Cyber Crime: Its Impact on Government, Society and the Prosecutor

An Aid for Assisting the Prosecutor in the Investigation, Trial and Conviction of the Cyber/Computer Criminal

Cyber Crime: Its Impact on Government, Society and the Prosecutor

Cyber crime has been increasing in complexity and financial costs since corporations started to utilize computers in the course of doing business.

As technology increases between governments that are involved in international business, criminals have realized that this is a cost effective method to make money.

This investigation and trial manual is meant to serve as a basic template on the lessons learned to prepare governments, and their prosecutors, for combating cyber crime. To delve deeply into computer technology requires both long study and technical expertise. Therefore, as in most crimes that are technical in nature, or have technical aspects to them, such as bank fraud, murder investigations that require the analysis of blood and spatter techniques, gun-shots that require extensive ballistics investigation, experts are advisable for use as an aid in directing your investigations, to act as a special aide in preparing for trial, and as an expert to testify in that trial.

However, experts are not absolutely required, particularly in identifying basic components that make up a cyber crime, and on how to prove the elements of that case. We all know that computer crimes can run from the simple to the ultra sophisticated. This does not mean they are not solvable, and explainable to the judiciary during any trial. The complexity in these crimes should not be feared. All that is required is for you to understand the basic concepts explained in this manual, follow its simple rules and use that knowledge you have acquired. You will then be able to adequately investigate, prepare and put on any case.

External Cyber Attacks

External cyber attacks are increasing in frequency and causing extensive damage to companies and organizations. Cyber criminals have also organized into criminal groups that will cause damage for the challenge, pay, extortion, blackmail, etc. External attacks are typically launched from the Internet and circumvent the poor security controls of a government or corporation.

Internal Cyber Threats

The internal cyber threat is the most damaging to an organization due to the insider knowledge that an internal source has of an agency or company. An example of an internal employee who caused grave damage to an organization is of a police officer that used his inside knowledge of his law enforcement organization and its network to steal sensitive information that he then exchanged with a foreign power for money.

Malicious Software

Viruses: Software that attaches itself to a normal file and then reproduces itself to cause damage to a computer system or network.

Worms: Software that looks for vulnerabilities in a computer system or network and then reproduces itself.

Trojan horse: This is a program that appears to be a normal program but in reality is used to introduce a malicious program to a computer system or network.
Backdoors: Programs that are placed by cyber criminals to gain access to a computer system or network at a later date and time.

Viruses

This malicious software can be transported by a variety of mechanisms like email. The best protection against viruses is to ensure that all systems have the latest anti-virus software.

E-Commerce Fraud

Criminals use the Internet and computer to defraud victims by posting items that do not exist or are damaged. E-Commerce Fraud is growing at an increasing rate due to the availability and use of the Internet to conduct commerce.

Phishing/Identity Theft

Phishing involves the use of email or web pages to convince victims to reveal their personal or financial information. The stolen information is then used for the criminal's benefit.

Web Hacking

Cyber criminals use web hacking to deface government or corporate web sites. This activity is conducted to embarrass and show that the agency or company has weak security.

Hacktivism

Hacktivism involves the use of computers and the Internet to conduct resistance against a government or corporation. Hacktivists will conduct Denial of Service (DoS) attacks, intrusions, and web defacing to make a point about their political views.

Cyber Espionage

Cyber Espionage involves the utilization of computer systems to aid in the act of stealing sensitive information. Cyber Espionage is generally sponsored by a State or a corporation that is attempting to gain an advantage over a competing/adversarial corporation, espionage group or target state or their agencies.

Financial Impact of Cyber Crime

The overall monetary impact of cyber crime on society and government are unknown. Some estimates are that viruses and worms cause damages into the billions of dollars a year. It is estimated that only 5 - 10% of cyber crime is reported to law enforcement authorities. Reasons why cyber crime is not reported varies from not knowing that a

cyber incident has occurred to not wanting the public to know that a company's security data may have been exposed.

Cyber Crime Unit Requirements

The impact of cyber crime has been, and will be in the future, felt by all governments and economies that are connected to the Internet. Criminals will use the Internet, computers and other digital devices to facilitate their illegal activities. Prosecutors and police must have resources, training and equipment required to address cyber crime in order to keep current on this newest method of crime fighting.

History of Cyber Crime

Cyber Crime

Criminals have been using computers to facilitate their criminal activity since the advent of the digital age. Computers are a tool that criminals use much like a lock picking tool or a counterfeiting machine. Criminals have learned that computers provide an anonymity that has previously been unattainable in society.

Hacker Profile

"Hackers" is a term that is currently used to identify individuals who break into computers. Hackers can be any age, creed or nationality. Hackers have gained a negative image due to their exploits in the past few years. Hackers may commit their criminal activity for excitement, the challenge or monetary reasons. Hackers tend to be young males who have extremely high intelligence and curiosity. There has been an increase in the number of females that have acquired the skills to break into computer systems.

Hackers may organize themselves into hacking groups that will in some cases compete against other hacker groups in order to see who can exploit the most computers in a set time frame.

Cyber Criminals

The advent of the Internet allows cyber criminals to conduct illegal activity from a computer far removed from where the crime is actually taking place. A criminal can break into a computer network a continent away and steal credit card and banking information without having to be physically present at the scene. Criminals are using computers to conduct narcotics trafficking, child pornography, bank fraud, etc. using a computer and the Internet as a vehicle for illegal activity.

Law enforcement officials need to be aware of the many methods that criminals use and how to respond to this new and emerging crime scene.

