Computer Forensic
Evidence Collection and Management

Chapter 3

Computer Forensic Examination Categories

Chapter Objectives

- Identify the various crimes and incidents that are involved in electronic forensic investigations.
- See how identity theft and fraud permeates all elements of the computer and electronics environment
- Look at the various types of evidence that can be gathered for each category of crime
- Become familiar with the various terms associated with these types of investigations.
- Understand the importance of security and computer-use policies
- Look at the various incidents that may be investigated by the corporate security department.

Introduction

- It has been estimated that computer crimes result in billions of dollars in losses worldwide.
  - There are general two categories of computer crimes:
  - Those that use a compute or some electronic device to commit a crime or incident
- Those that used against these devices.
- Some of the most prominent computer-style crimes and incidents are:
  - Network intrusions
  - Destruction of data and information
  - Modification of data or data-diddling
  - Denial-of-service and distributed DoS
  - Eavesdropping
  - Software piracy
  - Music piracy
  - Theft of logins and passwords
  - Malicious code and programs
  - Masquerading

  Illegal material content
  Spoofing of Internet protocol addresses
  Fraud
  Embezzlement
  Espionage
  Information warfare
  Cyber-terrorism
  Social engineering
  Dumpster diving
  Child molestation

Some of these items are techniques that are used to commit an actual crime.

Common Law Overview

- Main category of common law:

Civil Law:
Represents numerous laws recorded in volumes of legal code

Criminal Law:
Addresses violations enforced through state prosecution

Tort Law:
Allows individuals to seek redress in the courts

Most criminal computer and electronic investigations will be in supoort of some other major case category.

A kidnapping might be solved by digital evidence found in an e-mail, cell phone record, or on a suspect's computer system.

The electronic forensics investigators and examiners would be part of the primary case team.

.

Financial Crime Categories

This type of crime includes fraud, economic fraud, property theft, and identity theft.
A fraud is defined as a fraudulent conversion and obtaining money or property by false pretenses. .

Auction Fraud

Online frauds have become an issue with the advent of electronic business and electronic commerce activities in the Internet. These activities are known as

- *Business-to-consumer (Amazon.com)*
- *Consumer-to-consumer (EBay)*
- *Business-to-Business*

Action fraud occur on the Internet sites that offer consumer items for sale to the general public. There are groups of pope who offer to sell and buy items over these Internet sites, but have no intention of fulfilling the contract. Both search warrants and subpoenas will probable be required to collect forensic evidence.

Economic Fraud and Property Theft

Computer system software can be modified and manipulated by unscrupulous employees fore personal gain or as part of a conspiracy involving other insiders. These offenses could also involve online fraud and other crimes, such as counterfeiting, check laundering, money laundering, and identity-theft activates.
Some of the evidence findings are similar to those for auction and online fraud. These include:

Address books,	*Calendars*	*Check, currency, and money orders*
Credit card skimmers	*Customer information*	*Credit card data*
Databases	*E-mail transmissions*	*False financial transactions forms and screen shots*
False identification	*Financial records*	*Signature images*

Financial Crime Categories (cont.)

Identity theft

Identity theft is defined as the deliberate assumption of another person's identity, usually to gain access to the person's finances.
Numerous scams are perpetuated daily on the general public and specifically on Internet and e-mail users.

A brief review of the following lists provides some identification of the magnitude of identity theft crimes.

Hardware and software devices:
Credit card generators, credit card reader/writer, cameras, scanners, skimmers

Forged identification and identification templates include:
Check cashing cards, drivers' license, social security cards, electronic signatures, birth certificates vehicle registrations, proof of auto insurance scanned signatures .

Internet activates related to identity theft include:
E-mails and newsgroups postings, erased documents, online orders, online trading info, system files, file slack and unallocated space, web activity at suspect sites.

Negotiable instruments include:
Business checks, cashier's checks, counterfeit money, credit card numbers, fictitious court documents, fictitious gift certificates, fictitious loan documents, money orders, personal checks, stock transfer documents, vehicle transfer documents.

