

FAT File System

Alvaro Austin 216752180

1. Ringkasan Isi Video:

File Allocation Table (FAT) terdiri dari beberapa tipe seperti FAT12/16 (legacy), FAT32 (memory, USB, biasanya ukurannya tidak terlalu besar), exFAT(extended FAT) ukurannya lebih besar. Perbedaan mendasar antara FAT 16 (legacy) dengan FAT32 adalah:

- Schematic Representation: pada FAT16, root directory masih berada pada system area yang menyebabkan root directory tersebut memiliki besaran yang tetap (*fixed size*). Akan tetapi pada FAT32, root directory berada data area yang menyebabkan root directory bisa meningkat besarnya berdasarkan *space* yang kita miliki dalam area tersebut.
- Max Clustering Number: pada FAT16, cluster addressing berupa 2 bytes sehingga representasi maksimum (0xFFFF = 65536) namun pada FAT32, cluster addressing mencapai 3 bytes yaitu (0xFFFFFFF = 16777215). Cluster numbering mulai dari 2, sehingga jumlah maksimum cluster yang terdapat pada FAT16 adalah 65535 dan pada FAT32 adalah 16777216.

Berikut adalah struktur dari Volume Boot Record:

FAT32 VOLUME BOOT RECORD:	
00000000	EB 58 90 4D 53 44 4F 53-35 2E 30 00 02 08 1A 04 8X MSDOS5.0
00000010	02 00 00 00 00 F8 00 00-3F 00 FF 00 00 00 00 00 00 00 00
00000020	00 08 78 00 F3 1D 00 00-00 00 00 00 00 00 00 00 00 00
00000030	01 00 06 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00
00000040	80 00 29 EE 10 80 90 4E-4F 20 4E 41 4D 45 20 29) i - NO NAME
00000050	20 20 4E 41 54 33 32 20-20 20 33 C9 8E D1 BC F4 FAT32 3E-Nv6
00000060	7B 8E C1 8E D9 BD 00 7C-88 56 40 88 4E 02 8A 56 (A-U-1-V8-N-V
00000070	40 B4 41 BB AA 55 CD 13-72 10 81 FB 55 AA 75 0A 0 Aw*U! r-Qu-u-
00000080	F6 B4 01 74 05 FE 46 02-E8 2D 8A 56 40 B4 08 CD 0A-t-pF è-Vé-i
00000090	13 73 05 B9 FF FF 8A F1-66 0F Bc C6 40 66 0F B6 s-ÿy-fif Qeff-g
000000a0	D1 B0 22 3F F7 E2 86 CD-C0 ED 06 41 66 0F B7 C9 N à-à-ííí AE-É
000000b0	66 F7 E1 66 89 46 F8 83-7E 16 00 75 39 83 7E 2A f-áí-Fz-..-u9-*
000000c0	00 77 33 66 8B 46 1C 66-83 C0 0C BB 00 80 B9 01 w32-F-F Á »..
000000d0	00 E8 2C 00 E8 A8 03 AL-F8 7D 80 C4 7C 8B F0 AC è, é-, é-;æ] A] -s
000000e0	84 C0 74 17 3C FF 74 09-84 0E BB 07 00 CD 10 EB Át-<y-` ..-í-e
000000f0	E8 A1 FA 7D EB E4 A1 7D-80 EB DF 98 CD 16 CD 19 iú)éä;] èä-i-i-
00000100	66 60 80 7E 02 00 OF 84-20 00 66 GA 00 66 50 06 f' ..-..-fj-fp
00000110	53 66 68 10 00 01 B4-42 SA 56 40 8B F4 C0 13 5th-... B-V8-öi-
00000120	66 58 66 58 66 58-EB 33 60 3B 46 F8 72 03 FXXFMXXBX3;For-
00000130	F9 EB 2A 66 33 D2 66 OF-B7 18 66 F7 F1 FE C2 üe*30f- N-f-npA
00000140	8A CA 66 8B D0 66 C1 EA-10 F7 78 1A 86 D6 8A 56 Ef-DFAé -v- O-V
00000150	40 CA 8E CO 64 06 0A CC-B8 01 02 CD 13 66 61 OF 0 èhå..i..f-fa-
00000160	82 74 FF 81 C3 00 02 66-40 49 75 94 C3 42 4F 4F ty Á- f81u ÁB00
00000170	54 4D 47 52 20 20 20-20 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 00
000001a0	00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
000001b0	73 6B 20 65 72 6F 72-FF 0D A0 50 72 65 73 73 sk errory -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 08 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 00 00-AC 01 B9 01 00 00 55 AA

Terdapat beberapa informasi penting yang dapat diperoleh dari entri sebuah direktori pada sistem FAT32. Informasi-informasi penting tersebut dapat dilihat dari:

- 32 Byte pertama digunakan sebagai volume label
- Untuk setiap folder dan file akan ada Long File Name Entry dimana entri ini bergantung pada panjang dari nama folder/file tersebut.
- Terdapat base entry dimana mengandung meta data (32 Byte).

