

Digital Forensics – Lab05

Ahmad Abdullah i22-1609

Task#1: Find Byte per Sector and Sectors per Cluster for Image File? Pay attention to the endianness

From the Lab manual, we knew where to look.

0x0B 2 bytes Bytes per Sector

0x0D 1 Sectors per Cluster

Looking at those offset bits one by one we get the byte size per sector and then sectors per cluster.

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

```
0000000000 EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 82 18 EX-MSDOSS.0 @...
0000000016 02 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00 .....ø-?·ÿ.....
0000000032 00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00 .....øw-¿.....
0000000048 01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 .....
0000000064 80 00 29 10 AB 28 BE 4E-4F 20 4E 41 4D 45 20 20 ..)·«(%NO NAME
0000000080 20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4 FAT32 3E·N·wó
0000000096 7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56 {·Ã·Ü·|·VØ·N·V
0000000112 40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A @'A·*UÍ·r··ûU·u·
0000000128 F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD ôÃ·t·pF·ë-·VØ'·í
0000000144 13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6 ·s·ÿÿ·ñf·¶EØf·¶
0000000160 D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9 Ñ·â?+â·ÎÃi·Af··É
0000000176 66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A f+áf·Fø·-·u9·~*
0000000192 00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01 ·w3f·F·f·Ã·»·~·
0000000208 00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC ·è·,è"-;ø}·Ã|·ð-
0000000224 84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB ·Àt·<ÿt·'·»··í·ë
0000000240 EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19 i;ú)ëa; }·ëB·í·í·
0000000256 66 60 80 7E 02 00 0F 84-20 00 66 6A 00 66 50 06 f'·-·-·-·fj·fP·
0000000272 53 66 68 10 00 01 00 B4-42 8A 56 40 8B F4 CD 13 Sfh·-·-·B·VØ·ôí·
0000000288 66 58 66 58 66 58 66 58-EB 33 66 3B 46 F8 72 03 fXfXfXfXfXfXf;Før·
0000000304 F9 EB 2A 66 33 D2 66 0F-B7 4E 18 66 F7 F1 FE C2 ûë*f3Øf··N·f+ñpÃ
0000000320 8A CA 66 8B D0 66 C1 EA-10 F7 76 1A 86 D6 8A 56 ·Éf·ÐfÃë+·v··Ö·V
0000000336 40 8A E8 C0 E4 06 0A CC-B8 01 02 CD 13 66 61 0F Ø·ëÃ·-·I·-·í·fa·
0000000352 82 74 FF 81 C3 00 02 66-40 49 75 94 C3 42 4F 4F ·tÿ·Ã·-·f@Iu·ÃBOO
0000000368 54 4D 47 52 20 20 20 20-00 00 00 00 00 00 00 00 TMGR .....
0000000384 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0000000400 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
0000000416 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....Di
0000000432 73 6B 20 65 72 72 6F 72-FF 0D 0A 50 72 65 73 73 sk errorÿ·-Press
0000000448 20 61 6E 79 20 6B 65 79-20 74 6F 20 72 65 73 74 any key to rest
0000000464 61 72 74 0D 0A 00 00 00-00 00 00 00 00 00 00 00 art.....
```

