FILE SYSTEM ANALYSIS- PART II

COMP 597 – Computer Forensics

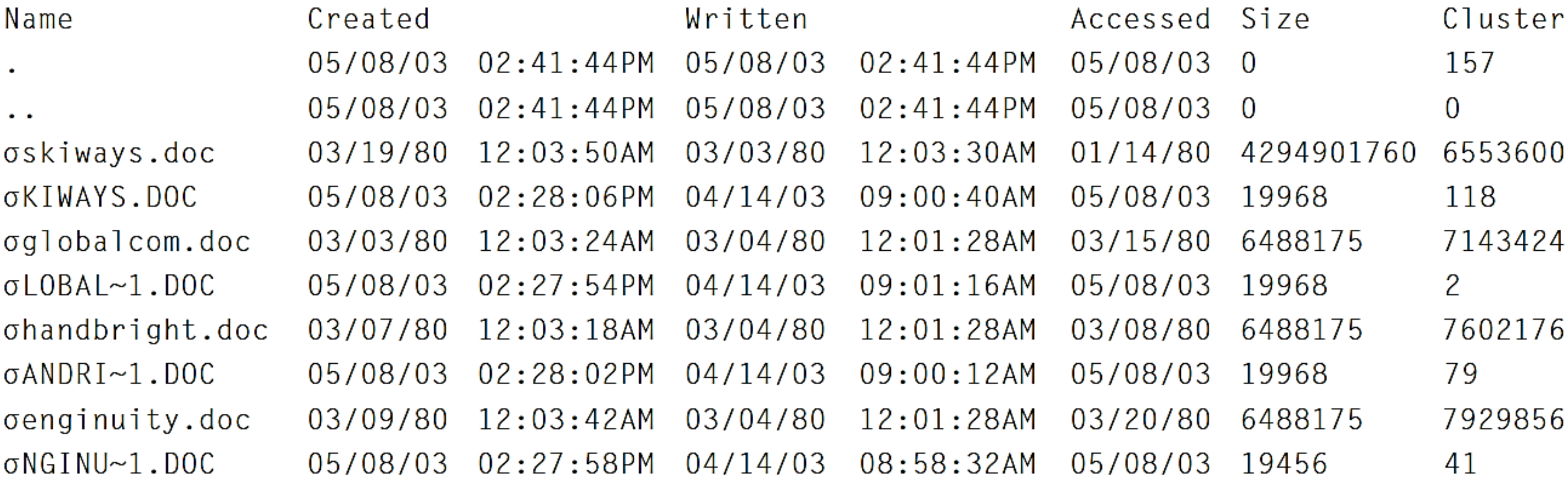
FAT

- Simple file system
- Used in USB drives

FAT

- A small number of data structures:
  - FAT
  - Directory entries

FAT - Directories



```
Name              Created               Written               Accessed Size       Cluster
.                 05/08/03 02:41:44PM   05/08/03 02:41:44PM   05/08/03 0          157
..                05/08/03 02:41:44PM   05/08/03 02:41:44PM   05/08/03 0          0
σskiways.doc      03/19/80 12:03:50AM   03/03/80 12:03:30AM   01/14/80 4294901760 6553600
σKIWAYS.DOC       05/08/03 02:28:06PM   04/14/03 09:00:40AM   05/08/03 19968      118
σglobalcom.doc    03/03/80 12:03:24AM   03/04/80 12:01:28AM   03/15/80 6488175    7143424
σLOBAL~1.DOC      05/08/03 02:27:54PM   04/14/03 09:01:16AM   05/08/03 19968      2
σhandbright.doc   03/07/80 12:03:18AM   03/04/80 12:01:28AM   03/08/80 6488175    7602176
σANDRI~1.DOC      05/08/03 02:28:02PM   04/14/03 09:00:12AM   05/08/03 19968      79
σenginuity.doc    03/09/80 12:03:42AM   03/04/80 12:01:28AM   03/20/80 6488175    7929856
σNGINU~1.DOC      05/08/03 02:27:58PM   04/14/03 08:58:32AM   05/08/03 19456      41
```

FAT Structure

- Why do we need this data structure?

