Laureate Online Education

Computer Forensics

Computer Forensics

Seminar for Week 1: Digital Evidence, Computer Crime, Technology and Law

WELCOME to this module on Computer Forensics. Over the next few weeks, we will be exploring, thinking about, and discussing ideas concerning the principles and practice of computer forensics. In particular, we will be covering topics including digital evidence and computer crime; technology and law; the investigative process; investigative reconstruction; digital evidence in the courtroom; techniques for discovering digital evidence; responding to electronic incidents; tracking communications through networks; understanding electronic media; Windows™ and UNIX™ system forensics; digital evidence on the Internet; investigating computer intrusions; sex offenders on the Internet; criminal profiling; and investigations of cyber-stalking.

As digital criminals have become more sophisticated, security-related incidents have become substantially more diverse in nature, and their impact on society is increasingly more destructive. Vulnerabilities within the information infrastructure have potentially profound consequences for the government, corporations, and millions of individuals. Detection of and response to digital incidents are vital components of modern information security programs at both macro and micro levels. Operating in today's dynamic computing environments, the forensic investigator must be able to detect and counter cyber-crime effectively. This module will provide students with opportunities to study, understand, and use the latest developments and best practices in computer forensics. Topics include basics of computer forensics (AAA, or Acquire the evidence, Authenticate the evidence, and Analyze the evidence), incident response handling, computer forensic mechanisms, computer forensic tools, computer forensic practices, and other issues.

What you can learn from this module

In this module, you will learn the following techniques:

- The basic process and the AAA techniques for computer forensics
- How to handle incident responses (that is, know the goals and objectives, roles and capabilities, incident response handling process, Criminal Justice System (CJS), structure of CJS, legal processes and issues)
- How to use computer forensic tools
- Forensic practices (computer forensics in Unix and Windows)
- Technology and law in different countries
- Future trends in computer forensics and international cooperation
- Understand ethical issues, legal issues, and criminal motives
- How to investigate sex offenders on the Internet

The purpose of this module is to teach you how to analyze and conduct a computer forensics examination and report the findings that will lead to the incarceration of the perpetrators. Through extensive hand-in assignments and projects, you will gain the knowledge and skills required to master the deployment of information infrastructure that keeps sufficient evidence for legal purpose when your system is under attack.

In the seminar, we will learn about the basics of computer forensics AAA. We will also learn about the technology and laws for different countries.

Digital Evidence and Computer Crime

Criminals are using advanced technology to facilitate their offenses and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals.

The textbook defines *digital evidence* as 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. By now, it is well known that attorneys and police are encountering progressively more digital evidence in their work.

Computers are used in two ways in criminal activities. Either a computer is used to commit a crime, or the computer itself is the target of a crime. “Digital evidence is becoming a feature of most criminal cases . . . Everything is moving in this direction" (Susan Brenner, professor of law and technology at the University of Dayton School of Law; see CNN (2005)). Child pornography, threatening letters, web phishing, identity theft, and theft of intellectual property are all crimes that leave electronic trials. Investigation into these types of crimes usually includes searching computers that are suspected of being involved in their commission. Such analysis involves sifting through huge amounts of data for specific keywords to see what happened at certain times, and hopefully providing evidence that a specific person did a specific illegal act—or that a specific person apparently did not commit an illegal act.

Computers themselves can be the victim of the crimes. This normally happens when computer systems are remotely attacked. Remote attacks have become far more common, taking advantage of increasingly complex and vulnerable network services. The CERT and US-CERT web sites have lists of vulnerabilities of network infrastructure systems that could be used to attack computer systems. Some of the attacks are also listed in these web sites.

Computer forensics involves evidence acquisition, evidence authentication, and evidence analysis. Digital evidence such as log files is often transparently created by the computer’s operating system without the knowledge of the computer operator and is often hidden from view. To find it, special forensics tool and techniques are needed. We need also keep in mind that criminals are also concerned with digital evidence and will attempt to manipulate computer systems to avoid apprehension (e.g., when an offender uses root kit to delete his/her electronic trails). This module will teach you the AAA forensic investigation methodologies using examples and specially designed tools. You need to extend these experiences and knowledge creatively to cases that you will meet in practice.

