Electronic Crime Scene Training

Overview Discussion and Questions

National Cyber Crime Training Partnership
Dr. Thomas A. Johnson
The California Sciences Institute

Entering Electronic Crime Scene...

- Awareness of the scope/uniqueness of electronic evidence in a crime
  - key concepts for recognition and collection of electronic evidence:
    - » fragility of evidence
    - » anonymity
    - » encryption and steganography
    - » technological change
    - » latent nature of the evidence
    - » difficult to detect

Entering Electronic Crime Scene...

- Awareness of the scope/uniqueness of electronic evidence in a crime
  - key concepts
    - » bifurcated nature of evidence/data
    - » global nature- extra-jurisdictional and multi-jurisdictional
    - » spoofing and impersonation

Entering Electronic Crime Scene...

- Awareness cont.
  - traditional crimes are now being facilitated by use of electronic devices/crimes
  - New Age crime
- The Role of the Computer in the Crime
  - Repository of information
  - Instrumentality (means to an end)
  - Target

Entering Electronic Crime Scene...

- Types of Electronic Devices
  - computers (laptops, work stations, servers)
  - peripherals
  - printers
  - power supplies
  - digital copiers
  - cell phones/satellite phones
  - scanners
  - fax machines
  - telephones

Entering Electronic Crime Scene...

- Types of Electronic Devices
  - » datalink devices (watches)
  - » GPS devices
  - » digital cameras
  - » voice data recorders
  - » pagers
  - » modems
  - » magnetic/optical storage devices (disks, tapes, CD-ROMs)
  - » PDA (pocket organizers, palm pilots)

Entering Electronic Crime Scene...

- Types of Related Materials at Electronic Crime Scene
  - » printed documents
    - manuals
    - user generated documents
  - » hand written notes
  - » installation software
  - » related magazines
  - » telephone numbers and bills
  - » financial records
  - » receipts

Entering Electronic Crime Scene...

- Legal issues
  - Authority to seize
  - State statutes
  - Federal statutes
  - 4th Amendment
  - No reasonable expectation of privacy (shared, banner)

Entering Electronic Crime Scene...

- Exceptions (without search warrant)
  - » exigent circumstances
  - » consent
  - » probable cause
  - » incident to arrest

Entering Electronic Crime Scene...

- Secure the scene
- Protect the evidence
- Evaluate the scene (can I handle it, need assistance)
- Collection of computer evidence (does not apply to other electronic devices)
  - document the scene, photographing, sketching
  - shutting down

Entering Electronic Crime Scene...

- Collection cont.
  - labeling
  - disassembling
  - packaging items
- Preservation
  - preserve integrity of electronic evidence
  - maintain chain of custody

Entering Electronic Crime Scene...

- Transportation Issues
  - avoid magnetic fields
  - avoid extreme environmental factors
  - avoid physical shock
- Storage
  - avoid magnetic fields
  - avoid extreme environmental factors
  - battery life
  - chain of custody
  - shelf life

Electronic Crime Scene Training

Questions

How are computers and other electronic equipment used in -

- Insider Crimes
  - theft of trade secrets
  - embezzlement
  - disgruntled employees
  - theft of equipment
  - inventory theft
  - theft of services

How are computers and other electronic equipment used in -

- Traditional Criminal Activity
  - drugs
  - gambling
  - fraud
  - sex abuse
  - harassment and stalking
  - black mail
  - extortion

How are computers and other electronic equipment used in -

- Traditional Criminal Activity
  - death investigation
  - theft
  - economic espionage
  - foreign espionage
  - terrorism
  - money laundering
  - software piracy
  - copyright infringement
  - telecommunications fraud

How are computers and other electronic equipment used in -

- Forgery/Identity Thefts
  - counterfeiting
  - spoofing
  - credit card fraud
  - electronic signatures
- Hacking and Phreaking (telecommunications fraud)
  - unauthorized access
  - theft of services
  - denial service
  - malicious damage
  - data theft
  - data alteration

How are computers and other electronic equipment used in -

- Child Exploitation
  - image capture/storage and transmission
  - communication (e-mail, I-Chat, BBS)
  - solicitation/enticement
- Stalking
  - communication (e-mail, I-Chat, BBS)

In what types of crimes are computers the target of criminal activity?

- Theft
- Virus attack
- Espionage
- Malicious code
- Unauthorized access
- Data alterations

What types of crimes are computers the instrumentality of criminal activity?