Computer Crime Categories

These type of crimes include software and video privacy, computer threats and intrusions, telecommunications fraud, and email issues.
Piracy is defined as the unauthorized duplication of goods protected by intellectual property law.

Software and video piracy

The Internet provides an available conduit for both computer software and video piracy activities. Proprietary products are stolen and often copied, cloned, and offered for resale at reduced prices, thereby denying revenue to legitimate business. When investigating these crime scenes, look for duplication, recording media, and packing materials.
Evidence might be uncovered from the following:
Software cracking items, E-mail transmissions, chat logs, Internet activities logs, product serial numbers, etc.

Computer threats and instructions

Major issues concerning computer users are threats involving the proliferation of viruses, worms, and Trojan horses.
Considerable hardware and software in the form of firewalls and routers are deployed across the organization's computer facilities.
Large computer centers often maintain a security function that monitors both inside and outside threats to the information technology resources.
There are a number of hardware and software tools that can be employed to monitor the computer system resources. Evidence might be found in the following:
Address books, configuration files, e-mail transactions, executable programs, Internet activity logs, system logs, IP address and usernames, etc.

Telecommunication crimes

These type of crimes include software and video privacy, computer threats and intrusions, telecommunications fraud, and email issues.
Piracy is defined as the unauthorized duplication of goods protected by intellectual property law.

Software and video piracy

The Internet provides an available conduit for both computer software and video piracy activities. Proprietary products are stolen and often copied, cloned, and offered for resale at reduced prices, thereby denying revenue to legitimate business. When investigating these crime scenes, look for duplication, recording media, and packing materials.
Evidence might be uncovered from the following:
Software cracking items, E-mail transmissions, chat logs, Internet activities logs, product serial numbers, etc.

Computer threats and instructions

Major issues concerning computer users are threats involving the proliferation of viruses, worms, and Trojan horses.
Considerable hardware and software in the form of firewalls and routers are deployed across the organization's computer facilities.
Large computer centers often maintain a security function that monitors both inside and outside threats to the information technology resources.
There are a number of hardware and software tools that can be employed to monitor the computer system resources. Evidence might be found in the following:
Address books, configuration files, e-mail transactions, executable programs, Internet activity logs, system logs, IP address and usernames, etc.

Telecommunication Fraud

Both criminal activities and malicious acts can be performed in the telecommunications and networking area. The telecommunications environment includes wired networks, wireless network, the broadband network, and local telephone service.
Most local exchange carriers maintain a security staff for investigating theft of services, sabotage, and incidents involving company personnel.
Useful evidence would include the following:

- *Cloning software*
- *Subscriber database records*
- *Electronic IDs*
- *Financial records*
- *Phreaking manuals*
- *Internet activities records*
- *Telephone records*
- *Blue-box device*

E-Mail issues

A number of issues can be associated with the e-mail system. These consist of threats, staling, harassment, fraud, phishing, span, etc. Corporate e-mail can be the vehicle for sexual harassment, pornography, violations of company policies, and the list is also endless.
Corporate computer centers usually operate an e-mail server that maintains traffic information and log files on all transmissions.
Evidence types would include:

- *Address books*
- *Diaries*
- *E-mail transmissions*
- *Financial records*
- *Graphic Image/photos*
- *Internet activity*
- *Legal documents*
- *Telephone and cell phone records*
- *E-mail system logs*
- *Victim research data*

Personal Crime Categories

Computer and electronic devices usually do not play a prominent role in these type for crimes; however, circumstantial evidence obtained from electronic devices can play a major part in investigating these types of crimes.