DIRECTORY ENTRIES:		
000	52 45 4D 4F 56 41 42 4C-45 20 20 08 00 00 00 00 00	REMovable
010	00 00 00 00 00 00 67 62-2B 53 00 00 00 00 00 00 00 00gb+S.....
020	42 20 00 49 00 6E 00 66-00 6F 00 0F 00 72 72 00	B -I-n-f-o...rr-
030	6D 00 61 00 74 00 69 00-6F 00 00 00 6E 00 00 00	m-a-t-i-o...n...
040	01 53 00 79 00 73 00 74-00 65 00 0F 00 72 6D 00	.S-y-s-t-e...rm-
050	20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00	.V-o-l-u...m-e-
060	53 59 53 54 45 4D 7E 31-20 20 20 16 00 4F 66 62	SYSTEM-1 ..-Ofb
070	2B 53 2B 53 00 00 67 62-2B 53 03 00 00 00 00 00 00 00	+S+S..gb+S.....
080	41 53 00 75 00 62 00 66-00 6F 00 0F 00 A1 6C 00	AS-u-b-f-o...j1-
090	64 00 65 00 72 00 5F 00-30 00 00 00 00 00 FF FF	d-e-r._-0.....yy
0a0	53 55 42 46 4F 4C 7E 31-20 20 20 10 00 84 04 54	SUBFOL-1T
0b0	2D 53 2D 53 00 00 05 54-2D 53 06 00 00 00 00 00 00 00	2S-S...T-S.....
0c0	41 44 00 6F 00 63 00 75-00 6D 00 0F 00 A7 65 00	AD-o-c-u-m...Se-
0d0	6E 00 74 00 35 00 2E 00-74 00 00 00 78 00 74 00	n-t-5..t...x-t.
0e0	44 4F 43 55 4D 45 7E 31-54 58 54 20 00 29 92 54	DOCUME~1TXT ..) -T
0f0	2D 53 2D 53 00 00 93 54-2D 53 10 00 F8 2A 00 00	-S-S...T-S...@^...

Pada metadata Base Entry, terdapat informasi-informasi penting juga yang perlu kita tafsirkan:

DIRECTORY ENTRIES -BASE ENTRY METADATA:	
41 44 00 6F 00 63 00 75-00 6D 00 0F 00 A7 65 00	AD-o-c-u-m...Se..
6E 00 74 00 35 00 2E 00-74 00 00 00 78 00 74 00	n-t-5..t...x-t.
44 4F 43 55 4D 45 7E 31-54 58 54 20 00 29 92 54	DOCUME~1TXT ..) -T
2D 53 2D 53 00 00 93 54-2D 53 10 00 F8 2A 00 00	-S-S...T-S...@^...
DOS 8.3 Converted file name (8 UC letters + 3 UC extension)	
File attribute (1 byte) - 0x20 or 0010 0000 in binary)	File Attributes:
Milliseconds of creation time - 0x29 (41 in decimal)	Need to convert to binary:
File Creation TIME - DOS Timestamp (Local time)	0000 0001 - read only
File Creation DATE - DOS (Local time)	0000 0010 - hidden
Last Access DATE - DOS (Local time)	0000 0100 - system file
Starting Cluster for the file contents (Higher Bits + Lower Bits)	0000 1000 - volume label entry
Content's modification TIME and DATE	0001 0000 - directory
FILE SIZE in BYTES - the max value is (0xFF FF FF FF = 4095MB)	0010 0000 - archive or normal file

Melalui metadata base entry tersebut, kita dapat menentukan cluster size, file size, file modification date, file attribute, dsb. Selanjutnya video akan lanjut kepada tahap praktik. Namun perlu diingat bahwa mempelajari metadata pada FAT file system merupakan hal yang penting karena sebagai seorang forensik digital, kita tidak sebaiknya terkecoh oleh struktur file system yang digunakan (seperti sifat *deleted file/folder* yang sebenarnya tidak dihapus dari file tersebut namun hanya ditandai sebagai dihapus).

2. Ringkasan Praktik:

Bagian FAT32 Example

- Melakukan inspeksi metadata pada *base record* yang berada pada *system folder*. Melalui meta data ini kita bisa mengetahui *file attributes*, di cluster mana file tersebut berada, dll. Contoh hal yang dilakukan pada bagian ini:

- Pada *base record* di *system folder*, terdapat *flag* dengan hex 16 (2 Byte) yaitu dapat direpresentasikan sebagai 0001 0110. Byte pertama (1) menandakan bahwa entri merupakan sebuah direktori (benar karena *system folder* merupakan sebuah direktori), bit (1) yang kedua menandakan bahwa entri tersebut adalah sebuah *system file* dan terakhir bit (1) yang ketiga menandakan bahwa file tersebut *hidden*.
- Akan tetapi pada Document 1.txt, dapat dilihat bahwa flagnya adalah 20 (0010 0000), dimana berarti bahwa ***archive or normal file***.
- System Folder:

00000050	20 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00	-V-o-1-u...m-e...
00000060	53 59 53 54 45 4D 7E 31-20 20 20 16 00 4F 66 62	SYSTEM~1 .Ofb

- Document 1.txt:

000000d0	6E 00 74 00 35 00 2E 00-74 00 00 00 78 00 74 00	n-t-5..t...x-t...
000000e0	44 4F 43 55 4D 45 7E 31-54 58 54 20 00 29 92 54	DOCUME~1TXT) -T

- Kita juga bisa menggunakan hex intepreter pada FTK imager untuk melihat makna hex code yang kita lihat (contoh lebih lagi dapat dilihat pada bagian screenshot praktik).

