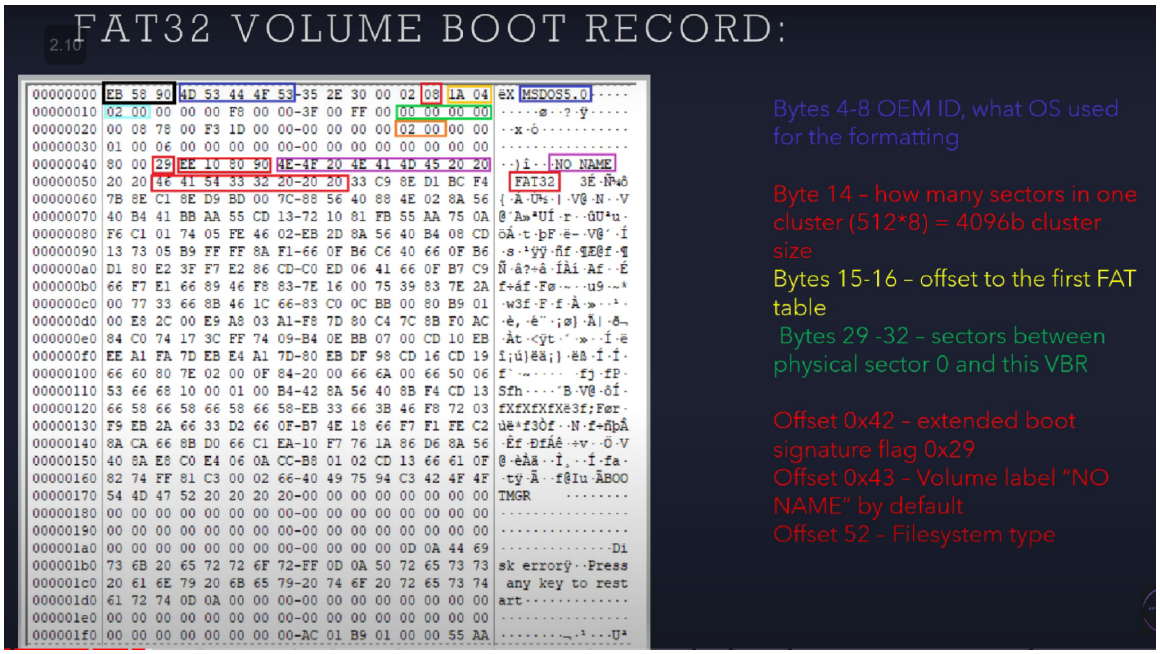
FAT File System
Alvaro Austin 216752180

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:

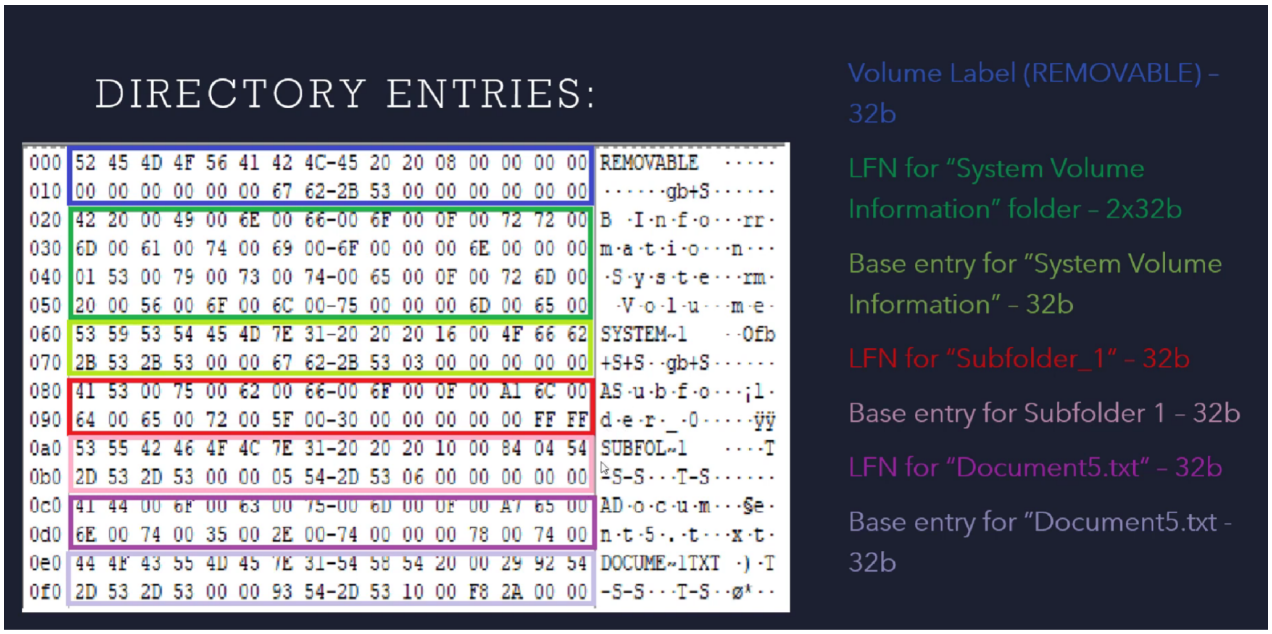
- Schematic Representation: pada FAT16, root directory masih berada pada system area yang menyebabkan root directory tersebut memiliki besaran yang tetap (*fixed size*). Akan tetapi pada FAT32, root directory berada data area yang menyebabkan root directory bisa meningkat besarannya beradasarkan *space* 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 (0xFFFFFF = 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:

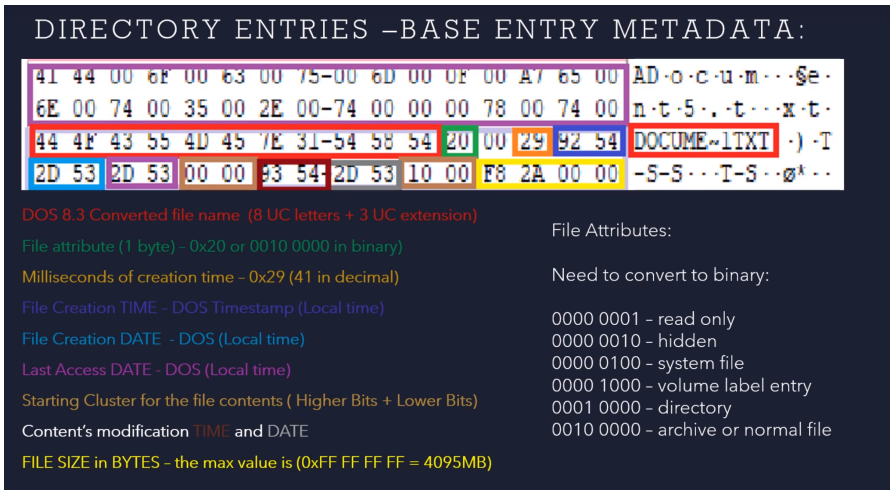


Terdapat beberapa informasi penting yang dapat diperoleh dari entri sebuah direktori pada system FAT32. Informasi-informasi penting tersebut dapat dilihat dari:

- 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).



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

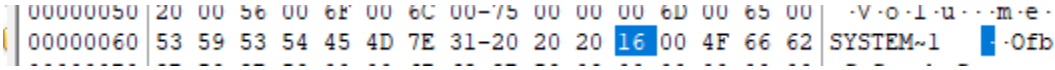


Melalui metadata base entry tersebut, kita dapat menentukkan cluster size, file size, file modification date, file attribute, dsb. Selanjutnya video akan lanjut kepada tahap praktik. Namun perlu diingat bahwa mempelajari metadata pada FAT file system merupakan hal yang penting karena sebagai seorang 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).

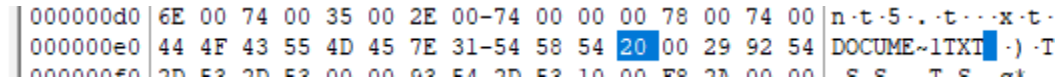
2. **Ringkasan Praktik:**

Bagian FAT32 Example

1. 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:

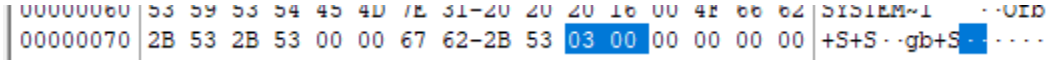


    - Document 1.txt:



    - 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).

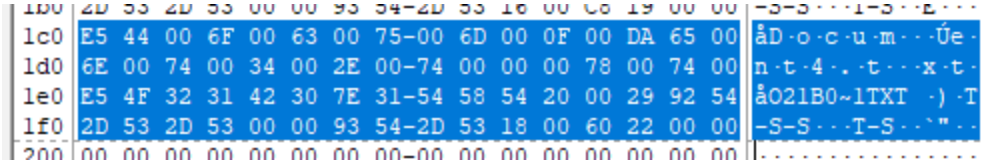
    - Melalui meta data tersebut, kita bisa melihat starting cluster contentnya, yaitu berada pada:



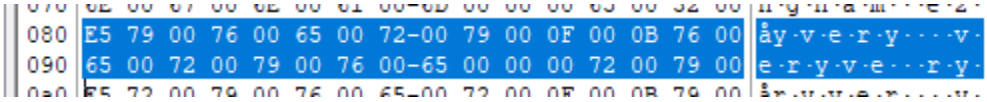
    - Cluster: 0x0003 = 3.
    - Selanjutnya kita bisa melakukan pengecekan pada cluster tersebut untuk melihat cluster berikutnya dimana suatu konten berada.

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 menandakkan 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*.



