ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Amir Alsbih and Christian Schindelhauer

Distributed Storage and

Computer Forensic

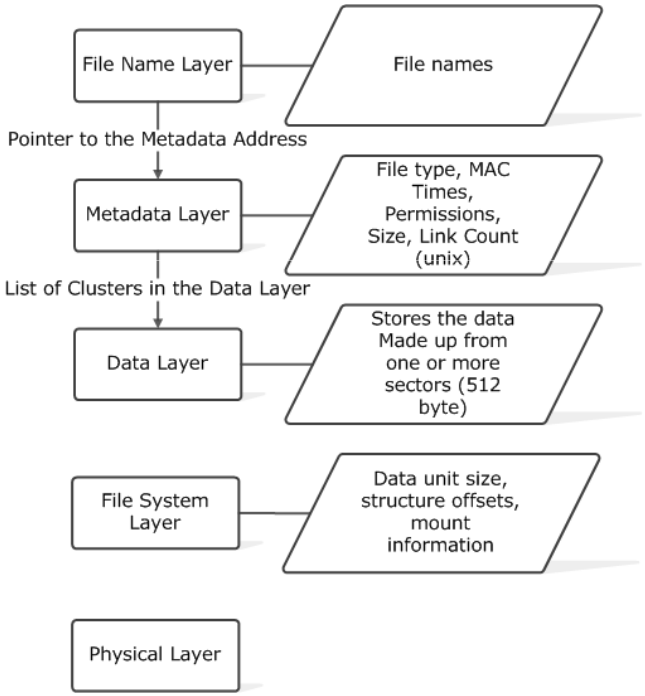
2

Follow Up

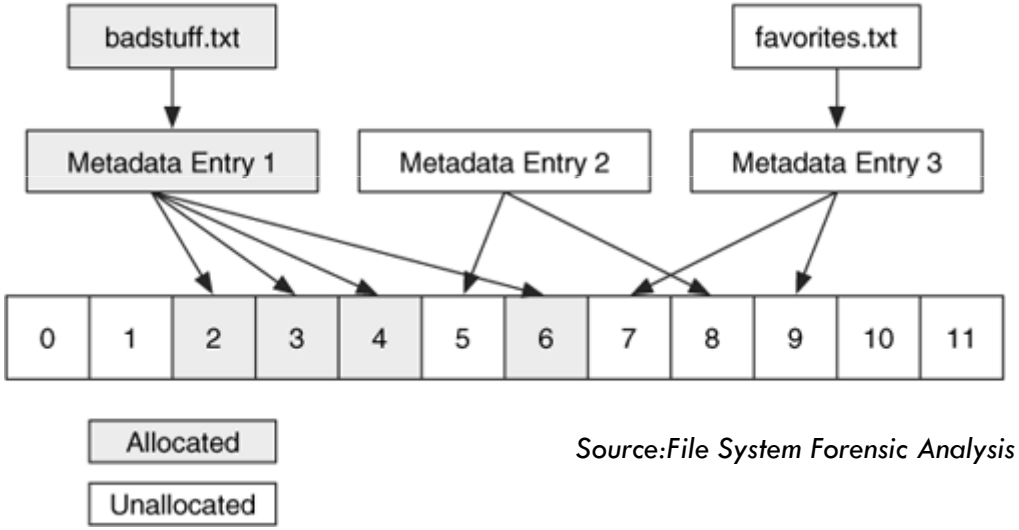
Forensic principles

- Minimize data loss: Computer evidence is subject to the "observer effect"
- Take notes about everything
- Analyze all data collected (start with the most volatile data)
- Whenever possible, rely on more than one tool
- Understand what you do and why

