Standard Operating Procedures -- Pueblo High-Tech Crimes Unit
Investigative and Technical Protocols -- Computer Forensics Processing Checklist
2 June 2000

Computer Forensics Processing Checklist

Pueblo High-Tech Crimes Unit

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

The purpose of this document is to provide computer forensic technicians working with our Pueblo High-Tech Crimes Unit basic guidelines so that we are all doing the same thing or at least considering the same issues as we work a case either with an investigator from our own agency, or a request from another agency.

This is an education guide, not an instruction. It details documentation requirements for a computer forensics media analysis case after search and seizure of media. This takes the media analysis process from check out of evidence from the evidence room until complete support closure and report writing.

This is a living process that must allow for changes and updates, as well as flexibility and room for decision-making on the part of the media analyst to fit particular requirements of each case. However, there are core requirements that must be met for each and every case, or nearly all cases, and those will be explained in training.

Techniques may vary depending on the circumstances of the case, equipment availability, and the experience of the computer forensic technician.

Preliminaries

1. Begin tracking the man-hours you put into the media analysis and administrative work.
2. Verify search authority, consent, warrant, subpoena for exact legal level of analysis. Ensure what level of analysis and what files you can examine (i.e., Does the warrant cover e-mail, unopened e-mail, etc.). Get a copy of this document and place it in your analysis case file.
3. Pull up the master of the case documentation file and place it in the analysis case file.
4. Create a modified boot disk for the forensic software (EnCase). Ensure it is of the current version loaded on the forensic machine.

Determine Best Method

Determine the best method to process any computer-related evidence. If the Pueblo High-Tech Crimes Unit forensic examiner cannot process the evidence seized due to lack of experience, lack of training, or lack of equipment, the officer submitting the evidence or the forensic examiner will complete a Colorado Bureau of Investigation "request for assistance" form and submit the evidence to the CBI lab.

Prepare the Case File

Fill out all the necessary and place all initial case documentation in this file so that you can keep track of important details from the start of the forensic exam. Ensure you have a search warrant or consent to search when you open a case file, and ask the submitting officer to fill out the "Official Request for Laboratory

Examination." The most important part of this form is for the officer to fill out the keywords in the investigation that he wants you to search the computer for.

Fill Out a Media Analysis Worksheet

The "Media Analysis Worksheet" is used to track the flow and process of media analysis support. On this form, you record important information on the support provided. The form also tracks information needed to report periodically to the agencies or internal units that you support forensically about the assistance you have provided.

Create a Report to Attach to the Media Analysis Worksheet

Keep notes as you work, and provide as much information as you can on the following:

1. Date and time of evidence CPU
2. Current date and time (include appropriate time zone)
3. Significant problems/broken items
4. Lapses in analysis
5. Findings -- evidence found. This will go into your final report in more detail; these are "working notes" so that anyone -- a forensic colleague, an investigating officer, or a supervisor -- can pick up the file and, at a glance, know exactly where you left off in your assessment of the seized computer and media.
6. Special techniques required or used above and beyond normal processes (e.g., password cracker)
7. Outside sources used (e.g., commercial companies that provided assistance, information provided by other trained CCIs over the Computer Forensic Investigators Digest listserv on the Internet, etc.)

Log Out Evidence - Visual Inspection and Inventory

1. Log out all computer media and machines seized and to be analyzed.

2. If there are diskettes to analyze or other removable media (JAZ cartridges, zip cartridges, etc.), make sure that they are labeled sequentially (A1, A2, A3 etc.) and that that same labeling system is used as you acquire this evidence into the EnCase case image.

- Note: When you receive evidence, ensure the evidence tag properly reflects the items seized. Note any damage not documented on the evidence tag, take pictures of the damage, and write a supplemental report in the department mainframe computer system to detail what you discovered.

3. Also perform a visual inspection/inventory of the physical makeup of the seized computer. It is most important that you document the computer condition thoroughly.

4. Open/remove the CPU case. Examine its internal circuitry, make note of all media (hard drives, removable media drives, floppy drives, etc.). Where appropriate, make note of all internal expansion cards (e.g., where unusual cards are located, or where the internal devices could be pertinent to the investigation). Look for presence of a video capture card board in a child pornography case, and other details pertinent to this type of investigation (e.g., amount of RAM, CPU speed, etc.). Be sure to look for alternative storage devices such as flash memory, disconnected hard drives, etc. Verify that the system is configured to boot from floppy diskette, and record which floppy drive is the boot disk.