- Melalui meta data tersebut, kita bisa melihat starting cluster contentnya, yaitu berada pada:

00000060	53 59 53 54 45 4D 7E 31-20 20 20 16 00 4F 66 62	SYSTEM~1 ..VID
00000070	2B 53 2B 53 00 00 67 62-2B 53 03 00 00 00 00 00	+S+S-.gb+S.....

- Cluster: 0x0003 = 3.
- Selanjutnya kita bisa melakukan pengecekan pada cluster tersebut untuk melihat cluster berikutnya dimana suatu konten berada.

Bagian FAT32 Example with Delete Files:

- Direktori entry dan base entry *Deleted Files* tidak menghilang dari image. Hal ini berarti bahwa kita masih dapat melihat meta data, file name, dll. Pada FAT file system, 0xE5 menandakan bahwa file/folder tersebut telah dihapus. Proses ini melakukan proses *overwrite* karakter pertama pada nama file/folder tersebut. Hal ini berarti file/folder yang memiliki character pertama 0xE5 pada FAT File system, harus disembunyikan dari user (*hide*), lalu membuat sistem memahami bahwa cluster tersebut sudah dapat di *overwrite*.

190	2D 53 2D 53 00 00 00 93 54-2D 53	E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 DA 65 00	-S-S...T-S...A...
1d0	6E 00 74 00 34 00 2E 00-74 00 00 00 78 00 74 00	n-t-4...t...x-t-	
1e0	E5 4F 32 31 42 30 7E 31-54 58 54 20 00 29 92 54	å021B0~1TXT) -T	
1f0	2D 53 2D 53 00 00 93 54-2D 53 18 00 60 22 00 00	-S-S...T-S...`"...	
200	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	

- Seperti yang dieksaminasi sebelumnya, LFN sendiri tidak terbatas hanya 32 Bytes saja, untuk nama file yang panjang, mereka akan berjumlah sebanyak Yx32b, dimana **Y** bergantung terhadap panjang dari filename tersebut. Apabila file dengan nama panjang tersebut dihapus maka untuk setiap entri pertama 32b pada LFN juga akan diubah menjadi 0xE5.

080	E5 79 00 76 00 65 00 72-00 79 00 0F 00 0B 76 00	åy·v·e·r·y···v·
090	65 00 72 00 79 00 76 00-65 00 00 00 72 00 79 00	e·r·y·v·e···r·y·
0a0	E5 72 00 79 00 76 00 65-00 72 00 0F 00 0B 79 00	åw·v·e·r·y···v·

Bagian FAT32 Example with Delete Files and overwritten:

- Pada Fat32 File system, file/folder yang di delete dapat di *overwritten* apabila tedapat cluster yang kosong/tidak digunakan. Contohnya, cluster yang harusnya dimiliki oleh Document 8.txt, sekarang ditempati oleh Subfolder 19 (pada cluster 41).

Bukti: (menggunakan meta data pada base entry untuk melihat clusternya).

190	2D 53 2D 53 00 00 00 93 54-2D 53	E5 00 00 44 00 00	-S-S...T-S...A...
1a0	E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 31 65 00	åD-o-c-u-m...Ùe-	
1b0	6E 00 74 00 39 00 2E 00-74 00 00 00 78 00 74 00	n-t-9...t...x-t-	
1c0	E5 4F 37 33 31 7E 31-54 58 54 20 00 29 92 54	å021B0~1TXT) -T	
1d0	2D 53 2D 53 00 00 93 54-2D 53	2E 00 58 4D 00 00	-S-S...T-S...XH...
1e0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
1f0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
200	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
210	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
220	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
230	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
240	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
250	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
260	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
270	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
280	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
290	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2a0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2b0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2c0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2d0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2e0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
2f0	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
300	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
310	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
320	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
330	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
340	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
350	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
360	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
370	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	
380	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00	

Hex Value Interpreter

Type	Si...	Value
signed int...	1-8	41
unsigned i...	1-8	41
FILETIME...	8	-
FILETIME...	8	-
DOS date	2	09/01/1980
DOS time	2	00:01:18
time_t (UT...	4	-
time_t (loc...	4	-

Byte Little endian Big endian

00027000	2E 20 20 20 20 20 20 20-20 20 20 10 00 0F 37 7D7}
00027010	2D 53 2D 53 00 00 38 7D-2D 53 29 00 00 00 00 00	-S-S...8)-S)
00027020	2E 2E 20 20 20 20 20 20-20 20 20 10 00 0F 37 7D7}
00027030	2D 53 2D 53 00 00 38 7D-2D 53 1A 00 00 00 00 00	-S-S...8)-S
00027040	41 53 00 75 00 62 00 66-00 6F 00 0F 00 A1 6C 00	AS-u-b-f-o...;1-
00027050	64 00 65 00 72 00 5F 00-31 00 00 00 39 00 00 00	d-e-r_-1...9...
00027060	53 55 42 46 4F 4C 7E 31-20 20 20 10 00 11 37 7D	SUBFOL~17}
00027070	2D 53 2D 53 00 00 38 7D-2D 53 2A 00 00 00 00 00	-S-S...8)-S*
00027080	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00

