Digital Forensics

Lab 05

Abdul Sami Qasim

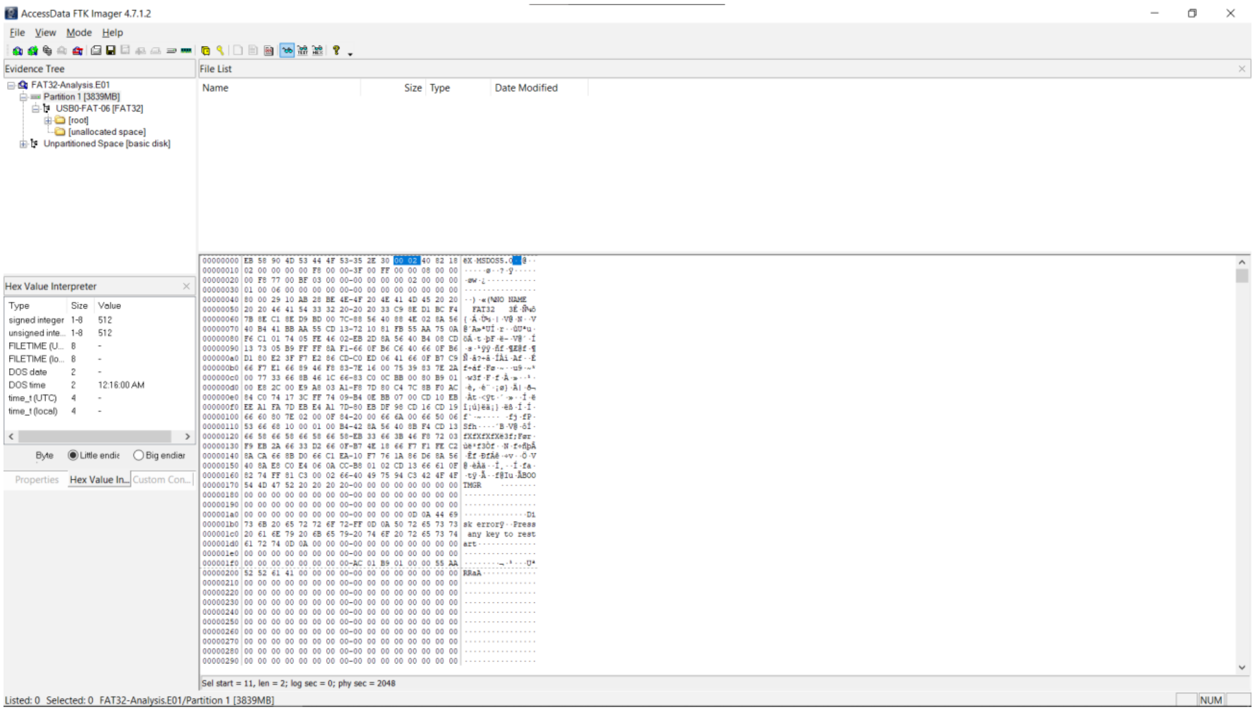
22i-1725

CY-D

Tasks:

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

Offset (Hex)	Size (Bytes)	Description	Value (Decimal)
0x0B	2	Bytes per Sector	512
0x0D	1	Sectors per Cluster	64



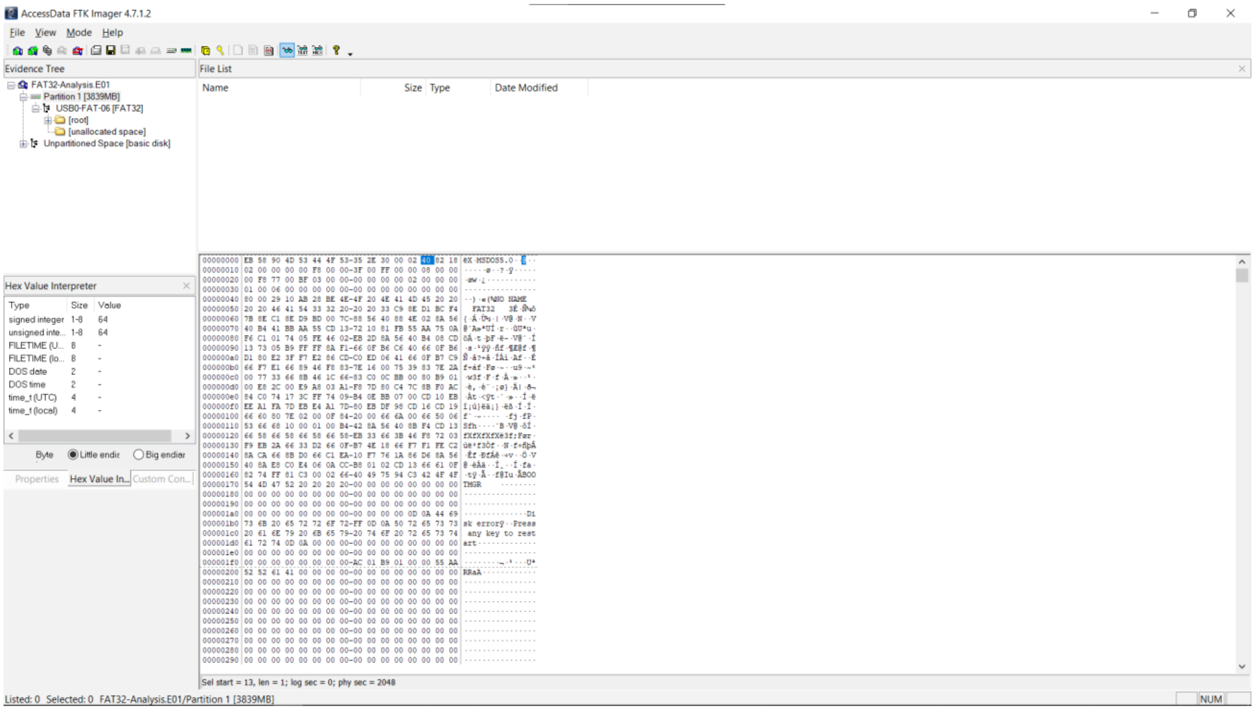
Type	Size	Value
signed integer	1-8	512
unsigned inte...	1-8	512
FILETIME (U...	8	-
FILETIME (lo...	8	-
DOS date	2	-
DOS time	2	12:16:00 AM
time_t (UTC)	4	-
time_t (local)	4	-

● Little endia ○ Big endian

```
00000000 EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 82 18 ëX·MSDOS5.0··@··
00000010 02 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00 ·····ø··?·ÿ·····
00000020 00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00 ·øw·¿···········
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 ··)·«(¾NO NAME
00000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É·Ñ¼ô
00000060 7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56 {·Á·Ù½·|·V@·N··V
00000070 40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A @´A»ªUÍ·r··ûUªu·
00000080 F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD öÁ·t·þF·ë-·V@´·Í
00000090 13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6 ·s·¹ÿÿ·ñf·¶Æ@f·¶
000000a0 D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9 Ñ·â?÷â·ÍÀí·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·À·»··¹·
000000d0 00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC ·è,·é¨·¡ø}·Ä|·ð¬
000000e0 84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB ·Àt·<ÿt·´·»··Í·ë
000000f0 EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19 î¡ú}ëä¡}·ëß·Í·Í·
00000100 66 60 80 7E 02 00 0F 84-20 00 66 6A 00 66 50 06 f`·~···· ·fj·fP·
00000110 53 66 68 10 00 01 00 B4-42 8A 56 40 8B F4 CD 13 Sfh····´B·V@·ôÍ·
00000120 66 58 66 58 66 58 66 58-EB 33 66 3B 46 F8 72 03 fXfXfXfXë3f;Før·
00000130 F9 EB 2A 66 33 D2 66 0F-B7 4E 18 66 F7 F1 FE C2 ùë*f3Òf··N·f÷ñþÂ
00000140 8A CA 66 8B D0 66 C1 EA-10 F7 76 1A 86 D6 8A 56 ·Êf·ÐfÁê·÷v··Ö·V
00000150 40 8A E8 C0 E4 06 0A CC-B8 01 02 CD 13 66 61 0F @·èÀä··Ì¸··Í·fa·
00000160 82 74 FF 81 C3 00 02 66-40 49 75 94 C3 42 4F 4F ·tÿ·Ã··f@Iu·ÃBOO
00000170 54 4D 47 52 20 20 20 20-00 00 00 00 00 00 00 00 TMGR    ········
00000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000001a0 00 00 00 00 00 00 00 00-00 00 00 00 0D 0A 44 69 ··············Di
000001b0 73 6B 20 65 72 72 6F 72-FF 0D 0A 50 72 65 73 73 sk errorÿ··Press
000001c0 20 61 6E 79 20 6B 65 79-20 74 6F 20 72 65 73 74  any key to rest
000001d0 61 72 74 0D 0A 00 00 00-00 00 00 00 00 00 00 00 art·············
000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000001f0 00 00 00 00 00 00 00 00-AC 01 B9 01 00 00 55 AA ········¬·¹···U ª
00000200 52 52 61 41 00 00 00 00-00 00 00 00 00 00 00 00 RRaA············
00000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Sel start = 11, len = 2; log sec = 0; phy sec = 2048

Listed: 0 Selected: 0 FAT32-Analysis.E01/Partition 1 [3839MB]



Evidence Tree:
- FAT32-Analysis.E01
  - Partition 1 [3839MB]
    - USB0-FAT-06 [FAT32]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

Name	Size	Type	Date Modified

Type	Size	Value
signed integer	1-8	64
unsigned inte...	1-8	64
FILETIME (U...	8	-
FILETIME (lo...	8	-
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	-
time_t (local)	4	-

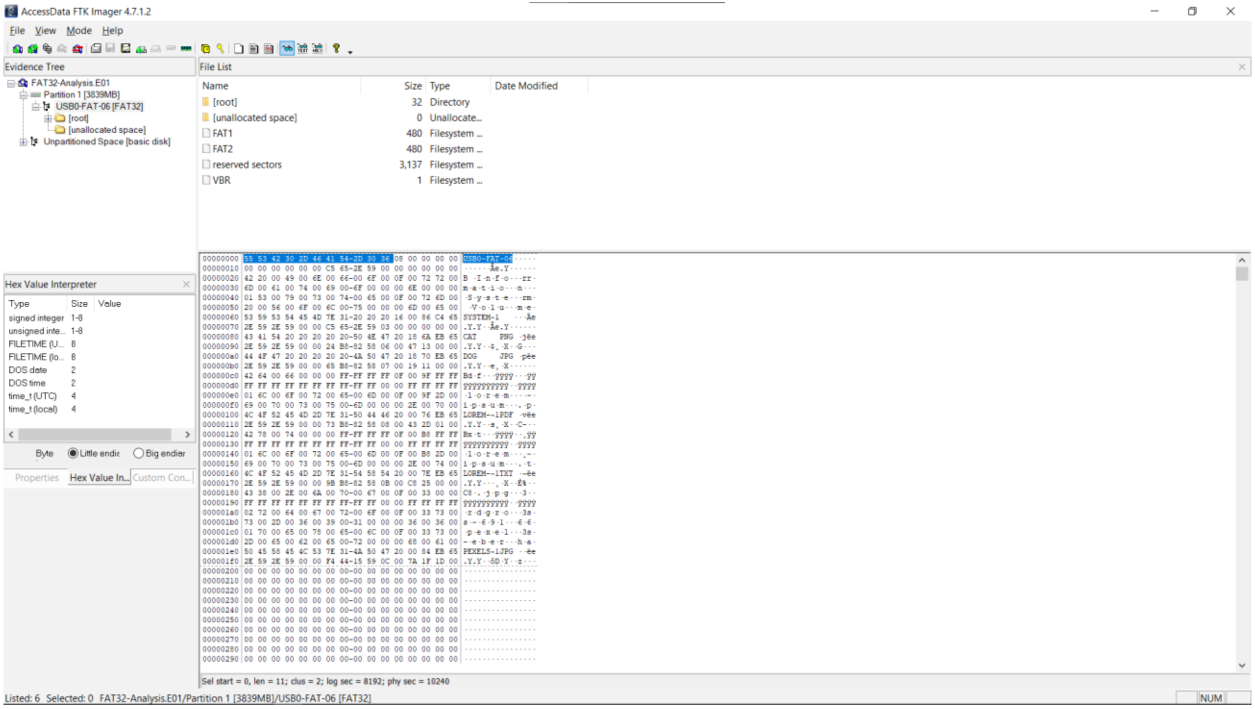
Byte ● Little endi ○ Big endiar

