WinHex

Chris P David

October 28, 2016

CSC 317

Professor MacDonald

Contents

1 Introduction

Essentially in the start sector (or the first sector) we see the MBR. What this does is tell or gives the file system to access the volume. Within this boot sector are is a table with fields that hold many values. Below is an explanation of the offsets followed by what is represented by that offset value.

Almost all of the data shown in this report was taken from some sites, which I will be referencing. For the table in the next section. I will be giving the offset hex value along with the value title, length in bytes if applicable, and lastly the hex value. I also converted the hex value to decimal for items I thought were more suited for a number based answer.

2 Start Sector

The values are as follows:
At **offset 0** is the JMP instruction with is basically in every boot record.
At **offset 3** is the OEM identifier, this is an eight-byte asci string that shows the system that formatted the disk.
At **offset B** is Bytes per sector, this is the size of a hardware sector.
At **offset D** is Sectors per cluster, because FAT is limited in the number of clusters it can track, volumes are helped by the ability to increase the numbers of sectors per cluster.
At **offset E** is Reserved sectors, basically these are sectors that precede the start of the first FAT.
At **offset 10** is Number of FATs, this is the number of copies of the FAT table on the disk.
At **offset 11** is Root Entries, this is the total number of file name entries that can be stored in the root directory of the volume.
At **offset 13** is the Number of Sector, this is used to store the number of sectors on the disk if the volume size is small enough.
At **offset 15** is Media Descriptor, this byte provides information about the media being used.
At **offset 16** is Sectors per FAT, this shows the numbers of sectors being occupied by each of the FATs on volume.
At **offset 18** is Sectors per Head, these values are a part of the disk geometry in use when the disk was formatted.
At **offset 1A** is Heads per Cylinder, like Sectors per head these values are a part of disk geometry, though these reflect the number of cylinders per head
At **offset 1C** is Hidden Sectors, is the number of sectors on the physical disk preceding the start of the volume, before the boot sector itself
At **offset 20** is Big number of Sectors, basically this is an indicator if the small sectors field is either zero or nonzero.
At **offset 24** is Big Sectors Per FAT, this is related to the BIOS physical disk number.
At **offset 28** is ExtFlags, a check for is if the FAT is in synch or not. Also for if FAT mirroring is disabled.
A Note the following fields are only defined for FAT32.
At **offset 2A** is FSVersion, version of file system.
At **offset 2C** is RootDirectoryStart, contains the number of the first cluster for the root directory.

At **offset 30** is FSInfoSector, this is the number for the file system information sector.

At **offset 32** is BackupBootSector, this is the sector number for the backup copy of the boot sector.

At **offset 34** is Reserved, reserved.

All information tanken from [1].

2.1 WinHex Table

Offset	Title	Length in bytes*	Hex(Value if require)
0	JMP instruction		33 C0 8E
3	OEM identifier		D0
B	Bytes per sector	2	BE:00 (190)
D	Sectors per cluster	1	7C (124)
E	Reserved sectors	2	BF:00 (191)
10	Number of FATs	1	06 (6)
11	Root Entries	2	B9 (185)
13	Number of Sector	2	02:FC (FC:02 or 64514)
15	Media Descriptor	1	F3
16	Sectors per FAT	2	50:A4 (20,644)
18	Sectors per Head	2	1C:68 (7,272)
1A	Heads per Cylinder	2	CB:06 (51,974)
1C	Hidden Sectors	4	00:04:B9:FB (309,755)
20	Big number of Sectors	4	80:07:BE:BD (2,147,991,229)
24	Big Sectors Per FAT	4	7C:00:00:7E(2,080,374,910)
28	ExtFlags	2	0F:0B(3,851)
2A	FSVersion	2	0E:85(3717)
2C	RootDirectoryStart	4	10:C5:83:01(281,379,585)
30	FSInfoSector	2	F1:E2(61,922)
32	BackupBootSector	2	18:CD(6,349)
34	Reserved	12	too big so 88:56:00:55:C6:46:11:05:C6:46:10:00
*Length give by reference 1			

3 Slack Space File

File Name- UNDERTALE.exe

File Extension- EXE

Size- 3.6MB

Creation Date-10/14/2016 16:03

Last Modification Date-06/23/2016 20:36

Last Access Date-10/26/2016

Attributes-A

[1] Detailed Explanation of the FAT Boot Sector

First Sector Number-53,991,744

(First) Cluster Number-1,686,220

Physical Sector Number-53,991,744

Logical Sector Number-53,991,776

The size of the file is 3.6 MB which is roughly 3774873 bytes.

Current Cluster number is 1,689,769 -¿ 1,689,770.

I then saved the block of slack space in my directory for this class.

4 Bibliography

Detailed Explanation of the FAT Boot Sector

Detailed Explanation of the FAT Boot Sector. Retrieved October 25, 2016,from

http://www.dewassoc.com/kbase/harddrives/bootsector