22i-1725

CY-D

Digital Forensics

Lab04

Tasks:

Naming Convention: i22xxxx_Lab04.pdf

For this practical you should consider yourself to be a Forensic Analyst with a private company that carries out work on behalf of your local Police Service. You should study the scenario below and then carry out your forensic examination as instructed.

Scenario:

You are assisting in the investigation of a suspect named Tony Smith, who is alleged to be involved in passing forged cheques and bank drafts using the pseudonym Michael, Mike, or Mickey McNugget. Smith has been arrested in England, where it is believed, he had gone to meet up with his partner in crime, who is named Roger Jones and from whom he buys counterfeit cheque books. His laptop has been seized and examined in England. The forensic examiner has reported that the laptop is encrypted with Symantec Whole Disk encryption and Smith has refused to provide the password. The investigating officer has been to Smith's home but only a USB device was found.

The USB device has been imaged by a technician in your company and the image files are available for examination inside Evidence.zip file. You should carry out a forensic examination and submit a forensic report on your findings.

The report should include screenshots and explanation for every single step you followed for all the questions. Use the tools and techniques from the previous labs.

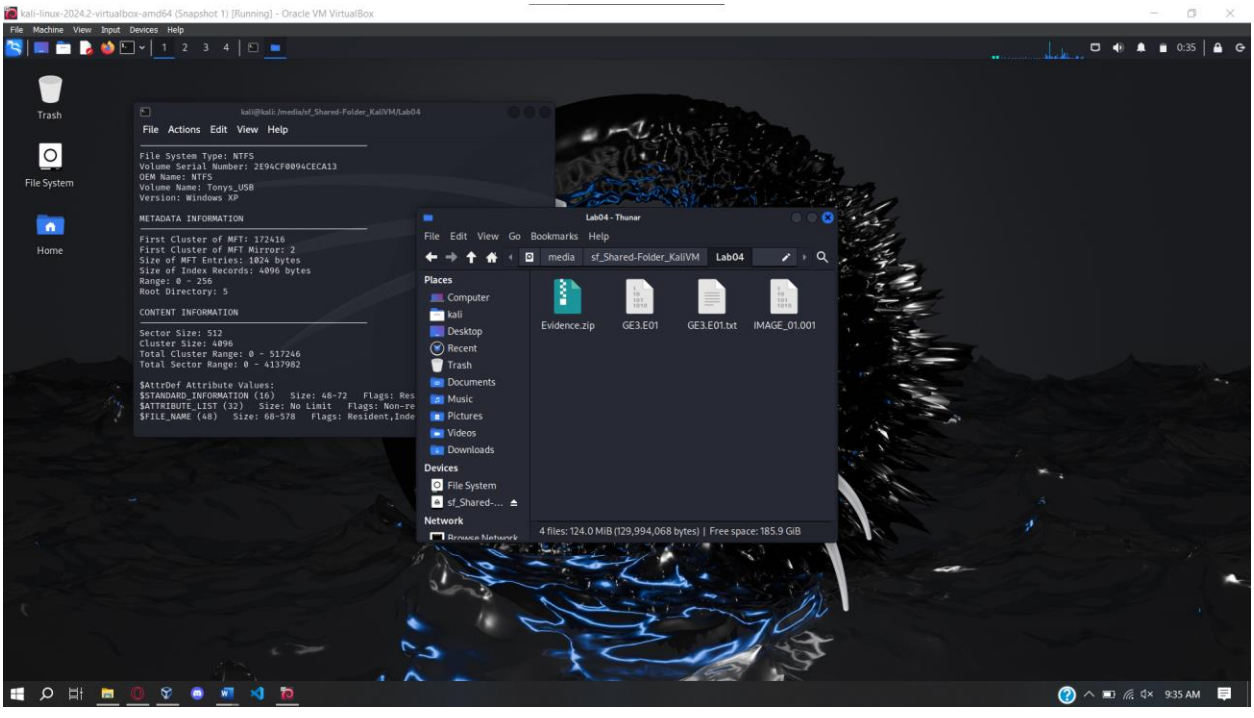
1. What is the Image File Format? (e.g., RAW, AFD, etc.)
2. What is the Volume Serial Number and Volume Name?
3. What is the File System Type? (e.g., FAT, EXT, etc.)
4. How many partitions are there?
5. Name the file with a mismatched extension. Hint: Hexed.it and Gary are close friends who share a lot with me.
6. Use Cipher Identifier if you encounter any encoded text, such as "kHrkn Bqqzon."

