National University
of computer and emerging sciences

Lab 05

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah

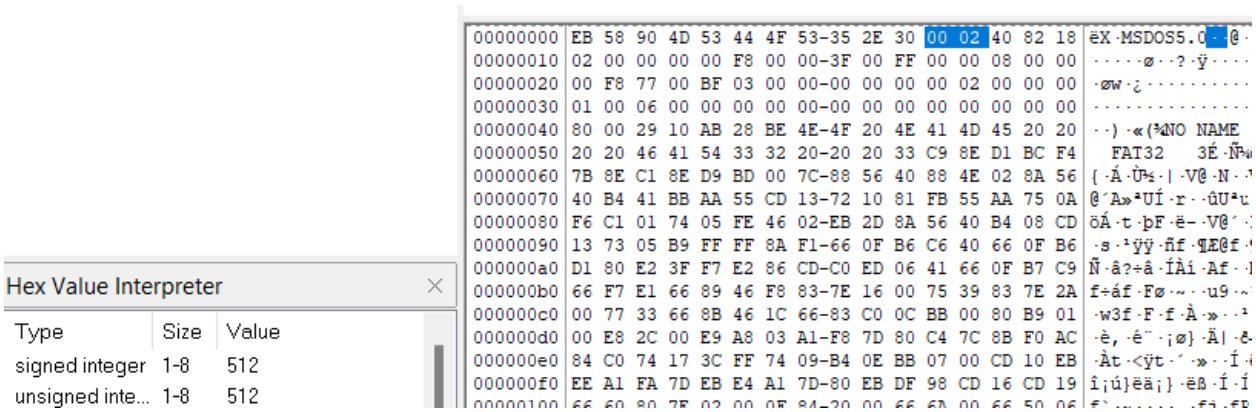
Department of Cyber Security BS(CY)

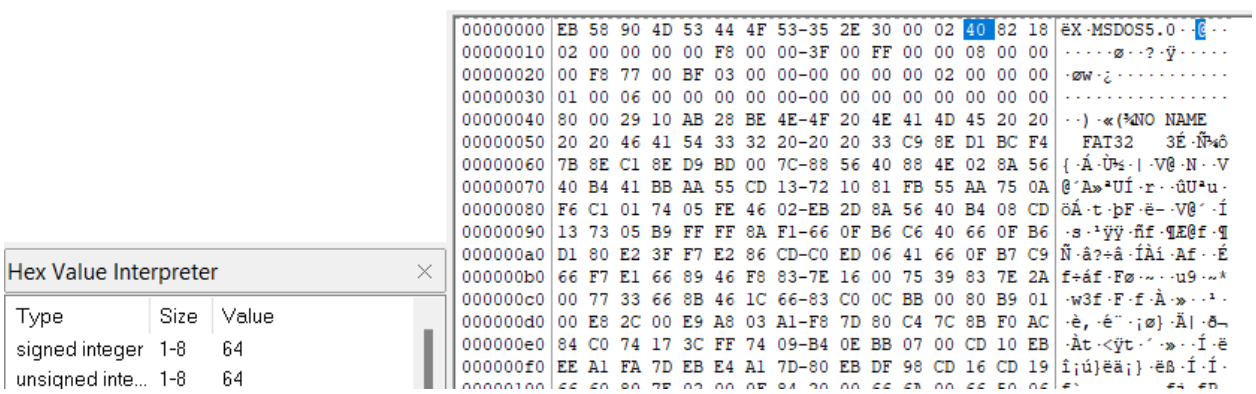
FAST-NUCES Islamabad

Q1 . Find Byte per Sector and Sectors per Cluster for Image File? Pay attention to the endianness.

The bytes per sector is taken by 0x0B and 0x0C which is 512 bytes in decimal.

The Sector per Cluster is taken by 0x0D which is 64 bytes in decimal.





Q2 . Show and explain where the volume label is stored by the FAT file system?

It's USB0-FAT-06 which was the first 11 bytes.

```
0 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06 ·
0 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 00 ·····Åe.Y···
```

Q3 . Check the FAT root directory, explain how the filename and extension can be extracted from these entries?

The 0x08 0x09 and 0x0A byte of each entry of file tells the Extension and 0x00 to 0x0A tells the Short name of the file.

The offsets start from the 3rd line.