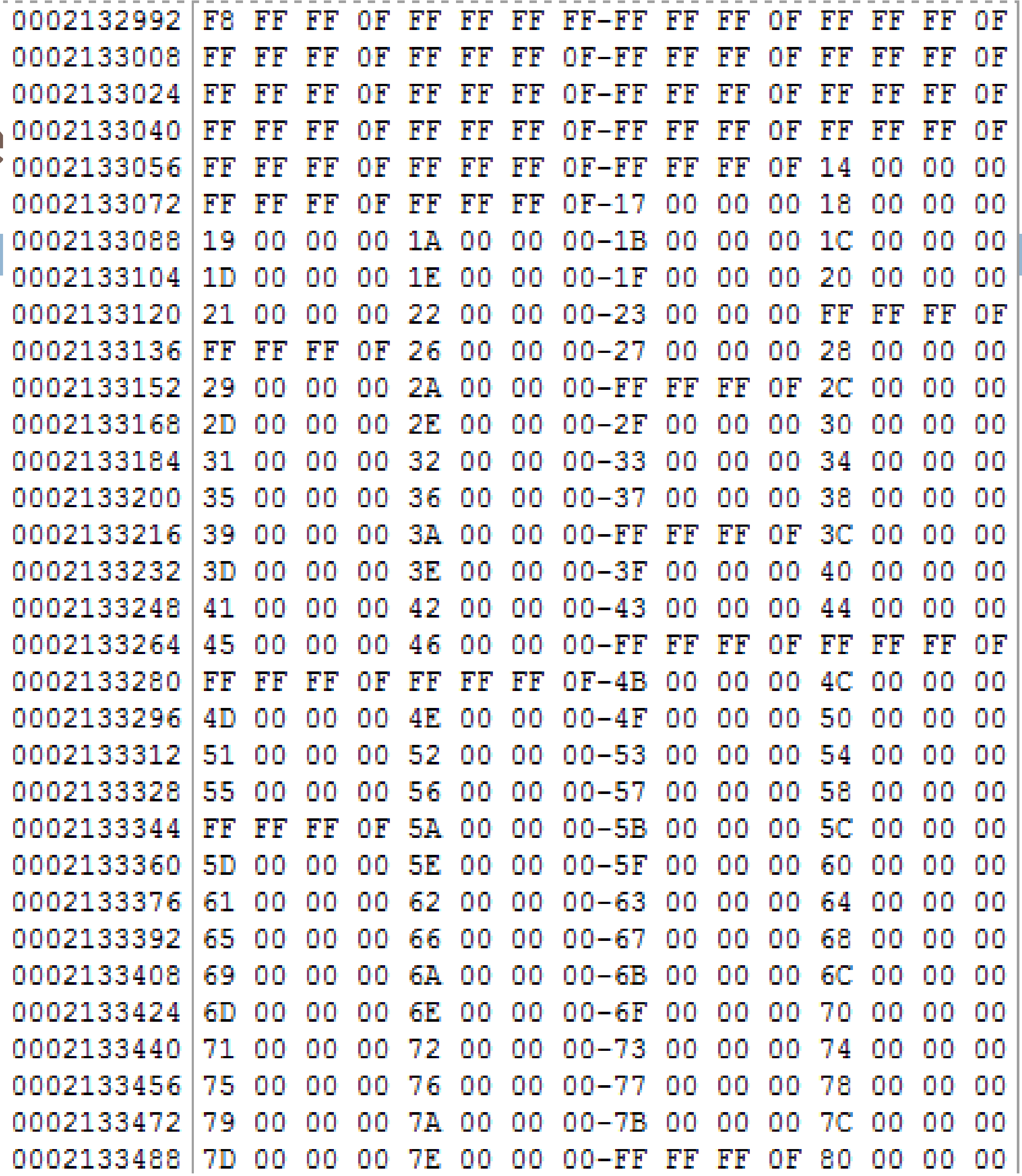
FAT Values

	FAT12	FAT16	FAT32
Available	0	0	0
Reserved	1	1	1
User Data	002-FF6	0002-FFF6	00000002-0FFFFFF6
Bad Cluster	FF7	FFF7	0FFFFFF7
End Marker	FF8-FFF	FFF8-FFFF	0FFFFFF8-0FFFFFFF

