Digital Evidence Collection and Use

CS 585

Fall 2009

Outline

I. Disclaimers

II. Crime Scene Processing

III. Legal considerations in Processing Digital Evidence

IV. A Question for Discussion

Disclaimers

- **IANAL**!
- This lesson is based on several publications from the National Institute of Justice (NIJ):

  [1] *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition* (April 2008, NCJ 219941)

  [2] *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (April 2004, NCJ 199408)

  [3] *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (January 2007, NCJ 211314)

  All available from **www.ojp.usdoj.gov/nij/**
- **This presentation does not make you an expert!**

Disclaimers

- Law Enforcement perspective
- Federal focus
  - State and local laws may vary
  - Federal laws do not override local laws, except regarding actions by federal law enforcement personnel

Why This is Important

- Evidence is collected to be used at trial
- To be useful in court, it must be
  - Admissible
    - Collected legally, not hearsay
  - Credible
    - Authentic, reliable, not subject to challenges
  - Persuasive
    - Helps the prosecution's (or plaintiff's, or defendant's) case

II. Crime Scene Processing

First Responders

Principles:

I. The process of collecting, securing and transporting digital evidence should not change the evidence.
   - Digital evidence is fragile; special care must be taken to preserve it.

II. Digital evidence should be examined only by those trained specifically for that function.
   - Trust is established by following techniques recognized by the courts as trustworthy.

III. Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.
   - Any gaps will lead to challenges and potential loss of credibility.

The First Step

- First responders need to either
  - Be trained themselves, or
  - Have access to someone with training in dealing with digital evidence
- "First responders without the propoer training and skills should not attempt to explore the contents of or recover information from a computer or other electronic device other than to record what is visible on the display screen. Do not press any keys or click the mouse." – NCJ 219941

1. Evaluating the Crime Scene

Primary considerations:

- Safety of Officers and everyone at the crime scene.
- Compliance with federal, state, and local laws.
- Visually identify all potential evidence and ensure its integrity is preserved.

2. Securing the Scene

- Follow department policy.
  - Note: department should have a written policy!
- Immediately secure all electronic devices, including personal and portable devices.
- Ensure that no unauthorized person has access to any electronic devices at the scene.
- Refuse offers of help or technical assistance from any unauthorized persons.
- Remove all persons from the crime scene or the immediate area from which evidence is collected.
- Ensure that the condition of any electronic device is not altered (including on/off state!).

3. Checking state of Computers

- Is it on? Look, listen to find out
- If on, look for indications of what it's doing
  - Running "format" or "rm –r …"
  - Look for in-progress communications, e.g. chat room windows

4. Interviewing Those Present

- Valuable source of initial information!
- Get as much information as possible:
  - Names of users of computers/devices
  - Internet user information including service provider, account names, screen names, …
  - Purposes of computers and devices; who uses them
  - Passwords if known
  - Any offsite storage
  - Documentation (e.g., manuals) for devices and installed software

5. Documenting the Scene

Goal: create a record to be used in the investigation

- Record everything at the scene:
  - Devices and their locations and states (power status, ongoing communications, running programs, etc.)
  - Serial numbers of equipment
  - Connections between devices
- Photograph or video-record the scene if possible
- Do all this **before** touching anything!

5. Documenting the Scene

"Other" devices that may contain evidence:

- Audio recorders/players (iPod)
- GPS accessories
- Answering machines
- Computer chips
- Thumb drives
- Pagers
- Copy machines; multifunction machines
- Printers
- Telephone Caller ID units
- Fax machines

6. Collecting the Evidence (Generic Algorithm)

1. Secure the scene and get everyone away from devices.
2. If computer is OFF, goto 7 (do NOT turn it on!).
3. If trained personnel are available, get them and goto 9.
4. If the system is networked, STOP and get help from trained personnel.
5. If destructive processes are running, goto 7.
6. If evidence is visible on the screen, thoroughly document and photograph ALL of it.
7. Remove the power cord from the back of the computer. Put tape over the power switch.
8. Label all connections on computers and devices, as well as cables and power supplies.

6. Collecting the Evidence (Generic Algorithm)

9. Locate and secure all evidence within the scope of authority for the specific circumstances

   (if you've come this far, you'd better have a warrant!)

10. Document, log, and photograph all computers, devices, connections, cables, and power supplies.

11. Log and secure all evidence for forensic examination according to agency policies.

- Laptop modification:

  Remove battery as well as power supply cord.