7. What is the password for the Password-Protected PDF? Hint: Hexed.it and the devil is in the details.
8. What are the contents of the Password-Protected PDF? Does it relate to the investigation?
9. Write a conclusion based on the investigation above.

Solution

1. What is the Image File Format? (e.g., RAW, AFD, etc.)

   The file format of the image is **EWF**.

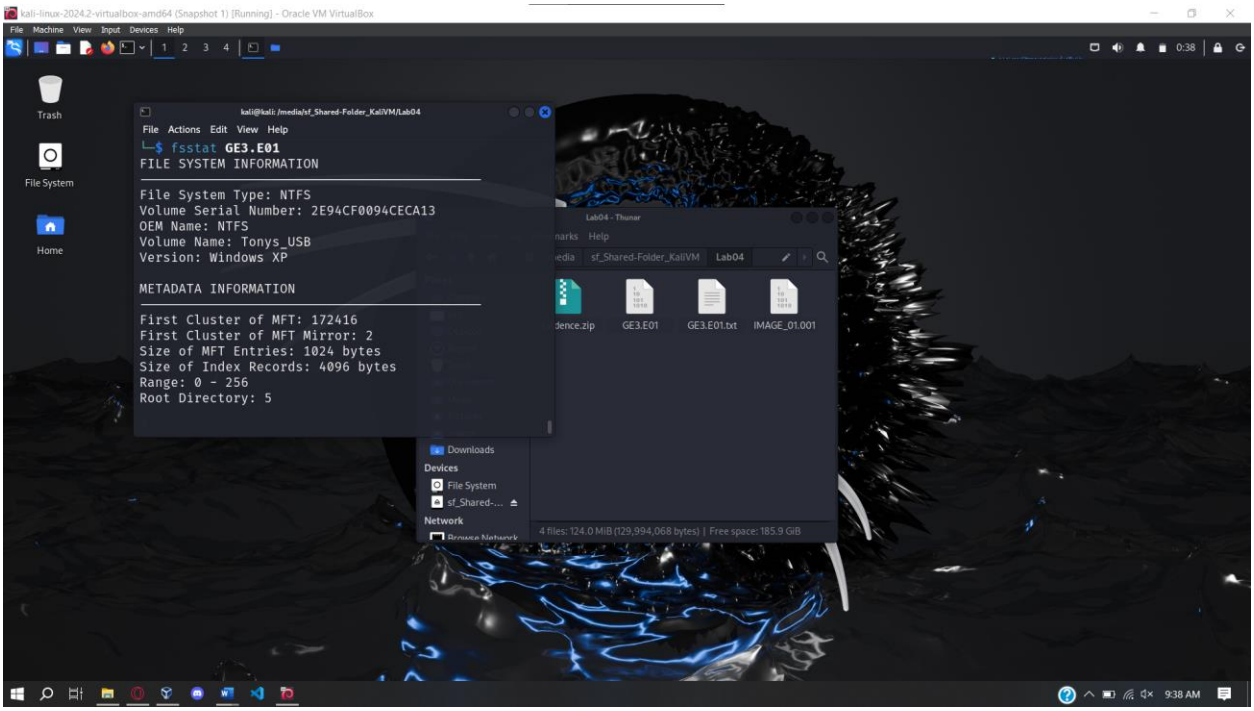


2. What is the Volume Serial Number and Volume Name?

   On using the command **"fsstat GE3.E01"**, the volume serial number and volume name are shown.

