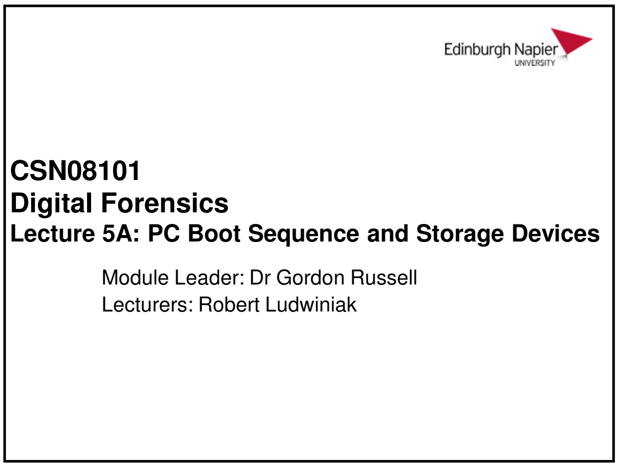
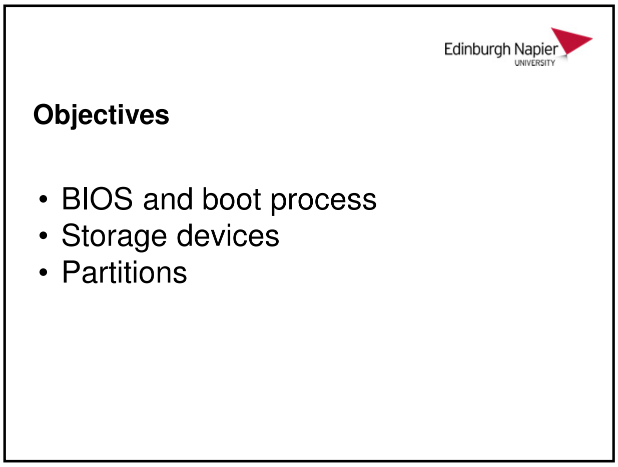


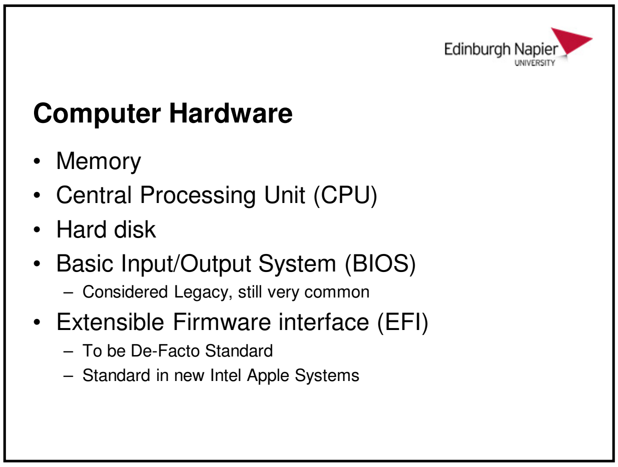
CSN08101
Digital Forensics
Lecture 5A: PC Boot Sequence and Storage Devices

Module Leader: Dr Gordon Russell
Lecturers: Robert Ludwiniak



Objectives

- BIOS and boot process
- Storage devices
- Partitions



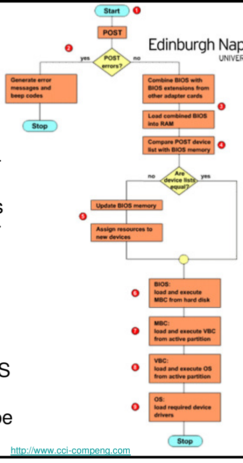
Computer Hardware

- Memory
- Central Processing Unit (CPU)
- Hard disk
- Basic Input/Output System (BIOS)
  - Considered Legacy, still very common
- Extensible Firmware interface (EFI)
  - To be De-Facto Standard
  - Standard in new Intel Apple Systems

Boot Process

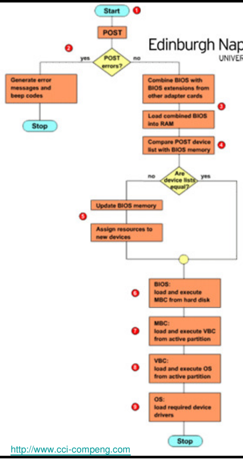
- BIOS Instructions
- Disk Sector 0 Instructions
- Partition Sector 0 Instructions
- Operating System Files

1. When the PC is turned on, the CPU begins executing the instructions in the ROM BIOS chip, starting at a pre-defined instruction location.
2. The BIOS performs the power-on-self-test (POST). If there are errors, the BIOS generates appropriate messages and / or beep codes, and the boot process stops.
3. If the POST tests are successful, the BIOS from any other adapter cards are combined with the normal BIOS and loaded into memory (shadowing), where they can be executed faster than in ROM.


