BIRMINGHAM CITY University

Digital Device Forensics

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

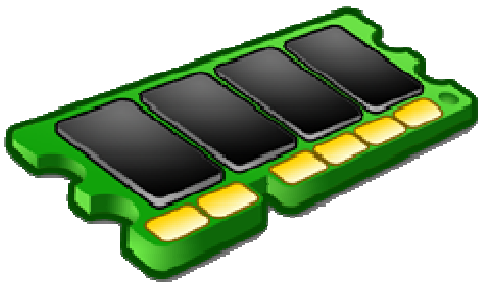
The Higher Education Academy

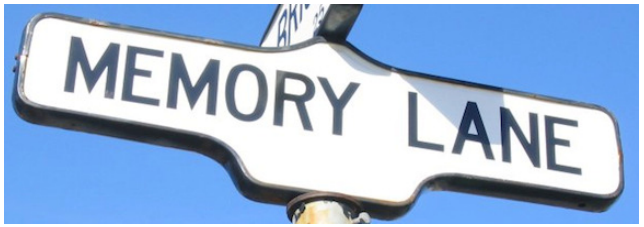
Outline

- Introduction
- Memory Forensics
- Write blockers, connectors, and readers
- Extracting information

Digital devices

- Primary storage
  - Volatile memory (RAM)
- Secondary storage
  - Hard drives
- Other classifications
  - Mobile devices
  - Tracking devices
  - Storage devices
  - …

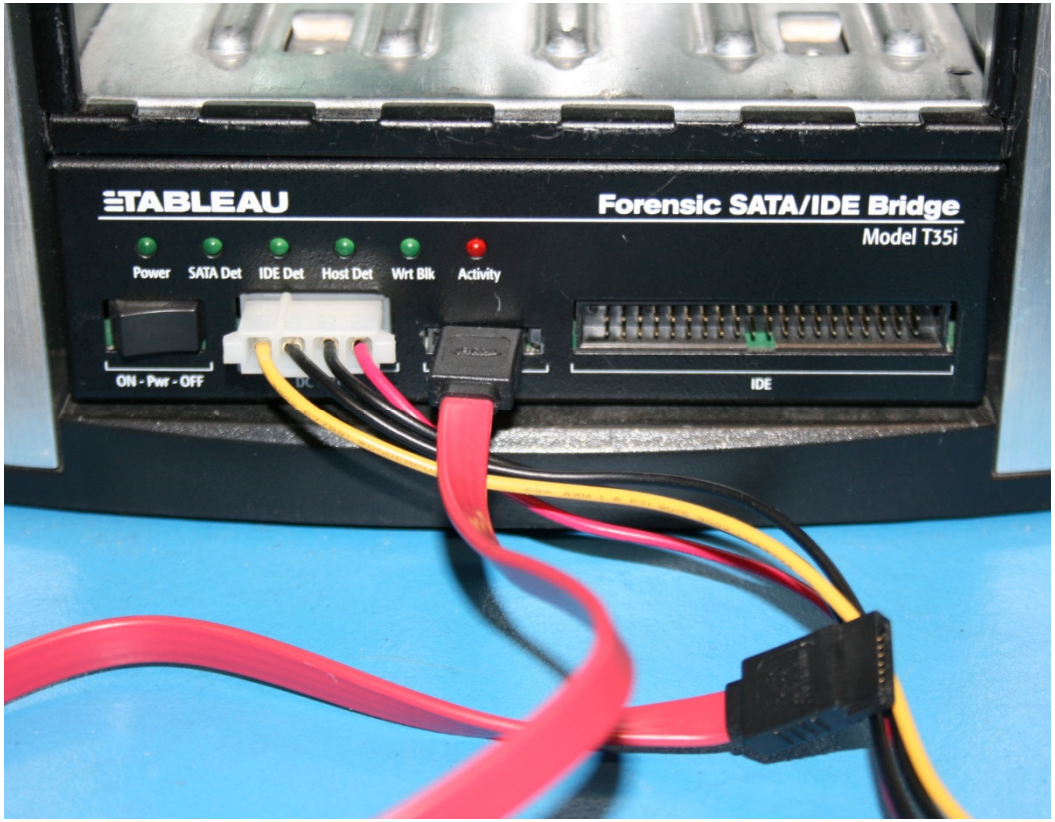




Memory Forensics

- Extracting data/information from different kind of digital memories
- Write-blockers are the absolute necessity
  - Hardware-based: Classical
  - Software-based: Contemporary
- Readers for these memory blocks
- Connectors to fetch data and provide power supply

