COEN 152 Computer Forensics

Master Boot Record Example

Review of the Master Boot Record on a Windows system.

Examination of a Master Boot Record and Partition Table

The MBR is located at sector 0, that is, at the sector located on head 0, cylinder 0, and sector 1 in CSH. Using WinHex, we see the following image

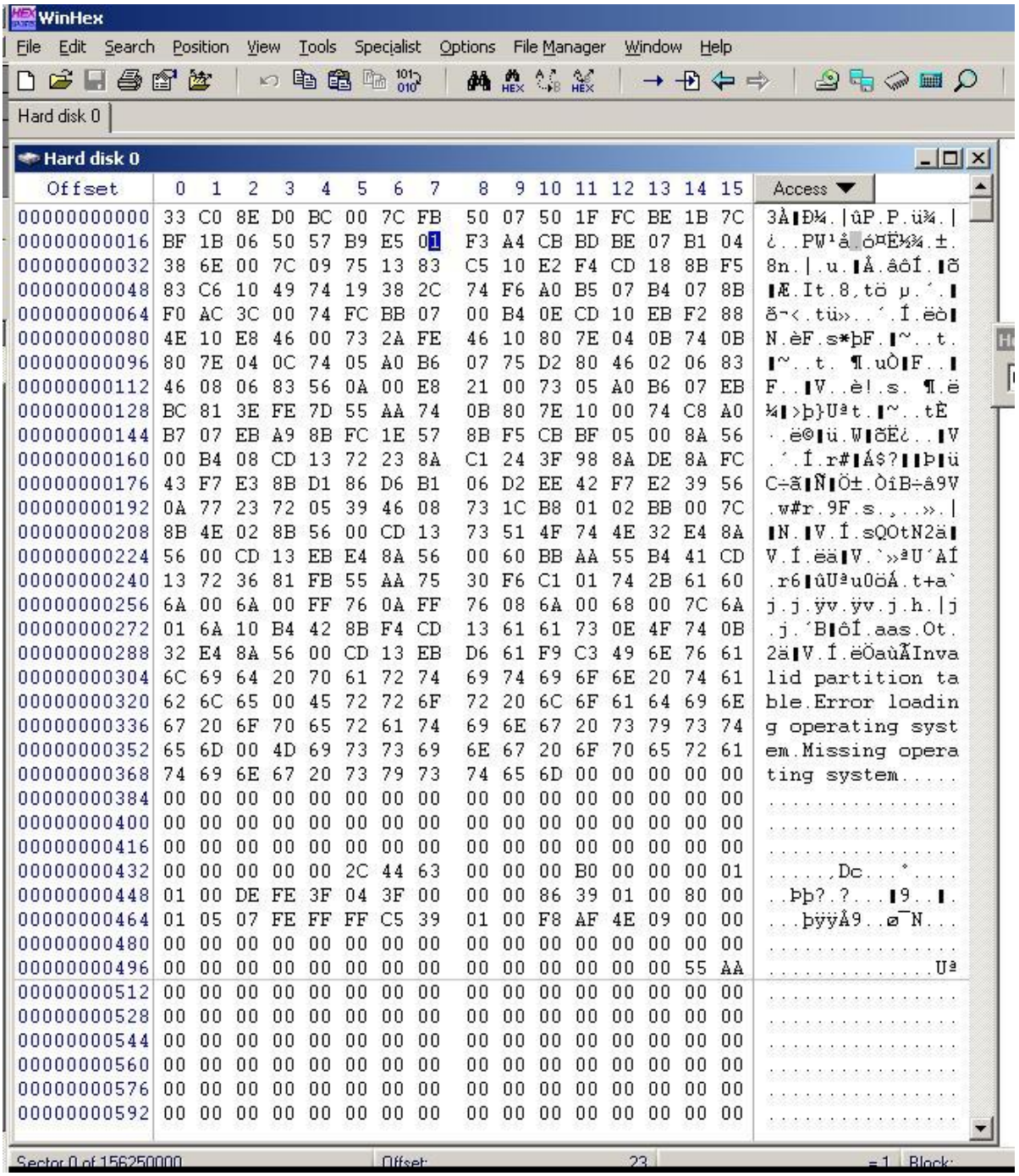
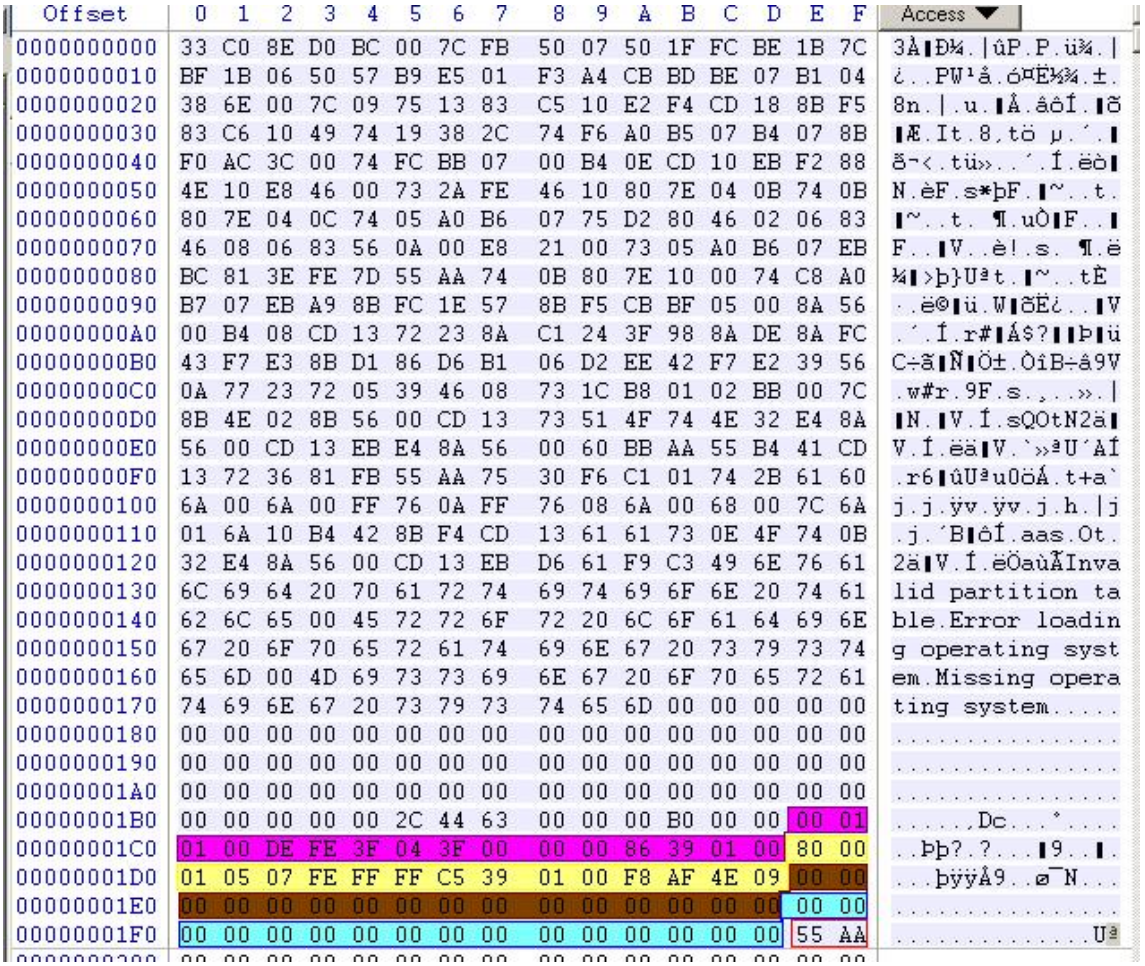