Hex Value Interpreter

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

0000000000	EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 40 B2 18	EX-MSDOS5.0
0000000016	02 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 08 00 00ø-?·ÿ.....
0000000032	00 F8 77 00 BF 03 00 00-00 00 00 00 02 00 00 00øw·z.....
0000000048	01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00
0000000064	80 00 29 10 AB 28 BE 4E-4F 20 4E 41 4D 45 20 20	...)·«(%NO NAME
0000000080	20 20 46 41 54 33 32 20-20 20 33 C9 8E D1 BC F4	FAT32 3E·Ñ·ô
0000000096	7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56	{·À·Ù·:· ·V@·N··V
0000000112	40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A	@'A»·Uí·r··úU·u·
0000000128	F6 C1 01 74 05 FE 46 02-EB 2D 8A 56 40 B4 08 CD	ôÃ·t·pF·ë··V@'·í
0000000144	13 73 05 B9 FF FF 8A F1-66 0F B6 C6 40 66 0F B6	·s·'ÿÿ·ñf·qE@f·q
0000000160	D1 80 E2 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9	Ñ·â?·â·IÃ1·Af··É
0000000176	66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A	f+áf·Fø·~··u9·~·*
0000000192	00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01	·w3f·F·f·À·»·~·~·
0000000208	00 E8 2C 00 E9 A8 03 A1-F8 7D 80 C4 7C 8B F0 AC	·è··é~·;ø}·Ã1·ô~
0000000224	84 C0 74 17 3C FF 74 09-B4 0E BB 07 00 CD 10 EB	·At·<ÿt·'·~··í·è
0000000240	EE A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19	í;ú)ëä;·}·ëB·í·í·
0000000256	66 60 80 7E 02 00 0F 84-20 00 66 6A 00 66 50 06	f'·~·~·~·~·~·fj·fP·
0000000272	53 66 68 10 00 01 00 B4-42 8A 56 40 8B F4 CD 13	Sfh·~·~·~·B·V@·ôí·
0000000288	66 58 66 58 66 58 66 58-EB 33 66 3B 46 F8 72 03	fXfXfXfXë3f;Før·
0000000304	F9 EB 2A 66 33 D2 66 0F-B7 4E 18 66 F7 F1 FE C2	ùë*f3ôf··N·f+ñpÃ
0000000320	8A CA 66 8B D0 66 C1 EA-10 F7 76 1A 86 D6 8A 56	·ëf·BfÃë·+v··Ö·V
0000000336	40 8A E8 C0 E4 06 0A CC-B8 01 02 CD 13 66 61 0F	@·èÃ·~·í··í·fa·
0000000352	82 74 FF 81 C3 00 02 66-40 49 75 94 C3 42 4F 4F	+ò·Ï·~·fãtñ·Ïrøn

After getting both byte size and cluster size we can easily determine the cluster size by the formula

Byte Size = 512 bytes

Sector Size = 64 Bytes

Cluster Size = byte size X Sector Size

Cluster Size = 512 x 64 = 32,768 bytes

Task#2: Show and explain where the FAT file system stores the volume label.

Just selecting the volume the first bytes we see are of volume label/name of the volume.

The screenshot shows the FAT32-Analysis.E01 interface. On the left, the 'Partition 1 [3839MB]' is selected, showing 'USB0-FAT-06 [FAT32]' and 'System Volume Information'. A red arrow points to 'USB0-FAT-06 [FAT32]'. On the right, the 'Name' column lists the root directory, unallocated space, FAT1, FAT2, reserved sectors, and VBR. The 'Size' column shows the size of each entry. The 'Date Modified' column shows the date and time of the last modification. The 'Data' column shows the hex values of the entries. The first entry, '[root]', has a size of 32 and is a directory. The second entry, '[unallocated space]', has a size of 0 and is unallocated space. The third entry, 'FAT1', has a size of 480 and is a filesystem metadata entry. The fourth entry, 'FAT2', has a size of 480 and is a filesystem metadata entry. The fifth entry, 'reserved sectors', has a size of 3,137 and is a filesystem metadata entry. The sixth entry, 'VBR', has a size of 1 and is a filesystem metadata entry. The 'Data' column shows the hex values of the entries. The first entry, '[root]', has a value of '55 53 42 30 2D 46 41 54-2D 30 36'. The second entry, '[unallocated space]', has a value of '00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00'. The third entry, 'FAT1', has a value of '42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00'. The fourth entry, 'FAT2', has a value of '6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00'. The fifth entry, 'reserved sectors', has a value of '01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00'. The sixth entry, 'VBR', has a value of '20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00'. The 'Data' column also shows the volume label 'USB0-FAT-06' in the first bytes of the FAT table.

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

We were required to find the file name and extension of lorem ipsum. PDF file along with its metadata.

1. Locate the file's short name. Usually, the 0x00 and 0x10 sectors are for files with short name and above files short name, the hex usually contains files long name.

