


Byte Intelligence

null Dubai Monthly Meet, March 2018



Computer
forensics

Dr. Mousa Al Falayleh,
PhD

Byte Intelligence

Your Presenter

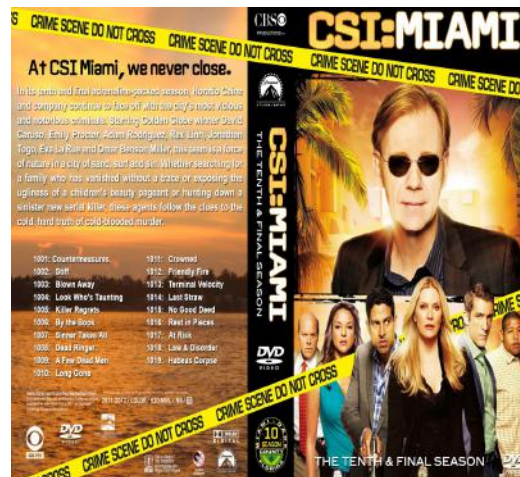
Dr. Mousa Falayleh
mousa@byte-intel.com
MD at Byte Intelligence DWC, www.byte-intel.com

Having over 22 years' experience in the information technology profession and holding doctorate degree in Information Security. Dr. Mousa build and manage IAT and AUE Digital Forensics Laboratories, develop master degree program in Enterprise Security and Assurance and have in-depth knowledge of Information Security theory and technique. He has worked closely with law enforcement in MENA region and with the INTERPOL on matters related to cybercrime investigations. In summary, Dr. Mousa is a passionate intercultural professional with a blend of experience in business, technology, research, public speaking and management in international and diverse settings.

Forensics Science

Forensic science is the application of science to law.

- Determine the reliability of evidence through a reliable scientific method..



Forensics Sciences

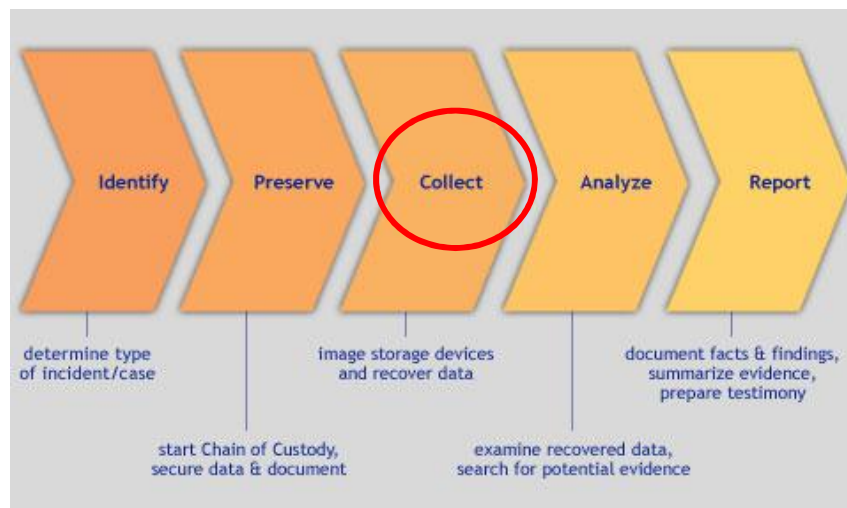


Digital Forensics

- A collection of specialized techniques, processes, and procedures used to preserve, extract, analyze, and present electronic evidence found in digital devices



Digital Forensics Process



Byte Intelligence

Targets & modern sources of evidence



The collage illustrates various modern sources of digital evidence. It includes a white smart electric car with 'smart electric drive' text, a white drone with red and yellow accents, a black smartwatch with a colorful app interface, a silver smart refrigerator with a digital display showing weather and calendar, and a large smart TV displaying a home screen with various app icons.

