Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 1

Introduction

- Modern desktop computers have enabled the criminal to automate their criminal activity.
    - Cheap computers and desktop printers allow the criminal to easily forge documents and financial instruments.
    - Access to the Internet allows criminals to easily share the knowledge of criminal activity, and sometimes the criminal material (CP).
    - With the explosion of the internet and the cyber-marketplace, cyber-crime has increased.
- **Computer Crime:** a general term that has been used to denote any criminal act that has been facilitated by computer use.
    - Examples: theft of computer components, counterfeiting, digital piracy or copyright infringement, hacking, and child pornography (CP). (Britz, 2013, p. 6)
- **Computer Related Crime:** criminal activities in which a computer was peripherally used.
    - Examples: traditional book making and theft where a computer is used to record the activity. (Britz, 2013, p. 6)
- **Digital Crime:** any criminal activity that involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. (Britz, 2013, p. 6)
- **Computer Forensics:** the forensic examination of computer components and their contents, such as hard drives, compact disks, and printers. (Casey, 2011, p. xxv)
- **Network Forensics:** the forensic examination of data traveling over computer networks. (Casey, 2011, p. xxv)
- **Mobile Forensics:** the forensic examination of mobile devices such as smart phones and tablet computers.
- **Digital Forensics:** the field of forensic science that encompasses all computer, network, and mobile device related forensic examinations. (Casey, 2011, p. xxv)
- U.S. Customs Cyber-smuggling Center has come to view every computer on the Internet in the U.S. as a port of entry.
- The largest robberies of our time have occurred on the Internet.
- News stories about online theft.
- **Digital Evidence:** is any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi. (Casey, 2011, p. 7)
- Before looking at the different types of digital evidence we must first consider the type of computer systems: **Open Computer System, Communication Systems, and Embedded Computer Systems.**

History

- In the late 80s and early 90s the law enforcement community saw an increase in computer related crimes and started to create training to investigate these new crimes.
- Due to the explosive growth in these types of crimes, the demand for their services where quickly overwhelming these new federal computer examiners.
- Now we have regional centers the help the LE community investigate these crimes.
    - See the RMRCFL annual report.
- These regional centers where also overloaded and so some local jurisdictions who had the resources created their own computer crimes units.
- Due to the rapid development of the technology there is a great demand for individuals that know how to collect and analyze digital evidence.
- A consortium of certification organizations has been convened to form a working group called the Council of Digital Forensic Specialists.

Principles of Digital Forensics:

- **Forensics** means a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof. (Casey, 2011, p. 14)
- **Forensic Science** is the application of science to law and is ultimately tested by use in court. (Casey, 2011, p. 15)
- Judicial Notice: why is it important and how does it apply to CF.
- Reason for use of forensically sound methods in private practice: terminating an employee and a law-suite is filed.
- Goal is to follow the trail of evidence until you can tie the suspect to the victim and crime scene.
- **Locard's Exchange Principal** states that contact between two objects will result in an exchange between the two objects. (Casey, 2011, p. 16)
- How does this apply to computer forensics?
- Absence of evidence is not evidence of absence.
- **Class Characteristics:** common traits in similar items. (Casey, 2011, p. 17)
- **Individual Characteristics:** unique traits that can be linked to specific person or activity with greater certainty. (Casey, 2011, p. 17)
- Note the word certainty. In forensics it is very rare to have absolute certainty. Why?
- Finding individual characteristics reduces the margin of error, which makes the link much less circumstantial and harder to refute.
- Digital evidence must be collected and stored in a forensically sound manner.
- Debate about altering the original evidence. DNA example.
- Even when using a write blocker, you could alter the source hard drive by the mere act of copying the drive. When accessing a drive (simply powering up) you may modify the information stored in the SMART system.

- What if you accidently change something?
- Key to being forensically sound is documentation. Document everything that you do.
- Part of the documentation has to be dates, times, MD5 hash values when data is acquired.
- Note the date/time that the computer is reporting and compare it to a known reliable source. Why?
- Also, there needs to be documentation that can prove the authentication of the data:
  Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record." (Casey, 2011, p. 21)
- Chain of custody. Very important aspect of authentication. Continuity of possession. Keep the number of individuals to a minimum.
- Integrity checks are used to show that evidence has not been altered from the time it was collected. Use hash values for this.
- Message digest algorithm: black box that accepts file, program, disk, etc. It spits out a message digest. The algorithm will always return the same digest for the same input. Good algorithm will return a different number for a different input. MD5, SHA-1 are two the most widely used algorithms.
- MD5 produces a 128 bit message digest. The conjecture is that it is unfeasible to produce two messages having the same message digest or to produce any message having a given prespecified target message digest.
- Hash collision. When two different messages produce the same message digest. All modern algorithms have been shown to be able to produce a collision under very controlled conditions. Very rare, but to help authenticate the integrity of the data, it is common practice to use two algorithms to get two hash values.
- Objectivity: if it appears that you are biased, the defense will question the validity of the work product. Look at CO DPH&E blood alcohol testing program.
- Repeatability: this comes from the fact that computer forensics is a science, you should be able to duplicate your results. Keep in mind that someone's "life hangs in the balance" and so you want to make sure what you did is correct. Documentation of all steps taken helps with showing repeatability.
- Digital evidence is considered physical evidence, but there are challenges there. Data is ever changing, there is a lot of it, and you are only interested in a small part of the whole.
- Digital evidence is easy to damage, which causes problems in of it self.
- Digital evidence is usually circumstantial. If you case relies on only one piece of digital evidence, it is VERY weak.

- Direct evidence supports the truth of an assertion (guilt or innocence). Think of a witness that saw the defendant shot the victim. No inference needed.
- Circumstantial evidence needs an inference to be drawn. Witness saw the same defendant fleeing the crime scene, or the defendant's fingerprints where found at the crime scene.
- Evidence dynamics and the introduction of error. Examples. What can happen if error is introduced into the evidence?
- Remember that crime on the Internet is a lot of times tied to crime in the "real world." Examples. Why does this mater?
- The Internet provides a sense of anonymity. This sometimes is true, but most of the time it isn't, which can aid in the investigation.
- With the wide spread use of "connected" device, even a crime that doesn't seem to have a digital aspect can. There could be a ton of evidence out there, you just have to know where to look.
- Problems with new cloud based systems and the gather of evidence. Subpoenas and crossing state lines. Finding all the pieces.

Works Cited

Britz, M. T. (2013). *Computer Forensics and Cyber Crime: an Introduction* (3rd Edition ed.). Clemson, SC, USA: Pearson.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd Edition ed.). Waltham, MA, USA: Academic Press (Elsevier).