Digital evidence creates several challenges for forensic examiners. First, it is a form of evidence that can be very difficult to handle. For example, an acquired hard drive contains huge amounts of data, though only a small portion might be relevant to the case. Second, digital evidence is generally an abstraction of some event or digital object. For example, when an email related to a case is intercepted, the content of the email gives only a partial view of what occurred. Third, digital evidence can be manipulated easily. For example, the evidence could be maliciously modified by offenders or be altered accidentally by system administrators. Fourth, digital evidence is usually circumstantial. Thus, special attention should be paid to the digital evidence collection process and to the chain of evidence that we will discuss later. For example, the Predator and Prey Alert (PAPA) that has recently been developed by Florida State University can be used to achieve high-quality digital evidence for the prosecution of cyber-stalking cases. The PAPA system allows a law enforcement agent to remotely shadow a victim, advise the victim by communicating through a separate side channel, and assume control of the victim's computer in order to interact directly with the stalker.

While criminals feel safe on the Internet, they are observable and thus vulnerable. We can take this opportunity to uncover crimes in the physical world that would not be visible without the Internet. Indeed, several murderers have been identified as a result of their online actions

(LJworld 2004). In addition, the Internet may contain digital evidence of the crime that may be not directly involved. For example, there are a growing number of sensors on the Internet such as cameras showing live highway traffic on the Web (e.g., you can view the real-time traffics in Montgomery County, Maryland, at http://www.ncsmartlink.org/cameras/; you can view regularly refreshed traffics in South Carolina at http://www.scdot.org/getting/cams/). These cameras may inadvertently capture evidence relating to a crime. Furthermore, digital networks usually contain a higher concentration of digital information about the individuals who use them, making it easier to find and collect relevant digital data. It is conceivable that a digital investigator could determine where an individual was throughout a given day using GPS information that the individual's wireless phone transmits to his/her service provider. Organizational computer log information can also be used to determine where an employee was and what she/he was doing during a given day. The challenge is that data can be spread over a group of adjacent buildings, several cities, states, or even countries; it is difficult to find and collect all relevant digital evidence. For all but the smallest networks, it is not feasible to take a snapshot of an entire network at a given instant. Also, network traffic is transient and must be captured while it is in transit.

History of Computer Crime Investigation

Before the 1970s, crimes related to computers consisted mainly of component (hardware) theft and CPU time theft (e.g., gaining unauthorized access to large time-shared computers). Although component theft has been a criminal activity, CPU time theft was an act that was not illegal at the time. There had been some legal struggles for crimes involving computers, as digital property was seen as intangible and, therefore, outside of the laws protecting physical property. The Florida Legislature passed the first computer crime statute in 1978 in response to the Flagler Dog Track incident near Miami, in which employees used a computer to print bogus winning trifecta tickets.

In response to the growth in computer-related crime, law enforcement agencies in the United States worked together and established training programs such as the Federal Law Enforcement Center (FLETC) and National White Collar Crime Center (NW3C).

In 1984, the FBI created the Magnetic Media Program, which later became the Computer Analysis and Response Team (CART). CART provides assistance to FBI field offices in the search and seizure of computer evidence as well as forensic examinations and technical support for FBI investigations.

In 1995, the International Organization on Computer Evidence (IOCE) was formed. In Moscow in 1997, the G8 countries declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes." In 1998, the IOCE was appointed by G8 to draw international principles for procedures relating to digital evidence in order to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state. In 1998, the International Forensic Science Symposium (INTERPOL) was formed.

In 1999, FBI CART case loads exceeded 2000 cases examining 17 terabytes of data. In 2000, the first FBI Regional Computer Forensic Laboratory was established (RCFL). In 2003, FBI CART case loads exceeded 6500 cases examining 782 terabytes of data.

In the early days of computer crime investigation, digital investigators usually used the evidentiary computer itself to obtain evidence. One risk of this approach was that operating the evidentiary computer could alter the evidence in a way that is undetectable. Since the 1990s, special tools such as SafaBack and DIBS were developed to enable investigators to collect all data on a computer disk for later analysis without altering the original evidence. Over the next few weeks, we will discuss the existing tools that could be used for forensic purposes.

