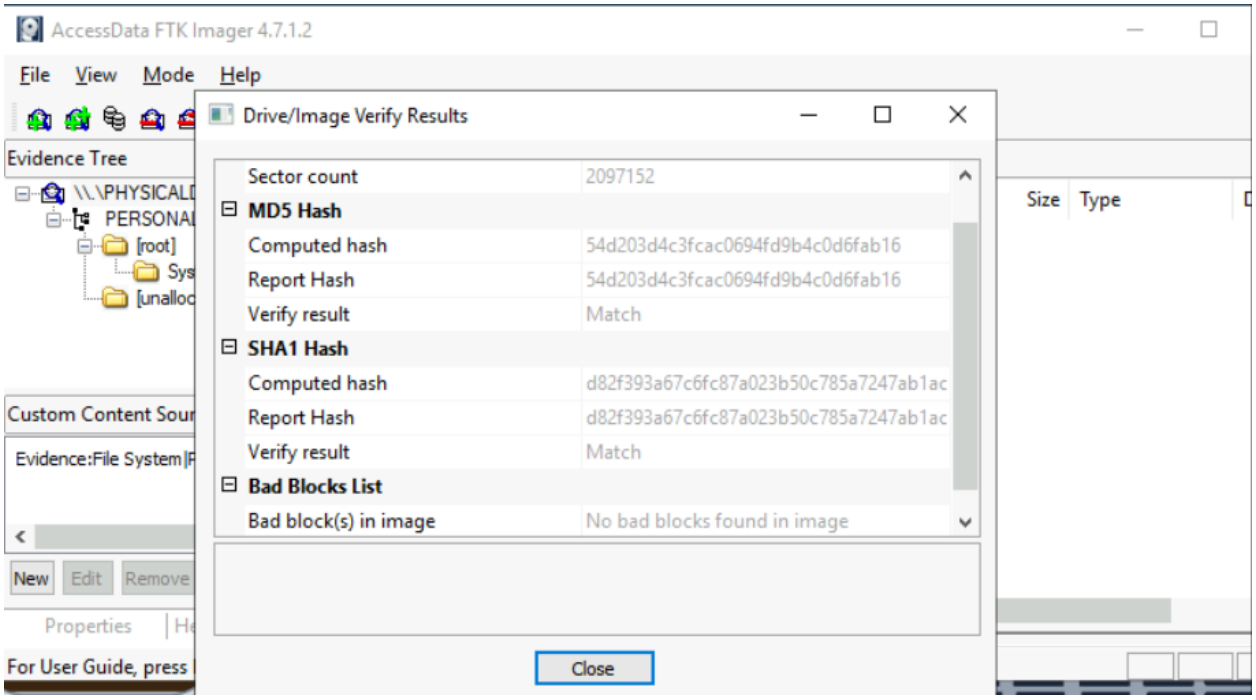
TryHackMe Digital Forensics Case B4DM755

Link:
https://tryhackme.com/room/caseb4dm755

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

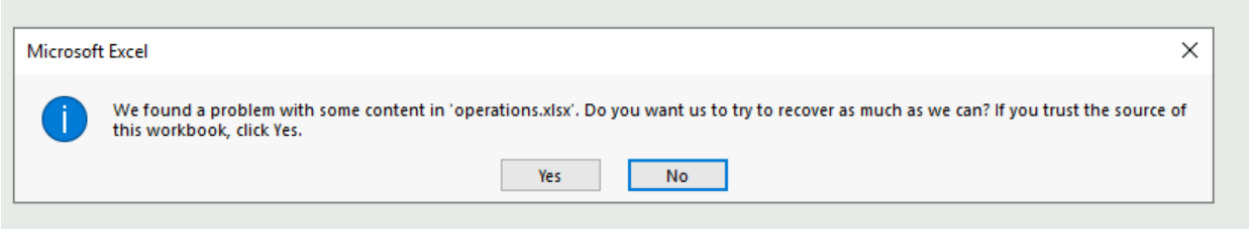


8 hidden files, 6 deleted files, and 3 recovered files. Files with an ‘x’ over the icon are deleted files that are still in memory, and files with a size of 0 are corrupted. The hidden files were counted based off of the equation hiddenFiled = totalFiles - deletedFiles - recoveredFiles

