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

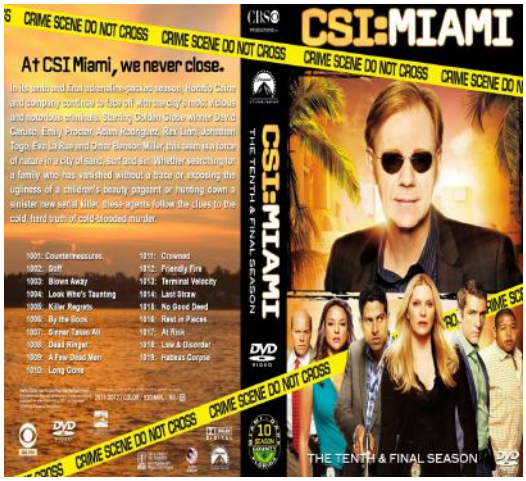
Having over 22 years' experience in the information technology profession and holding doctorate degree in Information Security. Dr. Mousa build and manage IAT and AUE Digital Forensics Laboratories, develop master degree program in Enterprise Security and Assurance and have in-depth knowledge of Information 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.

Byte Intelligence

Forensics Science

Forensic science is the application of science to law.

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



Byte Intelligence

Forensics Sciences

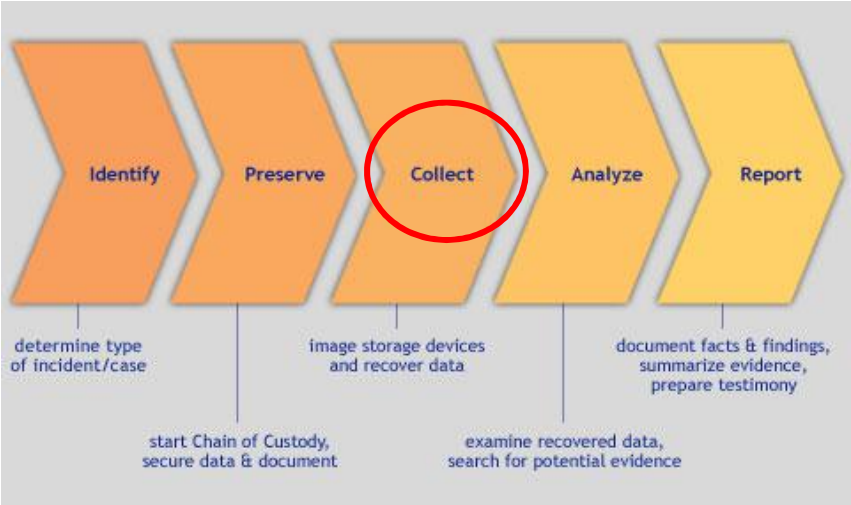
Byte Intelligence

Digital Forensics

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

Byte Intelligence

Digital Forensics Process



Byte Intelligence

Targets & modern sources of evidence

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

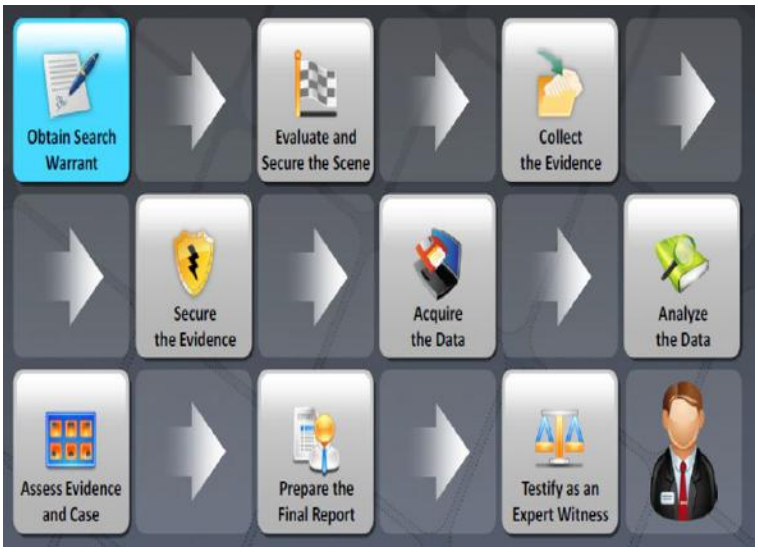
Byte Intelligence

Who is using Digital Forensics

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

Byte Intelligence

DF Investigation Methodology



Byte Intelligence

The Digital Crime Scene

Byte Intelligence

Role of Hardware in Crime

Hardware as Evidence كدليل

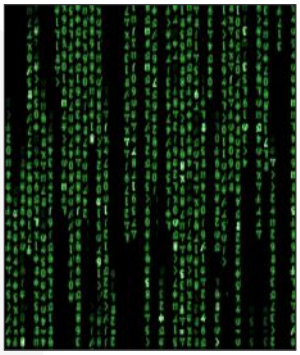
- **Device linked to the crime**
- Computers
- External hard drives
- Thumb drives
- Cell phones
- Voice over IP phones
- Answering machines
- iPods
- Electronic game devices
- Digital video recorders (Tivos)
- Digital cameras
- PDAs
- GPSs
- Routers
- Switches
- Wireless access points
- Servers
- Fax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

Byte Intelligence

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



Byte Intelligence

Identifying Devices

✓ **Disguised or Hidden Devices**

Evidence Preservation

Running Computers

- *hen 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

Byte Intelligence

What is RAM?

- *Random Access Memory*

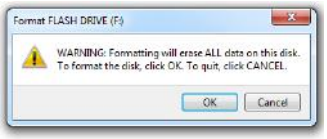
Why would RAM artifacts be important?

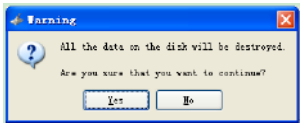
- *It's a snapshot of the current state of the system*
- *Contains loaded applications and data*
  - Text, pictures, etc.; Active Malware
- *May show network and Internet connections*
- *May contain passwords*

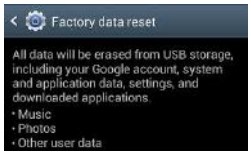
Byte Intelligence

Getting Control at the crime scene

- **Check for Destructive Activities**
  - ✓ ***Drive Formatting/Wiping***
  - ✓ ***Mobile Device Resetting/Destruction***