Byte Intelligence

Digital Forensics Activities

1. Computer Forensics: Static & Live Acquisition
2. Mobile Forensics: Logical & Physical Extraction
3. Network/Intrusion Forensics
4. Cloud Computing Forensics
5. Open Source Intelligence (OSINT) and Internet Investigation
6. Malware Analysis: Reverse Engineering

Who is using Digital Forensics

1. Police Forces
2. Military
3. Financial Fraud & Auditing
4. Threat Detection & Management
5. Incident Responders

DF Investigation Methodology



The Digital Crime Scene



Role of Hardware in Crime

Hardware as Evidence كدليل

- **Device linked to the crime**
- Computers
- External hard drives
- Thumb drives
- Cell phones
- Voice over IP phones
- Answering machines
- iPods
- Electronic game devices
- Digital video recorders (DVRs)
- Digital cameras
- PDAs
- GPSs
- Routers
- Switches
- Wireless access points
- Servers
- Fax machines
- Printers that buffer files
- Photo-copiers that buffer files
- Scanners that buffer files



Role of Data in Crime

Data as Evidence

- **Data linked to the crime**
- Documents
- Spreadsheets
- Databases
- Email
- Pictures and Videos
- Sound and music
- Chats and Tweets
- Maps
- Mobile data
 - Text messages
 - Multimedia messages
 - Contacts
 - Pictures, etc.
- Browser data
 - History
 - Cache
 - Cookies
- Social Media sites
- Operating System Artifacts
 - Link files
 - Log files
 - Deleted Files



Identifying Devices

✓ Disguised or Hidden Devices



Evidence Preservation

Running Computers

- *When in doubt, pull the plug!*



Running Cell Phones:

- *If off, leave it off*
- *If on, leave it on but protect with a Faraday Bag!*



RAM Acquisition



What is RAM?

- *Random Access Memory*

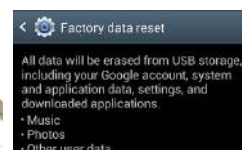
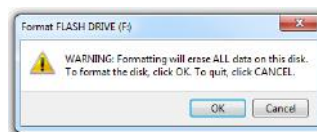
Why would RAM artifacts be important?

- *It's a snapshot of the current state of the system*
- *Contains loaded applications and data*
 - Text, pictures, etc.; Active Malware
- *May show network and Internet connections*
- *May contain passwords*

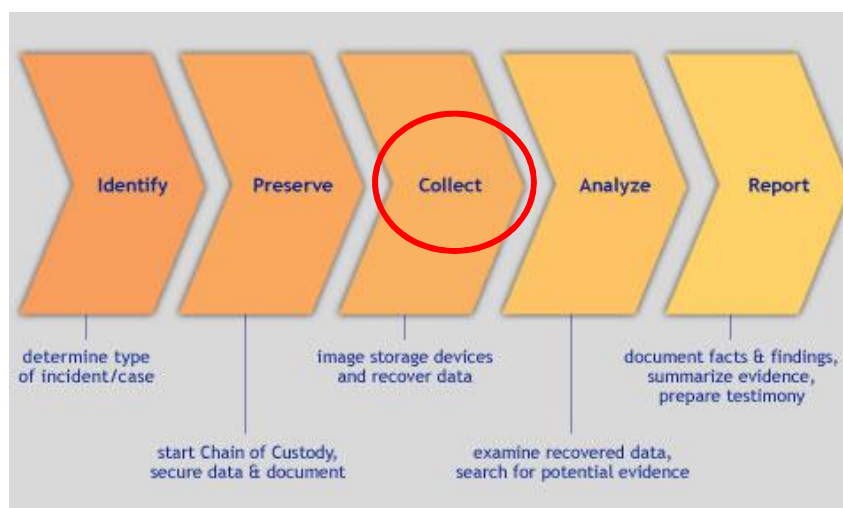
Getting Control at the crime scene

➤ Check for Destructive Activities

- ✓ *Drive Formatting/Wiping*
- ✓ *Mobile Device Resetting/Destruction*

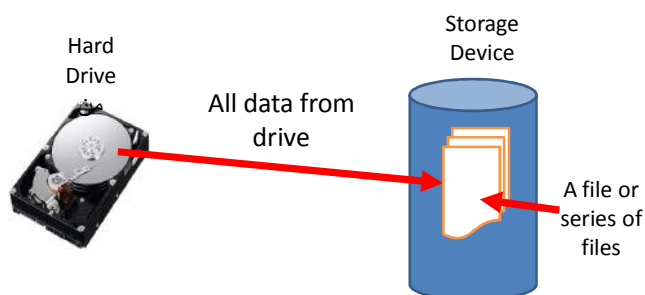


Digital Forensics Process



Evidence Acquisition

- **Forensic Imaging** is the process of copying the data from a suspect device to a file or set of files on another device.
- **Forensic cloning** is the process of 'cloning' one device to another device.