   Volume Serial Number = **2E94CF0094CECA13**

   Volume Name = **Tonys_USB**



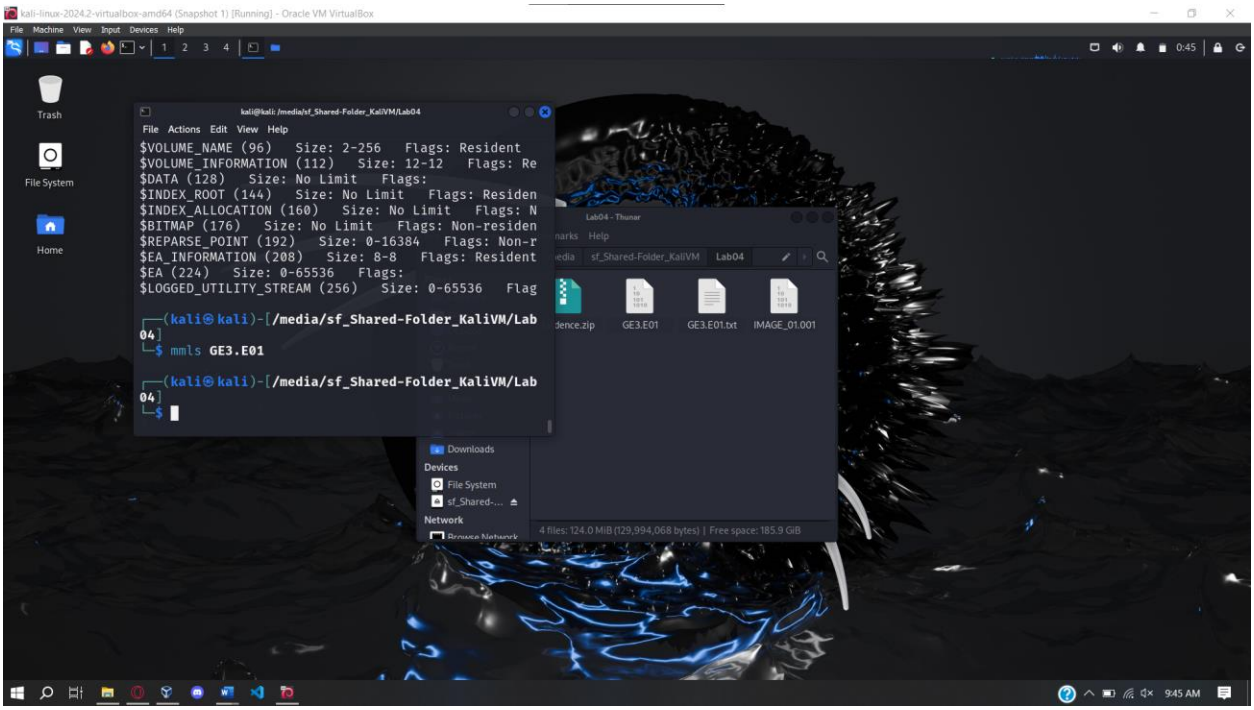
3. What is the File System Type? (e.g., FAT, EXT, etc.)

   The File System Type is **NTFS**, this is also shown by the “fsstat GE3.E01” command.

   (refer to the above screenshot)