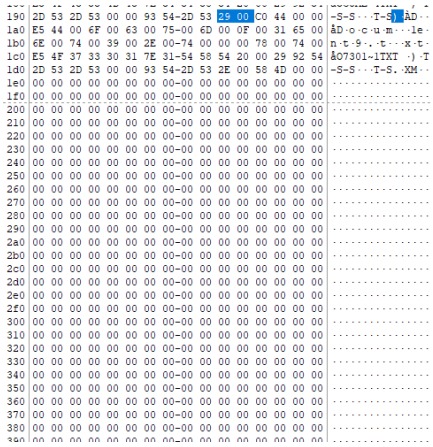
- Seperti yang dieksaminasi sebelumnya, LFN sendiri tidak terbatas hanya 32 Bytes saja, untuk nama file yang panjang, mereka akan berjumlah sebanyak **Y**x32b, dimana **Y** bergantung terhadap panjang dari filename tersebut. Apabila file dengan nama panjang tersebut dihapus maka untuk setiap entri pertama 32b pada LFN juga akan diubah menjadi 0xE5.

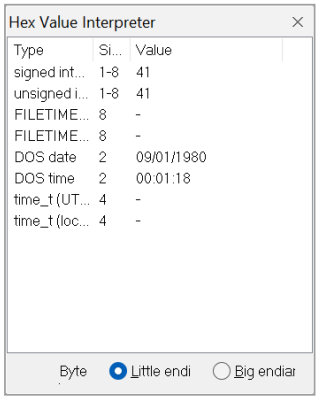


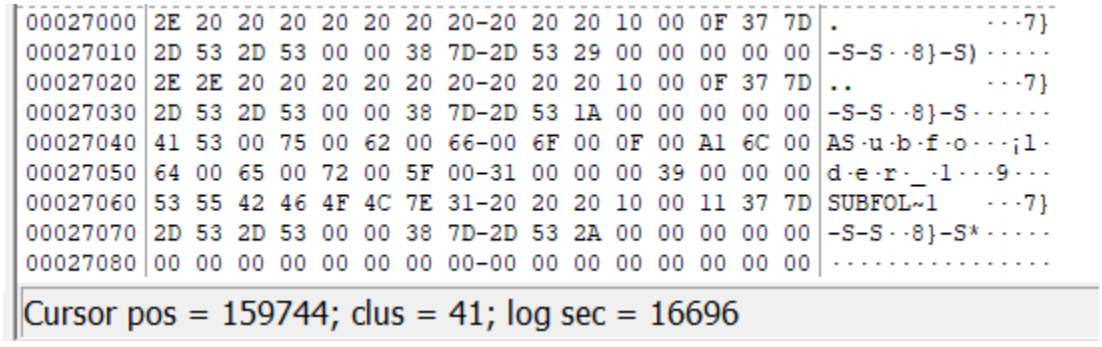
Bagian FAT32 Example with Delete Files and overwritten:

- 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).







- 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:

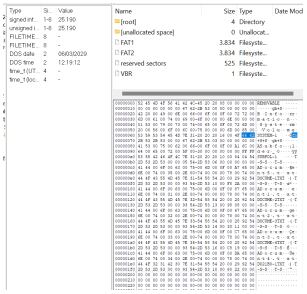
- Menggunakan autopsy, apabila orang tidak familiar dengan bagaimana proses overwritten deleted file dan folder bekerja pada FAT 32 File System, mereka dapat saja salah menangkap bahwa metadata suatu file/folder yang di *overwrite* tersebut adalah metadata yang sesungguhnya. Namun karena konten tersebut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

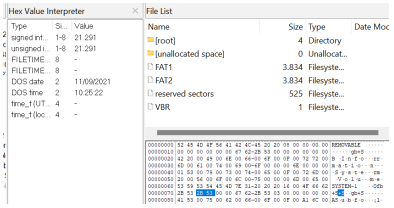
3. Screenshot Praktik:

Bagian FAT32 Example

- **Inspecting Meta Data**

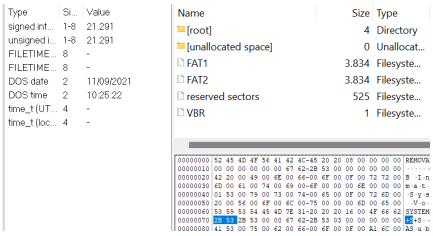
Creation Time:

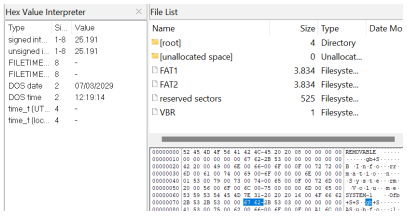




Content Modification Time:

Creation Date:

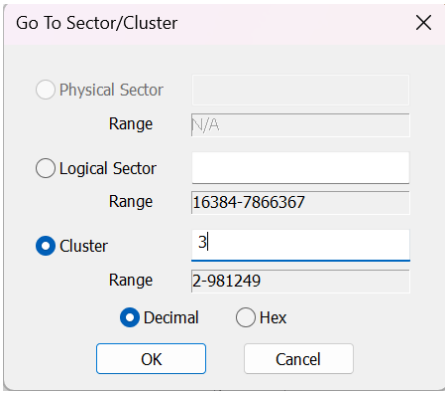




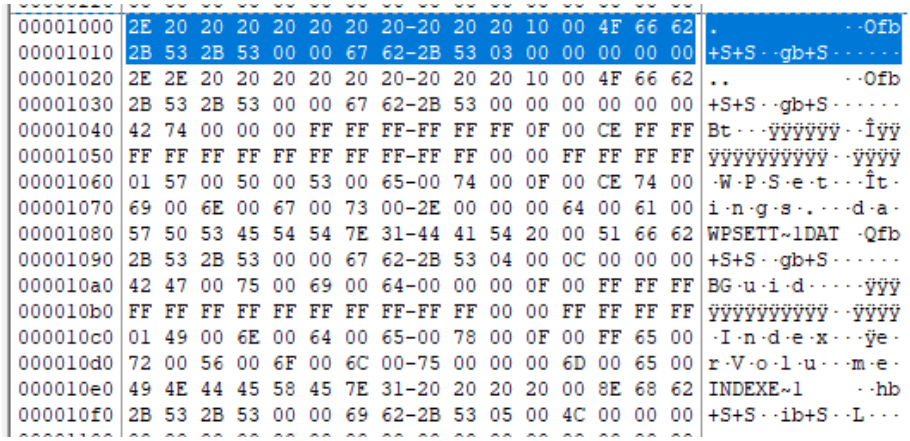
Cluster bit: 0003

Last Accessed Date:

- **Going to cluster 3**

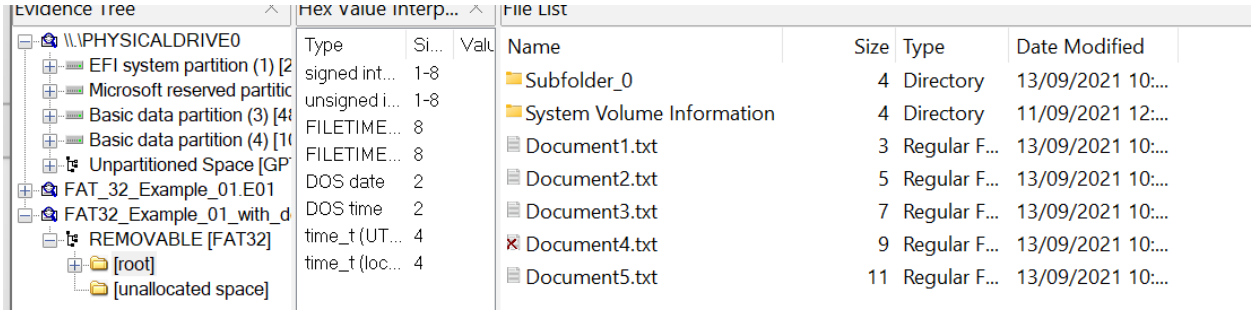


Metadata pada cluster 3:



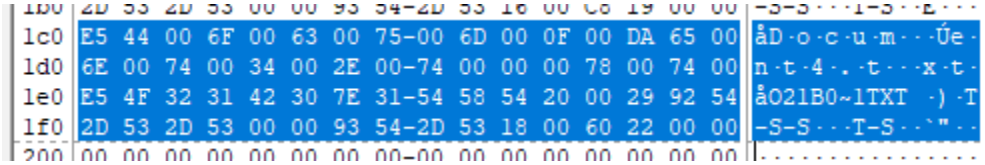
00001000	2E	20	20	20	20	20	20	20-20	20	20	10	00	4F	66	62	. ·Ofb
00001010	2B	53	2B	53	00	00	67	62-2B	53	03	00	00	00	00	00	+S+S··gb+S·····
00001020	2E	2E	20	20	20	20	20	20-20	20	20	10	00	4F	66	62	.. ·Ofb
00001030	2B	53	2B	53	00	00	67	62-2B	53	00	00	00	00	00	00	+S+S··gb+S·····
00001040	42	74	00	00	00	FF	FF	FF-FF	FF	FF	0F	00	CE	FF	FF	Bt···ÿÿÿÿÿÿ··Îÿÿ
00001050	FF	FF	FF	FF	FF	FF	FF	FF-FF	FF	00	00	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
00001060	01	57	00	50	00	53	00	65-00	74	00	0F	00	CE	74	00	·W·P·S·e·t···Ît·
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·····ÿÿÿ
000010b0	FF	FF	FF	FF	FF	FF	FF	FF-FF	FF	00	00	FF	FF	FF	FF	ÿÿÿÿÿÿÿÿÿÿ··ÿÿÿÿ
000010c0	01	49	00	6E	00	64	00	65-00	78	00	0F	00	FF	65	00	·I·n·d·e·x···ÿe·
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	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:



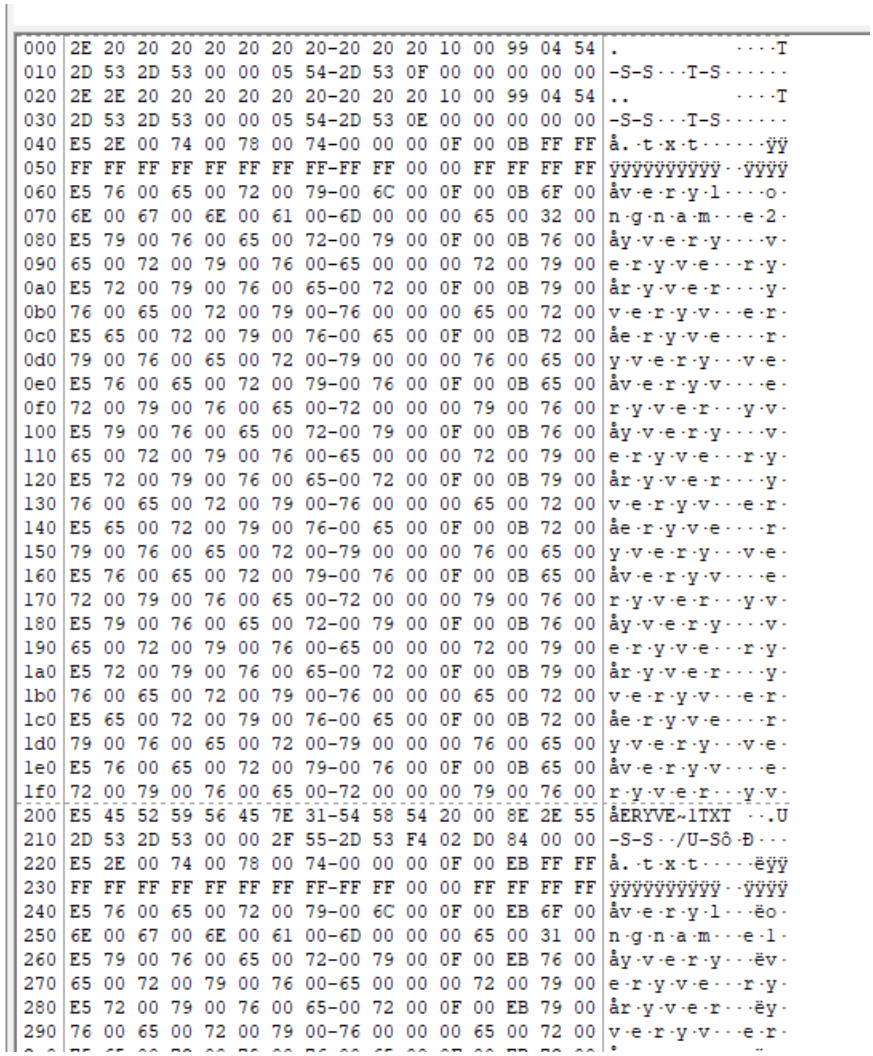
MetaData Document4.txt (LFN, Base Entry):

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	åD·o·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	åO21B0~1TXT ·)·T
1f0	2D	53	2D	53	00	00	93	54-2D	53	18	00	60	22	00	00	-S-S···T-S··`"··

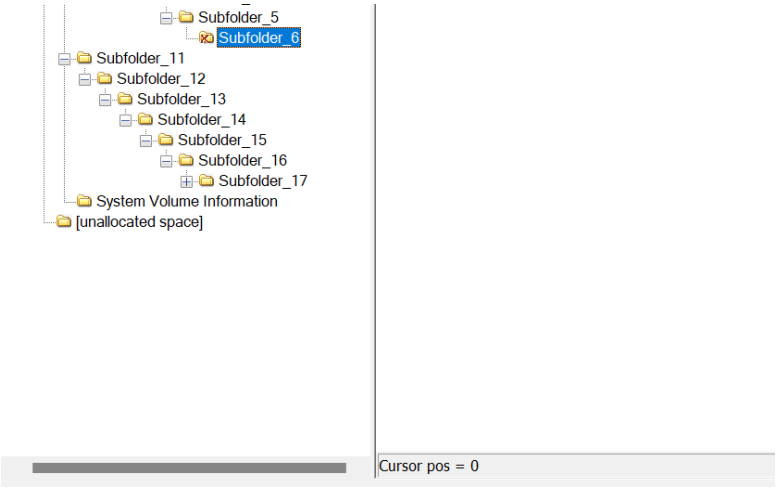
Metadata Subfolder 9 yang memiliki deleted files (karena directory sebelumnya dihapus juga) dengan nama yang panjang:



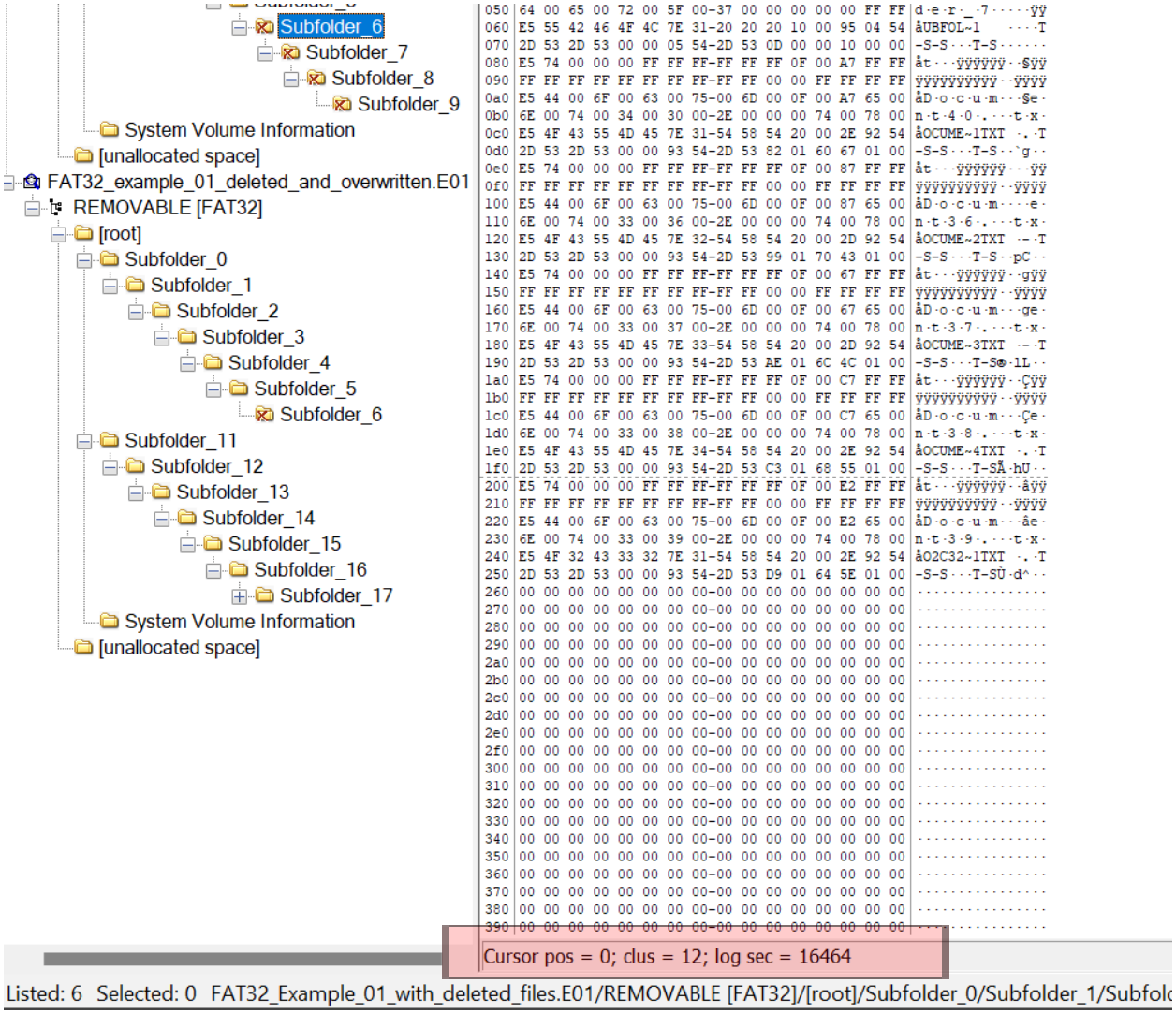
000	2E	20	20	20	20	20	20	20	20	20	10	00	99	04	54
010	2D	53	2D	53	00	00	05	54	2D	53	0F	00	00	00	00
020	2E	2E	20	20	20	20	20	20	20	20	10	00	99	04	54
030	2D	53	2D	53	00	00	05	54	2D	53	0E	00	00	00	00
040	E5	2E	00	74	00	78	00	74	00	00	00	0F	00	0B	FF
050	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF
060	E5	76	00	65	00	72	00	79	00	6C	00	0F	00	0B	6F
070	6E	00	67	00	6E	00	61	00	6D	00	00	00	65	00	32
080	E5	79	00	76	00	65	00	72	00	79	00	0F	00	0B	76
090	65	00	72	00	79	00	76	00	65	00	00	00	72	00	79
0a0	E5	72	00	79	00	76	00	65	00	72	00	0F	00	0B	79
0b0	76	00	65	00	72	00	79	00	76	00	00	00	65	00	72
0c0	E5	65	00	72	00	79	00	76	00	65	00	0F	00	0B	72
0d0	79	00	76	00	65	00	72	00	79	00	00	00	76	00	65
0e0	E5	76	00	65	00	72	00	79	00	76	00	0F	00	0B	65
0f0	72	00	79	00	76	00	65	00	72	00	00	00	79	00	76
100	E5	79	00	76	00	65	00	72	00	79	00	0F	00	0B	76
110	65	00	72	00	79	00	76	00	65	00	00	00	72	00	79
120	E5	72	00	79	00	76	00	65	00	72	00	0F	00	0B	79
130	76	00	65	00	72	00	79	00	76	00	00	00	65	00	72
140	E5	65	00	72	00	79	00	76	00	65	00	0F	00	0B	72
150	79	00	76	00	65	00	72	00	79	00	00	00	76	00	65
160	E5	76	00	65	00	72	00	79	00	76	00	0F	00	0B	65
170	72	00	79	00	76	00	65	00	72	00	00	00	79	00	76
180	E5	79	00	76	00	65	00	72	00	79	00	0F	00	0B	76
190	65	00	72	00	79	00	76	00	65	00	00	00	72	00	79
1a0	E5	72	00	79	00	76	00	65	00	72	00	0F	00	0B	79
1b0	76	00	65	00	72	00	79	00	76	00	00	00	65	00	72
1c0	E5	65	00	72	00	79	00	76	00	65	00	0F	00	0B	72
1d0	79	00	76	00	65	00	72	00	79	00	00	00	76	00	65
1e0	E5	76	00	65	00	72	00	79	00	76	00	0F	00	0B	65
1f0	72	00	79	00	76	00	65	00	72	00	00	00	79	00	76
200	E5	45	52	59	56	45	7E	31	54	58	54	20	00	8E	2E
210	2D	53	2D	53	00	00	2F	55	2D	53	F4	02	D0	84	00
220	E5	2E	00	74	00	78	00	74	00	00	00	0F	00	EB	FF
230	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	FF	FF	FF
240	E5	76	00	65	00	72	00	79	00	6C	00	0F	00	EB	6F
250	6E	00	67	00	6E	00	61	00	6D	00	00	00	65	00	31
260	E5	79	00	76	00	65	00	72	00	79	00	0F	00	EB	76
270	65	00	72	00	79	00	76	00	65	00	00	00	72	00	79
280	E5	72	00	79	00	76	00	65	00	72	00	0F	00	EB	79
290	76	00	65	00	72	00	79	00	76	00	00	00	65	00	72