Cursor pos = 159744; clus = 41; log sec = 16696

- Dapat dilihat bahwa apabila suatu directory dihapus, maka apabila ada yang melakukan proses *overwrite* pada directory tersebut, directory yang berada di dalam directory tersebut juga akan terkena proses *overwritten*. Contohnya,

subfolder 6 berada pada cluster 12 sebelumnya, subfolder 7 berada pada cluster 13, dan seterusnya. Namun, pada praktik ketiga, dilihat bahwa cluster 12, 13, dst ditempati oleh subfolder 11, 12, dst.

Bagian Autopsy:

- Menggunakan autopsy, apabila orang tidak familiar dengan bagaimana proses overwritten deleted file dan folder bekerja pada FAT 32 File System, mereka dapat saja salah menangkap bahwa metadata suatu file/folder yang di *overwrite* tersebut adalah metadata yang sesungguhnya. Namun karena konten tersebut sudah dilakukan *overwritten* maka kita sekarang sudah mengerti **metadata suatu deleted files/folders tidak selalu** merujuk pada metadata asli mereka.

3. Screenshot Praktik:

Bagian FAT32 Example

- Inspecting Meta Data

Creation Time:

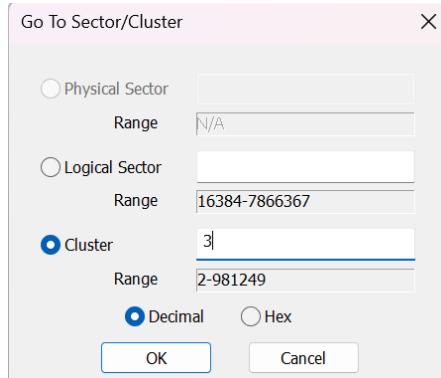
The screenshot shows two windows from the Autopsy tool. The left window, 'Hex Value Interpreter', displays memory dump data with several entries for 'signed int' and 'unsigned int' at addresses 18 and 21. The right window, 'File List', shows a tree view of the file system structure. The root directory contains a file named '[root]' and an 'unallocated space' entry. Below the root are two FAT tables (FAT1 and FAT2), a 'reserved sectors' entry, and a VBR (Volume Boot Record). The 'File List' pane also includes a 'File List' table with columns for Name, Size, Type, and Date Mod.

Creation Date:

This screenshot is similar to the previous one but focuses on creation date metadata. It shows the same 'Hex Value Interpreter' and 'File List' panes. The 'File List' table shows the same structure as before, with the addition of 'FILETIME' entries under the root directory. These entries represent the creation times of the files and folders in the file system.

Last Accessed Date:

- Going to cluster 3



Content Modification Time:

This screenshot shows the 'Hex Value Interpreter' and 'File List' panes again. The 'File List' table includes 'FILETIME' entries under the root directory, representing the last modified times of the files and folders. The 'File List' table columns are Name, Size, Type, and Date Mod.

Cluster bit: 0003

Metadata pada cluster 3:

00001000	2E 20 20 20 20 20 20 20-20 20 20 10 00 4F 66 62	.	·Ofb
00001010	2B 53 2B 53 00 00 67 62-2B 53 03 00 00 00 00 00	+S+S ·gb+S ·.....	
00001020	2E 2E 20 20 20 20 20 20-20 20 20 10 00 4F 66 62	..	·Ofb
00001030	2B 53 2B 53 00 00 67 62-2B 53 00 00 00 00 00 00	+S+S ·gb+S ·.....	
00001040	42 74 00 00 00 FF FF FF-FF FF FF 0F 00 CE FF FF	Bt ··yyyyyy ·iy	
00001050	FF FF FF FF FF FF FF FF 00 00 FF FF FF FF	yyyyyyyyyyyy ·yyyy	
00001060	01 57 00 50 00 53 00 65-00 74 00 0F 00 CE 74 00	·W·P·S·e·t···ít·	
00001070	69 00 6E 00 67 00 73 00-2E 00 00 00 64 00 61 00	i·n·g·s···d·a·	
00001080	57 50 53 45 54 54 7E 31-44 41 54 20 00 51 66 62	WPSETT~1DAT ·Qfb	
00001090	2B 53 2B 53 00 00 67 62-2B 53 04 00 0C 00 00 00	+S+S ·gb+S ·.....	
000010a0	42 47 00 75 00 69 00 64-00 00 00 0F 00 FF FF FF	BG·u·i·d···yyy	
000010b0	FF FF FF FF FF FF FF FF 00 00 FF FF FF FF	yyyyyyyyyyyy ·yyy	
000010c0	01 49 00 6E 00 64 00 65-00 78 00 0F 00 FF 65 00	·I·n·d·e·x···ye·	
000010d0	72 00 56 00 6F 00 6C 00-75 00 00 00 6D 00 65 00	r·V·o·l·u···m·e·	
000010e0	49 4E 44 45 58 45 7E 31-20 20 20 00 8E 68 62	INDEXE~1 ··hb	
000010f0	2B 53 2B 53 00 00 69 62-2B 53 05 00 4C 00 00 00	+S+S ·ib+S ·L··	

