Procedures for

Seizing Computers

Pueblo High-Tech Crimes Unit

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

PRE-SEARCH

- Before seizure, gather as much intel as you can about the system and suspect actions. Check "Fourth Amendment and Computer Seizures" document for probable cause requirements and options for searching by use of consent. Consider "The Independent Component Doctrine" on Page 35 to plan what equipment you can/cannot seize.
  - Use informants, undercover, and surveillance to identify:
    - The **computer system** (MacIntosh, Apple, IBM, LAN, etc.)
      - "Hi, Mr. Jones. We are giving away free floppy disks…etc. What type of computer are you running?"
      - Or use SEARCH/NCMEC computer survey format to gather intel.
    - How **MANY** computers
    - **Location** of computers on the site.
    - The **users and time used**
      - **Who owns the system? Who can give consent to search?**
      - **How vital to the daily operation of the business are the computer and the files it contains?**
        - **How much data must you examine? How soon can it be returned to the business? Can you mirror image and leave copies with suspect? Can you make him rent a similar system?**
    - **Software programs** used by the suspects
    - **Passwords** (and where they are kept)
    - **What kind of storage media is used (**floppies, magnetic tape, zip disks, etc.)
    - **Modem?**
    - **Nature and frequency of criminal activity?**
    - **How sophisticated is the suspect?**
      - **Any indications of booby traps or alterations that could result in loss of data?**
      - **Is he running a web site or bulletin board system out of the house?**
    - **Are you dealing with a mainframe, mini, or networked system?**
      - **Get the appropriate expertise lined up. Will someone inside help? Other LE trained specialist?**

  - **Need a wiretap or data scope?**

SEARCH WARRANT

- **Proper wording**, and include everything seizable.
- Proper wording in affidavits to indicate computers are used in this type of activity and that they NEED to be seized to be examined for evidence.
- Review the search warrant or consent-to-search form prior to entry. **Familiarize yourself with what is appropriate to seize and what is not.**
- **"Reasonable expectation of privacy?"** (Signed employee statement, disclaimer on screen at login "all files subject to security audits at any time." Signs displayed? If not, you will need a search warrant, not just employer consent to search.
- **Is there undelivered e-mail?**
  - **If you do not have a warrant, you cannot look at it.** Payment comes out of your pocket! Electronic Communications Act.

SEARCH and SEIZURE at the Crime Scene

- SECURITY OF OFFICERS is still the No. 1 priority**.**
  EVERYONE GOES HOME ALIVE!!!
  - Power switch on computer wired to C-4 explosive?
  - Boot-up electronic signals tied to a pipe bomb?
  - Hard drive controller card wired to pipe bomb?
  - Watch the suspect; check the entire rest of the home or business to ensure no other threats. Stand watch over the seizure team as they work. If unsure about threat environment, everyone wears protective vests, and is armed.
- Second priority is security of the computer system. ***GET EVERYONE AWAY FROM THE COMPUTER.*** At no time should the suspect be allowed direct access to the system without a court order. He can easily erase everything.
- DO NOT examine the machine on site if it can be avoided, and ALWAYS use a law enforcement computer crimes specialist to document and preserve the evidence in appropriate ways that will stand up in court.
- Choose one of these **options**:
  - Take everything.
  - Make copies, take the originals and leave the copies,
    use your system to do disk analysis.
  - Make copies, take the copies and leave the originals,
    use your system to do disk analysis.
  - Rent a similar computer setup so you don't need to take the hardware.

- Wear **latex gloves** at the scene to protect yourself. If fingerprint gathering is necessary, do electronic exam first, then dust or fume hood. Data is more important. You can always tie the floppy to the suspect in other ways -- only one with access to computer, etc.
- **Set up laptop near exit/choke point.** Every item carried out is recorded. Print evidence labels right there.
- **Start chronological case work sheet** (See table at bottom of these procedures. Fill this in electronically, then save table as a separate file in a folder named for this particular investigation. The file name should be the case report number followed by - followed by suspect name - last- first).
  - List the date, time, and description of the computer.
  - List the names of those assisting you and witnesses to your activity.
  - List the date, time, and action taken as you perform your search.
  - Record your investigative clues and leads that you might follow up on later.
- Evaluate the condition of the computer.
  - Is the computer on or off?
  - If the computer is on, what is it doing? If on, there is a good chance it might be tied into a bulletin board, Internet site, word-processing program with evidence, etc. Do not shut off before examining these possibilities.
  - Assess the potential for loss of data due to outside threats such as weather, electrical, and magnetic conditions.

