



**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.

Hex Value Interpreter			
Type	Size	Value	
signed integer	1-8	512	
unsigned inte...	1-8	512	

00000000	EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 82 18	EX-MSDOS5.0
00000010	02 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00	.....?..y.....
00000020	00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00	...w...z.....
00000030	01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00	.....
00000040	80 00 29 10 AB 28 BE 4E-4F 20 4E 41 4D 45 20 20	..) «(%NO NAME
00000050	20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4	FAT32 3E.N
00000060	7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56	{.Ä.Ü.   .VØ .N .
00000070	40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A	@'A»*UÍ .r .úU*u
00000080	F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD	öÄ .t .pF .ë - .VØ' .
00000090	13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6	.s .ÿÿ .ñf .Æ@f .
000000a0	D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9	Ñ .ä?+ä .íÄi .Af .
000000b0	66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A	f+áf .Fø .~ .u9 .
000000c0	00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01	.w3f .F .f .Ä » .
000000d0	00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC	.è , .é .  ø} .Ä   .ø
000000e0	84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB	.Ät .<y t . ' » . .í .ë
000000f0	EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19	í;ú}ëä; } .ëB .í .í
00000100	66 60 80 7F 02 00 0F 84-20 00 66 60 00 66 60 06	f . . . . . fÄ .Fø

Hex Value Interpreter			
Type	Size	Value	
signed integer	1-8	64	
unsigned inte...	1-8	64	

00000000	EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 82 18	EX-MSDOS5.0
00000010	02 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00	.....?..y.....
00000020	00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00	...w...z.....
00000030	01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00	.....
00000040	80 00 29 10 AB 28 BE 4E-4F 20 4E 41 4D 45 20 20	..) «(%NO NAME
00000050	20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4	FAT32 3E.N
00000060	7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56	{.Ä.Ü.   .VØ .N .V
00000070	40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A	@'A»*UÍ .r .úU*u
00000080	F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD	öÄ .t .pF .ë - .VØ' .í
00000090	13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6	.s .ÿÿ .ñf .Æ@f .¶
000000a0	D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9	Ñ .ä?+ä .íÄi .Af .É
000000b0	66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A	f+áf .Fø .~ .u9 .*
000000c0	00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01	.w3f .F .f .Ä » .
000000d0	00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC	.è , .é .  ø} .Ä   .ø
000000e0	84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB	.Ät .<y t . ' » . .í .ë
000000f0	EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19	í;ú}ëä; } .ëB .í .í
00000100	66 60 80 7F 02 00 0F 84-20 00 66 60 00 66 60 06	f . . . . . fÄ .Fø

## 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	.....Ae.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-ipsu.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.

Hex Value Interpreter

Type	Size	Value
FILETIME (lo...	8	-
DOS date	2	9/14/2024
DOS time	2	11:09:28 AM
time_t (UTC)	4	-
time_t (local)	4	-

00a0	44	4F	47	20	20	20	20	20	4A	50	47	20
00b0	2E	59	2E	59	00	00	65	B8	82	58	07	00
00c0	42	64	00	66	00	00	00	FF	FF	FF	FF	0F
00d0	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00
00e0	01	6C	00	6F	00	72	00	65	00	6D	00	0F
00f0	69	00	70	00	73	00	75	00	6D	00	00	00
0100	4C	4F	52	45	4D	2D	7E	31	50	44	46	20
0110	2E	59	2E	59	00	00	73	B8	82	58	08	00
0120	42	78	00	74	00	00	00	FF	FF	FF	FF	0F
0130	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00
0140	01	6C	00	6F	00	72	00	65	00	6D	00	0F
0150	69	00	70	00	73	00	75	00	6D	00	00	00

Hex Value Interpreter

Type	Size	Value
FILETIME (lo...	8	-
DOS date	2	9/14/2024
DOS time	2	11:09:28 AM
time_t (UTC)	4	-
time_t (local)	4	-