The term *computer forensics* means different things to different people. It usually refers to the forensic examination of computer components and their contents, such as hard drives, compact disks, and printers. However, the term is sometimes used to describe the forensic examination of all forms of digital evidence, including data traveling over networks (cf. network forensics). In

2001, the first annual Digital Forensic Research Workshop (DFRWS) proposed *digital forensic science* to describe the field as whole. The terms *forensic computer analysis* and *forensic computing* have also become widely used.

Technology and Law

Laws have been passed in many countries to address computer-related crimes. Obviously, there are jurisdictional problems associated with the international character of the Internet that make prosecution difficult and sometimes impossible. Some of the international organizations that are addressing computer crime are the United Nations (UNODC), Interpol, the European Union (EU), and the G8's leading industrial nations.

There are many types of legal systems in the world that differ in how they treat evidence, the rights of the accused, and the role of the judiciary. Examples of these different legal systems are common law (Common Law), Islamic and other religious law (Islamic Law), and civil law (Civil Law). The common law system is employed in the United States, United Kingdom, Australia, and Canada. Civil law systems are used in France, Germany, and Quebec, Canada.

Under the common law system of the United States, there are three branches of government that make the laws: the legislative branch, the administrative agencies, and the judicial branch. The legislative branch makes the statutory law, the administrative agencies create the administrative laws, and the judicial branch makes the common laws found in court decisions. Statutory laws are collected as session laws, which are arranged in order of enactment or as statutory codes that arrange the laws according to subject matter. In the United States, at the federal level, the session laws are found in the Statutes at Large, and the statutory codes are held in the United States Code. The statutory laws for the states are also arranged in these two categories.

The main categories of laws under the common law system are criminal law, civil law (tort), and administrative/regulatory law. Criminal laws are about individual conduct that violates government laws enacted for the protection of the public. Punishment can include financial penalties and imprisonment. Civil laws are about a wrong inflicted upon an individual or organization that results in damage or loss. Punishment cannot include imprisonment, but financial awards comprised of punitive, compensatory, or statutory damages can be mandated. Administrative/regulatory laws are standards of performance and conduct expected by government agencies from industries, organizations, officials, and officers. Violations of these laws can result in financial penalties and/or imprisonment.

Other categories of law under the common law system that relate to information systems are intellectual property and privacy laws. The intellectual property laws include patent, copyright, trade secret, and trademark.

Patent provides the owner of the patent with a legally enforceable right to exclude others from practicing the invention covered by the patent for a specified period of time. For example, the current term of protection of a United States patent is seventeen years, measured from the grant of the patent (US Patent), and the current term of protection of an international patent (PCT) is twenty years (PCT). Patent law protects inventions and processes ("utility" patents) and ornamental designs ("design" patents). Copyright protects "original works of authorship." It protects the right of the author to control the reproduction, adaptation, public distribution, and performance of these original works and can be applied to software and design. Trade secret secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner. Corollaries to this definition are that the owner has invested resources to develop this information, it is valuable to the business of the owner, it would be valuable to a competitor, and it is non-obvious. Trademark establishes a word, name, symbol, color, sound, product shape, device, or combination of these that will be used to identify goods and to distinguish them from those made or sold by others.

The protection of information about private individuals from intentional or unintentional disclosure or misuse is the goal of the information privacy laws. This intent and scope of these laws varies widely from country to country. The EU has defined privacy principles that in general are more

protective of individual privacy than those applied in the United States. Therefore, the transfer of personal information from the EU to the United States, when equivalent personal protections are not in place in the United States, is prohibited.

A typical example of the privacy law in the United States is the Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA), which addresses the issues of health care privacy and plan portability in the United States. With respect to privacy, this Act stated the following: "Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of health and Human Services shall submit . . . detailed recommendations on standards with respect to the privacy of individually identifiable health information."

The Platform for Privacy Preferences (P3P) was developed by the W3C to implement privacy practices on Web sites. The W3C P3P specification states that "P3P enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents." P3P user agents will allow users to be informed of site practices and to automate decision-making based on these practices when appropriate.

