

Criminal Investigation,

Seventh Edition

Chapter Eighteen

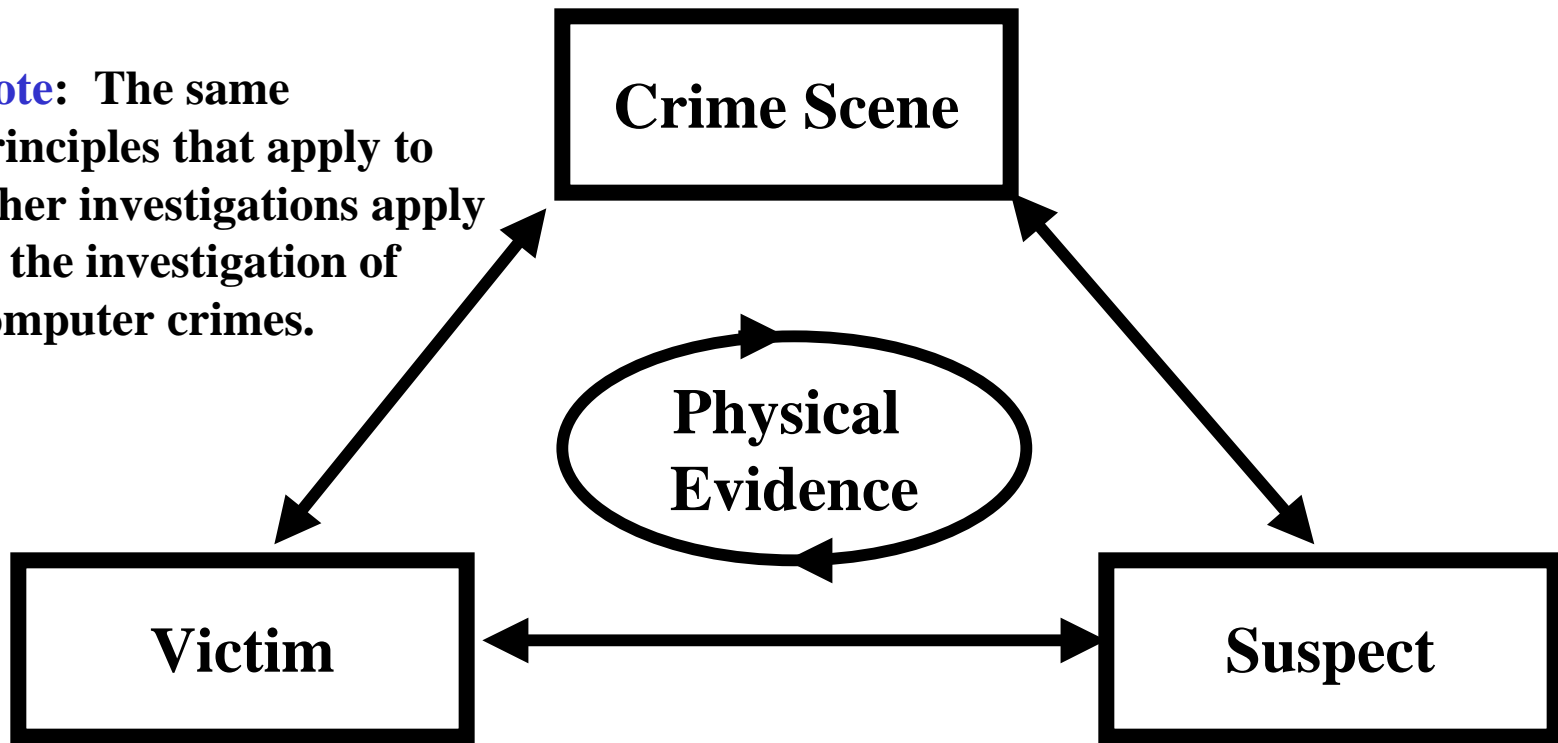
Computer Crime

Future of Computer Crime

- Crime against and with a computer is a growing field. Additionally, investigators need to know how to use a computer to investigate crimes.
- This section is presented in three primary areas:
 - Crimes against a computer (target).
 - Crimes with a computer (instrumentality).
 - Investigative use of a computer.
- This section makes use of the text and *Digital Evidence and Computer Crime*, Eoghan Casey, Academic Press, 2000.

Locard's Exchange Principle

Note: The same principles that apply to other investigations apply to the investigation of computer crimes.



Investigators work to make connections between the suspect and the victim, as there are more connections between the crime and the victim the chances of a successful prosecution increase.

Digital Evidence

1. Digital evidence can be duplicated exactly and the duplicate can be examined just as the original – thus avoiding possible damage to the original.
2. It is possible to determine when digital evidence has been altered.
3. Digital evidence is difficult to destroy, even if it has been deleted.
4. When individuals work to destroy digital evidence, copies can remain that they are not aware of.

Digital Evidence



Computers are generally connected to a system and much of the evidence available from computers can be obtained from the systems that the local computer can be connected to or with as part of the system.

Digital Evidence

- When seizing evidence investigators need to take into account that the following items are of evidentiary value:
 1. Hardware as contraband or fruits of the crime.
 2. Hardware as an instrumentality.
 3. Hardware as evidence.
 4. Information as contraband or fruits of crime.
 5. Information as an instrumentality.
 6. Information as evidence.

Computer Crime Definitions

- **Application** – Software that performs a specific function or gives individuals access to Internet/network services.
- **Bulletin board system (BBS)** – An application that can run on a personal computer enabling people to connect to the computer using a modem and participate in discussions, exchange e-mail and transfer files. This is part of the Internet.
- **Computer Cracker** – individuals who breaks into computers much like safe crackers break into safes. They find weak points and exploit them using specialized tools and techniques.

Computer Crime Definitions

- **Cookies** – a cookie is a small piece of information that is sent to a user's web browser by a particular web site's server. The information is saved on the user's hard drive in a file and has a set expiration date, which may be so far into the future that in effect it will not expire. A cookie keeps track of what sites a computer has visited by providing users with unique identifiers. Cookies can be helpful, as they allow a web server to “remember” specific information about a user. Cookies can also be used by law enforcement during a computer investigation to view a history of potentially illicit activity while the suspect was on the internet.

Computer Crime Definitions

- **Cyberspace** – refers to the connections and conceptual locations created using computer networks. It has become synonymous with the Internet in everyday usage.
- **Cybertrail** – any convergence of digital evidence that is left behind by a victim or an offender. Used to infer behavioral patterns.
- **Data-link Layer** – Provides reliable transit of data across a physical link using a network technology such as Ethernet, encapsulates data into frames or cells before sending it and enables multiple computers to share a single physical medium using a media access control method like CSMA/CD.

Computer Crime Definitions

- **Digital evidence** – encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator.
- **E-mail, or email** – A service that enables people to send electronic messages to each other.
- **Ethernet** – A local area networking technology to control access to the physical medium, a standard that allows connection of computers.

Computer Crime Definitions

- **Internet** – A global computer network linking smaller computer networks, that enables information sharing via common communication protocols. Information may be shared using electronic mail, newsgroups, the WWW, and synchronous chat. The Internet is not controlled or owned by a single country, group, organization or individual. Many privately owned networks are not a part of the Internet.

Computer Crime Definitions

- **Internet/network service** – A useful function supported by the Internet/network such as e-mail, the Web, Usenet, or IRC. Applications give individuals access to these useful functions.
- **Internet Service Provider, or ISP** – Any computer or organization that provides individuals with access to, or data storage on, the Internet.
- **Internet Relay Chat (IRC)** – An Internet service that enables individuals from around the world to convene and have synchronous (live) discussions.

Computer Crime Definitions

- **Modem (see Modulator/demodulator)** – A piece of equipment that is used to connect computers together using a serial line (usually a telephone line). Converts digital data into analog signal into digits that a computer can process.
- **Network Interface Card** – A piece of hardware used to connect a host to the network.
- **Newsgroups** – The online equivalent of public bulletin boards, enabling asynchronous communication that often resembles a discussion.

Computer Crime Definitions

- **Port** – A number that TCP/IP uses to identify Internet services/application.
- **Router** – A host connected to two or more networks that can send network messages from one network to another.
- **Search Engine** – A database of Internet resources that can be explored using key words and phrases.
- **Software** – Computer programs that perform some function.

Computer Crime Definitions

- **Synchronous chat network** – By connecting to a synchronous chat network via the Internet, individuals can interact in real-time using text, audio, video and more. Most synchronous chat networks are comprised of chat rooms, sometimes called channels, where people with similar interests gather. An asynchronous “chat” is similar to a newsgroup or bulletin board where messages are left and others may respond to the note. In synchronous chat people chat with each other, in asynchronous “chat” the people are not “chatting” at the same time.

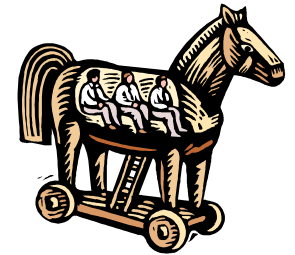
Computer Crime Definitions

- **Usenet (User's Network)** – A global system of newsgroups that enable people around the world to post messages to the equivalent of an online bulletin board.
- **World Wide Web (WWW)** – A service on the Internet providing individual users with access to a broad range of resources, including e-mail, newsgroups and multimedia (images, text, sound, etc.).

Crimes Against a Computer (Target)

- The computer is the target of the crime. Individuals commit crimes against what is stored in the computer or the uses of the computer. Examples include Trojan Horses, Salami Techniques, viruses, and others. Each of these will be discussed in this section.

Types of Crimes



- Trojan Horse:
 - Replaces the normal software with a program that captures every password entered into the program. The criminals then use the passwords to gain access to otherwise secure programs.
- Packet Sniffers:
 - Sits on or in the computer and keeps track of passwords and credit card information entered in or sent along through the computer. The criminals then use this information to commit crimes.

Types of Crimes

- Salami Techniques:
 - Takes small amounts of funds from numerous accounts and deposits them in a different account. In the case of a bank it may take a small amount of the interest earned from each account and deposit it in another account. Given the number of accounts in a large bank the funds mount up.

Types of Crimes

- Back Doors:
 - A programmer puts a way for the author of the program to later enter into the program through a different way, a hidden way. This access can be used for stealing funds, accessing information or other criminal activities.
- Logic Bombs:
 - The program is designed to operate only at a specific time or upon the entering of specific information. The entry of this information then allows the individual to use information for illegal purposes.

Types of Crimes

- Viruses:
 - A computer virus is a rogue program that is secretly inserted into a normal software program or into the computer's operating system. The purpose of the virus may vary, but generally the virus corrupts the computer by destroying the hard disk, erasing the hard disk, sending e-mail to others (with the virus attached) and other activities.
 - A virus can be used to threaten or extort actions or funds from others.

A Computer Virus

Virus
Created

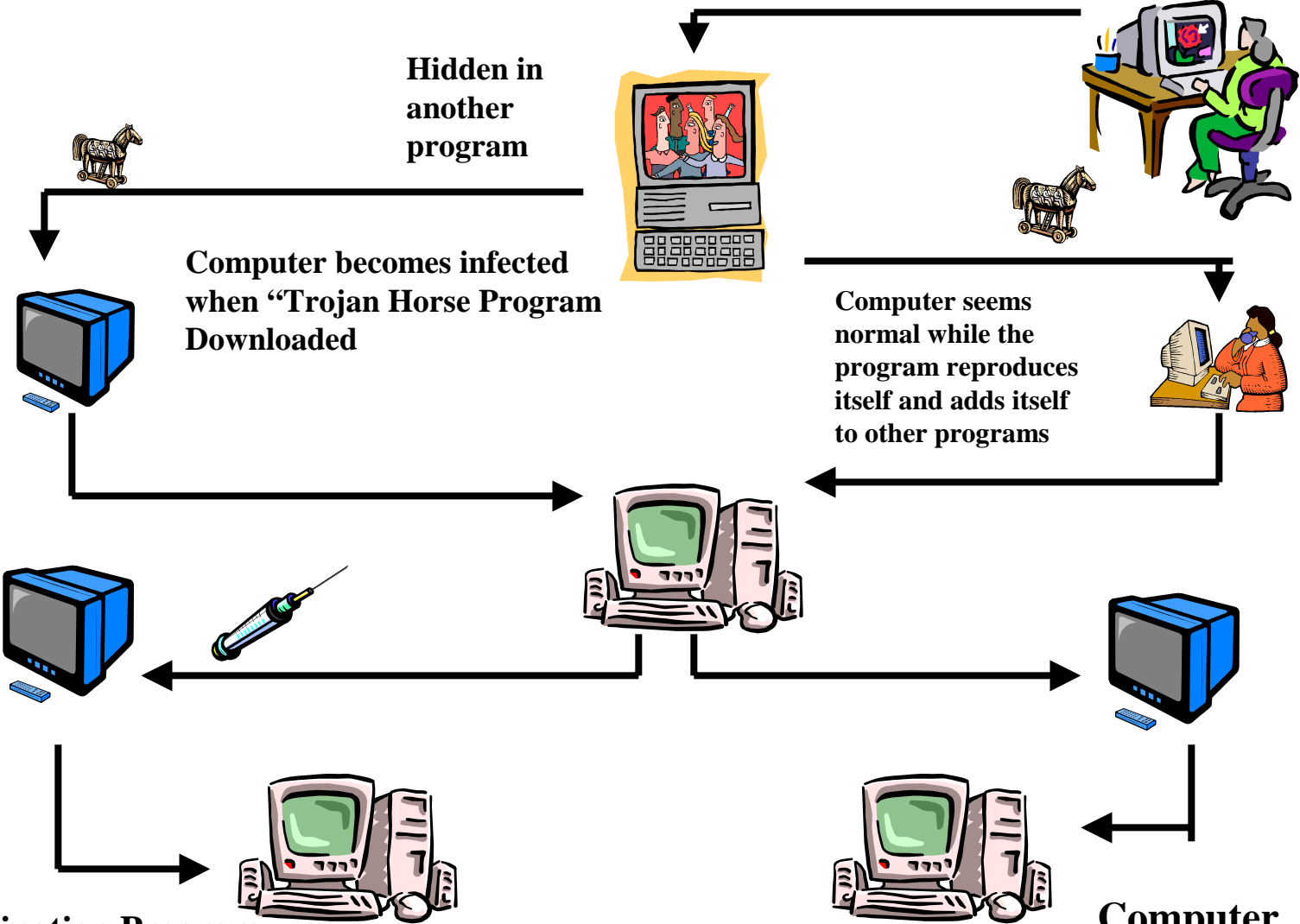
Hidden in
another
program

Computer becomes infected
when "Trojan Horse Program
Downloaded

Computer seems
normal while the
program reproduces
itself and adds itself
to other programs

Vaccination Program
Removes Virus

Computer
Corrupted



Types of Crimes

- Hacking:
 - Unauthorized entry into a computer system. Once entry is gained the “hacker” may use the access to compromise the system, extort funds, destroy the system and other activities.

Crimes with a Computer

(Instrumentality)

- Computers used as a way of committing a crime. Examples include using the computer to commit a con game, send illegal material, threaten individuals and other activities.
- In some cases it is difficult to determine if the crime involves the use of the computer as an instrumentality or if the computer is a target. For purposes of the investigator and the student the difference is artificial and is simply a means of trying to distinguish types of computer crimes.

Scams

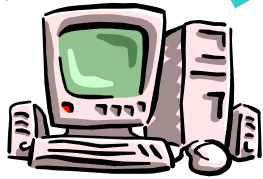
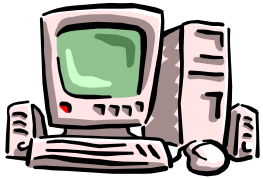
- Web Auctions – selling items and not delivering the goods.
- Internet services – charging for services that are ordinarily free of charge.
- Selling of goods and not delivering the goods.
- Pyramid and multi-level marketing.
- Work-at-home plans.
- Prizes and sweepstakes.
- Other methods of supporting criminal enterprises.
- Invasion of privacy.

E-Mail Forgery and Tracking

- Electronic mail is similar to regular mail in many ways. There are computers on the Internet, called Message Transfer Agents (MTA), which are the equivalent of post officer for electronic mail. When you send an e-mail message, it first goes to your local MTA. Just as a post office stamps letters with a postmark, your local MTA puts the current time and the name of the MTA along with some technical information, at the top of your e-mail message. This e-mail equivalent of a postmark is called a Received header. Your message is then passed from one MTA to another until it reaches the destination MTA.

E-Mail

Sender



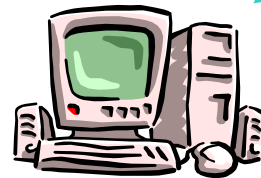
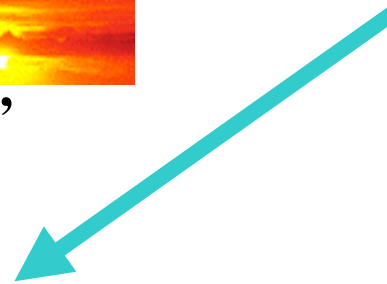
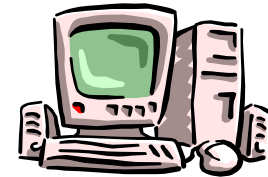
MTA1



“Black Box”



MTA2



Receiver

E-Mail

- Every MTA that receives the message puts a Received header at the top of message. An analogy is a stack of pancakes, with the newest pancakes on the top of the stack. The last computer to handle the message is at the top, with the first computer at the bottom. Thus to track an e-mail back to the sender you simply retrace the route that the e-mail traveled by reading through the e-mail's Received headers.

E-Mail

- It is possible to find a “trusting” computer and use a fake name and pretend to be someone you are not and send an e-mail to a person.
- MTA’s exchange e-mail using a standard protocol called Simple Mail Transfer Protocol (SMTP). A protocol is nothing fancy, just an agreed to way of “speaking.”

E-Mail

- In four broken English sentences (helo, mail from, rept to, data) one MTA (mta.sending.com) can say “helo” and ask another MTA (mta.receiving.edu) to pass an e-mail message on to its destination.
- Some people mistakenly think that using a free e-mail service like Hotmail will protect their identity. However, e-mail sent from these free services contain information about the originating computer that can be used to track down the sender.
- It is possible to track other senders using similar methods, even if the individual used IRC or USENET.

Investigative Use of a Computer

- Computers can be a valuable source of information for investigators. The uses include obtaining information, analyzing information, storing information and other uses.

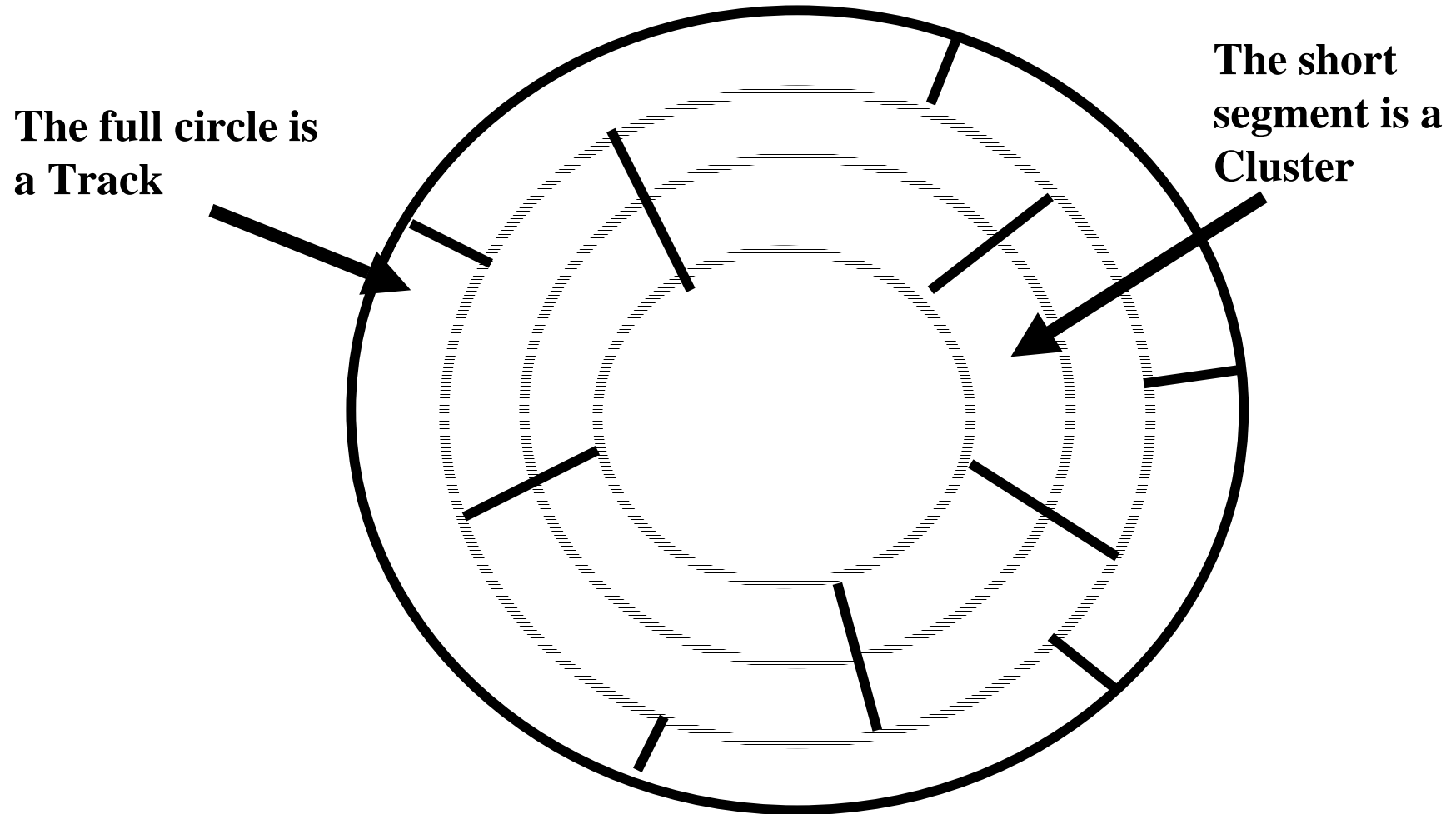
Use of Forensic Sciences

1. Detecting, processing and examining fingerprints and DNA.
2. Making an exact copy of digital evidence.
3. Collecting digitized data that is being transmitted through networks.
4. Using a message digest algorithm to verify that digital evidence has not been modified.
5. Signing digital evidence digitally to affirm that it is authentic and to preserve chain of evidence.
6. Determining the unique characteristics of a piece of evidence.

The Computer as Evidence

- When a computer user erases a file on the hard disk, what they actually erase is the computer address for the piece of evidence. The actual file continues to exist on the hard disk until it is erased or over-written by the computer. The disk has tracks and clusters. A track is similar to the track on an old vinyl record and a cluster is a short part of the track. However, computer track does not spiral around the disk as an old vinyl record track would.

Computer Disk



Computer Disk

- The disk can hold a lot of information. The “address” to the cluster is erased, but until the cluster is actually destroyed by restructuring the disk (defragging) or by actually erasing the information.

Searching the World Wide Web

(WWW)

- The Web provides a source of valuable information. For a list of resources and sites that are of value, visit my web site at <http://clem.mscd.edu/~neesii> Examples of resources include those listed below.
- **Academy of Forensics Sciences**

Membership includes physicians, criminalists, toxicologists, attorneys, dentists, physical anthropologists, document examiners, engineers, psychiatrists, educators and others who practice and perform research in the many diverse fields relating to forensic science.

Searching the World Wide Web

(WWW)

- **American College of Forensic Examiners**

The American College of Forensic Examiners (ACFE) is a private, nonprofit, tax-exempt scientific and professional society. This website contains information on membership, certification, conferences, discussion groups, and online publications.

Searching the World Wide Web

(WWW)

- **American Society of Crime Lab Directors**

The American Society of Crime Laboratory Directors (ASCLD) is a nonprofit professional society devoted to the improvement of crime laboratory operations through sound management practices. Its purpose is to foster the common professional interests of its members; to promote and foster the development of laboratory management principles and techniques; to acquire, preserve and disseminate information related to the utilization of crime laboratories; to maintain and improve communications among crime laboratory directors;

Searching the World Wide Web

(WWW)

- **American Society of Crime Lab Directors**
(Continued) to promote, encourage and maintain the highest standards of practice in the field of crime laboratory services; and to to strive for the suitable and Proper accomplishment of the purposes and objectives of this professional association.

The End