        - Use the compass in the forensic kit to check doorways for degaussers (magnetic fields that could damage hard drive as you carry it out).
- Determine if the computer is connected to other computers by network or modem.
- Consider all the above conditions to determine if the computer should be turned off or left running for a period of time and photograph the screen with a video camera.
- Photograph the computer
    - Photograph the screen using a 35mm, Polaroid, video or digital camera.
    - Photograph the front and back of the computer.
    - Photograph the cables.
    - Photograph attached hardware.
    - Take pictures of anything that might be of value or used for evidence. This could be the hidden location of floppies, printed material, hard drives, and other hardware.
    - Sketch the scene, and take lots of notes.
- Search everywhere.
    - Begin from the computer and work your way outward, to include trash cans, etc.
    - Seize all printouts, diskettes, manuals, and examine any notebooks or notes for relevant material (passwords, security access, etc.)
        - Look for passwords on sticky notes around the monitor, under lamps, inside desks, inside covers of computer manuals.
    - Look for evidence of computer system ownership.
    - Check music CDs for computer CDs.
- Boot the computer from the floppy drive.
    - Decide whether to go to a:\> from a running computer or to reboot from a floppy. 999 times out of 1000 this is OK, but there are systems that have been modified to cause problems for anyone not knowledgeable in their use. Also, if a virus is active, you could infect your diskettes and hard drive.
    - If the computer is off, ALWAYS boot from a clean, write-protected floppy systems disk. Your latest version of MS-DOS (7.0, 6.0, etc.) should be able to handle the majority of all computers encountered.
    - Determine if special drivers (Super Store, Stacker, Disk Manager) are present. If so, you will need them in your boot disk CONFIG.SYS.
    - First, start a computer hard disk-lock program so destructive disk writes are not made to the suspect's computer. Run a virus scan, then save the CMOS, boot sector, AUTOEXEC.BAT, CONFIG.SYS, and device drivers to a floppy disk. Save a directory of the suspect computer files to a floppy disk. You can run software utilities by Andy Fried and Dan Mares on a disk using PROFILE.BAT to accomplish all this automatically against each disk drive and partition on the computer.
    - Obtain a printout of directories on site using the tree >prn command.
    - Back up the computer with LapLink, Safeback, network software, or EnCase to removable media. (See Chapter 3 in the book, Investigating Computer Crime, for tips on how to do this, or check EnCase training notes.)
- Mark and tag all cables and hardware.
    - Use wire tags and stick-on labels to ensure you can return the computer to its original configuration.

    - If you are seizing more than one computer system, first number the computers and then tag the cables and hardware using the computer number so that when you get the whole mess back to the shop, they can be put back together properly.
- Prepare the computer for transport.
    - Park the hard drive, unless it is a newer one that doesn't need parking.
    - Shut down the computer. Document keystrokes involved in securing the computer system.
    - Leave system disks in the computer while it is being transported to protect the floppy disk read/write. Floppy drives should be sealed in a manner that blocks access. Cover with tape, and initial over the top.
    - Label all of the components with case number, date, and initials.
    - Package the computer, cables, and other hardware in boxes after entering the evidence description in the search warrant program in the high-tech crimes unit laptop computer.
        - Pack CPU, monitor and printer separately, and cushion with bubble wrap, foam, blankets, etc.
        - Suspect still have original boxes? Doesn't hurt to ask, as he, too, would like his system protected.
    - Keep boxes for each computer together during transport and storage. That way, it makes it easier to group components with the system they came with.
        - Place one label on the item or its bag.
        - Place another label on the box identifying each item in the box.
    - DO NOT leave computer equipment sitting in your vehicle for any length of time. Cold, heat and direct sunlight can affect storage media. Extreme temperature variances can cause the hard disk to shrink or expand, which can create problems in reading the data.
- Seizing floppies and other removable media:
    - Color-code or number rooms to note where stuff was taken from. Electronics stores have tagging systems with duplicate numbers. Or ask officers to affix a different color-coded circle for each room.
    - Start an investigative notebook for floppies.
    - If a file is open and of apparent evidentiary value, save it to a clean floppy disk, NOT to the suspect hard drive.
    - Run floppies through Mares' Diskcat or similar diskette cataloging program and number them appropriately; or use EnCase to add them to the case file. Do not use pencils or ballpoint pens on the floppies as they can damage the media. Use instead indelible colored marker or labels.
    - Write protect all diskettes prior to review. Virus check (Don't erase viruses from disks, but instead note on the floppy that it is infected).
    - Create a diskette log, and **label each diskette a-1, a-2, a-3** etc., **"Contents,"** (games, credit card info, access code files, etc.) **"Disposition"** (directory printed, files printed, incriminating evidence obtained, file copied, etc.). Include hardware identification and operating system (Gateway PC, MS-DOS ver. 6.0).
    - Print a directory of each diskette and label the printout with an adhesive label bearing the same alphanumeric designation as the diskette.

