Umer Farooq 22i-0518 CY-A

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

Running the img stat command we see the type of the image is ewf.(Expert Witness Format)

```
$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ img_stat GE3.E01
IMAGE FILE INFORMATION
--------------------------------------------
Image Type:             ewf

Size of data in bytes:  2118647808
Sector size:    512
MD5 hash of data:       86844605ec6a53f6e2a0998e29ca2437

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$
```

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

```
┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ file GE3.E01
GE3.E01: EWF/Expert Witness/EnCase image file format

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ fsstat GE3.E01
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 2E94CF0094CECA13
OEM Name: NTFS
Volume Name: Tonys_USB
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 172416
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 517246
Total Sector Range: 0 - 4137982
```

Using the file system stat command we see the Volume serial number and volume name is given above.

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

```
┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ file GE3.E01
GE3.E01: EWF/Expert Witness/EnCase image file format

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ fsstat GE3.E01
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 2E94CF0094CECA13
OEM Name: NTFS
Volume Name: Tonys_USB
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 172416
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 517246
Total Sector Range: 0 - 4137982
```

Using the same command we see that the file system type is NTFS format.

4. How many partitions are there?

```
┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ mmls GE3.E01

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$
```

Since there was no output on this command we see that there are no partitions on this disk and it is a single partition.

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

a lot with me.

Writing a script to extract all the suspicious files from the image.

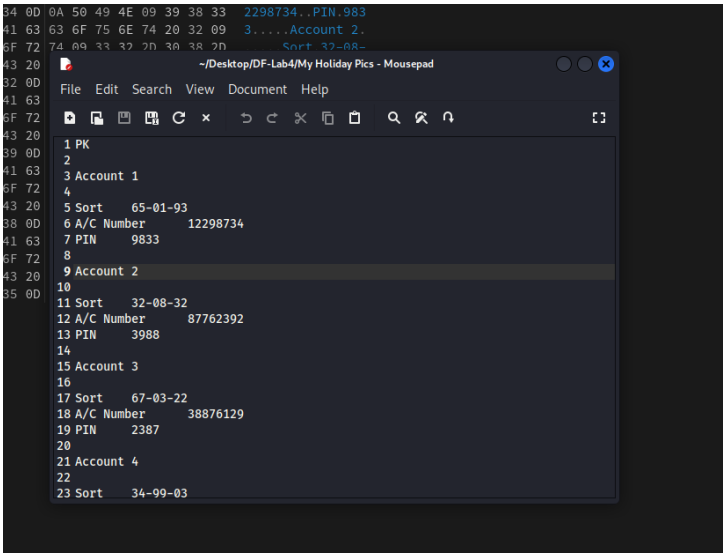
```
┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$ cat script.sh
#!/bin/bash

# Define the image file
image="GE3.E01"

# Extract and save files using icat with their original names
icat -i ewf -f ntfs "$image" 47 > "Delete evidence of files on my PC.pdf"
icat -i ewf -f ntfs "$image" 40 > "For Printing on Cheques"
icat -i ewf -f ntfs "$image" 41 > "Bernard Gordon.jpg"
icat -i ewf -f ntfs "$image" 42 > "George Jenkins.jpg"
icat -i ewf -f ntfs "$image" 43 > "Henry Alexander.jpg"
icat -i ewf -f ntfs "$image" 44 > "James Wilson.jpg"
icat -i ewf -f ntfs "$image" 39 > "My Holiday Pics.zip"
icat -i ewf -f ntfs "$image" 46 > "Phone number.txt"
icat -i ewf -f ntfs "$image" 36 > "System Volume Information"
icat -i ewf -f ntfs "$image" 38 > "IndexerVolumeGuid"
icat -i ewf -f ntfs "$image" 37 > "WPSettings.dat"
icat -i ewf -f ntfs "$image" 48 > "Transfer of Funds.pdf"
icat -i ewf -f ntfs "$image" 49 > "Video Project.doc"

┌──(kali㉿kali)-[~/Desktop/DF-Lab4]
└─$
```

Searching for mismatched magic bytes we see that the zip file magic bytes do not match with the standard.it is actually a morphed version of .docx format.

ZIP	ZLock Pro encrypted ZIP
`50 4B 03 04 14 00 06 00`	`PK.....`
DOCX, PPTX, XLSX	Microsoft Office Open XML Format (OOXML) Document **NOTE:** There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file; look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively. **Trailer:** Look for `50 4B 05 06` (`PK..`) followed by 18 additional bytes at the end of the file.

