Lets talk about the filesystem

- Recall the boot process…
  - BIOS starts POST
  - Finds DRIVES using BIOS sequence
  - Finds BOOTABLE MEDIA
    - Based on MBR (512 Bytes)

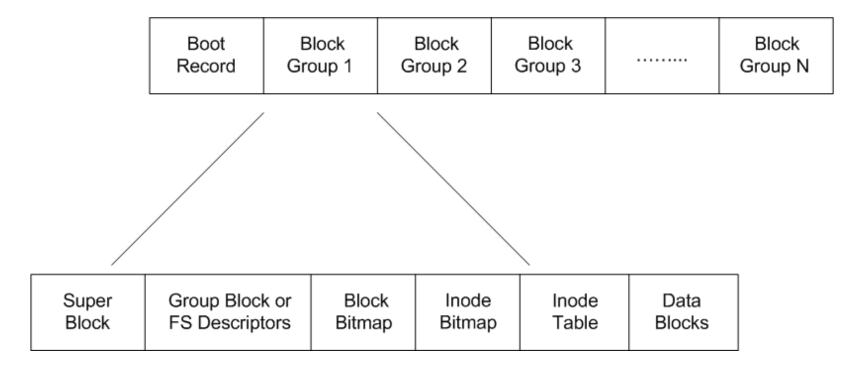# MBR structure

- MBR executable code starts at offset 0x0000, total 446 bytes
  - The MBR messages start at offset 0x008b
- The partition table starts at offset 0x01be
  - 64 bytes in four 16 bytes sections
  - 1st partition Entry starts at offset 0x01be
  - 2nd partition entry starts at offset 0x01ce
  - 3rd partition entry starts at offset 0x01de
  - 4th partition entry starts at offset 0x01ee
- The signature is at offset 0x01fe, 2 bytes (55AAh)
- Total 512 bytes

Disk Structure

- Disks are partitioned
- Each partition contains the following areas:
  - An optional boot block
  - A super block defining the boundaries of the other areas.
  - Block Bitmap
  - Inode Bitmap
  - A set of file information blocks known as I-nodes
  - The data blocks (free and used intermingled)

Functionality

- ext2/ext3 filesystem structure

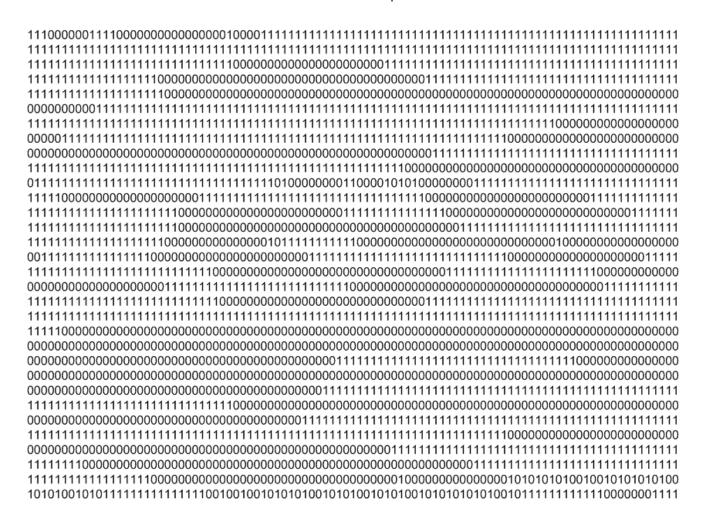| Boot Record	Block Group 1	Block Group 2	Block Group 3	....	Block Group N

Super Block	Group Block or FS Descriptors	Block Bitmap	Inode Bitmap	Inode Table	Data Blocks

Functionality

Block Bitmap

```
1110000001110000000000000000001000011111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111110000000000000000000000111111111111111111111111111111111111111111111
1111111111111111111000000000000000000000000000000000001111111111111111111111111111111111111111111
1111111111111111111100000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111110000000000000000000
0000011111111111111111111111111111111111111111111111111111111111111111000000000000000000000000000
0000000000000000000000000000000000000000000000000000000001111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111110000000000000000000000000000000000000000000
0111111111111111111111111111111110100000000110000101010000000111111111111111111111111111111111111
1111100000000000000000000001111111111111111111111111111110000000000000000000000001111111111111111
1111111111111111111110000000000000000000001111111111111110000000000000000000000001111111111111111
1111111111111111111100000000000000000000000000000000000011111111111111111111111111111111111111111
1111111111111111111100000000000000010111111111110000000000000000000000000000001000000000000000000
0011111111111111111100000000000000000000001111111111111111111111111111110000000000000000000011111
1111111111111111111111111100000000000000000000000000001111111111111111111111111110000000000000000
0000000000000000001111111111111111111111111111110000000000000000000000000000000000001111111111111
1111111111111111111111110000000000000000000000000001111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000011111111111111111111111111111111111111111100000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000011111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111110000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111100000000000000000000000000000000000000
0000000000000000000000000000000000000011111111111111111111111111111111111111111111111111111111111
1111111100000000000000000000000000000000000000000011111111111111111111111111111111111111111111111
1111111111111111110000000000000000000000000000000000010000000000000001010101010010010101010100
101010010101111111111111100100100101010100101010010101010010101010101001011111111111111100000001111
```