Criminals also form into cyber gangs that may be dispersed across the continent. They utilize the specific skills of individuals who may be proficient at breaking into

databases. These cyber criminals typically use "handles" or "NIC's" to identify themselves to the group.

Case Study:

In 1999, an individual acquired unauthorized access to a nation's National Institute of Health (NIH) network. He accessed the network using a backdoor that he created on the system when he was an employee of the NIH. He downloaded documents that provided information on medical dosage recommendations for patients.

A subpoena was obtained for the Internet Protocol (IP) address of the computer that accessed the NIH network. A search warrant was obtained for the individual's residence. During the search, 3 computers were identified and seized as evidence. Analysis on the 3 computers identified the files that he had illegally downloaded from NIH along with child pornography. At his trial, his lawyers tried to suppress evidence based on search warrant procedures. The judge allowed the evidence and this individual was found guilty.

Cyber Crime Methodology

Cyber criminals typically follow a methodology when they are conducting their illegal activity. The process is based on their experience acquired through attempting to break into, and subsequently breaking into computer systems. What this provides law enforcement is a Modus Operandi (MO) with patterns that prosecutors and police can use to build their case. Law enforcement officials should establish databases on the MO of cyber criminals in their sectors.

Cyber criminals will typically need to use a computer network that is difficult if not impossible to identify. This is done to make it difficult for law enforcement to identify the perpetrator of the cyber crime. Cyber criminals will "hack" into a victim computer or will use cyber café's to commit their illegal activity.

Role of Computers

- Victim
  - A computer that is the object of an intrusion or unauthorized activity.
- Instrumentality
  - Computers that are used to conduct illegal activity.
- Evidence
  - Computers that are used to store evidence of the crime.

A Closer Look at Methodology

- Hackers will initially conduct intelligence gathering during the first phase of their illegal activity.
- They want to learn network range, extranet connections, etc.

- Hackers next conduct network discovery to identify the number and operating systems of the target victim's computer network.

- Hackers will also conduct host enumeration in order to identify vulnerabilities that exist of the system.

- The computer's vulnerabilities will then be exploited by the criminal.

- Cyber criminals will also install password crackers on the network. These "crackers" will allow them to "break" the passwords of the authorized users.

- Once the network has been compromised, cyber criminals will usually install "sniffers" that allow them to capture user id/passwords and other sensitive information.

- Hackers may use stegonagraphy in order to hide important data from law enforcement personnel.

- Stegonagraphy is very easy to use with automated software.

What is Steganography?

Steganography or stego is the science of hiding information. Steganography is derived from the Greek word for *covered writing* Stego is used by narcotics traffickers, child pornographers, terrorists and other assorted criminals to hide messages. The use of stego is increasing as individuals and organizations engaged in criminal activity realize the benefit of hiding their information from law enforcement.

A History of Steganography

Steganography has been around since the dawn of man's history. The Ancient Greeks hid messages by scraping the wax off of tablets, writing on the wood, and then covering the message with a new coat of wax. The message was thus hidden from plain view.

In the modern ages, intelligence agencies have used, among other techniques, micro-dots to hide their messages. The advent of digital technology has refined stego to a new level. Computers now make it possible to "hide" documents, pictures, etc… inside of another document, picture, music file. The hidden information can be stored on a computer, removable media or e-mailed.

There are no laws or regulations that bar the use of steganography to hide information.

Detecting Steganography

The detection of steganography is difficult and there are not many tools that will provide the investigators with conclusive information to the presence of stego.

One method would be to compare file size. A "suspect" file that contains hidden data "MAY" be larger than the original. Investigators can on occasion "SEE" subtle changes in an image that is being used to hide data.

- In both of these cases, the original and the "suspect" file are required to make the comparison.

- Investigators, when conducting an analysis of a suspect system, need to be aware of the tools that are available to hide information.

- The possession of these tools by the suspect is an indication that this individual is using stego to hide data.

Stego Software

- S-Tools3/4 – Hides messages in BMP, GIF, WAV files.

- BMP Secrets – Hides messages in BMP files.

- Gif It Up – Hides messages in GIF files.

- StegoHide – Hides messages in BMP files.

- MP3Stego – Hides messages in MP3 files.

Law Enforcement's Response to Cyber Crime

The investigation of a cyber criminal is very similar to a traditional investigation. The major difference is that cyber investigations have a technology component that needs to be identified and addressed. Not identifying and reviewing the technical component is similar to not reviewing and leaving unexamined the materials contained in a file cabinet that is located in the criminal's home/office.

Investigative Technique

- Computer/Firewall/ Intrusion Detection System/Network Logs

- Data Interception and Monitoring

- Informants

- Search Warrants

- Digital Forensics

- Interviews

- Liaison with Internet Service Providers

Return on Investment

- Provides the IP address, date and time of unauthorized access.
- Provides information on what the hacker did while on the system.
- Provides information on the type of attack and data stolen.
- Provides information on what the hacker is doing.
- Allows investigators to conduct an on-going investigation.
- It may be difficult to read the data.
- Keep your eyes & ears on the Internet.
    - Group infiltration
    - IRC
    - Consensual recordings of audio and IRC
- Main PC for Search Warrants & Wiretap.
- Crucial to have good informants. Critical for recovering computers and digital media.
- Requires trained prosecutors and investigators to present the facts to a judge.
- Provides information on activity that occurred on the computer.
- Critical evidence may be located on the digital media.
- Training for digital forensics is long and expensive.
- Confessions are easier to obtain when the criminal is confronted by reality.
- Information on other cyber criminals.
- Completion of missing details.
- Can provide information on the location of cyber criminal.
- Can intercept data for the investigation.
- A defendant may not cooperate with Law Enforcement. It can provide all the material you need.