7. Transporting and Storing Evidence

- Chain of custody:
  - Be able to prove that evidence was secure and under the control of some particular party at all times.
  - Take steps to ensure that evidence is not damaged in transit or storage.
    - Example: if stored for a long time, batteries may die, causing loss of information in "CMOS" memory (e.g., BIOS configuration)
    - Example: transport digital evidence in static-free containers: paper or special foil – NOT plastic bags
- Nota Bene: Digital evidence has two parts – the physical medium and the information (bits) itself
  - Chain of custody must be maintained for **both parts**

7. Transporting and Storing Evidence

- At the evidence room or lab: inventory and store appropriately
- Storage: climate-controlled location not subject to temperature or humidity extremes
- Protect from exposure to magnetic fields, moisture, dust, vibration, etc.
  - Defense Attorney: "Isn't it true, officer, that you transported that hard drive on the seat of your Saab, with the seat warmer turned on?"

Discussion

- List the things that first responders did wrong in the Ryan case.

III. Legal Considerations

Wiretap Act (18 USC §2510 et seq)

- Focuses on interception of content of communications **in transit** ("on the wire")
  - Telephone wiretaps
  - Network sniffers
  - Bugging a room to pick up conversations
- Prohibits anyone (in the US) who is not a participating party to a private communication from intercepting the communication among the participants using an "electronic, mechanical or other device" unless one of several statutory exemptions applies.

Wiretap Act

- Exception: court order authorizing interception issued by a "court of competent jurisdiction".
  - It is nontrivial to obtain such a court order.
- Violation can lead to criminal and civil liability.
- Violation by government officials may result in suppression of evidence obtained.
- Some states have versions of Wiretap Act that are more restrictive than the Federal version; state and local LE must comply with those acts even if Federal act does not apply.

Pen Register and Trap and Trace Statute (18 USC §3121 et seq)

- The "Pen/Trap Statute"
- Governs collection of dialing, routing, addressing and signaling information relating to communications.
  - Telephony: numbers called and calling
  - Internet: IP address and port information
- "Forbids nonconsensual real-time acquisition of noncontent information by any person about a wire or electronic communication unless a statutory exception applies.
  - Where no exception applies, LE must obtain a Pen/Trap order from the court before acquiring such information
- Again, some states have versions that are more restrictive.

ECPA (Stored Communications Provisions)

- Electronic Communications Privacy Act, stored communications chapter (18 USC §2701 et seq)
- Provides privacy protections to subscribers to certain communications services providers.
- Applies when LE seeks to obtain records (billing, dates of service, etc.) about a customer or subscriber from a communications service provider (cell phone, Internet)
- Says what information requires what kind of authorization for LE to obtain

ECPA (Stored Communications Provisions)

- Subpoena
  - Identity info: name, address, phone numbers outgoing/ incoming, phone number, period of service, means of payment, DHCP address assigned
  - Stored communications (email) that a customer has "retrieved" but left on a private provider's server
    - Note well: distinction between private and public provider (employer vs. ISP)
- Court Order
  - Log of IP addresses communicated with
  - Addresses of those with whom email was exchanged
  - "Buddy lists"
  - Stored communications retrieved from public provider or unretrieved but older than 180 days

ECPA (Stored Communications Provisions)

- Search Warrant
  - Unretrieved communications stored on a provider's server, whether public or private.

Privacy Protection Act (42 USC §2000aa et seq)

- Restricts what LE can seize under a search warrant
- Applies to materials possessed for the purpose of public dissemination
  - Work products (e.g., a newsletter or pamphlet)
  - Documentary materials (supporting information for work products)

Privacy Protection Act (42 USC §2000aa et seq)

- Does not apply when:
  - Material is contraband (child pornography, e.g.)
  - There is reason to believe seizure is necessary to prevent death or serious injury
  - Material is believed to be related to commission of a crime
- Remedy: civil damages
- Note: violation of PPA does not lead to suppression

Fourth Amendment to the US Constitution

- In general: LE must obtain a warrant for any search of a location where a "reasonable expectation of privacy" applies
  - Computer as "closed container" by some courts
- Warrantless search possible under the following exceptions:
  - Consent
  - Exigent Circumstances
  - Search incident to arrest
  - Inventory search (untested in courts)
  - Plain view doctrine

Fourth Amendment Exceptions

- Consent – may come from several sources
  - Login banners
  - Terms-of-use agreements
  - Company policy
  - Private-sector employer may consent to search of an employee's workplace computer
- Consent may be limited as to subject matter, duration, etc. Can be withdrawn at any time.

Fourth Amendment Exceptions

- Plain View Doctrine
  - May apply to computers in some instances
  - LE must legitimately be in position to observe evidence
  - Incriminating nature must be immediately apparent
  - cf. BALCO case!