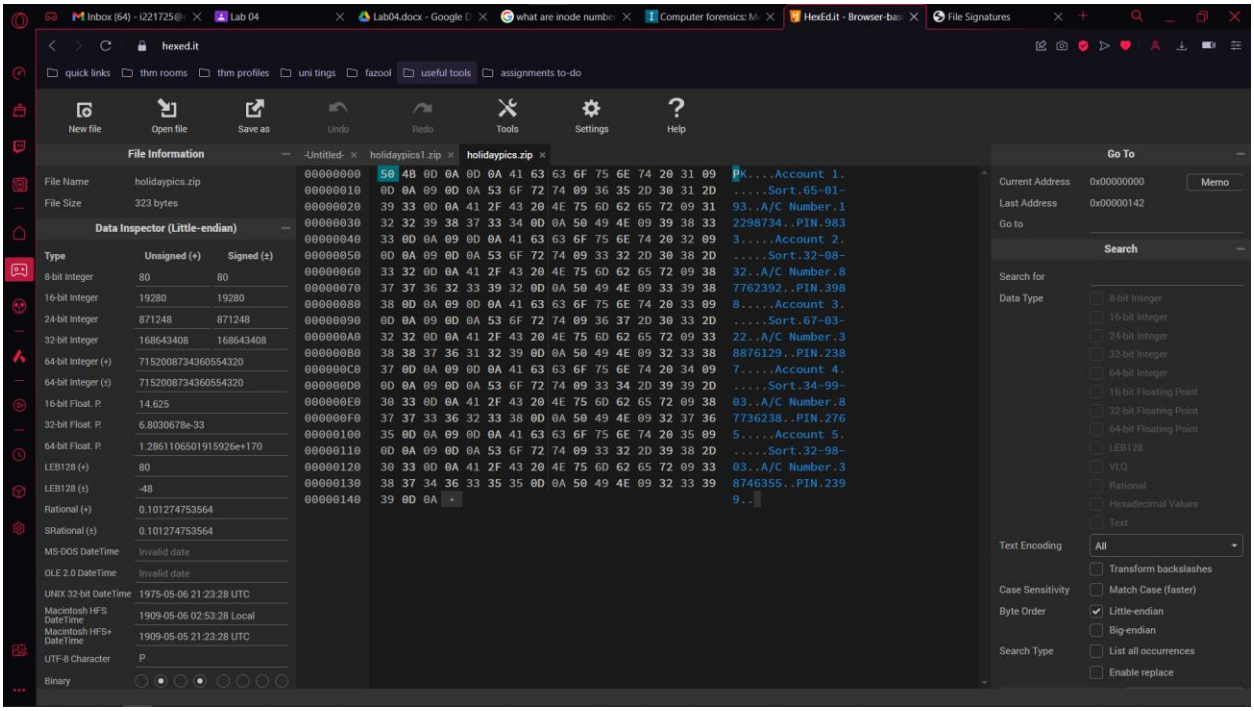
4. How many partitions are there?

   There is only **one partition** in the given GE3.E01 file as no partitions are listed down upon the usage of “**mmls GE3.E01”**.