Start
1
POST
2
yes
POST errors?
no
Generate error messages and beep codes
Stop
Combine BIOS with BIOS extensions from other adapter cards
3
Load combined BIOS into RAM
Compare POST device list with BIOS memory
4
no
Are device lists equal?
yes
Update BIOS memory
5
Assign resources to new devices
6
BIOS: load and execute MBC from hard disk
7
MBC: load and execute VBC from active partition
8
VBC: load and execute OS from active partition
9
OS: load required device drivers
Stop

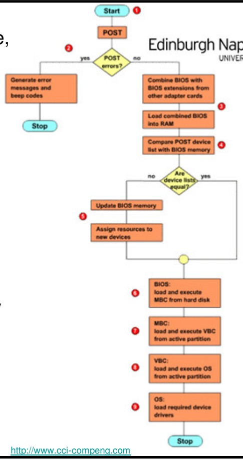
http://www.cci-compeng.com

4. The list of devices found during the POST is compared with the list of devices in the non-volatile BIOS memory (CMOS) chip.
5. If the lists differ, then a new device must have been added. In this case, the BIOS memory is updated accordingly, and available system resources (such as IRQs) are assigned to the new devices.
6. The BIOS loads and executes the master boot code in the master boot record of the first bootable device.


Start
1
POST
2
yes
POST errors?
no
Generate error messages and beep codes
Stop
Combine BIOS with BIOS extensions from other adapter cards
3
Load combined BIOS into RAM
Compare POST device list with BIOS memory
4
no
Are device lists equal?
yes
Update BIOS memory
5
Assign resources to new devices
6
BIOS: load and execute MBC from hard disk
7
MBC: load and execute VBC from active partition
8
VBC: load and execute OS from active partition
9
OS: load required device drivers
Stop

http://www.cci-compeng.com

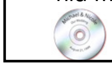
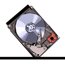
7. The master boot code locates the active partition of that device, then locates and executes the volume boot code in the volume boot record of that partition.
8. The volume boot code of the active partition locates and executes the operating system files on the partition, and transfers control to them.
9. The operating system now completes the boot process by loading appropriate device drivers. If device drivers for any new devices cannot be found, the operating system will generate an appropriate message, and give the user an opportunity to install the drivers now, or at a later time.


Start
1
POST
2
yes
POST errors?
no
Generate error messages and beep codes
Stop
Combine BIOS with BIOS extensions from other adapter cards
3
Load combined BIOS into RAM
Compare POST device list with BIOS memory
4
no
Are device lists equal?
yes
Update BIOS memory
5
Assign resources to new devices
6
BIOS: load and execute MBC from hard disk
7
MBC: load and execute VBC from active partition
8
VBC: load and execute OS from active partition
9
OS: load required device drivers
Stop

http://www.cci-compeng.com

Storage Media

- Hard disks, floppy disk, thumb drives etc.
- Hard disks are the richest in digital evidence
- Integrated Disk Electronics (IDE) or Advanced Technology Attachment (ATA)
- Higher performance SCSI drives
- Fireware is an adaptation of SCSI standards that provides high speed access to a chain of devices
- All hard drives contain platters made of light, rig-hid material such aluminum, ceramic or glass

More on Hard Drives

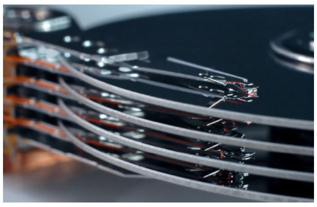
- Platters have a magnetic coating on both sides and spin between a pair of read/write heads
- These heads move like a needle on top of the old LP records but on a cushion of air created by the disk above the surface
- The heads can align particles of magnetic media called writing, and can detect how the magnetic particles are assigned – called reading
- Particles aligned one way are considered “0” and aligned another way “1”

