Christian Schindelhauer & Amir Alsbih

Freiburg, the 17th January, 2012
Discussion 23rd January, 2012

Exercise for the lecture

# Distributed Storage and Computer Forensic

Winter 2011/12

Sheet 10

**EXERCISE 10:**

1. Take a look at the following dump of a MBR:

```
0000000: fa33 c08e d0bc 007c 8bf4 5007 501f fbfc
0000010: bf00 06b9 0001 f2a5 ea1d 0600 00be be07
0000020: b304 803c 8074 0e80 3c00 751c 83c6 10fe
0000030: cb75 efcd 188b 148b 4c02 8bee 83c6 10fe
0000040: cb74 1a80 3c00 74f4 be8b 06ac 3c00 740b
0000050: 56bb 0700 b40e cd10 5eeb f0eb febf 0500
0000060: bb00 7cb8 0102 57cd 135f 730c 33c0 cd13
0000070: 4f75 edbe a306 ebd3 bec2 06bf fe7d 813d
0000080: 55aa 75c7 8bf5 ea00 7c00 0049 6e76 616c
0000090: 6964 2070 6172 7469 7469 6f6e 2074 6162
00000a0: 6c65 0045 7272 6f72 206c 6f61 6469 6e67
00000b0: 206f 7065 7261 7469 6e67 2073 7973 7465
00000c0: 6d00 4d69 7373 696e 6720 6f70 6572 6174
00000d0: 696e 6720 7379 7374 656d 0000 0000 0000
00000e0: 0000 0000 0000 0000 0000 0000 0000 0000
00000f0: 0000 0000 0000 0000 0000 0000 0000 0000
0000100: 0000 0000 0000 0000 0000 0000 0000 0000
0000110: 0000 0000 0000 0000 0000 0000 0000 0000
0000120: 0000 0000 0000 0000 0000 0000 0000 0000
0000130: 0000 0000 0000 0000 0000 0000 0000 0000
0000140: 0000 0000 0000 0000 0000 0000 0000 0000
0000150: 0000 0000 0000 0000 0000 0000 0000 0000
0000160: 0000 0000 0000 0000 0000 0000 0000 0000
0000170: 0000 0000 0000 0000 0000 0000 0000 0000
0000180: 0000 0000 0000 0000 0000 0000 0000 0000
0000190: 0000 0000 0000 0000 0000 0000 0000 0000
00001a0: 0000 0000 0000 0000 0000 0000 0000 0000
00001b0: 0000 0000 0000 0000 0000 0000 0000 0001
00001c0: 1400 0403 60da 3300 0000 4ded 0000 0000
00001d0: 0000 0000 0000 0000 0000 0000 0000 0000
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000
00001f0: 0000 0000 0000 0000 0000 0000 0000 55aa
```

What partitions can be found on this image? What can you tell about these partitons?

2. Take a look at the following dump of a FAT12 Boot sector:

```
0000000: eb3e 9050 7772 5368 6f74 2000 0220 0100
0000010: 0200 024d edf8 0600 2000 0400 3300 0000
0000020: 0000 0000 8000 2911 28d2 2943 414e 4f4e
0000030: 5f44 4320 2020 4641 5431 3220 2020 33ff
0000040: 8edf be00 7c8d 9ce4 018e 4702 fcb9 0002
0000050: f3a4 c707 5800 ff2f 8cc8 fa8e d0bc 0006
0000060: fb8b ec83 ec16 c536 7800 8976 f68c 5ef8
0000070: 8d7e eab9 0b00 57f3 a45f 8ed9 be78 0089
0000080: 3c8c 4402 0e1f c645 0412 c645 090f b200
0000090: 91cd 13a0 1800 f626 1a00 8946 fa83 3eea
00000a0: 0100 7520 a010 0098 f626 1600 0306 0e00
00000b0: a3ea 0191 b820 00f7 2611 00f7 360b 0003
00000c0: c1a3 ec01 33d2 a1ea 01b9 0100 c41e e001
00000d0: e890 00b0 20f6 26e8 01c4 3ee0 0103 f8be
00000e0: f101 b90b 00f3 a674 24be a501 e849 0032
00000f0: e4cd 16e8 0200 cd19 33c0 8ed8 bb78 00c4
0000100: 7ef6 893f 8c47 02c3 becc 01eb dfc4 1ee0
0000110: 018b 16ee 01a1 ec01 8a0e f001 b500 e842
0000120: 00e8 d4ff bb84 002e 8a16 2400 c747 02ff
0000130: ff89 172e ff2e e001 ac0a c074 25b4 0ebb
0000140: 0700 cd10 ebf2 0306 1c00 1316 1e00 f776
0000150: fa89 46fe 8bc2 f636 1800 8846 fcfe c488
0000160: 66fd c3e3 fd52 5051 e8db ffb8 0100 50e8
0000170: 1900 5872 9359 5f5a 2bc8 03f8 83d2 0052
0000180: 57f7 260b 0003 d858 5aeb d88b 56fe b106
0000190: d2e6 0a76 fd8b ca86 e98a 1624 008a 76fc
00001a0: b402 cd13 c34e 6f20 5379 7374 656d 206f
00001b0: 6e20 4469 736b 0d0a 5072 6573 7320 4573
00001c0: 6320 746f 2052 6562 6f6f 7400 4469 736b
00001d0: 2042 6f6f 7420 4661 696c 7572 6500 0000
00001e0: 0000 7000 0000 000c 0000 0000 0000 0000
00001f0: 0049 424d 4249 4f20 2043 4f4d 0080 55aa
```

Try to give all the information fsstat would read from this.