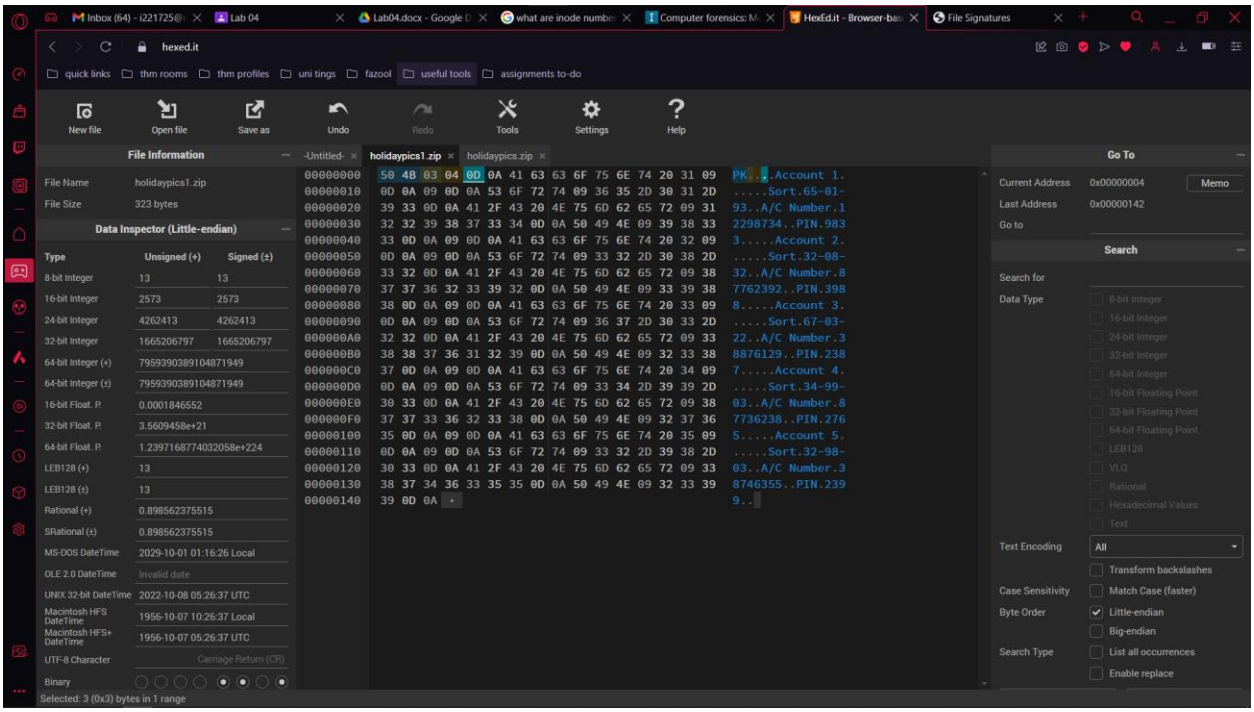


5. Name the file with a mismatched extension. Hint: Hexed.it and Gary are close friends who share a lot with me.

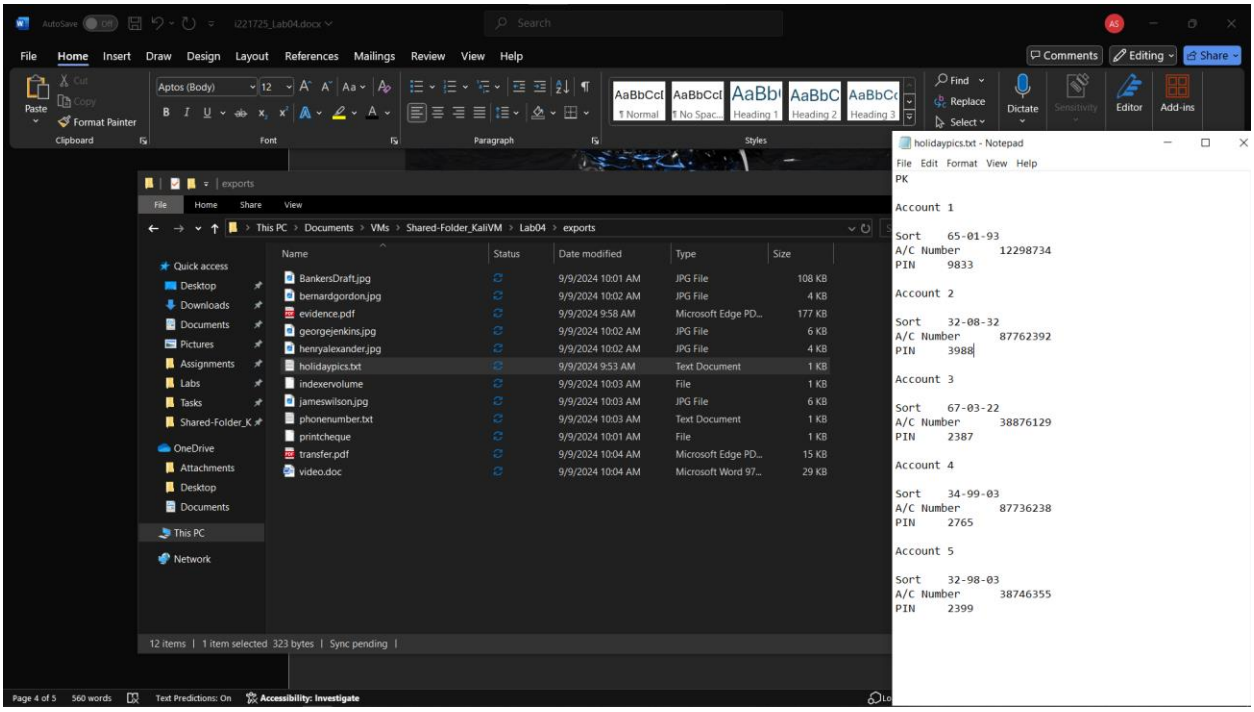
I found the file **“My Holiday Pics.zip”** to have an incorrect header.