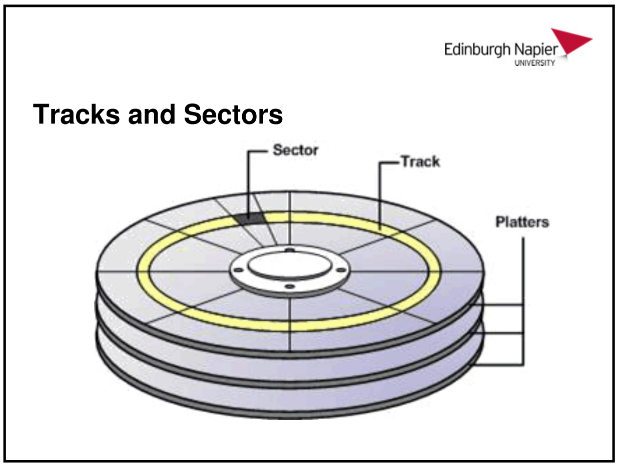
Hard Disks

Storage

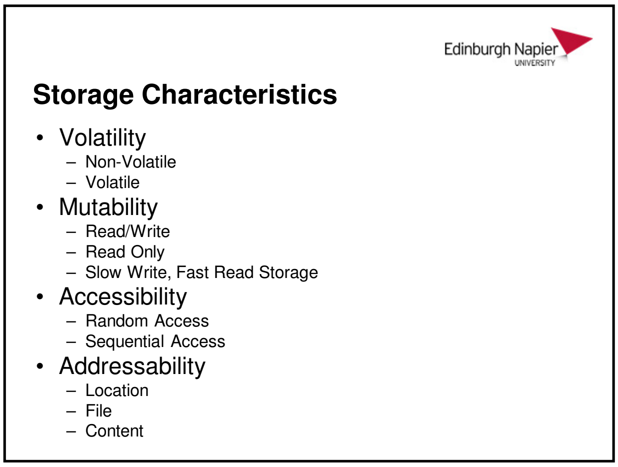
- Cylinders are the data tracks that the data is being recorded on
- Each track/cylinder is divided into *sectors* that contain 512 bytes of information
  - 512*8 bits of information
- Location of data can be determined by which *cylinder* they are on which *head* can access them and which *sector* contains them or CHS addressing
- Capacity of a hard drive # of C*H*S*512

Hard Disk Platters



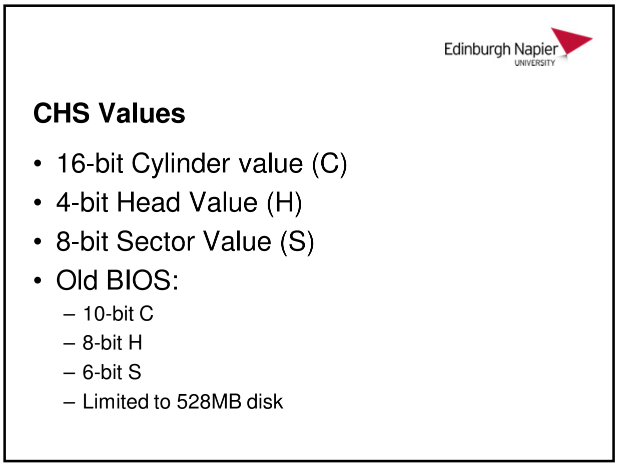


Tracks and Sectors



Storage Characteristics

- Volatility
  - Non-Volatile
  - Volatile
- Mutability
  - Read/Write
  - Read Only
  - Slow Write, Fast Read Storage
- Accessibility
  - Random Access
  - Sequential Access
- Addressability
  - Location
  - File
  - Content



CHS Values

- 16-bit Cylinder value (C)
- 4-bit Head Value (H)
- 8-bit Sector Value (S)
- Old BIOS:
  - 10-bit C
  - 8-bit H
  - 6-bit S
  - Limited to 528MB disk

Logical Block Address (LBA)

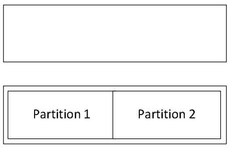
- LBA address may not be related to physical location of data
- Overcomes the 8.1 GB Limitation of CHS
- Plug old CHS values into:

LBA = (((CYLINDER * heads_per_cylinder) * HEAD) * sectors_per_track) + SECTOR -1

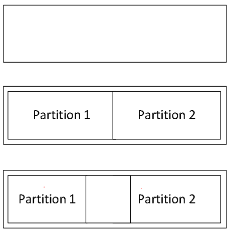
E.g. CHS 0,0,1 = LBA 0

Storage Volume

Storage Volume

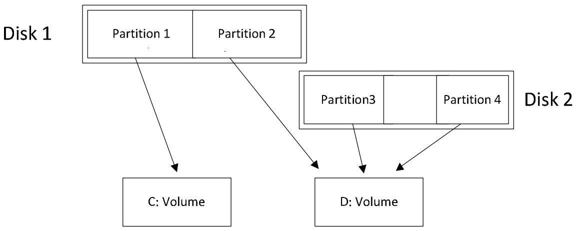


Storage Volume



Volume vs Partition

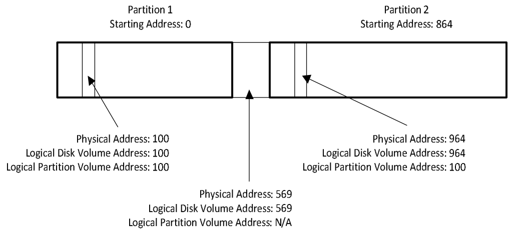
- Volume
  - A selection of addressable sectors that can be used by an OS or application. These sectors do not have to be consecutive
- Partition
  - A selection of addressable sectors that are consecutive. By definition, a partition is a volume



Partition Analysis

- A Partition organises the layout of a volume
- Sector Addressing
  - Physical Address (LBA or CHS)
  - Logical Disk Volume Address
  - Logical Partition Volume Address

Sector Addressing

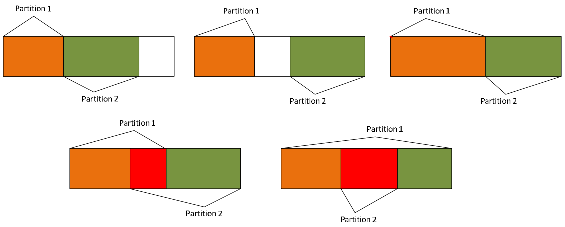

Partition 1
Starting Address: 0
Partition 2
Starting Address: 864
Physical Address: 100
Logical Disk Volume Address: 100
Logical Partition Volume Address: 100
Physical Address: 964
Logical Disk Volume Address: 964
Logical Partition Volume Address: 100
Physical Address: 569
Logical Disk Volume Address: 569
Logical Partition Volume Address: N/A

B Carrier, File System Forensic Analysis, pp75

Partition Analysis

- Analyse Partition Tables
  - Process them to identify the layout
  - Can then be used to process partition accordingly
  - Determine the type of data inside the partition
- Perform a sanity check to ensure that the partition table is telling the truth
  - This is important when imaging

Sanity Check

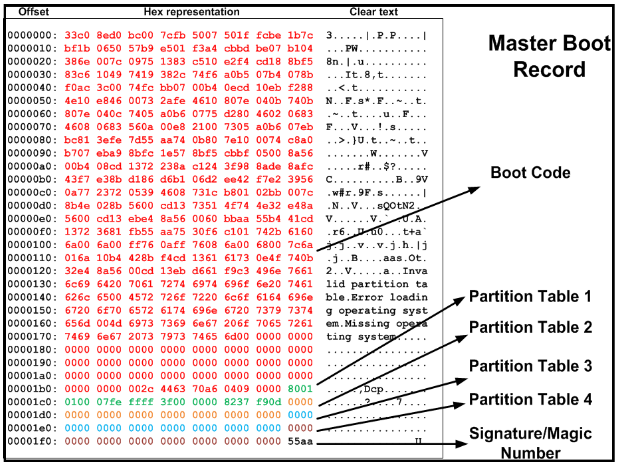


B Carrier, File System Forensic Analysis, pp76

Master Boot Record

- No standard reference
- Master Boot Record in first sector (1st 512 byte)
  - Boot Code
  - Partition Table
  - Signature Value
- MBR Supports a maximum of 4 partitions