R1: Write-blockers



R1: Write-blockers

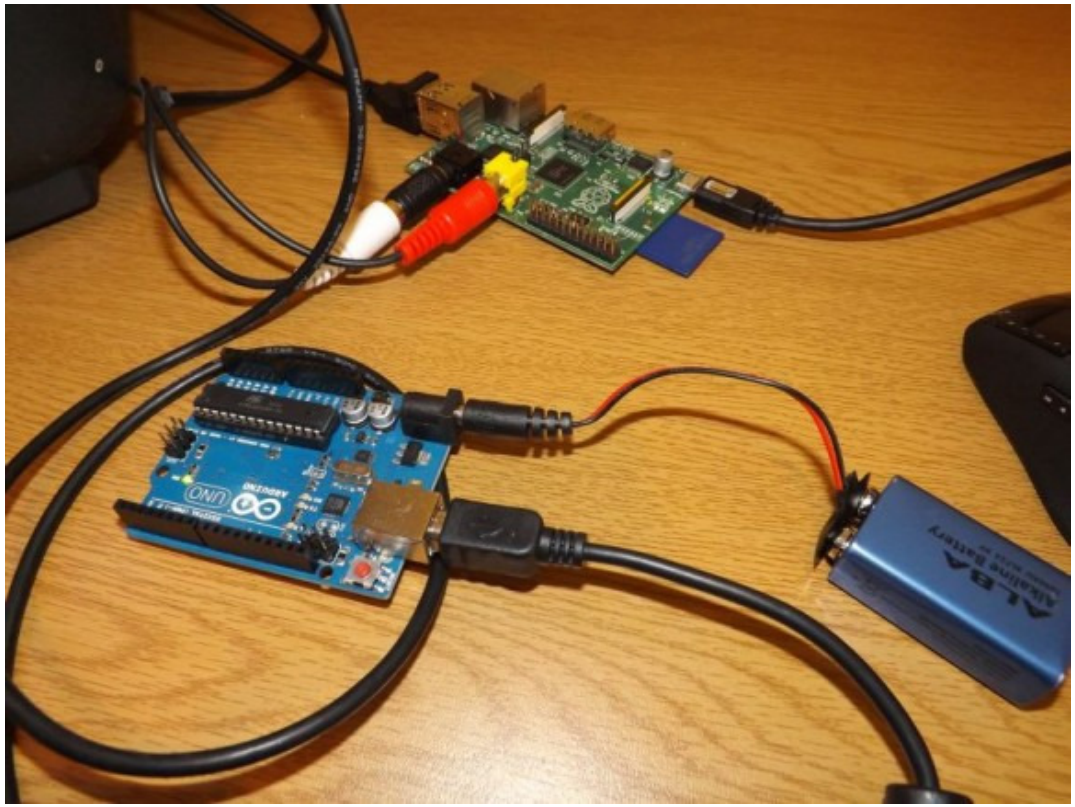
R1: Write-blockers

R1: Write-blockers

R2: Readers & Connectors

R2: Readers & Connectors

DIY Solutions!