The screenshot shows the FAT32-Analysis.E01 interface. On the left, the 'Partition 1 [3839MB]' is selected, showing 'USB0-FAT-06 [FAT32]' and 'System Volume Information'. A red arrow points to 'USB0-FAT-06 [FAT32]'. On the right, the 'File List' table shows the files and their metadata. The 'Name' column lists the files: 'System Volume Information', 'cat.png', 'cat.png.FileSlack', 'dog.jpg', 'dog.jpg.FileSlack', 'lorem-ipsum.pdf', 'lorem-ipsum.pdf.FileSlack', 'lorem-ipsum.txt', 'lorem-ipsum.txt.FileSlack', 'pexels-eberhardgross-691668.jpg', and 'pexels-ebhardgross-691668.jpg.FileSlack'. The 'Size' column shows the size of each file. The 'Type' column shows the file type. The 'Date Modified' column shows the date and time of the last modification. The 'Data' column shows the hex values of the entries. The first entry, 'System Volume Information', has a size of 32 and is a directory. The second entry, 'cat.png', has a size of 5 and is a regular file. The third entry, 'cat.png.FileSlack', has a size of 28 and is a file slack. The fourth entry, 'dog.jpg', has a size of 5 and is a regular file. The fifth entry, 'dog.jpg.FileSlack', has a size of 28 and is a file slack. The sixth entry, 'lorem-ipsum.pdf', has a size of 76 and is a regular file. The seventh entry, 'lorem-ipsum.pdf.FileSlack', has a size of 21 and is a file slack. The eighth entry, 'lorem-ipsum.txt', has a size of 10 and is a regular file. The ninth entry, 'lorem-ipsum.txt.FileSlack', has a size of 23 and is a file slack. The tenth entry, 'pexels-eberhardgross-691668.jpg', has a size of 1,864 and is a regular file. The eleventh entry, 'pexels-ebhardgross-691668.jpg.FileSlack', has a size of 25 and is a file slack. The 'Data' column shows the hex values of the entries. The first entry, 'System Volume Information', has a value of '55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00'. The second entry, 'cat.png', has a value of '00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00'. The third entry, 'cat.png.FileSlack', has a value of '42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00'. The fourth entry, 'dog.jpg', has a value of '6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00'. The fifth entry, 'dog.jpg.FileSlack', has a value of '01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00'. The sixth entry, 'lorem-ipsum.pdf', has a value of '20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00'. The seventh entry, 'lorem-ipsum.pdf.FileSlack', has a value of '53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65'. The eighth entry, 'lorem-ipsum.txt', has a value of '2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00'. The ninth entry, 'lorem-ipsum.txt.FileSlack', has a value of '43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65'. The tenth entry, 'pexels-eberhardgross-691668.jpg', has a value of '2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00'. The eleventh entry, 'pexels-ebhardgross-691668.jpg.FileSlack', has a value of '44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65'. The 'Data' column also shows the volume label 'USB0-FAT-06' in the first bytes of the FAT table.