Digital evidence admissibility: In order for digital evidence to be admissible in a court of law in most countries, evidence must meet certain stringent requirements. In particular, the evidence must be relevant, legally permissible, reliable, properly identified, and properly preserved. To be relevant, the evidence must be related to the crime in that it shows that the crime has been committed. To be legally permissible, the evidence should be obtained in a lawful manner. To be reliable, the evidence should have not been tampered with or modified. To be identifiable, the evidence should be properly identified without changing or damaging the evidence. In computer forensics, this process includes labeling printouts with permanent markers, identifying the operating system used, identifying the hardware types, recording serial numbers, and labeling evidence without damaging it or by placing it in marked and sealed containers. To be properly preserved, the evidence should not be subject damage or destruction. The recommended procedure for preservation includes these instructions: Do not prematurely remove power, back up the hard disk image by using disk imaging hardware or software, avoid placing magnetic media in the proximity of sources of magnetic fields, store media in a dust- and smoke-free environment at a proper temperature and humidity, write-protect media, and authenticate the file system by creating a digital signature based on the contents of a file or disk sector.

Type of evidence: Legal evidence can be classified into the following types (Digital Evidence):

- Best evidence: Original or primary evidence rather than a copy or duplicate of the evidence.
- Secondary evidence: A copy of evidence or oral description of its contents; not as reliable as best evidence.
- Direct evidence: Proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses.
- Conclusive evidence: Incontrovertible; overrides all other evidence.
- Opinions: There are two kinds of opinions, expert (opinion based on personal expertise and facts) and non-expert (testify only as to facts).
- Circumstantial evidence: Inference of information from other, intermediate, relevant facts.
- Hearsay evidence (third party): Evidence that is not based on personal, first-hand knowledge of the witness but that was obtained from another source. Under the U.S. Federal Rules of Evidence, hearsay evidence is generally not admissible in court. Computer-generated records and other business records fall under the category of hearsay. However, there are certain exceptions to the hearsay rule for records that are made during the regular conduct of business and authenticated by witnesses familiar with their use, relied upon in the regular course of business, made by a person with knowledge of the records, made by a person with information transmitted by a person

with knowledge, made at or near the time of occurrence of the act being investigated, and in the custody of the witness on a regular basis.

Searching and seizing computers: In several countries (e.g., Unites States, England, and Ireland), law enforcement must obtain legal authorization to search a location and seize evidence including computers. In making a request for a search warrant, law enforcement officers in the United Kingdom are required to state the grounds for their application, including the law that has been broken. Also, as in the United States, the application must specifically describe the premises that will be searched and, as much as possible, the items or individuals that are being sought.

Conducting investigation: There are many issues involved in the process of computer crime investigation. For example, in a corporation environment, an investigation should involve management, corporate security, human recourses, the legal department, and other appropriate staff members. If a computer crime is suspected, it is important not to alert the suspect. A preliminary investigation should be conducted to determine whether a crime has been committed by examining the audit records and system logs, interviewing witnesses, and assessing the damage incurred. It is critical to determine whether disclosure to legal authorities is required by law or regulation. U.S. Federal Sentencing Guidelines require organizations to report criminal acts. Once an outside entity such as law enforcement is involved, information dissemination is out of the hands of the organization. The timing of requesting outside assistance from law enforcement is another major issue. In the United States, law enforcement personnel are bound by the Fourth Amendment to the U.S. Constitution and must obtain a warrant to search for evidence. Specifically, this amendment states that “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”; it also stipulates that a search warrant “describe[s] the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person’s belongings.” The amendment protects individuals from unlawful search and seizure. Search warrants are court authorizations for law enforcement officers to search for and to seize records, or other information, as part of a criminal investigation. Many immoral acts are not necessarily criminal, so warrants cannot be issued for them. Further, some states restrict issuance of a search warrant to felonies, prohibiting their use in misdemeanors or petty offenses. Therefore, officers may not be able to obtain a warrant. Private individuals in the United States are not held to this strict requirement; thus, in some cases, a private individual can conduct a search for possible evidence without a warrant. However, if a private individual were asked by a law enforcement officer to search for evidence, a warrant would be required because the private individual would be acting as an agent of law enforcement. An exception to the search warrant requirement for law enforcement officers is the Exigent Circumstances Doctrine. Under this doctrine, if probable cause is present and destruction of the evidence is deemed imminent, the search can be conducted without the delay of having the warrant in-hand.