The correct magic bytes for a .zip file are **50 4B 03 04.**

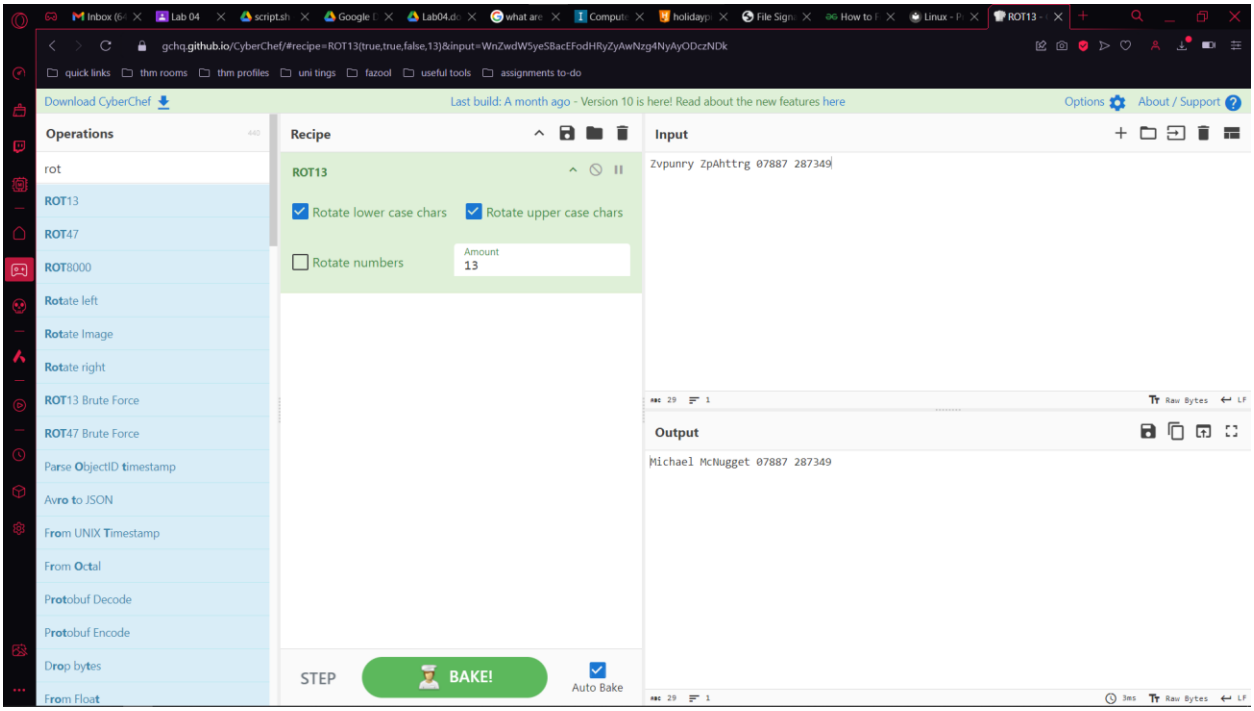


The file didn't open so I changed the extension to .txt and it worked.



