Standard Operating Procedures -- Pueblo High-Tech Crimes Unit
Investigative and Technical Protocols -- EnCase Forensic Imaging and Evidence Acquisition
2 June 2000

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

EnCase Forensic Evidence Acquision and Analysis

GENERAL PROCEDURES

The following outlines standard processing procedures used in examining fixed and removable media. Selecting which procedures are appropriate is at the discretion of the computer forensic examiner, in consultation with the case officer. Decisions on which techniques are used depend on the facts of the case and information presented by the investigator, coupled with training and experience of the computer forensic examiner. No two cases of forensic examination are exactly alike due to these and other factors.

1. The examining computer system is a sheriff's office-owned, DOS-based Gateway E-3000 running under MS-DOS 7.0 and Windows 95. The system is equipped with one 3.5" floppy drive, a read-only CD-ROM drive, another CD-ROM that is write-able (able to "burn" or copy evidentiary information from suspect files) and an external Iomega 100 mb zip drive. The zip drive and floppy drive are both capable of reading/writing to removable media. The primary government media for examining images of a SUBJECT's computer is a 40-gigabyte hard drive in a removable hard drive bay. The machine has an additional removable hard drive bay where we can place a SUBJECT's IDE hard drive for direct drive-to-drive imaging, as well as a SCSI cable we can use to acquire an image from a SUBJECT's SCSI hard drive. In addition, we have a Hewlett Packard SureStore T20 tape drive attached that we can use to back up evidentiary files up to 10 gigabytes native or 20 gigabytes in a compressed format.
2. Prior to analyzing the hard drives from the CPUs seized, we **use EnCase to make an exact duplicate of each hard drive.** These image files are then archived to the HP SureStore tape drive for future reference, and, if necessary, can be transferred to a write-able CD-ROM or a larger-capacity Travan 20-gig tape for investigators and prosecutors, and eventually for use in the discovery process.
3. Our **EnCase version is 1.99.** EnCase, a forensic data acquisition program for Windows 95/98/NT, is based on law enforcement specifications and requirements. It reads all DOS and Windows hard disk and removable media, including FAT 32 drives, and allows the forensic investigator to save an exact snapshot of a disk to an evidence file, including hidden and deleted files, even the data contained in unallocated disk space and partitions. Every file is an exact, sector-by-sector copy of a floppy, zip disk or hard disk; every byte of the file verified using a 32-bit CRC (cyclical redundancy check -- similar to a checksum). In essence, this compares two very large, unique numbers to one another to say, for a certainty, that the evidence file

created matches exactly the files captured from the original media. That way, the forensic examiner can assure investigators, attorneys, and indeed judge and jury, if necessary, that the two match and have not been altered in any way. Odds that two different strings produce the same CRC are roughly 1 in 4 billion.

4. **EnCase allows us to tie directly into the suspect computer** with our evidence processing computer via a standard null modem cable and do a duplicate image so that we search and work on the image of the original evidence, and do not do the examination directly on the suspect's files, which prevents alteration of any kind. We can also remove the hard drive from the SUBJECT's machine and place it in the evidence processing machine to acquire an image drive-to-drive, which is faster than the parallel-port method.
5. **We can use EnCase to view files without changing the file contents or time stamps,** and to acquire, authenticate and build a case out of the most common types of media -- floppies, zip disks, jaz, and all IDE and SCSI hard disks.
6. **EnCase allows us to quickly search a hard drive by keywords, cutting down on investigative time** and preventing access to computer files not the subject of the examination by virtue of a specific search warrant. The program allows us to pull up and view deleted files automatically, see fragments of information in the "slack" (where bits of erased files reside until overwritten), and bookmark interesting files and file segments to come back to later or to save to another media for permanent storage of evidence. We can also export any part of a file, any selected files, or even an entire folder or tree (folders, subfolders, and files) with ease. We can also restore an entire hard disk volume back to its original state.
7. EnCase allows us to view graphic files (possible pornography) in a "thumbnail" view that can be easily copied or put on a CD-ROM, making it unnecessary to use other computer investigative software.
8. The EnCase program prints nicely formatted reports that show the contents of the case, dates, times, investigators involved, and information on the computer system itself. Those reports are enclosed with the "Computer Forensic Investigative Analysis Report."
9. In processing these machines, we use the EnCase DOS version to make a "physical" image; in other words, we got the entire hard drive, without being selective as to files captured in the EnCase image file. We then copy what we find to disks to relay to investigators, district attorney's office, and the defense. Following examination, we make a copy of the EnCase image file and evidentiary files "saved," and back them up on a Travan Technology 20-gigabyte cartridge in case law enforcement investigators or 10th Judicial District investigators and attorneys need other questions answered from this computer seizure. We then return the original evidence in the SUBJECT's computers with hard drive intact (nothing changed) to the submitting agency's evidence room.

