



**National University**  
of computer and emerging sciences

## Lab 04

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

*Submitted to: Sir Ubaid Ullah Bhai*

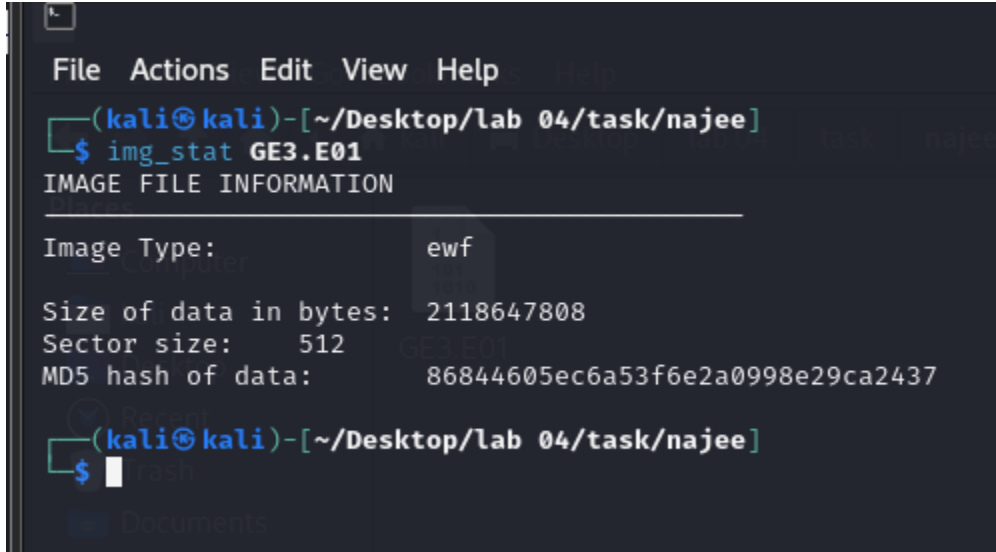
Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

---

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

The file was EWF in format, as we can see in the ss, the command used was `img_stat`



```
(kali㉿kali)-[~/Desktop/lab 04/task/najee]
$ img_stat GE3.E01
IMAGE FILE INFORMATION
-----
Image Type:                ewf
Size of data in bytes:     2118647808
Sector size:               512
MD5 hash of data:          86844605ec6a53f6e2a0998e29ca2437

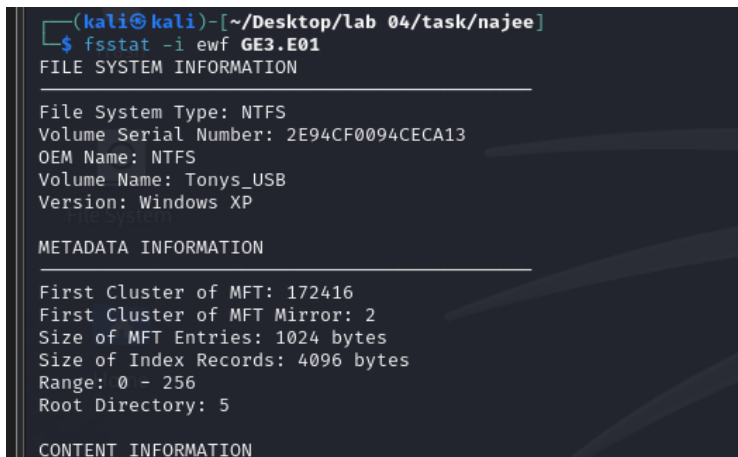
(kali㉿kali)-[~/Desktop/lab 04/task/najee]
$
```

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

The volume serial number is 2E94CF0094CECA13 and name is Tonys\_USB.

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

NTFS



```
(kali㉿kali)-[~/Desktop/lab 04/task/najee]
$ fsstat -i ewf 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
```

#### 4. How many partitions are there?

There are no partitions because mmls give no output.

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

```
(kali@kali)-[~/Desktop/Lab 04/task/najee]
$ fls -i ewf GE3.E01
r/r 4-128-1: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-4: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
r/r 2-128-1: $LogFile
r/r 0-128-6: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 10-128-4: $UpCase:$Info
r/r 3-128-3: $Volume
r/r 45-128-1: Bankers Draft.jpg
r/r 47-128-1: Delete evidence of files on my PC.pdf
d/d 40-144-1: For Printing on Cheques
r/r 39-128-1: My Holiday Pics.zip
r/r 46-128-1: Phone number.txt
d/d 36-144-1: System Volume Information
r/r 48-128-1: Transfer of Funds.pdf
r/r 49-128-1: Video Project.doc
V/V 256: $OrphanFiles
```

I extracted the file using icat command to extract the My Holiday pics.zip, and opened it in hexed.it

After that I changed the extension to txt.