Write Blockers

Byte Intelligence

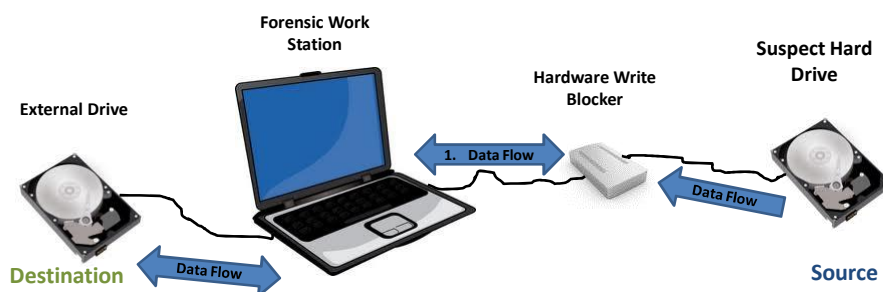
- **Hardware or software device or application**
- **Allow forensic acquisition of data without alteration**
- **Forensic imaging is a recognized international court approved process**



Imaging with a write blocker:

External Drive as Destination

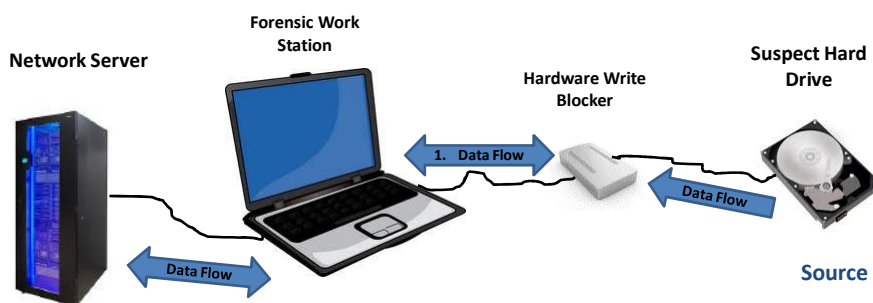
- *Forensic image taken from 'suspect' drive through forensic workstation to external media*

