Challenge: DiskFiltration

Platform: TryHackMe

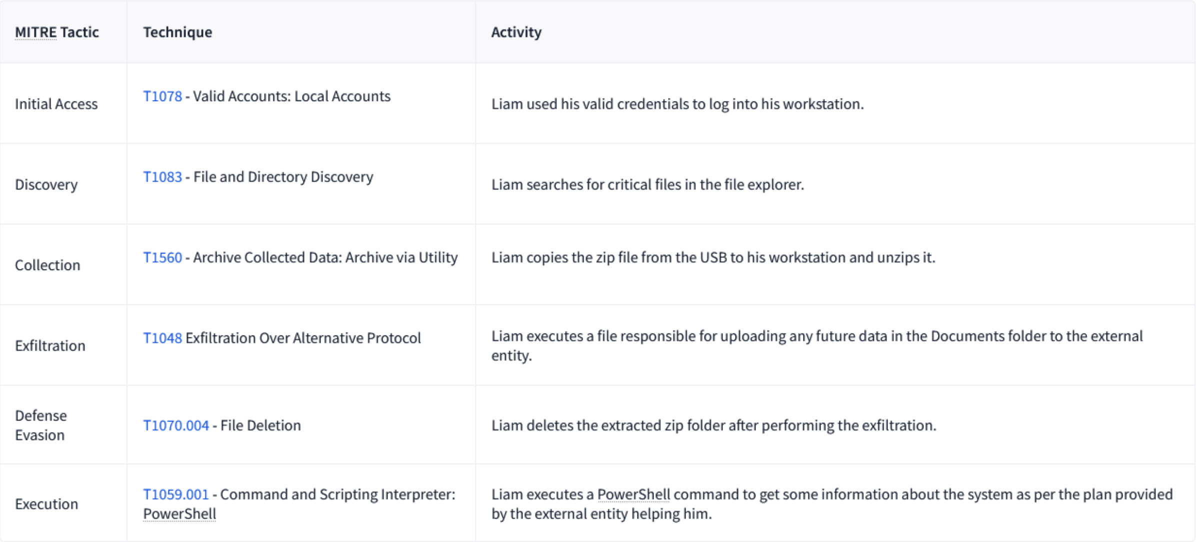
Category: Endpoint Forensics

Difficulty: Hard

Tools Used: Autopsy, Timeline Explorer, MFTECmd, Exiftool, HxD

Summary: This challenge involved analysing a disk image using a variety of forensic tools. It challenges you to explore a bunch of forensic artifacts on the Windows OS, like the UsnJrnl, PowerShell History, ShellBags, and more. I found it very challenging, but super enjoyable. For those who have completed digital forensic challenges before and understand the basic forensic artifacts on a Windows system, I recommend doing this challenge.

Scenario: Tech THM discovered their critical data had been leaked to the competitors. After an internal investigation, the company suspects Liam, a recently terminated employee who was working as a system engineer with Tech THM. This suspicion was raised as Liam had access to the leaked data in his company-provided workstation. He often worked late hours without clear justification for his extended presence. He was also caught roaming around the critical server room and taking pictures of the entry gate. Following these suspicions, Liam's workstation (provided by the company) was investigated. The initial investigation suggests that an external entity was also helping Liam.



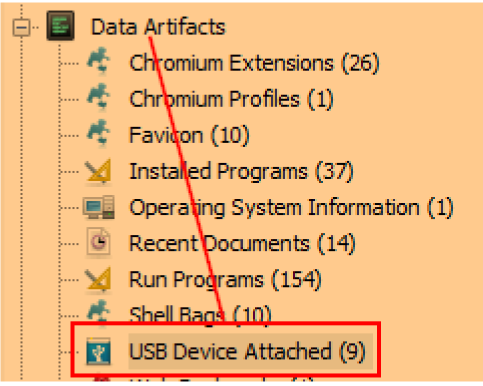
MITRE Tactic	Technique	Activity
Initial Access	T1078 - Valid Accounts: Local Accounts	Liam used his valid credentials to log into his workstation.
Discovery	T1083 - File and Directory Discovery	Liam searches for critical files in the file explorer.
Collection	T1560 - Archive Collected Data: Archive via Utility	Liam copies the zip file from the USB to his workstation and unzips it.
Exfiltration	T1048 Exfiltration Over Alternative Protocol	Liam executes a file responsible for uploading any future data in the Documents folder to the external entity.
Defense Evasion	T1070.004 - File Deletion	Liam deletes the extracted zip folder after performing the exfiltration.
Execution	T1059.001 - Command and Scripting Interpreter: PowerShell	Liam executes a PowerShell command to get some information about the system as per the plan provided by the external entity helping him.

What is the serial number of the USB device Liam used for exfiltration?