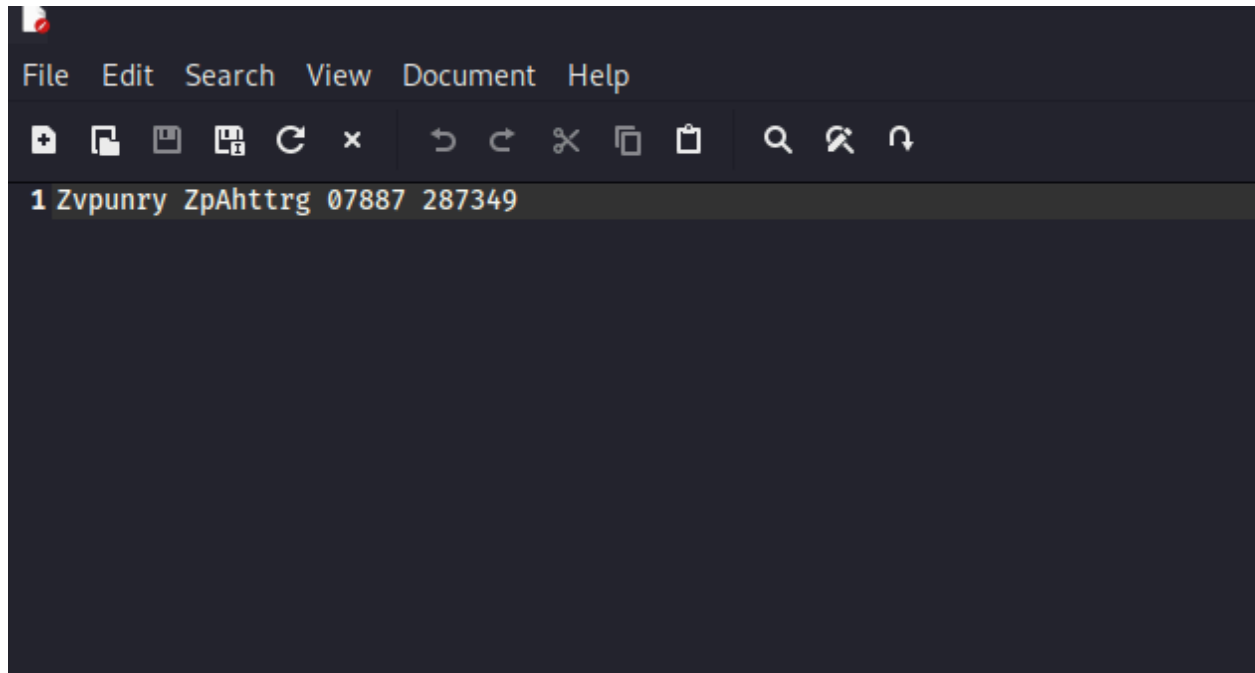
And it had this

```
2
3 Account 1
4
5 Sort    65-01-93
6 A/C Number    12298734
7 PIN    9833
8
9 Account 2
10
11 Sort    32-08-32
12 A/C Number    87762392
13 PIN    3988
14
15 Account 3
16
17 Sort    67-03-22
18 A/C Number    38876129
19 PIN    2387
20
21 Account 4
22
23 Sort    34-99-03
24 A/C Number    87736238
25 PIN    2765
26
27 Account 5
28
29 Sort    32-98-03
30 A/C Number    38746355
31 PIN    2399
32
```

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

The phone number.txt had a name that after decrypting came Michael McNugget

So the text was



Michael McNugget 07887 287349

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

The password was “Catchme”

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

It had the transactions of money.

	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
<b>MORE POUNDS WITH MONEYCORP...</b>		<b>£3,317</b>
* Indicative rate at time of publication (March 2011).		

## 9. Write a conclusion based on the investigation above.

The case included some evidence of Some Transactions of money. All the evidence was presented in the report. So the conclusion was that The Suspect is guilty given the proof of These illegal Transactions.