  - If incriminating information is found, print the file contents and label the printout with an adhesive label bearing the same alphanumeric designation as the diskette and the directory printout.
  - Keep magnetic media separated from other seized items. This will help later in inspection of the disks so you do not have to look through dozens of boxes and envelopes for diskettes.
  - Placed seized diskettes in separate boxes for each room. It will save you a lot of time and trouble when sorting through them later.
  - Package in paper, not plastic, which can damage diskettes with static electricity.
- Search the area carefully. Diskettes hide themselves in the strangest places. They are often found inside books, taped to the bottom of keyboards, in chests of drawers, in shirt pockets, in wallets, in the trash, taped to the underside of drawers, and in other surprising places. Check them all.
- Pack the property van with care.
  - Place the CPU and other computer-related hardware and software in a safe place for transport.
    - Place them where they won't bounce around.
    - Place them away from magnets in radios in the trunks of vehicles. Radios and heat can damage hardware and media. Also be careful of electric motors and cell phones.
- Be wary of potential magnets and degaussing equipment at the crime scene. A simple compass will detect any strong electromagnetic currents.
- Before leaving the scene, print out search and seizure inventory (return) for the suspect.
- Debrief at the scene with the team to eliminate any unresolved questions. Ask them to document any new problems so we can build into future procedures checklists.

Guessing the suspect's password

Common password sources you might be able to learn about
in interviewing suspect and witnesses:

- Suspect name, first, middle, last, nickname, including backwards and initials, aliases.
- Social security number
- Birthdays (his own, spouse's, children's, parents'…)
- Anniversaries
- Names of children (first, middle, nickname)
- Name of pet
- Name of spouse
- Name of victim
- Name of favorite teacher
- Address
- Favorite sports figure
- Favorite fictional character
- Favorite television show (Star Trek fans -- "Kirk," "Spock," "Phaser," "Bones"

- Favorite computer manufacturer
- Other identification information

Back at the Shop

- Be sure that all evidence and equipment is stored in evidence away from phones, generators, magnets, etc. Tobacco smoke will also damage.
- To ensure no unauthorized person accesses the computer while you are processing it back at the shop, take the AC cord out of the back of the computer and lock it up so no one can power the system up.

Assignments at the Seizure Site

Entry team	➢ Announce the raid and breach entry ➢ Secure the site; looks for other threats throughout the structure ➢ Help the computer securing officer get everyone away from the computer ➢ Keep watch over computer seizure team as they work ➢ Function as arrest team; arrange for transportation of suspects arrested by uniformed patrol officers ➢ Take lots of notes		
Computer securing officer	➢ Get everyone away from the computer ➢ Unplug at wall socket after systematically shutting the system down ➢ Disconnect modems ➢ Disconnect and package computer and peripherals ➢ Check with compass for degaussing possibilities before removal ➢ Take lots of notes		
Interview Team	➢ Interview each witness and suspect ➢ Take lots of notes		Interview in an area away from the computers

Sketch and Photo Team	➢ Assign room letters or color code ➢ Photograph active screen ➢ Photograph system components, cables (strongly recommend videotape -- caution all on scene to watch what they say as video cam rolls) ➢ Sketch the scene ➢ Take lots of notes		
Physical Search Team	➢ Search each room ➢ Locate and mark evidence with colored stick-on dots for easy identification by seizure team ➢ Communicate each find with person logging all evidence on laptop computer ➢ Take lots of notes		Should be local officers as they will be needed in court for chain-of-custody issues. They do not need to be computer experts but should be thoroughly briefed on items to search for; and the should be thorough. They should know basics of how to handle electronic and magnetic evidence.
Technical Evidence Seizure and Logging Team	➢ Enter evidence data into computer ➢ Label and place evidence in bags or boxes ➢ Label boxes after evidence is photographed ➢ Take lots of notes		This team should include at least two people, one of whom is a computer investigator, the other a computer professional trained to handle and evaluate evidence. This team will also conduct forensic analysis later.

Case # **Location:**

Officer logging:

1	Date	Time	Action Taken/Investigative Leads
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			

Raid Preparation

- Tell other officers going in what ***NOT*** to do.
- Brief the plan of attack from your notes above, plus:
  - Mission (what you want to accomplish)
  - Execution (how best to do this, and when)
  - Avenues of approach and escape
  - Communications (how you will talk to one another -- radio and cell phones)
  - Diagram of the scene
- Assign areas of responsibility.
- Review officer safety information
- Review back-up plans
- Synchronize timing, especially if taking down more than one site
- Test equipment
- Time raid so you have best control and coordination with other teams
  - Go in before 6 a.m. before anyone is awake, or go into a business just as it is to open for business.
  - Control suspects
  - Check for booby traps, both physical and electronic
- Team debriefing at the scene to eliminate unresolved problems
  - If you encounter new problems, write them down so that we can build them into procedures checklists in the future