Law Enforcement Scene

Most law enforcement agencies recognize the need for computer literate personnel. Increased cooperation between the US and other governments is crucial for investigation. Crime extends beyond traditional borders. Crimes with this type of

scope in the crime make it difficult for local prosecution. Treaties of cooperation with other governments will be extremely helpful.

What Law Enforcement Can Do

They must combine technical skills & investigative experience into a unified group. They must provide national & global cooperation. They must apply more traditional investigative techniques along with the technical expertise that opens up cases. There must be a long-term commitment of resources, which assists everyone.

Legal Response to Cyber Crime

Cyber Crime Legal Approaches

Governments have passed a variety of laws to address the increase of computer crimes. The first computer crime statutes were passed in 1986. Local and regional areas have also passed laws to address cyber crime at their level. Local and regional laws generally mirror the national laws.

Large Nation Response to Cyber Crime

One nation created a Computer Crime & Intellectual Property Section (CCIPS) to formulate policy on computer crime. CCIPS is responsible for issuing country-wide guidelines on the search and seizure of digital data. Each individual Attorney General's Office has a specially trained prosecutor that is responsible for the prosecution of crimes where a computer is utilized.

Title 18, USC 1029 and Other Laws (Examples of national laws)

This law is designed to prosecute individuals for trafficking or trading passwords or credit cards numbers that they are not authorized to possess. The law prosecutes individuals who use software or hardware to produce or distribute passwords or credit card numbers. Criminals utilize credit card generators or trade stolen credit card numbers on the Internet in ever increasing numbers. They have to be stopped or the entire economy suffers.

Title 18, USC 1029 Penalties

Individuals convicted for violation of 1029 can be sentenced to 15 years in prison for the first offense.

Individuals convicted a second time for a previous violation of 1029 can be sentenced to 20 years in prison.

Title 18, USC 1030

This law is used to prosecute individuals who intentionally access a nationally protected computer without authorization.

Nationally protected computers are government computers and those determined by the government to be involved in interstate commerce. An example would be bank chain of locations that uses the Internet and has a system of computers to track their transactions. There must also be damage in excess of $5,000 or harm to public safety and/or national security. This law is also used to prosecute individuals for releasing viruses or worms that cause damage.

Title 18, USC 1030 Penalties

Individuals convicted for violation of 1030 can be sentenced to 15 years in prison. Individuals convicted a second time for a previous violation of 1030 can be sentenced to 20 years in prison.

Title 18, USC 1362

This law is used to prosecute individuals for willfully harming or destroying telecommunications systems. An example would be an Internet Service Provider. The act can also be used to prosecute individuals for planning to conduct the offense.

Title 18, USC 1362 Penalties

Individuals convicted for violation of 1362 can be sentenced to 10 years in prison for the first offense.

Title 18, USC 2511

This law is used to prosecute individuals for intentionally intercepting wire, oral and electronic communications. The law is also used to prosecute individuals who use equipment to cause communications to be intercepted.

Title 18, USC 2511 Penalties

Individuals convicted for violation of 2511 can be sentenced to five years in prison for the first offense.

Title 18, USC 2701

This law is used to prosecute individuals for intentionally accessing, without authorization, a facility where electronic communications are provided and stored.

Title 18, USC 2701 Penalties

Individuals convicted for violation of 2701 can be sentenced to two years in prison for the first offense.

Title 18, USC 2702

This law is used to prosecute individuals for intentionally disclosing stored electronic communications. This section provides for the prosecution of individuals who provide the information to unauthorized recipients of the data contents.

Patriot Act

This Act was passed in response to the attacks on the World Trade Centers in New York and the Pentagon in Washington DC on September 11, 2001. The Act supplements existing laws by expanding and increasing penalties for crimes committed with computers. The Act has a specific provision for cyber terrorism. The U.S. government is required to expand their cyber forensics capability.

The Act authorizes intercept voice communications on the Internet. It expands the definition of a "Protected Computer" to include computers in foreign countries. This was done to address the interdependence of computers on the Internet.

> Note: A significant problem with investigation of cyber crime is the lack of an established legal framework, particularly in an international setting. Jurisdictional issues and lack of laws in countries makes it extremely difficult to conduct investigations across national borders.

International Legal Framework

As previously indicated, a significant problem with investigation of cyber crime is the lack of established legal framework. Jurisdictional issues and lack of laws in countries makes it extremely difficult to conduct investigations across national borders. Cyber criminals utilize this dysfunction to their advantage. They "bounce" across numerous computer systems in countries without appropriate laws that address cyber crime.

Cyber Crime Incident Response

What is Incident Response?

Information systems (network devices, servers, hosts, etc.) are subject to malicious activity on a regular basis. Fortunately, the vast majority of attacks are unsuccessful. Incidents on networks and systems, whether from internal or external sources, will continue to challenge law enforcement officers and information security personnel. The challenges include how to respond, what persons/companies/local or regional authorities/country-wide authorities/international authorities or groups to notify, and to preserve "evidence".

An incident is typically caused by an anomalous event on a computer network. That event can be caused by an intruder who gains unauthorized access to a company email server or a hacker who causes a web face defacement of a victim corporation. When an incident by a hacker or criminal is detected, law enforcement personnel need to respond in a manner whereby the digital evidence is not going to be compromised by improper handling.

Prosecutors may need to issue subpoenas or warrants that allow law enforcement personnel to acquire the data of the investigation.