Figure 1: WinHex image of Sector 0

Most of the first sector (up to offset 511) is the bootstrap program. We can see the message table starting at offset 300. To find the partition table, we go to the end of the MBR. The very last two bytes are a signature, they should be always 55 AA, but the boot strap could have been altered for good reasons. The partition table sits on top of these two bytes. Each entry is 16B long or one (broken) in this WinHex setting. The partition table is always 64B long.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Access
0000000000	33	C0	8E	D0	BC	00	7C	FB	50	07	50	1F	FC	BE	1B	7C	3À▮Ð¼.|û|P.P.ü¾.|
0000000010	BF	1B	06	50	57	B9	E5	01	F3	A4	CB	BD	BE	07	B1	04	¿..PW¹å.ó¤Ë½¾.±.
0000000020	38	6E	00	7C	09	75	13	83	C5	10	E2	F4	CD	18	8B	F5	8n.|.u.▮Å.âôÍ.▮õ
0000000030	83	C6	10	49	74	19	38	2C	74	F6	A0	B5	07	B4	07	8B	▮Æ.It.8,tö µ.´.▮
0000000040	F0	AC	3C	00	74	FC	BB	07	00	B4	0E	CD	10	EB	F2	88	ð¬<.tü».´.Í.ëò▮
0000000050	4E	10	E8	46	00	73	2A	FE	46	10	80	7E	04	0B	74	0B	N.èF.s*þF.▮~..t.
0000000060	80	7E	04	0C	74	05	A0	B6	07	75	D2	80	46	02	06	83	▮~..t. ¶.uÒ▮F..▮
0000000070	46	08	06	83	56	0A	00	E8	21	00	73	05	A0	B6	07	EB	F..▮V..è!.s. ¶.ë
0000000080	BC	81	3E	FE	7D	55	AA	74	0B	80	7E	10	00	74	C8	A0	¼▮>þ}Uªt.▮~..tÈ
0000000090	B7	07	EB	A9	8B	FC	1E	57	8B	F5	CB	BF	05	00	8A	56	·.ë©▮ü.W▮õË¿..▮V
00000000A0	00	B4	08	CD	13	72	23	8A	C1	24	3F	98	8A	DE	8A	FC	.´.Í.r#▮Á$?▮▮Þ▮ü
00000000B0	43	F7	E3	8B	D1	86	D6	B1	06	D2	EE	42	F7	E2	39	56	C÷ã▮Ñ▮Ö±.Ò▮B÷â9V
00000000C0	0A	77	23	72	05	39	46	08	73	1C	B8	01	02	BB	00	7C	.w#r.9F.s.¸..».|
00000000D0	8B	4E	02	8B	56	00	CD	13	73	51	4F	74	4E	32	E4	8A	▮N.▮V.Í.sQOtN2ä▮
00000000E0	56	00	CD	13	EB	E4	8A	56	00	60	BB	AA	55	B4	41	CD	V.Í.ëä▮V.`»ªU´AÍ
00000000F0	13	72	36	81	FB	55	AA	75	30	F6	C1	01	74	2B	61	60	.r6▮ûUªu0öÁ.t+a`
0000000100	6A	00	6A	00	FF	76	0A	FF	76	08	6A	00	68	00	7C	6A	j.j.ÿv.ÿv.j.h.|j
0000000110	01	6A	10	B4	42	8B	F4	CD	13	61	61	73	0E	4F	74	0B	.j.´B▮ôÍ.aas.Ot.
0000000120	32	E4	8A	56	00	CD	13	EB	D6	61	F9	C3	49	6E	76	61	2ä▮V.Í.ëÖaùÃInva
0000000130	6C	69	64	20	70	61	72	74	69	74	69	6F	6E	20	74	61	lid partition ta
0000000140	62	6C	65	00	45	72	72	6F	72	20	6C	6F	61	64	69	6E	ble.Error loadin
0000000150	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74	g operating syst
0000000160	65	6D	00	4D	69	73	73	69	6E	67	20	6F	70	65	72	61	em.Missing opera
0000000170	74	69	6E	67	20	73	79	73	74	65	6D	00	00	00	00	00	ting system.....
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000001B0	00	00	00	00	00	2C	44	63	00	00	00	B0	00	00	00	01	.....,Dc...°....
00000001C0	01	00	DE	FE	3F	04	3F	00	00	00	86	39	01	00	80	00	..Þþ?.?...▮9..▮.
00000001D0	01	05	07	FE	FF	FF	C5	39	01	00	F8	AF	4E	09	00	00	...þÿÿÅ9..ø¯N...
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA	..............Uª

Figure 2: Partition Table Entries Highlighted

Figure 2 locates the partition table and its four entries. (Notice that by clicking on the Offset field to the right, WinHex changes to hexadecimal notation.) We now analyze the second (yellow) entry in detail.