```
00000000 EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 82 18 ëX.MSDOS5.0..@..
00000010 02 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00 .....ø..?.ÿ.....
00000020 00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00 .øw.¿...........
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 ..).«(¾NO NAME  
00000050 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4   FAT32   3É.Ñ¼ô
00000060 7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56 {.Á.Ù½.|.V@.N..V
00000070 40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A @´A»ªUÍ.r..ûUªu.
00000080 F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD öÁ.t.þF.ë-.V@´.Í
00000090 13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6 .s.¹ÿÿ.ñf.¶Æ@f.¶
000000a0 D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9 Ñ.â?÷â.ÍÀí.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.À.»..¹.
000000d0 00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC .è,.é¨.¡ø}.Ä|.ð¬
000000e0 84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB .Àt.<ÿt.´.»..Í.ë
000000f0 EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19 î¡ú}ëä¡}.ëß.Í.Í.
00000100 66 60 80 7E 02 00 0F 84-20 00 66 6A 00 66 50 06 f`.~.... .fj.fP.
00000110 53 66 68 10 00 01 00 B4-42 8A 56 40 8B F4 CD 13 Sfh....´B.V@.ôÍ.
00000120 66 58 66 58 66 58 66 58-EB 33 66 3B 46 F8 72 03 fXfXfXfXë3f;FøHow.
00000130 F9 EB 2A 66 33 D2 66 0F-B7 4E 18 66 F7 F1 FE C2 ùë*f3Òf.·N.f÷ñþÂ
00000140 8A CA 66 8B D0 66 C1 EA-10 F7 76 1A 86 D6 8A 56 .Êf.ÐfÁê.÷v..Ö.V
00000150 40 8A E8 C0 E4 06 0A CC-B8 01 02 CD 13 66 61 0F @.èÀä..Ì¸..Í.fa.
00000160 82 74 FF 81 C3 00 02 66-40 49 75 94 C3 42 4F 4F .tÿ.Ã..f@Iu.ÃBOO
00000170 54 4D 47 52 20 20 20 20-00 00 00 00 00 00 00 00 TMGR    ........
00000180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000001a0 00 00 00 00 00 00 00 00-00 00 00 00 0D 0A 44 69 ..............Di
000001b0 73 6B 20 65 72 72 6F 72-FF 0D 0A 50 72 65 73 73 sk errorÿ..Press
000001c0 20 61 6E 79 20 6B 65 79-20 74 6F 20 72 65 73 74  any key to rest
000001d0 61 72 74 0D 0A 00 00 00-00 00 00 00 00 00 00 00 art.............
000001e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
000001f0 00 00 00 00 00 00 00 00-AC 01 B9 01 00 00 55 AA ........¬.¹...Uª
00000200 52 52 61 41 00 00 00 00-00 00 00 00 00 00 00 00 RRaA............
00000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Sel start = 13, len = 1; log sec = 0; phy sec = 2048

Listed: 0 Selected: 0 FAT32-Analysis.E01/Partition 1 [3839MB]

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



Evidence Tree:
- FAT32-Analysis.E01
  - Partition 1 [3839MB]
    - USB0-FAT-06 [FAT32]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

Name	Size	Type	Date Modified
[root]	32	Directory	
[unallocated space]	0	Unallocate...	
FAT1	480	Filesystem ...	
FAT2	480	Filesystem ...	
reserved sectors	3,137	Filesystem ...	
VBR	1	Filesystem ...	

Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte ● Little endi ○ Big endiar

