EnCase: A Case Study in Computer-Forensic Technology

Lee Garber

If you talk to many of the police departments in the US with computer-forensics units, they'll tell you that the tool they use most often is EnCase.

In fact, about 2,000 law-enforcement agencies around the world use it, according to Jennifer Higdon, spokesperson for Guidance Software, manufacturer of EnCase.

EnCase, a 1-Mbyte program written in C++, offers an integrated set of forensic utilities. Up to 15 tools were required to provide the same functionality in the past, which made the investigative process time-consuming, expensive, and sometimes incomplete, said company president and general counsel John M. Patzakis.

With EnCase, investigators start by placing a suspect's hard drive in their forensic computer. The drive can be from a Windows, Macintosh, Linux, or DOS machine. EnCase then makes a bit-stream mirror image of the drive.

The mirror image is mounted as a read-only evidence file. This prevents investigators from altering the data and thereby invalidating it as evidence, said Bob Sheldon, Guidance's vice president and director of training. To verify that mirror-image data is the same as the original, EnCase calculates cyclical redundancy checksums and MD5 hashes.

EnCase subsequently reconstructs the drive's file structure using logical data in the mirror image. The investigator can then examine the drive via a Windows GUI, as shown in the figure. The Windows interface lets investigators use multiple tools to multitask, something that past forensic tools' DOS interfaces didn't permit, Sheldon noted.

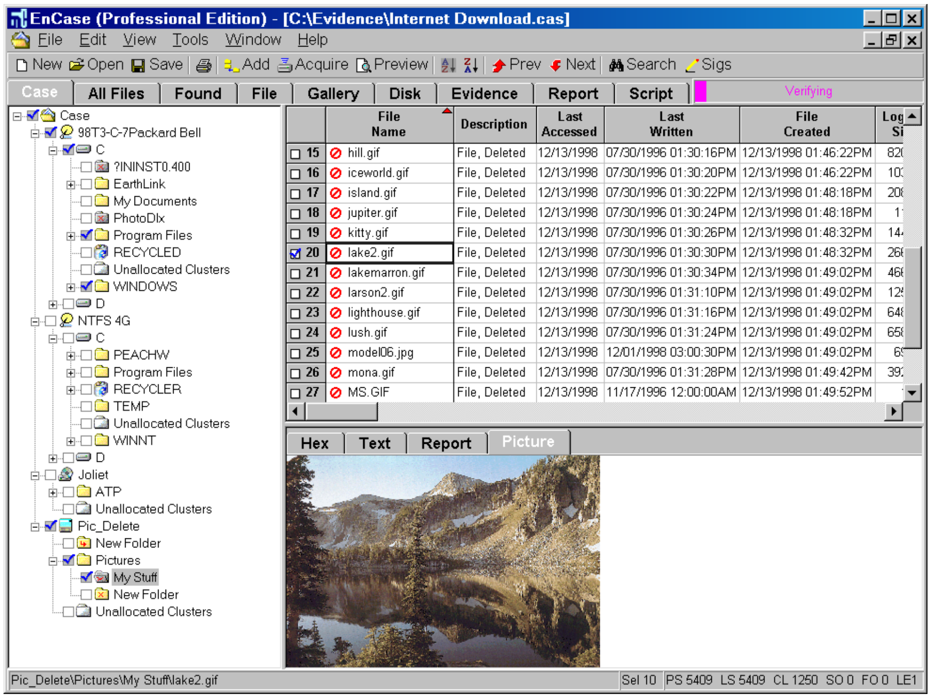
In examining a drive, EnCase goes beneath the operating system to view all of the data—including file slack, unallocated space, and Windows swap files—in which deleted files and other potential evidence can be stored, said Sheldon. Users generally could not view such areas of the drive via the operating system alone.

In displaying files, EnCase can sort them based on various criteria, such as extension or time stamp. In addition, EnCase compares known file signatures with file extensions so investigators can determine whether the user has tried to hide evidence from detection by changing its extension. Guidance also offers an EScript macro language that lets advanced users build EnCase tools to provide customized functionality.

