CSC414
COMPUTER SYSTEM FUNDAMENTALS

EXPLORING THE FAT FILE SYSTEM

PART II: FAT BOOT SECTOR

DIGITAL FORENSICS CENTER
DEPARTMENT OF COMPUTER SCIENCE AND STATICS

THINK BIG WE DO

THE UNIVERSITY OF RHODE ISLAND

http://www.forensics.cs.uri.edu

00:00

FAT PARTITION FORMAT

THE UNIVERSITY OF RHODE ISLAND
THINK BIG WE DO

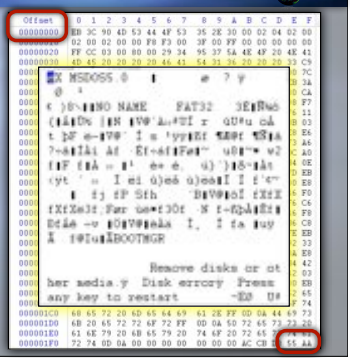
- **Boot Record**
  - **Boot** Sector
    - BIOS Parameter Block (***BPB***)
  - Two extra sectors for **FAT32**:
    - File System Information Sector
      - **FSInfo** Sector
    - **Reserved** (empty) Sector
  - **FAT32** maintains copy of the three boot sectors
  - Starts at **Sector #6**
- **File Allocation Table**
  - Two copies for safety (**FAT1** & **FAT2**)
- **Root Directory of File System**
  - Directory of files and their attributes
- **Data Area**
  - Divided into clusters
    - Starts at **Cluster #2**
  - For **FAT32**,
    - Root Directory is part of the data area

00:19

FAT BOOT SECTOR

THE UNIVERSITY OF RHODE ISLAND
THINK BIG WE DO

- **Located at `Sector 0` of Partition**
- **BIOS Parameter Block (BPB)**
  - Size and number of logical sectors
  - Size of clusters
  - Size and number of file allocation tables (FATs)
  - Size and location of root directory
  - Volume identification information
    - Serial number
    - Label
    - File System
  - Signature (`55 AA`)



00:43

BIOS PARAMETER BLOCK

THE UNIVERSITY OF RHODE ISLAND
THINK BIG WE DO

BPB Parameter (First 32 bytes)	Offset (in Hex)	Offset (Decimal)	Length (in Bytes)	Common Values
Jump Instruction	00	0	2	0xEB 0x3C
NOP Instruction	02	2	1	0x90
OEM Name (ID of OS that formatted partition)	03	3	8	MSDOS5.0
Bytes Per Sector	0B	11	2	512
Sectors per Cluster	0D	13	1	2 to 64
Reserved Sectors (# of sectors that make up the Boot Record)	0E	14	2	varies
Number of File Allocation Tables (original + copy)	10	16	1	2
Number of Root Directory Entries (N/A for FAT32)	11	17	2	512
Number of Sectors in Partition (if partition < 32MB) (N/A for FAT32)	13	19	2	0
Media Descriptor (0xF8 for Hard Disks)	15	21	1	0xF8
Number of Sectors per FAT (N/A for FAT32)	16	22	2	varies
Number of Sectors Per Track	18	24	2	varies
Number of Heads	1A	26	2	varies
Number of Hidden Sectors	1C	28	4	0
Number of Sectors in Partition (if partition > 32MB)	20	32	4	varies

02:13

BIOS PARAMETER BLOCK

THE UNIVERSITY OF RHODE ISLAND
THINK BIG WE DO

BPB Parameter (FAT12 / FAT16)	Offset (in Hex)	Offset (Decimal)	Length (in Bytes)	Common Values
Drive Number	24	36	1	0x80
Reserved	25	37	1	N/A
Signature (Extended boot sector description)	26	38	1	0x29
Volume ID (Volume Serial Number)	27	39	4	varies
Volume Label (if not present, see first entry in Root Directory)	2B	43	11	VARIES
File System Type	36	54	8	FAT16
Executable Code	3E	62	448	
End of Boot Sector Marker	01FE	510	2	0x55 0xAA