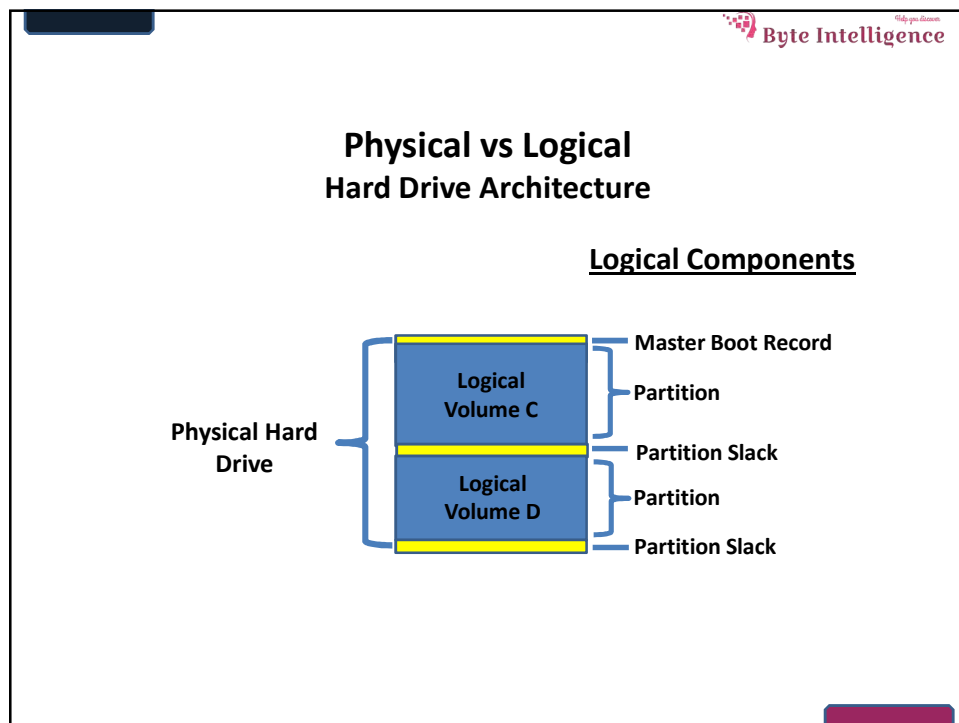
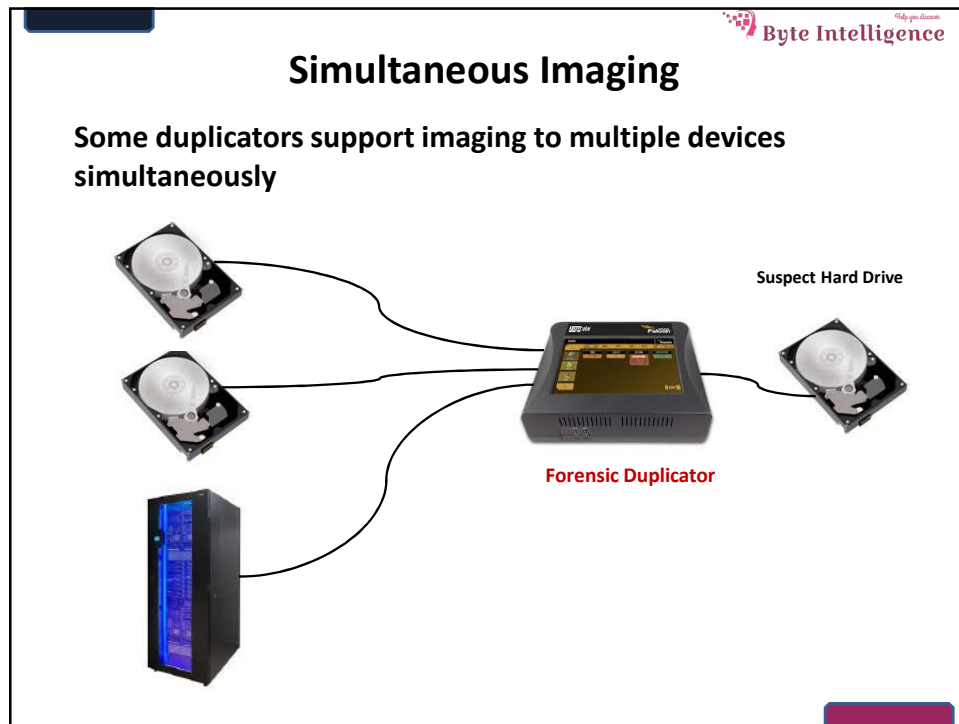


Imaging with a Write Blocker:

Network as Destination

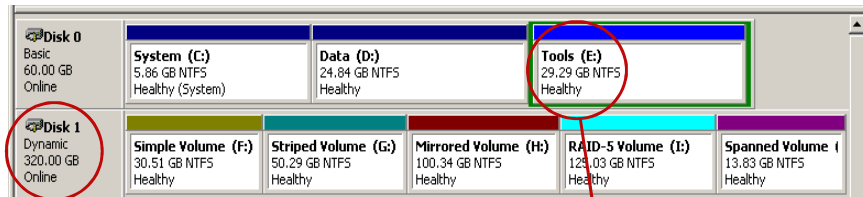
- *Forensic image taken from 'suspect' drive through forensic workstation to network storage*





