Identifying and Seizing Digital Evidence

Dr. Philip Craiger

Associate Professor

School of Engineering Technology

DAYTONA STATE COLLEGE

NSF

Objectives and topics

- Identifying types of evidence
- Securing the scene
- Documenting
- To unplug, or not …

Scenarios

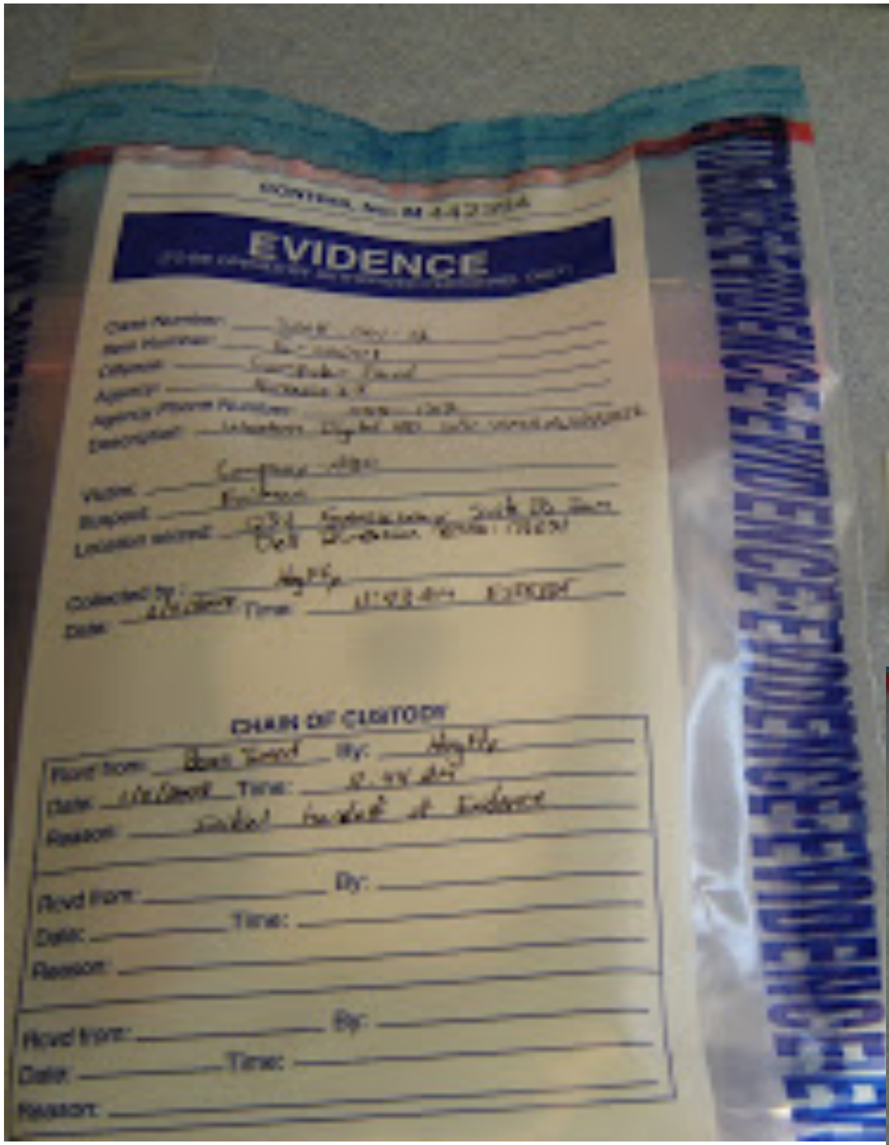
- You are a forensic examiner for a law enforcement agency. You've been asked to help deputies, who have a search and seizure warrant, to identify and seize evidence at a suspect's house.
- You are a computer security specialist for a Fortune 500 company. An employee is suspected of copying sensitive information to removable devices, and selling it to another company.

Canon
PowerShot SD780 IS
DIGITAL ELPH
LEXAR Media
4x
CompactFlash
USB ENABLED
256 MB
MEGAPIXEL
CD-R
Memorex
700MB 80min
swissbit
64MB
MENU

Acquiring Evidence

- Secure the area and document
  - Take photos of crime scene
  - Take photographs of system components
    - Monitor
    - Back of CPU
    - Papers, disk, peripherals
  - Inventory Items
    - Tag all pieces of evidence
    - Tag each cable, indicating end points

Schulz & Shumway (2002). Incident response. New Riders.
U.S. Secret Service. Best Practices for Seizing Electronic Evidence (version 3)



CONTROL No. M 442394

EVIDENCE

Case Number: 2008-[illegible]

Item Number: [illegible]

Offense: Computer Fraud

Agency: [illegible]

Agency Phone Number: [illegible]

Description: Western Digital HD S/N [illegible]

Victim: [illegible]

Suspect: [illegible]

Location seized: [illegible]

Collected by: [illegible]