Why Incident Response?

In order to identify and recover from the breach of a corporation's network and have a process that law enforcement officers use, established procedures must be in place to mitigate the damage caused by the unauthorized criminal activity.

- Without a formalized process in place, critical information may not be properly identified or may be lost as evidence.
- These processes can be thought of as the Incident Response (IR) Cycle.
- The IR Cycle is critical for the proper acquisition and analysis of digital evidence.

What is an Incident?

In order to respond to an "incident", we must know what an "incident" is: An "incident" can be thought of as an "adverse event" that threatens the confidentiality, integrity or accessibility of a computing resource. An "adverse event" would be a negative action that can be observed. Examples being a reconnaissance of a network, a Denial of Service attack, unauthorized access to a corporate email server.

Incident Response

Unauthorized access is normally acquired in the following methods:

- Valid User Credential – A criminal/hacker may acquire a valid user ID and password from co-workers or by capturing the information from a computer network. Valid user credentials allow a criminal access without setting off many alarms.
- Vulnerable Services – Computer that are not "patched" or properly cared for are vulnerable to a variety of attacks by criminals or hackers. An individual can break into a computer and then create valid user credentials for themselves thus making it difficult for law enforcement officers to identify.
- Backdoors – A backdoor is typically a program that is created on a computer that provides unauthorized access to the computer. Backdoors can be created by hackers to allow themselves access to the computer when they want.

Role Computers Have in IR

Computers are used by criminals and hackers to conduct their illegal activity. Prosecutors and law enforcement officers need to know how to differentiate between the varying roles that computers have in computer crime.

- Victim: A computer that is the object of an intrusion or unauthorized activity. Critical evidence can be located on the system.

- Instrumentality: Computers that are used to conduct illegal activity. A hacker's computer is an example of an instrumentality. These systems can also have critical evidence of a crime and must be seized by law enforcement.

- Evidence: Computers that are used to store evidence of the crime. These can be the victim or hackers computer, which contain digital evidence that must be seized and analyzed by law enforcement.

Incident Response Cycle

- Preparation

- Detection

- Analysis

- Recovery

- After-Action

Preparation involves:

1. Incident Response Policy – Policy must be formulated that describes who responds.

2. Incident Response Procedures – This describes the actions that must take placed during an unauthorized incident.

3. Identification of Team – Certain personnel will be responsible for searching and seizing digital evidence, for analyzing the evidence, etc.

4. Training of Team – Without proper training, the team will not be able to properly respond to computer crime.

5. Equipment for Team – The proper equipment is vital to the success of a cyber investigation.

6. Liaison with law enforcement – Contact must be maintained with different law enforcement agencies due to the transnational nature of cyber crime.

7. Liaison with other CIRT's, ISP's, etc. – Liaison with government or corporate incident response teams is important due to the sharing of

information that can provide law enforcement officers with important information on hacker techniques.

Detection involves:

1. Identification of the incident. In order to investigate an incident, law enforcement officers must be aware that illegal activity has taken place. There are a number of mechanisms for this identification:

a. Intrusion Detection Systems (IDS). – IDS detect incidents and captures the information for analysis.
b. Honey pot's (traps) – Hardware and software that is used to identify the techniques that criminals are using to break into computer networks.
c. Unexplained high network bandwidth utilization. – A high use of a network can be a hint that an unauthorized individual has acquired access.
d. Unexplained user accounts. – User IDs that do not belong to any known personnel are typically a sign that an unauthorized individual has acquired access to the network.
e. Unexplained utilization of disk storage. – Low disk space on computer systems is another indicator of unauthorized access. Criminals/hackers typically use computer networks that they "hack" into to store or hide their criminal data.

2. Categorization of the incident. An incident must be categorized in order for the proper response to be conducted.

1. Malicious code. – In this kind of incident, viruses, worms or other software that is used by hackers must be analyzed to determine what kind of illegal activity is occurring.
2. Unauthorized Access – This type of incident is conducted when an intruder/or criminal acquires illegal access to the computer network.
3. Denial of Service. – A DoS attack is a criminal event whereby an individual or groups of individuals attack computer systems to cause damage.

3. Prioritization of Incident

Level 1 – Root or Administrator Account Compromise /Access.
Level 2 – User Account Compromise/Access.
Level 3 – Unauthorized access to a system.
Level 4 – Network or System Scanning.

Analysis involves determining what took place:

– Live System Forensics – This is the methodology of identifying and processing digital evidence from a computer that can not be turned off due to its critical function. It may be a computer that is used to run a hospital and thus can not be turned off due to the medical implications to patients. These systems are typically:

- Network Devices – Routers or switches that run a company.
- Servers – Critical systems that may be used to process a water treatment plant or electrical facility and thus can not be turned off.

– Traditional Computer Forensics – In most circumstances, law enforcement officers will be in a position to turn off a computer system that may contain digital evidence of a crime. In this situation, the computer is turned off and seized as evidence using proper forensic techniques.

– Stand-alone systems – These types of computers are typically individual workstations or laptop computers. They can also be portable devices.

– Reporting – The process of reporting the information that is identified is critical for law enforcement officers. Without proper reporting, important evidence may not listed for prosecution purposes.

Incident Response Issues – There are a number of issues that law enforcement officers need to be aware of when investigating cyber crime.

Operating Systems – No individual law enforcement officer can possibly know the many different operating systems that are in use. It is important that law enforcement offices learn as much as possible about the different operating systems that are in available.

– Microsoft – This is the most common and popular operating system in existence and will be seen extensively as evidence in cyber crime.