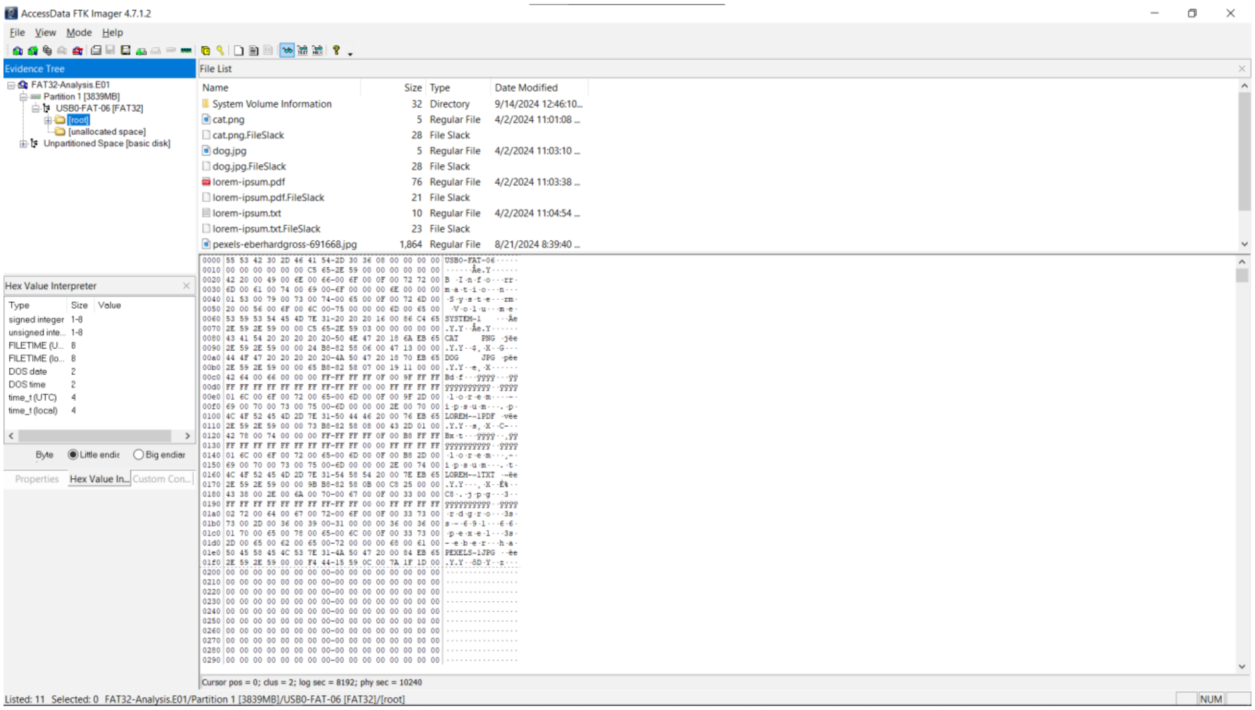
```
00000000 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06.....
00000010 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 00 ......Åe.Y......
00000020 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B .I.n.f.o...rr.
00000030 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m.a.t.i.o...n...
00000040 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 .S.y.s.t.e...rm.
00000050 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00  .V.o.l.u...m.e.
00000060 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM~1   ....Äe
00000070 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y..Åe.Y......
00000080 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT     PNG .jëe
00000090 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y..$¸.X..G...
000000a0 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG     JPG .pëe
000000b0 2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00 .Y.Y..e¸.X......
000000c0 42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF Bd.f...ÿÿÿÿ...ÿÿ
000000d0 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
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
00000130 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
00000140 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00 .l.o.r.e.m...¸-.
00000150 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i.p.s.u.m.....t.
00000160 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM-~1TXT .~ëe
00000170 2E 59 2E 59 00 00 9B B8-82 58 0B 00 C8 25 00 00 .Y.Y...¸.X..È%..
00000180 43 38 00 2E 00 6A 00 70-00 67 00 0F 00 33 00 00 C8...j.p.g...3..
00000190 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ..ÿÿÿÿ
000001a0 02 72 00 64 00 67 00 72-00 6F 00 0F 00 33 73 00 .r.d.g.r.o...3s.
000001b0 73 00 2D 00 36 00 39 00-31 00 00 00 36 00 36 00 s.-.6.9.1...6.6.
000001c0 01 70 00 65 00 78 00 65-00 6C 00 0F 00 33 73 00 .p.e.x.e.l...3s.
000001d0 2D 00 65 00 62 00 65 00-72 00 00 00 68 00 61 00 -.e.b.e.r...h.a.
000001e0 50 45 58 45 4C 53 7E 31-4A 50 47 20 00 84 EB 65 PEXELS~1JPG ..ëe
000001f0 2E 59 2E 59 00 00 F4 44-15 59 0C 00 7A 1F 1D 00 .Y.Y..ôD.Y..z...
00000200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Sel start = 0, len = 11; clus = 2; log sec = 8192; phy sec = 10240

Listed: 6 Selected: 0 FAT32-Analysis.E01/Partition 1 [3839MB]/USB0-FAT-06 [FAT32]

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

When we select the root folder in the evidence tree, there's a hex dump below the file list that has entries of all the files in the partition. In here, we can find the file name and it's extension.



- FAT32-Analysis.E01
  - Partition 1 [3839MB]
    - USB0-FAT-06 [FAT32]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

Name	Size	Type	Date Modified
System Volume Information	32	Directory	9/14/2024 12:46:10...
cat.png	5	Regular File	4/2/2024 11:01:08 ...
cat.png.FileSlack	28	File Slack	
dog.jpg	5	Regular File	4/2/2024 11:03:10 ...
dog.jpg.FileSlack	28	File Slack	
lorem-ipsum.pdf	76	Regular File	4/2/2024 11:03:38 ...
lorem-ipsum.pdf.FileSlack	21	File Slack	
lorem-ipsum.txt	10	Regular File	4/2/2024 11:04:54 ...
lorem-ipsum.txt.FileSlack	23	File Slack	
pexels-eberhardgross-691668.jpg	1,864	Regular File	8/21/2024 8:39:40 ...

Type	Size	Value
signed integer	1-8	
unsigned inte...	1-8	
FILETIME (U...	8	
FILETIME (lo...	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

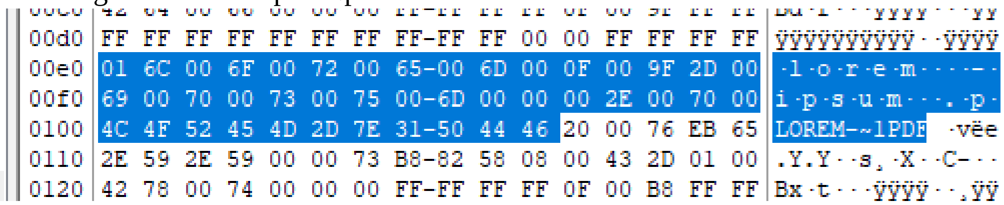
Byte ● Little endi ○ Big endiar

```
0000 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06·····
0010 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 00 ······Åe.Y······
0020 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B ·I·n·f·o···rr·
0030 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m·a·t·i·o···n···
0040 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 ·S·y·s·t·e···rm·
0050 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00  ·V·o·l·u···m·e·
0060 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM~1   ···Äe
0070 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y··Åe.Y······
0080 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT     PNG ·jëe
0090 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y··$¸·X··G···
00a0 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG     JPG ·pëe
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···¸-·
0150 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i·p·s·u·m···.·t·
0160 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM-~1TXT ·~ëe
0170 2E 59 2E 59 00 00 9B B8-82 58 0B 00 C8 25 00 00 .Y.Y···¸·X··È%··
0180 43 38 00 2E 00 6A 00 70-00 67 00 0F 00 33 00 00 C8·.·j·p·g···3··
0190 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
01a0 02 72 00 64 00 67 00 72-00 6F 00 0F 00 33 73 00 ·r·d·g·r·o···3s·
01b0 73 00 2D 00 36 00 39 00-31 00 00 00 36 00 36 00 s·-·6·9·1···6·6·
01c0 01 70 00 65 00 78 00 65-00 6C 00 0F 00 33 73 00 ·p·e·x·e·l···3s·
01d0 2D 00 65 00 62 00 65 00-72 00 00 00 68 00 61 00 -·e·b·e·r···h·a·
01e0 50 45 58 45 4C 53 7E 31-4A 50 47 20 00 84 EB 65 PEXELS~1JPG ··ëe
01f0 2E 59 2E 59 00 00 F4 44-15 59 0C 00 7A 1F 1D 00 .Y.Y··ôD·Y··z···
0200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0220 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0230 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0240 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0250 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0260 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0280 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0290 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

Cursor pos = 0; clus = 2; log sec = 8192; phy sec = 10240

Listed: 11 Selected: 0 FAT32-Analysis.E01/Partition 1 [3839MB]/USB0-FAT-06 [FAT32]/[root]

Zooming in for lorem-ipsum.pdf



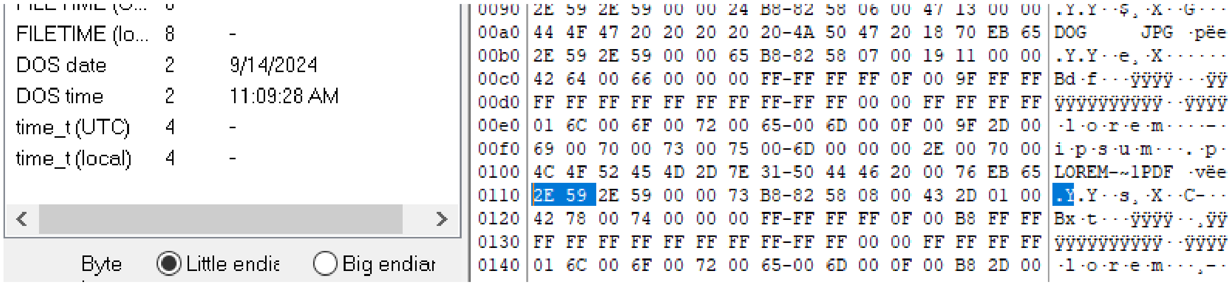
```
00d0 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
00e0 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 ·l·o·r·e·m····-·
00f0 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i·p·s·u·m···.·p·
0100 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM-~1PDF ·vëe
0110 2E 59 2E 59 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
```

The first two lines are the long filename and the third line is the short filename. The name of the file is **lorem-ipsum.pdf**

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

File Creation info at 0x10 (2 Bytes)
File Modified info at 0x12 (2 Bytes)

File Creation:

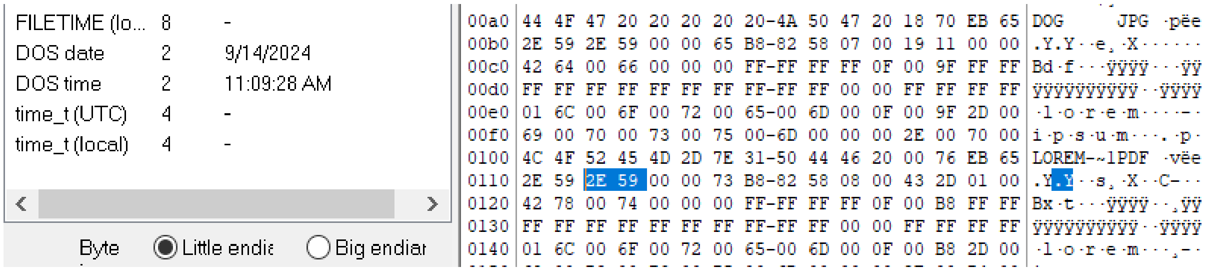


FILETIME (lo...	8	-
DOS date	2	9/14/2024
DOS time	2	11:09:28 AM
time_t (UTC)	4	-
time_t (local)	4	-

Byte ● Little endi ○ Big endiar

```
0090 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y··$¸·X··G···
00a0 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG     JPG ·pëe
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···¸-·
```

File Modified:



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

Byte ● Little endi ○ Big endiar

```
00a0 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG     JPG ·pëe
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···¸-·
```

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

Cluster Size for the Image file is: 32768 bytes

Size of Source File “lorem-ipsum.”: 77123 bytes

RAM Slack

RAM slack refers to the additional space between the end of a file and the end of the last sector allocated for that file in RAM (Random Access Memory). In FAT32 file systems, RAM slack can occur due to the sector size used by the file system.

```
Required:

- File Size: ? bytes

           77123

- Sector Size: ? bytes

           512

File Size modulo Sector Size = File Size % Sector Size

                           = 77123 % 512

                           = 323

RAM Slack = Sector Size - (File Size modulo Sector Size)

           = 512 - 323

           = 189
```

Drive Slack:

Drive slack refers to the additional space between the end of the last sector allocated for a file and the end of the cluster it resides in on a disk drive.

```
Given:

- File Size: ? bytes

           77123

- Sector Size: ? bytes
```

512

- Cluster Size: ? bytes

32768

Drive Slack = Cluster Size - (File Size % Cluster Size)

= 32768 – (77123 % 32768)

= 32768 – 11587

= 21181

File Size modulo Sector Size = File Size % Sector Size

Drive Slack = 21181

File Slack:

Given:

- File Size: ? bytes

77123

- Cluster Size: ? bytes

32768

Step 1: Determine the Number of Clusters Needed

Number of Clusters Needed = File Size / Cluster Size

= 77123 / 32768

= 2

Step 2: Check for Additional Cluster Needed

If (File Size modulo Cluster Size <> 0), add 1 additional cluster needed

File Size modulo Sector Size = File Size % Sector Size

= 77123 % 512

= 323

Since the remainder is not zero, an additional cluster is needed.