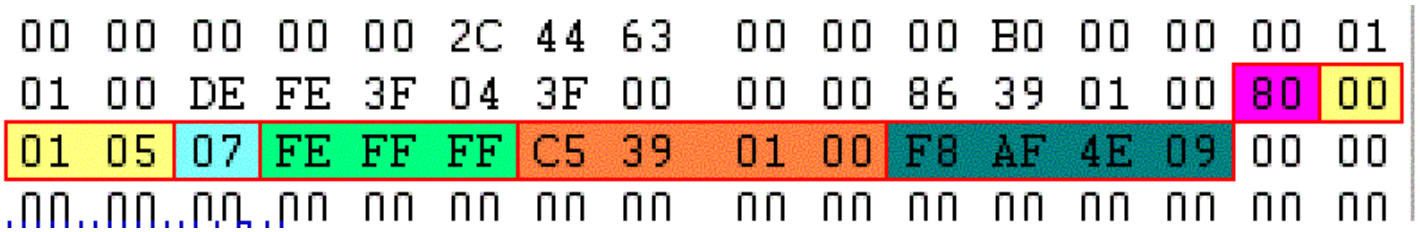
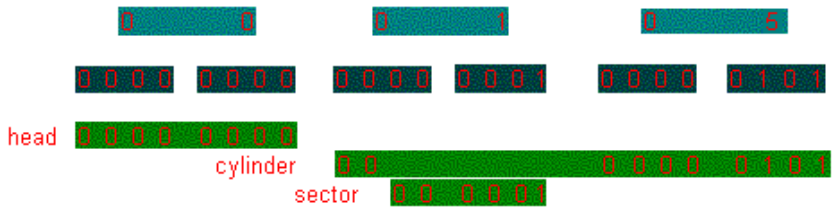


Figure 3: Partition Table Entry

- The first entry is the one byte long boot flag. Only one bit of the byte is used, so there are only two possible values: 80 for a bootable partition and 00 for a non-bootable partition. The boot process jumps to the boot sector in the first bootable partition, which would be this one.
- The next three bytes (in yellow) give the start of the partition using the CHS format. To read this field, we need to break it up into bits.



The first 8 bits form the head number, so the head is 0. The cylinder is made up of the last byte plust the leading two bits of the middle byte. The cylinder number is 5. The sector number is made up of the six least significant digits of the middle byte, here it is 1.

- The next field (the blue one) is the partition type. Go to Andries Brouwer Partition type table to find out what it means. There are a number of possibilities, OS/2 (not supported for a long time), Windows NT NTFS, advanced

UNIX, or an old version for QNX2. The only real choice is an NTFS partition.

- The green field gives the CHS of the end of the partition. We write the value in binary: 1111 1110 1111 1111 1111 1111 and extract the bits. The head bits are 1111 1110 in binary or 254 in decimal. The cylinder bits are 11 1111 1111 or 1023 in decimal, and the sector value is 11 1111 or 63 in binary. (These numbers do not have a lot to do with the physical geometry of the hard drive, rather, the hard drive interface pretends to have these many heads in order to allow all sectors to be addressed.
- The orange field is the Logical Block Address (or LBA) of the start sector. We translate first from little endian to obtain the hexadecimal value 00 01 39 C5, which translates to 80325 in decimal. This is the same sector number that the CHS value gives. (WinHex supports both physical and logical sector addresses.)
- The dark green field is the number of sectors. Translated from little endian, we obtain 09 4E AF F8 or 156,151,800 sectors. If we multiply this by the number of bytes in the sector, we obtain 79,949,721,600 or about 80GB.

To continue investigating this partition, we move to the first sector: NTFS Example