– Linux – This is a free operating system that is popular with hackers.

– Solaris – This operating system is popular in large corporations.

– Cisco – This operating system that runs on network devices like routers and switches can be difficult to operate and to locate digital evidence.

– PDA – Personnel Digital Assistants are popular and carried by narcotic traffickers, hackers and cyber criminals. Law enforcement officers must be aware that critical data are contained on these devices and that they must be seized.

"Live" System Forensics

What if the system that has been compromised cannot be powered down because it is has a critical business function? How do you respond to this incident? The response mechanism will be conducted on a "live" system. Typically, the following information should be gathered from a system that cannot be powered down:

1. System date and time. – The current date and time must be captured for evidentiary purposes. They show the date and time of the system and can be used to validate the date and time of unauthorized activity.

2. A list of currently running processes. – This list will show what programs are running on the computer. This is important if a virus or some other illegal program has been installed.

3. A list of currently open sockets. – This list will show what programs could be available for a cyber criminal to connect.

4. The applications listening on open sockets. This list will show the programs that have connections; they could be from a "hacker".

5. A list of the users that are currently logged on. – This list will show who is connected to the computer and from where.

6. A list of the systems that have current or had recent connections to the system. – It is critical to acquire this information because the cyber criminal may have already left the system and it is important to identify where he came from.

The following are the specific Windows and Unix/Linux operating system commands that must be used to gather the digital evidence that was just referenced. It is necessary to utilize a forensic floppy disk or CD in case the cyber criminal has altered any of these commands to delete or overwrite evidence.

	Windows	**Unix/Linux**
Establish a trusted shell	cmd.exe	*/bin/bash*
Record the system date and time	date/time	*w*
Determine who is logged on	Logged on	*w*
Record time/date stamps	dir	*ls*
Record open sockets	netstat	*netstat -an*
List Processes that open sockets.	fport	*lsof/netstat -anp*
List currently running processes.	pslist	*ps*
List systems recently connected	nbtstat	*netstat* *w*

Record system time	date/time	*script, vi*
Record the steps taken	doskey	*history*

Traditional Computer Forensics –The vast majority of law enforcement officer response will be on computer systems that have been turned off and seized as evidence. The following processes are a generalized view of what takes place during the forensic investigation:

- Physical image is made of the magnetic media. – A forensic image or copy is made of the evidence and the original is then stored. Proper forensic tools and techniques must be utilized during this process. If not conducted properly, critical evidence may be altered or destroyed.

- Logical image is made of the magnetic media. – A logical copy is made which will provide an investigator with the data that exists on the computer system. A logical image will not provide deleted files and other information that is crucial to an investigation.

- Physical image is restored to sterile media for processing. – If required, the forensic image is copied to another hard drives for processing. Never conduct forensic analysis on the original evidence.

- Physical image is processed for:

  - Directory Listing – This shows all the directory and files on the computer system.
  - Hidden Files – During the forensic analysis, hidden files are identified.
  - Deleted Files – Deleted files are recovered for analysis.
  - Encryption – A search is made for files that may be encrypted. A search is also made for passwords.
  - File Slack – A detailed analysis is made of file slack in order to identify critical data that may be stored on the computer.

Incident Response Cycle

- Containment and Recovery involves:

  - Identification of other systems that may be compromised – During the response phase, law enforcement officers may also need to identify other computers or networks that have also been the victim of cyber activity. In many instances, this will require a prosecutor to acquire subpoenas or search warrants.
  - Minimizing the impact to the network – It is important to minimize any additional potential damage to a computer that has been the victim of a

cyber crime. Law enforcement officers must do all that is possible to keep damage to a minimum.
- Restoring systems to normal operation – Once the computer has been forensically copied, it may require that the system be restored and returned to the owner.

- After Action Involves:

  - How did the incident occur? - It is critical to identify the nature of the attack and how they were able to circumvent security.
  - How to prevent similar incident from occurring in the future? - Information must be shared with other CIRT's, law enforcement agencies, etc. in order that preparation can be made to minimize the impact from similar attacks.
  - What worked/didn't work during the response? - Every incident response should be seen as a learning experience and law enforcement officers must learn from their mistakes in order that they don't repeat them in the future.

Case Study:

Victim Company's Information Technology (IT) director (hereafter referred to as Acme) receives a phone call from the Information Security (IS) director of a multinational corporation. The IS director advises the Acme IT director that they are monitoring unauthorized activity originating from the Acme network. The unauthorized activity involves the breach and access of the multinational company's internal network.

The IS director advises Acme that they have identified five (5) IP addresses originating from the Acme network. The IS director advises that one of the IP addresses, within Acme's network range, has contact information in Russia, based on the "who is" lookup. IS director and staff attempt to determine if an Acme employee is responsible for the unauthorized activity.

Acme IT staff locate two (2) of the five (5) IP's provided by the multinational corporation. The two devices identified are a Citrix server and a Checkpoint Firewall. Acme personnel are unsure of what actions to take to identify what activity is taking place. Acme brings in outside assistance.