File System Layers



recover files by their unallocated name



Source:File System Forensic Analysis

Slack Space

- Slack Space: When the size of a file is not a multiple of the block size the file will have “slack space”.
- There are two places for slack space:
  - between the end of the file and the end of the sector in which the file ends. (typically this days filled with 0x00)
  - The sectors after the end of the file to the end of the block. (can contain older data)

dd if=… bs=512 skip=0 count=1 | xxd

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG


```
…
00001b0: 0000 0000 0000 0000 f4fe  8f8a 0000 0001
00001c0: 0100 041f 3f19 3f00 0000 81cc 0000 0000
00001d0: 011a 041f 3f33 c0cc 0000 c0cc 0000 0000
00001e0: 0134 041f 3f4d 8099 0100 c0cc 0000 0000
00001f0: 014e 051f 3f9a 4066 0200 605e 0200 55aa
```

mmls image.dd


```
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0000052415   0000052353   DOS FAT16 (0x04)
03:  00:01   0000052416   0000104831   0000052416   DOS FAT16 (0x04)
04:  00:02   0000104832   0000157247   0000052416   DOS FAT16 (0x04)
05:  Meta    0000157248   0000312479   0000155232   DOS Extended (0x05)
06:  Meta    0000157248   0000157248   0000000001   Extended Table (#1)
07:  -----   0000157248   0000157310   0000000063   Unallocated
08:  01:00   0000157311   0000209663   0000052353   DOS FAT16 (0x04)
09:  -----   0000209664   0000209726   0000000063   Unallocated
10:  01:01   0000209727   0000262079   0000052353   DOS FAT16 (0x04)
11:  Meta    0000262080   0000312479   0000050400   DOS Extended (0x05)
12:  Meta    0000262080   0000262080   0000000001   Extended Table (#2)
13:  -----   0000262080   0000262142   0000000063   Unallocated
14:  02:00   0000262143   0000312479   0000050337   DOS FAT16 (0x06)
```

9

File Allocation Table (FAT)

FAT variations

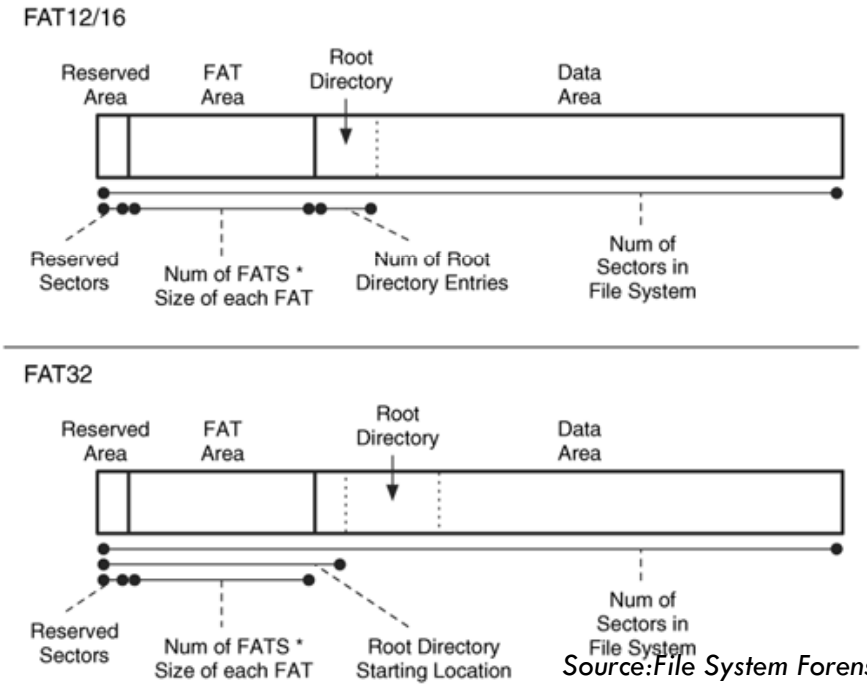
- FAT12
  - Cluster Size: 512 bytes – 8 KB
  - 2^{12} addressable clusters
  - Maximum volume size 32 MB (4096 clusters)
- FAT16
  - Cluster Size: 512 bytes – 64 KB
  - 2^{16} addressable clusters
  - Maximum volume size 4 GB (65536 clusters)

Limited root directory with 512 entries (32 bytes)

- FAT32
  - Cluster Size: 512 bytes – 32 KB
  - 2^{28} addressable clusters
  - Maximum volume size 8 TB (268435456 clusters)

Root directory works with cluster chain – no limit

FAT FORMAT (File System Layer)