Overview of What A Forensic Examiner Can Do With EnCase

- Determine whether a computer system contains evidence and is within the scope of our investigation
- View files without changing the file contents or time stamps
- Acquire, authenticate and build a case out of the most common types of media. Read:
  - Floppies
  - Zips
  - Jaz
  - All IDE and SCSI hard disks
- Do a basic keyword search of the entire case using any number of search terms
- Do advanced searches using the powerful UNIX GREP syntax
- Sort files according to any number of fields, including all three time stamps
- Bookmark interesting files and file segments and save these for future browsing
- Export any part of a file, any selected files, or even entire folder trees with ease
- Restore entire disk volumes back to their original state
- Recognize and validate file signatures and add your own signatures
- Browse basic file system artifacts such as the swap file, file slack and spooler files, and the recycle bin
- Recover printed and faxed pages just as they came out on the printer
- Prepare computer evidence for court presentation
- View the entire case at once
- Print a nicely formatted report that shows:
  - contents of the case
  - dates
  - times
  - investigators involved
  - a graphical map that shows disk allocation by cluster or sector including layout of any file
- Access a bookmark table to show a list of every bookmark the examiner created for easy reference and locating evidence found later for case consultation and presentation
- Access a search view that shows every search with the results
- Remotely preview a computer with a parallel cable, without creating an image file first
  - View and copy files (even graphics) without changing a bit of the suspect drive
  - Perfect for quick searches and overviews of the SUBJECT's computer when consent is obtained to search
- View graphic files in a “thumbnail” view that can be easily copied or put on a CD-ROM

What is EnCase???

- A forensic data acquisition and analysis program for Windows 95/98/NT
- Based on law enforcement specs and requirements
- Purpose: To aid in computer-related investigations

EnCase Features

- Read all DOS and Windows hard disks and removable media, including new FAT32 drives
- Password protect any piece of evidence to control chain of custody
- Save an exact snapshot of a disk to an evidence file, including hidden and unallocated disk space and partitions
- Combine evidence files to create a case that you can search as a unit
- View files without changing file contents or time stamps
- View, search, filter and sort every file from every disk and computer in the case in one pass; see the results graphically on the screen
- Graphical Allocation Map shows a disk cluster by cluster
- Formatted report shows all case-related information
- Powerful search features include background search and GREP keywords

Installation is simple…

- One small floppy disk
  - Run
  - A:\SETUP
  - OK
- To run EnCase, either:
  - Double-click icon, or
  - START-PROGRAMS-ENCASE
- Hardware key (dongle) is necessary to use the copyrighted program
  - Activates complete features of EnCase
  - Place on parallel port before starting EnCase program

Acquiring evidence…

- Make a “logical” image with the Windows version, or
- Make a “physical” image with the DOS version (EN.EXE)
- To create an evidence file in Windows:
  - Click “Create” button, or select FILE-CREATE EVIDENCE FILE
  - Select the volume you want to scan
  - NEXT
  - Choose highest level of lock you can for the media
  - NEXT

- Choose the level of compression
    - Specify output file
    - NEXT
    - Fill in all relevant case information
    - Use notes to describe where you found the disk/system
    - NEXT
    - Enter password to protect evidence file, if necessary
    - FINISH
    - EnCase starts creating an evidence file. Progress bar indicates bytes read and time to completion.

Creating a DOS boot disk

- Used to boot the evidence computer to a safe version of DOS
- Open the case containing the search terms you wish to use
- Insert a 1.44 MB disk in lab computer
- TOOLS-CREATE BOOT DISK
- CREAT DISK
- Make sure to check the **Copy System Files** option
- START
- Test diskette by rebooting from the floppy and running EnCase DOS from disk

Determining whether a drive contains evidence

- Do you have probable cause to collect evidence???
- Turn off computer
- Open to inspect for unusual connections or configurations
- Insert DOS boot diskette and turn on computer
- Run CMOS setup routine to ensure all physical disks are recognized by BIOS
- At A:\ prompt, type EN to run EnCase for DOS
- Drives and partitions seem right ? SPACE to continue
- Want to search Drive 0? YES
- When prompted for name of case file (SEARCH.CAS), choose, or specify a CR delimited text file you have created with search terms. Type in filename, ENTER to begin searching. ESC to quit, SPACE to pause.
- When search text string found, EnCase writes text and surrounding text to screen, and highlights the keyword.
- Create evidence file? YES if you are satisfied suspect computer contains evidence.