Total Clusters Needed = 3

Step 3: Calculate File Slack

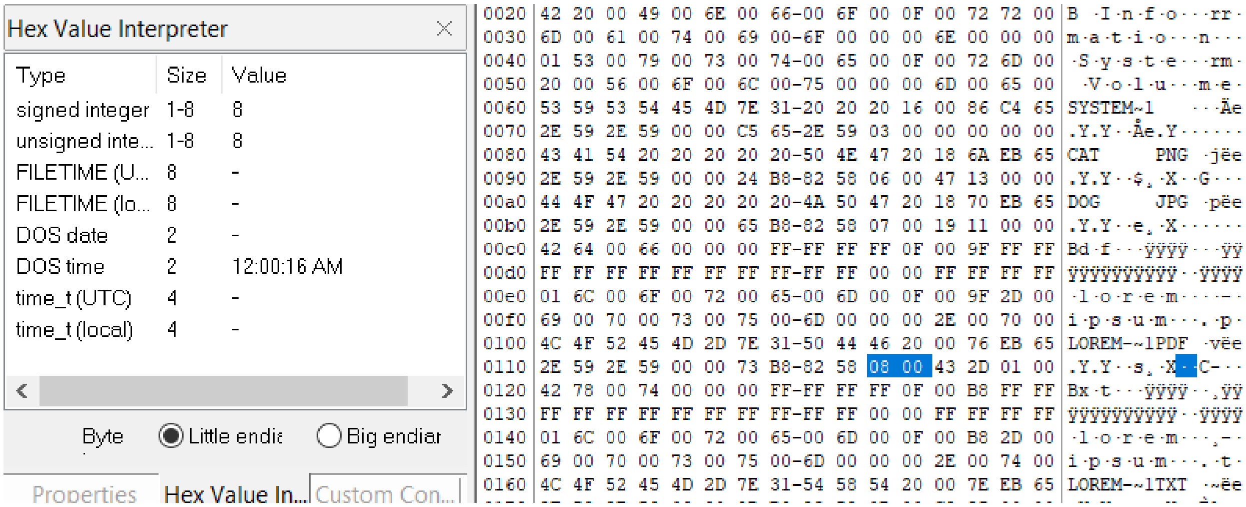
```
        File Slack = (Clusters Needed * Cluster Size) - File
Size

                        = (3 * 32768) - 77123

                        = 98304 - 77123

                        = 21181
```

6. 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.

Cluster is at 0x1A

File Size is at 0x1C

The cluster where the file is located is at 0x1C address of the short filename.



Hex Value Interpreter

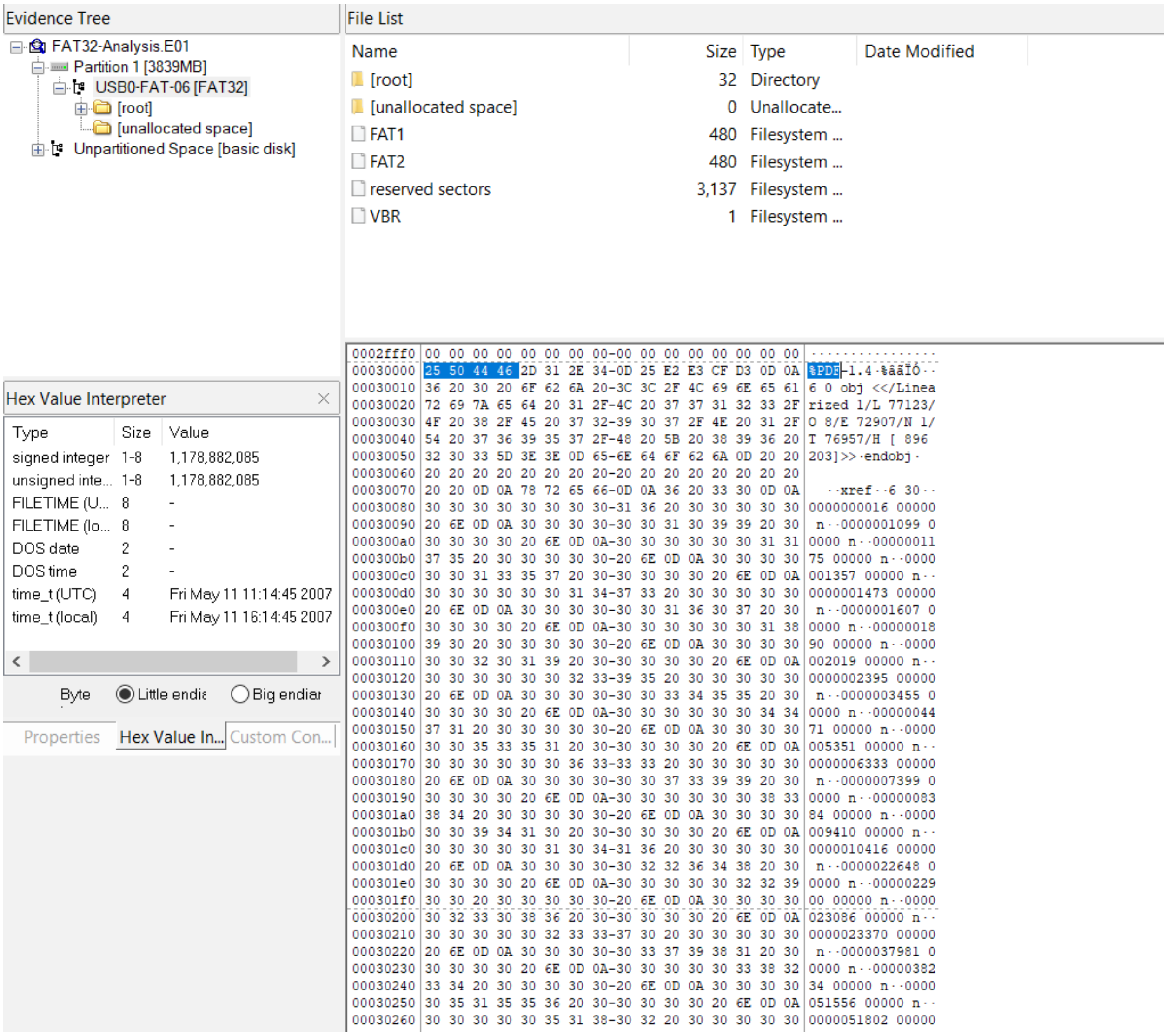
Type	Size	Value
signed integer	1-8	8
unsigned inte...	1-8	8
FILETIME (U...	8	-
FILETIME (lo...	8	-
DOS date	2	-
DOS time	2	12:00:16 AM
time_t (UTC)	4	-
time_t (local)	4	-

Byte ● Little endi ○ Big endiar

Properties | Hex Value In... | Custom Con...

```
0020 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B ·I·n·f·o···rr·
0030 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m·a·t·i·o···n···
0040 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 ·S·y·s·t·e···rm·
0050 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00  ·V·o·l·u···m·e·
0060 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM~1    ···Äe
0070 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y··Åe.Y······
0080 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT     PNG ·jëe
0090 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y··$¸·X··G···
00a0 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG     JPG ·pëe
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···¸-·
0150 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i·p·s·u·m···.·t·
0160 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM-~1TXT ·~ëe
```

Selecting the 2 bytes including 0x1C to see the cluster, we get the answer **8**



Evidence Tree

- FAT32-Analysis.E01
  - Partition 1 [3839MB]
    - USB0-FAT-06 [FAT32]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

File List

Name	Size	Type	Date Modified
[root]	32	Directory	
[unallocated space]	0	Unallocate...	
FAT1	480	Filesystem ...	
FAT2	480	Filesystem ...	
reserved sectors	3,137	Filesystem ...	
VBR	1	Filesystem ...	