Source:File System Forensic Analysis

Boot Sector

- OEM name: eight-character string (Byte 3-10)
  - Win95: MSWIN4.0
  - Win98: MSWIN4.1
  - WinXP / Win-2000: MSDOS5.0
- Bytes per sector (Byte 11-12)
- Sectors per cluster (Byte 13)
- Number of FAT Tables (Byte 16)
- Number of files in the root directory (Byte 17-18)
- Total Sectors (Byte 19-20)

blkcat image 0 | xxd


```
0000000: eb3c  904d 5344 4f53 352e 3000 0201 0200
0000010: 0200 0281 ccf8  cb00 3f00  ff00  3f00  0000
0000020: 0000 0000 8000 2948 9405 284e 4f20  4e41
0000030: 4d45 2020 2020 4641 5431 3620 2020 33c9
0000040: 8ed1 bcf0  7b8e d9b8 0020 8ec0  fcbd  007c
```

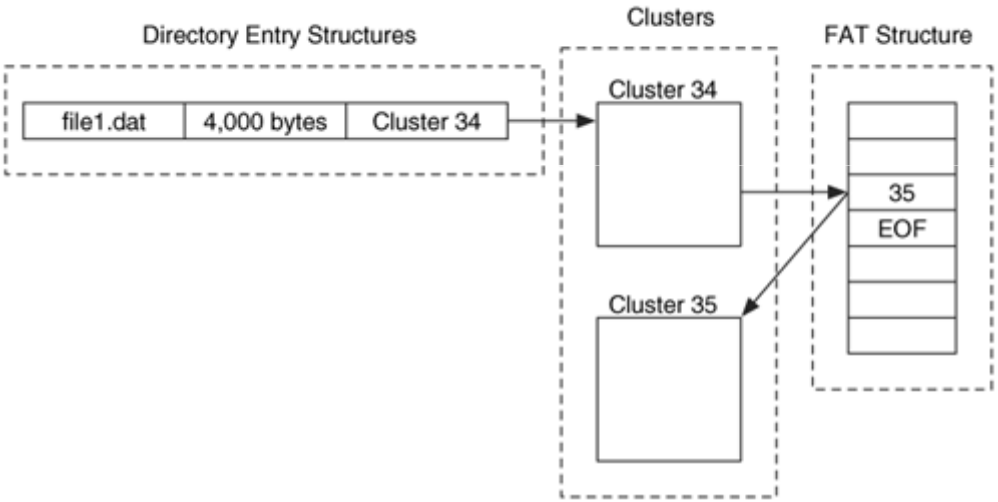
fsstat


```
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0x28059448
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 63

File System Layout (in sectors)
Total Range: 0 - 52352
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 204
* FAT 1: 205 - 407
* Data Area: 408 - 52352
** Root Directory: 408 - 439
** Cluster Area: 440 - 52352

METADATA INFORMATION
--------------------------------------------
Range: 2 - 831126
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 51914
```

FAT Directory Entry (Metadata Layer)

- File Name: (8 main and 3 for the extension)
- Modified, Access and Creation Date/Time
- File Size
- First Cluster Number of the Data Area (Pointer to the FAT Cluster Chain)

FAT FORMAT 2



Source:File System Forensic Analysis

istat


```
Directory Entry: 2
Allocated
File Attributes: Directory
Size: 16384
Name:

Directory Entry Times:
Written:        Thu Jan  1 00:00:00 1970
Accessed:       Thu Jan  1 00:00:00 1970
Created:        Thu Jan  1 00:00:00 1970

Sectors:
408 409 410 411 412 413 414 415
416 417 418 419 420 421 422 423
424 425 426 427 428 429 430 431
432 433 434 435 436 437 438 439
```

FAT Directory Entry (Normal)