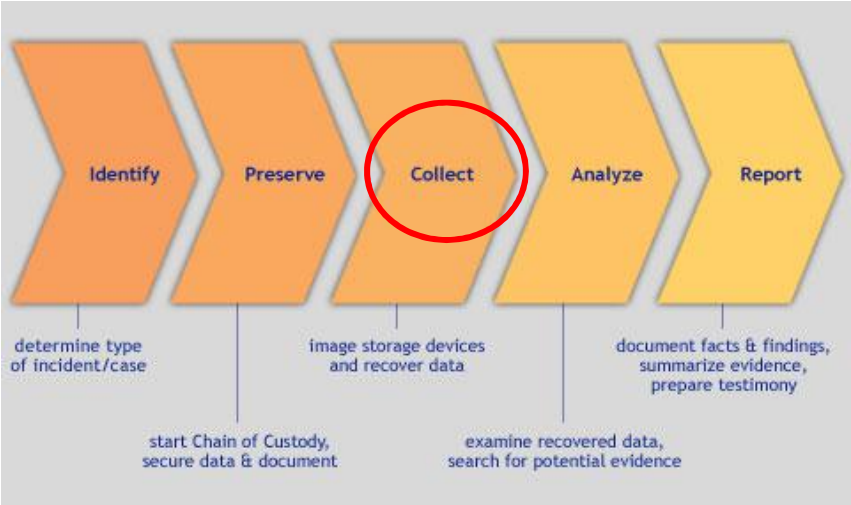






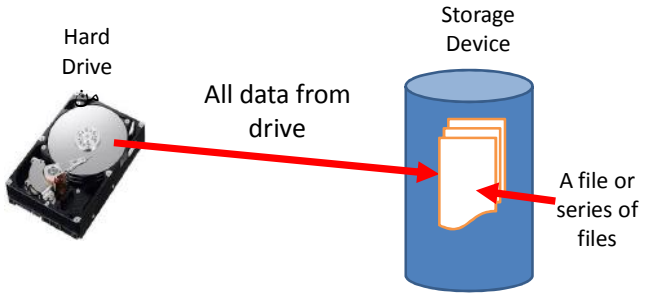
Byte Intelligence

Digital Forensics Process



Evidence Acquisition

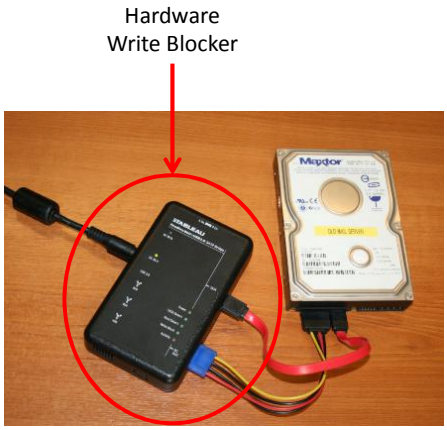
- **Forensic Imaging is the process of copying the data from a suspect device to a file or set of files on another device.**
- **Forensic cloning is the process of 'cloning' one device to another device.**



Byte Intelligence

Write Blockers

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

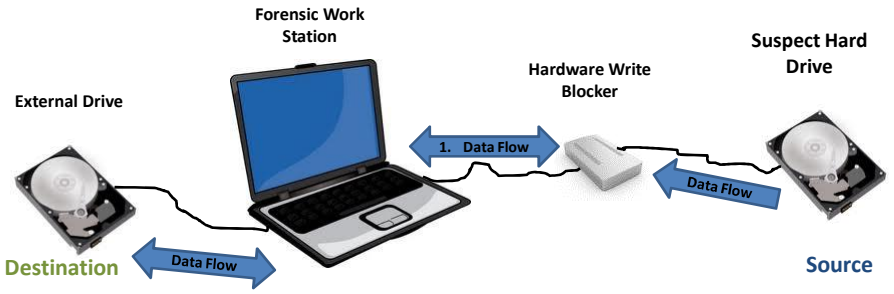


Byte Intelligence

Imaging with a write blocker:

External Drive as Destination

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

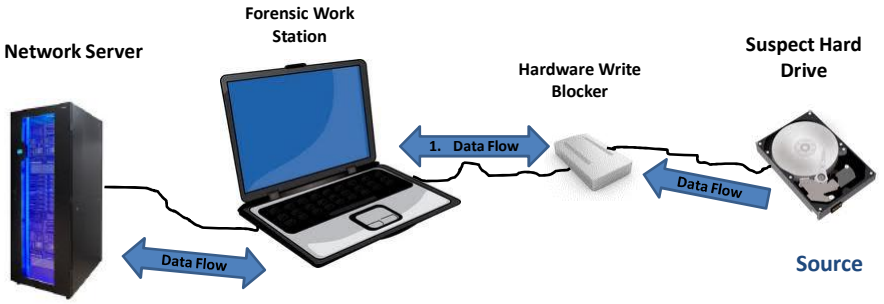


Byte Intelligence

Imaging with a Write Blocker:

Network as Destination

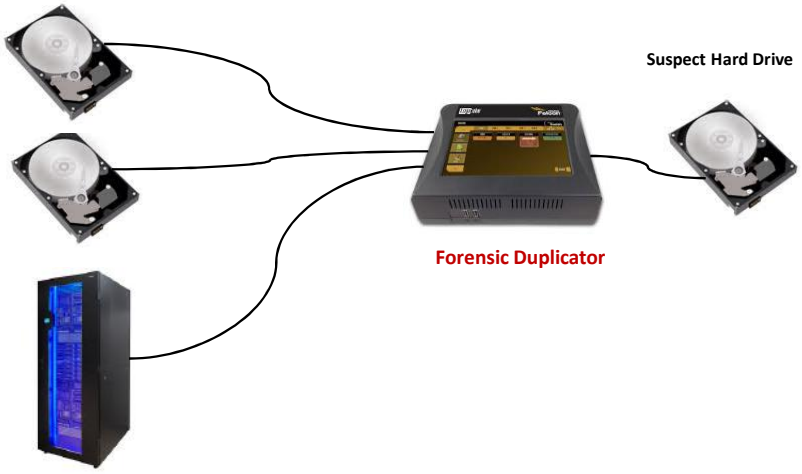
- *Forensic image taken from 'suspect' drive through forensic workstation to network storage*