Although EnCase automates the examination process, Patzakis said, "It is still not something the layman can pick up right away. Even an IT person needs a good week of training on the software."

Some criminals apparently are also aware of EnCase. Detective Christopher Hapsas of the Los Angeles County Sheriff's Department's High-Tech Crimes Detail said there is a utility called Evidence Eliminator that zeroes out a hard drive, rendering EnCase useless.

Nonetheless, said William D. Taylor, president and CEO of the International Association of Computer Investigative Specialists, "It's a great program. I use it every day. It does the work for you, if you know what you're doing."


EnCase (Professional Edition) - [C:\Evidence\Internet Download.cas]
File Edit View Tools Window Help
New Open Save Add Acquire Preview Prev Next Search Sigs
Case All Files Found File Gallery Disk Evidence Report Script
Verifying
Hex Text Report Picture

- ☑ Case
  - ☑ 98T3-C-7Packard Bell
    - ☑ C
      - □ ?ININST0.400
      - □ EarthLink
      - □ My Documents
      - □ PhotoDlx
      - ☑ Program Files
      - □ RECYCLED
      - □ Unallocated Clusters
      - ☑ WINDOWS
    - □ D
  - □ NTFS 4G
    - □ C
      - □ PEACHW
      - □ Program Files
      - □ RECYCLER
      - □ TEMP
      - □ Unallocated Clusters
      - □ WINNT
    - □ D
  - □ Joliet
    - □ ATP
    - □ Unallocated Clusters
  - ☑ Pic_Delete
    - □ New Folder
    - ☑ Pictures
      - ☑ My Stuff
      - □ New Folder
    - □ Unallocated Clusters

	File Name	Description	Last Accessed	Last Written	File Created	Log Si
□ 15	hill.gif	File, Deleted	12/13/1998	07/30/1996 01:30:16PM	12/13/1998 01:46:22PM	820
□ 16	iceworld.gif	File, Deleted	12/13/1998	07/30/1996 01:30:20PM	12/13/1998 01:46:22PM	103
□ 17	island.gif	File, Deleted	12/13/1998	07/30/1996 01:30:22PM	12/13/1998 01:48:18PM	208
□ 18	jupiter.gif	File, Deleted	12/13/1998	07/30/1996 01:30:24PM	12/13/1998 01:48:18PM	1
□ 19	kitty.gif	File, Deleted	12/13/1998	07/30/1996 01:30:26PM	12/13/1998 01:48:32PM	14
☑ 20	lake2.gif	File, Deleted	12/13/1998	07/30/1996 01:30:30PM	12/13/1998 01:48:32PM	26
□ 21	lakemarron.gif	File, Deleted	12/13/1998	07/30/1996 01:30:34PM	12/13/1998 01:49:02PM	46
□ 22	larson2.gif	File, Deleted	12/13/1998	07/30/1996 01:31:10PM	12/13/1998 01:49:02PM	12
□ 23	lighthouse.gif	File, Deleted	12/13/1998	07/30/1996 01:31:16PM	12/13/1998 01:49:02PM	64
□ 24	lush.gif	File, Deleted	12/13/1998	07/30/1996 01:31:24PM	12/13/1998 01:49:02PM	65
□ 25	model06.jpg	File, Deleted	12/13/1998	12/01/1998 03:00:30PM	12/13/1998 01:49:02PM	6
□ 26	mona.gif	File, Deleted	12/13/1998	07/30/1996 01:31:28PM	12/13/1998 01:49:42PM	39
□ 27	MS.GIF	File, Deleted	12/13/1998	11/17/1996 12:00:00AM	12/13/1998 01:49:52PM	

Pic_Delete\Pictures\My Stuff\lake2.gif Sel 10 PS 5409 LS 5409 CL 1250 SO 0 FO 0 LE1

EnCase lets investigators examine digital evidence files via a Windows interface. EnCase also can combine related evidence files from different drives into one case file. On the left is a case file's directory structure, at the top right is the list of evidence files in the directory the user has accessed, and at bottom right is the selected file.