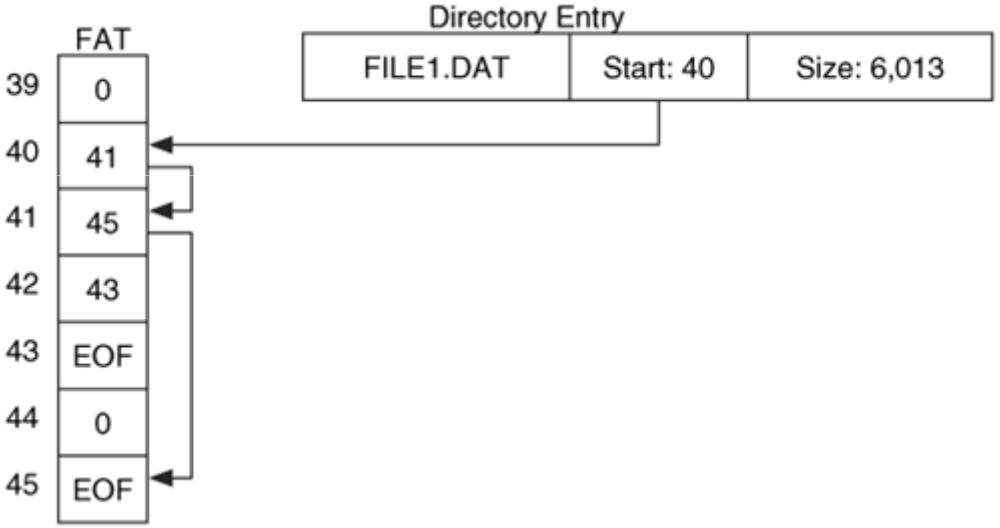
Byte Range	Description
0-0	First character of file name in ASCII and allocation status (0xe5 or 0x00 if unallocated)
1-10	Characters 2 to 11 of file name in ASCII
11-11	File Attributes (0x10 Dir, 0x08 Volume Label, 0x0f Long file name)
20-21	High 2 bytes of first cluster address (0 for FAT12 and FAT16)
26-27	Low 2 bytes of first cluster address
28-31	Size of file (0 for directories)

FAT Directory Entry (Long)

Byte Range	Description
0-0	Sequence number (Ored with 0x40) and allocation status (0xe5 if unallocated)
1-10	Characters 1 to 5 of file name in Unicode
11-11	File Attributes (0x10 Dir, 0x08 Volume Label, 0x0f Long file name)
13-13	Checksum
14-25	File name characters 6-11 Unicode
28-31	File name characters 12-13 Unicode

```
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......
```

FAT Directory Entry



Source:File System Forensic Analysis

Directory Entry

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Cluster 110

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

Cluster 196

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

Source:File System Forensic Analysis

After Directory reallocation

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

A)

Cluster 45

.	45
..	26
bad.jpg	105
dir1	210
good.jpg	153

Cluster 210

.	210
..	45
file1.txt	211
file2.txt	250
file3.txt	273

B)