Subpoena for records: A subpoena is a court order used to compel the testimony of witnesses in a trial or other adversarial proceeding. Subpoenas are issued in the name of the judge presiding over the case in which the witness is to testify. The subpoena is used with almost all applications throughout the common law systems. The civil law system in the United Kingdom uses the term *witness summons* instead of *subpoena*. *Subpoena duces tecum* is a specific form of subpoena that requires a person to bring certain documents or other evidence to the court.

Recidivism: Recidivism refers to the fact that a person repeats a crime after they have been found guilty and have served his/her sentence. Repeated offenders will generally receive stricter sentences.

Legal advice: Before you start any investigation, you are recommended to consult your legal service for advice on what you can and cannot do. For example, courts normally will rule that company-owned computers/handheld devices/cell phones do not contain any “personal” information. But you need to make sure that your company has policies in place to alert employees to that fact, and you have the authority to access this “personal” information if it is

there. The legal system is complicated. It is good to know what laws cover the various computer crimes, but it is more important to know what you legally can or cannot access.

Ethics: Sometimes it is difficult to distinguish unethical behaviors and illegal actions. Many organizations have defined the codes for ethical computing. The IETF RFC 1087 defines the Internet Activities Board (IAB) and Internet ethical computing as the following: Access and use of the Internet is a privilege and should be treated as such by all users of the systems. In particular, it states that the IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure, which characterizes as unethical and unacceptable any activity that purposely:

1. seeks to gain unauthorized access to the resources of the Internet;
2. disrupts the intended use of the Internet;
3. wastes resources (people, capacity, computer) through such actions;
4. destroys the integrity of computer-based information; and/or
5. compromises the privacy of users.

Bibliography

Computer Technology Investigators Northwest (CTIN): http://www.ctin.org/

High Technology Crime Investigation Association (HTCIA): http://www.htcia.org/

CNN (2005) http://www.cnn.com/2005/LAW/01/28/digital.evidence/

CERT http://www.cert.org

US-CERT http://www.us-cert.gov

PAPA system http://www.fsu.edu/news/2005/09/08/cyberstalkers/

LJworld (2004) e.g., http://www2.ljworld.com/news/2004/dec/10/web_evidence_used/

FLETC http://www.fletc.gov/

NW3C http://www.nw3c.org/

CART http://www.fbi.gov/hq/lab/org/cart.htm

IOCE, http://www.ioce.org/

INTERPOL, http://www.interpol.org/

RFCL http://www.rcfl.gov/

DFRWS http://www.dfrws.org/

UNODC http://www.unodc.org/unodc/index.html

EU http://europa.eu.int/information_society/index_en.htm

Common Law http://en.wikipedia.org/wiki/Common_law

Islamic and other religious law http://www.soas.ac.uk/Centres/IslamicLaw/Materials.html

civil law http://en.wikipedia.org/wiki/Civil_law_(legal_system)

US Patent http://www.uspto.gov/web/offices/com/doc/uruguay/SUMMARY.html

PCT http://www.wipo.int/portal/index.html.en

HIPPA http://aspe.hhs.gov/admnsimp/pl104191.htm

P3P http://www.w3.org/P3P/

Digital Evidence http://en.wikipedia.org/wiki/Digital_evidence

U.S. Constitution http://caselaw.lp.findlaw.com/data/constitution/amendment04/

IETF RFC 1087 http://www.ietf.org/rfc/rfc1087.txt

Additional Reading

Casey, E., (2011) *Digital evidence and computer crime: forensic science, computers and the internet*. 3rd ed. New York: Elsevier Academic Press.

Reading Requirements

Read textbook chapters 1, 2, 4, 5. Skim Chapter 3.