Hex Value Interpreter

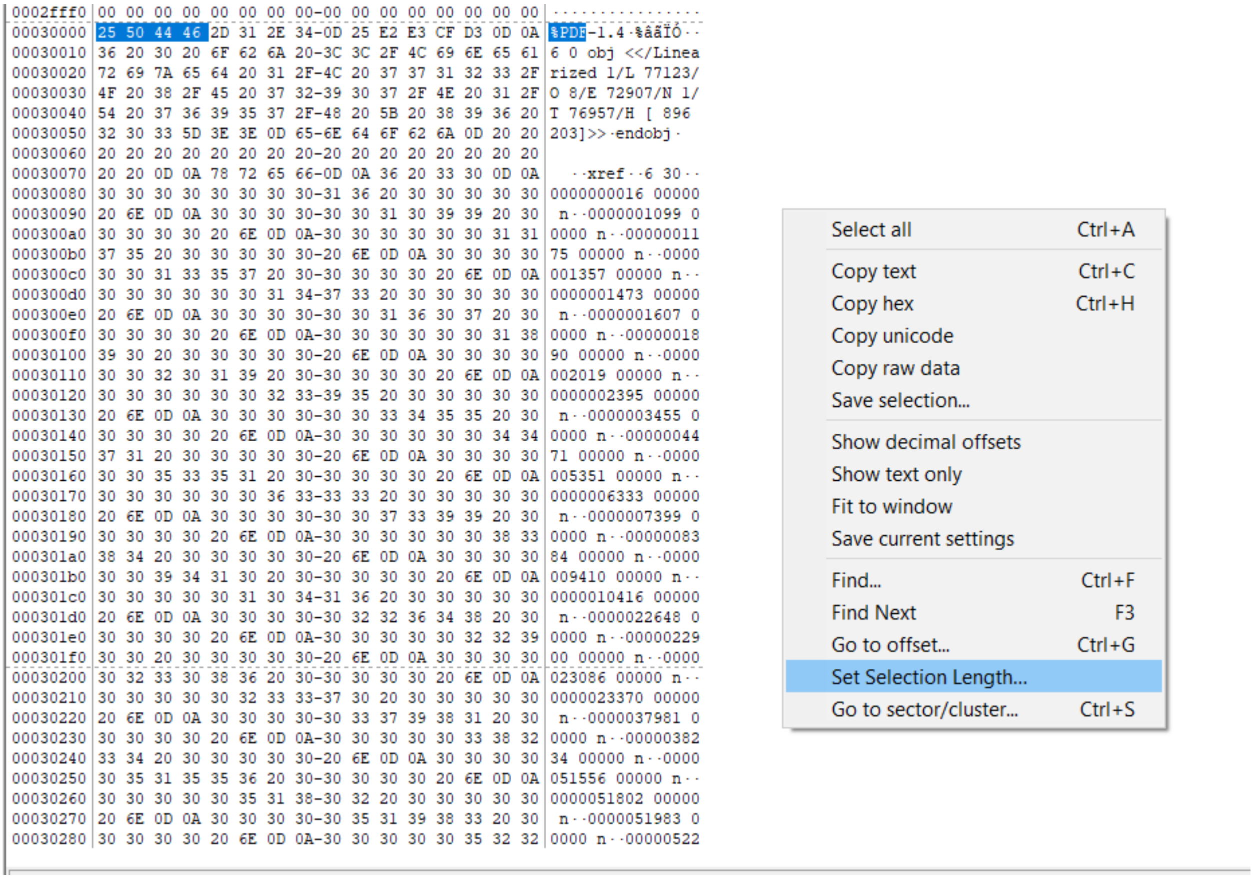
Type	Size	Value
signed integer	1-8	1,178,882,085
unsigned inte...	1-8	1,178,882,085
FILETIME (U...	8	-
FILETIME (lo...	8	-
DOS date	2	-
DOS time	2	-
time_t (UTC)	4	Fri May 11 11:14:45 2007
time_t (local)	4	Fri May 11 16:14:45 2007

Byte ● Little endia ○ Big endiar

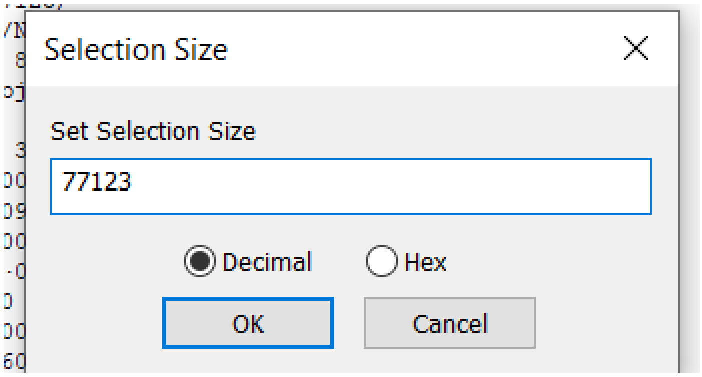
```
0002fff0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00030000  25 50 44 46 2D 31 2E 34-0D 25 E2 E3 CF D3 0D 0A  %PDF-1.4·%âãÏÓ··
00030010  36 20 30 20 6F 62 6A 20-3C 3C 2F 4C 69 6E 65 61  6 0 obj <</Linea
00030020  72 69 7A 65 64 20 31 2F-4C 20 37 37 31 32 33 2F  rized 1/L 77123/
00030030  4F 20 38 2F 45 20 37 32-39 30 37 2F 4E 20 31 2F  O 8/E 72907/N 1/
00030040  54 20 37 36 39 35 37 2F-48 20 5B 20 38 39 36 20  T 76957/H [ 896
00030050  32 30 33 5D 3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20  203]>>·endobj·
00030060  20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
00030070  20 20 0D 0A 78 72 65 66-0D 0A 36 20 33 30 0D 0A    ··xref··6 30··
00030080  30 30 30 30 30 30 30 30-31 36 20 30 30 30 30 30  0000000016 00000
00030090  20 6E 0D 0A 30 30 30 30-30 30 31 30 39 39 20 30   n··0000001099 0
000300a0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 31  0000 n··00000011
000300b0  37 35 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  75 00000 n··0000
000300c0  30 30 31 33 35 37 20 30-30 30 30 30 20 6E 0D 0A  001357 00000 n··
000300d0  30 30 30 30 30 30 31 34-37 33 20 30 30 30 30 30  0000001473 00000
000300e0  20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30   n··0000001607 0
000300f0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 38  0000 n··00000018
00030100  39 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  90 00000 n··0000
00030110  30 30 32 30 31 39 20 30-30 30 30 30 20 6E 0D 0A  002019 00000 n··
00030120  30 30 30 30 30 30 32 33-39 35 20 30 30 30 30 30  0000002395 00000
00030130  20 6E 0D 0A 30 30 30 30-30 30 33 34 35 35 20 30   n··0000003455 0
00030140  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 34 34  0000 n··00000044
00030150  37 31 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  71 00000 n··0000
00030160  30 30 35 33 35 31 20 30-30 30 30 30 20 6E 0D 0A  005351 00000 n··
00030170  30 30 30 30 30 30 36 33-33 33 20 30 30 30 30 30  0000006333 00000
00030180  20 6E 0D 0A 30 30 30 30-30 30 37 33 39 39 20 30   n··0000007399 0
00030190  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 38 33  0000 n··00000083
000301a0  38 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  84 00000 n··0000
000301b0  30 30 39 34 31 30 20 30-30 30 30 30 20 6E 0D 0A  009410 00000 n··
000301c0  30 30 30 30 30 31 30 34-31 36 20 30 30 30 30 30  0000010416 00000
000301d0  20 6E 0D 0A 30 30 30 30-30 32 32 36 34 38 20 30   n··0000022648 0
000301e0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 32 32 39  0000 n··00000229
000301f0  30 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  00 00000 n··0000
00030200  30 32 33 30 38 36 20 30-30 30 30 30 20 6E 0D 0A  023086 00000 n··
00030210  30 30 30 30 30 32 33 33-37 30 20 30 30 30 30 30  0000023370 00000
00030220  20 6E 0D 0A 30 30 30 30-30 33 37 39 38 31 20 30   n··0000037981 0
00030230  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 33 38 32  0000 n··00000382
00030240  33 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  34 00000 n··0000
00030250  30 35 31 35 35 36 20 30-30 30 30 30 20 6E 0D 0A  051556 00000 n··
00030260  30 30 30 30 30 35 31 38-30 32 20 30 30 30 30 30  0000051802 00000
```

Highlighting the PDF extension header to show that we are in the correct cluster (as per requirement).