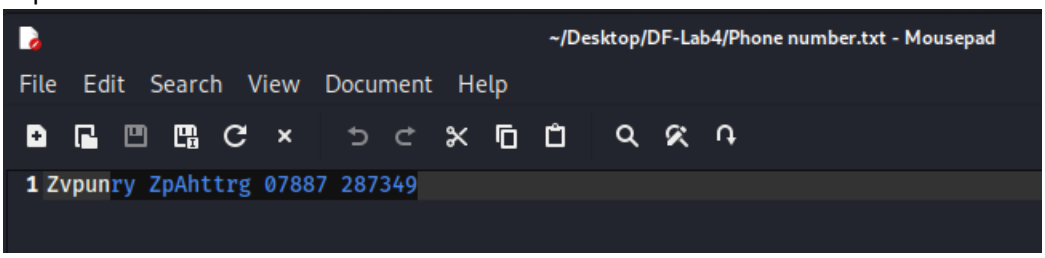
```
-Untitled-   Delete evidence of file...   For Printing on Chequ...   Phone number.txt   Video Project.doc   My Holiday Pics.zip
00000000   50 4B 0D 0A 0D 0A 41 63 63 6F 75 6E 74 20 31 09   PK....Account 1.
00000010   0D 0A 09 0D 0A 53 6F 72 74 09 36 35 2D 30 31 2D   .....Sort.65-01-
00000020   39 33 0D 0A 41 2F 43 20 4E 75 6D 62 65 72 09 31   93..A/C Number.1
00000030   32 32 39 38 37 33 34 0D 0A 50 49 4E 09 39 38 33   2298734..PIN.983
00000040   33 0D 0A 09 0D 0A 41 63 63 6F 75 6E 74 20 32 09   3.....Account 2.
00000050   0D 0A 09 0D 0A 53 6F 72 74 09 33 32 2D 30 38 2D   .....Sort.32-08-
00000060   33 32 0D 0A 41 2F 43 20 4E 75 6D 62 65 72 09 38   32..A/C Number.8
00000070   37 37 36 32 33 39 32 0D 0A 50 49 4E 09 33 39 38   7762392..PIN.398
00000080   38 0D 0A 09 0D 0A 41 63 63 6F 75 6E 74 20 33 09   8.....Account 3.
00000090   0D 0A 09 0D 0A 53 6F 72 74 09 36 37 2D 30 33 2D   .....Sort.67-03-
000000A0   32 32 0D 0A 41 2F 43 20 4E 75 6D 62 65 72 09 33   22..A/C Number.3
000000B0   38 38 37 36 31 32 39 0D 0A 50 49 4E 09 32 33 38   8876129..PIN.238
000000C0   37 0D 0A 09 0D 0A 41 63 63 6F 75 6E 74 20 34 09   7.....Account 4.
000000D0   0D 0A 09 0D 0A 53 6F 72 74 09 33 34 2D 39 39 2D   .....Sort.34-99-
000000E0   30 33 0D 0A 41 2F 43 20 4E 75 6D 62 65 72 09 38   03..A/C Number.8
000000F0   37 37 33 36 32 33 38 0D 0A 50 49 4E 09 32 37 36   7736238..PIN.276
00000100   35 0D 0A 09 0D 0A 41 63 63 6F 75 6E 74 20 35 09   5.....Account 5.
00000110   0D 0A 09 0D 0A 53 6F 72 74 09 33 32 2D 39 38 2D   .....Sort.32-98-
00000120   30 33 0D 0A 41 2F 43 20 4E 75 6D 62 65 72 09 33   03..A/C Number.3
00000130   38 37 34 36 33 35 35 0D 0A 50 49 4E 09 32 33 39   8746355..PIN.239
00000140   39 0D 0A                                          9..
```

Now removing the extension and simply opening it, It opens as a document.

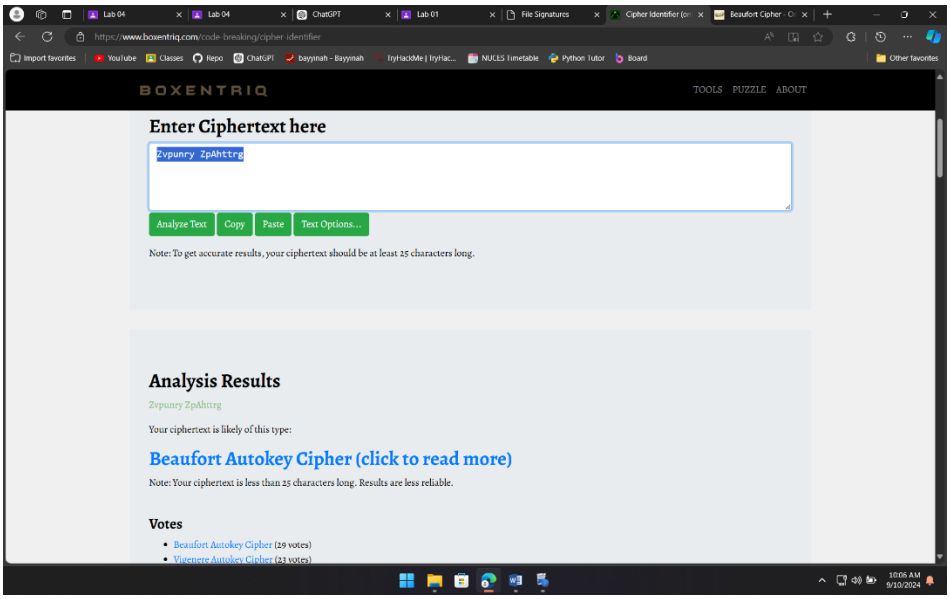


6. Use Cipher Identifier if you encounter any encoded text, such as “kHrkn Bqqzon”

In phonenumber.txt we see



Entering it into the cipher identifier online we see:



Beaufort Autokey Cipher.

7. What is the password for the Password-Protected PDF?

The password for Password-Protected PDF is “Catchme”, we’ll go through the process of finding this password in MFT Analysis Lab, Lab 05.

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

It is an image with a receipt for a transaction.

	Bank	Moneycorp
Charge for depositing draft	€525	€100
Transfer fee	€900	€175
Amount of euros to exchange	€148,575	€149,725
Exchange rate* GBP/EUR	1.171	1.150
Total GBP received	£126,879	£130,196
MORE POUNDS WITH MONEYCORP...		£3,317

* Indicative rate at time of publication (March 2011).

9. Write a conclusion based on the investigation above.

In conclusion we have found multiple incriminating evidences against the owner of this USB as it contains much of the data the criminal and how he performed his crimes.