Bagian FAT32 Example with Deleted Files:

Evidence tree	Hex Value Interp...	File LIST																																
<ul style="list-style-type: none"> \\\PHYSICALDRIVE0 <ul style="list-style-type: none"> EFI system partition (1) [2] Microsoft reserved partition Basic data partition (3) [4] Basic data partition (4) [10] <ul style="list-style-type: none"> Unpartitioned Space [GP] FAT_32_Example_01.E01 FAT32_Example_01_with_d <ul style="list-style-type: none"> [root] [unallocated space] 	Type Si... Valu	<table border="1"> <thead> <tr> <th>Name</th><th>Size</th><th>Type</th><th>Date Modified</th></tr> </thead> <tbody> <tr><td>Subfolder_0</td><td>4</td><td>Directory</td><td>13/09/2021 10:...</td></tr> <tr><td>System Volume Information</td><td>4</td><td>Directory</td><td>11/09/2021 12:...</td></tr> <tr><td>Document1.txt</td><td>3</td><td>Regular F...</td><td>13/09/2021 10:...</td></tr> <tr><td>Document2.txt</td><td>5</td><td>Regular F...</td><td>13/09/2021 10:...</td></tr> <tr><td>Document3.txt</td><td>7</td><td>Regular F...</td><td>13/09/2021 10:...</td></tr> <tr><td>Document4.txt</td><td>9</td><td>Regular F...</td><td>13/09/2021 10:...</td></tr> <tr><td>Document5.txt</td><td>11</td><td>Regular F...</td><td>13/09/2021 10:...</td></tr> </tbody> </table>	Name	Size	Type	Date Modified	Subfolder_0	4	Directory	13/09/2021 10:...	System Volume Information	4	Directory	11/09/2021 12:...	Document1.txt	3	Regular F...	13/09/2021 10:...	Document2.txt	5	Regular F...	13/09/2021 10:...	Document3.txt	7	Regular F...	13/09/2021 10:...	Document4.txt	9	Regular F...	13/09/2021 10:...	Document5.txt	11	Regular F...	13/09/2021 10:...
Name	Size	Type	Date Modified																															
Subfolder_0	4	Directory	13/09/2021 10:...																															
System Volume Information	4	Directory	11/09/2021 12:...																															
Document1.txt	3	Regular F...	13/09/2021 10:...																															
Document2.txt	5	Regular F...	13/09/2021 10:...																															
Document3.txt	7	Regular F...	13/09/2021 10:...																															
Document4.txt	9	Regular F...	13/09/2021 10:...																															
Document5.txt	11	Regular F...	13/09/2021 10:...																															

MetaData Document4.txt (LFN, Base Entry):

Dimana 1c0 - 1d0: LFN dan 1e0 - 1f0: Base Entry

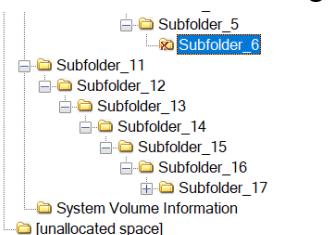
1c0	E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 DA 65 00	-d-c-u-m-Úe-
1d0	6E 00 74 00 34 00 2E 00-74 00 00 00 78 00 74 00	n·t·4···t··x·t·
1e0	E5 4F 32 31 42 30 7E 31-54 58 54 20 00 29 92 54	·021B0~1TXT ·)·T
1f0	2D 53 2D 53 00 00 93 54-2D 53 18 00 60 22 00 00	-S-S··T-S··`··

Metadata Subfolder 9 yang memiliki deleted files (karena directory sebelumnya dihapus juga) dengan nama yang panjang:

000	2E 20 20 20 20 20 20 20 20-20 20 20 10 00 99 04 54T
010	2D 53 2D 53 00 00 05 54-2D 53 0F 00 00 00 00 00	-S-S	...T-S.....
020	2E 20 20 20 20 20 20 20-20 20 20 10 00 99 04 54T
030	2D 53 2D 53 00 00 05 54-2D 53 0E 00 00 00 00 00	-S-S	...T-S.....
040	E5 2E 00 74 00 78 00 74-00 00 00 0F 00 0B FF FF	å.	.t-x-t.....ÿÿ
050	FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF FF	ÿÿÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿ
060	E5 76 00 65 00 72 00 79-00 6C 00 0F 00 0B 6F 00	åv	e-r-y-l...o-
070	6E 00 67 00 6E 00 61 00-6D 00 00 00 65 00 32 00	n-g-n-a-m...e-2-	
080	E5 79 00 76 00 65 00 72-00 79 00 0F 00 0B 76 00	åy	v-e-r-y...v-
090	65 00 72 00 79 00 76 00-65 00 00 00 72 00 79 00	e-r-y-v-e...r-y-	
0a0	E5 72 00 79 00 76 00 65-00 72 00 0F 00 0B 79 00	år	y-v-e-r...y-
0b0	76 00 65 00 72 00 79 00-76 00 00 00 65 00 72 00	v-e-r-y-v...e-r-	
0c0	E5 65 00 72 00 79 00 76-00 65 00 0F 00 0B 72 00	åe	r-y-v-e...r-
0d0	79 00 76 00 65 00 72 00-79 00 00 00 76 00 65 00	y-v-e-r-y...v-e-	
0e0	E5 76 00 65 00 72 00 79-00 76 00 0F 00 0B 65 00	åv	e-r-y-v...e-
0f0	72 00 79 00 76 00 65 00-72 00 00 00 79 00 76 00	r-y-v-e-r...y-v-	
100	E5 79 00 76 00 65 00 72-00 79 00 0F 00 0B 76 00	åy	v-e-r-y...v-
110	65 00 72 00 79 00 76 00-65 00 00 00 72 00 79 00	e-r-y-v-e...r-y-	
120	E5 72 00 79 00 76 00 65-00 72 00 0F 00 0B 79 00	år	y-v-e-r...y-
130	76 00 65 00 72 00 79 00-76 00 00 00 65 00 72 00	v-e-r-y-v...e-r-	
140	E5 65 00 72 00 79 00 76-00 65 00 0F 00 0B 72 00	åe	r-y-v-e...r-
150	79 00 76 00 65 00 72 00-79 00 00 00 76 00 65 00	y-v-e-r-y...v-e-	
160	E5 76 00 65 00 72 00 79-00 76 00 0F 00 0B 65 00	åv	e-r-y-v...e-
170	72 00 79 00 76 00 65 00-72 00 00 00 79 00 76 00	r-y-v-e-r...y-v-	
180	E5 79 00 76 00 65 00 72-00 79 00 0F 00 0B 76 00	åy	v-e-r-y...v-
190	65 00 72 00 79 00 76 00-65 00 00 00 72 00 79 00	e-r-y-v-e...r-y-	
1a0	E5 72 00 79 00 76 00 65-00 72 00 0F 00 0B 79 00	år	y-v-e-r...y-
1b0	76 00 65 00 72 00 79 00-76 00 00 00 65 00 72 00	v-e-r-y-v...e-r-	
1c0	E5 65 00 72 00 79 00 76-00 65 00 0F 00 0B 72 00	åe	r-y-v-e...r-
1d0	79 00 76 00 65 00 72 00-79 00 00 00 76 00 65 00	y-v-e-r-y...v-e-	
1e0	E5 76 00 65 00 72 00 79-00 76 00 0F 00 0B 65 00	åv	e-r-y-v...e-
1f0	72 00 79 00 76 00 65 00-72 00 00 00 79 00 76 00	r-y-v-e-r...y-v-	
200	E5 45 52 59 56 45 7E 31-54 58 54 20 00 8E 2E 55	åERYVE~1TXT	..U
210	2D 53 2D 53 00 00 2F 55-2D 53 F4 02 D0 84 00 00	-S-S	..-/U-S6-D...
220	E5 2E 00 74 00 78 00 74-00 00 00 0F 00 EB FF FF	å.	.t-x-t.....ÿÿ
230	FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF FF	ÿÿÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿ
240	E5 76 00 65 00 72 00 79-00 6C 00 0F 00 EB 6F 00	åv	e-r-y-l...ëo-
250	6E 00 67 00 6E 00 61 00-6D 00 00 00 65 00 31 00	n-g-n-a-m...e-1-	
260	E5 79 00 76 00 65 00 72-00 79 00 0F 00 EB 76 00	åy	v-e-r-y...ëv-
270	65 00 72 00 79 00 76 00-65 00 00 00 72 00 79 00	e-r-y-v-e...r-y-	
280	E5 72 00 79 00 76 00 65-00 72 00 0F 00 EB 79 00	år	y-v-e-r...ëy-
290	76 00 65 00 72 00 79 00-76 00 00 00 65 00 72 00	y-e-r-y-v...e-r-	"

Bagian FAT32 Example with Deleted Files and Overwritten:

Subfolder 6 sekarang:



Cursor pos = 0

Subfolder 6 sebelumnya:

File System Structure:

```

    └── Subfolder_0
        ├── Subfolder_1
        │   ├── Subfolder_2
        │   │   ├── Subfolder_3
        │   │   │   ├── Subfolder_4
        │   │   │   └── Subfolder_5
        │   │   └── Subfolder_6
        │   ├── Subfolder_7
        │   └── Subfolder_8
        └── Subfolder_9
    └── System Volume Information
    └── [unallocated space]