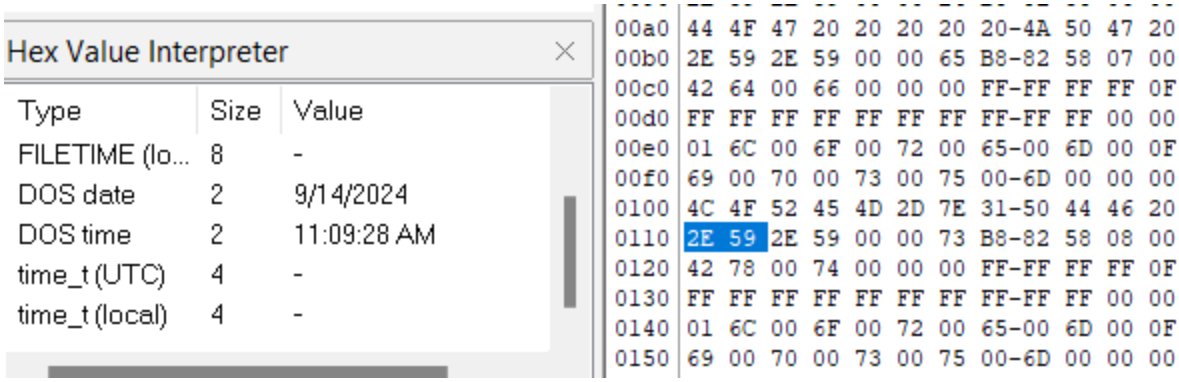
And the Large name is the next two bytes before the small name of the File entry.

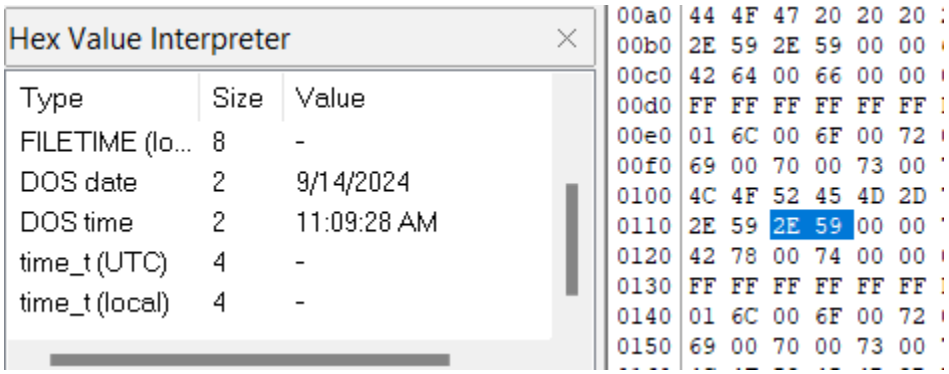
```
01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 ·l·o·r·e·m····-·
69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i·p·s·u·m···.·p·
4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM-~1PDF ·vëe
2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 .Y.Y··s¸·X··C-··
```

Q4 . Determine the date and time when the file “lorem-ipsum.pdf” was created / modified based on the root entry hex data?

The 0x10 and 0x11 tell the Created time which is 9/14/2024 11:09:28 AM.

The 0x12 and 0x13 tell the Modified time which is 9/14/2024 11:09:28 AM which is the same.





Q5 . Compute the RAM, Drive and File slack for the file "lorem-ipsum.pdf" then extract the slack and confirm that your computations are correct?

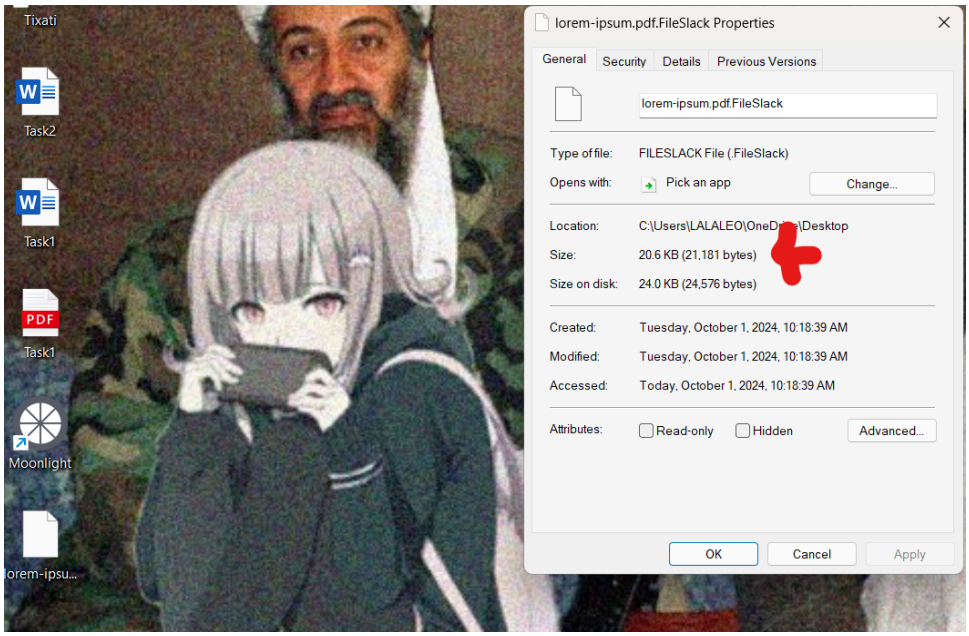
RAM SLACK = 512 - (77123 % 512) = 189.