FAT Structure

- FAT12
- FAT16 (max 65,525 clusters)
- FAT32

FAT Structure



```
0002132992 F8 FF FF 0F FF FF FF FF-FF FF FF 0F FF FF FF 0F
0002133008 FF FF FF 0F FF FF FF 0F-FF FF FF 0F FF FF FF 0F
0002133024 FF FF FF 0F FF FF FF 0F-FF FF FF 0F FF FF FF 0F
0002133040 FF FF FF 0F FF FF FF 0F-FF FF FF 0F FF FF FF 0F
0002133056 FF FF FF 0F FF FF FF 0F-FF FF FF 0F 14 00 00 00
0002133072 FF FF FF 0F FF FF FF 0F-17 00 00 00 18 00 00 00
0002133088 19 00 00 00 1A 00 00 00-1B 00 00 00 1C 00 00 00
0002133104 1D 00 00 00 1E 00 00 00-1F 00 00 00 20 00 00 00
0002133120 21 00 00 00 22 00 00 00-23 00 00 00 FF FF FF 0F
0002133136 FF FF FF 0F 26 00 00 00-27 00 00 00 28 00 00 00
0002133152 29 00 00 00 2A 00 00 00-FF FF FF 0F 2C 00 00 00
0002133168 2D 00 00 00 2E 00 00 00-2F 00 00 00 30 00 00 00
0002133184 31 00 00 00 32 00 00 00-33 00 00 00 34 00 00 00
0002133200 35 00 00 00 36 00 00 00-37 00 00 00 38 00 00 00
0002133216 39 00 00 00 3A 00 00 00-FF FF FF 0F 3C 00 00 00
0002133232 3D 00 00 00 3E 00 00 00-3F 00 00 00 40 00 00 00
0002133248 41 00 00 00 42 00 00 00-43 00 00 00 44 00 00 00
0002133264 45 00 00 00 46 00 00 00-FF FF FF 0F FF FF FF 0F
0002133280 FF FF FF 0F FF FF FF 0F-4B 00 00 00 4C 00 00 00
0002133296 4D 00 00 00 4E 00 00 00-4F 00 00 00 50 00 00 00
0002133312 51 00 00 00 52 00 00 00-53 00 00 00 54 00 00 00
0002133328 55 00 00 00 56 00 00 00-57 00 00 00 58 00 00 00
0002133344 FF FF FF 0F 5A 00 00 00-5B 00 00 00 5C 00 00 00
0002133360 5D 00 00 00 5E 00 00 00-5F 00 00 00 60 00 00 00
0002133376 61 00 00 00 62 00 00 00-63 00 00 00 64 00 00 00
0002133392 65 00 00 00 66 00 00 00-67 00 00 00 68 00 00 00
0002133408 69 00 00 00 6A 00 00 00-6B 00 00 00 6C 00 00 00
0002133424 6D 00 00 00 6E 00 00 00-6F 00 00 00 70 00 00 00
0002133440 71 00 00 00 72 00 00 00-73 00 00 00 74 00 00 00
0002133456 75 00 00 00 76 00 00 00-77 00 00 00 78 00 00 00
0002133472 79 00 00 00 7A 00 00 00-7B 00 00 00 7C 00 00 00
0002133488 7D 00 00 00 7E 00 00 00-FF FF FF 0F 80 00 00 00
```

File System Layout

- Boot Sector
- FAT
- Data Area

Boot Sector

Byte Range	Description
0–2	Assembly instruction to jump to boot code.
3–10	OEM Name in ASCII.
11–12	Bytes per sector
13–13	Sectors per cluster
14–15	Size in sectors of the reserved area.
16–16	Number of FATs
17–18	# of Directory entries in root
19–20	Number of sectors in file system (16-bit)
22–23	16-bit size in sectors of each FAT
24–25	Sectors per track of storage device.
26–27	Number of heads in storage device.
28–31	Number of sectors before the start of partition.
32–35	Number of sectors in file system (32-bit)

Boot Sector

FAT12 - FAT16

39–42	Volume serial number
43–53	Volume label in ASCII
54–61	File system type label in ASCII
62–509	Boot code
510–511	Signature value (0xAA55).