6. Use Cipher Identifier if you encounter any encoded text, such as "kHrkn Bqqzon."

The file “**Phone Number.txt**” contained the encoded text.
The Decoded Text is: **Michael McNugget**



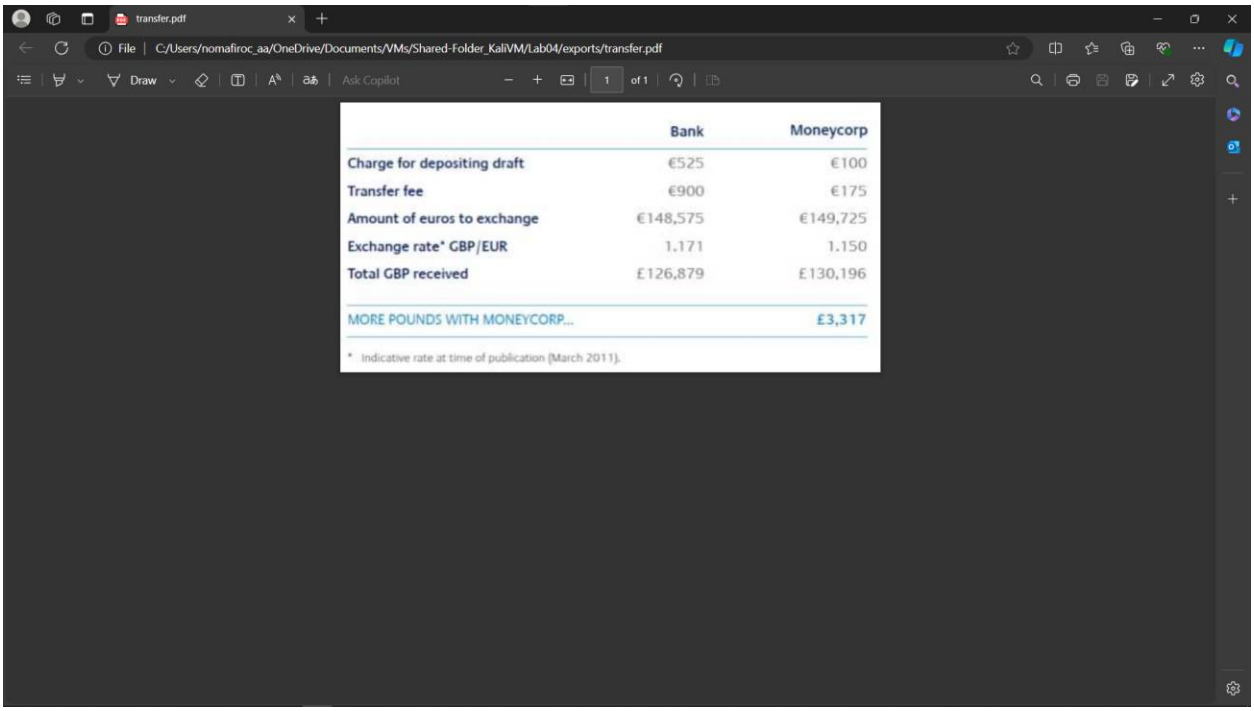
7. What is the password for the Password-Protected PDF? Hint: Hexed.it and the devil is in the details.

   Password = Catchme

8. What are the contents of the Password-Protected PDF? Does it relate to the investigation?

   The extracted content is a transfer receipt containing the amount transferred (148,575 Euros), the transfer rate, exchange rate and charge for depositing draft.

   Yes, this is related to the investigation as it shows the amount transferred and the fact that the bank draft was deposited.



9. Write a conclusion based on the investigation above.

Concluding the investigation, the following evidence was found

- A transfer receipt indicating that a bank draft was deposited.
- 4 photos (.jpg) of signatures of Bernard Gordon, George Jenkins, Henry Alexander and James Wilson.
- A pdf named "**Delete evidence of files on my PC.pdf**" including screenshots of a chat with the topic being on how to remove files from a PC.
- A .txt file hidden by changing the extension to .zip containing 5 account numbers along with passwords. (filename being "**My Holiday Pics.zip"**)
- Micheal McNugget's phone number