Master Boot Record



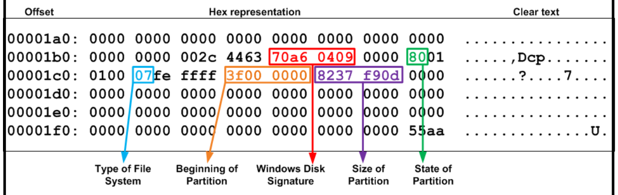
```
Offset              Hex representation                        Clear text
0000000: 33c0 8ed0 bc00 7cfb 5007 501f fcbe 1b7c  3.....|.P.P....|
0000010: bf1b 0650 57b9 e501 f3a4 cbbd be07 b104  ...PW...........
0000020: 386e 007c 0975 1383 c510 e2f4 cd18 8bf5  8n.|.u..........
0000030: 83c6 1049 7419 382c 74f6 a0b5 07b4 078b  ...It.8,t.......
0000040: f0ac 3c00 74fc bb07 00b4 0ecd 10eb f288  ..<.t...........
0000050: 4e10 e846 0073 2afe 4610 807e 040b 740b  N..F.s*.F..~..t.
0000060: 807e 040c 7405 a0b6 0775 d280 4602 0683  .~..t....u..F...
0000070: 4608 0683 560a 00e8 2100 7305 a0b6 07eb  F...V...!.s.....
0000080: bc81 3efe 7d55 aa74 0b80 7e10 0074 c8a0  ..>.}U.t..~..t..
0000090: b707 eba9 8bfc 1e57 8bf5 cbbf 0500 8a56  .......W.......V
00000a0: 00b4 08cd 1372 238a c124 3f98 8ade 8afc  .....r#..$?.....
00000b0: 43f7 e38b d186 d6b1 06d2 ee42 f7e2 3956  C..........B..9V
00000c0: 0a77 2372 0539 4608 731c b801 02bb 007c  .w#r.9F.s......|
00000d0: 8b4e 028b 5600 cd13 7351 4f74 4e32 e48a  .N..V...sQOtN2..
00000e0: 5600 cd13 ebe4 8a56 0060 bbaa 55b4 41cd  V......V.`..U.A.
00000f0: 1372 3681 fb55 aa75 30f6 c101 742b 6160  .r6..U.u0...t+a`
0000100: 6a00 6a00 ff76 0aff 7608 6a00 6800 7c6a  j.j..v..v.j.h.|j
0000110: 016a 10b4 428b f4cd 1361 6173 0e4f 740b  .j..B....aas.Ot.
0000120: 32e4 8a56 00cd 13eb d661 f9c3 496e 7661  2..V.....a..Inva
0000130: 6c69 6420 7061 7274 6974 696f 6e20 7461  lid partition ta
0000140: 626c 6500 4572 726f 7220 6c6f 6164 696e  ble.Error loadin
0000150: 6720 6f70 6572 6174 696e 6720 7379 7374  g operating syst
0000160: 656d 004d 6973 7369 6e67 206f 7065 7261  em.Missing opera
0000170: 7469 6e67 2073 7973 7465 6d00 0000 0000  ting system.....
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 002c 4463 70a6 0409 0000 8001  .....,Dcp.......
00001c0: 0100 07fe ffff 3f00 0000 8237 f90d 0000  ......?....7....
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  ..............U.
```

Partition Table

- Starting CHS Address
- Ending CHS Address
- Starting LBA Address
- Number of Sectors in Partition
- Type of Partition
- Flags

- Limitation
  - 2 Terabyte Disk Partition Limitation
    - MBR Partition size field is 32 bits

