Computer Forensic
Evidence Collection and Management

Chapter 1

Investigation Basics

Chapter Objectives

- Understand the basic concepts that make up the field of computer forensics
- Identify the four-step process for computer forensic investigations.
- Identify the different types of evidence that are elements of computer forensics
- Become familiar with the various risk, threats, and incidents that relate to computer forensics
- Look at the differences between criminal and business policy investigations

Introduction

- Technological revolution in communication and information exchange is taking place within business, industry, government and our homes.
- Americans use computer and networking facilities to bank and transfer money electronically.
- The internet, computer networks, and automated data systems provide an enormous opportunity for illegal activities.
- This computer technology is being used to commit crimes against persons, organizations, governments and property.
- Common criminals, drug cartels, and crime syndicates all use the network to conduct worldwide operations.
- Procedures concerning forensic practices must include evidence collection, examination, analysis, protection and reporting.
- Accounting forensic specialist are using computer technology to gaterh evidence for criminal prosecution.

Definition

- Forensics is formally defined as a study or practice relating to legal proceeding or augmentations.
- Traditional Forensics uses DNA evidence to identify suspects and victims to solve cases. Computer forensics uses computer digital technology to develop and provide investigative evidence to prove or disprove some allegations.
- Computer forensics is therefore described as those activities associated with the identification and preservation of computer or electronic evidence in support of some official or legal action.

Four basic situations where a computer device is involved in some type of crime:

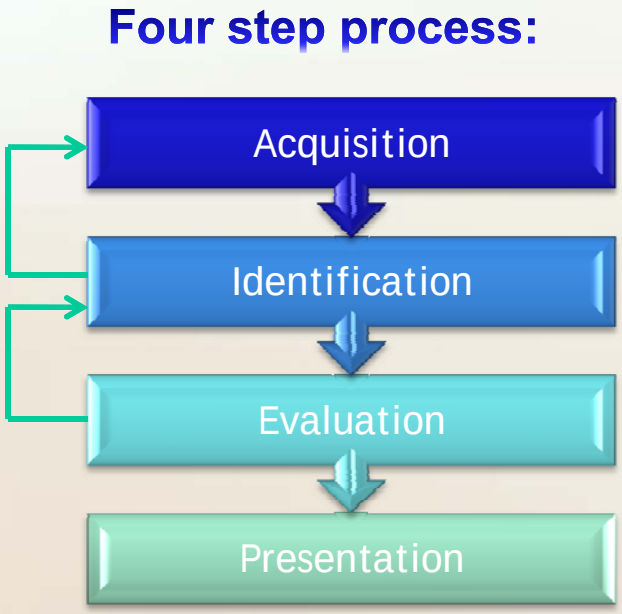
- Target of some illegal activity
- The medium through which the illegal activity is committed.
- Incidental to the commission of the illegal activity
- A combination of the previous three situations

Computer Forensic Science

- It was created to address the specific requirements of law enforcement that would leverage this new form of electronic evidence.
- It is the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media.
- Rather than producing interpretative conclusions (such as DNA), it produces direct information and data that may have significance in a case.
- Computer forensic examinations are conducted in forensic laboratories, data processing departments, and in some cases, the investigator's squad room.

Four step process

- Computer forensic investigations are very detailed and complex .
- Most important to the incident is the preservation of any evidence in its original form.
- Any modifications to the data and times stamps or the data itself must be avoided; otherwise, the usefulness of the evidence may be deemed inadmissible.



Acquisition

Two scenarios:

Incident has already occurred

- .

Incident is currently in progress

- A different approach and different tools would be required in the investigation

Chain-of-custody is the rout the evidence takes from initial procession until final disposition.

Identification

Evidence is presented in:
Physical: relates to the hardware or software components, such as a particular disk drive.
Logical: The relationship might include the address or location of the evidence on a disk drive.

** It is essential that all information relating to the steps taken and the computer instructions issued be documented, and can be replicated repeatedly.*

Evaluation

•A computer forensics investigator in concert with a computer forensics examiner must determine the relevance and validity of the evidence collected by the first responder.

•It is important to determine if the chain-of-custody has been maintained and also that the credibility of the evidence has not been tainted.

•It is essential that the forensic team only collect information that is relevant to the case being investigated.

Presentation

•During a formal presentation, the forensic team must decide as to the worthiness of the various pieces of evidence.

•Some evidence that may cloud the issue should be discarded during the presentation.

•A lack of knowledge on the part of any forensic participant will degrade the presentation in the other's favor. The evaluation's handling and processing of the electronic or computer evidence will be subjected to scrutiny by the opposing side of the argument. The chain-of-custody can be expected to be challenged.

What is Electronic Evidence?

•It is data and information of some investigative value that are stored on or transmitted by an electronic device, usually in digital form.
•The evidence is not readily viewable and requires various hardware and software elements to make it visible.
•The objective of the forensic team is to identify any evidence that might be found on the devices.

Type of evidence:

•Circumstantial evidence which is indirect evidence. It is the result of combining seemingly unrelated facts that when considered together, can be used to infer a conclusion.

•Physical evidence: is evidence that does not forget and is not confused by the excitement of the moment. It is direct, clear, and tangible evidence of something, requiring no assumptions or added logic to prove it to be true.

•Hearsay evidence consists of statements made out of court by someone who is not present to testify under oath at trial. This is evidence based on what someone has told the witness and not on direct knowledge.

