 18:15:10 UTC	LogicalFileSet1
History				google.com	rockyou text download	Google Chrome	2021-04-29 18:16:41 UTC	LogicalFileSet1
History				google.com	password cracking lists	Google Chrome	2021-04-29 18:17:38 UTC	LogicalFileSet1
History				google.com	password cracking lists	Google Chrome	2021-04-29 18:17:38 UTC	LogicalFileSet1
History				google.com	7zip	Google Chrome	2021-04-30 01:02:58 UTC	LogicalFileSet1
History				google.com	7zip	Google Chrome	2021-04-30 01:02:58 UTC	LogicalFileSet1

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 235 of 238 Result

Web Search

Term: password cracking lists

Time: 2021-04-29 18:17:38 UTC

Domain: google.com

Program Name: Google Chrome

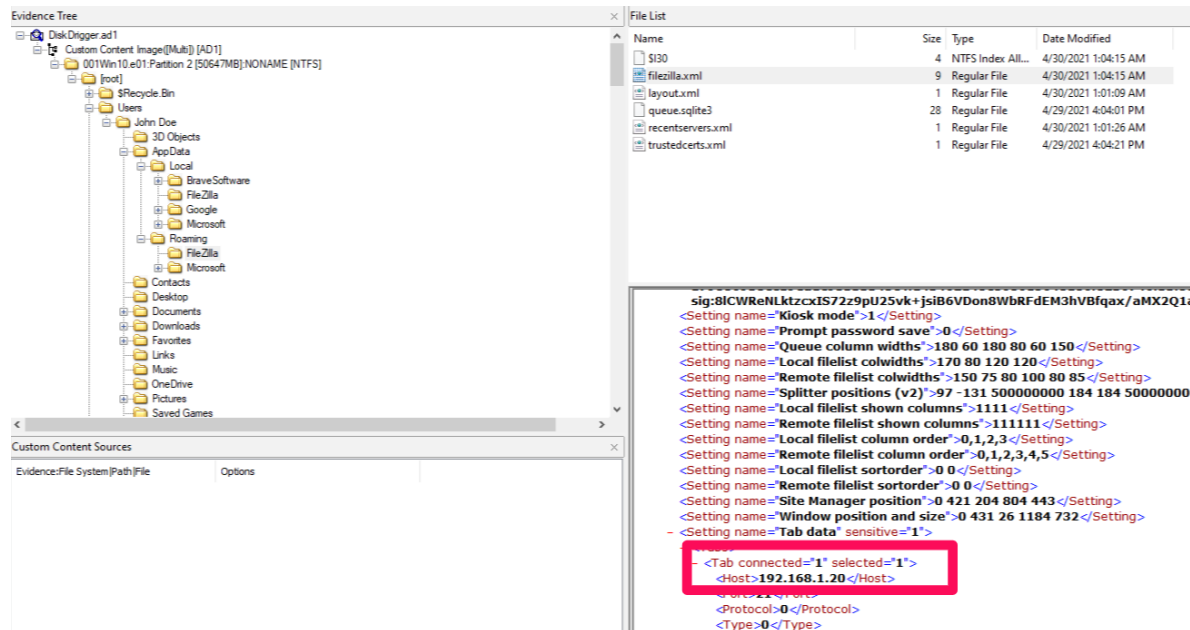
Source

Data Source: LogicalFileSet1

File: /LogicalFileSet1/files and folders/001win10.201_Partition 2 [50647MB] [NO NAME] [NTFS]/(root)/Users/John Doe/Appdata/Local/Google/Chrome/User Data/Default/History

#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.

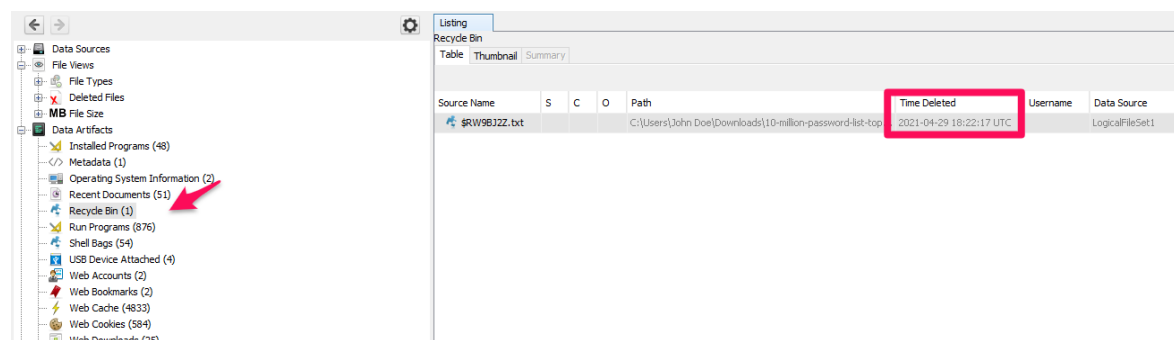


#4 What date and time was a password list deleted in UTC? (YYYY-MM-DD HH:MM:SS UTC)

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

S o u r c e F i l e n a m e	E x e c u t a b l e N a m e	H a s h	S i z e	V e r s i o n	R u n C o u n t	L a s t R u n	P r e v i o u s R u n 0	P r e v i o u s R u n 1	P r e v i o u s R u n 2	P r e v i o u s R u n 3	P r e v i o u s R u n 4	P r e v i o u s R u n 5	P r e v i o u s R u n 6	V o l u m e 0 N a m e	V o l u m e 0 S e r i a l	V o l u m e 0 C r e a t e d	V o l u m e 1 N a m e	V o l u m e 1 S e r i a l	V o l u m e 1 C r e a t e d
--	--	------------------	------------------	---------------------------------	--------------------------------------	---------------------------------	--	--	--	--	--	--	--	---	---	--	---	---	--

ParsingError

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

[illegible]

Using Autopsy checked Web History, filter domain you can identify the email address in the bottom box in view details.

Visit Details
Title: Inbox | dreammaker82@protonmail.com | ProtonMail
Date Accessed: 2021-04-30 01:05:11 UTC
Domain: protonmail.com
URL: https://mail.protonmail.com/inbox
Referrer URL: https://mail.protonmail.com/inbox
Program Name: Google Chrome

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

The screenshot shows a Windows File Explorer window with three panes. The left pane displays a file tree for 'Disk Drigger.ad1', showing a custom content image partition. The right pane shows a file list with columns for Name, Size, Type, and Date Modified, listing 'ConsoleHost_history.txt'. The bottom pane shows the 'Custom Content Sources' tab with the 'File System(Path)\File' view.

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

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

The screenshot shows a file analysis interface. On the left is a tree view with categories like Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Analysis Results, OS Accounts, Tags, and Reports. The 'Analysis Results' section is expanded, showing 'EXIF Metadata (14)'. The main panel on the right displays a table of image files. Below the table, the 'File Metadata' tab is selected, showing details for the item '20210429_152043.jpg'. The 'Analysis Result 1' section, which is highlighted with a red box, contains the following information:

Name	S	C
background-2.jpg		
background-3.jpg		
1196d63c.jpg		
4254396c.jpg		
4683b0e5.jpg		
6973a695.jpg		
8fce0f3.jpg		
CachedImage_1024_768_POS4.jpg		
CachedImage_1662_931_POS4.jpg		

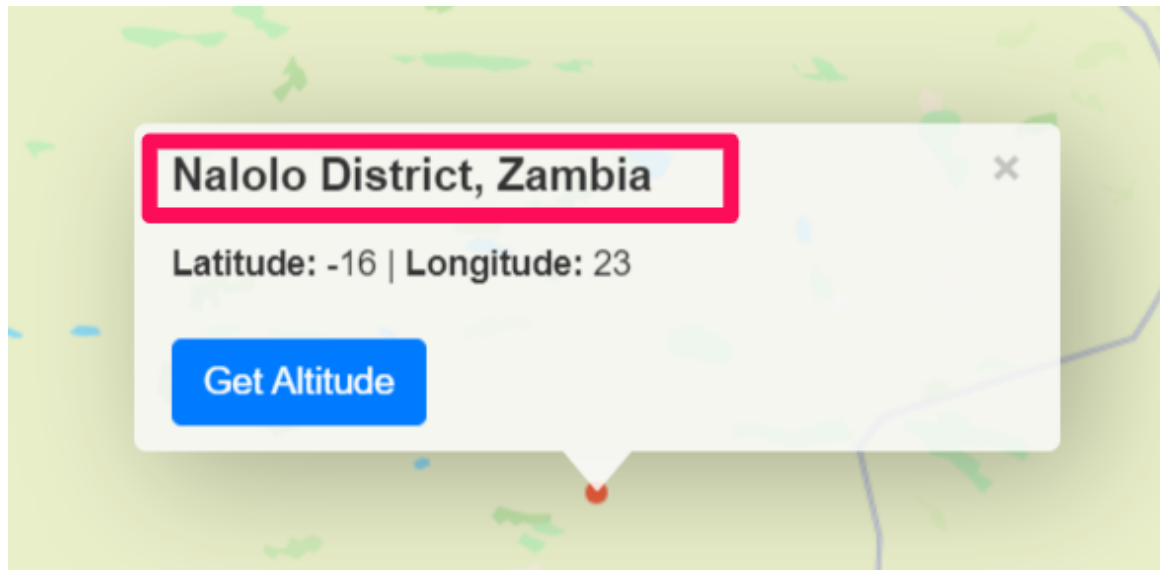
Item: 20210429_152043.jpg
Aggregate Score: Not Notable

Analysis Result 1

Score: Not Notable
Type: EXIF Metadata
Configuration:
Conclusion:
Altitude: 0.0
Date Created: 2021-04-29 20:50:43 IST
Device Make: LG Electronics
Device Model: LM-Q725K
Latitude: -16.0
Longitude: 23.0

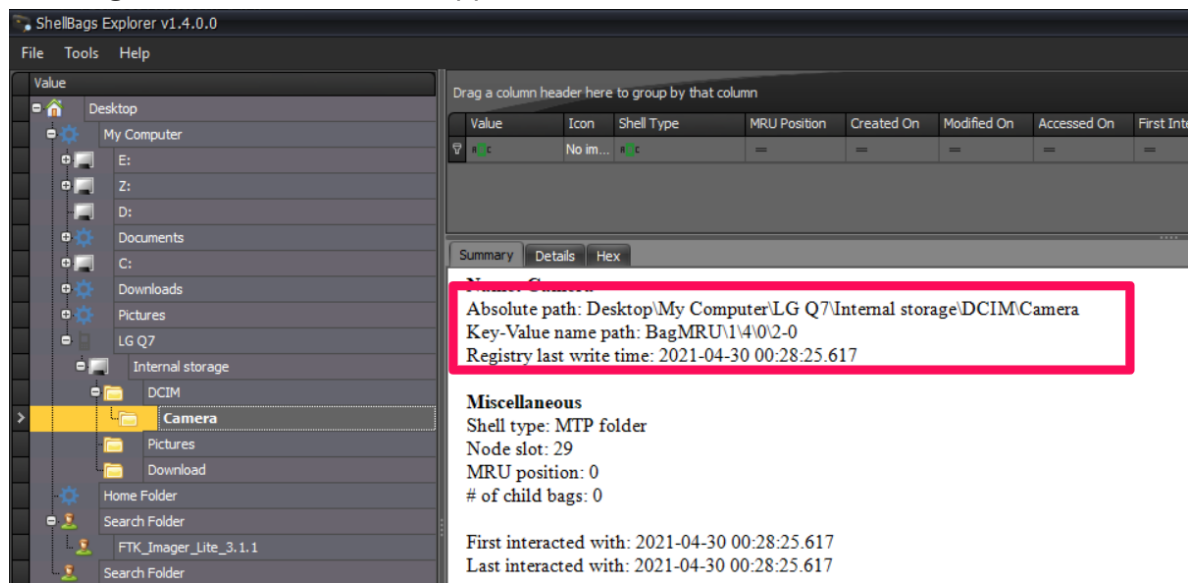
Analysis Result 2

Score: Unknown
Type: User Content Suspected
Configuration:
Conclusion:
Comment: EXIF metadata data exists for this file.



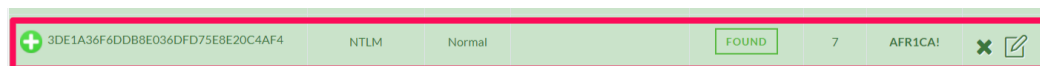
#9 What is the parent folder name picture "20210429_151535.jpg" was in before the suspect copy it to "contact" folder on his desktop? Answer: (Camera)

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.