00a0	44	4F	47	20	20	20
00b0	2E	59	2E	59	00	00
00c0	42	64	00	66	00	00
00d0	FF	FF	FF	FF	FF	FF
00e0	01	6C	00	6F	00	72
00f0	69	00	70	00	73	00
0100	4C	4F	52	45	4D	2D
0110	2E	59	2E	59	00	00
0120	42	78	00	74	00	00
0130	FF	FF	FF	FF	FF	FF
0140	01	6C	00	6F	00	72
0150	69	00	70	00	73	00

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

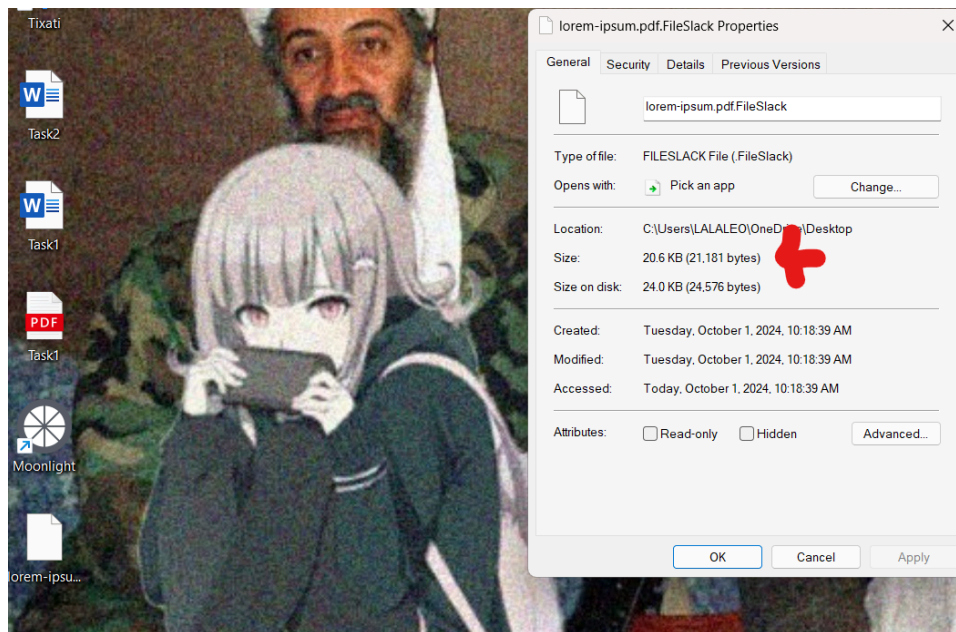
**RAM SLACK** =  $512 - (77123 \% 512) = 189$ .

**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.

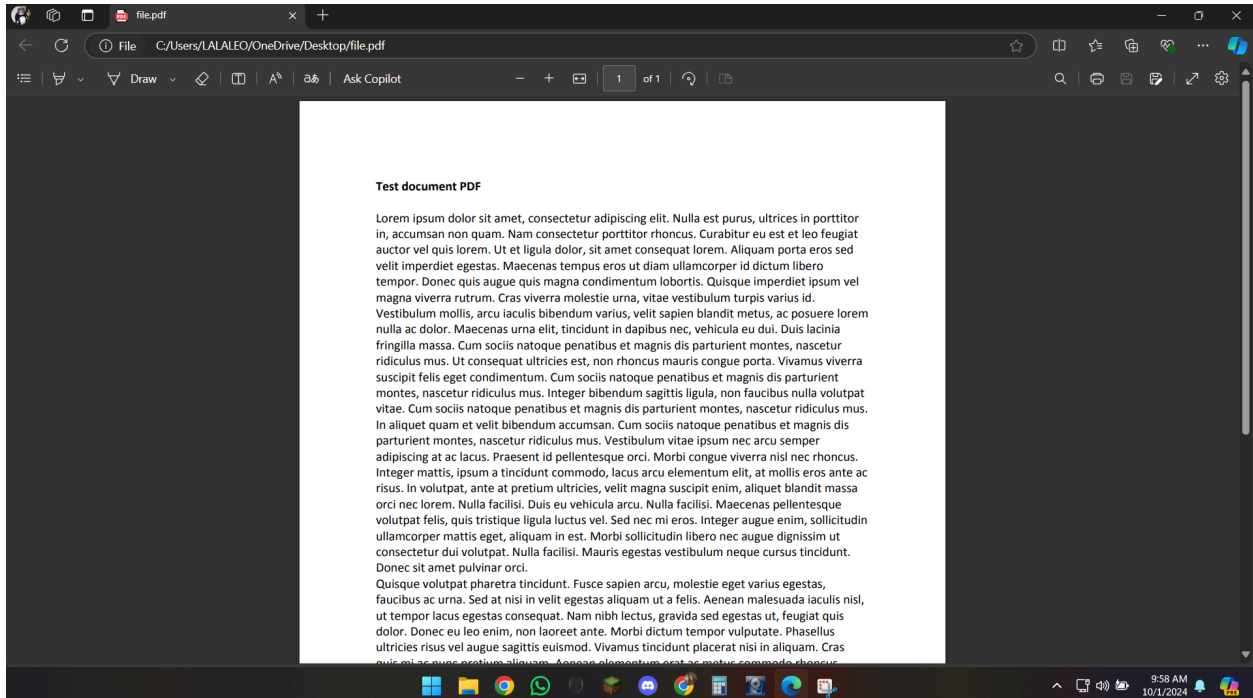
```
0000 42 04 00 00 00 00 00 00 1F 1F 1F 01 00 91 1F 1F
00d0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
00e0 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00
00f0 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00
0100 2C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65
0110 4E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00
0120 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF
```

