Handling Digital Evidence

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davepet@cops.org

Our efforts to safeguard the hardware, software, and data can be an important aspect not only of our investigation, but also in the prosecution of a suspected computer crime.

- Proper procedures for search and seizure at the scene
  - Computerized log of all evidence seized at the scene (federal Dept. of Human Services software)
  - Detailed return given to owner of the computer equipment
  - Report describing each action taken
  - See checklist in front of black manual that we take on-scene
- Credentialed examiners
  - The only assurance of integrity is the trustiworthiness of the examiners, who have the skills and knowledge to properly process electronic evidence
- Detailed report on processing and structure of the suspect's hard drive
  - Name personnel involved
  - Record times and places
  - Identify materials, names and serial numbers of all equipment and computer programs used
  - **EnCase report contains a lot of this information, and more… (Review EnCase report and process from lesson plan)**
- Maintain regular chain of custody, as for other types of evidence
- Keep electronic evidence in a proper environment (within limits for heat, humidity, dust, magnetic fields, etc.)
- Evidence processing procedures (EnCase)
- Labeling-identifying storage media other than the hard drive
  - Data storage mediums (tape, cartridge, zip or floppy disk, CD-ROM), if removable, will be positively identified as follows:
    - Contents
    - Date certified/tested/examined
    - Examiner's name
    - Disk write-protected prior to review, diskcopied, work on copy, not original; virus checked.
      - Label each diskette a-1, a-2, etc.
    - Print a directory for each diskette
    - If incriminating information found, print the file contents and label the printout with same alphanumeric designation
- Procedures for providing discovery copies to public defender, defense attorney, etc.
  - Make a working copy of the original evidence
  - Print the report from the copy made, unless too large or too much volume. If so…
  - Brief in a report, submit copied electronic evidence
  - Data contained in computer storage devices and computer-readable media (magnetic tape, hard drives, removable disks such as floppies and zip disks or attachable tape backup drives) are sometimes needed as evidence in a human-readable form, such as printing.
- Technical presentation in court
  - Simple and nearly free of computer technology
  - PowerPoint presentations explaining complex concepts simply
    - Particular Internet crimes
    - How the Internet works