5. Determine if the CPU (case itself) contains potentially valuable information that would justify analysis. Verify that the CPU is functional, or at least contains some form of media. You might also look for

any hardware that could be used in the commission of the offense alleged in this case (a video capture board in a pornography case, etc.).

6. Record the position of all internal devices, to include hard drives, floppy drives, expansion cards, etc. Pay special attention to record jumpers, cabling, and other items that might need to be modified for analysis.

7. Photograph the system to document its condition upon arrival at the media analysis lab.

8. Review all seized items for evidence of mishandling or other damage. Look for out-of-place or broken cards, drives, etc.

9. Compare any damage to that noted on the evidence tag, and record any appropriate changes. Photograph ALL damage to evidence, regardless of severity. If the damage will impede analysis, advised the requesting official or case officer.

Split Evidence Tag Procedures

1. On some occasions, you will have to remove a hard drive from the computer system in order to do the analysis. If the hard drive is separated from the original evidence, then you must tag it separately, or use an indelible Sharpie-type marker to record the case number, suspect name, machine number, etc. on the hard drive you have taken out.

2. The new evidence tag will be the same as the original, but be followed by an "A," "B," or similar designator. You can number the hard drives found in the machine so that they can identified separately.

3. A description on the hard drive evidence tag might read: "This hard drive (serial number, model, etc.) was removed from Tag # (XX) for purposes of analysis. This is a continuation of Tag # (XX) and completed by Officer John Doe.

4. Note the person receiving the property initially and the name of the forensic examiner who removed the hard drive from the machine.

5. Maintain the chain of custody of the hard drive using this new tag until analysis is finished and the hard drive is reinstalled in the original CPU.

6. If you return the CPU minus the hard drive back to the evidence custodian, then note the original tag in the "chain of custody" report as follows:

Released by -- forensic examiner's name
Purpose: Released to evidence custodian
Condition: Changed. Removed hard drive for analysis (see Tag XX-A)
Received by: Evidence custodian

7. After analysis of the hard drive is completed, reinstall the drive into the original CPU. Annotate Tag XX-A in the "chain of custody" report as follows:

Released by: Name of forensic examiner
Purpose: Released to evidence custodian
Condition: Changed. Reinstalled hard drive into CPU
Received by: Evidence custodian

8. After the hard drive is reinstalled and Tag XX-A is annotated appropriately, attach Tag # XX-A to the original tag XX.

NOTE: After you visually inspect the hardware, you are ready to start the analysis.
NOTE: Take photos (digital pictures are even better) of media and place this in your case file.

Create An Analysis Directory

Create a directory for the analysis on the government-owned forensic examination computer. This is the directory that will be used during the analysis to deposit potential evidence, keyword files, and disk images.

Create a Keyword List

Review all case data in order to render a potential analysis process (suicide, child porn, murder, fraud, etc.). Create a list of keywords to be searched or get the list from the officer on the case. Place a copy of this in your analysis case file.

Subject's Computer

1. Check the computer's CMOS settings to be sure the computer is configured to boot from floppy diskette and boot the machine from the modified EnCase boot disk.

2. Verify that the system clock reflects the actual date and time. Record in your analysis notes the correct date, time, and time zone, the date, time and time zone reported by the SUBJECT's computer, and the difference.
3. Identify all hard drives by make, model, capacity and condition. Record this information, as well as whether the device is internal or external. Where necessary, photograph individual hard disks to document damage or other unusual condition.
4. Power down the computer and identify the hard drive master/slave settings (if IDE) or SCSI ID settings (if SCSI). Record these settings, and change where necessary to mount into the government-owned forensic examination computer. Be sure to note any and all changes to evidentiary media.
5. Locate the parameters of the hard drive itself by going to the manufacturer's home page (e.g., www.seagate.com). Where necessary, manually modify the government computer's CMOS settings to accurately reflect the correct settings for the particular drive being analyzed.

Government Computer Media Analysis Workstation

1. Based on what media you have on hand to do the job, the size of the suspect evidentiary media, and the like, select the most appropriate backup utility (usually EnCase, but maybe SAFEBACK or another alternative). Where possible, use a hard disk of equal size and interface (EIDE, SCSI, etc.). For drives larger than the available media, use 8mm DAT. Verify the target media is large enough to hold the image of the evidence media. If a hard drive is to be used as the target media, mount it so it is accessible to the analysis computer, without being subject to the drive write-protect software.
2. Attach the SUBJECT's hard drive to the government computer for analysis, or hook into the suspect machine with a parallel port cable for parallel-to-parallel imaging.
3. Check the computer's CMOS settings to be sure the computer is configured to boot from a floppy diskette. Boot the machine using the modified boot disk, following instructions on using the EnCase forensic software.
4. As you work to acquire an image, compare the reported information with that indicated on the suspect machine to verify the forensic computer has correctly identified the drive.
5. Create an image using EnCase with the SUBJECT's hard drive.
6. Return evidence to secure storage. Where appropriate, return to evidence custodian for safekeeping.