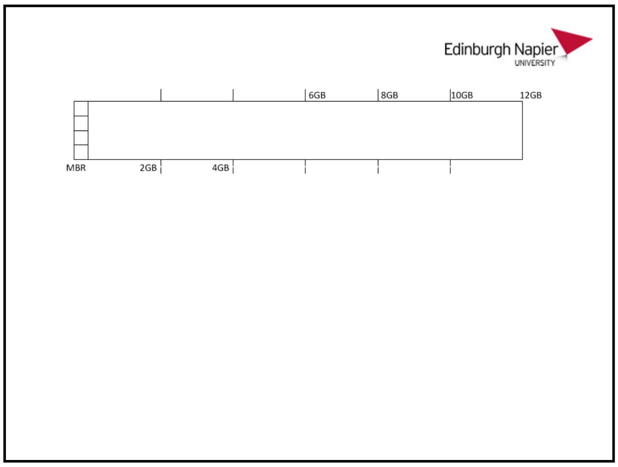
Example of Partition Table



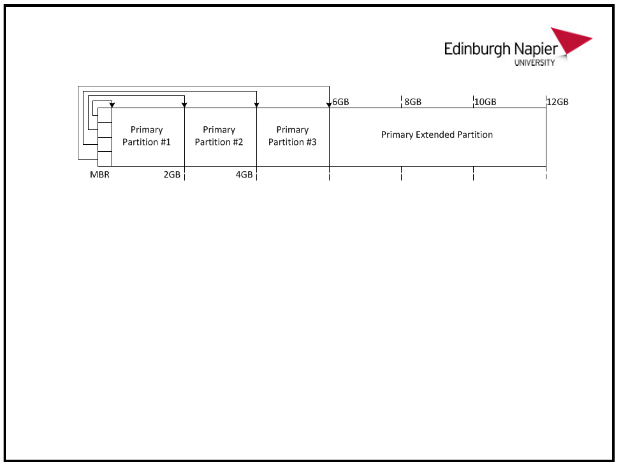
```
Offset                    Hex representation                        Clear text
00001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001b0: 0000 0000 002c 4463 70a6 0409 0000 8001  .....,Dcp.......
00001c0: 0100 07fe ffff 3f00 0000 8237 f90d 0000  ......?....7....
00001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Extended Partitions

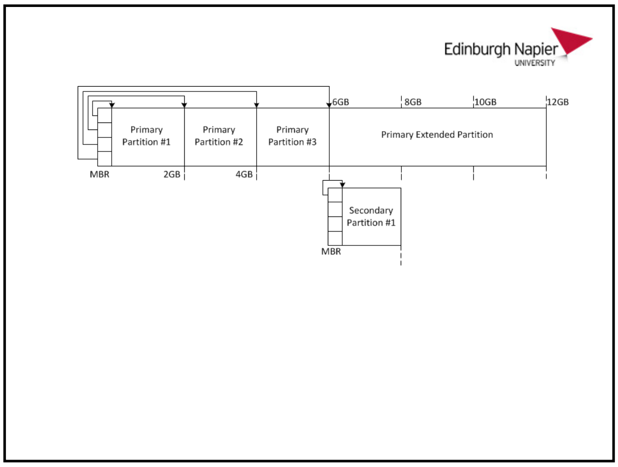
- Limitation of 4 Primary Partitions
- Creation of 3 Primary Partitions and 1 primary extended partition
- Primary Extended partition uses a similar MBR layout in order to create a linked list of records, showing where each new extended partitions exists in relation to the start of the last



6GB
8GB
10GB
12GB
MBR
2GB
4GB

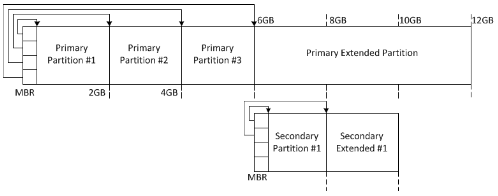


6GB
8GB
10GB
12GB
Primary Partition #1
Primary Partition #2
Primary Partition #3
Primary Extended Partition
MBR
2GB
4GB

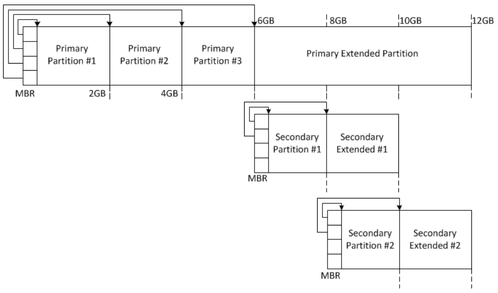


6GB
8GB
10GB
12GB
Primary Partition #1
Primary Partition #2
Primary Partition #3
Primary Extended Partition
MBR
2GB
4GB
Secondary Partition #1
MBR

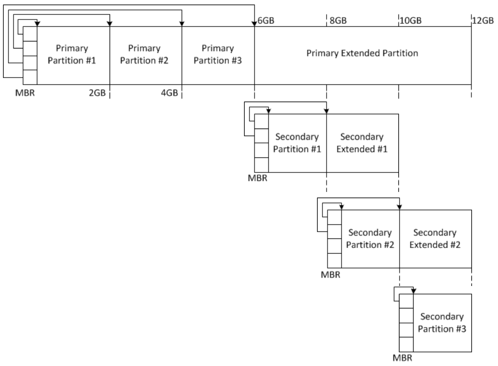
Edinburgh Napier UNIVERSITY



Edinburgh Napier UNIVERSITY



Edinburgh Napier UNIVERSITY



Disk Analysis

- MMLS - displays the contents of a volume system (media management). In general, this is used to list the partition table contents so that you can determine where each partition starts, ends, length of the partition and the type.
- SIGFIND - searches through a storage volume and looks for the hex-signature at a given offset. This can be used to search for lost boot sectors, superblocks, and partition tables.
- GPART – command that can scan drives and re-create a partition table based on "guesses“. This command can identify a number of file system types by testing sectors and assessing which file system type is the most probable

MMLS

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot     Start        End          Length       Description
00: Meta     0000000000   0000000000   0000000001   Primary Table(#0)
01: -----    0000000000   0000000062   0000000063   Unallocated
02: 00:00    0000000063   0003894911   0003894849   NTFS (0x07)
03: -----    0003894912   0004999679   0001104768   Unallocated
```