A review of DShield.org logs reveal that 2 of the systems have been reported to the site for conducting unauthorized activity. If your IP address is listed, you have probably been compromised:

IP Address	Host Name
82.166.52.125 $^{65308}/_{65293}$	82-166-52-125.barak.net.il
62.101.69.61	
218.190.37.157	
82.182.99.32 $^{65238}/_{65237}$	1-1-7-48a.msp.mlm.bostream.se
218.197.191.123 $^{65228}/_{65227}$	
80.54.239.171 $^{65475}/_{65462}$	dq171.neoplus.adsl.tpnet.pl
220.49.236.43 $^{65218}/_{65197}$	YahooBB220049236043.bbtec.net
80.191.163.12 $^{3258}/_{3047}$	
213.22.90.229	a213-22-90-229.netcabo.pt
218.102.114.150 $^{65196}/_{65175}$	pcd582150.netvigator.com

A "live' analysis is conducted to identify ongoing activity from the two systems. Analysis identifies an IRC channel that is active. Traditional forensic analysis is conducted of the two identified systems. The rule set on the Checkpoint Firewall is set to ANY. Large amounts of Warez are located on the Firewall. Forensic analysis is conducted on the Citrix server. The analysis identifies numerous scanning and password cracking programs like nmap and l0phtcrack. Also located are large password files and Warez.

The forensic analysis also identifies that VMware has been installed on the Citrix server with Red Hat Linux 8 as the installed OS. An IRC server has been installed on

the Linux system. A review of the Firewall logs reveals. Acme's IT staff are contacted and asked if they had installed any of the scanning, password cracking, Vmware or Linux on the Citrix server.

Acme personnel respond that those programs where not installed by their staff. Forensic analysis of the SWAP file (Pagefile.sys) identifies numerous Linux commands being run and being used to conduct attacks against victim multi-national corporation and many others. Firewall logs were not being reviewed. No policy or process was in place to respond to incidents.

IT personnel did not recognize anomalous activity on their network that included massive bandwidth utilization. IT personnel did not even have a current network topology of their systems. It was a situation that was ripe for a cyber attack.

Computer Forensic Investigative Techniques

Computer Forensics – Why?

Imagine the following:

- You didn't recognize critical evidence or information.
- You could not locate vital data.
- You could not use any documents or records.
- You accidentally destroyed evidence.
- You now needed to resolve an allegation or an issue.

Now you should see why computer forensics are required.

Computer Forensics – What is it?

Definition: Computer forensics is the discipline of acquiring, preserving, identifying and examining digital media. It involves retrieving computer data in order to meet standards for admissibility as evidence in legal proceedings. Computer forensic data recovery is the basis for seizure of evidence in all computer-based investigations. Note: <u>The most critical component is that the original media CANNOT be altered.</u>

Computer Forensics

Advances in technology have made computers a ubiquitous device that is becoming indispensable for entertainment or work. Hard drive storage area has become so large that the computer can be thought of as the modern day filing cabinet. Just as a filing cabinet would be seized during an investigation, so must all computers and digital media.

Law Enforcement Response

Law enforcement authorities, ie. Police, Prosecutors, etc. must have trained and experienced investigators that know how to supervise or conduct proper computer forensics investigations. Investigations can receive great assistance from the evidence that is recovered from computers, personal data assistants and removable media (floppy disks, CD's, Zip disks).

95% of all information generated is in DIGITAL form

How Much Data?

- One Byte = 8 bits
    - One Byte = 1 character
- One Kilobyte = 1024 bytes
- One Megabyte = 1,048,576 bytes
    - One Megabyte = 1,000 -1,400 pages of printed text.
- One Gigabyte = 1,073,741,824 megabytes
    - One Gigabyte = 100,000 – 140,00 of printed text.

Computers Forensics

- Identify the perpetrator of the act, can be criminal or civil in nature.
- Identify the means and methods by which access was gained to the computer or network.
- Conduct a damage assessment of the victim computer.
- Preserve the evidence for judicial recourse.

Where is the Evidence?

- Removable Media: Floppy Disk; Zip Disk
- Hard Drive: IDE; SCSI
- CDROM
- Magnetic Tape
- Electronic Organizers

Computer Forensics – Issues

- Operating Systems

Microsoft
Unix
Linux
Cisco
Apple
Handspring

Examination of Evidence

- Reliability of evidence.
- Adherence to accepted protocols and practices (standards).
- Use of proven / accepted software.
- Ability to testify as to methods and results of analysis.
- Trained and certified computer forensics examiners.
- Proper training is crucial for testimonial purposes.

Exploitation of Evidence Requires:

Separating pertinent evidence from non-pertinent. There then must be an evaluation of the evidence for criticality and usability in judicial environment. There must always be a documentation of actions taken by the examiner.

Computer Forensics - Methodology

1. Chain of custody.
2. Forensic copy is made of the digital evidence with "hashing" (digital fingerprint).
3. Forensic copy is made to a sterilized media.
4. Forensic copy is processed for:
    - Directory listing
    - Key word search
    - Latent data
    - Hidden files
    - Email
    - Encryption

Digital Evidence

- Digital evidence is composed of three categories:
    - Active Data – Folders and files that are visible and available to the Operating System.
    - Ambient Data – Information that is composed of:
        1. Deleted files
        2. File slack

3. Random Access Memory (RAM) slack
4. Unallocated space
5. Metadata
6. Temp files

– Archival Data – Information that is backed-up and stored independently of the computer.

Forensic Software - EnCase

EnCase is a Microsoft based program that can make a forensic copy of the evidence and also create a "hash". The EnCase software is also utilized to conduct forensic analysis of the evidence file that is created

Digital Evidence

This is an example of an Active word document (credit card information) that can be viewed by the EnCase forensic software.