Task#4: Determine the date and time when the file “lorem-ipsu

Hex Value Interpreter			00000 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06-----
Type	Size	Value	00016 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 -----Äe.Y-----
signed integer	1-8	22,830	00032 42 20 00 49 00 00 6E 00 66-00 6F 00 0F 00 72 72 00 B-I-n-f-o-r-r-
unsigned integer	1-8	22,830	00048 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m-a-t-i-o-n-
FILETIME (UTC)	8	-	00064 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 -S-y-s-t-e-rm-
FILETIME (local)	8	-	00080 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00 -V-o-l-u-m-e-
DOS date	2	14/09/2024	00096 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM-1 --Äe
DOS time	2	11:09:28 am	00112 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y--Äe.Y-----
time_t (UTC)	4	-	00128 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT PNG-jëe
time_t (local)	4	-	00144 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y--\$,X-G---
			00160 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG JPG-pëe
			00176 2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00 .Y.Y--e,X-----
			00192 42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF Bd-f---ÿÿÿÿ--ÿÿ
			00208 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00224 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 -l-o-r-e-m---p-
			00240 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i-p-s-u-m---p-
			00256 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM--lPDF-vëe
			00272 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 .Y.Y--s,X-C---
			00288 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF Bx-t---ÿÿÿÿ--ÿÿ
			00304 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00320 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00 -l-o-r-e-m---p-
			00336 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i-p-s-u-m---t-
			00352 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM--lTXT-vëe
			00368 2E 59 2E 59 00 00 9B B8-82 58 0B 00 C8 25 00 00 .Y.Y---X-Ès---
			00384 43 38 00 2E 00 6A 00 70-00 67 00 0F 00 33 00 00 C8-.j-p-g---3--
			00400 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00416 03 72 00 64 00 67 00 72-00 6F 00 0F 00 33 73 00 -r-d-g-r-o---3s-
			00432 73 00 2D 00 36 00 39 00-31 00 00 00 36 00 36 00 s--6-9-l---6-6-
			00448 01 70 00 65 00 78 00 65-00 6C 00 0F 00 33 73 00 -p-e-x-e-l---3s-
			00464 2D 00 65 00 62 00 65 00-72 00 00 00 68 00 61 00 -e-b-e-r---ha-
			00480 50 45 58 45 4C 53 7E 31-4A 50 47 20 00 84 EB 65 PEXELS-lJPG-vëe
			00496 2E 59 2E 59 00 00 F4 44-15 59 0C 00 7A 1F 1D 00 .Y.Y--öD-Y--g---
			00512 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 -----

pexels-eberhardgross-691668.jpg 1,864 Regular File 21/08/2024 8:39:40 am

pexels-eberhardgross-691668.jpg.FileSlack 25 File Slack

Hex Value Interpreter			00000 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06-----
Type	Size	Value	00016 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 -----Äe.Y-----
signed integer	1-8	22,830	00032 42 20 00 49 00 00 6E 00 66-00 6F 00 0F 00 72 72 00 B-I-n-f-o-r-r-
unsigned integer	1-8	22,830	00048 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m-a-t-i-o-n-
FILETIME (UTC)	8	-	00064 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 -S-y-s-t-e-rm-
FILETIME (local)	8	-	00080 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00 -V-o-l-u-m-e-
DOS date	2	14/09/2024	00096 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM-1 --Äe
DOS time	2	11:09:28 am	00112 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y--Äe.Y-----
time_t (UTC)	4	-	00128 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT PNG-jëe
time_t (local)	4	-	00144 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y--\$,X-G---
			00160 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG JPG-pëe
			00176 2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00 .Y.Y--e,X-----
			00192 42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF Bd-f---ÿÿÿÿ--ÿÿ
			00208 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00224 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 -l-o-r-e-m---p-
			00240 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i-p-s-u-m---p-
			00256 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM--lPDF-vëe
			00272 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 .Y.Y--s,X-C---
			00288 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF Bx-t---ÿÿÿÿ--ÿÿ
			00304 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00320 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00 -l-o-r-e-m---p-
			00336 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i-p-s-u-m---t-
			00352 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM--lTXT-vëe
			00368 2E 59 2E 59 00 00 9B B8-82 58 0B 00 C8 25 00 00 .Y.Y---X-Ès---
			00384 43 38 00 2E 00 6A 00 70-00 67 00 0F 00 33 00 00 C8-.j-p-g---3--
			00400 FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF ÿÿÿÿÿÿÿÿ--ÿÿÿÿ
			00416 02 72 00 64 00 67 00 72-00 6F 00 0F 00 33 73 00 -r-d-g-r-o---3s-
			00432 73 00 2D 00 36 00 39 00-31 00 00 00 36 00 36 00 s--6-9-l---6-6-
			00448 01 70 00 65 00 78 00 65-00 6C 00 0F 00 33 73 00 -p-e-x-e-l---3s-
			00464 2D 00 65 00 62 00 65 00-72 00 00 00 68 00 61 00 -e-b-e-r---ha-
			00480 50 45 58 45 4C 53 7E 31-4A 50 47 20 00 84 EB 65 PEXELS-lJPG-vëe
			00496 2E 59 2E 59 00 00 F4 44-15 59 0C 00 7A 1F 1D 00 .Y.Y--öD-Y--g---
			00512 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 -----

Task#5: Determine the date and time when the file “lorem-ipsu.pdf” was created / modified based on the root entry hex data?