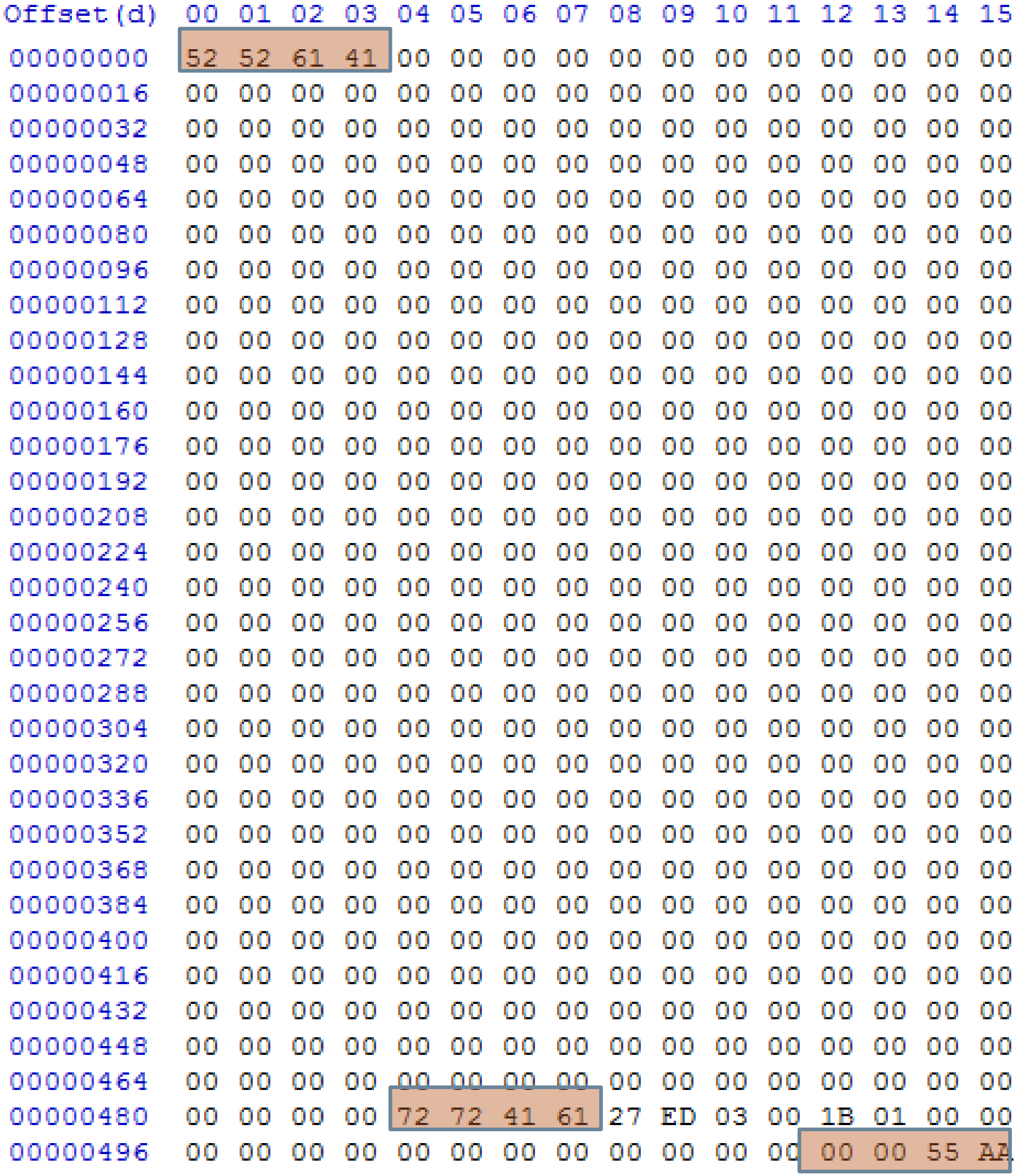
FAT32

36–39	32-bit size in sectors of one FAT.
40–41	How multiple FAT structures are written to
42–43	The major and minor version number.
44–47	Cluster where root directory can be found.
48–49	Sector where FSINFO structure can be found.
50–51	Sector where backup copy of boot sector
67–70	Volume serial number
71–81	Volume label in ASCII
82–89	File system type label in ASCII
90–509	Boot code
510–511	Signature value (0xAA55).