Now Selecting the full file information using the file size that we have found (77123 in this case).



```
0002fff0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00030000 25 50 44 46 2D 31 2E 34-0D 25 E2 E3 CF D3 0D 0A %PDF-1.4·%âãÏÓ··
00030010 36 20 30 20 6F 62 6A 20-3C 3C 2F 4C 69 6E 65 61 6 0 obj <</Linea
00030020 72 69 7A 65 64 20 31 2F-4C 20 37 37 31 32 33 2F rized 1/L 77123/
00030030 4F 20 38 2F 45 20 37 32-39 30 37 2F 4E 20 31 2F O 8/E 72907/N 1/
00030040 54 20 37 36 39 35 37 2F-48 20 5B 20 38 39 36 20 T 76957/H [ 896
00030050 32 30 33 5D 3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20 203]>>·endobj·
00030060 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
00030070 20 20 0D 0A 78 72 65 66-0D 0A 36 20 33 30 0D 0A   ··xref··6 30··
00030080 30 30 30 30 30 30 30 30-31 36 20 30 30 30 30 30 0000000016 00000
00030090 20 6E 0D 0A 30 30 30 30-30 30 31 30 39 39 20 30  n··0000001099 0
000300a0 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 31 0000 n··00000011
000300b0 37 35 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 75 00000 n··0000
000300c0 30 30 31 33 35 37 20 30-30 30 30 30 20 6E 0D 0A 001357 00000 n··
000300d0 30 30 30 30 30 30 31 34-37 33 20 30 30 30 30 30 0000001473 00000
000300e0 20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30  n··0000001607 0
000300f0 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 38 0000 n··00000018
00030100 39 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 90 00000 n··0000
00030110 30 30 32 30 31 39 20 30-30 30 30 30 20 6E 0D 0A 002019 00000 n··
00030120 30 30 30 30 30 30 32 33-39 35 20 30 30 30 30 30 0000002395 00000
00030130 20 6E 0D 0A 30 30 30 30-30 30 33 34 35 35 20 30  n··0000003455 0
00030140 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 34 34 0000 n··00000044
00030150 37 31 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 71 00000 n··0000
00030160 30 30 35 33 35 31 20 30-30 30 30 30 20 6E 0D 0A 005351 00000 n··
00030170 30 30 30 30 30 30 36 33-33 33 20 30 30 30 30 30 0000006333 00000
00030180 20 6E 0D 0A 30 30 30 30-30 30 37 33 39 39 20 30  n··0000007399 0
00030190 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 38 33 0000 n··00000083
000301a0 38 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 84 00000 n··0000
000301b0 30 30 39 34 31 30 20 30-30 30 30 30 20 6E 0D 0A 009410 00000 n··
000301c0 30 30 30 30 30 31 30 34-31 36 20 30 30 30 30 30 0000010416 00000
000301d0 20 6E 0D 0A 30 30 30 30-30 32 32 36 34 38 20 30  n··0000022648 0
000301e0 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 32 32 39 0000 n··00000229
000301f0 30 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 00 00000 n··0000
00030200 30 32 33 30 38 36 20 30-30 30 30 30 20 6E 0D 0A 023086 00000 n··
00030210 30 30 30 30 30 32 33 33-37 30 20 30 30 30 30 30 0000023370 00000
00030220 20 6E 0D 0A 30 30 30 30-30 33 37 39 38 31 20 30  n··0000037981 0
00030230 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 33 38 32 0000 n··00000382
00030240 33 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30 34 00000 n··0000
00030250 30 35 31 35 35 36 20 30-30 30 30 30 20 6E 0D 0A 051556 00000 n··
00030260 30 30 30 30 30 35 31 38-30 32 20 30 30 30 30 30 0000051802 00000
00030270 20 6E 0D 0A 30 30 30 30-30 35 31 39 38 33 20 30  n··0000051983 0
00030280 30 30 30 30 20 6E 0D 0A-30 30 30 30 30 35 32 32 0000 n··00000522
```



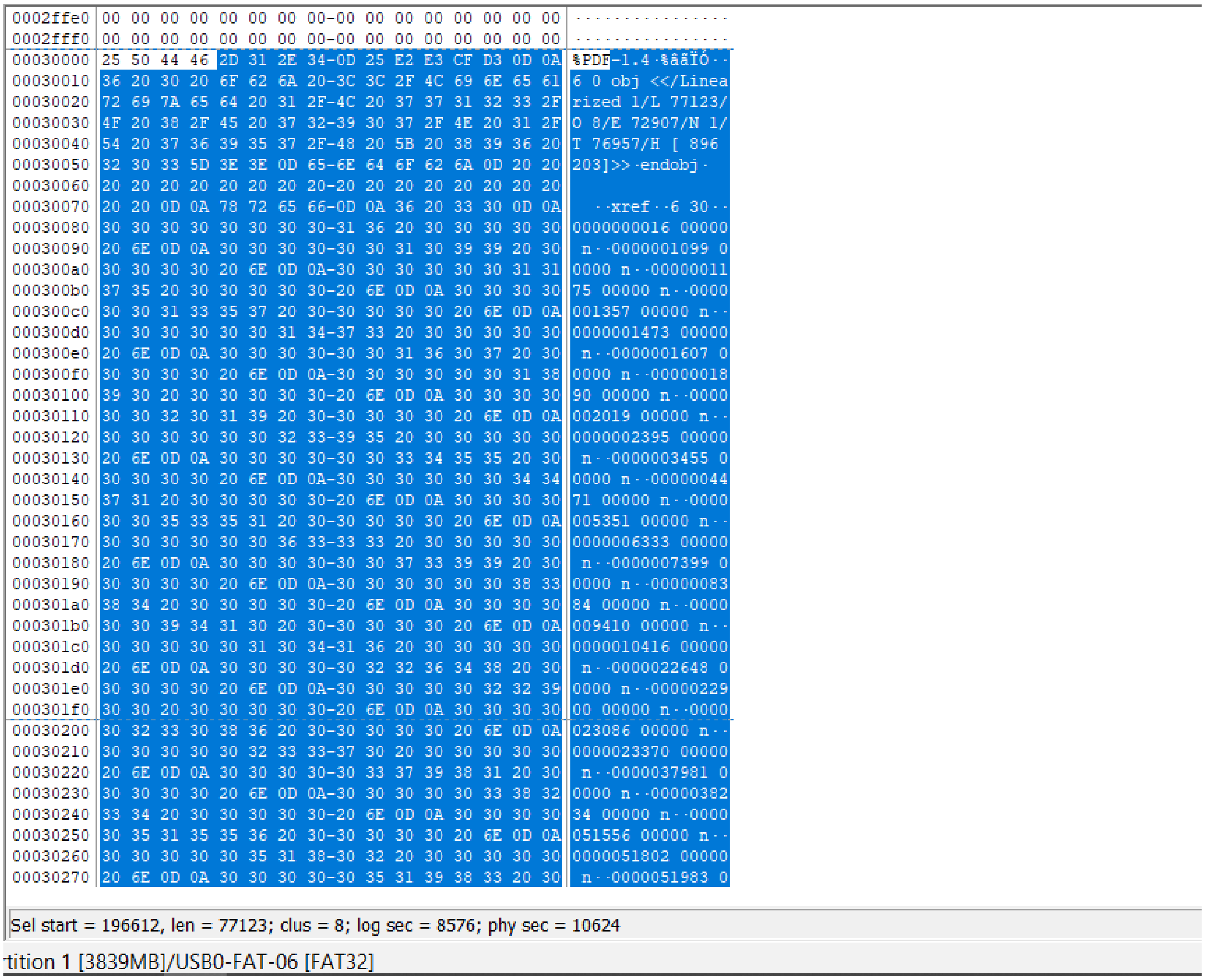
Selection Size

Set Selection Size

77123

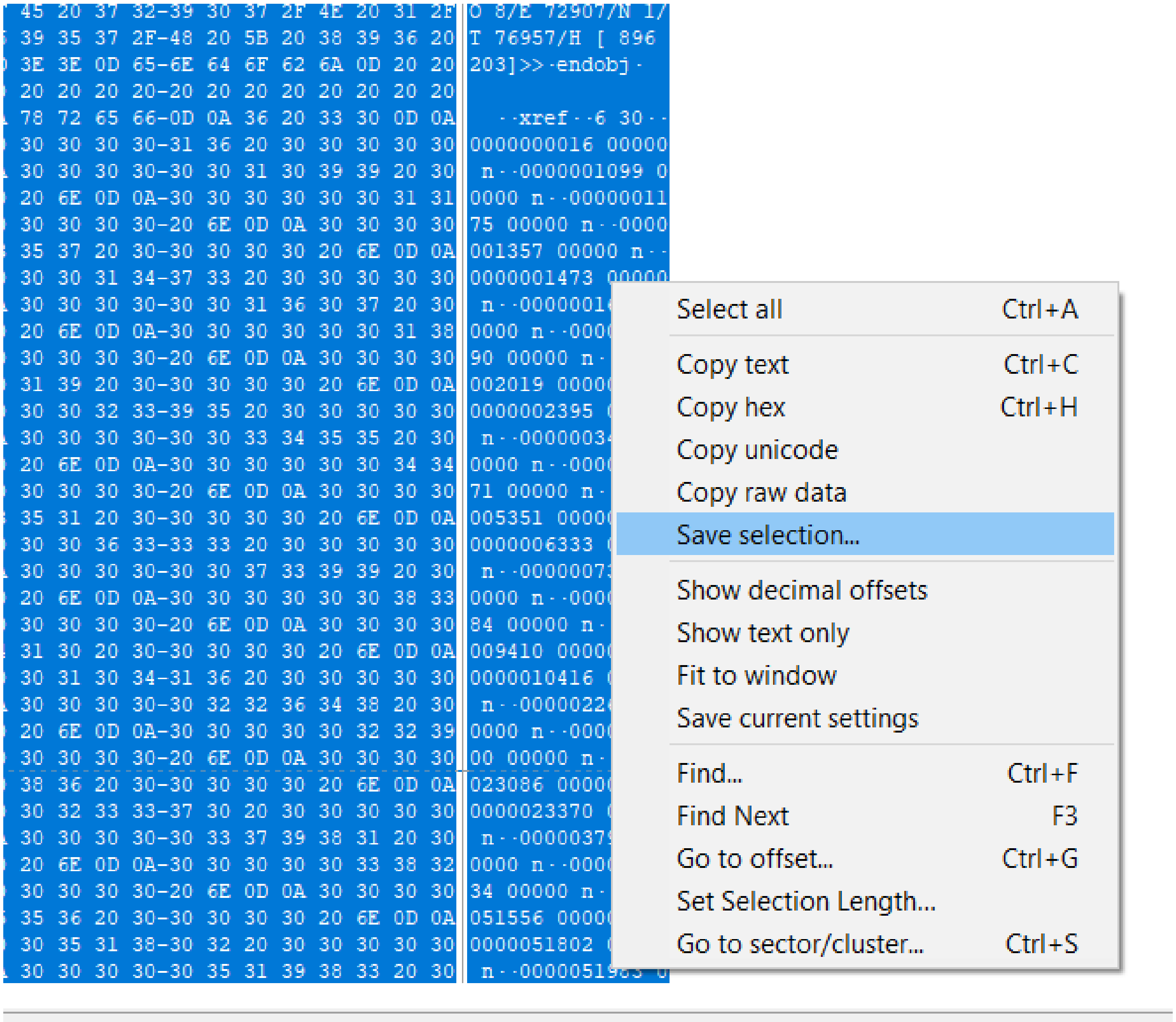
● Decimal ○ Hex

The full file information is selected.