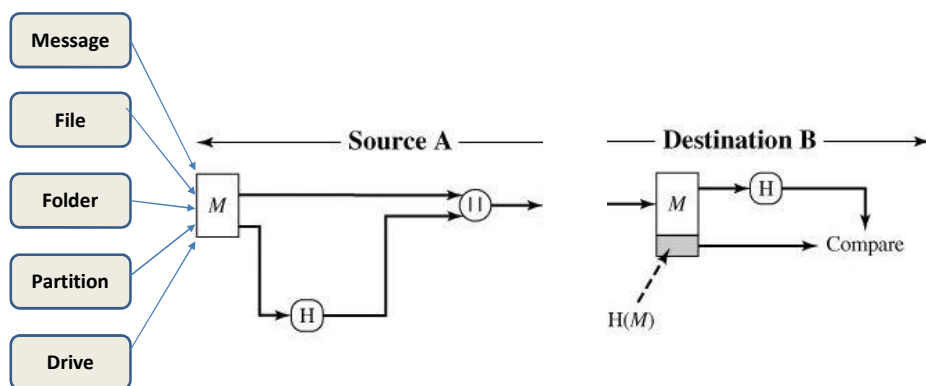
Disk Partitions

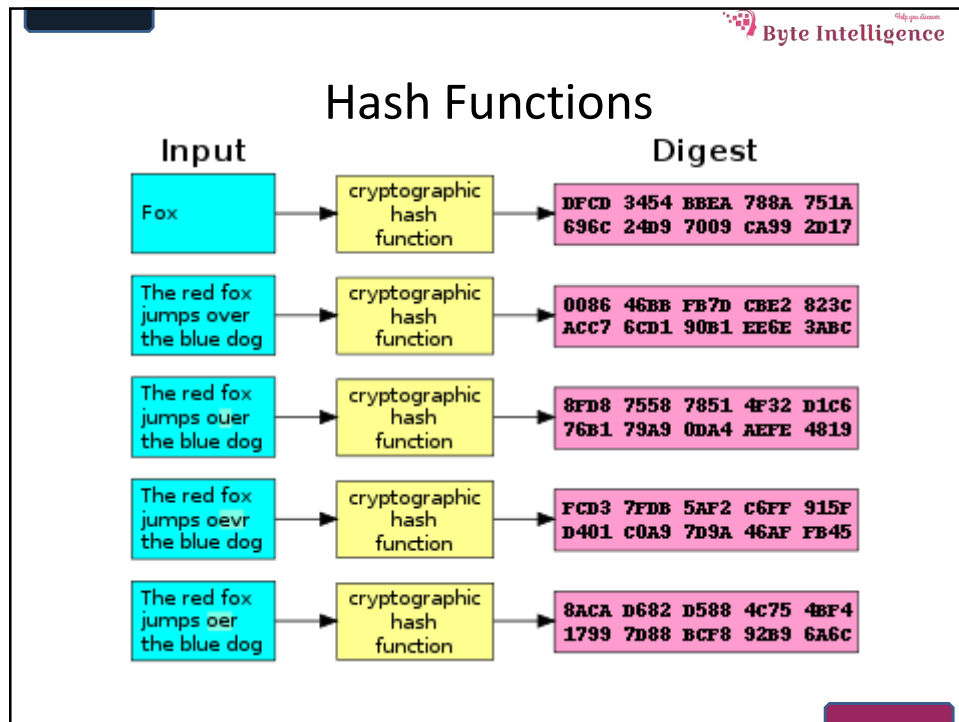
Windows Disk Management Utility (diskmgmt.exe)



- Physical Drive
- Complete Actual
- Logical Drive
- Partition
- Physical Drive may contain one or more of the Logical drives where one of them is the primary partition.

Hash Functions





Byte Intelligence

Hashing Algorithms

- **The Message-Digest algorithm 5 (MD5):**
 - MD5 hash value size is:

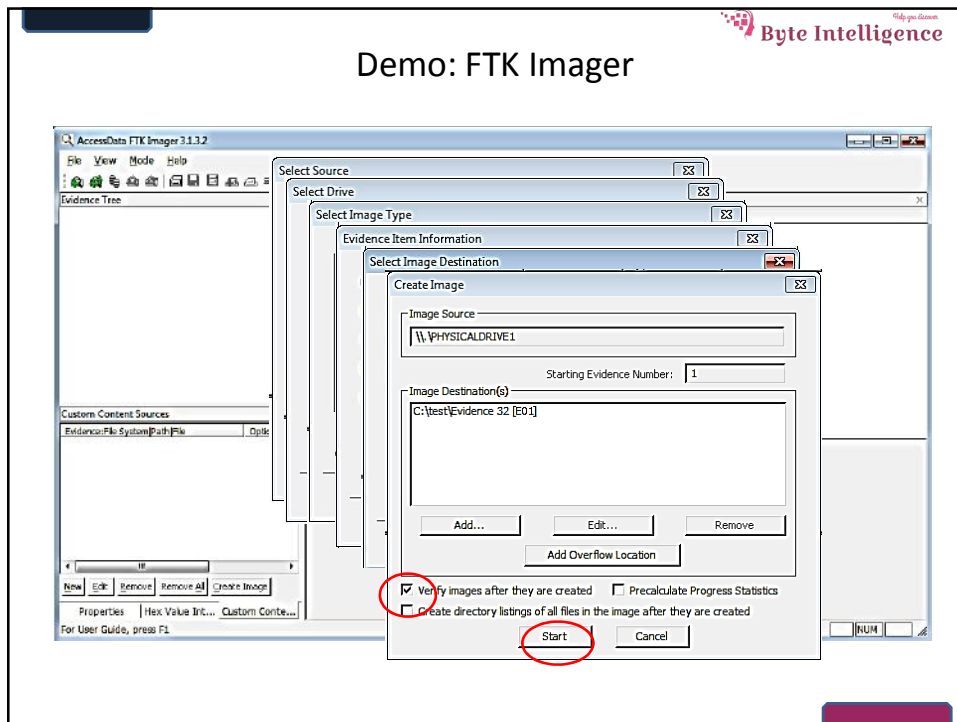
128-bit = 16-byte = 32 hexadecimal digits
 - Example: **9e107d9d372bb6826bd81d3542a419d6**
- **SHA-1 (Secure Hash Algorithm):**
 - SHA-1 hash value size is:

160-bit = 20-byte = 40 hexadecimal digits
 - Example:

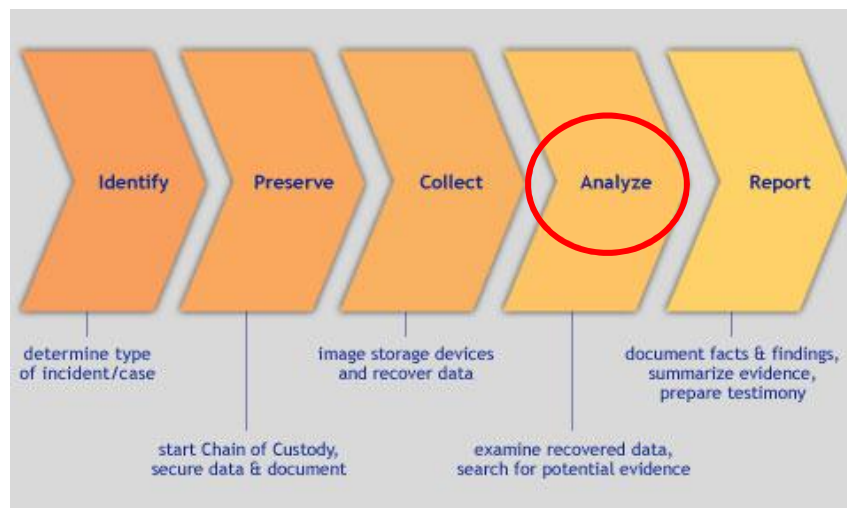
da39a3ee5e6b4b0d3255bfef95601890afd80709

