Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 2

Language of Computer Crime Investigation

- Virtually every class of crime can involve some form of digital evidence.
- To understand computer crime it is helpful to know some history, language, and legislation.
- (late) 1960's to (early) 1970's students were learning how to hack into shared mainframes to get "free" run time. This was not illegal at the time.
- 1970's LEOs try to make existing laws governing "real" property fit computer crimes; but courts ruled that computer crimes where intangible.
- FL adopted the first law: Florida Computer Crimes Act of 1978. Since then there has been many new laws against computer intrusion.
- Review computer crime v. computer related crime.
- Forensic Examination v. Analysis.
    - A thorough examination results in all relevant data being organized and presented in a manner that facilitates a detailed analysis.
- The computer examination process is generally more susceptible to computer automation then the analysis process.
- Parker's four categories of the role of a computer in crime:
    1. Object of a crime: it is affected by the crime (i.e. stolen),
    2. Subject of the crime: the computer is the environment in which the crime is committed (i.e. a virus, or you disable a computer system),
    3. Tool of the crime: the computer is used to facilitate the crime, i.e. counterfeiting, and
    4. Symbol of the crime: not really used, but the "idea" of a computer is injected into the crime (i.e. extortion, pay me the money or I will post on the Internet …).
- A target of a crime is the object of an attack from the offender's point of view.
- An intended victim of a crime is the person, group, or organization that is meant to suffer the harm.
- Collateral victims of a crime are victims that an offender causes to suffer loss or harm in the pursuit of another victim.
- Symbol: any person or thing that represents an idea, a belief, a group, or even another person.
- A 5th category that has emerged since Parker created his categories is that of a computer as evidence of a crime.
- New trend towards not seizing the hardware since it is merely the container of the evidence if data is what you are after.
- Now more searches are being on site instead of seizing the systems and taking them back to the lab.

- DOJ Manual: "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (2009). It spelled out the difference between the hardware being the target of your search and the information.
- Digital crime scene v. physical crime scene.
- Three categories (each one can be applied to hardware or software):
    - Contraband or fruits of the crime,
    - Instrumentality (played *significant* role in the crime), or
    - Evidence.
- Hardware as contraband or fruits of a crime:
    - What is contraband,
    - What is fruits of a crime.
- 4th Amendment of the United States Constitution:
  The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
- Seizure of contraband or fruits of a crime (4th Amendment):
    - "court will examine whether the circumstances would have led a reasonably cautious agent to believe that the object was contraband or fruit of a crime."
    - Why do we seize contraband and fruits of crime?
- Seizing instrumentality of a crime. Why can we seize it?
- In 1972 "mere evidence" of a crime could not be seized. What problem could this cause? FRCP 41b now allow the seizure of any property that constitutes evidence of the commission of a crime.
- Probable Cause v. Reasonable Suspicion.
- When can you seize something?
- Information can be the instrumentality of the crime. What if it is the information that allows you to commit the crime?
- Information as evidence. This is the big one!!!!