```

File List:

```

050: 64 00 65 00 72 00 5F 00-37 00 00 00 00 00 FF FF d-e-r- -7-----yy
060: E5 55 42 46 4F 4C 7E 31-20 20 20 10 00 95 04 54 ÅUBFOL-1 -----T
070: 2D 53 2D 53 00 00 05 54-2D 53 0D 00 00 10 00 00 -S-S---T-S-----
080: E5 74 00 00 00 FF FF FF-FF FF FF 00 A7 FF FF Å---yyyyy-SYY
090: FF FF FF FF FF FF FF FF FF 00 00 FF FF FF FF FFFFFF yyyyyyyyyy-yyyy
0a0: E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 A7 65 00 ÄD-o-c-u-m---Se-
0b0: 6E 00 74 00 34 00 30 00-2E 00 00 00 74 00 78 00 n-t 4-0-----t-x-
0c0: E5 4F 43 55 4D 45 7E 31-54 58 54 20 00 2E 92 54 ÅOCUME-1TXT ..-T
0d0: 2D 53 2D 53 00 00 93 54-2D 53 82 01 60 67 01 00 -S-S---T-S---g-
0e0: E5 74 00 00 00 FF FF FF-FF FF FF 00 08 7F FF Å---yyyyy-yy
0f0: FF FFFFFF yyyyyyyyyy-yyyy
100: E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 87 65 00 ÄD-o-c-u-m---e-
110: 6E 00 74 00 33 00 36 00-2E 00 00 00 74 00 78 00 n-t 3-6-----t-x-
120: E5 4F 43 55 4D 45 7E 32-54 58 54 20 00 2D 92 54 ÅOCUME-2TXT ..-T
130: 2D 53 2D 53 00 00 93 54-2D 53 99 01 70 43 01 00 -S-S---T-S---pC-
140: E5 74 00 00 00 FF FF FF-FF FF FF 00 07 FF FF Å---yyyyy-gyy
150: FF FFFFFF yyyyyyyyyy-yyyy
160: E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 67 65 00 ÄD-o-c-u-m---ge-
170: 6E 00 74 00 33 00 37 00-2E 00 00 00 74 00 78 00 n-t 3-7-----t-x-
180: E5 4F 43 55 4D 45 7E 33-54 58 54 20 00 2D 92 54 ÅOCUME-3TXT ..-T
190: 2D 53 2D 53 00 00 93 54-2D 53 AE 01 6C 40 01 00 -S-S---T-S---1L-
1a0: E5 74 00 00 00 FF FF FF-FF FF FF 00 07 C7 FF FF Å---yyyyy-Cyy
1b0: FF FFFFFF yyyyyyyyyy-yyyy
1c0: E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 C7 65 00 ÄD-o-c-u-m---Ce-
1d0: 6E 00 74 00 33 00 38 00-2E 00 00 00 74 00 78 00 n-t 3-8-----t-x-
1e0: E5 4F 43 55 4D 45 7E 34-54 58 54 20 00 2E 92 54 ÅOCUME-4TXT ..-T
1f0: 2D 53 2D 53 00 00 93 54-2D 53 C3 01 68 55 01 00 -S-S---T-S---hU-
200: E5 74 00 00 00 FF FF FF-FF FF FF 00 02 E2 FF FF Å---yyyyy-äyy
210: FF FFFFFF yyyyyyyyyy-yyyy
220: E5 44 00 6F 00 63 00 75-00 6D 00 0F 00 E2 65 00 ÄD-o-c-u-m---æ-
230: 6E 00 74 00 33 00 39 00-2E 00 00 00 74 00 78 00 n-t 3-9-----t-x-
240: E5 4F 32 43 33 32 7E 31-54 58 54 20 00 2E 92 54 Å02C32-1TXT ..-T
250: 2D 53 2D 53 00 00 93 54-2D 53 D9 01 64 5E 01 00 -S-S---T-S---d^-
260: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
270: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
280: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
290: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2a0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2b0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2c0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2d0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2e0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
2f0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
300: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
310: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
320: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
330: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
340: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
350: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
360: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
370: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
380: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-
390: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-

```

Cursor pos = 0; clus = 12; log sec = 16464

Listed: 6 Selected: 0 FAT32_Example_01_with_deleted_files.E01/REMOVABLE [FAT32]/[root]/Subfolder_0/Subfolder_1/Subfol

Cluster 12 sekarang:

Bagian Autopsy:

Name	S	C	O	Modified Time	Change Time	Access Time	Cr
Subfolder_6				2021-09-13 10:32:10 EEST	0000-00-00 00:00:00	2021-09-13 00:00:00 EEST	2021-09-13 00:00:00
Document8.txt				2021-09-13 10:36:38 EEST	0000-00-00 00:00:00	2021-09-13 00:00:00 EEST	2021-09-13 00:00:00
Document9.txt				2021-09-13 10:36:38 EEST	0000-00-00 00:00:00	2021-09-13 00:00:00 EEST	2021-09-13 00:00:00
Document4.txt				2021-09-13 10:36:38 EEST	0000-00-00 00:00:00	2021-09-13 00:00:00 EEST	2021-09-13 00:00:00

4. Refleksi:

- Menurut saya untuk materi seperti membaca metadata dalam suatu file merupakan hal yang sulit. Banyak sekali hal-hal yang perlu ditentukan (mungkin karena saya belum terbiasa) seperti metadata pada base entry (misalnya menentukan File Creation Time, File Creation Date, File attribute, dll).
- Melalui video ini, saya belajar bahwa, hal-hal tersebut membutuhkan pengetahuan dan juga pengalaman yang lumayan banyak menurut saya. Hal ini juga tentunya merupakan hal baru untuk saya, biasanya saya tidak terlalu memperhatikan metadata dan hanya menginspeksi informasi-informasi file melalui tool seperti autopsy, dll.