FSINFO

Bytes	Content
0-3	0x41615252 (FSINFO signature)
4-483	Reserved
484-487	0x61417272 (FSINFO signature)
488-491	Free cluster count
492-495	Next free cluster
496-507	Reserved
508-511	0xaa550000 (sector signature)

FSINFO



```
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00000000  52 52 61 41 00 00 00 00 00 00 00 00 00 00 00 00
00000016  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000032  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000064  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000096  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000112  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000128  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000144  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000176  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000192  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000208  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000224  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
00000256  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000272  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000288  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000304  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000336  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000352  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000368  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000384  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000416  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000432  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000448  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000464  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000480  00 00 00 00 72 72 41 61 27 ED 03 00 1B 01 00 00
00000496  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

File System Layout

- Where can we hide data?

Directory

- Uses 1 or more clusters
- A table of directory entries
- What is the size of a directory in an entry?

Directory Entries

- Why do we need this data structure?

Directory Entries

Bytes	***Size***	***Description***
0-7	8 bytes	Filename
8-10	3 bytes	Filename extension
11	1 byte	File attributes
12	1 byte	Reserved
13-17	5 bytes	Created Date
18-19	2 bytes	Accessed Day
20-21	2 bytes	Starting cluster (high bytes)
22-25	4 bytes	Modified Date
26-27	2 bytes	Starting cluster (low bytes)
28-31	4 bytes	File size (bytes)

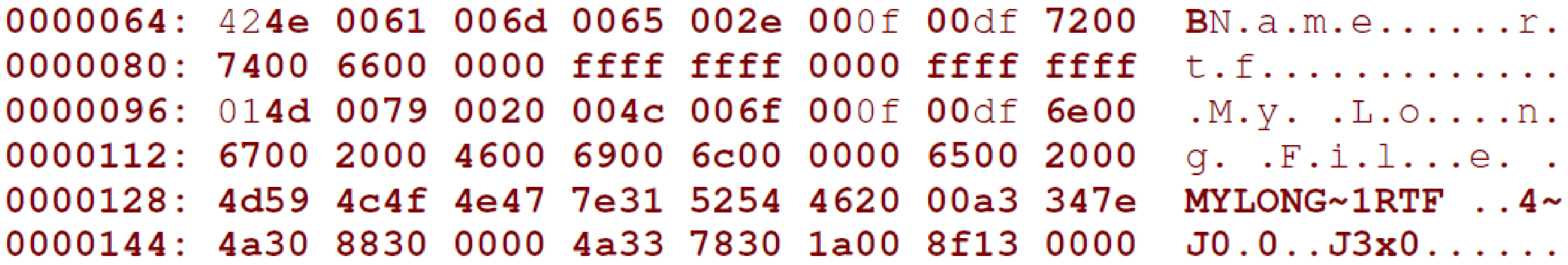
Directory Entries – File Attributes

Flag Value	**Description**
0000 0001 (0x01)	Read only
0000 0010 (0x02)	Hidden file
0000 0100 (0x04)	System file
0000 1000 (0x08)	Volume label
0000 1111 (0x0f)	Long file name
0001 0000 (0x10)	Directory
0010 0000 (0x20)	Archive

Long File Name

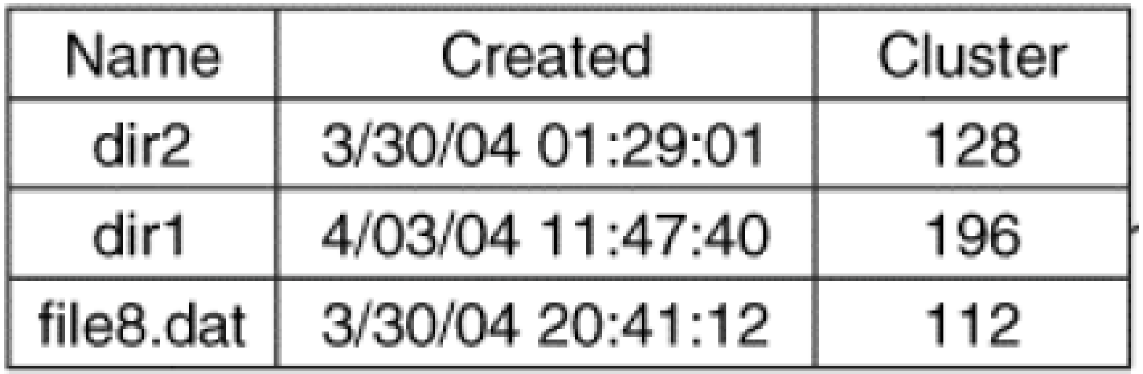
Byte	Description
0–0	Sequence number
1–10	File name characters 1–5
11–11	File attributes (0x0f)
12–12	Reserved
13–13	Checksum
14–25	File name characters 6–11
26–27	Reserved
28–31	File name characters 12–13

Long File Name

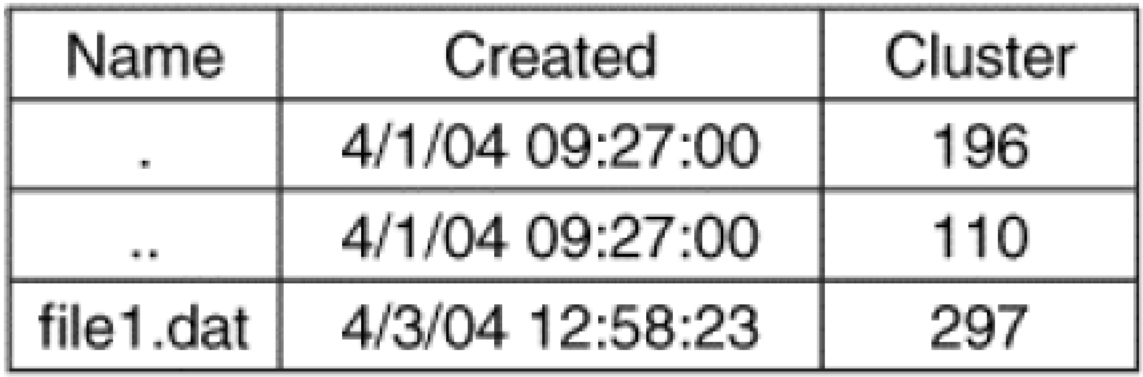


