Digital Forensics

- The use of specialized tools and techniques for preservation, analysis, recovery, and authentication of electronic data. Often involves:
  - reconstruction of computer usage,
  - recovery and examination of residual data,
  - authentication of data or explanation of technical features of data or computer usage.
- Procedures adhere to the standards of evidence so that digital evidence is admissible in a court of law.

Introduction to Digital Forensics

- Identification and Preservation
  - Identify media that may have evidence
  - Preserve it exactly as first seized or received
- Analysis and Review
  - Examine working copies of data using forensic tools
- Evaluation and Assessment
  - Working with the case agent to determine importance of data
- Reporting
  - Documenting evidence, chain of custody and procedures
- Court Presentation
  - Translating all of the work into layman's terms

Digital Evidence

- When is digital evidence used?
- Who uses digital evidence?
- Where can digital evidence be found?
- What evidence can be found?
- How can digital evidence be used?

- When is Digital Evidence Used?
  - hacking
  - fraud
  - child porn
  - defamation
  - immigration fraud
  - narcotics trafficking
  - credit card cloning
  - identity theft
  - software piracy
  - electoral law
  - embezzlement
  - perjury
  - forgery
  - murder
  - sexual harassment
  - data theft – industrial espionage
  - divorce
  - and more!
Digital Evidence

Where can digital evidence be found?
- Hard drives
- Floppy, Zip and Jazz disks
- CDs/DVDs
- Tapes
- Memory Cards and USB Sticks
- Printers and Fax Machines
- Digital cameras
- Cell Phones and Smart Phones
- iPods, MP3 players and PDAs
- DVRs and Gaming Consoles
- Networks
- Logs
- Intercepts/traces
- Just about everywhere!!!!!!!!

What evidence can be found?
- Files
  - Listed in standard directory search
  - Hidden files
  - Deleted files
  - Encrypted Files
  - Intentionally embedded (steganographic) files
- Email
  - Deleted email
- Certain Instant Messaging
- User Credentials
  - Login IDs / Usernames
  - Passwords
- Web Browsing Activity
  - Web sites visited
  - Searches performed
  - Cookies
- Logs
  - Network traces
  - Owners of servers
- Time!
- Image Originality - Real or CGI?

How Can Digital Evidence be Used?
- Related to Who - Criminal, Civil, Organizational
- Fourth Amendment
  - No "unreasonable" search and seizure
  - Computer data and network activity is private
  - Warrant (probable cause) required for government agents
- Rules of Evidence
  - Computer data is treated as document
  - Recent law - US Patriot Act
  - Easier access to public and private Internet activities
  - Easier to get warrant for digital evidence
- Department of Justice 2002 Guidelines:
  - "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"
  - Guidelines on how digital evidence must be seized
  - Copy, hash (fingerprint), chain of custody
  - Frye and Daubert tests of scientific admissibility
  - New Challenges
    - Image Originality - Real or CGI?