Drive SLACK = 32768 - (77123 % 32768) = 21181.

File SLACK = (((77123 / 32768)+1) * 32768) - 77123

((2 + 1) * 32768) - 77123 = 21181

I saved the file slack of the file to my drive and the file slack size was 21181 bytes



Q6 . Analyze the root directory entry, compute the start and end offsets where the data of the file is located and manually extract the file using a hex editor. Compute hash values for the original file (i.e., original copy that you still have on your laptop PC) and the manually extracted file (i.e., from the USB) and verify if they match.

```
000000e0 | 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 | ·l·o·r·e·m····-·
000000f0 | 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 | i·p·s·u·m···.·p·
00000100 | 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 | LOREM-~1PDF ·vëe
00000110 | 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 | .Y.Y··s¸·X··C-··
00000120 | 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF | Bx·t···ÿÿÿÿ··¸ÿÿ
```

```
00f0 | 69 00 70 00 73 00 75 00-6D 00 00 00 2
0100 | 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 0
0110 | 2E 59 2E 59 00 00 73 B8-82 58 08 00 4
0120 | 42 78 00 74 00 00 00 FF-FF FF FF 0F 0
```

This shows that the DIR_FstClusHI is 0 so it is a FAT12/16 File volume.

Type	Size	Value
signed integer	1-8	8
unsigned inte...	1-8	8
FILETIME (U...	8	-

```
00d0 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF
00e0 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00
00f0 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00
0100 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65
0110 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00
```

And the starting cluster is 8.