NTFS Boot Sector

```
000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 02 00 00  ëR□NTFS    •••••
016 00 00 00 00 F8 00 00 3F 00 40 00 3F 00 00 00     •••••ø••?•@•?•••
032 00 00 00 00 80 00 80 00 00 EE 1F 00 00 00 00 00  ••••□•□••î••••••
048 55 52 05 00 00 00 00 00 80 FB 07 00 00 00 00 00  UR••••••□û••••••
064 01 00 00 00 04 00 00 00 2D EB C5 70 F0 C5 70 42  ••••••••-ëÅpðÅpB
080 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB B8 C0 07  ••••ú3À□Ð¼•|û¸À•
096 8E D8 E8 16 00 B8 00 0D 8E C0 33 DB C6 06 0E 00  □Øè••¸•• □À3ÛÆ••
112 10 E8 53 00 68 00 0D 68 6A 02 CB 8A 16 24 00 B4  •èS•h• hj•Ë□•$•´
128 08 CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66  •Í•s•¹ÿÿ□ñf•¶Æ@f
144 0F B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F  •¶Ñ□â?÷â□ÍÀí•Af•
160 B7 C9 66 F7 E1 66 A3 20 00 C3 B4 41 BB AA 55 8A  •Éf÷áf£ •Ã´A»ªU□
176 16 24 00 CD 13 72 0F 81 FB 55 AA 75 09 F6 C1 01  •$•Í•r•□ûUªu •öÁ•
192 74 04 FE 06 14 00 C3 66 60 1E 06 66 A1 10 00 66  t•þ••••Ãf`••f¡••f
208 03 06 1C 00 66 3B 06 20 00 0F 82 3A 00 1E 66 6A  ••••f;• ••□:••fj
224 00 66 50 06 53 66 68 10 00 01 00 80 3E 14 00 00  •fP•Sfh••••□>•••
240 0F 85 0C 00 E8 B3 FF 80 3E 14 00 00 0F 84 61 00  •|••è³ÿ□>••••□a•
256 B4 42 8A 16 24 00 16 1F 8B F4 CD 13 66 58 5B 07  ´B□•$•••□ôÍ•fX|•
272 66 58 66 58 1F EB 2D 66 33 D2 66 0F B7 0E 18 00  fXfX•ë-f3Òf••••••
288 66 F7 F1 FE C2 8A CA 66 8B D0 66 C1 EA 10 F7 36  f÷ñþÂ□Êf□Ðf Áê•÷6
304 1A 00 86 D6 8A 16 24 00 8A E8 C0 E4 06 0A CC B8  ••□Ö□•$•□èÀä• Ì¸
320 01 02 CD 13 0F 82 19 00 8C C0 05 20 00 8E C0 66  ••Í••□••□À• •□Àf
336 FF 06 10 00 FF 0E 0E 00 0F 85 6F FF 07 1F 66 61  ÿ•••ÿ••••|oÿ••fa
352 C3 A0 F8 01 E8 09 00 A0 FB 01 E8 03 00 FB EB FE  Ã ø•è • û•è••ûëþ
368 B4 01 8B F0 AC 3C 00 74 09 B4 0E BB 07 00 CD 10  ´•□ð¬<•t ´•»••Í•
384 EB F2 C3 0D 0A 41 20 64 69 73 6B 20 72 65 61 64  ëòÃ  A disk read
400 20 65 72 72 6F 72 20 6F 63 63 75 72 72 65 64 00   error occurred•
416 0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69   NTLDR is missi
432 6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F  ng•  NTLDR is co
448 6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73  mpressed•  Press
464 20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F   Ctrl+Alt+Del to
480 20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00   restart  ••••••
496 00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AA  ••••••••□ ³É••Uª
```

NTFS Boot Sector

• 0x00	3B	Jump Instruction
• 0x03	8B	OEM ID
• 0x0B	25B	BPB
• 0x24	48B	Extended BPB
• 0x54	426B	Bootstrap Code.
• 0x1FE	2B	End of Sector Marker

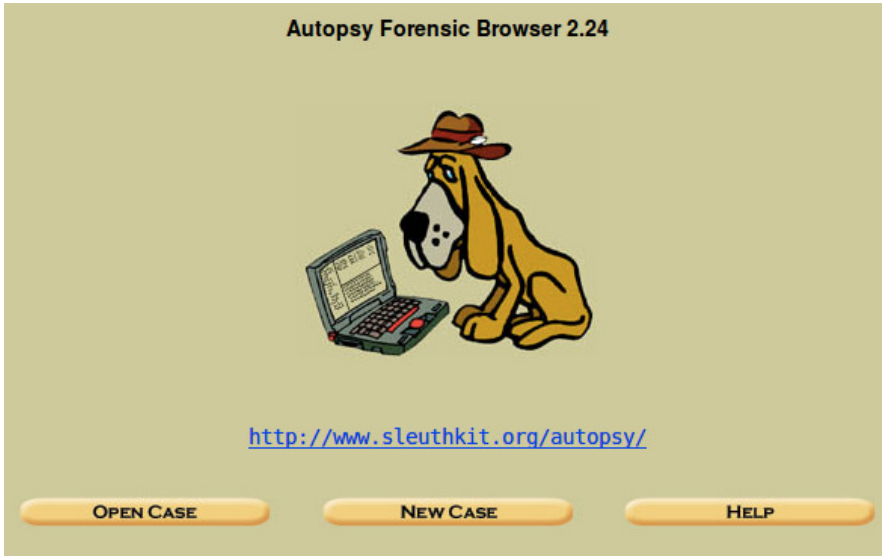
OEM ID: Original Equipment Manufacturer IDentification