Hex Value Interpreter			
Type	Size	Value	
signed integer	1-8	77,123	
unsigned integer	1-8	77,123	
FILETIME (UTC)	8	-	
FILETIME (local)	8	-	
DOS date	2	-	
DOS time	2	-	
time (UTC)	4	Thu Jan 1 21:25:23 1970	

00000	55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00	USB0-FAT-06----
00016	00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 00Äe.Y.....
00032	42 20 00 49 00 00 6E 00 66-00 6F 00 0F 00 72 72 00	B-I-n-f-o-o-r-r-
00048	6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00	m-a-t-i-o-n-
00064	01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00	.S-y-s-t-e-m-
00080	20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00	.V-o-l-u-m-e-
00096	53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65	SYSTEM-1 ..Äe
00112	2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00	.Y.Y-Äe.Y.....
00128	43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65	CAT PNG-jëe
00144	2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00	.Y.Y-ç,X-G-
00160	44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65	DOG JPG-pëe
00176	2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00	.Y.Y-e,X-
00192	42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF	Bd-f-ÿÿÿÿ-ÿÿ
00208	FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF	ÿÿÿÿÿÿÿÿ-ÿÿÿÿ
00224	01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00	.l-o-r-e-m-
00240	69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00	i-p-s-u-m-.p-
00256	4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 FB 65	LOREM--lPDF-ève
00272	2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00	.Y.Y-s,X-C-
00288	42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF	Bx-t-ÿÿÿÿ-ÿÿ
00304	FF FF FF FF FF FF FF FF-FF FF 00 00 FF FF FF FF	ÿÿÿÿÿÿÿÿ-ÿÿÿÿ
00320	01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00	.l-o-r-e-m-.p-
00336	69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00	i-p-s-u-m-.t-

RAM, Drive and File Slack:

RAM Slack

- File Size: 77,123 bytes
- Sector Size: 512 bytes

File Size modulo Sector Size = File Size % Sector Size

= 77123 % 512

= 323

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

= 512 - 323

= 189 bytes

Drive Slack

- File Size: 77,123 bytes
- Sector Size: 512 bytes
- Cluster Size: 32,768 bytes

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

= 32768 - (77123%32,768)

$$= 32768 - 11587$$

$$= 21181 \text{ bytes}$$

File Slack

- File Size: 77,123 bytes

- Cluster Size: 32,768 bytes

Step 1: Determine the Number of Clusters Needed

Number of Clusters Needed = File Size / Cluster Size

Number of Clusters Needed = $77,123 / 32,768 \approx 2$ cluster

Step 2: Check for Additional Cluster Needed

If (File Size modulo Cluster Size $\neq 0$), add 1 additional cluster needed

File Size modulo Cluster Size = $45,334 \bmod 32,768 = 12,566$

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

Total Clusters Needed = 3 clusters

Step 3: Calculate File Slack

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

File Slack = $(3 * 32,768) - 77123$

File Slack = $98304 - 77123$

File Slack = 21181 bytes

Task#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.