2
8

Demo: FTK Imager



Digital Forensics Process



Analyzing Computer-Based Evidence



Forensics Workstations

Byte Intelligence


- Typically come with fast, built-in Write Blockers

Portable
Forensics
Workstation




Fixed
Forensics
Workstation






Computer Numbering Conventions

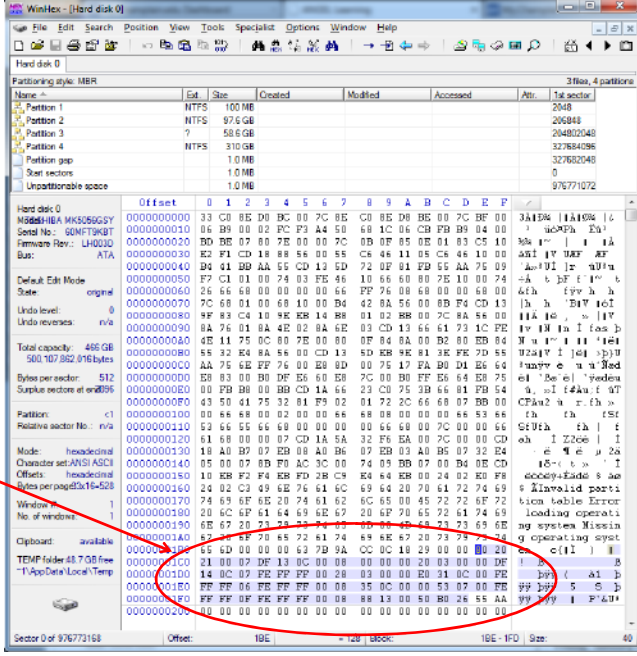


It's fundamentally all Zeros and ones!

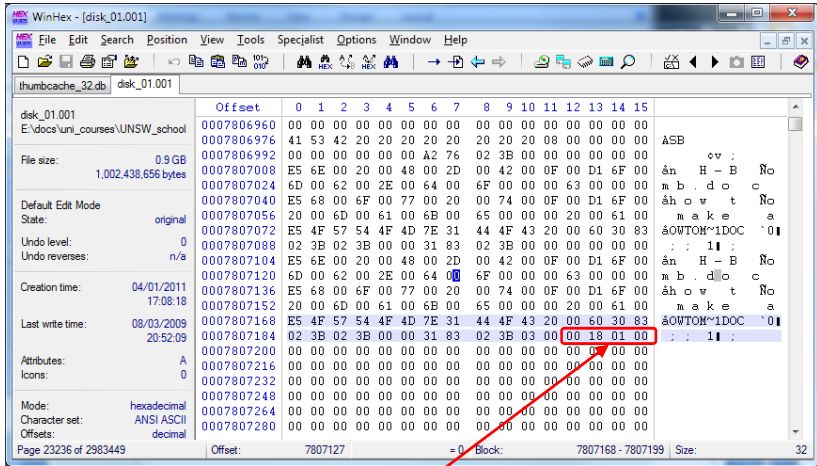


Why do we care?

Partition tables



Byte Intelligence



WinHex - [disk_01.001]

File size: 0.9 GB
1,002,438,656 bytes

Creation time: 04/01/2011 17:08:18
Last write time: 08/03/2009 20:52:09

Attributes: A
Icons: 0

Mode: hexadecimal
Character set: ANSI ASCII
Offsets: decimal

Page 23236 of 2983449

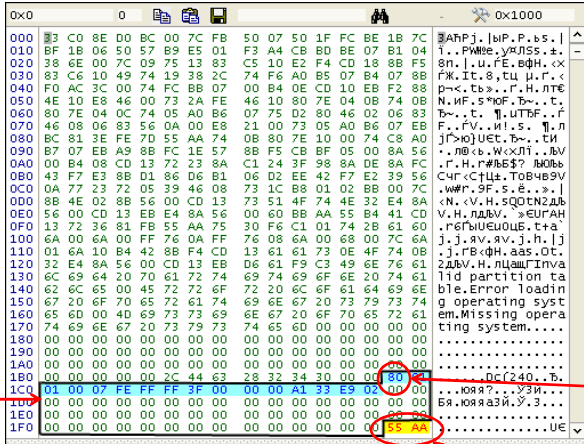
Offset: 7807127 = 0 Block: 7807168 - 7807199 Size: 32

File size in Hex in Little Endian - 00 18 01 00

Byte Intelligence

Demo: Hex Viewers

MBR 'Hex' View, File Signature Analysis



0x0 0 0x1000

000 3 C0 8E 0D BC 00 7C FB 50 07 50 1F FC BE 1B 7C 3 ARPJ. [WP.P.b.s.]

010 BF 1B 06 50 57 B9 E5 01 F3 A4 CB BD BE 07 B1 04 1..PWise,ykLSS.z.

020 38 6E 00 7C 09 75 13 83 C5 10 E2 F4 CD 18 8B F5 8n. |.u.FE.0FH.cX

030 83 C6 10 49 74 19 38 2C 74 F6 A0 B5 07 B4 07 8B Fж. It.8,ц |.r.<

040 F0 AC 3C 00 74 FC BB 07 00 B4 0E CD 10 EB F2 8B p<.c.b>..f.H.лtE

050 4E 10 E8 46 00 73 2A FE 46 10 80 7E 04 0B 74 0B N.WF.5'nof.b>..t.