Domestic Violence

It is defined as physical and/or emotional harm suffered by a person who is a family member of, or residing in the same home as , the offender who cause the harm or injury. Considerable supporting evidence might be found on computers, e-mail, cell phones, and personal digital assistants that located at the crime scene. Evidence sources could include the following:

- *Address books*
- *Diaries*
- *E-mail transmission*
- *Financial records*
- *Medical records*
- *Telephone and cell phone records*
- *Police report history*
- *Neighbors and relatives*

Extortion

It is used to obtain property or money by the use of violence, threats, or intimidation. Extortion can be related to other crimes, such as kidnapping and threats. E-mail transmissions and Web traffic can be subpoenaed from Internet services providers. Cell phone traffic could be a source to establish time, date and location information

Evidence sources could include the following:

- *Date and time stamps*
- *E-mail transmission*
- *Internet activity logs*
- *History logs*
- *Temporary Internet files*
- *User names*

Personal Crime Categories (cont.)

Gambling

It is the unlawful engaging in playing, operating, or assisting in operating a game of chance for money or some other stake. Gambling can be related to organized crime. Investigative techniques include following the money through financial organizations and looking at e-mail and telephone records to identify participates.

Evidence sources could include the following:

- *Address books*
- *Calendar*
- *Customer database*
- *Play records*
- *Electronic cash*
- *E-mail transmissions*
- *Financial records*
- *Internet activity logs*
- *Online financial institutions*
- *Sport-betting statistics*

Controlled Substances

Drugs and certain other chemicals, both narcotic and non-narcotic, which come under the jurisdiction of federal and state laws regulating their manufacture, sale, distribution, use, and disposal are designated controlled substances. Customer database can often be located on laptop computers. Cell phone data may contain contact numbers for customers, suppliers, and runners and cell phone rescores can show time, data and called numbers. E-mail servers could contain evidence of activities.

Evidence sources could include the following:

- *Address books*
- *Calendar*
- *Database*
- *Drug recipes*
- *E-mail transmissions*
- *False identification*
- *Financial records*
- *Internet activity logs*
- *Prescription form images*

Personal Crime Categories (cont.)

Prostitution

It includes sex offenses, including attempts, of a commercialized nature. Customer lists can be maintained on a computer. Data could include customers names, costs, addresses, and phone numbers.
Evidence sources could include the following:

- *Address books*
- *Biographies*
- *Calendar*
- *Customer database*
- *E-mail transmissions*
- *False identification*
- *Financial records*
- *Internet activity logs*
- *Medical records*
- *Web ads*

Death and Assault Investigation

Assault is the crime of violence against another person. Computer forensic investigation would be in support of the primary incident of assault or death. E-mail, cell phone , and Internet records can all contain valuable leads in these investigations.
Evidence sources could include the following:

- *Address books*
- *Diaries*
- *E-mail transmissions*
- *Financial records*
- *Images*
- *Internet activity logs*
- *Legal documents and wills*
- *Medical records*
- *Telephone and cell phone records*

Personal Crime Categories (cont.)

Child Exploitation

It could include trafficking, prostitution, molestation, abuse, and pornography. The Internet is the primary vehicle for transmission of pornographic images. Pornography evidence might be found on a number of Web sites and be also be attachments to e-mail transmissions.

Evidence sources could include the following:

- *Chat logs*
- *Date and time stamps*
- *Cameras*
- *E-mail transmissions*
- *Graphic edits and viewing software*
- *Graphic images*
- *Photographs*
- *Internet activity logs*
- *Movies*
- *File directories*

Cyber-Terrorism and Information Warfare

Cyberspace is defined as the global network of interconnected computers and communication systems. As the Internet becomes more pervasive in all areas of human endeavor, individual or groups can us the anonymity afforded by cyberspace to threaten, citizen, specific groups, communities, and entire countries, without the inherent change of capture, injury, or death to the attacker.

Cyber Terrorism

According to the FBI, cyber-terrorism is any “premeditated, politically motivated attack against information, computer system, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents”.

Cyberspace is constantly under assault since cyber-spice, thieves, saboteurs, and thrill-seekers break into computer and networking systems. These individuals steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and system, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and organizations.

Information Warfare

It is a kind of warfare where information and attacks on information and its systems are used as a tool of warfare. Information warfare may include transmitting propaganda to enemies to convince them to give up, and denying them information that might lead to their resistance.

Information warfare, proactive and reactive, could include the following activities.