Cluster 45

.	45
..	26
bad.jpg	105
newfile	**400**
good.jpg	153

Cluster 210

.	210
..	45
file1.txt	211
file2.txt	250
file3.txt	273

Source:File System Forensic Analysis

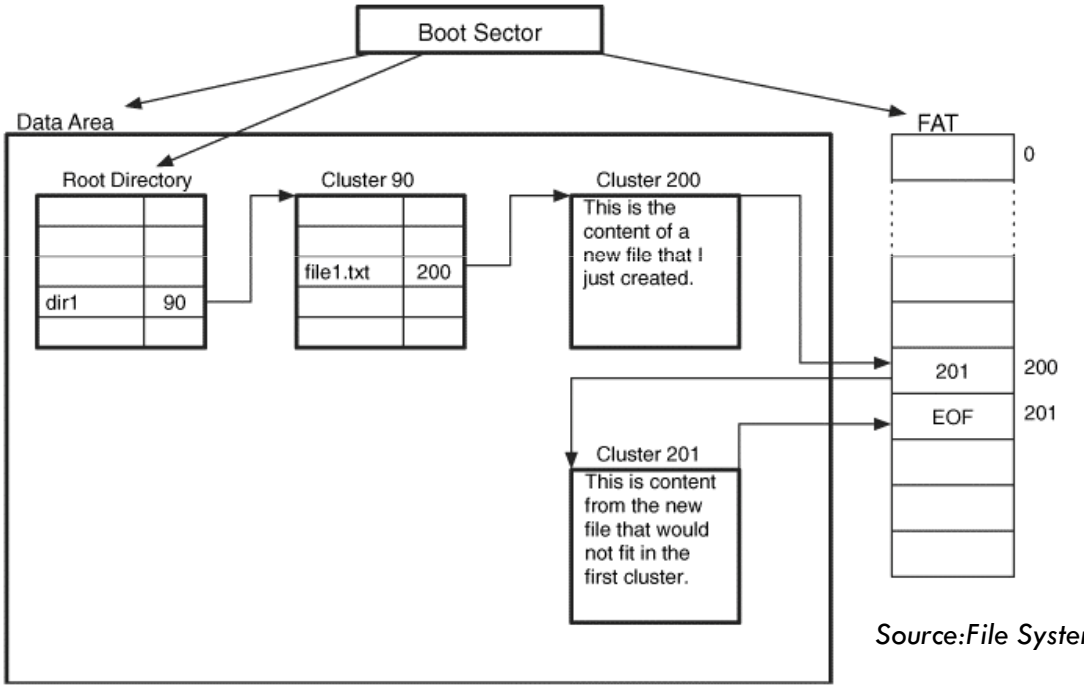
After File deletion

- Filename Layer
  - First letter of file name will replaced by 0xe5
- Metadata Layer
  - Modification/Creation Times and Access Date
  - File Type, Size and Cluster addresses
- Data Layer
  - Data clusters in FAT will be marked as unallocated (0x00) but data will be preserved at the orginal cluster locations
  - Slack Space

fsstat

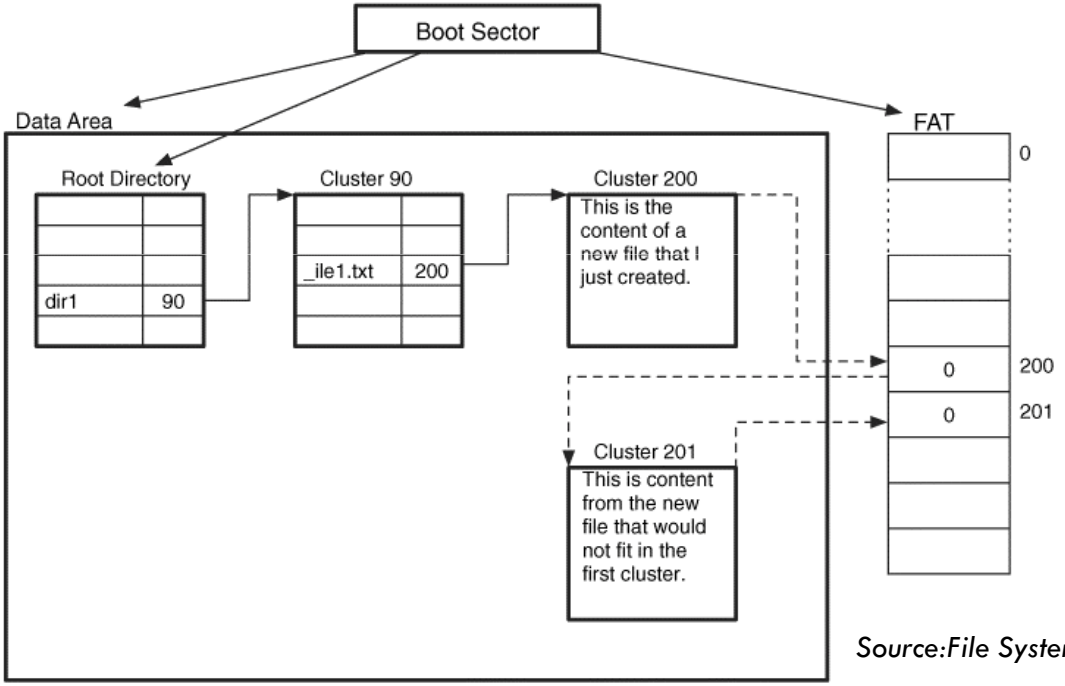

```
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0x28059448
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory):
File System Type Label: FAT16

Sectors before file system: 63

File System Layout (in sectors)
Total Range: 0 - 52352
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 204
* FAT 1: 205 - 407
* Data Area: 408 - 52352
** Root Directory: 408 - 439
** Cluster Area: 440 - 52352

METADATA INFORMATION
--------------------------------------------
Range: 2 - 831126
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 51914
```

File Allocation Example



Source:File System Forensic Analysis

After File Deletion



Source:File System Forensic Analysis