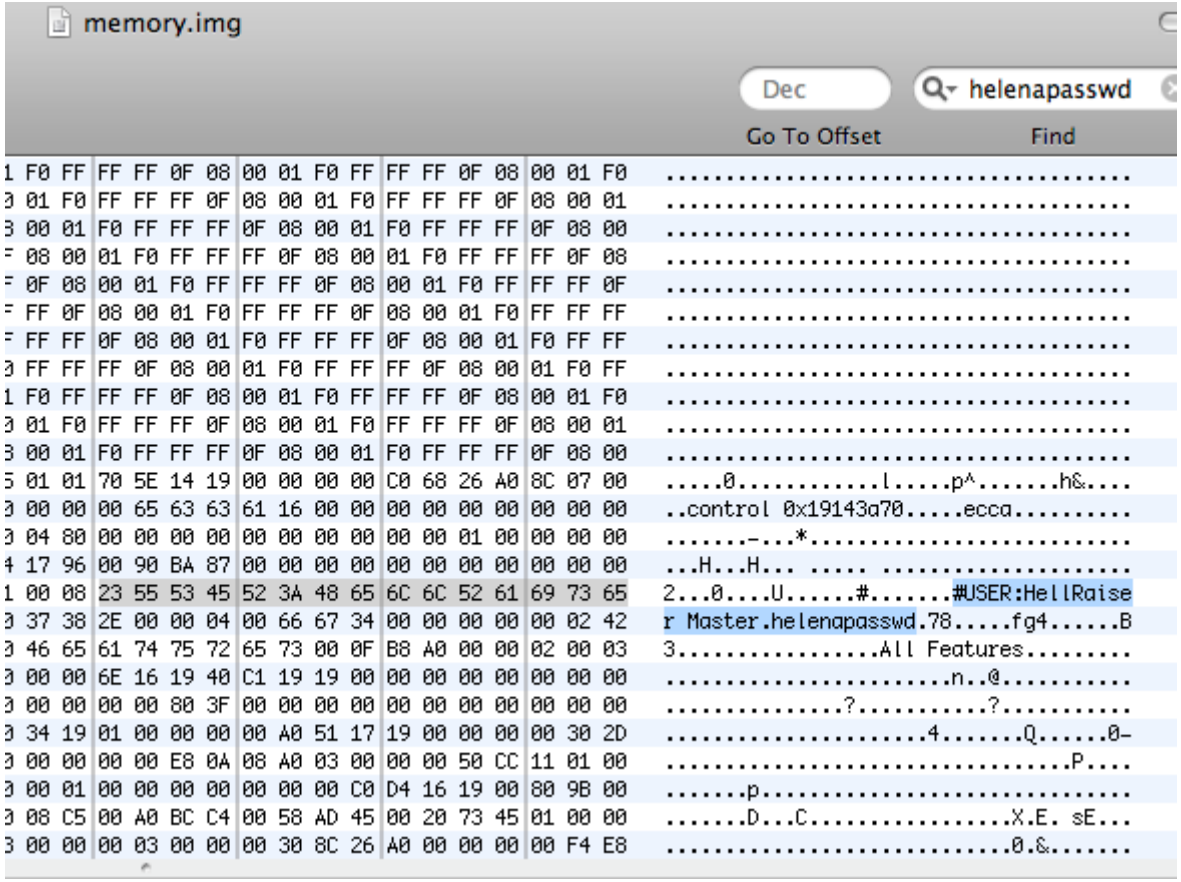
BPB: BIOS Parameter Block

NTSF Boot Sector

- 0x0B, Bytes per sector.
- 0x0D Sectors per Cluster
- 0x15 Media descriptor. F8: HD; F0: HD Floppy
- 0x28 Total sectors.
- 0x30 Logical cluster number for the MFT
- 0x38 Logical cluster number copy of the MFT
- 0x40 Clusters per MFT Record.
- 0x48 Volume serial

Sleuth Kit


Autopsy Forensic Browser 2.24
http://www.sleuthkit.org/autopsy/
OPEN CASE
NEW CASE
HELP

Penguin Sleuth

Suavetech 0xED Hex editor