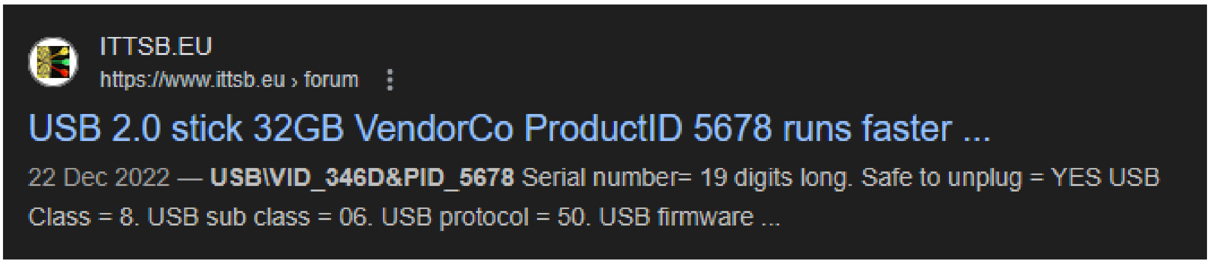
You can find an Autopsy case file located at:

C:\Users\Administrator\Documents\New Folder\Liam's Disk\

If you double click this file or open it up in Autopsy, it will eventually load the Autopsy results that were generated from the disk image. Under the Data Artifacts tab, there is a section called “USB Device Attached”:



We can then see a device model called VID_346D&PID_5678. After a quick Google search, this appears to be a USB drive:

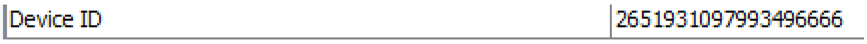


ITTSB.EU
https://www.ittsb.eu › forum

USB 2.0 stick 32GB VendorCo ProductID 5678 runs faster ...

22 Dec 2022 — **USB\VID_346D&PID_5678** Serial number= 19 digits long. Safe to unplug = YES USB Class = 8. USB sub class = 06. USB protocol = 50. USB firmware ...

The serial number of this device is simply the Device ID:



Device ID	2651931097993496666

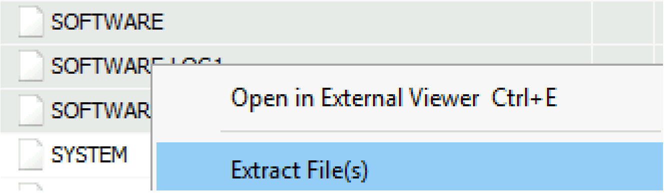
Answer: 2651931097993496666

What is the profile name of the personal hotspot Liam used to evade network-level detection?

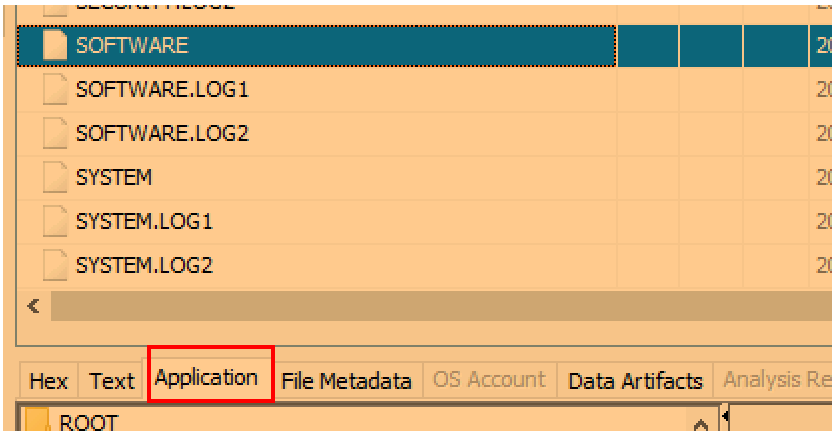
You can find stored wireless networks in many locations. First, we need to dump the SOFTWARE registry hive. You can do so by navigating to:

Windows/System32/config

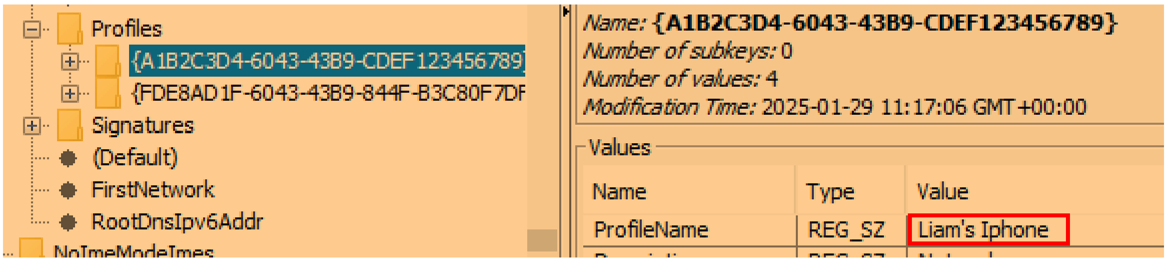
Scroll down until you see the SOFTWARE file:



If you click on the registry hive, make sure to look at the Application view shown near the bottom of the screen:



After doing so, navigate to Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Profile, this is where information regarding network profiles such as network name and connection history are stored:


Profiles
{A1B2C3D4-6043-43B9-CDEF123456789}
{FDE8AD1F-6043-43B9-844F-B3C80F7DF
Signatures
(Default)
FirstNetwork
RootDnsIpv6Addr
NoImeModeImes

Name: **{A1B2C3D4-6043-43B9-CDEF123456789}**
Number of subkeys: 0
Number of values: 4
Modification Time: 2025-01-29 11:17:06 GMT+00:00

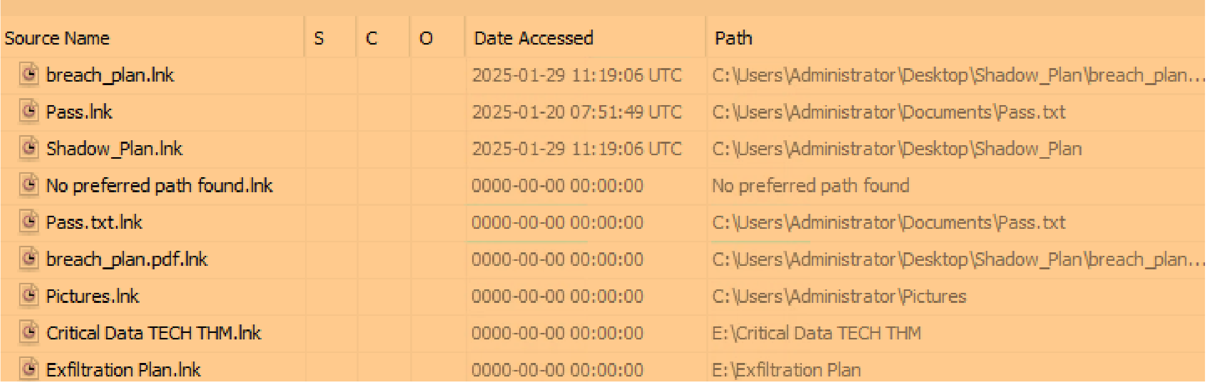
Values

Name	Type	Value
ProfileName	REG_SZ	Liam's Iphone

Answer: Liam's Iphone

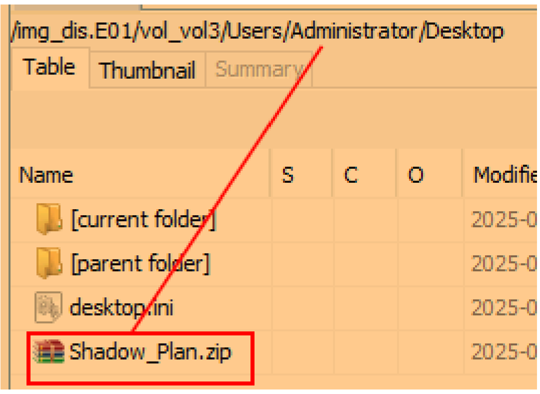
What is the name of the zip file Liam copied from the USB to the machine for exfiltration instructions?

Shellbags are a forensic artifact that contains details about what folders a user has accessed. If you look at the Recent Documents section under Data Artifacts, we can see some interesting files:



Source Name	S	C	O	Date Accessed	Path
breach_plan.lnk				2025-01-29 11:19:06 UTC	C:\Users\Administrator\Desktop\Shadow_Plan\breach_plan…
Pass.lnk				2025-01-20 07:51:49 UTC	C:\Users\Administrator\Documents\Pass.txt
Shadow_Plan.lnk				2025-01-29 11:19:06 UTC	C:\Users\Administrator\Desktop\Shadow_Plan
No preferred path found.lnk				0000-00-00 00:00:00	No preferred path found
Pass.txt.lnk				0000-00-00 00:00:00	C:\Users\Administrator\Documents\Pass.txt
breach_plan.pdf.lnk				0000-00-00 00:00:00	C:\Users\Administrator\Desktop\Shadow_Plan\breach_plan…
Pictures.lnk				0000-00-00 00:00:00	C:\Users\Administrator\Pictures
Critical Data TECH THM.lnk				0000-00-00 00:00:00	E:\Critical Data TECH THM
Exfiltration Plan.lnk				0000-00-00 00:00:00	E:\Exfiltration Plan

Take note of the path, it all points to the Administrator account. Let's go check out what files this user has. After looking around, I found a zip file within the users Desktop directory:



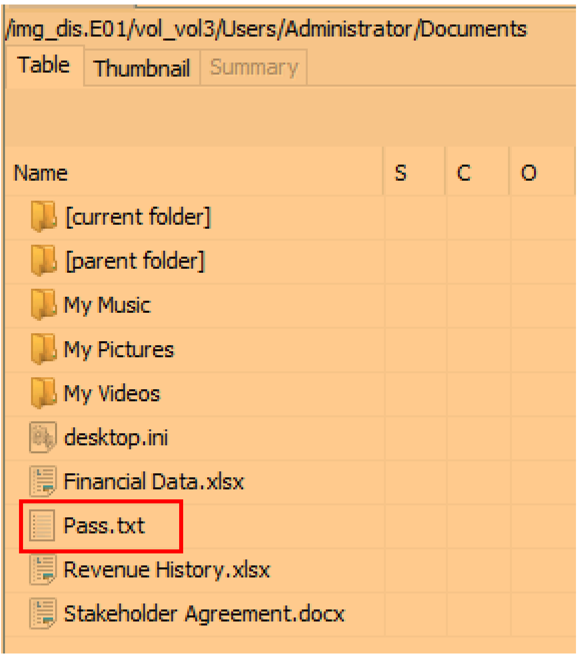
/img_dis.E01/vol_vol3/Users/Administrator/Desktop

Name	S	C	O	Modifie
[current folder]				2025-0
[parent folder]				2025-0
desktop.ini				2025-0
Shadow_Plan.zip				2025-0

Answer: Shadow_Plan.zip

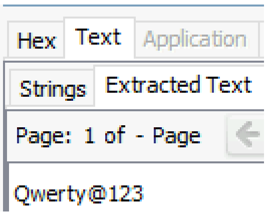
What is the password for this zip file?

If you look at the recent documents, you can see that a file called Pass.txt is located in the administrator users Documents directory. Upon navigating to this path, we can find the file:



/img_dis.E01/vol_vol3/Users/Administrator/Documents

Name	S	C	O
[current folder]			
[parent folder]			
My Music			
My Pictures			
My Videos			
desktop.ini			
Financial Data.xlsx			
Pass.txt			
Revenue History.xlsx			
Stakeholder Agreement.docx			

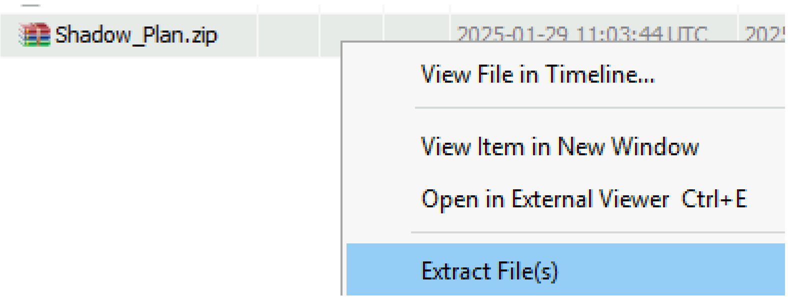


Qwerty@123

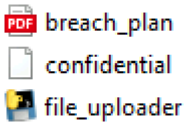
Answer: Qwerty@123

Time to reveal the external entity helping Liam! Who is the author of the PDF file stored in the zip file?

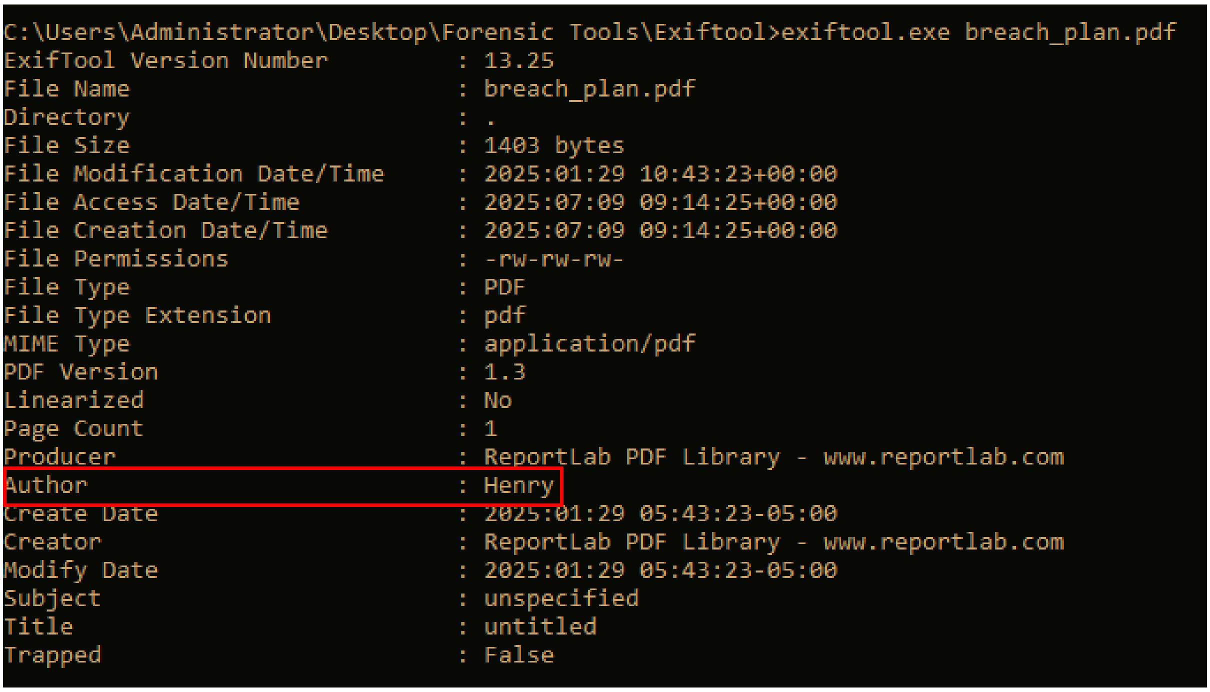
First, we need to export the zip file by right clicking it and selecting extract files:



Navigate to this file and extract it with the password found previously. Within this file is a pdf called breach_plan among 2 other files:



Within the Forensic Tools folder on the Desktop is a tool called Exiftool. We can use this tool to get the metadata of the PDF file, and likely the original author:

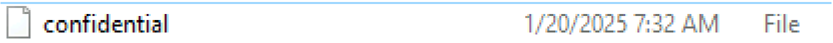


```
C:\Users\Administrator\Desktop\Forensic Tools\Exiftool>exiftool.exe breach_plan.pdf
ExifTool Version Number         : 13.25
File Name                       : breach_plan.pdf
Directory                       : .
File Size                       : 1403 bytes
File Modification Date/Time     : 2025:01:29 10:43:23+00:00
File Access Date/Time           : 2025:07:09 09:14:25+00:00
File Creation Date/Time         : 2025:07:09 09:14:25+00:00
File Permissions                : -rw-rw-rw-
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.3
Linearized                      : No
Page Count                      : 1
Producer                        : ReportLab PDF Library - www.reportlab.com
Author                          : Henry
Create Date                     : 2025:01:29 05:43:23-05:00
Creator                         : ReportLab PDF Library - www.reportlab.com
Modify Date                     : 2025:01:29 05:43:23-05:00
Subject                         : unspecified
Title                           : untitled
Trapped                         : False
```

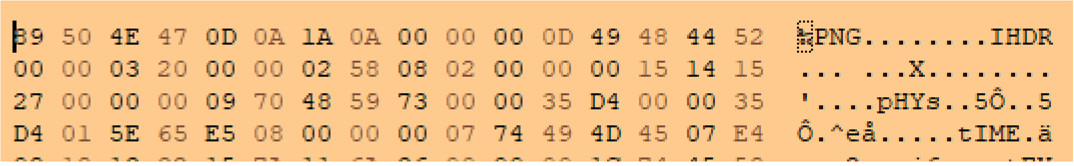
Answer: Henry

What is the correct extension of the file that has no extension in the zip folder?

Within the Forensic Tools folder on the Desktop is another tool called HxD. After installing it, we can open up the file with no extension:



```
confidential                         1/20/2025 7:32 AM     File
```



```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52  ‰PNG........IHDR
00 00 03 20 00 00 02 58 08 02 00 00 00 15 14 15  ... ...X........
27 00 00 00 09 70 48 59 73 00 00 35 D4 00 00 35  '....pHYs..5Ô..5
D4 01 5E 65 E5 08 00 00 00 07 74 49 4D 45 07 E4  Ô.^eå.....tIME.ä
```

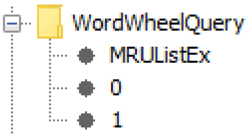
89 50 4E 47 0D 0A 1A 0A is the file signature of PNG files in HEX. As you can see in the above image, this file with no extension has the file signature of a PNG file. To test this, simply append the .png file extension and open up the file:

Answer: png

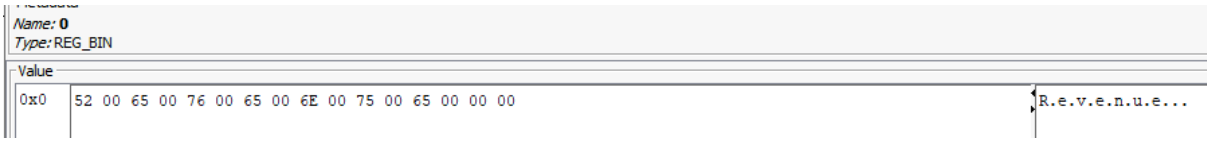
It looks like Liam searched for some files inside the file explorer. What are the names of these files? (alphabetical order)

WordWheelQuery is a forensic artifact that keeps track of all the terms that are searched for in the File Explorer. It is located at:

NTUSER.dat: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery



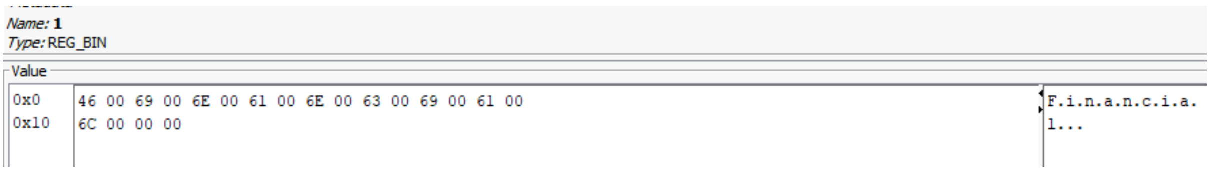
```
WordWheelQuery
  MRUListEx
  0
  1
```



Name: 0
Type: REG_BIN

Value

```
0x0   52 00 65 00 76 00 65 00 6E 00 75 00 65 00 00 00     R.e.v.e.n.u.e...
```



Name: **1**
Type: REG_BIN

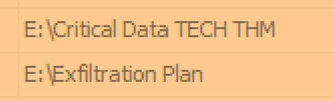
Value

```
0x0   46 00 69 00 6E 00 61 00 6E 00 63 00 69 00 61 00     F.i.n.a.n.c.i.a.
0x10  6C 00 00 00                                         l...
```

Answer: Financial, Revenue

What are the names of the folders that were present on the USB device? (alphabetical order)

Within the Recent Documents section, we can see an E: drive and two folders:



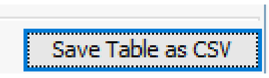
E:\Critical Data TECH THM
E:\Exfiltration Plan

Answer: Critical Data TECH THM, Exfiltration Plan

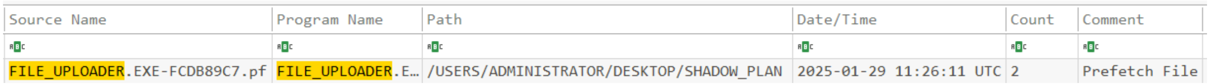
The external entity didn't fully trust Liam for the exfiltration so they asked him to execute file_uploader.exe, through the instructions in PDF. When was this file last executed and how many times was it executed? (YYYY-MM-DD HH:MM:SS, number of execution times)

Autopsy has an entire section called Run Programs that has parsed the many evidence of execution artifacts (like User Assist, Prefetch, etc):

I saved this list as CSV, which you can do by clicking the following button:



After exporting this CSV into Timeline Explorer and searching for file_uploader, we can find when it was last executed:

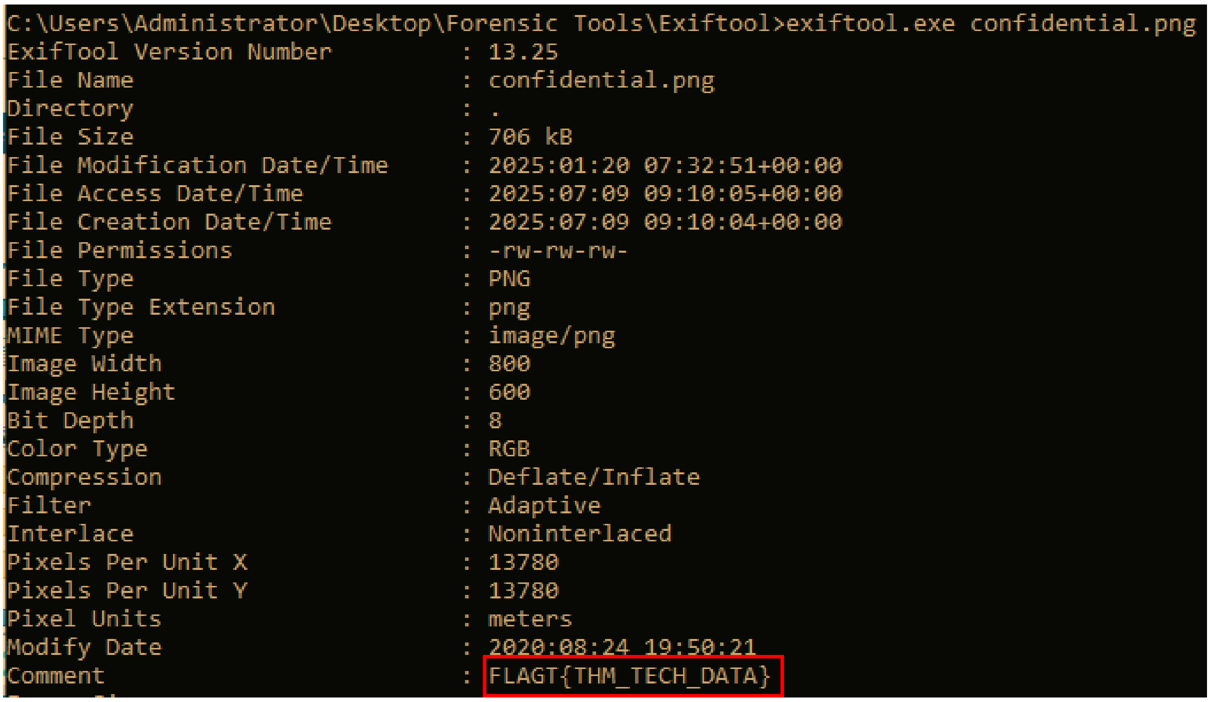


Source Name	Program Name	Path	Date/Time	Count	Comment
FILE_UPLOADER.EXE-FCDB89C7.pf	FILE_UPLOADER.E…	/USERS/ADMINISTRATOR/DESKTOP/SHADOW_PLAN	2025-01-29 11:26:11 UTC	2	Prefetch File

Answer: 2025-01-29 11:26:09, 2

Liam received a hidden flag inside a file (in the zip folder) from the external entity helping him. What was that?

Recall previously we found a file in the zip folder without an extension that turned out to be a PNG file. If you execute exiftool against this file, you can find the flag in the Comment field:



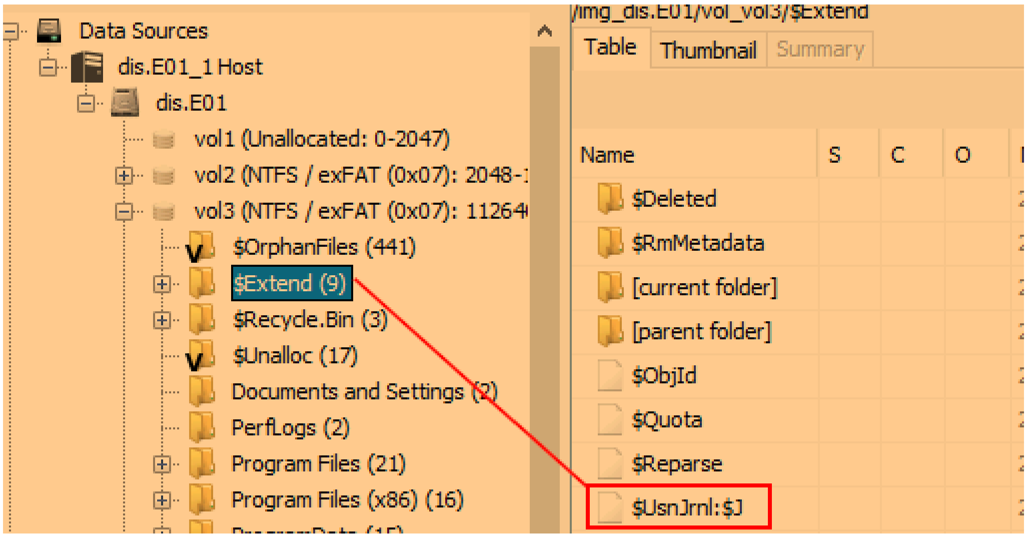
```
C:\Users\Administrator\Desktop\Forensic Tools\Exiftool>exiftool.exe confidential.png
ExifTool Version Number         : 13.25
File Name                       : confidential.png
Directory                       : .
File Size                       : 706 kB
File Modification Date/Time     : 2025:01:20 07:32:51+00:00
File Access Date/Time           : 2025:07:09 09:10:05+00:00
File Creation Date/Time         : 2025:07:09 09:10:04+00:00
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 800
Image Height                    : 600
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Pixels Per Unit X               : 13780
Pixels Per Unit Y               : 13780
Pixel Units                     : meters
Modify Date                     : 2020:08:24 19:50:21
Comment                         : FLAGT{THM_TECH_DATA}
```

Answer: FLAGT{THM_TECH_DATA}

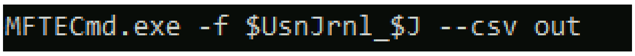
It seems like Liam caused one last damage before leaving. When did Liam delete "Tax Records.docx"? (YYYY-MM-DD HH:MM:SS)

The Usn Journal file is a valuable forensic artifact for tracking file and directory changes on a Windows system. It is located at:

$Extend\$UsnJrnl

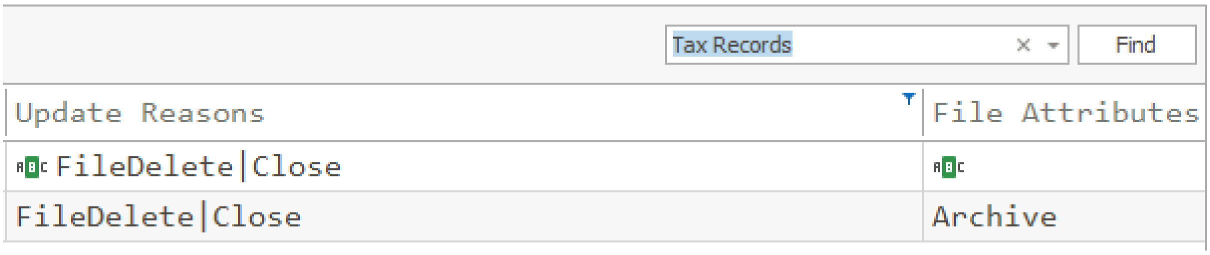


Make sure to extract this file. We can then use a tool called MFTECmd to parse this file:



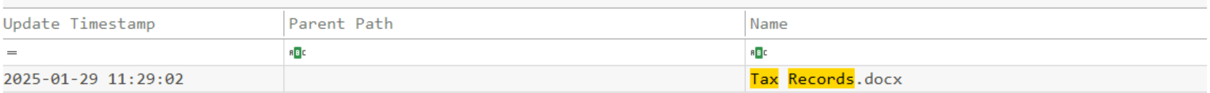
```
MFTECmd.exe -f $UsnJrnl_$J --csv out
```

I then took this CSV file and loaded it into Timeline Explorer. We can then search for the file in question and make sure the update reason is filtered to file delete:



Update Reasons	File Attributes
FileDelete|Close	Archive

This will give you one result, where the Update Timestamp shows when this file was deleted:

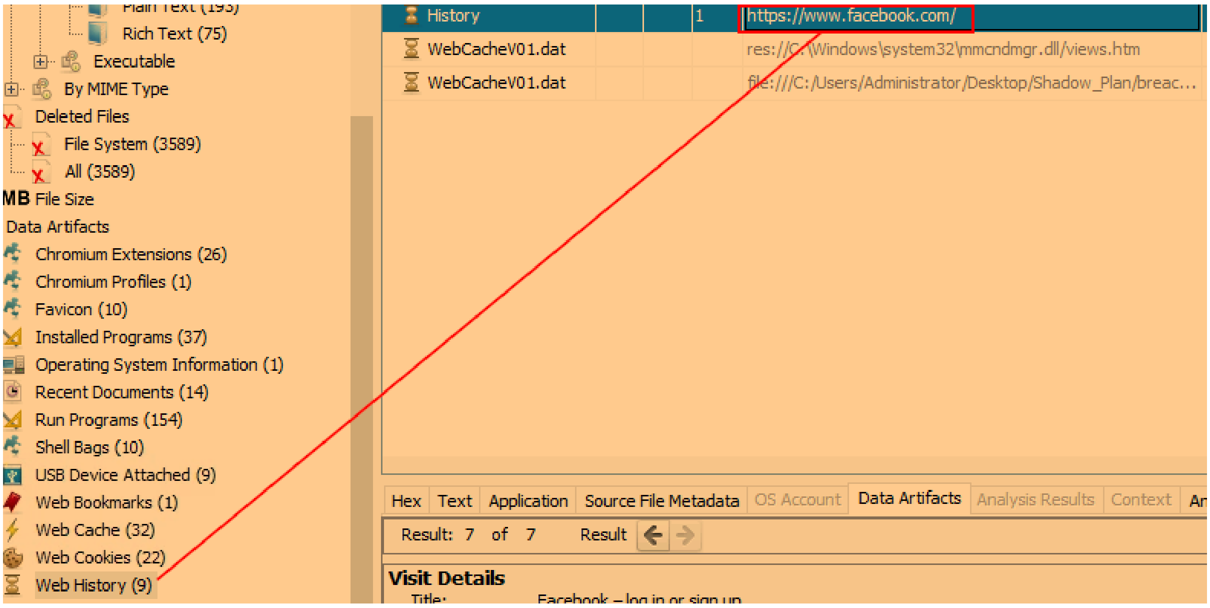


Update Timestamp	Parent Path	Name
2025-01-29 11:29:02		Tax Records.docx

Answer: 2025-01-29 11:29:02

Which social media site did Liam search for using his web browser? Likely to avoid suspicion, thinking somebody was watching him. (Full URL)

Luckily for us, Autopsy has an entire section for Web History. Here we can see that Liam searched for facebook.com:



History		1	https://www.facebook.com/
WebCacheV01.dat			res://C:\Windows\system32\mmcndmgr.dll/views.htm
WebCacheV01.dat			file:///C:/Users/Administrator/Desktop/Shadow_Plan/breac...

Result: 7 of 7 Result

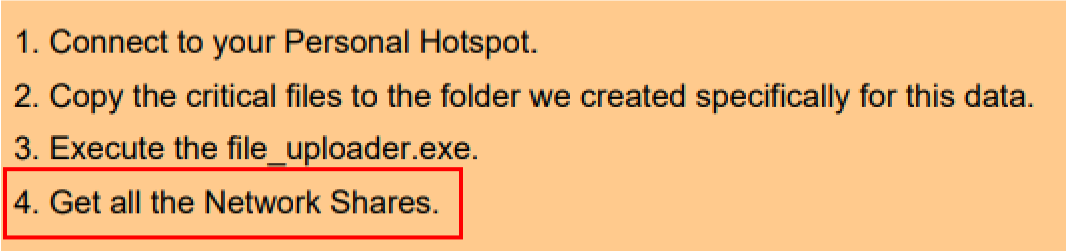
Visit Details

Title: Facebook – log in or sign up

Answer: https://www.facebook.com

What is the PowerShell command Liam executed as per the plan?

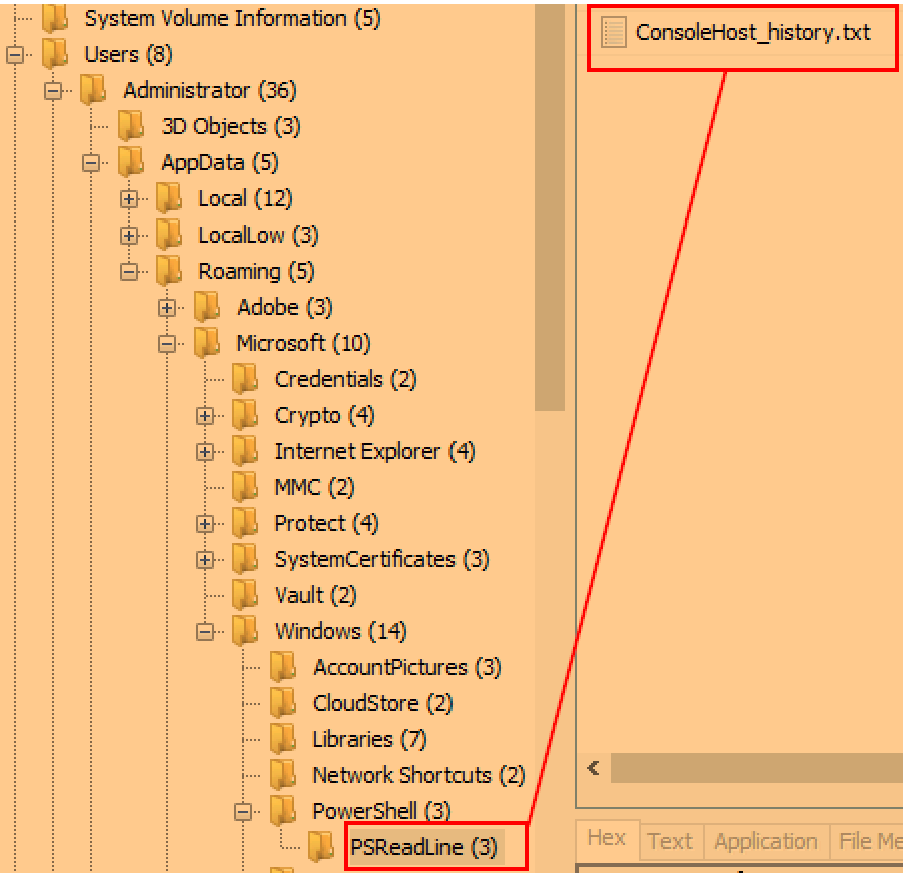
The breach_plan PDF that was within the password protected zip file from earlier had 4 steps:

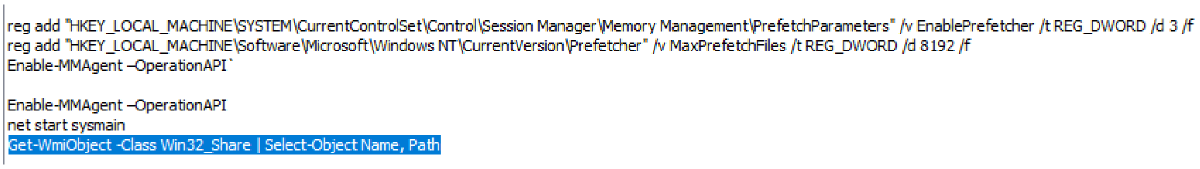


1. Connect to your Personal Hotspot.
2. Copy the critical files to the folder we created specifically for this data.
3. Execute the file_uploader.exe.
4. Get all the Network Shares.

The PowerShell history file which stores commands from previous sessions is located within a user's AppData directory:

APPDATA\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt





```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters" /v EnablePrefetcher /t REG_DWORD /d 3 /f
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Prefetcher" /v MaxPrefetchFiles /t REG_DWORD /d 8192 /f
Enable-MMAgent –OperationAPI`

Enable-MMAgent –OperationAPI
net start sysmain
Get-WmiObject -Class Win32_Share | Select-Object Name, Path
```

The final command, which is highlighted in the above image, lists all shared folders on the machine. Therefore, it is save to assume that this is the answer.

Answer: Get-WmiObject -Class Win32_Share | Select-Object Name, Path