

Introduction to Cyber Crime & Computer Forensics

FSC 140

September 29 & October 1, 2008

Levi White, CEECS

CyberCrime Defined

- Cybercrime is any crime that involves or is committed with a computer or other digital device.
- Two categories of CyberCrime
 1. Crimes committed against a computer
 2. Crimes committed with the aid of a computer

Crimes Against a Computer

- Intrusion incident
 - Gaining illegal access
- Denial of service
 - Overloading a website to shut the site down
- Security breach
 - Gaining illegal access for malicious purposes

Crimes Committed with the aid of a Computer

- Child pornography / exploitation
- Threatening letters / emails
- Fraud
- Embezzlement
- Theft of intellectual property

The New Wild West

The world of cyber crime is often called the new Wild West for many reasons

- It is one of the few crimes still on the rise
- Cyber criminals are often better trained than law enforcement officers
- There are no borders in cyber space
- Laws are still being established

Who are Cyber Criminals?

- Pedophiles
 - Largest amount of cybercrime at 70-80%
- Hackers
 - Black Hat Hackers
 - Purpose is to defeat security measures for criminal purposes
 - White Hat Hackers
 - Purpose is to defeat security measures for the improvement of internet security
 - WHH are still operating outside of the law
- Con-artists
 - Nigerian Money Scam
- Embezzlers
- Terrorists
 - Hack websites to display messages of hate
 - Develop viruses and wage cyber warfare

“Geek with a Gun”

- Cyber Investigator or Examiner
 - Geek with a gun
 - Handle law enforcement & computer world
 - Part systems administrator
 - Know computers and keep everything up to date to work with new systems
 - You never know what system will come in for analysis, so you must be prepared
 - Part scientist
 - Must be able to test, validate, and defend their tools
 - There will always be new devices to learn and new tools to master

Cyber Investigator Tasks

- Data recovery
- Web history reconstruction
- Password breaking
- Activity reconstruction
- Email tracing
- Much more !!!

Major Players in Cyber Crime

- FBI
 - National Computer Crime Squad
 - Computer Assistance and Response Team (CART)
 - Regional Computer Forensics Laboratories (RCFL)
- US Dept. of Justice
 - Computer Crimes and Intellectual Property Section
 - www.cybercrime.gov
- Secret Service – Electronic Crimes Task Force
- Internal Revenue Service
- Department of Defense
- State Police Agencies
- State Crime Labs

Computer Forensics & Digital Evidence

- Computer Forensics, or Digital Forensic Science, involves the preservation, identification, extraction, documentation, and interpretation of computer/digital data.
- Digital Evidence is potentially anything that is stored on or transmitted with a computer or other digital device

Digital Evidence Uses from Vacca's “Computer Forensics Computer Crime Scene Investigation”

- Criminal Prosecution
 - Homicides
 - Financial Fraud
 - Drug and Embezzlement
 - Record Keeping
 - Child Pornography
- Corporate Investigation
 - Sexual Harassment
 - Embezzlement
 - Theft or Misappropriation
 - Corporate espionage
- Individuals
 - Wrongful Termination
 - Sexual Harassment
 - Age Discrimination
- Civil Litigation
 - Fraud
 - Divorce
 - Discrimination
 - Harassment
- Law Enforcement
 - Pre-search warrant prep
 - Post-seizure handling
 - Individuals

Types of Evidence

Computer can be viewed as a room that contains potential evidence of a crime

- Present
- Deleted
- Encrypted
- Hidden
- Compressed
- Corrupted

Crime Scene vs. CyberCrime Scene

- | Crime Scene | CyberCrime Scene |
|--|-------------------------------------|
| 1. Photograph the crime scene | 1. Photograph the computer setup |
| 2. Search the crime scene for evidence | 2. Take the crime scene with you |
| 3. Take samples from the crime scene | 3. Search the computer for evidence |
| 4. Interpret the results | 4. Interpret the results |
| 5. Prepare a report | 5. Prepare a report |

3 A's of Computer Forensics

- **A**cquire
 - Evidence must be acquired without any changes being made to it
- **A**uthenticate
 - It must be proven without a doubt that nothing is added or taken away from the evidence during the investigation
- **A**nalyze
 - The evidence must be analyzed without modification

Common Mistakes

- Turning the computer on/off during or after seizure
- Improper storage/transfer
- Failing to obtain proper search warrant or authorization
- Searching through the original media

Mistakes cause problems because:

- Easily destroyed or corrupted
- Can be volatile (only there until power is removed)
- Large amounts can be easily hidden
 - Data streams
- Not always possible to determine the author
- Computer data changes quickly
- Can only be viewed with the use of special tools
- Technology is quick to change
- Collecting the evidence can potentially change the evidence

Evidence Acquisition (A#1)

1. Obtain a search warrant or proper authorization
2. Secure suspect
(WHY?)
3. Secure the communication lines
(WHY?)
4. Photograph and document the scene
5. Identify and document items to be taken
6. Secure the evidence for transportation

ANSWER: Logic bombs and file shredders

What to look for?



- Also look for
 - Special connection wires
 - Instruction manuals
 - CDs & DVDs
 - Installation disks
 - Other relative hardware/software

Expectation of Privacy

In the following, when does an individual not have an expectation of privacy?

- Deleted file
- Computer turned in for repair
- Contents of your computer at home
- Your files on your roommate's computer
- Computer thrown in the garbage at the edge of your property
- Your computer being shipped via the US Postal service

Plain View Doctrine and CF

- The plain view doctrine allows officers to seize evidence that is in plain view during the course of an investigation
- Suppose an investigator is looking for records of drug dealer contact information and discovers child porn by accident. The investigator can seize the one picture, but cannot search for additional pictures without first obtaining an additional search warrant.
- QUESTION: Why would someone open an image file when looking for text information?

Protecting the Evidence

- Before analysis of digital media, two additional copies of the digital media are made.
- 1 = Original Copy
 - Stored in a secure location
 - Never used for investigation purposes
- 2 = Backup Copy
 - Stored in a secure location
 - Used only if working copy is faulty
- 3 = Working Copy
 - Used for analysis purposes

Steps in Imaging

1. Prepare source media
2. Apply write blocker as needed
3. Image the suspect's media
4. Hash source media
5. Hash image
6. Create proper documentation including hash values

Evidence Authentication (A#2)

- Authentication deals with proving that nothing has been added or taken away from the evidence in any stage of investigation

Physically

- Chain of Custody
- Documentation
- Photographs
- Secure Storage

Logically

- Never work from the original
- Access the original as little as possible
- Use write-blocking
- Use Hash functions

Hash Functions

- Hash Function
 - A mathematical function that takes a variable length input and produces a fixed length output
- No matter how many numbers are placed in the function, it will always produce a set number of digits
- Essentially the "fingerprint" for a given media
- No details can be gathered from the hash value, but if the evidence is altered in any way, the "fingerprint" will change drastically
- Two examples of hash functions
 - MD5 (128bit, 1991, most used)
 - SHA-1 (160bit by the NSA)

Analyze the Evidence (A#3)

- Can be done by using forensic tools such as:
 - AccessData
 - FTK
 - PRTK
 - NTI
 - Encase
 - ILook
 - Freeware Tools

Data Recovery

- When is data really gone?
- What really happens when data is deleted?
- How do you recover deleted data?
- What are the chances of recovering deleted data?
- How do you permanently erase data?

Levels of Destruction

1. Deleting
 - a) Moves the file to the “Recycler”
2. Removing from the recycle bin
 - a) Marks the space as reusable
3. Formatting
 - a) Rewrites file system structure (removes index)
 - b) Does not touch actual data
4. Wiping
 - a) Changes everything to zero's or one's
5. Physical destruction
6. Total disk destruction (shredding or melting)

Data Carving

- Data Space Types
 - Free Space
 - Any space that is not currently in use
 - Slack Space (internal fragmentation)
 - Swap/Page Space
 - An area on the hard drive that is used to temporarily store parts of RAM when more RAM space is needed
- Data carving cannot reproduce
 - Original name
 - Time stamps
 - Owner information
 - Security attributed

Digital Crime Scene Processing Overview

FSC 140
September 29 & October 1, 2008
Levi White, CEECS

Secure the Suspect

- Move everyone away from the area where the computer is located
- Do not allow ANYONE to touch the keyboard/mouse
- Data traps/bombs may be activated very easily

Initial Computer Protocol

- Computer On
 - Photograph screen to note actions of suspect before seizure
- Sleep Mode On or Screen Saver
 - Move the mouse or tap shift key to “wake”
 - Photograph screen
- Remove power connection from back of computer
 - Remove battery source of laptop first
- General Rule
 - IF IT LOOKS WEIRD OR COMPLICATED, CALL A PROFESSIONAL

Bag & Tag

- Disconnect any outside communication
- Record & mark the location of all cables
- Note make, model, and serial numbers
- TAKE EVERYTHING
 - Collect all software, manuals, notes, and any other written documentation
 - Collect and label all hardware attached and unattached to the computer/electronic device (except some monitors)
 - Label disks carefully with a marker. Ball point pens will damage electronic media

Packaging & Transportation

- Small bumps may damage large amounts of information
- Transport away from extremes (heat/cold/magnetic)
- Keep away from magnetic sources
 - Radios, speakers, cell phones, batteries
- Packaging
 - DO NOT use standard plastic bags
 - Use paper bags, cardboard boxes, or anti-static bags
- Use evidence tape over openings to disk drives
- Bag cables/cords, keyboards, mice, small peripherals together
- Bag loose media (floppy disks, CD's. etc.) together
- Use original packaging material if available

Summary Checklist (1)

- Remove everyone (especially the suspect) away from the computer and data storage area
- Photograph the screen and decide if immediate power cut off is necessary
- Disable power to the system
- Disable or disconnect the modem/cable connection/LAN
- Disconnect the power to the printer and other peripherals
- Remove diskettes from drives and process the evidence; place a strip of tape over the drive openings
- Interview suspects/contacts regarding the computer evidence and possible password information

Summary Checklist (2)

- Photograph connections and the entire area around the computer
- Diagram and label all connections to/from the computer for reassembly later
- Search the scene specifically for passwords or other related information
- Seize all books, manuals, disks, software, hardware, and information related to the system
- Carefully package and transport evidence – keep away from all electromagnetic fields
- Photograph the area when search is completed