Bagian FAT32 Example with Deleted Files and Overwritten:

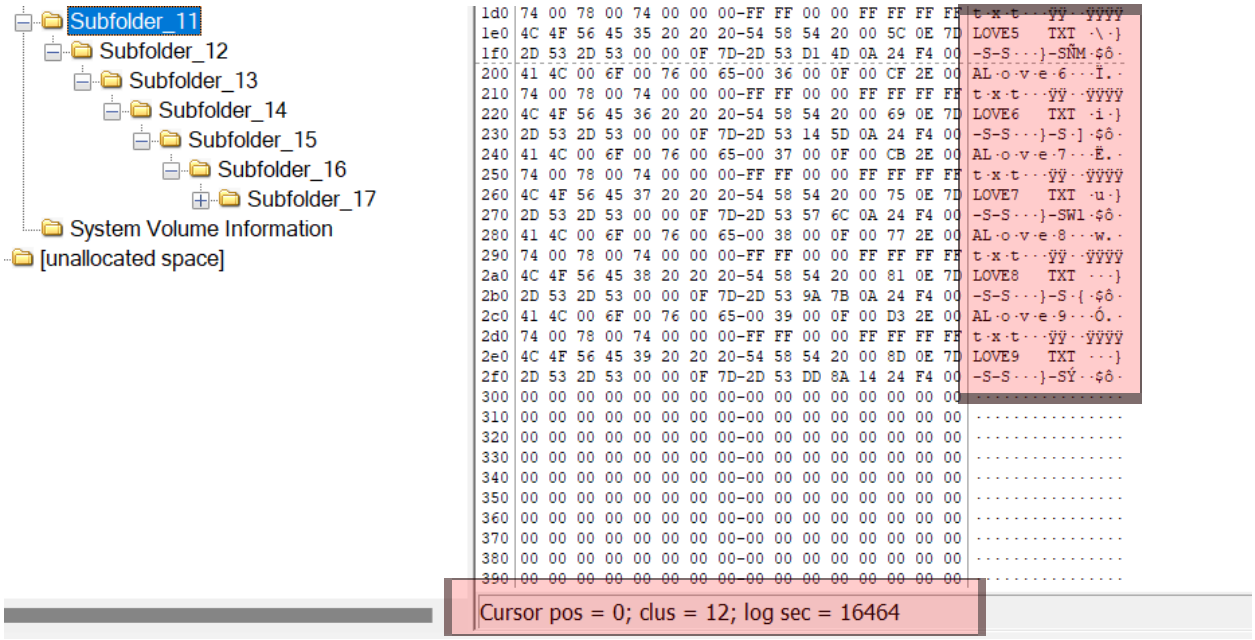
Subfolder 6 sekarang:



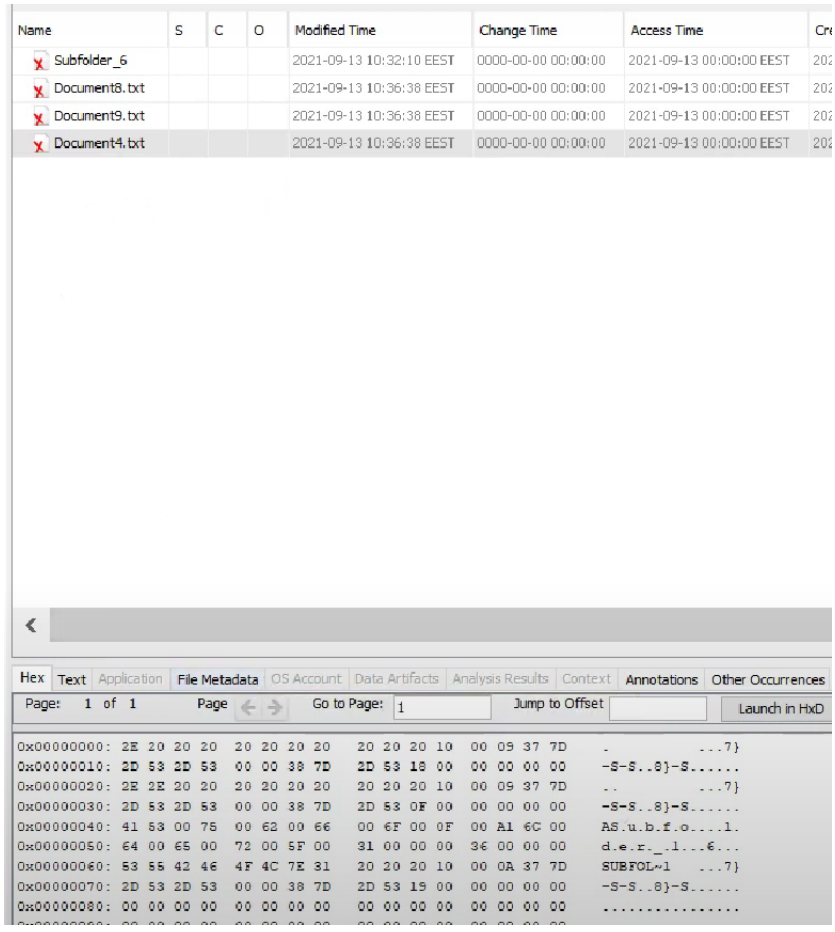
Subfolder 6 sebelumnya:



Cluster 12 sekarang:

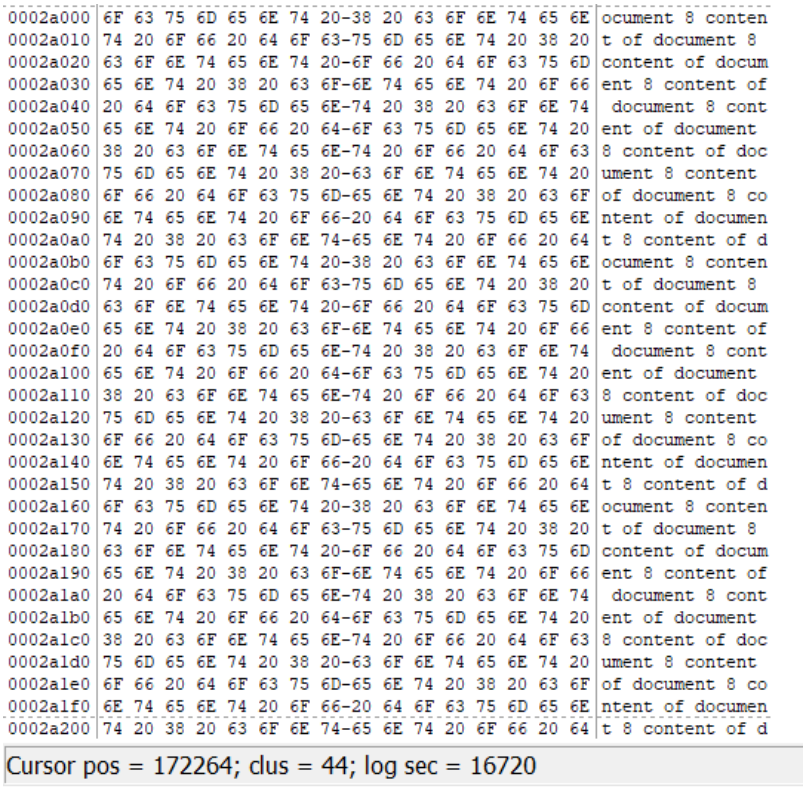


Bagian Autopsy:



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 meta data 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 menandakkan 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	ocument 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	ocument 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	ocument 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