Size is 77123

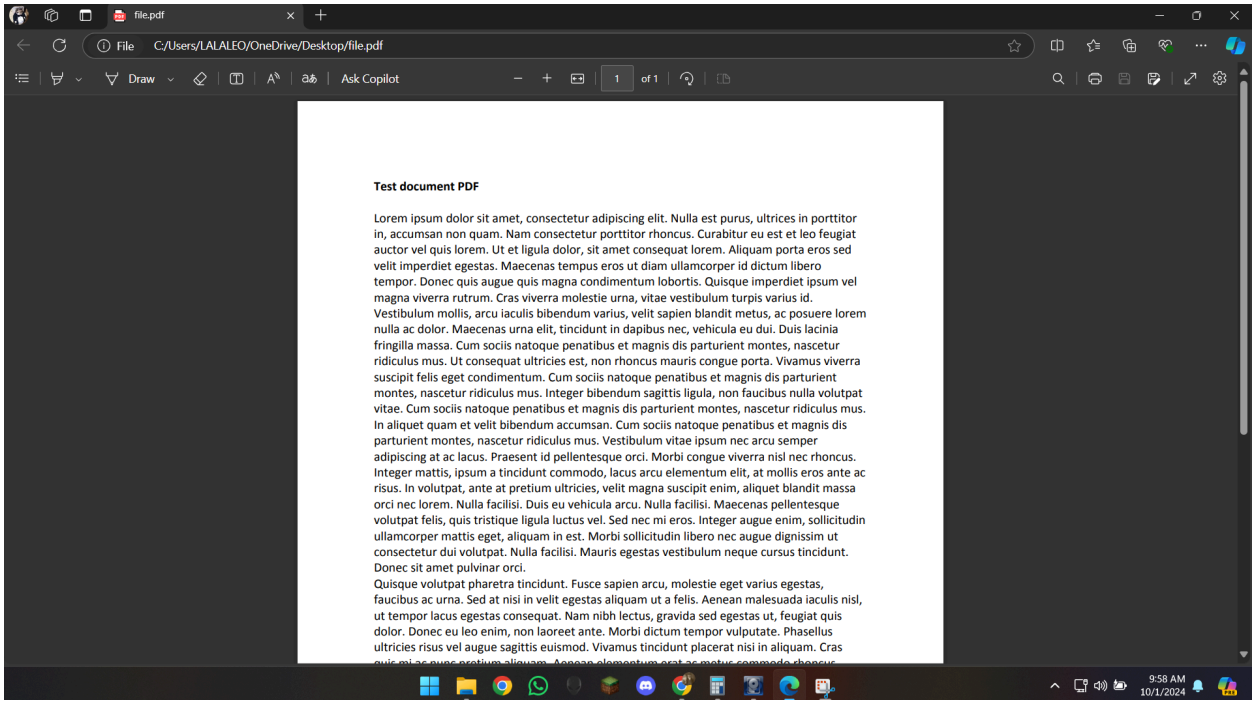
Hex Value Interpreter

Type	Size	Value
signed integer	1-8	77,123
unsigned inte...	1-8	77,123
FILETIME (U...	8	-
FILETIME (lo...	8	-
DOS date	2	-

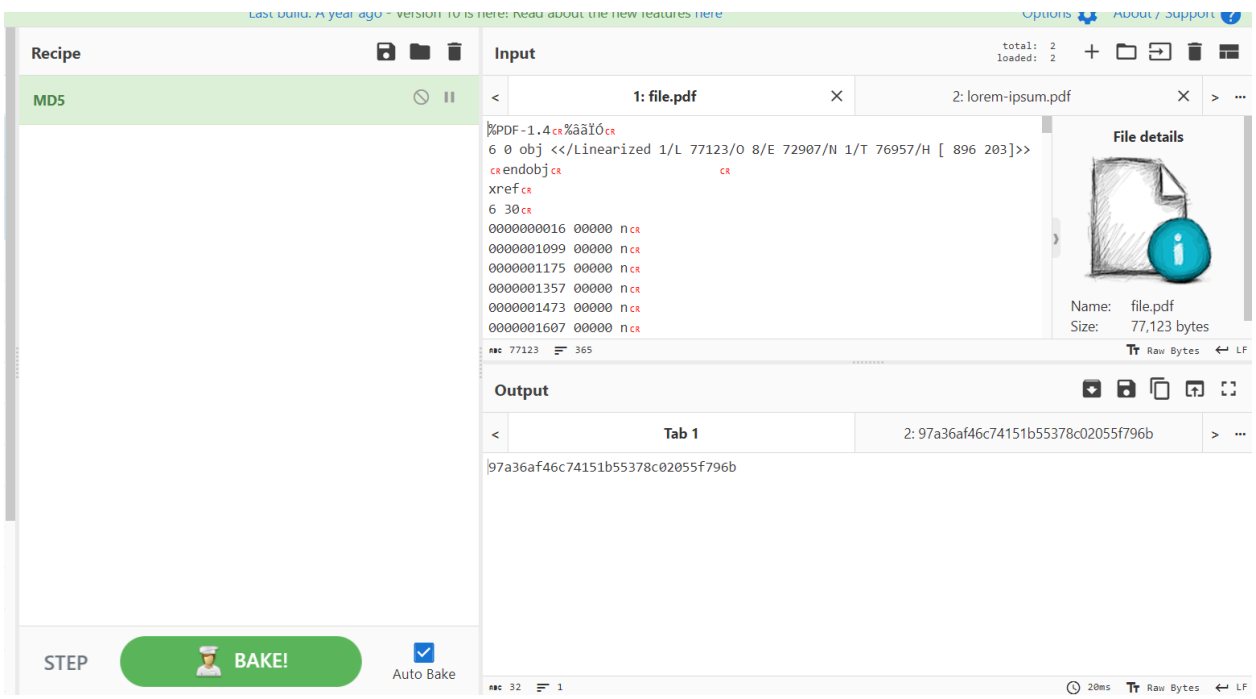
```
00b0 2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00 .Y.Y··e¸·X·····
00c0 42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF Bd·f···ÿÿÿÿ···ÿÿ
00d0 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
00e0 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 ·l·o·r·e·m····–·
00f0 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i·p·s·u·m···.·p·
0100 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM-~1PDF ·vëe
0110 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 .Y.Y··s¸·X··C-··
0120 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF Bx·t···ÿÿÿÿ··¸ÿÿ
0130 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
0140 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00 ·l·o·r·e·m···¸-··
```

```
30000 25 50 44 46 2D 31 2E 34-0D 25 E2 E3 CF D3 0D 0A %PDF-1.4·%âãÏÓ··
30010 36 20 30 20 6F 62 6A 20-3C 3C 2F 4C 69 6E 65 61 6 0 obj <</Linea
30020 72 69 7A 65 64 20 31 2F-4C 20 37 37 31 32 33 2F rized 1/L 77123/
30030 4F 20 38 2F 45 20 37 32-39 30 37 2F 4E 20 31 2F O 8/E 72907/N 1/
30040 54 20 37 36 39 35 37 2F-48 20 5B 20 38 39 36 20 T 76957/H [ 896
30050 32 30 33 5D 3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20 203]>>·endobj·
30060 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
30070 20 20 0D 0A 78 72 65 66-0D 0A 36 20 33 30 0D 0A   ··xref··6 30··
30080 30 30 30 30 30 30 30 30-31 36 20 30 30 30 30 30 0000000016 00000
30090 20 6E 0D 0A 30 30 30 30-30 30 31 30 39 39 20 30  n··0000001099 0
300a0 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 31 0000 n··00000011
300b0 37 35 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 75 00000 n··0000
300c0 30 30 31 33 35 37 20 30-30 30 30 30 20 6E 0D 0A 001357 00000 n··
300d0 30 30 30 30 30 30 31 34-37 33 20 30 30 30 30 30 0000001473 00000
300e0 20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30  n··0000001607 0
300f0 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 38 0000 n··00000018
30100 39 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 90 00000 n··0000
```