Functionality

I-Node Bitmap

11100000001110000000000000000001000011111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111100000000000000000000001111111111111111111111111111111111111111111111
11111111111111111110000000000000000000000000000000000000111111111111111111111111111111111111111111
11111111111111111110000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111110000000000000000000
00001111111111111111111111111111111111111111111111111111111111111111111111110000000000000000000000
00000000000000000000000000000000000000000000000000000001111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111110000000000000000000000000000000000000000000000
01111111111111111111111111111111111010000000011000010101000000001111111111111111111111111111111111
11110000000000000000000001111111111111111111111111111111100000000000000000000011111111111
11111111111111111110000000000000000000000011111111111111100000000000000000000000001111111
11111111111111111110000000000000000000000000000000000000011111111111111111111111111111111111111111
11111111111111111110000000000000101111111111100000000000000000000000000000100000000000000000
00111111111111111110000000000000000000001111111111111111111111111111100000000000000000000011111
11111111111111111111111000000000000000000000000001111111111111111111111111000000000000
00000000000000000001111111111111111111111111111000000000000000000000000000000001111111111
11111111111111111111111110000000000000000000000000001111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000001111111111111111111111111111111111111110000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111110000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000001111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111110000000000000000000000
00000000000000000000000000000000000111111111111111111111111111111111111111111111111111111111111111
11111110000000000000000000000000000000000000000000001111111111111111111111111111111111111
11111111111111111110000000000000000000000000000010000000000000001010101010010010101010100
10101001010111111111111111001001001010101001010100101010100101010101010100101111111111111100000001111

superblock

- Superblock contains
  - Magic Number
    - For EXT2, it is 0xEF53
  - Mount Count and Maximum Mount Count
  - Block Size, for example 4096B
  - Inode count and Block count
  - Number of free disk blocks
  - Number of free inodes on the system
  - First inode
    - This is the inode number of the first inode in the file system. The first inode in an EXT2 root file system would be the directory entry for the '/' directory
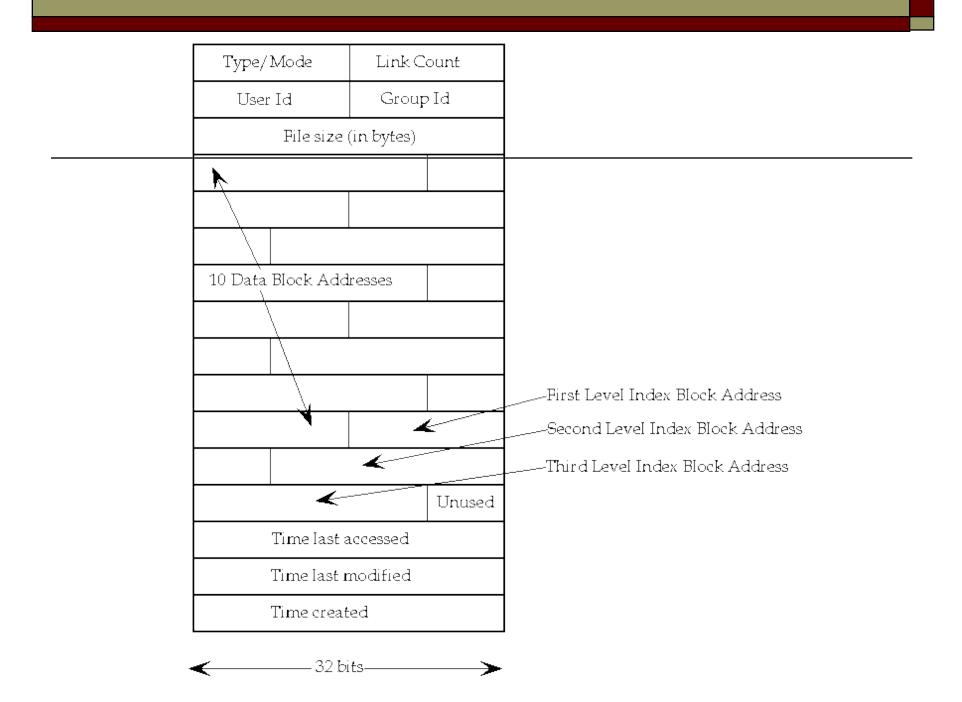
Inodes

- Contain META data (info about files)
  - type
  - Owner
  - Permission bits
  - MAC times
  - Links to the file (link count)
  - Data block addresses

I-nodes System V

- An I-node consists of 16 32 bit words
  - Word 0 is split into two 16 bit words
    - These contain the file type and mode and the link count (more later).
  - Word 1 is split into two 16 bit words
    - The user and group ids
  - Word 2 gives the file size in bytes
    - Implying a maximum filesize of 4 GB

I-nodes System V cont.

- Word 13 contains the time of last access

- Word 14 contains the time of last data modification

- Word 15 contains the time of the last file status change.

Type/Mode	Link Count
User Id	Group Id
File size (in bytes)	

10 Data Block Addresses	
	Unused

First Level Index Block Address

Second Level Index Block Address

Third Level Index Block Address

Time last accessed
Time last modified
Time created

← 32 bits →

Inode pointer structure (From wikipedia)

Directories

- Everything in Linux is a file

- Directory is a simple file whose data is a sequence of file entries which contains:

  - Inode number

  - Byte offset in directory (or the length of this entry)

  - File name

Directory example

Byte offset in directory	Inode number	File name
0	70	.
16	35	..
32	123	file1
48	345	file2
64	90	file3

Directory entry

Carrier B., Why Recovering a Deleted Ext3 File
Is Difficult . . .