Acquiring evidence in DOS

- Proceed as you did above, then…
- Like to search Drive 0? NO.

- Create an evidence file for Drive 0? YES
- Enter case number, investigator, etc.
- Assign numeric code for this piece of evidence (the computer)
- Enter description: Desktop 1, Laptop, etc.
- System date and time OK? ENTER
- Enter relevant notes ENTER
- Create a compressed evidence file? YES (if you want to do…)
- Enter path where you will store evidence (Drive letter of attached tape backup drive, zip drive, laptop, etc.) e.g. d:\disk ENTER
- Exchange disk if evidence drive fills up
- Label disk with filename EnCase assigns
- JSMITH.E01, .E02, ...

Using a Lap-Link connection in DOS

- Ensure power-saving features of your computer, if any, are disabled.
  Make sure ports on both computers are set to ECP.
- Connect computer's parallel port to lab computer with null-modem parallel (lap-link) cable.
- Insert DOS Boot disk, and turn on evidence computer.
- EN/S to run EnCase for DOS server mode.
- Run EN on your lab computer.
  - Will detect and configure the connection automatically
- Everything you see on your lab laptop will be a reflection of the evidence computer
- Proceed as you would for normal evidence acquisition, using your lab computer to "drive" the evidence computer

Building a case

- EnCase can organize different types of media together so that they can be searched as a unit rather than individually.
  - hard drive
  - floppies
  - file fragments
  - zip disks
- To keep the case organized:
  - Create a new folder for every case
  - Put all evidence files and the case file in the folder to keep them together

Creating a new case

- FILE-NEW CASE
- EnCase Report appears and indicates that this case currently has no evidence
- FILE-SAVE
- .cas extension automatically added to the file
- Save each case in a separate folder

Adding evidence to a case

- FILE-ADD EVIDENCE (or click on the + icon)
- Select an evidence file and click Open
- 7 “views”
  - Report View
  - Evidence View
  - Case View
  - All Files View
  - File View
  - Volume View
  - Bookmark View
  - Search View

Report view

- Description of the case contents
- Dates
- Times
- Investigator
- Technical elements of the evidence file
- Bookmarked sections automatically summarized here
- Provides a clear, concise chain of custody

Evidence view

- A table of every evidence file in the case
- To verify the integrity of evidence in this view:
  - Select the row, and choose VIEW-VIEW FILE INTEGRITY

Case view

- Works like Windows Explorer
- Tree-structured view of evidence, showing how each file relates to the others hierarchically
- Presents each evidence file as a folder that contains files

- Tree of case folders on the left side, listing of files in the folders on the right side
  - Displays
    - name
  - file attributes
  - type
  - size
  - creation date
- Sort columns by **double-clicking** in the column header
- Find an interesting file? Come back to it later by clicking in the box to the left of the row number
- Add up to 5 columns to sort -- Select the column, VIEW- ADD COLUMN TO SORT
- To view contents of a file, **double click** the file; works for all files:
  - text files
  - audio and movie files
  - pictures

All files view

- Displays a table of every file in the entire case.
- See EVERYTHING in one place!
- If you want to look at every JPEG file on the hard drive, sort by file extension and look at them as a group.
- Path column shows file locations

File view

- Shows contents of the selected file in hexadecimal and text format
- File slack is shown in red
- Use button on far right to switch between hex and text view

Volume view

- Top half displays a cluster map
- Bottom half displays selected cluster's contents
- Each colored box represents a cluster
- Disk view is similar to volume view, except that the disk is shown by sector rather than cluster. Each colored box represents one cluster on the physical disk.

Bookmark view

- Shows a table of bookmarks added by the user.
- Click on the **File View** tab to return to the place in the file where the bookmark is located.

Search view

- Shows a “tree” of past searches.
- When a search is completed, results will be shown in this view under the name you typed in when the search began.
- Keywords associated with the match (coke, deal, etc.) pop up when you click **Matches** to view all the hits found in the search.