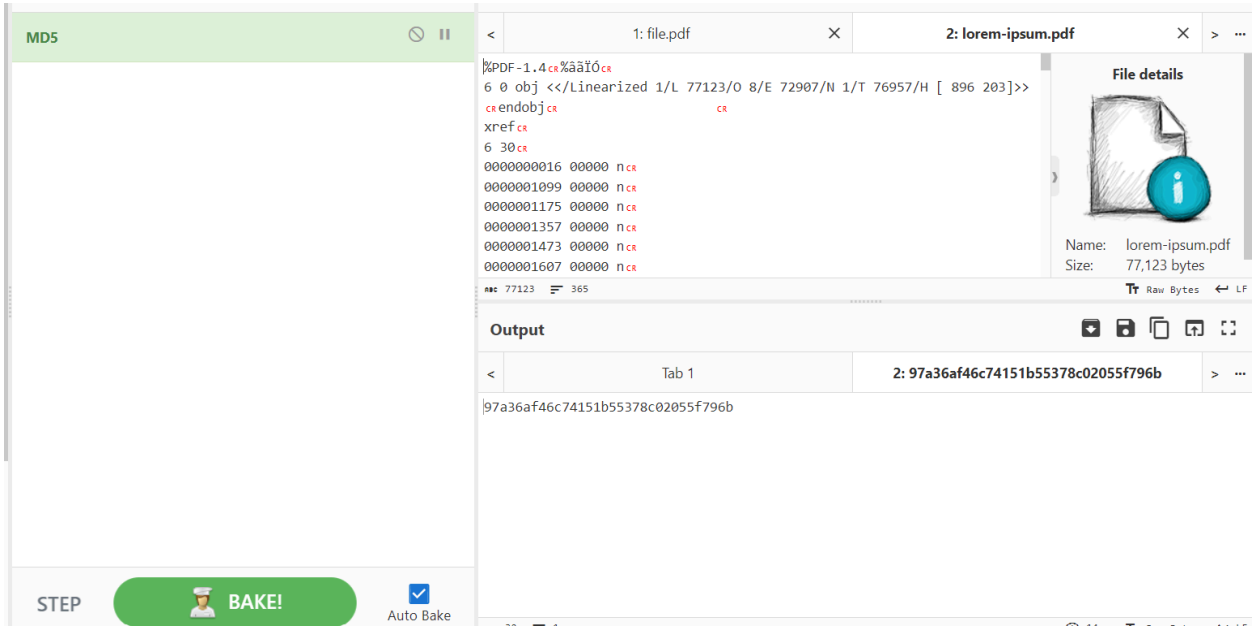
So I selected the file bytes, and made a file out of it.



Now comparing the Files in cyber chef



Md5 of first file



Md5 of 2nd file.

And both are the same, so The file I carved was Accurate.