Credit Card Number	Expiration Date
4948 3939 4973 2094	12/05
3765 2906 1836 3947	1/07
3845 8276 1048 5097	4/07
3394 2093 9842 9829	8/08
2873 8872 1928 4487	12/08
3987 4730 4873 0938	4/07
3280 0983 8729 0973	3/06
2827 4830 7349 8283	5/07
7648 7436 2949 7493	5/05
3498 7638 3298 0947	3/06
6374 9872 0943 8734	2/07
3487 0837 9849 8393	4/09
3748 2987 5647 8127	5/08
4857 0938 7638 7649	8//08
8574 1287 4905 8729	7/09
3874 9876 2937 3487	4/07
5783 9832 0874 9832	7/06
3838 7382 9834 9032	9/09
5483 8763 6384 9263	3/05
3874 7483 9073 2389	8/07
3847 8973 2738 1028	1/06
3847 8730 3874 4987	8/08
9847 8758 7643 9874	3/08
8596 8739 3784 7638	2/05
3874 9850 2871 2973	6/06

EnCase can be utilized to examine Active, Latent and Archival data without altering the evidence. The EnCase software is utilized by most law enforcement agencies around the world for computer forensics.

Forensic Software - FTK

FTK is also a Windows based digital forensics program that is able to make forensic copies and "hash" the evidence. FTK is well known for software's ability to index data and process email. FTK is easy to use and provides an investigator the ability to view Active, Latent and Archival data without altering the evidence. FTK is also used extensively by law enforcement to process digital evidence.

Tools - I Look

I Look is a forensic analysis tool that combines functions, under a unified interface examination, that at one time you would use many different tools to perform analysis. An Explorer-like interface allowing you to view and navigate the file system as it originally appeared on the suspect computer. Three built-in search engines (standard, bulk search and indexed search modes) to utilize. Link points to investigator defined viewer technology. Inbuilt multi-format file viewing. I Look is generally restricted to law enforcement personnel; forensic personnel working for law enforcement agencies with a statutory role; military investigators

E-Mail Investigations

E-MAIL

E-Mail is probably one of the most pervasive communication mediums in world. It was estimated that over 12 billions email were sent every day in 2001. (Jupiter Communications) E-Mail can be received not only through the traditional means of the computer, but also through Cell-Phones, Kiosks, Pagers and Personnel Digital Assistants (PDAs). E-Mail is used by criminals to communicate, commit fraud, send threats to schools, etc. E-mail provides an individual with unprecedented anonymity. E-mail can be "spoofed" to appear to come from another individual or computer.

Law enforcement officials must be able to locate, retrieve, read and interpret e-mail when conducting an investigation. Reading and interpreting e-mail headers is a crucial to tracing the origination of a suspect's e-mail. E-Mail is usually formatted in ASCII text and is readable. Non-text files (pictures, movies, sound) can also be sent, but they are in binary format. Binary data can only be read with special software.

- There are three components required for an e-mail system:

    1. Mail User Agents (MUA) – Programs like Outlook, Outlook Express, Netscape Navigator, Eudora, etc.

    2. Mail Transfer Agents (MTA) – The servers that "send" e-mail to its intended destination. The Simple Mail Transport Protocol (SMTP) is normally used.

    3. Mail Delivery Agents (MDA) – The servers (that "receive" e-mail for a recipient. The Post Office Protocol (POP) and Internet Messaging Access Protocol (IMAP) are normally used.

    The three different components interact with each other in order to send and deliver e-mail.

Each machine adds its own header information to the original e-mail header information.

Spoofed E-mail

- E-mail can easily be made to appear to come from another person. This is known as "spoofing" e-mail.

- In order to "spoof" e-mail, the subject conducts the following:

  - 1. Finds an e-mail server that does not require authentication and telnets to port 25 (SMTP):
    - Telnet (IP ADDRESS of server) 25

  - 2. Enters the following commands:
    - HELO
    - MAIL FROM: (Sender fake e-mail address)
    - RCPT TO: (Recipient true e-mail address)
    - SUBJECT: (Subject of e-mail)
    - DATA (Information being sent)
    -

Investigating E-mail

In order to determine the "sender" of an e-mail message (spoofed or normal), the law enforcement official will need to view the e-mail header. The e-mail header provides details on the MTA's that were utilized to forward the e-mail that is being investigated.

- The header information provides the following information on MTA's:
  - 1. IP address
  - 2. Date and time email received
  - 3. Message ID

- The e-mail header is read from the bottom to top.

- The first Received From entry provides information on the server name and IP address of the sending MUA.

- A WHOIS query (Netscan tools, Sam Spade) is required in order to determine the registered owner of the server and IP address.

- Once the registered owner or Internet Service Provider (ISP) is identified, a court order is typically required for the following information (dependent on laws):

  - Subscriber – Name, address, account status, etc.
  - Transaction – Log on/off times and dates.
  - Content - Actual contact of the email.

Investigators need to serve subpoenas or search warrants very quickly on an ISP. ISP's normally do not keep the referenced information for more than a few days to weeks. If it will take a significant amount of time to receive a subpoena or warrant, telephonically advise the ISP of the pending court order so that they can preserve the

information that will be requested. Be aware that some ISP's may not be law enforcement friendly and may compromise the investigation.

E-Mail

E-mail headers provide a vast amount of information on the sender.

E-Mail (MS OUTLOOK Viewing)

To view MS Outlook, double click the e-mail that is to be reviewed for header information. In the e-mail, click the View menu to Options to see the header information. Cut and paste the Internet headers to a document for review. E-Mail headers provide a vast amount of information on the sender.

E-Mail (MS EXPRESS)

To view MS Outlook Express, click once to highlight e-mail headers to be viewed. Click the File menu then the Properties. The header info is viewed in the Details window. Click the Message Source button to view the header information.