pexeis-ebemargross-091008.jpg.files\black

File black

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

```

00000 55 53 42 30 2D 46 41 54-2D 30 36 08 00 00 00 00 USB0-FAT-06.....
00016 00 00 00 00 00 00 C5 65-2E 59 00 00 00 00 00 .....Äe.Y.....
00032 42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00 B I-n-f-o-r-r
00048 6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00 m-a-t-i-o-n...
00064 01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00 S-y-s-t-e-rm-
00080 20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00 V-o-l-u-m-e-
00096 53 59 53 54 45 4D 7E 31-20 20 20 16 00 86 C4 65 SYSTEM-1 ...Äe
00112 2E 59 2E 59 00 00 C5 65-2E 59 03 00 00 00 00 00 .Y.Y-Äe.Y.....
00128 43 41 54 20 20 20 20 20-50 4E 47 20 18 6A EB 65 CAT PNG jëe
00144 2E 59 2E 59 00 00 24 B8-82 58 06 00 47 13 00 00 .Y.Y-$.X-G...
00160 44 4F 47 20 20 20 20 20-4A 50 47 20 18 70 EB 65 DOG JPG pëe
00176 2E 59 2E 59 00 00 65 B8-82 58 07 00 19 11 00 00 .Y.Y-e,X.....
00192 42 64 00 66 00 00 00 FF-FF FF FF 0F 00 9F FF FF Bd-f-ÿÿÿÿ-ÿÿ
00208 FF FF FF FF FF FF FF FF-FF FF FF 00 00 FF FF FF ÿÿÿÿÿÿÿÿ-ÿÿÿÿ
00224 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 9F 2D 00 l-o-r-e-m.....
00240 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 70 00 i-p-s-u-m....p
00256 4C 4F 52 45 4D 2D 7E 31-50 44 46 20 00 76 EB 65 LOREM~1PDF vëe
00272 2E 59 2E 59 00 00 73 B8-82 58 08 00 43 2D 01 00 .Y.Y-s,X-C...
00288 42 78 00 74 00 00 00 FF-FF FF FF 0F 00 B8 FF FF Bx-t-ÿÿÿÿ-ÿÿ
00304 FF FF FF FF FF FF FF FF-FF FF FF 00 00 FF FF FF ÿÿÿÿÿÿÿÿ-ÿÿÿÿ
00320 01 6C 00 6F 00 72 00 65-00 6D 00 0F 00 B8 2D 00 l-o-r-e-m....-
00336 69 00 70 00 73 00 75 00-6D 00 00 00 2E 00 74 00 i-p-s-u-m....t
00352 4C 4F 52 45 4D 2D 7E 31-54 58 54 20 00 7E EB 65 LOREM~1TXT wëe
00368 2E 59 2E 59 00 00 9B B8-82 58 0B 00 C8 25 00 00 .Y.Y-,.X-E$...
00384 43 38 00 2E 00 6A 00 70-00 67 00 0F 00 33 00 00 C8-.j-p-g...3..
00400 FF FF FF FF FF FF FF FF-FF FF FF 00 00 FF FF FF ÿÿÿÿÿÿÿÿ-ÿÿÿÿ
00416 02 72 00 64 00 67 00 72-00 6F 00 0F 00 33 73 00 r-d-g-r-o...3s-
00432 73 00 2D 00 36 00 39 00-31 00 00 00 36 00 36 00 s--6-9-1...6-6-
00448 01 70 00 65 00 78 00 65-00 6C 00 0F 00 33 73 00 p-e-x-e-l...3s-
00464 2D 00 65 00 62 00 65 00-72 00 00 00 68 00 61 00 -e-b-e-r-h-a-
00480 50 45 58 45 4C 53 7E 31-4A 50 47 20 00 84 EB 65 PEXELS~1JPG ëëe
00496 2E 59 2E 59 00 00 F4 44-15 59 0C 00 7A 1F 1D 00 .Y.Y-ôD-Y-z...
00512 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
00528 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....

```

Selection Size

Set Selection Size (Bytes):

77123

☒ Decimal ☐ Hex


OK Cancel

Both Files have same Hash which tells us that file was not modified.

Input

```
%PDF-1.4
6 0 obj <</Linearized 1/L 77123/O 8/E 72907/N 1/T 76957/H [ 896 203]>>
xref
6 30
0000000016 00000 n
0000001099 00000 n
0000001175 00000 n
0000001357 00000 n
0000001473 00000 n
0000001607 00000 n
0000001890 00000 n
```

File details



Name: lorem.pdf
Size: 77,123 bytes
Type: application/pdf

Output

97a36af46c74151b55378c02055f796b


Input

1: lorem.pdf

3: lorem-ipsu.pdf

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

File details



Name: lorem-ipsu.pdf

Output

Tab 1

3: 97a36af46c74151b55378c02055f796b

97a36af46c74151b55378c02055f796b