Pertanyaan:

- Hal yang cukup membingungkan bagi saya adalah pada praktik **FAT32_example_01_deleted_and_overwritten**. Melalui base entry yang menandakan tempat **Document8.txt** berada pada cluster 41 dimana cluster 41 berisi informasi mengenai subfolder 19. Akan tetapi mengapa pada cluster 44, terdapat content **Document8.txt**?

```
0002a000| 6F 63 75 6D 65 6E 74 20-38 20 63 6F 6E 74 65 6E | document 8 conten
0002a010| 74 20 6F 66 20 64 6F 63-75 6D 65 6E 74 20 38 20 t of document 8
0002a020| 63 6F 6E 74 65 6E 74 20-6F 66 20 64 6F 63 75 6D | content of docum
0002a030| 65 6E 74 20 38 20 63 6F-6E 74 65 6E 74 20 6F 66 | ent 8 content of
0002a040| 20 64 6F 63 75 6D 65 6E-74 20 38 20 63 6F 6E 74 | document 8 cont
0002a050| 65 6E 74 20 6F 66 20 64-6F 63 75 6D 65 6E 74 20 | ent of document
0002a060| 38 20 63 6F 6E 74 65 6E-74 20 6F 66 20 64 6F 63 | 8 content of doc
0002a070| 75 6D 65 6E 74 20 38 20-63 6F 6E 74 65 6E 74 20 | ument 8 content
0002a080| 6F 66 20 64 6F 63 75 6D-65 6E 74 20 38 20 63 6F | of document 8 co
0002a090| 6E 74 65 6E 74 20 6F 66-20 64 6F 63 75 6D 65 6E | ntent of documen
0002a0a0| 74 20 38 20 63 6F 6E 74-65 6E 74 20 6F 66 20 64 | t 8 content of d
0002a0b0| 6F 63 75 6D 65 6E 74 20-38 20 63 6F 6E 74 65 6E | document 8 conten
0002a0c0| 74 20 6F 66 20 64 6F 63-75 6D 65 6E 74 20 38 20 t of document 8
0002a0d0| 63 6F 6E 74 65 6E 74 20-6F 66 20 64 6F 63 75 6D | content of docum
0002a0e0| 65 6E 74 20 38 20 63 6F-6E 74 65 6E 74 20 6F 66 | ent 8 content of
0002a0f0| 20 64 6F 63 75 6D 65 6E-74 20 38 20 63 6F 6E 74 | document 8 cont
0002a100| 65 6E 74 20 6F 66 20 64-6F 63 75 6D 65 6E 74 20 | ent of document
0002a110| 38 20 63 6F 6E 74 65 6E-74 20 6F 66 20 64 6F 63 | 8 content of doc
0002a120| 75 6D 65 6E 74 20 38 20-63 6F 6E 74 65 6E 74 20 | ument 8 content
0002a130| 6F 66 20 64 6F 63 75 6D-65 6E 74 20 38 20 63 6F | of document 8 co
0002a140| 6E 74 65 6E 74 20 6F 66-20 64 6F 63 75 6D 65 6E | ntent of documen
0002a150| 74 20 38 20 63 6F 6E 74-65 6E 74 20 6F 66 20 64 | t 8 content of d
0002a160| 6F 63 75 6D 65 6E 74 20-38 20 63 6F 6E 74 65 6E | document 8 conten
0002a170| 74 20 6F 66 20 64 6F 63-75 6D 65 6E 74 20 38 20 t of document 8
0002a180| 63 6F 6E 74 65 6E 74 20-6F 66 20 64 6F 63 75 6D | content of docum
0002a190| 65 6E 74 20 38 20 63 6F-6E 74 65 6E 74 20 6F 66 | ent 8 content of
0002a1a0| 20 64 6F 63 75 6D 65 6E-74 20 38 20 63 6F 6E 74 | document 8 cont
0002a1b0| 65 6E 74 20 6F 66 20 64-6F 63 75 6D 65 6E 74 20 | ent of document
0002a1c0| 38 20 63 6F 6E 74 65 6E-74 20 6F 66 20 64 6F 63 | 8 content of doc
0002a1d0| 75 6D 65 6E 74 20 38 20-63 6F 6E 74 65 6E 74 20 | ument 8 content
0002a1e0| 6F 66 20 64 6F 63 75 6D-65 6E 74 20 38 20 63 6F | of document 8 co
0002a1f0| 6E 74 65 6E 74 20 6F 66-20 64 6F 63 75 6D 65 6E | ntent of documen
0002a200| 74 20 38 20 63 6F 6E 74-65 6E 74 20 6F 66 20 64 | t 8 content of d
```

Cursor pos = 172264; clus = 44; log sec = 16720