```
0000064: 424e 0061 006d 0065 002e 000f 00df 7200  BN.a.m.e......r.
0000080: 7400 6600 0000 ffff ffff 0000 ffff ffff  t.f.............
0000096: 014d 0079 0020 004c 006f 000f 00df 6e00  .M.y. .L.o....n.
0000112: 6700 2000 4600 6900 6c00 0000 6500 2000  g. .F.i.l...e. .
0000128: 4d59 4c4f 4e47 7e31 5254 4620 00a3 347e  MYLONG~1RTF ..4~
0000144: 4a30 8830 0000 4a33 7830 1a00 8f13 0000  J0.0..J3x0......
```

Directory – Example 1



Name	Created	Cluster
dir2	3/30/04 01:29:01	128
dir1	4/03/04 11:47:40	196
file8.dat	3/30/04 20:41:12	112



Name	Created	Cluster
.	4/1/04 09:27:00	196
..	4/1/04 09:27:00	110
file1.dat	4/3/04 12:58:23	297

Directory – Example 2

- How does a file system creates Docs\mail.txt (1.2KB)?
- How does a file system deletes Deal\Pics\i.txt?
- How do we find the full path of amp.txt?
- What happens when we delete *Pics*?
- What happens when we delete amp.txt and tmp.txt?

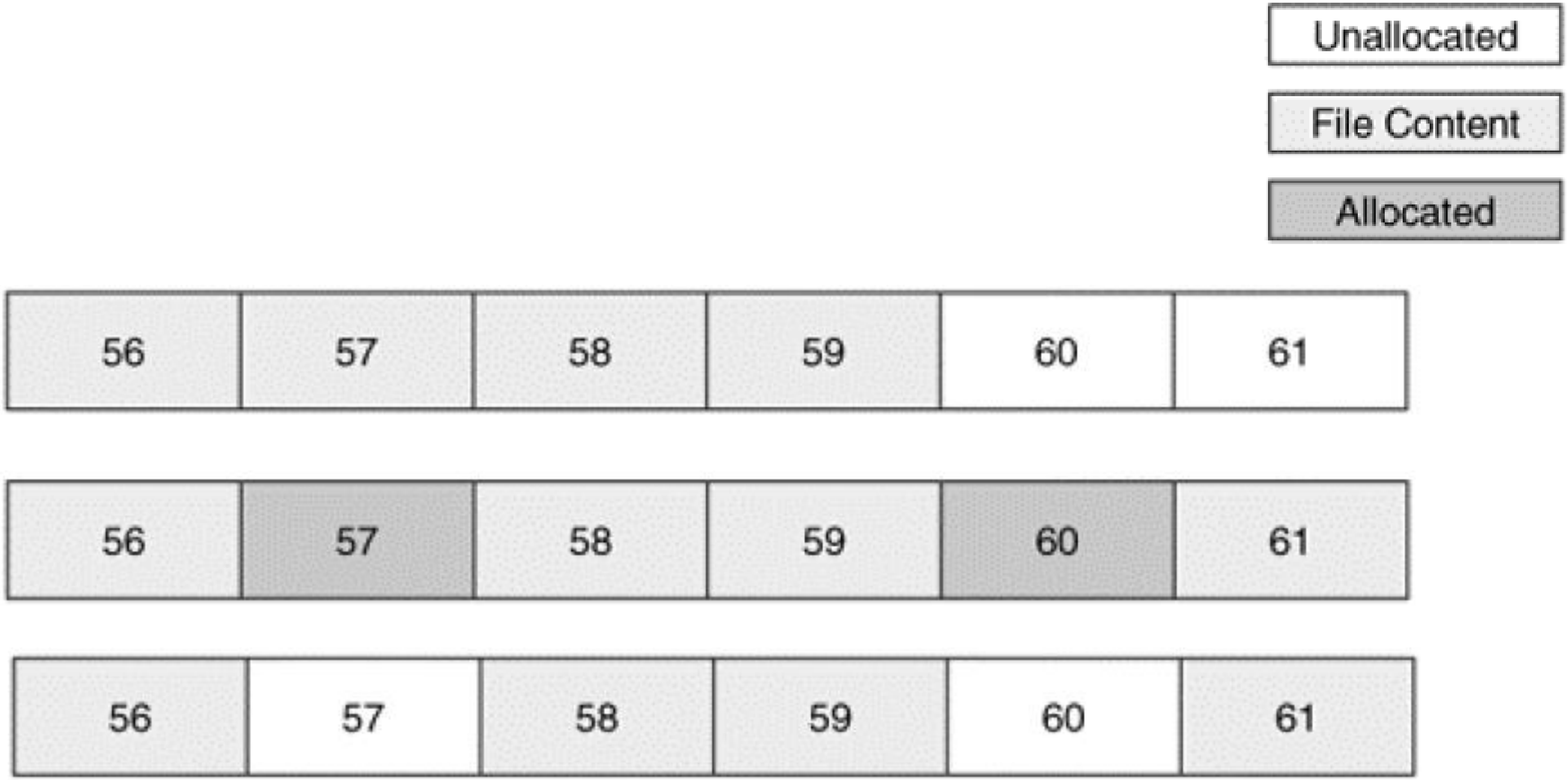
Date Values

- Year (7 bits)
- Month (4 bits)
- Day (5 bits)

Time Values

- Hour (5 bits)
- Minute(6 bits)
- Second (5 bits)

File Recovery



Unallocated

File Content

Allocated

56 57 58 59 60 61

56 57 58 59 60 61

56 57 58 59 60 61

Forensic Example

You were given a file system to investigate. The file system has very few files and directories.

What do you conclude?

References

1. Digital Evidence and Computer Crime, 3rd edition, Eoghan Casey, 2011.
2. File System Forensic Analysis, 2nd edition, Brian Carrier, 2005.