- Phone phreaking
- Stalking
- Child Porn
- Unauthorized access
- Forgery
- Fraud
- Data alteration
- Hacking
- Software piracy

What types of crimes are computers the instrumentality of criminal activity?

- Gambling
- Drugs and Drug Methods
- Telemarketing

What types of crimes are computers the repository of criminal evidence?

- Phone phreaking
- Stalking
- Child Porn
- Unauthorized access
- Forgery
- Fraud
- Data alteration
- Hacking
- Software piracy
- Gambling
- Drugs and Drug Methods
- Telemarketing

What should officers & investigators think about before they reach the crime scene?

- Understand the location(s)
- Nature of the crime/complaint (role of computer)
- Pre-search intelligence
- Scope out the scene
- Level of sophistication
- Publisher
- ISP
- Time of usage
- Equipment (network or stand alone)

- Seizure/onsite backup
- Scope of warrant
- Language to include
- How to get help

What should officers & investigators do when encountering a potential electronic crime scene?

- Nature of the crime/complaint (role of computer)
- Level of sophistication
- ISP
- Scope of the scene
- How to get help
- Handling collection and storage

How do you assess whether a computer or other electronic device may have been used in a criminal activity?

- Plain view
- Interviews/Statements
- Other investigative information
- Nature of the complaint/crime

An investigator learns of a potential electronic crime scene and wants to seize all computer hardware, software and manuals (printers, tape drives, optical drives, hardware manuals and software manuals) for evaluation as potential evidence.

What must a search warrant contain in order to seize electronic devices?

- Describe with particularity the items to be seized
  - independent component
- Describe location
- Decide the evidence to be seized
- Tie the item to be seized back to the crime

Why in some cases may it be important to take hardware, software and manuals?

- proprietary software and hardware
- could be evidence
- to enable the discovery of evidence
- it may be evidence showing the ability to commit the crime
- copyright/licensing

Do the items taken have to be returned? What is the time frame and procedure?

- Depends on the role of the item
- Contraband (seized as evidence- does not have to be returned)
- Whatever the court orders
- Reasonable amount of time

Describe appropriate affidavit language for seizing computer-related evidence.

- Possible question for exam.

Describe Exigent Circumstances

Possible question for exam.

Special considerations involved in executing a search warrant for seizing a computer?

- Follow standard protocols
  - Officer safety
  - Protective Sweep
- Electronic devices
  - Remove people from electronic devices
  - Don’t allow anyone to execute commands

What are the proper steps for shutting down and powering down a computer?

- Shutting it down properly vs. pulling the plug on stand-alone
- On network, do not pull plug on server
- Protect the scene and call for help when a network is suspected

What are the steps in physically seizing the equipment?

- Securing, marking, disassembling, packaging and transporting
- Documenting
- Labeling
- Seizure Kit

What computer hardware and components are important to identify in the execution of a computer-related search warrant? Why?

- Connectors on expansion cards
- Network adapter
- Modem
- SCSI Adapter
- IR Ports

A computer system is found during the execution of a search warrant, where no computer was anticipated.

How should an agent secure such a computer system?

- First, should I secure it?
- There is no difference, still need to secure it
- Follow the same steps

How can the evidence be accidentally or intentionally altered?

- Something as simple as booting up the computer and/or running the operating system can destroy data.
- Viruses can be executed
- Short-cut keys
- Altered commands
- As part of normal shut-down procedures
- Pulling the plug (may lose data)

How can the normal operation of a computer destroy evidence?

- Overwriting temp files, swap files, destroying “deleted” files
- The operating system can be altered to destroy evidence when standard operating system commands are performed
- Saving new files

What destructive processes/devices can be planted to destroy computer evidence?

- Electromagnets, planted Trojan horse programs, bombs tied to the power-off button, basic commands altered (DIR to FORMAT C:)

Possible defense challenges?

- Altered evidence
- Improper search warrant
- Improper chain of custody
- Physical damage
- Improperly trained officer
- Not following accepted practices
- No authority to seize
- Search warrant may be improperly executed

Three Points of Defense Attack

- Pre-trial motion to suppress
  - Improper search and seizure questions
- Evidentiary challenges
- Witness credibility

What are mistakes made in the process of getting a search warrant?

- Improper description
- Failure to specify items to be seized
- Going to the wrong court (lacks jurisdiction)
- Insufficient probable cause
- Staleness of information