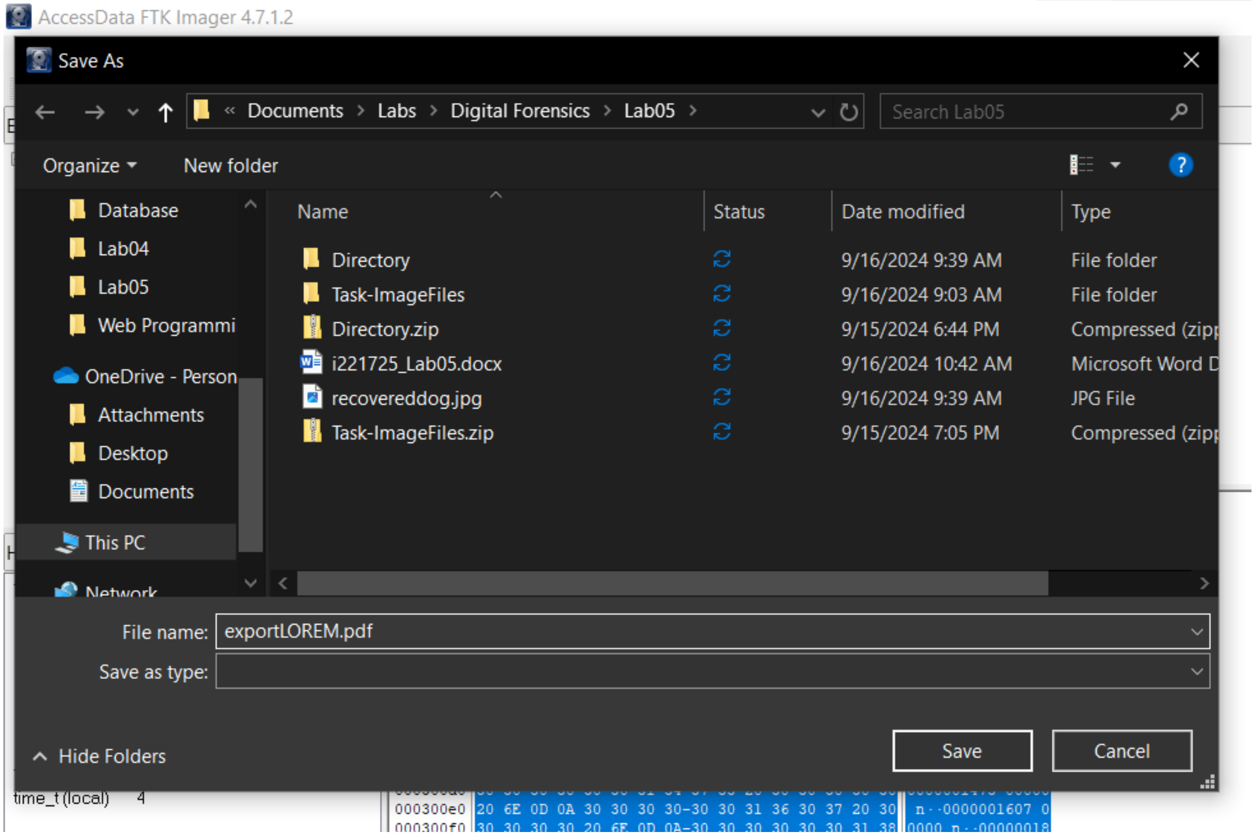


```
0002ffe0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0002fff0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
00030000  25 50 44 46 2D 31 2E 34-0D 25 E2 E3 CF D3 0D 0A  %PDF-1.4·%âãÏÓ··
00030010  36 20 30 20 6F 62 6A 20-3C 3C 2F 4C 69 6E 65 61  6 0 obj <</Linea
00030020  72 69 7A 65 64 20 31 2F-4C 20 37 37 31 32 33 2F  rized 1/L 77123/
00030030  4F 20 38 2F 45 20 37 32-39 30 37 2F 4E 20 31 2F  O 8/E 72907/N 1/
00030040  54 20 37 36 39 35 37 2F-48 20 5B 20 38 39 36 20  T 76957/H [ 896 
00030050  32 30 33 5D 3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20  203]>>·endobj·  
00030060  20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20                  
00030070  20 20 0D 0A 78 72 65 66-0D 0A 36 20 33 30 0D 0A    ··xref··6 30··
00030080  30 30 30 30 30 30 30 30-31 36 20 30 30 30 30 30  0000000016 00000
00030090  20 6E 0D 0A 30 30 30 30-30 30 31 30 39 39 20 30   n··0000001099 0
000300a0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 31  0000 n··00000011
000300b0  37 35 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  75 00000 n··0000
000300c0  30 30 31 33 35 37 20 30-30 30 30 30 20 6E 0D 0A  001357 00000 n··
000300d0  30 30 30 30 30 30 31 34-37 33 20 30 30 30 30 30  0000001473 00000
000300e0  20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30   n··0000001607 0
000300f0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 31 38  0000 n··00000018
00030100  39 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  90 00000 n··0000
00030110  30 30 32 30 31 39 20 30-30 30 30 30 20 6E 0D 0A  002019 00000 n··
00030120  30 30 30 30 30 30 32 33-39 35 20 30 30 30 30 30  0000002395 00000
00030130  20 6E 0D 0A 30 30 30 30-30 30 33 34 35 35 20 30   n··0000003455 0
00030140  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 34 34  0000 n··00000044
00030150  37 31 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  71 00000 n··0000
00030160  30 30 35 33 35 31 20 30-30 30 30 30 20 6E 0D 0A  005351 00000 n··
00030170  30 30 30 30 30 30 36 33-33 33 20 30 30 30 30 30  0000006333 00000
00030180  20 6E 0D 0A 30 30 30 30-30 30 37 33 39 39 20 30   n··0000007399 0
00030190  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 38 33  0000 n··00000083
000301a0  38 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  84 00000 n··0000
000301b0  30 30 39 34 31 30 20 30-30 30 30 30 20 6E 0D 0A  009410 00000 n··
000301c0  30 30 30 30 30 31 30 34-31 36 20 30 30 30 30 30  0000010416 00000
000301d0  20 6E 0D 0A 30 30 30 30-30 32 32 36 34 38 20 30   n··0000022648 0
000301e0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 32 32  0000 n··00000229
000301f0  30 30 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  00 00000 n··0000
00030200  30 32 33 30 38 36 20 30-30 30 30 30 20 6E 0D 0A  023086 00000 n··
00030210  30 30 30 30 30 32 33 33-37 30 20 30 30 30 30 30  0000023370 00000
00030220  20 6E 0D 0A 30 30 30 30-30 33 37 39 38 31 20 30   n··0000037981 0
00030230  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 30 33 38  0000 n··00000382
00030240  33 34 20 30 30 30 30 30-20 6E 0D 0A 30 30 30 30  34 00000 n··0000
00030250  30 35 31 35 35 36 20 30-30 30 30 30 20 6E 0D 0A  051556 00000 n··
00030260  30 30 30 30 30 35 31 38-30 32 20 30 30 30 30 30  0000051802 00000
00030270  20 6E 0D 0A 30 30 30 30-30 35 31 39 38 33 20 30   n··0000051983 0

Sel start = 196612, len = 77123; clus = 8; log sec = 8576; phy sec = 10624
tition 1 [3839MB]/USB0-FAT-06 [FAT32]
```