Obtaining a Warrant

- Two requirements:
  - Reasonable suspicion of a crime
  - Description of the particular items sought
- These apply to electronic evidence as well
  - Again, see the 9th circuit decision in BALCO case

IV. A Question for Discussion

Does the 4th Amendment apply to Crime Scene Evidence Collection?

Example Case

- Woman decides to solve her overwhelming problems by ending her life and the life of her husband of many years.
- Shoots husband; writes suicide note; takes overdose of sleeping pills.
- Has change of heart; calls daughter for help.
- Daughter notifies sheriff, rushes over.
- Deputies arrive; daughter admits them.

Example Case

- Husband is dead; woman, unconscious, transported to hospital and eventually recovers.
- Deputies search house for other victims or suspects, then secure it.
- 35 minutes later, homicide investigators arrive, conduct a 2-hour "general exploratory search for evidence of a crime".
  - Examined every room of the house
  - Recovered evidence:
    - a pistol (found in a chest of drawers)
    - torn note (found in a wastepaper basket)
    - suicide note (tucked inside a Christmas card on top of chest of drawers)

Example Case

- Woman charged with 2nd degree murder.
- Prior to trial, moved to suppress the three items of evidence
  - On the grounds that her 4th Amendment rights were violated
- After various reversals, the case goes all the way to the Supreme Court
- Court ruled that the "exploratory search" was a violation of the Fourth Amendment; ordered the critical evidence suppressed.

4th Amendment Applicability

The Court ruled in this case ("Thompson") that:

a) The deputies did not obtain a warrant prior to the search (no argument about this)

b) None of the 4th amendment exceptions applied

[Do TV writers know about this?]

4th Amendment Applicability

"Whenever agents of the government intrude into an area where there is a reasonable expectation of privacy, a Fourth Amendment search has occurred that must be justified by either a warrant or one of the exceptions to the warrant requirement."

-- "Crime scene searches: the need for Fourth Amendment compliance", Kimberly A. Crawford, *The FBI Law Enforcement Bulletin*

Fourth Amendment Applicability

- In the 1978 case of Mincey v. Arizona, the Court refused to recognize a "crime scene search" as one of the "well-delineated exceptions".
- Thus: crime scenes given no special consideration under the Fourth Amendment.
- If a crime occurs where there is a reasonable expectation of privacy, law enforcement is restricted to "plain view" evidence unless a warrant is obtained.

(All of the abovequoted from Crawford, Op. Cit.)

Getting a warrant

Two requirements:

1. Probable cause
   - By definition a "crime scene" provides this!
2. Description of the particular evidence sought
   - This is more difficult
   - One approach: department is prepared with generic lists of evidence that is typically involved with or relevant to the type of crime: arson, sexual assault, murder…

Problem: may not be time to get a warrant, especially if a violent crime has occurred.

Fourth Amendment Exceptions

- Consent
  - Question: why didn't the consent exception apply in the Thompson case?
  - Consent must come from someone with authority to grant permission to search the premises.
    - Does a landlord qualify?
  - "Officers must ask precise, carefully crafted questions designed to determine whether the person being asked to give consent has lawful access and control over the area to be searched
  - Once sufficient information is gathered to allow officers to reach that conclusion, a specific request for consent should be made.
  - If possible, the consent should be written." – Crawford, *op. cit.*

Fourth Amendment Exceptions

- Exigent Circumstances
  - Three types traditionally recognized by courts:
    - Threats to personal safety
    - Destruction or removal of evidence
    - Escape (of suspect)
  - Generally any one of these is sufficient to allow an officer to enter the scene and address the emergency
  - Once the emergency has been mitigated, the authority ends

Another Case Example*

- Police respond to a report that 14-year-old Angela is being held in the defendant's apartment.
- They knock on the door; she answers from within.
  - But says she cannot let them in because defendant has locked her behind an armored gate.
- They force entry, free Angela.
- Th girl tells them the defendant had raped her several times at gunpoint, and threatened to kill her and her family if she tried to escape.

*Also taken from the Crawford Article

Another Case Example

- Angela shows the officers the closet where defendant keeps his weapons.
- They search the closet, find (& seize) three guns and some ammunition.
  - Rest of the apartment not searched at that time.
- Defendant (a convicted felon) was indicted for possessing weapons and ammunition.

Another Case Example

- Defendant filed a pretrial motion to dismiss the evidence (guns and ammo); court ruled against.
- Appeals court ruled that searching the closet violated the 4th amendment.

