* Digital Forensics
  + Investigative process of digital materials
* File Carving
  + Reconstructing files without metadata
  + Use magic numbers
* File signature analysis
* Memory
  + Volatile
    - Not saved on power-off
    - RAM
  + Non-volatile
    - Stays without power
    - Hard drive
* File Systems
  + Windows
    - NTFS
  + Apple
    - HFS+
  + Linux
    - EXT
* HPA
  + Host protected Area
  + Space on HD reserved for restoration
* Allocated space
  + Area where data is being stored
* Slack space
  + Unused area within allocated space
  + Data smaller than minimum block size
* Cluster
  + Defined by OS and File system
  + Can be as small as 1 sector
* Sector
  + Smallest physical unit on HD (hardware defined)
  + Usually 512 bytes
* Computing environment
  + Stand-alone
    - 1 computer
  + Network
  + Mainframe
  + Cloud
* Cybercrime
  + Unlawful activity done with digital tools
  + Malware, DDOS, phishing
  + Honeypot
    - Fake system easy to access, used to track anyone who is trying to get into a network
* Cyber Law
  + Criminal Charge
    - Brought by government
    - jail/fine
  + Civil Charge
    - Brought by individual or company
* Search Authority
* 4th Amendment
  + No unlawful search and seizure from the government
  + Not private search
* Expectation of privacy
* ECPA
  + Electronic communication and privacy act
  + Wire Act
    - Wiretapping phones and other
  + Stored communication act
    - Email can’t be used without warrant after 180 days
  + Pen Register/ Trap and trace statue
    - Tracking info, path history
* Warrant exception
  + Consent
* Warrant
  + What they are looking for
  + Specific location
* E-Discovery
  + Process of collecting digital stuff
* Expert Witness
  + Explain to jury all the digital stuff
* Evidence
  + Admissible
    - Legally obtained
  + Credible
    - Chain of custody
  + Persuasive
    - Related to the crime
  + 2 Categories
    - Inculpatory
      * supports
    - Exculpatory
      * Refutes
* Federal rules of evidence
* Digital Evidence
  + 2 Types
    - User created
    - Computer/network created
      * Logs, metadata
  + Handling digital evidence
    - 4 steps
      * Identify
      * Collect, preserve
      * Analyze
      * Verify
  + Need documentation
    - Chain of custody
  + Duty to preserve evidence
    - Must keep integrity
* Order of volatility
  + Most volatile: CPU Cache
  + Least: archive (tape/CD)
* Bit-stream Image
  + Copy seized drive onto a drive written with all 0
  + Bit-by-bit mirror of drive
  + Need forensically Clean
    - Allocated and unallocated are both 0
    - Multiple passes
  + Write protection
    - Prevent source drive from changing
    - Hardware prefered
* Live/dead system analysis
  + Live - still running
  + Dead - not running
  + Live Evidence collection
    - Integrity check - use hash
* Procedure of digital forensics
  + 9 steps Abstract model
  + Pre-incidents preparation
  + Forensic readiness
  + Challenges
  + Live response
* Data Acquisition
  + Live
    - Limitation of live Acquisition
    - 2 ways
      * Local
      * Network
  + Dead
  + Error Handling
  + 2 options for copying
    - Disk
    - File
      * Image file
      * Raw File - only file
      * Embedded file - contains metadata, hash, date
* Authentication
  + 3 factors
    - Knowledge
    - Ownership
    - Adherence
  + Strength
  + 4 main types
    - Password
    - Certificate
    - e-token
    - Biometric
      * Physical
      * Behavioral
      * Benefits?
* Data Analysis
  + File System
  + Network
* Steganography
  + 4 types
    - Text
    - Image
    - Audio
    - tcp/ip
  + LSB
* Hash
  + What is it
  + How to use
  + What do you use it for
  + Give example
  + Collisions
    - How to handle
      * Separate chaining
      * Open addressing
        + Linear probing
        + Quadratic
* Cryptography
  + 2 types
    - Symmetric
      * Single key
    - Asymmetric
      * Public private
      * Diagram
  + DSA
    - 2 very large numbers
  + Hashing
    - 1 way encryption
* Disk drive
  + HDD vs SSd
  + Volume, partition
  + Image
  + Raid
* VM
  + Difficult to analyze
* File system
  + Atributes of file
  + FAT 16 limitations
    - 8 bytes
    - 3 bytes for extensions
    - 8.3 convention