SIGFIND

```
Block size: 512  Offset: 510  Signature: 55AA
Block: 0             (-)
Block: 63            (+63)
Block: 92795         (+92732)
Block: 92796         (+1)
Block: 94839         (+2037)
Block: 94855         (+16)
Block: 237724        (+142869)
OUTPUT OMITTED ...
Block: 3473830       (+109635)
Block: 3894911       (+421081)
Block: 3894912       (+1)
Block: 3894975       (+63)
Block: 3894976       (+1)
Block: 3894983       (+1)
Block: 3905831       (+10848)
error reading bytes 4999680
```

```
0000000: eb52 904e 5446 5320 2020 2000 0204 0000  .R.NTFS    .....
0000010: 0000 0000 00f8 0000 3f00 8000 3f00 0000  ........?...?...
0000020: 0000 0000 8000 8000 406e 3b00 0000 0000  ........@n;.....
0000030: daf3 0400 0000 0000 c86d 0700 0000 0000  .........m......
0000040: f600 0000 0200 0000 f343 0504 7405 042a  .........C..t..*
0000050: 0000 0000 fa33 c08e d0bc 007c fbb8 c007  .....3.....|....
0000060: 8ed8 e816 00b8 000d 8ec0 33db c606 0e00  ..........3.....
0000070: 10e8 5300 6800 0d68 6a02 cb8a 1624 00b4  ..S.h..hj....$..
0000080: 08cd 1373 05b9 ffff 8af1 660f b6c6 4066  ...s......f...@f
0000090: 0fb6 d180 e23f f7e2 86cd c0ed 0641 660f  .....?.......Af.
00000a0: b7c9 66f7 e166 a320 00c3 b441 bbaa 558a  ..f..f. ...A..U.
00000b0: 1624 00cd 1372 0f81 fb55 aa75 09f6 c101  .$...r...U.u....
00000c0: 7404 fe06 1400 c366 601e 0666 a110 0066  t......f`..f...f
00000d0: 0306 1c00 663b 0620 000f 823a 001e 666a  ....f;. ...:..fj
00000e0: 0066 5006 5366 6810 0001 0080 3e14 0000  .fP.Sfh.....>...
00000f0: 0f85 0c00 e8b3 ff80 3e14 0000 0f84 6100  ........>.....a.
0000100: b442 8a16 2400 161f 8bf4 cd13 6658 5b07  .B..$.......fX[.
0000110: 6658 6658 1feb 2d66 33d2 660f b70e 1800  fXfX..-f3.f.....
0000120: 66f7 f1fe c28a ca66 8bd0 66c1 ea10 f736  f......f..f....6
0000130: 1a00 86d6 8a16 2400 8ae8 c0e4 060a ccb8  ......$.........
0000140: 0102 cd13 0f82 1900 8cc0 0520 008e c066  ........... ...f
0000150: ff06 1000 ff0e 0e00 0f85 6fff 071f 6661  ..........o...fa
0000160: c3a0 f801 e809 00a0 fb01 e803 00fb ebfe  ................
0000170: b401 8bf0 ac3c 0074 09b4 0ebb 0700 cd10  .....<.t........
0000180: ebf2 c30d 0a41 2064 6973 6b20 7265 6164  .....A disk read
0000190: 2065 7272 6f72 206f 6363 7572 7265 6400   error occurred.
00001a0: 0d0a 4e54 4c44 5220 6973 206d 6973 7369  ..NTLDR is missi
00001b0: 6e67 000d 0a4e 544c 4452 2069 7320 636f  ng...NTLDR is co
00001c0: 6d70 7265 7373 6564 000d 0a50 7265 7373  mpressed...Press
00001d0: 2043 7472 6c2b 416c 742b 4465 6c20 746f   Ctrl+Alt+Del to
00001e0: 2072 6573 7461 7274 0d0a 0000 0000 0000   restart........
00001f0: 0000 0000 0000 0000 83a0 b3c9 0000 55aa  ..............U.
```