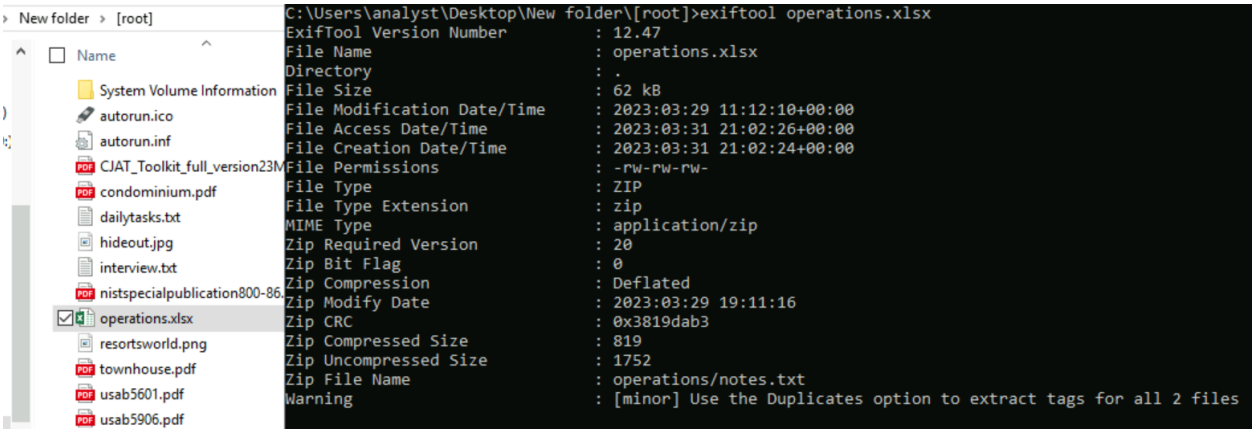
File List

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	

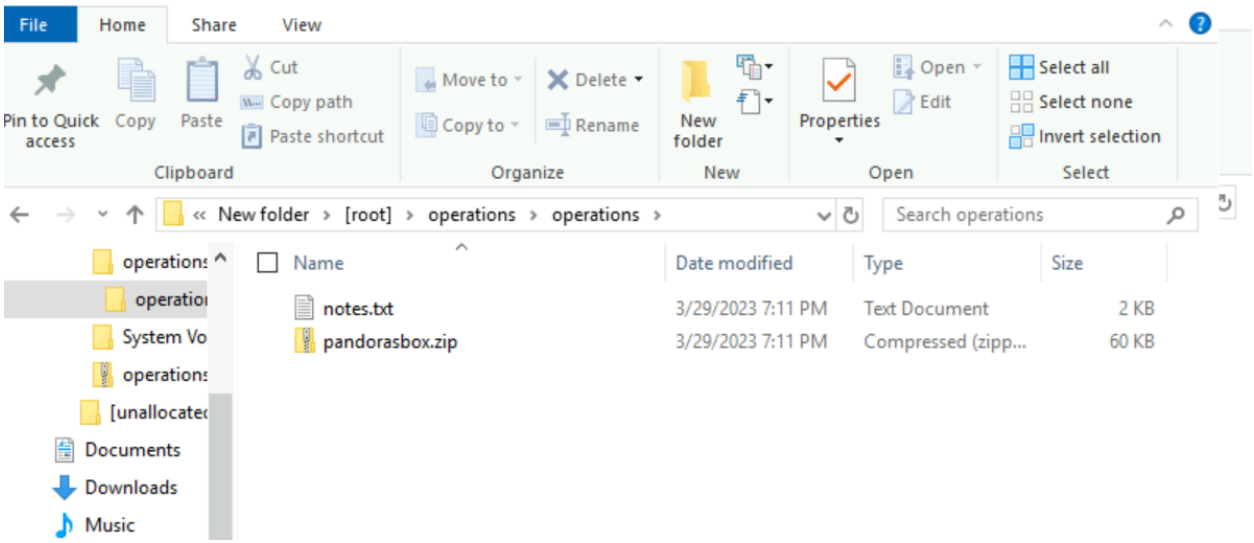
We then export the files to the desktop for ease of viewing. Click through all of the files that are corrupted/wrong extension and try to open them. Utilizing ‘exiftool’, we can see the actual extension of the file, a few pdfs that are supposed to be jpg, then one xlsx that should be a zip. Zip file,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