Size is 77123

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

Offset	Hex	ASCII
0000	25 50 44 46 2D 31 2E 34-0D 25 E2 E3 CF D3 0D 0A	%PDF-1.4-%åãÏÖ..
0010	36 20 30 20 6F 62 6A 20-3C 3C 2F 4C 69 6E 65 61	6 0 obj <</Linea
0020	72 69 7A 65 64 20 31 2F-4C 20 37 37 31 32 33 2F	rized 1/L 77123/
0030	4F 20 38 2F 45 20 37 32-39 30 37 2F 4E 20 31 2F	O 8/E 72907/N 1/
0040	54 20 37 36 39 35 37 2F-48 20 5B 20 38 39 36 20	T 76957/H [ 896
0050	32 30 33 5D 3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20	203]>> .endobj .
0060	20 20 20 20 20 20 20 20-20 20 20 20 20 20 20	
0070	20 20 0D 0A 78 72 65 66-0D 0A 36 20 33 30 0D 0A	. .xref . .6 30 .
0080	30 30 30 30 30 30 30 30-31 36 20 30 30 30 30 30	0000000016 00000
0090	20 6E 0D 0A 30 30 30 30-30 30 31 30 39 39 20 30	n . .0000001099 0
00a0	30 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 31 31	0000 n . .00000011
00b0	37 35 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30	75 00000 n . .0000
00c0	30 30 31 33 35 37 20 30-30 30 30 30 20 6E 0D 0A	001357 00000 n . .
00d0	30 30 30 30 30 30 31 34-37 33 20 30 30 30 30 30	0000001473 00000
00e0	20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30	n . .0000001607 0
00f0	30 30 30 30 20 6E 0D 0A-30 30 30 30 30 31 38	0000 n . .00000018
0100	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

Recipe

MD5

Input

total: 2  
loaded: 2

1: file.pdf

2: lorem-ipsum.pdf

File details

Name: file.pdf  
Size: 77,123 bytes

Output

Tab 1

97a36af46c74151b55378c02055f796b

STEP

BAKE!

Auto Bake

20ms


Md5 of first file

MD5

1: file.pdf

2: lorem-ipsu.pdf

File details



Name: lorem-ipsu.pdf  
Size: 77,123 bytes

PDF-1.4 %  
6 0 obj <<Linearized 1/L 77123/O 8/E 72907/N 1/T 76957/H [ 896 203]>>  
endobj  
xref  
6 30  
0000000016 00000 n  
0000001099 00000 n  
0000001175 00000 n  
0000001357 00000 n  
0000001473 00000 n  
0000001607 00000 n

77123 365

Raw Bytes

Output

Tab 1

2: 97a36af46c74151b55378c02055f796b

97a36af46c74151b55378c02055f796b

STEP

BAKE!

Auto Bake

Md5 of 2nd file.

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