



Introduction to Computer Forensics

David Nardoni CISSP, EnCE
dnardoni@firstresponseconsulting.com

Chi So
chiso@usc.edu



Overview

Introduction to computer forensics

- Hand out and discuss syllabus
- Introduction of instructors
- Goal for class “How to not screw up an investigation that involves digital evidence”
- What do you want from the class?
- Questions
- Skill assessment Quiz
- Current news related to information security and computer forensics
- Introduction to computer forensics



ONE THING TO REMEMBER

WITHOUT THE PROPER TRAINING OR SKILLS, NO ONE SHOULD ATTEMPT TO EXPLORE THE CONTENTS OR RECOVER DATA FROM A COMPUTER (DO NOT TOUCH THE KEYBOARD OR CLICK THE MOUSE) OR OTHER ELECTRONIC DEVICE OTHER THAN TO RECORD WHAT IS VISIBLE ON THE DISPLAY.



Brief History to Computer Forensics

- Early in 1970's students discovered how to gain unauthorized access to large time-shared computer systems.
- 1978 the Florida Computer Crime Act was the 1st law to help deal with computer fraud and intrusion. Employees at a dog track used a computer to print fraudulent winning tickets. The act also defined all unauthorized access as a crime.
- 1984 US Federal Computer Fraud and Abuse Act was passed. (Morris Worm 1988)
 - Recent Events
 - Kevin Mitnick helping LE
 - 13yr girls teaching FBI to catch child predators
- Responding to computer crime in the 80's and 90's law enforcement training programs were started at SEARCH, FLETC and NW3C.



What types of jobs exist

- Law Enforcement
 - CIA, FBI, Local PD, Sheriff
- Private Sector
 - Information security company, Large corporation, Big four accounting firm, Law Firm
- Military



Electronic or Digital Evidence

Definitions

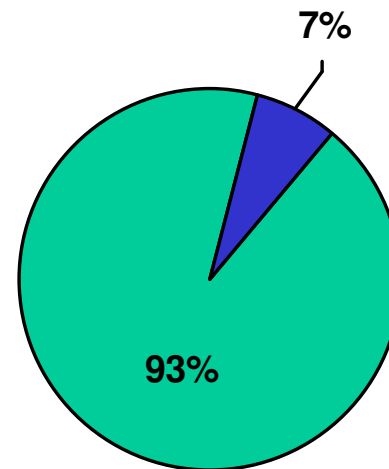
Electronic record : any data that is recorded or preserved on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

Computer Forensics : Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.



Digital evidence is everywhere

Digital vs. Non-Digital



■ Digital ■ Non-digital

According to a study by University of California-Berkeley in 2001 found that 93% of all new information at that time was created entirely in digital format.



Properties of digital evidence

- Digital evidence is any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi. (Casey, Eoghan. Digital Evidence and Computer Crime, p12)
- Digital evidence is extremely fragile similar to a fingerprint.
- Digital evidence is also “Latent” which means it can not been seen in it’s natural state, much like DNA. Any actions that can alter, damage or destroy digital evidence will be scrutinized by the courts.
- Digital evidence is often constantly changing and can be very time sensitive
- Digital evidence can transcend borders with ease and speed



Recognizing Potential Evidence

- Contraband or fruits of a crime?
- A tool of the offense? (instrumentality)
- Only incidental to the offense? (hardware/information as evidence)
- Both instrumental to the offense and a storage device for evidence?



Contraband or fruits of a crime

- Stolen Computer Equipment (Mortgage Company)
- Stolen Software (Gateway credit card processor)



A tool of the offense

- Theft committed using computer
- Fraud committed using computer
- E-mail sent from a computer
- Sex offense committed after being arranged on computer
- Fraudulent money or ID's made with computer



Only incidental to the offense

- Drug dealer maintaining records or ordering supplies
- Child molester keeping records on children
- Suicide notes or pictures of the crime stored online
- Victim keeping diary or electronic journal
- Suspect searching the web for info about crime
- Credit card fraud records being kept on computer
- Child pornography being stored on computer

- Case of the blood sucking Ex (deleted emails)



Both instrumental to the offense and a storage device for evidence

- Hacker uses computer to attack another system and stores the information on their computer.
- Child pornographer uses computer to manufacture, distribute and store pornography



Types of crime that might involve digital evidence

- Types of crimes that may involve digital evidence
- Online auction fraud
- Child exploitation/Abuse
- Computer Intrusion
- Homicide
- Domestic Violence
- Economic Fraud, Counterfeiting
- Threats, Harassment, Stalking
- Extortion
- Gambling
- Identity Theft
- Narcotics
- Prostitution
- Software Piracy
- Telecom Fraud



Types of investigations

- **Internal:** no search warrant or subpoena needed, quickest investigation
 - Corporate investigation that involves IT administrator reviewing documents that they should not be viewing.
- **Civil:** other side may own the data, may need subpoena
 - One party sues another over ownership of intellectual property, must acquire and authenticate digital evidence so it can be submitted in court.
- **Criminal:** highest stakes, accuracy and documentation must be of highest quality, slowest moving
 - Child porn investigation that involves possession and distribution of contraband.



Qualities of a good investigator

- Highest level of ethics
- Unbiased
- State facts not opinions (unless requested to do so)
- Aware of when to call for help
- Has good documentation skills
- Good communications skills
- Follows same process/methodology every time