Byte Intelligence

Simultaneous Imaging

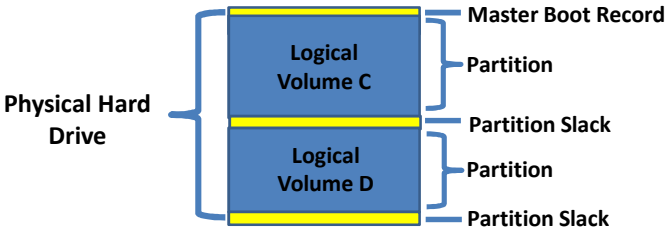
Some duplicators support imaging to multiple devices simultaneously



Byte Intelligence

Physical vs Logical
Hard Drive Architecture

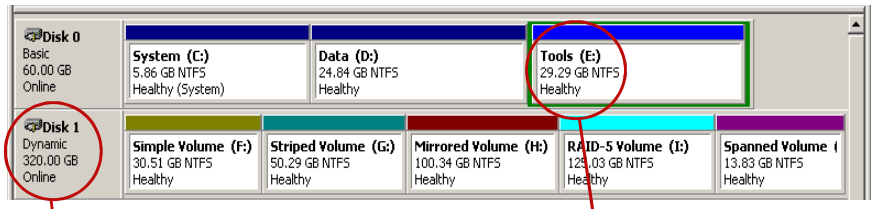
Logical Components



Byte Intelligence

Disk Partitions

Windows Disk Management Utility (diskmgmt.exe)



