

Computer Forensics

- Discovery and recovery of digital evidence
 - Usually post facto
 - Sometimes real time
- Types of forensic investigations
 - Liturgical
 - Going to court
 - Crimes, etc.
 - Non-Liturgical
 - Administrative adjudication
 - Industry

Purpose

- Prove or disprove criminal activity
- Prove or disprove policy violation
- Prove or disprove malicious behavior to or by the computer/user

If the evidence is there, the case is yours to lose with very little effort.

Dual use technology

- All tools can be used to commit crime
- All procedures can be used to hide crime

Business Issues

- No interruption of business
- Know the policies of the business
- Sensitive to the business costs during an investigation

Privacy Issues

- Rights of the suspect
- Liabilities of the investigator
- Public versus private storage of information
- Expectation of privacy

Evidence

- Forensics is all about evidence.
- Something that tends to prove or disprove the existence of an alleged fact.

Evidence

- Admissible
 - must be legally obtained and relevant
- Reliable
 - has not been tainted (changed) since acquisition
- Authentic
 - the real thing, not a replica
- Complete
 - includes any exculpatory evidence
- Believable
 - lawyers, judge & jury can understand it

Definition of Forensics

- Discipline of digital evidence discovery, protection and presentation.
- Technologies, techniques, and responsibilities of a criminal or civil investigation involving computers, networks, network service providers and electronic evidence.

Types of Forensic Exams

- Legal or Liturgical
 - Will go to trial
- Civil
 - Similar to liturgical probably for negotiation or extortion
- Business
 - Termination or reprimand an employee
- Disaster Recovery
 - What happened, how to prevent
- Illegal/Surveillance

Areas of Forensics

- Physical
- Digital
- Chemical
- Accounting
- Etc.

Physical

- Ballistics
- Fingerprints
- Artifacts
- etc.

Digital Forensics

Computer Forensics

- Evidence contained in computers
- Evidence contained in digital devices
 - Phones
 - Cameras
 - Memory sticks
 - Smart cards
- Evidence contained in networks

Chemical

- Blood
- DNA
- Explosives
- Drugs
- Fiber analysis
- Etc.

Accounting

- Fraud
- Multiple sets of books
- Stock manipulation
- Insider trading

Digital Devices

- Computers, Laptops
- Palm pilots
- Cell phones
- iPods
- Cameras
- Camcorders
- etc.

Digital Evidence

- Records and Logs
- Results of activities
- Statement of intent
- Contraband
- Indication of time line

Skills and Knowledge

- Be aware of the many types of digital devices and their components and potential contents
- Develop a Web behavior profile
- Learn how to seize a computer and other devices
- Proper handling of digital evidence
- How to search a computer for evidence
- Analyze a phishing scam
- Become more knowledgeable about the digital/information world