GPART Scan

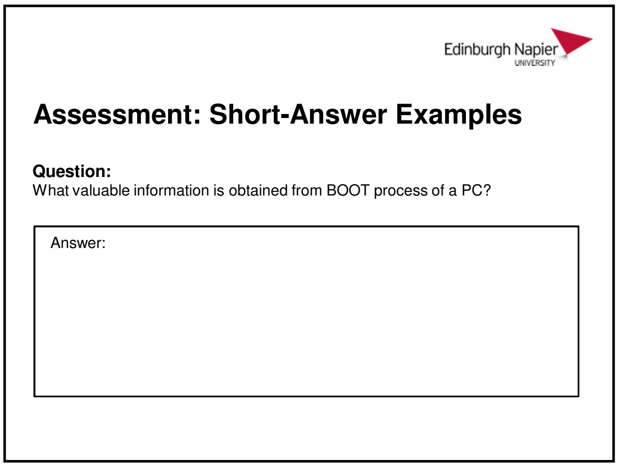
```
Begin scan...
Possible partition(Windows NT/W2K FS), size(1901mb), offset(0mb)
Possible partition(DOS FAT), size(539mb), offset(1901mb)
End scan.

OUTPUT OMITTED …

Guessed primary partition table:
Primary partition(1)
   type: 000(0x00)(unused)
   size: 0mb #s(0) s(0-0)
   chs:  (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r

Primary partition(2)
   type: 000(0x00)(unused)
   size: 0mb #s(0) s(0-0)
   chs:  (0/0/0)-(0/0/0)d (0/0/0)-(0/0/0)r
```

ANY QUESTIONS …

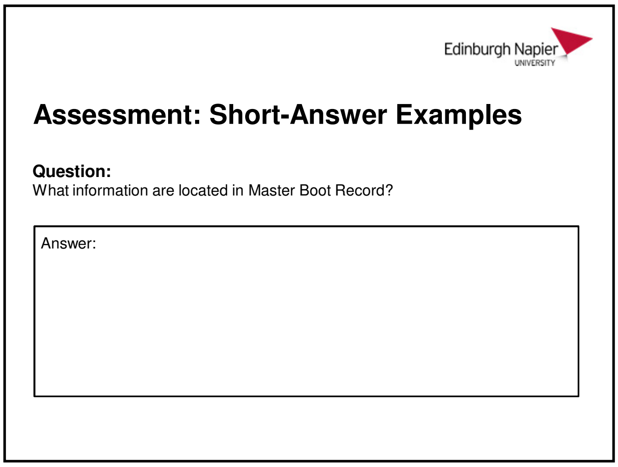


Edinburgh Napier UNIVERSITY

Assessment: Short-Answer Examples

Question:
What valuable information is obtained from BOOT process of a PC?

Answer:

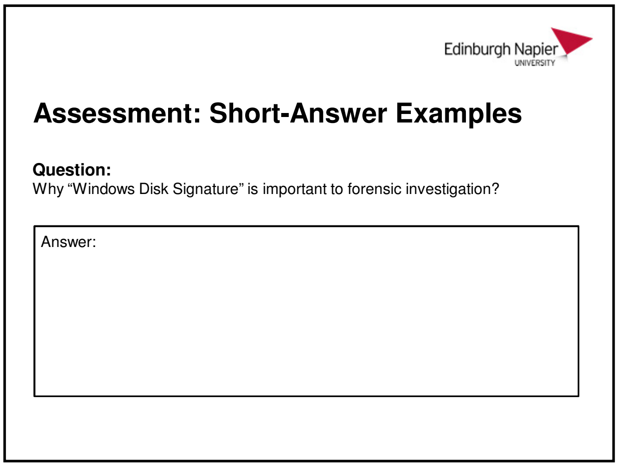


Edinburgh Napier UNIVERSITY

Assessment: Short-Answer Examples

Question:
What information are located in Master Boot Record?

Answer:



Edinburgh Napier UNIVERSITY

Assessment: Short-Answer Examples

Question:
Why “Windows Disk Signature” is important to forensic investigation?

Answer: