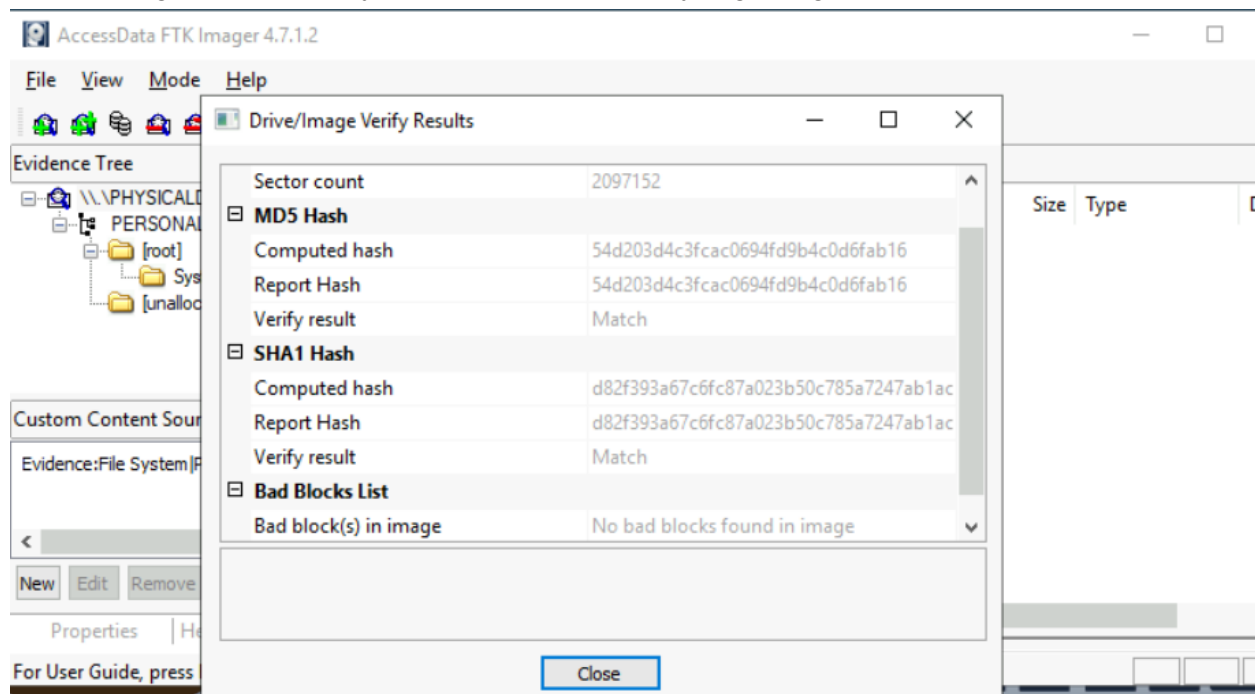


TryHackMe Digital Forensics Case B4DM755

Link:

<https://tryhackme.com/room/caseb4dm755>

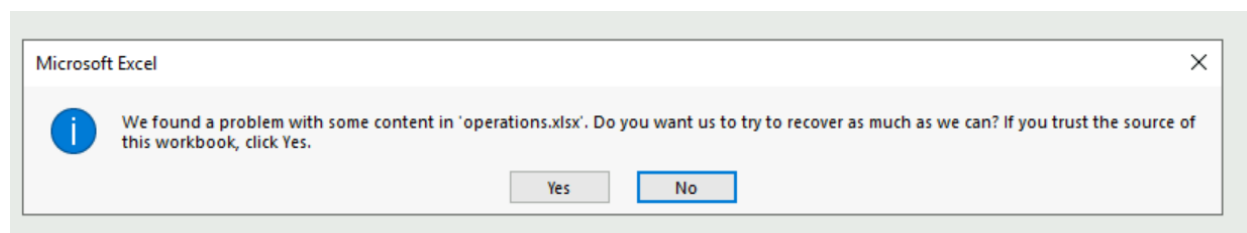
After making a forensic copy of the item we are analyzing, we get hash values:



8 hidden files, 6 deleted files, and 3 recovered files. Files with an 'x' over the icon are deleted files that are still in memory, and files with a size of 0 are corrupted. The hidden files were counted based off of the equation $\text{hiddenFiles} = \text{totalFiles} - \text{deletedFiles} - \text{recoveredFiles}$

File List				
Name	Size	Type	Date Modified	
autorun.inf	1	Regular File	3/20/2023 6:07:46 AM	
autorun.inf.FileSlack	4	File Slack		
CJAT_Toolkit_full_version23Mar10all.pdf	9,111	Regular File	10/8/2022 4:37:18 PM	
CJAT_Toolkit_full_version23Mar10all.pdf....	2	File Slack		
condominium.pdf	0	Regular File	3/18/2023 7:02:14 PM	
dailytasks.txt	2	Regular File	3/19/2023 10:45:40 AM	
dailytasks.txt.FileSlack	3	File Slack		
hideout.pdf	4,585	Regular File	9/11/2022 4:31:48 AM	
hideout.pdf.FileSlack	4	File Slack		
interview.txt	2	Regular File	3/31/2023 5:52:52 AM	
interview.txt.FileSlack	3	File Slack		
nistspecialpublication800-86.pdf	2,753	Regular File	10/8/2022 3:51:34 PM	
nistspecialpublication800-86.pdf.FileSlack	4	File Slack		

We then export the files to the desktop for ease of viewing. Click through all of the files that are corrupted/wrong extension and try to open them. Utilizing 'exiftool', we can see the actual extension of the file, a few pdfs that are supposed to be jpg, then one xlsx that should be a zip. Zip file, when we try to open it as the current extension '.xlsx'



Zip file within exiftool output

New folder > [root]

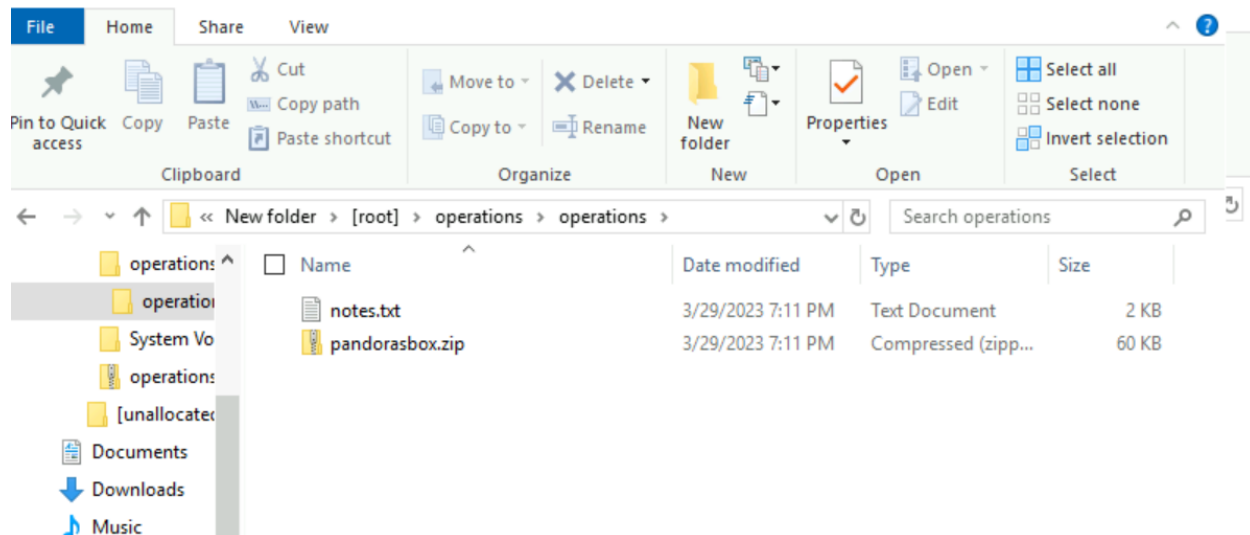
- System Volume Information
- autorun.ico
- autorun.inf
- CJAT_Toolkit_full_version23Mar10all.pdf
- condominium.pdf
- dailytasks.txt
- hideout.jpg
- interview.txt
- nistspecialpublication800-86.pdf
- operations.xlsx**
- resortsworld.png
- townhouse.pdf
- usab5601.pdf
- usab5906.pdf

```

C:\Users\analyst\Desktop\New folder\[root]>exiftool operations.xlsx
ExifTool Version Number      : 12.47
File Name                    : operations.xlsx
Directory                    : .
File Size                     : 62 kB
File Modification Date/Time   : 2023:03:29 11:12:10+00:00
File Access Date/Time        : 2023:03:31 21:02:26+00:00
File Creation Date/Time      : 2023:03:31 21:02:24+00:00
File Permissions              : -rw-rw-rw-
File Type                     : ZIP
File Type Extension           : zip
MIME Type                     : application/zip
Zip Required Version          : 20
Zip Bit Flag                  : 0
Zip Compression               : Deflated
Zip Modify Date               : 2023:03:29 19:11:16
Zip CRC                       : 0x3819dab3
Zip Compressed Size           : 819
Zip Uncompressed Size         : 1752
Zip File Name                 : operations/notes.txt
Warning                       : [minor] Use the Duplicates option to extract tags for all 2 files

```

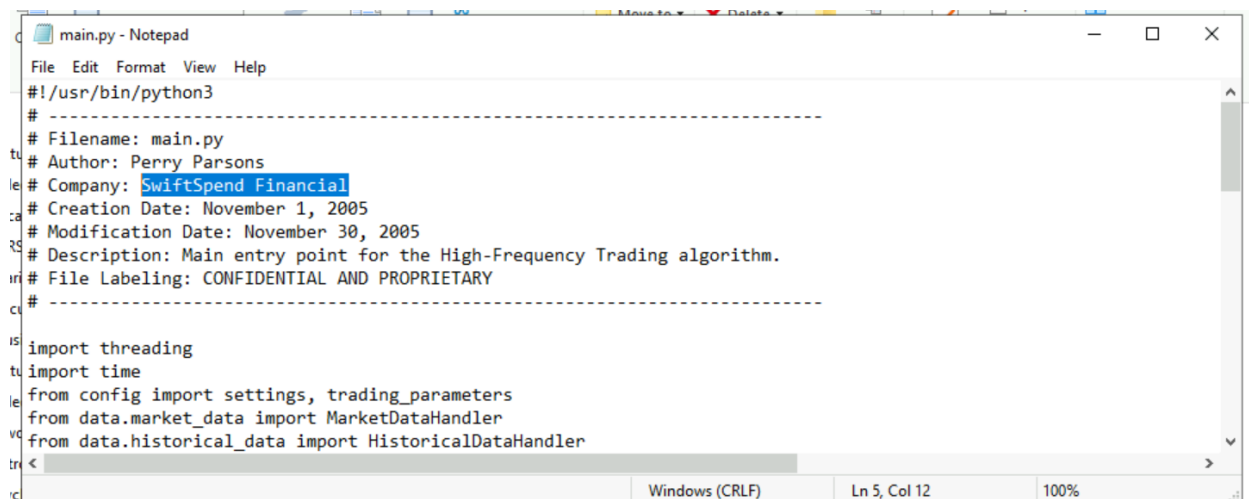
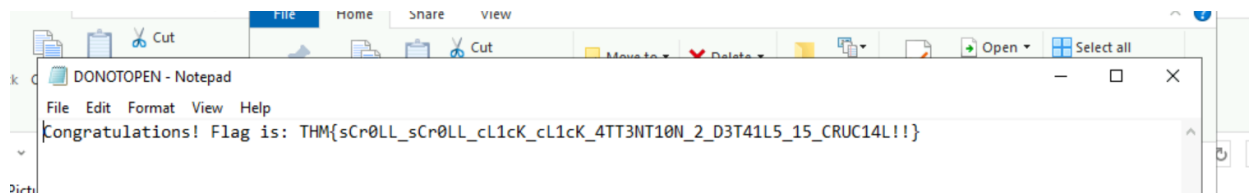
After unzipping, we see that there is a notes file and another zip file. The other zip file is password protected however.



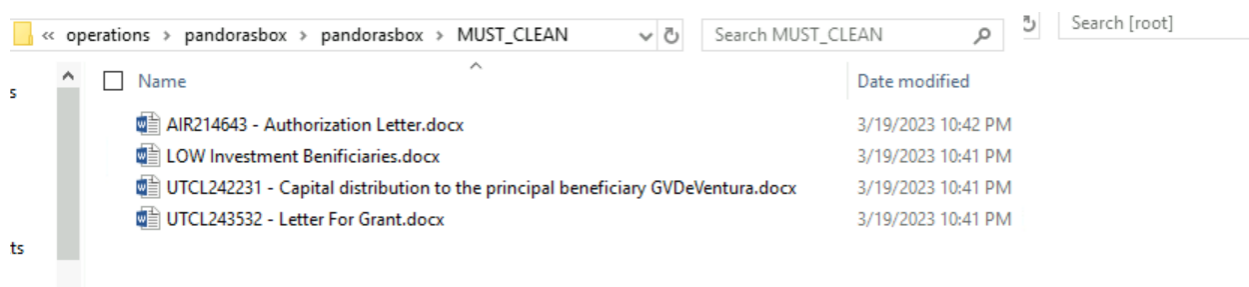
Looking in “notes.txt”, we can see PoC, coordinates, and a password that we can use to solve the questions in the room:

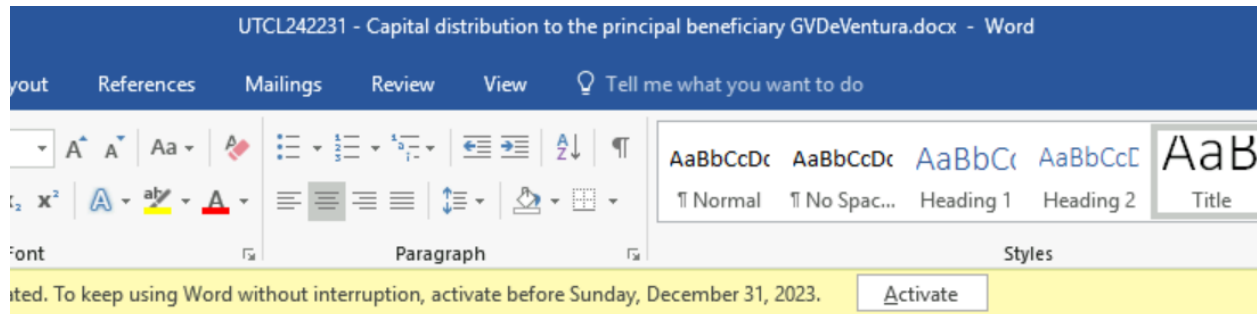


After inputting the password that we discovered above, we can view the password protected zip items:



Beneficiary:





RESOLUTION OF THE EXECUTIVE COMMITTEE OF ALESSIO-DEVENTURA TRUST COMPANY LTD MADE THE 1st DAY OF October 2008.

On written request from the beneficiary.

IT WAS RESOLVED that the Trustee make a capital distribution the sum of \$420,000 as settlement to **the Principal Beneficiary, Mr. Giovanni Vittorio DeVentura** from the trust fund in accordance with the powers conferred on the trustees by Article 7.1 of the trust deed dated 24th day of February 2008.