7. Using EnCase, examine the file structure and browse directories and subdirectories looking for evidentiary files.
8. At the same time, search the image by keywords of the investigation.
9. Search for all files with extensions that would indicate the file requires special handling. These include .zip, .arc, .tar, .gz, etc. Also examine application files that might be password-protected (MS Word, Excel, Quicken, etc.). If merited by the allegation (computer intrusion, etc.), or specifically addressed in the request for support, it may be necessary a review of the file headers. Where found, decompress all compressed files and review their contents.
10. Examine the file structure for applications that could be pertinent to the investigation (for example, a file conversion utility/viewer in a pornography case).
11. Execute any applications that could provide information valuable to the analysis. Take note of any log files/configuration settings or other potential sources of information. Record the names of those applications executed, and any valuable data gathered during runtime.
12. Create an "Analysis and Findings" directory on government-owned media (i.e., zip disk, hard drive, Jaz disk, etc.). Report and transfer all findings to a separate directory under your findings directory that reflects location where files originated from.

Diskette Analysis

1. To simplify analysis, separate all floppy diskettes and verify each diskette is write-protected. On a 3.5" floppy diskette, if facing you, the write-protect slot (if present) is found on the upper right hand corner and should be covered.

2. Using your EnCase program, perform an image copy of each diskette, then add these individual evidence file to your case.

3. Prior to any acquisition, scan each diskette using a trusted virus protection utility. If the program alerts to presence of a virus, label SUBJECT's diskette as infected to prevent accidental contamination of other media. Record the virus' presence (name, infected files, etc.) in your analyst notes.

Create Findings and Analysis CDs

1. Copy evidentiary files from your "save" subdirectory on the evidence-processing computer to a CD-ROM. Be certain to include the appropriate utilities on the CD-ROM for recreation of the original files by the end user (district attorney, investigator, defense).
2. Be sure to make a spare copy of this evidentiary CD to place in evidence. Include in the final report the EnCase report (keyword listing, logical file listings, search results, and a thorough listing of physical image files, free space, slack space, and deleted files, where appropriate).

Case Report Writing and Documentation

1. Document the entire computer media analysis and your conclusions in an "Investigative Analysis Report." Provide this report directly to the case officer. Provide the case officer with the following:

- Signed original "Computer Forensic Investigative Analysis Report"
- All forms used
- Analysis notes, where appropriate
- Items produced as a result of the analysis (CDs created, printouts, etc.)
- Copy of authority to search (consent, search warrant, etc.)
- Evidence listing
- Media Analysis Worksheet
- Keyword lists used

- Request for support
- Other forms, documents, or important correspondence

2. Identify any files pertinent to the investigation and print them out for inclusion as attachments to the analysis report.
3. Where large numbers of files found are pertinent to the investigation, coordinate with the district attorney to discuss need for prints. If too much in quantity, representative samples may be printed for inclusion in the case file. An example would be the presence of several hundred child pornography pictures on a SUBJECT's hard drive. Twenty or 30 representative samples may be all that is necessary to print and include as a hard-copy attachment. One gigabyte of information on a hard drive might result in 150,000 pages of printed material. The purpose of including the findings CD is to eliminate the need for printed material.

Notes of Importance

It is important to remember a few things while writing your report:

1. Don't make any assumptions. If you discover an e-mail, don't assume you know the recipient's name from the e-mail address alone. An e-mail addressed to "Matt," whose e-mail address is msmith@iex.net, does not necessarily mean that the recipient's name is Matt Smith. E-mail addressed can be faked easily.
2. Do not identify any leads. The report is for the case officer, and it is his or her job to identify the leads. If you discover something important during your analysis, write it up so it is obvious to the officer without providing a lead.
3. Spellcheck is your friend. Don't wait for a supervisor or district attorney to proofread your report! Spellcheck it before it leaves your machine.
4. Double-check your findings media. If you create a findings CD, make sure the data is really on it before you turn it in to your case officer.