E-Mail (EUDORA)

To view Eudora e-mail, double click the e-mail that is to be reviewed for header information. Click the Blah, Blah button to view the e-mail headers. Cut and paste the Internet headers to a document for review.

Web-Based E-mail

Web-based e-mail is email that is not transported via the normal SMTP. Web-based e-mail is not normally kept on a server or the client computer, unless saved to the computer. An individual can sign up for a web-based e-mail account and send e-mail from anywhere in the world. The web-based service providers normally "capture" the initial IP address that establishes the account (Important). Web-based e-mail is becoming the universal front-end to sending and receiving mail. Each time a user connects to their web-based e-mail, a "snap-shot" image is made and held temporarily in the Internet cache folders. These folders can sometimes be recovered by examining the cache folders, HTML files and unallocated space.

Remailer E-Mail

Remailer's are web-based applications that allow an individual who wants to remain anonymous to hide their e-mail identity. Remailer's make it virtually impossible to determine the identity, identifiers or origin of a particular e-email. Examples of Remailer e-mail include Anonymizer, Sendfakemail and W3.

Important: Each machine strips off the original header information and adds its own header information.

Locating E-Mail

- The inbox file contains mail that has been delivered to the recipient.
- The outbox file contains mail that that has been prepared but not sent to the recipient.

- The sent file contains mail that has been sent to its destination.

- The deleted file contains mail that has been deleted. (Once e-mail has been deleted from the file, it can only be located in unallocated space).

- E-mail can be restored by importing the suspect .pst/.dbx/.mbx file to a clean copy of MS Outlook or MS Outlook Express.

- The e-mail file is then restored and can be viewed by the law enforcement official.

- Steps for importing e-mail to MS Outlook:

    1. Install Outlook or Outlook Express on Forensic Workstation.
    2. Delete any default Microsoft messages from inbox and also from the deleted file.
    3. Click File button, drop down to Import and Export button.
    4. In the Import Export Wizard window, highlight Import Internet Mail and Addresses and click Next.
    5. Select e-mail client to import and click Next.
    6. Click Finish in next window.

Further Location of E-Mail

- MS Outlook – Is normally located in the default individual e-mail user folder (FOR WIN2K):
    - C:\Documents and Settings\(username)\Local Settings\Application Data\Microsoft\Outlook\outlook.pst
        - TO CONFIRM, DO A SEARCH FOR *.PST

- MS Express 6 & 5 – Is normally located in the default individual e-mail user folder (FOR WIN2K).
    - C:\Documents and Settings\(username)Local Settings\Application Data\Identities\HEX #)\Microsoft\Outlook Express*.dbx
        - TO CONFIRM, DO A SEARCH FOR *.DBX

- MS Express 4 – Is normally located in the default individual e-mail user folder (FOR WIN2K).
    - C:\Documents and Settings\(username)\My Documents\email*.mbx
        - TO CONFIRM, DO A SEARCH FOR *.MBX

E-Mail Revisited: Suggestions

During the course of an investigation, if a victim site cannot be visited to retrieve "suspicious" e-mail, the e-mail can be sent to the law enforcement official as an

attachment. Never have the e-mail forwarded. This will cause the victim's header information to replace the "suspicious" e-mail header information.

Introduction to the Internet

The Internet

The Internet started as a network for scientists and educators. It was used to allow communication between disparate networks. The Internet was designed with redundancy in mind. It was felt that if one part of the Internet became disabled, then the communication could be routed on a different node. It is a Network of Networks.

How the Internet works

The computers that link the Internet have Internet Protocol (IP) Addresses. No two machines can have the same IP number when communicating. IP addresses are global and standardized. All networks connected to the Internet agree to use the same scheme for establishing an address. Example: Uniform Resource Locator and Domains: URL: 123.456.78.90 = Domain name

Examining the Internet more closely we know that every house on a street has a unique address. The name on the mailbox in front of the house probably identifies the occupants and is relatively unique. The same is true on the Internet.

- Dynamic Vs. Static Assignment
  - Dynamic - randomly assigned to user
    - America On Line, Local ISP Supported
    - Changes with each sign on
    - Traceable through ISP
  - Static - always the same address for user
    - Domain Hosting Services
    - Always the same
    - Traceable through ISP

Internet Services

- **What you need to access the Internet**
  - Computer with modem or broadband connection.
  - Web Browser (MSIE, Netscape, Opera)
  - Optional Software and Plugins
    - ISP Specific (AOL, AT&T, Prodigy, Local Provider)
    - Usenet (Newsgroups) Software
    - Internet Relay Chat (IRC) Software (Pirch, MIRC)
- **Hypertext Transfer Protocol (http)**

- How browsers talk to servers and read Web pages
- Configure graphics, text, sounds and files
- Use specially written programs to execute commands:
  - JAVA Applets and scriptlets
  - CGI Script
  - Shockwave, VRML, etc**.**

- http://www.microsoft.com
- extensions determine the type of site:
  1. .org - organization
  2. .edu - education
  3. .com - commercial
  4. .net - network
  5. .mil - military
  6. .gov - government
- Packets
  1. Like birds on a wire - each lined up in order
  2. They fly in groups to their destination
  3. Arrive in the original order in which they departed
  4. Although one or two may have strayed from the flock
  5. The sending and receiving machines maintain communication

END NOTES

This section is added for your compiling additional notes. Over the course of time you may acquire supplemental knowledge that is important in your cyber crime investigative and/or trial procedures. Increasing our knowledge is what this volume is about, and what keeps us one step ahead of the cyber criminal