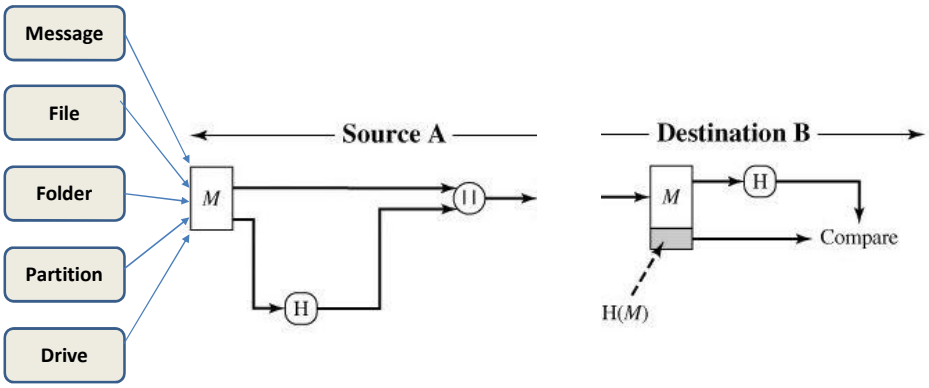
- Physical Drive
- Complete Actual

- Logical Drive
- Partition

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

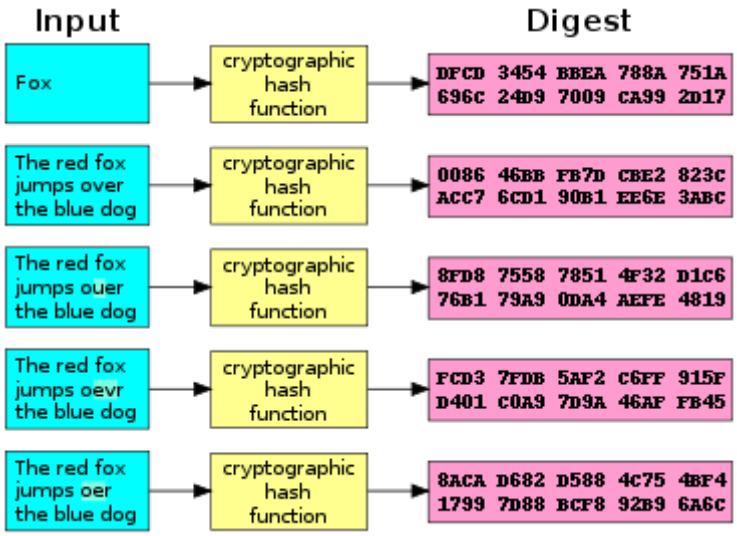
Byte Intelligence

Hash Functions



Byte Intelligence

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

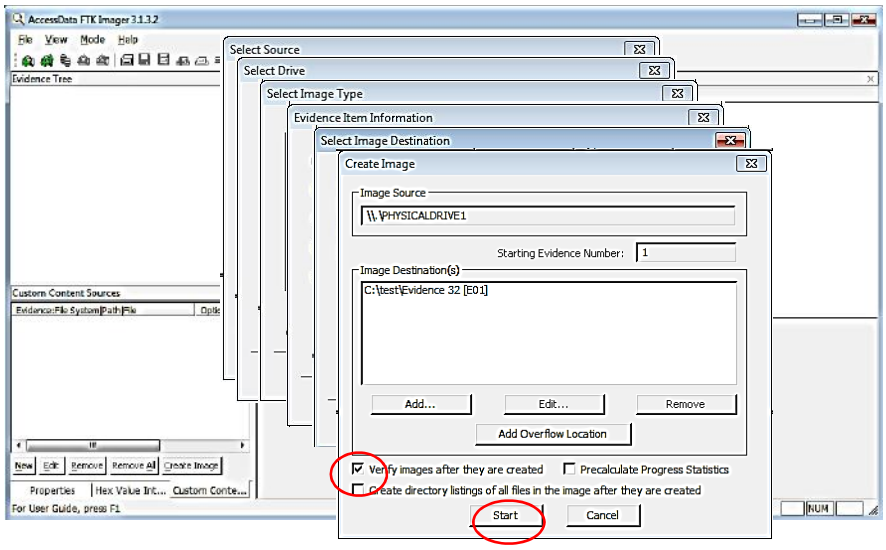
- SHA-1 (Secure Hash Algorithm):
- SHA-1 hash value size is:
  160-bit =20-byte = 40 hexadecimal digits

Example:
da39a3ee5e6b4b0d3255bfef95601890afd80709

28

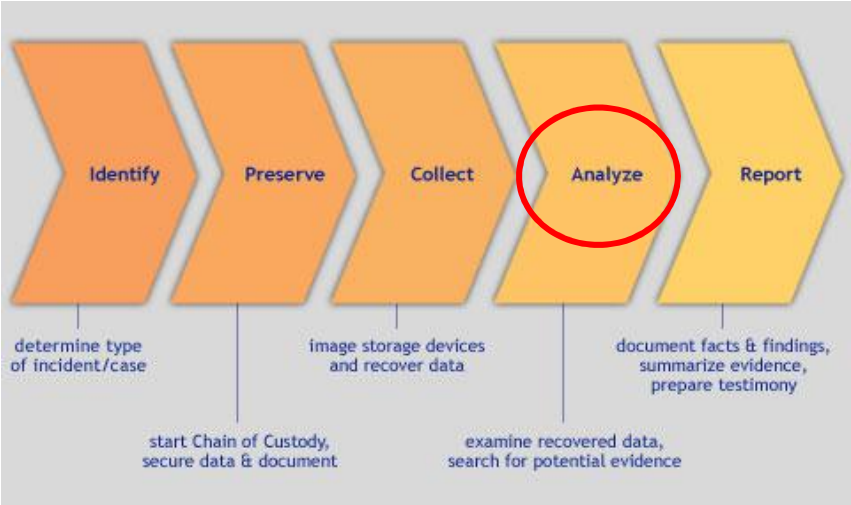
Byte Intelligence

Demo: FTK Imager



Byte Intelligence

Digital Forensics Process



Analyzing Computer-Based Evidence

Forensics Workstations

Byte Intelligence

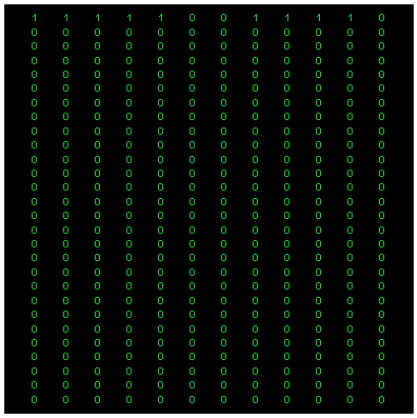
- **Typically come with fast, built-in Write Blockers**