Bombing a telephone switching facility
Destroying the telephone switching facility’s software
Hardening and defending the switching facility against air attack
Using an antivirus program to protect the facility’s software.

Forensic Accounting

It is accounting that is suitable for legal review by including data that has been arrived at in a scientific fashion. Forensic accounting techniques include auting for fraud, investigative techniques, court and legal proceedings, rules of evidence, legal processes, money tracing, valuation methods, and investigating mergers and acquisitions.

Forensic Account

Forensic accounting incidents fall into one of four categories:

- ❖Economic damages
- ❖Fraud and other forms of economic crime
- ❖Business valuation
- ❖Family law

Forensic accountants utilize an understanding of business information and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and investigative techniques, and litigation process and procedures to perform their work.

Corporate Security and Computer-Use Policies

Most violations that occur in the corporate environment do not require law enforcement intervention. Most incidents involve a violation of a corporate security policy or an official computer-use policy.
A policy designates a required process or procedure within an organization.

E-mail and Internet users are particularly tempted to download malicious code from e-mail attachments and hostile Web pages. Users also tend to download and install applications including freeware, shareware, beta or demo tryouts, and instant messaging from the Internet, which could involve licensing and security issues. Information obtained from visit Web sites may be inaccurate, misleading, or hateful, leading to the need for quality control, copyright awareness, and /or filtering of websites.

E-mail and web monitoring should address poly violations in the following areas:

- *Software downloading*
- *SPAM control*
- *Inappropriate material*
- *Intellectual property.*
- *Viruses, worms, and Trojan horses*
- *Malicious intruders*
- *DoS and DDoS*

Corporate Security Investigations

Members of the organization's security team could be responsible for investigations that involve violating detection and evidence collection. They may also be responsible for restoring systems to a production status with the assistance of Information Technology services. Team members must be thoroughly trained in the proper steps required for a successful computer forensic.

Note that cyber crimes can be categorized as premeditated or inadvertent.

Evidence collection, logging and security must be in accordance with the standard enforcement type of investigation because the corporate incident could become a criminal matter.

Corporate Security and Computer-Use Policies (cont.)

Computer –Abuse Investigations

Internal computer-abuse investigations usually involve several phases. This could involve human resource and/or senior management. If warranted, an investigation is initiated that cold include the following steps:

Define the scope of the investigation
Document and maintain a log of investigation activities
Secure computer and electronic devices
Document hardware and software configurations of a system
Collect and print any results that show misconduct.
Etc.

Four examination steps would be appropriate, usually based on the specific type of allegation.

Step1: Examine Web browser. Look at subject lines and addresses to identify trivial or minimal, non-work related Web activity. This evidence might be located in the following areas:
Cookies, cache, bookmarks, history, Windows swap files, Web mail

Step 2: Examine e-mail. Look at trivial, minimal no-work related e-mail on various clients. Evidence may be found in folder indexed, attachments, or message content.

Step 3: Examine UseNet: Search. Search trivial, minimal non-work-related UseNet activity. Check both UseNet Client and UseNet Activity.

Step 4: Additional review options: A good place to start is to examine all relevant log files. Examine directories for installed programs and executables to identify pirated code.

Compliance Analysis Investigation

Computer forensics involves preserving digital evidence for a criminal trial. Examiners must prove that there have been no changes to the data on the seized system.

Compliance analysis, on the other hand, is a simpler and faster process that involves viewing a defendant/offenders' file at "arm's length" (i.e., pornographic images, Word documents relating to identity theft, and temporary Internet files relating to identity theft, and temporary Internet file relating to credit card fraud. To do this, the investigator does not have to make a copy of the hard drive.

A computer forensic examination is usually conducted after a full investigation by a law enforcement agency and after a search or arrest warrant has been executed.

A compliance analysis "field kit" can be composed of the following items:

Analysis application: An application designed to scan files for images keywords, etc that can be launched from a CD-ROM or other removable medium.
USB flash drive
Various freeware/shareware/software tools:
Blank floppy disks and CDR/W
Labels, twist ties, and small evidence bags
Notebook or journal