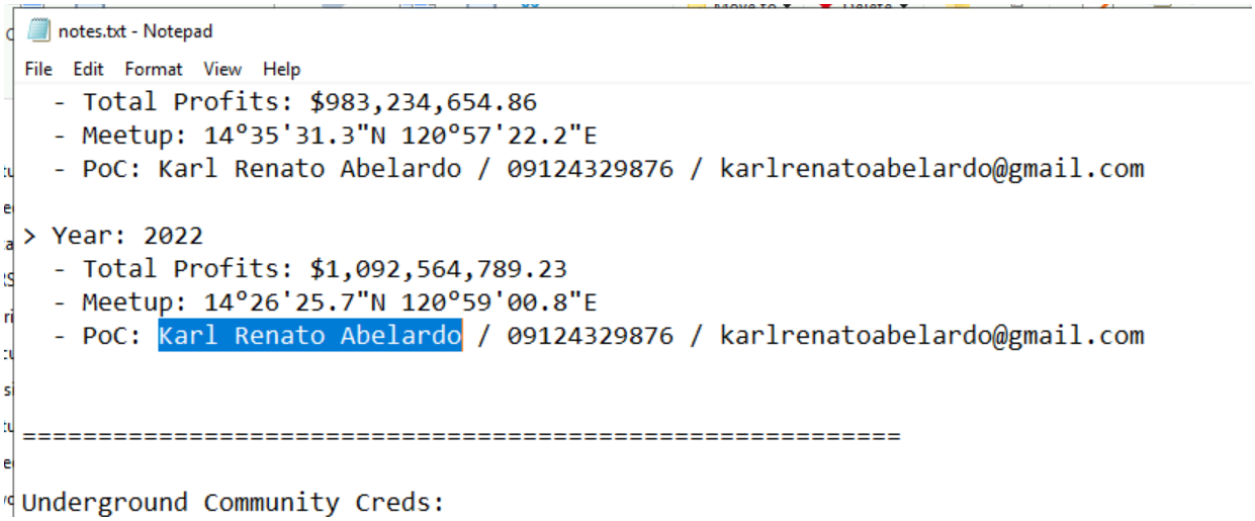
Zip file within exiftool output



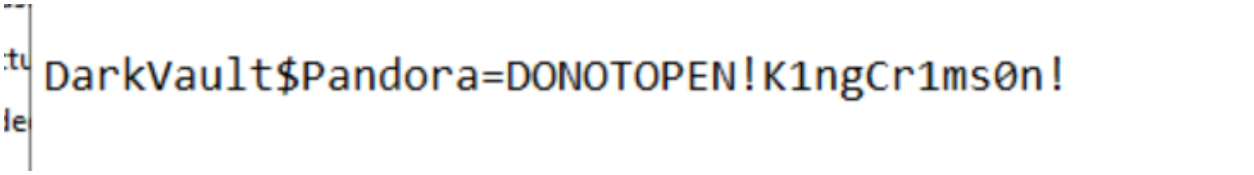
After unzipping, we see that there is a notes file and another zip file. The other zip file is password protected however.



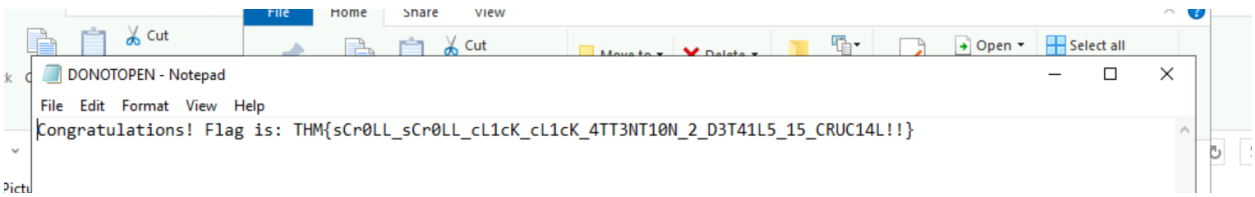
Looking in “notes.txt”, we can see PoC, coordinates, and a password that we can use to solve the questions in the room:

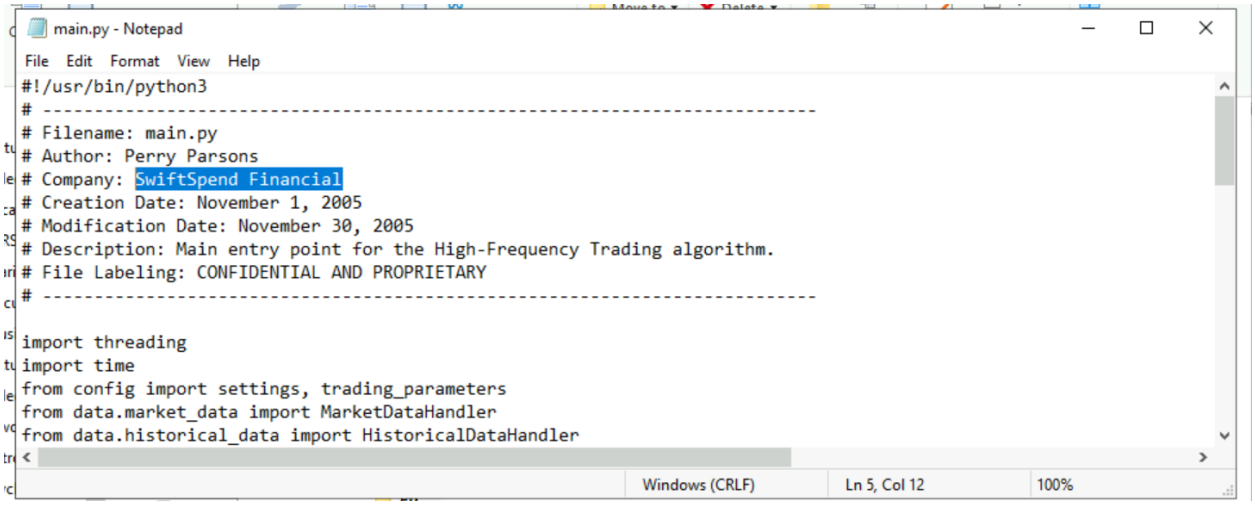


Bottom of the same file:

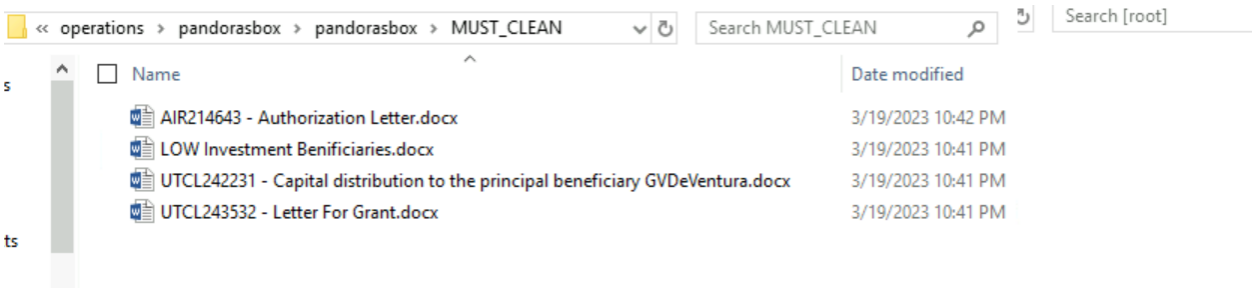


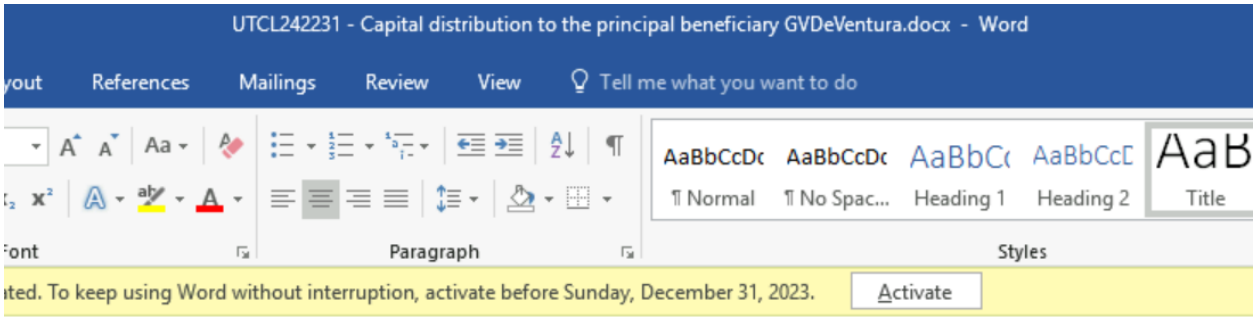
After inputting the password that we discovered above, we can view the password protected zip items:





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.