Portable Forensics Workstation

Fixed Forensics Workstation

Byte Intelligence

Computer Numbering Conventions

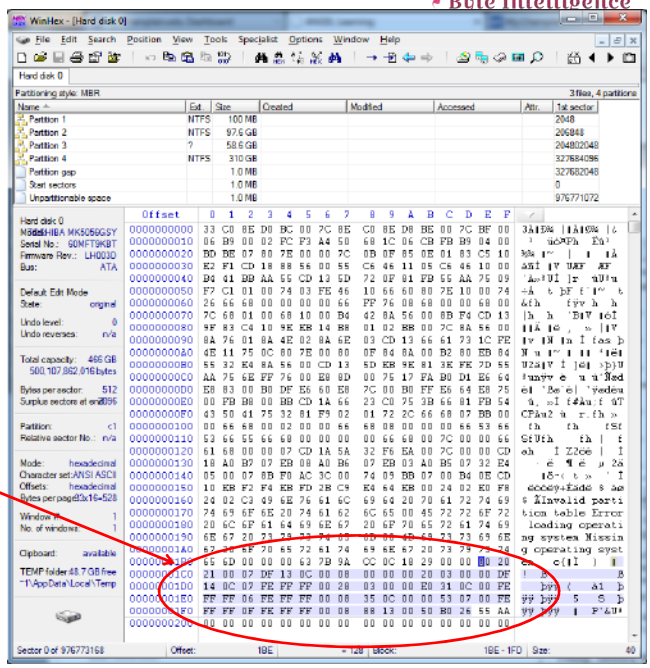


It's fundamentally all Zeros and ones!

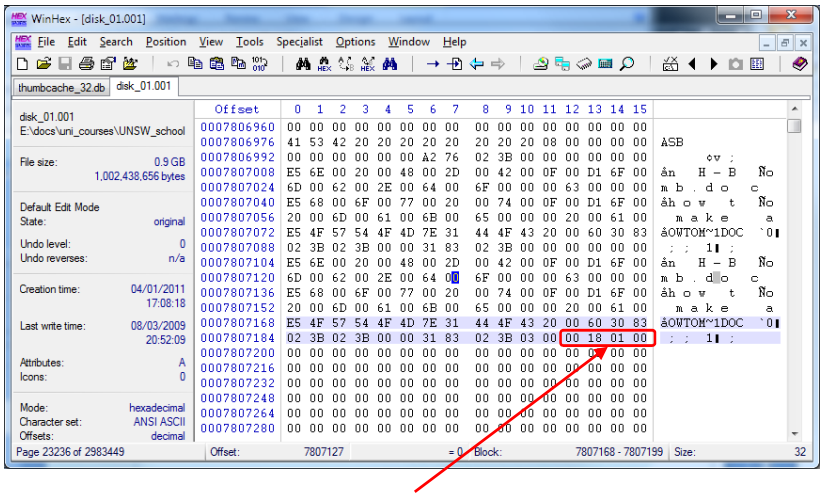
Byte Intelligence

Why do we care?

Partition tables



Byte Intelligence



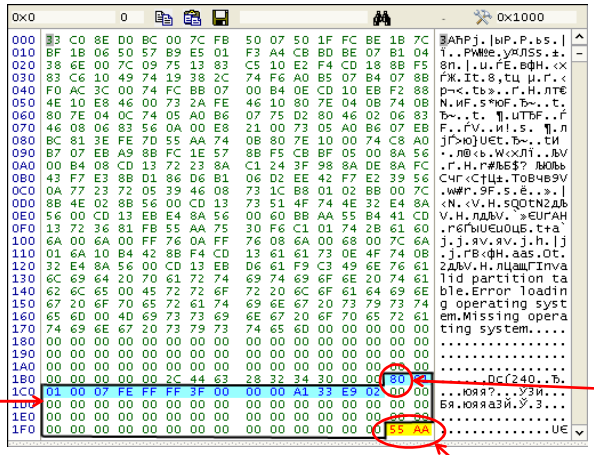
File size in Hex in Little Endian - **00 18 01 00**

Byte Intelligence

Demo: Hex Viewers

MBR 'Hex' View,

File Signature Analysis



One Sector 512 Byte

Active Partition Marker

Partition Table

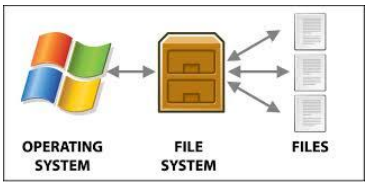
End of File Marker

Byte Intelligence

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.

Byte Intelligence

Demo: Case Analysis with FTK

The Overview Tab groups files by type.

- Documents
- Spreadsheets
- Pictures
- Multimedia
- Etc.

Very useful for certain types of investigations