Now extracting the file.



```
45 20 37 32-39 30 37 2F 4E 20 31 2F  O 8/E 72907/N 1/
39 35 37 2F-48 20 5B 20 38 39 36 20  T 76957/H [ 896
3E 3E 0D 65-6E 64 6F 62 6A 0D 20 20  203]>>·endobj·
20 20 20 20-20 20 20 20 20 20 20 20
78 72 65 66-0D 0A 36 20 33 30 0D 0A    ··xref··6 30··
30 30 30 30-31 36 20 30 30 30 30 30  0000000016 00000
30 30 30 30-30 30 31 30 39 39 20 30   n··0000001099 0
20 6E 0D 0A-30 30 30 30 30 30 31 31  0000 n··00000011
30 30 30 30-20 6E 0D 0A 30 30 30 30  75 00000 n··0000
35 37 20 30-30 30 30 30 20 6E 0D 0A  001357 00000 n··
30 30 31 34-37 33 20 30 30 30 30 30  0000001473 00000
30 30 30 30-30 30 31 36 30 37 20 30   n··0000001
20 6E 0D 0A-30 30 30 30 30 30 31 38  0000 n··000
30 30 30 30-20 6E 0D 0A 30 30 30 30  90 00000 n·
31 39 20 30-30 30 30 30 20 6E 0D 0A  002019 0000
30 30 32 33-39 35 20 30 30 30 30 30  0000002395
30 30 30 30-30 30 33 34 35 35 20 30   n··0000003
20 6E 0D 0A-30 30 30 30 30 30 34 34  0000 n··000
30 30 30 30-20 6E 0D 0A 30 30 30 30  71 00000 n·
35 31 20 30-30 30 30 30 20 6E 0D 0A  005351 0000
30 30 36 33-33 33 20 30 30 30 30 30  0000006333
30 30 30 30-30 30 37 33 39 39 20 30   n··0000007
20 6E 0D 0A-30 30 30 30 30 30 38 33  0000 n··000
30 30 30 30-20 6E 0D 0A 30 30 30 30  84 00000 n·
31 30 20 30-30 30 30 30 20 6E 0D 0A  009410 0000
30 31 30 34-31 36 20 30 30 30 30 30  0000010416
30 30 30 30-30 32 32 36 34 38 20 30   n··0000022
20 6E 0D 0A-30 30 30 30 30 32 32 39  0000 n··000
30 30 30 30-20 6E 0D 0A 30 30 30 30  00 00000 n·
38 36 20 30-30 30 30 30 20 6E 0D 0A  023086 0000
30 32 33 33-37 30 20 30 30 30 30 30  0000023370
30 30 30 30-30 33 37 39 38 31 20 30   n··0000037
20 6E 0D 0A-30 30 30 30 30 33 38 32  0000 n··000
30 30 30 30-20 6E 0D 0A 30 30 30 30  34 00000 n·
35 36 20 30-30 30 30 30 20 6E 0D 0A  051556 0000
30 35 31 38-30 32 20 30 30 30 30 30  0000051802
30 30 30 30-30 35 31 39 38 33 20 30   n··000005198
```



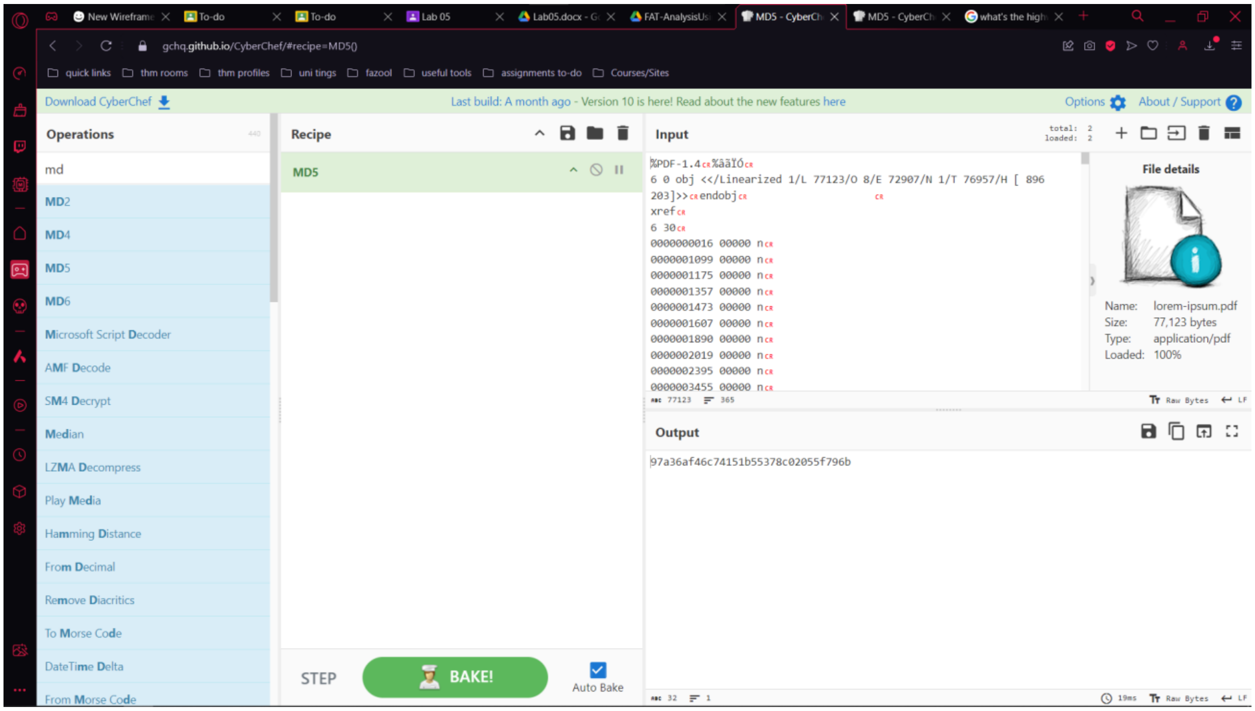
Name	Status	Date modified	Type
Directory		9/16/2024 9:39 AM	File folder
Task-ImageFiles		9/16/2024 9:03 AM	File folder
Directory.zip		9/15/2024 6:44 PM	Compressed (zipp
i221725_Lab05.docx		9/16/2024 10:42 AM	Microsoft Word D
recovereddog.jpg		9/16/2024 9:39 AM	JPG File
Task-ImageFiles.zip		9/15/2024 7:05 PM	Compressed (zipp

File name: exportLOREM.pdf

Save as type:

```
time_t (local)    4
000300e0  20 6E 0D 0A 30 30 30 30-30 30 31 36 30 37 20 30  n··0000001607 0
000300f0  30 30 30 30 20 6E 0D 0A-30 30 30 30 30 31 38     0000 n··00000018
```

Now checking the hashes:



md

MD2
MD4
MD5
MD6
Microsoft Script Decoder
AMF Decode
SM4 Decrypt
Median
LZMA Decompress
Play Media
Hamming Distance
From Decimal
Remove Diacritics
To Morse Code
DateTime Delta
From Morse Code

MD5

total: 2
loaded: 2

```
%PDF-1.4%âãÏÓ
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
0000001890 00000 n
0000002019 00000 n
0000002395 00000 n
0000003455 00000 n
```

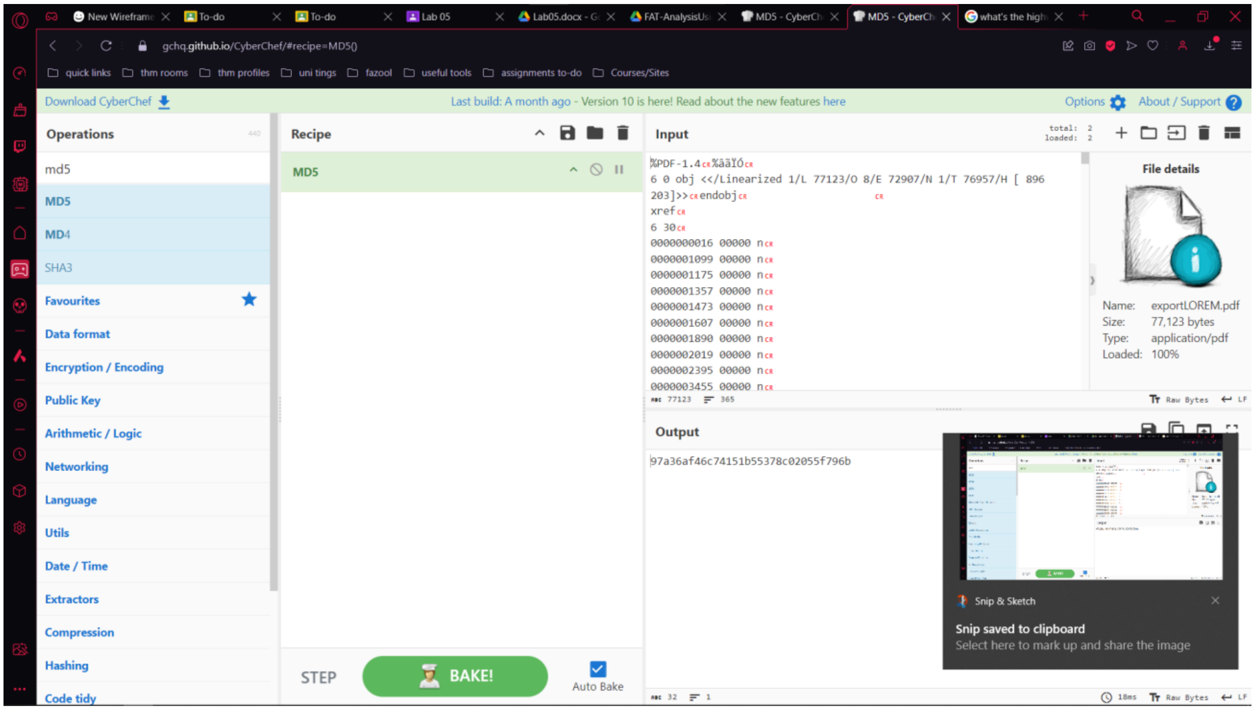
77123   365   Raw Bytes   LF

File details

Name: lorem-ipsum.pdf
Size: 77,123 bytes
Type: application/pdf
Loaded: 100%

```
97a36af46c74151b55378c02055f796b
```

32   1   19ms   Raw Bytes   LF



```
%PDF-1.4 %âãÏÓ
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
0000001890 00000 n
0000002019 00000 n
0000002395 00000 n
0000003455 00000 n
```

Name: exportLOREM.pdf
Size: 77,123 bytes
Type: application/pdf
Loaded: 100%

```
97a36af46c74151b55378c02055f796b
```

Both the Hashes are same.

Hash of extracted file : 97a36af46c74151b55378c02055f796b

Hash of original file : 97a36af46c74151b55378c02055f796b