Searching the case

- Starting the search
  - **TOOLS-SEARCH**
  - Search the entire case or only selected files
  - Check **Verify File Signature** to examine each file’s extension and compare it with the file’s signature - flag file
  - **Checking File Slack** option tells EnCase whether or not to check the area between the logical and physical end of the file for evidence
  - **Search Priority option**
    - Choose amount of computer resources to devote to search
  - **Adding keywords**
    - Select the **Keywords** tab in the search dialog box
    - Click **Add**
    - **Add Search Text** dialog box appears
    - Enter keyword in the text textbox
      - Actual text
      - GREP expression
    - Keywords are NOT case-sensitive. To change:
      - Check the **Case Sensitive** option
    - Check **GREP Expression** if you entered a GREP
    - OK to add keyword to list
    - Repeat for each keyword
    - **Searching in the background**
    - Click **OK** to begin searching the case in the background
    - To stop:
      - **TOOLS-CANCEL SEARCH**

Viewing search results

- Each search is shown by the name you typed in when you ran the search.
- Click **Matches** node to show all the file fragments that contain hits.
- The keyword associated with the match is in the column just to the right of the text strings found.
- GREP expressions

- GREP is a UNIX search utility with powerful, flexible syntax
    - Uses characters such as:
    - .
    - *
    - +
    - #
    - [ ]
    - ^
    - [-]
    - \
        - They **DO NOT** have the same meaning as in DOS
- **GREP examples**
    - john.smith
        - The "." period matches any character. This expression finds "john" followed by any character followed by "smith"
    - john smith
    - john,smith
    - johnQsmith
- http://www\[a-z]*\.com
    - This expression matches "http://www." followed by any alphabetic characters followed by ".com." Good way to look for web site references.
- http://www.bozo.com
    - **NOT** http://www.bozo.org
- ###-###-###
    - The "#" character matches any number. This expression matches a social security number with the numbers separated by dashes.
        - 123-36-3410
        - NOT 123456789
        - NOT 456
    - (*###[) \-]*### [\-] *####
        - This expression matches a U.S.phone number in several formats.
        - (909) 875-4125
        - NOT 1233456ABC
            - NOT 456

File signatures

- Signature at beginning of document files and graphics files well-defined
- Allows viewers to recognize the type of file regardless of file extension
- EnCase uses this convention to look for files that have been renamed in order to hide their true contents.
- Picture.bmp file changed to readme.txt file
- Search shows mismatches as part of search results

Bookmarks

- Can mark files or sections of a file that you are interested in
- All bookmarks saved along with the case
- View anytime by clicking the **Marked** tab
- Find a file you want to remember?
  - Right click the file
  - **ADD BOOKMARK**
  - Add a comment to the bookmark to help you remember its purpose later
- **Bookmarking a range of data**
  - If you see an interesting group of characters in a file in the file view…
  - Select the range
  - Right-click inside the highlighted area
  - **ADD BOOKMARK**
  - **Add a comment to remember it**
    - “the night of the murder”
- **Viewing bookmarks**
  - Click **Marked** tab
  - Double click **Bookmark** to view evidence in its context
  - Preview bookmark data in the column next to the short name you gave the bookmark

Viewing and recovering data

- Recover files in the **simplest way possible** while still maintaining the **integrity of the evidence**!!!
- **Viewing file contents**
  - Click on **File** to view contents.
  - In hex view, status bar at bottom of the screen shows exact position of the cursor in the file, volume, and disk.
- **Selecting files**
  - Click on the square to the left of the number in the file view
  - To select entire folder:
    - Click on square next to folder in tree view
- **Copying/unerasing files**
- When copying a deleted file, EnCase will, if possible, unerase it automatically.
  - This means you can treat normal and deleted files consistently.
- **To copy a group of selected files:**
  - **VIEW-COPY/UNERASE**
  - NEXT
  - Choose the character to put in front of the deleted file names
  - NEXT, and choose destination for the copy
  - FINISH

- **Copying entire folders**
  - Click the **Case** tab, and select the folder you would like to copy.
  - Choose **VIEW-COPY** FOLDER
  - Choose a destination on your lab computer
- **Evidence file authentication**
  - Evidence file format:
  - Every file is an exact, sector by sector, copy of a floppy or hard disk
  - Every byte of the file is verified using a 32-bit CRC
  - It is e**xtremely difficult, if not impossible** to tamper with evidence once it has been acquired!!!
- **Checksum**
  - CRC
    - CRC is a variation of the checksum, and works in much the same way. Odds that two different strings produce the same CRC are roughly **1 in 4 billion!!!**
- **Verifying an evidence file automatically**
  - To verify manually
    - Choose the evidence tab
      - **VIEW-VERIFY FILE INTEGRITY-VERIFY**

Free technical support

Phone (626) 441-3915
FAX (626) 799-4364
Free Internet minor updates and bug fixes

Contact information for EnCase

Mail: Guidance Software Inc., 729 Mission St., Suite 170, South asadena, CA 91030

Phone: (626) 441-3915

FAX: (626) 799-4364

E-mail: info@guidancesoftware.com

World Wide Web: www.guidancesoftware.com