060 80 7E 04 0C 74 05 A0 B6 07 75 D2 80 46 02 06 83 b>..t. |.UTb>..f

070 46 08 06 83 56 0A 00 E8 21 00 73 05 A0 B6 07 EB F..fv..и.1.s. |.л

080 BC 81 3E FE 7D 55 AA 74 08 80 7E 10 00 74 C8 A0 j|>no|UET.b>..ц

090 E7 07 EB A9 8B FC 1E 57 8B F5 CB BF 05 00 8A 56 ..лb>.wXLT..лb>

0A0 00 B4 08 CD 13 72 23 8A C1 24 3F 98 8A DE 8A FC .f.H.r'w|b>? NOOb

0B0 43 F7 E3 8B D1 86 D6 B1 06 D2 EE 42 F7 E2 39 56 Cчr<Ctц. TOB4B9V

0C0 0A 77 23 72 05 39 46 08 73 1C B8 01 02 BB 00 7C .wMf.9F.s.e..>.|

0D0 8B 4E 02 8B 56 00 CD 13 73 51 4F 74 4E 32 E4 8A .N..v.H.sQOT2Ab

0E0 56 00 CD 13 EB E4 8A 56 00 60 BB AA 55 B4 41 CD V.H.лb>. >EURLH

0F0 13 72 36 81 FB 55 AA 75 30 F6 C1 01 74 2B 61 60 .p.fy|Ue|Ue.t+a

100 6A 00 6A 00 FF 76 0A FF 76 08 6A 00 68 00 7C 6A j.j.yv.yv.j.h.|j

110 01 6A 10 B4 42 8B F4 CD 13 61 61 73 0E 4F 74 0B .j.rfBqH.aas.Oc.

120 32 E4 8A 56 00 CD 13 EB 06 61 F9 C3 49 6E 76 61 2AbV.H.лb>лTnVa

130 6C 69 64 20 70 61 72 74 69 74 69 6F 6E 20 74 61 lld partition ta

140 62 6C 65 00 45 72 72 6F 72 20 6C 6F 61 64 69 6E ble.Error loadin

150 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74 g operating syst

160 65 6D 00 40 69 73 73 69 6E 67 20 6F 70 65 72 61 em.Missing opera

170 74 69 6E 67 20 73 73 73 74 65 6D 00 00 00 00 ting system....

180 00 00 00 00 00 00 00 00 00 00 00 00 00 00
190 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1C0 01 00 07 FE FF FF 3F 00 00 00 A1 33 E9 02 00 00 ..>.kяя7..y3H...
1D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..>.kяяя3H..y.3...
1E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AAUE

Partition Table

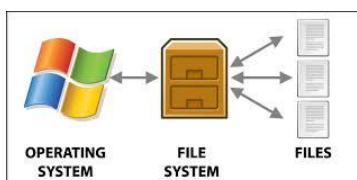
One Sector 512 Byte

Active Partition Marker

End of File Marker

File Systems vs Hard Drives

- **Hard Drives**
 - The mechanical bits
 - Storage Configurations
 - *Tracks, Cylinders, Clusters, Sectors, etc.*
 - *Partitions and Formats*
- **File Systems**
 - A system to organize, track and hold files
 - The File System must be recognized and supported by the Operating System running on the system



The Analysis Phase

- Many cases will require a more thorough analysis
- ✓ **Computers:**
 - Load the image file(s) with an approved Forensic Tool
 - *EnCase, FTK, etc.*
 - Configure the tool according to the case needs
 - *Use 'Known File Filters' to eliminate benign files, set carving conditions, etc.*
 - Initiate the tool's case processing/indexing feature
 - *A large file set could take hours/days to complete*
 - Monitor the tool's process, restart if necessary, etc.

Demo: Case Analysis with FTK

The Overview Tab groups files by type.

- Documents
- Spreadsheets
- Pictures
- Multimedia
- Etc.

Very useful for certain types of investigations