Date: [illegible] Time: [illegible]

CHAIN OF CUSTODY

Rcvd from: [illegible] By: [illegible]

Date: [illegible] Time: [illegible]

Reason: [illegible] of Evidence

Rcvd from: By:

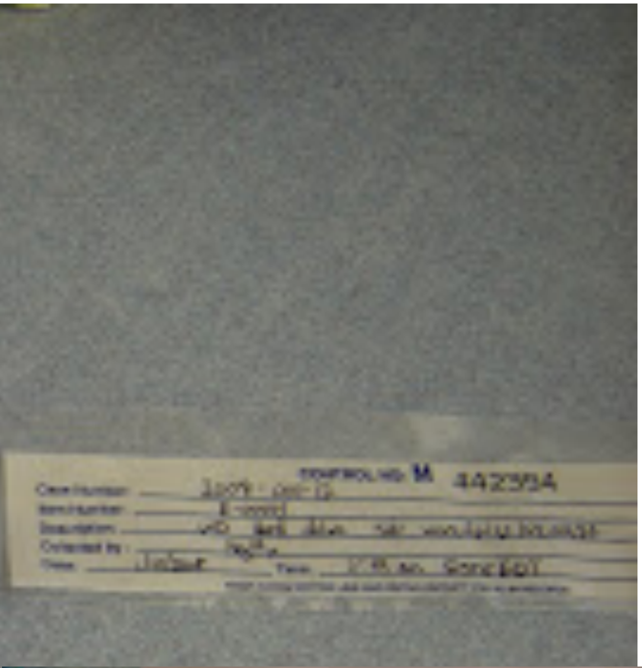
Date: Time:

Reason:

Rcvd from: By:

Date: Time:

Reason:



CONTROL NO. M 442394

Case Number: 2008-[illegible]

Item Number: [illegible]

Description: WD [illegible] S/N [illegible]

Collected by: [illegible]

Date: [illegible] Time: [illegible]

Crime scene vs ‘Tech’ scene

- “Evidence”
  - – usually denotes something pertaining to a crime and the law
- “Artifacts”
  - – What if a user violates acceptable use policy, harassing a co-worker. While not against the law, the person could be fired. Is that ‘evidence?’
    - Child pornography vs pornography

Has a crime been committed?

- How we deal with the electronic ‘stuff’ we need to identify depends on a lot of variables
  - Was a crime committed?
    - Yes, then contact authorities
      - They will get a search warrant to seize the evidence
    - No, deal with in-house (perhaps)
      - It might BE a crime!
      - Deal with the evidence as if it was a crime.
      - Don’t be sloppy
      - Document what you do

Incident Response: Acquiring Evidence

- Secure the system
  - If computer is seized intact
    - Seal floppy and CD drives
    - Check to see if a floppy or CD is still in the drive!
  - Place tape across
    - Floppy drive
    - Power button
    - Cable connectors

Schulz & Shumway (2002). Incident response. New Riders.
U.S. Secret Service. Best Practices for Seizing Electronic Evidence (version 3)

Incident Response: Acquiring Evidence

- Prepare the system
  - If computer is NOT seized
    - Carefully open case
    - Take photographs of inside of case prior to disconnecting cables
    - Disconnect power leads to HD

Schulz & Shumway (2002). Incident response. New Riders.
U.S. Secret Service. Best Practices for Seizing Electronic Evidence (version 3)

To unplug or not?

- Secure a homicide crime scene?
  - Yellow tape
  - Only authorized trained personnel inside scene
- Secure a computer crime scene?
  - Equivalent of yellow tape?
  - Pull the plug
    - Computer shuts down ‘dirty’ regardless of OS
    - Can then use bootable CD to mount HD read-only for analyses

Schulz & Shumway (2002). Incident response. New Riders.
U.S. Secret Service. Best Practices for Seizing Electronic Evidence (version 3)

To unplug or not?

- Problem?
  - What if there is ongoing activity?
  - Volatile evidence will be lost
    - Contents of RAM
    - Network connections
    - etc.
  - Powering down computer causes hundreds of changes
  - Powering on causes hundreds of changes
  - Leaving computer on results in changes

To unplug or not?

- Don't automatically shutdown.
    - Investigate **first.**
- Response strategy will determine whether to unplug or not
    - If a forensic image duplication is required, must unplug
    - If there is ongoing activity, will need a live-response

Need to unplug…

- If you find you need a forensic image you must shutdown.
  - Unplug the network cable
  - Unplug the power cable
  - System will shut down **uncleanly**
    - Files in RAM that need to be written to disk will not
    - “Dirty’ bit will not be reset
- What do you need to image?
  - HD, Floppies, CDs, Any media
- WRT HD
  - Need information regarding number, type, partitions, geometry,etc.

References

- Schulz & Shumway (2002). *Incident response*. New Riders.
- U.S. Secret Service. *Best Practices for Seizing Electronic Evidence, version 3.*