05:37

BIOS PARAMETER BLOCK

THE UNIVERSITY OF RHODE ISLAND
THINK BIG WE DO

BPB Parameter (FAT32)	Offset (in Hex)	Offset (Decimal)	Length (in Bytes)	Common Values
Number of Sectors Per FAT	24	36	4	varies
Flags	28	40	2	0
Version of FAT32 Drive (High Byte = Major Version, Low Byte = Minor)	2A	42	2	0
Cluster Number of the Start of the Root Directory	2C	44	4	2
Sector Number of File System Information Sector	30	48	2	1
Sector Number of Backup Boot Sector	32	50	2	6
Reserved	34	52	12	00 … 00
Logical Drive Number of Partition	40	64	1	0x80
Unused	41	65	1	0
Extended Signature (0x29)	42	66	1	0x29
Serial Number of Partition	43	67	4	varies
Volume Name of Partition	47	71	11	VARIES
FAT Name (FAT32)	52	82	8	FAT32
Executable Code	5A	90	420	
End of Boot Sector Marker [0x55 0xAA]	01FE	510	2	0x55 0xAA

06:35

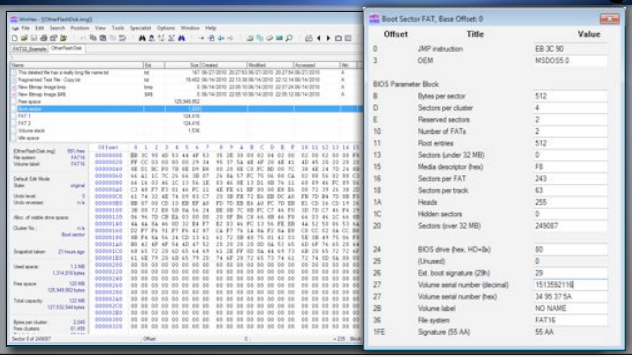
File System Info Sector

- **FSInfo Sector (FAT32 only)**
  - Immediately follows the first sector, (BIOS Parameter Block)

FSInfo Sector for FAT32	Offset (in Hex)	Offset (Decimal)	Length (in Bytes)
Signature for FSInfo Sector (0x52 0x52 0x61 0x41) RRaA	00	0	4
Reserved	04	4	480
Signature for Start of FSInfo Data (0x72 0x72 0x41 0x61) rrAa	01E4	484	4
Number of Free Clusters on Partition (Set to -1 or FF FF FF FF if unknown)	01E8	488	4
Cluster Number of Cluster that was most recently Allocated (Set to -1 or FF FF FF FF if unknown)	01EC	492	4
Reserved	01F0	496	14
End of FSInfo Sector Marker [0x55 0xAA]	01FE	510	2

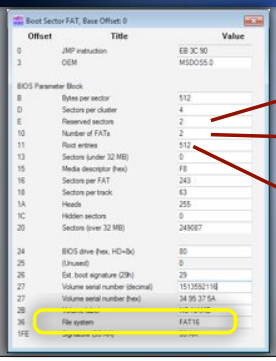
08:11

FAT16 BPB Information



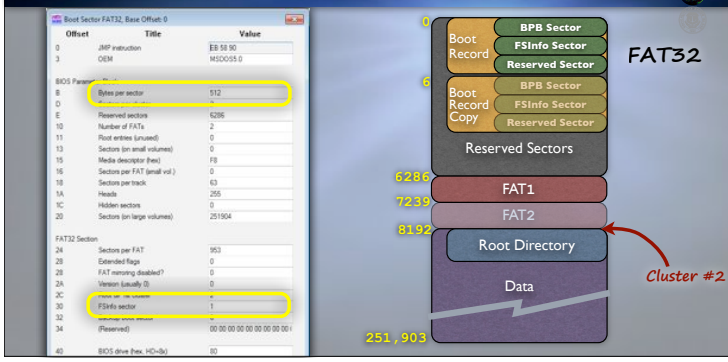
09:01

FAT16 BPB Information



09:23

FAT32 BPB Information



11:05

Exploring The FAT File System

Part II: FAT Boot Sector

Digital Forensics Center
Department of Computer Science and Statics
THINK BIG WE DO
The University of Rhode Island
http://www.forensics.cs.uri.edu

13:00