Accepted Exigent Circumstances

- If a body is found at the scene, bringing in the Medical Examiner to view and collect the body.
- If officers have reason to believe the crime scene contains evidence that will be destroyed if not quickly recovered, it may be collected under the emergency exemption.
- Securing the crime scene is also considered reasonable.

The Bottom Line

- "Because officers arriving on the scene of a crime have no way of knowing whether the ultimate defendant is going to be someone with enough authority to object to the search of the scene, the dictates of the Fourth Amendment must be scrupulously honored to ensure the admissibility of evidence."

-- Crawford, Op. Cit.


Digital Evidence:
the Process

Digital Evidence Process

The Steps:

1. Policy and Procedure Development
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination & Analysis
5. Documenting and Reporting

1. Policy and Procedure Development

Principle (recall from earlier…)

1. Policy and Procedure Development

Principle: Computer forensics demands specially trained personnel, dedicated resources, and standardized procedures.

1. Policy and Procedure Development

Considerations:

- Job qualifications
- Process for service to be requested
  - Request forms, point of contact, required documentation, acceptance criteria
- Case management procedures
  - Assigning priorities to cases
- Evidence handling and retention
- Standard Operating Procedures

2. Evidence Assessment

Principle: The digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action.

2. Evidence Assessment

Steps:

1. Review the request for service.
   - Identify legal authority for the examination.
   - Verify documentation of chain of custody.
2. Discuss with case examiner: what might be discovered, whether other forensic procedures are needed (e.g., DNA analysis), whether other digital evidence might be needed (e.g., ISP preservation order), relevant info like usernames, emails, etc.
   - Determine the nature of the evidence sought.
3. Assess skill level of users involved. Crypto? Steganography?

2. Evidence Assessment

Steps:

5. Prioritize order of examining evidence.
6. Determine resource requirements for the examination.
7. Determine extent of the authority to search.

3. Evidence Acquisition

Principle: Digital evidence is fragile, and can be altered or destroyed by improper handling. Failure to take precautions and follow procedures can result in unusable evidence, or lead to an inaccurate conclusion.

3. Evidence Acquisition

1. Secure the evidence according to documented procedures.
2. Document configuration (hw & sw) of examiner's system.
3. Disassemble cases to get access to devices (disks).
4. Document internal devices and hardware configuration:
   - Drive make, model, size, jumper settings, interface
   - Other internal components
5. Disconnect drives' power and data connections.

3. Evidence Acquisition

6. Retrieve (and document) config information from system using controlled boot (go into BIOS mgr):
   - Boot sequence
   - Date/time
   - Any kind of BIOS-stored password
7. Reconfigure boot sequence to boot from forensic boot disk
   - Record drive configuration info per BIOS
8. Power down, remove drive.

3. Evidence Acquisition

8. Whenever possible, remove drive, examine in a separate system with known, documented configuration.

   Situations where you might not remove:

   - RAID
   - Laptop
   - Legacy equipment (may not be readable in newer system)
   - Network storage

9. Ensure examiner's system is forensically clean before connecting the evidence drive

10. Acquire contents and store to examiner's storage
    - Use write protection!

4. Evidence Examination

Principle: General forensic principles apply. Different types of cases and media may require different methods of examination. Training is required, etc.

1. Preparation: set up working directories, removable media, etc.
2. Extraction
   - Physical: raw data, block-by-block (e.g. keyword search on output of dd)
   - Logical: Interpret file system (e.g., reassemble deleted files)

4. Evidence Examination

3. Analysis
   - Timeframe analysis
   - Data hiding analysis
     - E.g., correlate file extensions with contents (headers)
   - Application and file analysis
   - Ownership and possession (whose data is this?)
4. Draw conclusions

5. Documenting and Reporting

"Principle: The Examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination."

-- "Forensice Examination of Digital Evidence", NCJ

5. Documenting and Reporting

- Take notes throughout the whole process!
- Keep copies of all documentation – service request, warrants, chain of custody documentation, etc.
- Document any irregularities encountered and any actions taken regarding the irregularities during the examination.
- Document changes made to the system by the examiner or LE.
- Document any information found that is beyond the scope of the current legal authority – and bring to the attention of the case agent.

5. Documenting and Reporting

- Examiner's report:
  - Summary of findings
  - Details of findings
    - Files found
    - Techniques used
    - Indications of ownership
    - Timeline information
  - Supporting materials (e.g., printouts of logs)
  - Glossary (if needed)

5. Documenting and Reporting

- Presenting evidence in court (next time!)