Repeatability and Reproducibility

•The National Institute of Standards and Technology (NIST) requires that computer forensic test results be repeatable and reproducible.

•Repeatability is defined as the ability ot get the same test results in the same testing environment (same computer, disk, mode of operations, etc.)

•Reproducibility is defined as the ability to get the same test results in a different testing environment (different computer, hard disk, operator, etc).

•Quality control and documentation of the testing process are essential to ensure repeatability and reproducibility of test results.

•Every step of the process must be documented at a level of detail that will provide enough information that the testing process, form setup to completion , could be repeated and analyzed.

Who is at risk?

•Crime is everywhere and the Internet is providing additional avenues for individuals to engage in illegal activities.
•The internet is available to every one.
•Criminals believe that they can remain anonymous and escape detection and prosecutions.

•The Internet is also used for activities that are not necessarily illegal.
•Use of the Internet at work may be a violation of corporate policies.
•Mino children may be exposed to situations that are not in their best interest.

•A computer forensic investigation might be initiated for a number of reasons.
    •Some suspected violation of company policies (employee Internet abuse, unauthorized disclosure of confidential information, inappropriate email use, use of company resources for personal use, etc)
    •Some criminal indecent
    •Effort to recover lost data.

Incidents

•A partial list of incidents using electronic devices that could occur in a commercial, educational, or government organization includes:

- *User or customer errors*
- *Intellectual properly theft*
- *Delays of processing data*
- *Loss of data or information*
- *Unauthorized disclosure of data or information*
- *Data duplication*
- *Corruption*
- *Breach of contracts*
- *Phone phreaking*
- *Safety-related issues*
- *Disloyal employees*
- *E-mail abuse*
- *Inappropriate network abuse*
- *Computer break-ins*
- *Pornography*
- *Sexual harassment*
- *Blackmail*
- *Errors in billing*
- *Disclosure of confidential information*
- *Loss of operations.*

Threats

•The Internet has become the vehicle for numerous threats against business enterprises, government, and private citizens. Many of these threats are originating in foreign countries. These threats may originate from criminals, terrorist, students, organizations, business and the general population. A short list of threats that might originate on the internet includes:

- *Fraud against customers, suppliers, and employers*
- *Repudiation of sales*
- *False claims*
- *Identity theft*
- *Money laundering*
- *Piracy*
- *Child pornography*
- *Child exploitation*
- *Sabotage*
- *Denial-of-service(DoS) attacks*
- *Hacking*
- *Trojan horses*
- *Worms*
- *Viruses.*

Many of the listed Internet activities may result in criminal prosecution and require sophisticated and lengthy electronic and computer forensic investigations.

Criminal Activities

•The use of electronic and compute devices by the criminal element is increasing daily, as is the use of the internet to commit a wide variety of crimes.
•The use of computer forensic evidence is of major significance for both corporate and criminal investigations.
•Common criminal activities involving major crimes that could be addressed using electronic and compute forensics in the investigations include:

Murder Kidnapping Theft Assault Staking Burglary
Espionage Forgery Drugs Organized crime Prostitution
Robbery

These investigations would be in direct support of the normal investigative processes and other supporting forensic categories, such as DNA identification.

A case of an employee accused of improper accounting practices might well turn into a fraud or theft issue.

A new filed of forensic accounting is emerging as a source for financial system investigations. Forensic accounting focuses on the evidentiary nature of accounting data.
Topic includes:

- *Accounting fraud and fraud auditing*
- *Compliance, due diligence, and risk assessment*
- *Detection of financial statement misrepresentation and tax evasion*
- *Bankruptcy and valuation studies*
- *Money and information laundering*
- *etc*

Network and Computer Center Threats

•There are many opportunities for threats and miscellaneous incidents to occur in the computer and networking environment. This is particularly true in the internetworking environment, where attackers, crackers and hackers abound.
•Threats can be listed in generic terms; however, they usually involve fraud, theft of data, destruction of data, blockage of access, and carelessness. Investigations of these incidents can be very difficult and usually require a forensic scientist's expertise.
•The must common networking threats to an organization include the following:

Virus, worm, Trojan horses
Device failures
Internal attackers
Equipment theft
External hackers
Natural disasters
Industrial espionage

There is information on the Internet that provides instructions on how to attack almost any type of protocol, OS, or hardware environment. After identifying the various threats, the next step is to identify the various computer and networking components that compose the treat environment. This includes:

•Computer, servers, PCs, and administrative workstations
•Communication circuits
•Router, gateways, and switches
•Hubs, media access units (MAUs), repeaters, and bridges
•Modems, data service units (DSUs), and network termination 1 (NT1s)
•Front-end processors, communication controllers, and multiplexers
•Network and operating system software
•Application software
•Power and air-conditioning systems.

Proactive vs. Reactive Policies

•Policies are plans or courses of action deigned by organizations to influence and determine decisions and actions for some particular situation.

•*Proactive policies establish expected behavior in anticipation of some incident*
•*Reactive polices happen after some incident occurs and are, therefore, too late to impact some situation*

White-Collar and Blue-Collar Crimes are on the rise. Accounting fraud is becoming a nationwide issue.
Accounting forensic specialist are using computer technology to gather evidence for criminal prosecution. These subject matter experts must often work with computer forensics investigators and examiners to extract pertinent evidence form compute devices.

There are numerous federal and state laws and acts that have been enacted to counter Internet, computer and electronic crimes.