

REAL EVIDENCE, VIRTUAL CRIMES

THE ROLE OF COMPUTER FORENSIC EXPERTS

By Paul H. Luehr

The incoming e-mail demanded that Best Buy Co. pay \$2.5 million. The message came from jamieweathersby@netscape.net, and according to a company spokeswoman, the sender “said he found a security glitch and was going to use it to put customer data on our site unless we paid him. . . .” (See *Mississippi man denies Best Buy blackmail*, C/Net News, (Jan. 7, 2004), http://news.com.com/2100-7355_3-5136932.html). Best Buy found no security breaches, but immediately reported the extortion attempt to federal authorities. After several weeks of investigation, 26-year-old Thomas E. Ray III, of Jackson, Mississippi, was arrested and indicted.

At trial, the government presented evidence that “Jamie Weathersby’s” Netscape e-mail box had been accessed from an AOL dial-up account, telephone number, and street address assigned to the home where Ray lived with his parents in Jackson. The government also presented evidence that previous extortion demands from “Jamie Weathersby” were tied to Ray. Most importantly, an FBI forensic expert showed that Ray’s computer contained several screen shots of the “Jamie Weathersby” Netscape e-mail box and copies of extortion e-mails sent to Best Buy.

The defense argued that some evidence could be traced to locations outside Mississippi and that some extortion e-mails were missing from Ray’s computer. The defense also presented two forensic experts who testified that the defendant’s

computer once contained a virus that might have allowed a hacker to take over Ray’s machine and send the offending e-mails. On cross-examination and in rebuttal, the government elicited testimony that the virus was only known to replace the home page within a computer’s Internet browser, not take full control of the machine. The government’s computer forensic expert also showed that the virus had not infected Ray’s computer, but rather the lab computer belonging to the defense expert himself. After six days of trial, the jury convicted Ray of extortion and making threats to damage computers. He was sentenced to 18 months in federal prison.

Cybercrime trials often turn on a battle between competing computer forensic experts. As a result, both prosecutors and defense attorneys are asking: What types of evidence can computer forensic experts provide? How can computer evidence be recovered and preserved? How should an attorney go about finding a qualified expert? How should the expert’s testimony be presented at trial? What issues do experts commonly contest in cybercrime cases? This article attempts to answer each of these questions.

Evidence provided by computer forensic experts

The range of evidence that experts can provide in cybercrime trials is as wide and varied as the cases themselves. An expert on network security can explain the vulnerabilities exploited by hackers in a distributed denial of service (DDoS) attack or Web site defacement. An expert on adolescent development can use the so-called “Tanner scale” or other methods to analyze body proportions and estimate the age of a victim in a child pornography case. And a psychologist or criminal profiler can analyze threatening e-mails sent to a company CEO. By far, though, the most common and powerful expert used in cybercrime cases is the computer forensic examiner.

The evidentiary value of computer data. The power of computer forensics arises from both the quantity and quality of digital evidence being mined. In sheer volume, digital evidence often overwhelms the testimonial, physical, or documentary evidence in the possession of the trial lawyer. This is even true in white-collar cases where prosecutors and defense attorneys are swimming in bankers’ boxes full of paper. Consider the fact that one CD can contain the equivalent of 325,000 typewritten pages, that a 40-gigabyte hard drive in a laptop computer can hold 20 million pages, and that one terabyte of storage on a corporate computer network can hold the equivalent of 500 billion typewritten pages. (See *THE MANUAL FOR COMPLEX LITIGATION* (4th ed.) § 11.446 (2004).) In more philosophical terms, consider two professors’ estimate that world information is growing by 30 percent every year and that 92 percent of all new information is stored on magnetic media, primarily hard drives. (See Peter Lyman & Hal R. Varian, *How Much Information 2003?*, <http://www.sims.berkeley.edu/research/projects/how-much-info-2003>). That’s a lot of potential evidence to think about.

Adding to both the volume and value of digital evi-

dence, a computer contains much more information than meets the eye. We often think of digital evidence in terms of the contents of a document, e-mail message, or Web page that we see on a computer monitor when we point and click on a particular file; yet a computer hard drive contains many types of *latent* data that are less accessible and less apparent, but no less important to a cybercrime case.

Metadata. The metadata about each computer file are probably the most important latent information that can be recovered by a computer forensic expert. This “data about the data” can help determine who wrote a smoking-gun memo; who received, opened, edited, copied, moved, or printed the memo; and when these actions occurred. On a laptop or desktop computer running Microsoft Windows, metadata come in two flavors. “File system metadata” show when each file was “created” within a particular hard-drive folder or location, either after the contents were typed in and saved by a user, or after the user copied a file to the hard drive from another source, such as the Internet or a floppy disk. File system metadata also show when the contents of a file were last “modified” and when the file was last “accessed” or opened. “Embedded metadata,” on the other hand, record information *within* a file. In a Microsoft Word document, the embedded data may show the author, number of revisions, names of people who made changes or last saved the document, and the date the document was last printed.

Deleted data. Another important source of latent evidence are the data that a user deleted, but which still reside on the hard drive. To understand how “deleted” data can remain on a hard drive, it is helpful to understand how data are written to a hard drive in the first place.

A hard drive contains tracks of data that run in concentric circles around one or more platters or disks, much like the grooves that encircle a vinyl record album. A computer fills these tracks with “clusters” of data and uses a file allocation table (FAT) or master file table (MFT) to index the locations of clusters for each named file on the hard drive. When a user tries to get rid of a file by hitting the delete key, the file is assigned to the “recycle bin.” When the recycle bin is emptied, the name of the file is simply removed from the FAT or MFT, but the underlying file contents remain intact. The only difference is that the deleted contents now sit in “free” or “unallocated” space that can be overwritten by new data. Some deleted files may be recovered in their entirety because no new data have overwritten them. Other deleted files may exist in fragments because a new file did not completely fill out its assigned clusters. The extra space at the end of the newly

Paul H. Luehr is vice president and deputy general counsel of Stroz Friedberg, LLC, a national computer forensics and technical consulting firm. Previously, he served as an assistant U.S. attorney and the computer crimes coordinator in Minneapolis, Minnesota, and as assistant director of marketing practices at the Federal Trade Commission in Washington, D.C.

written file is called “slack space,” and it allows previously deleted data to peek out from under the new file, much like the segment of an old TV show that remains on a VHS tape after you record a shorter show over it.

Temporary data. Latent data also can exist in “swap space” and “temporary files” on a hard drive. Swap space enables a user to move easily through pages of data or toggle quickly between several different applications that are running at the same time. Temporary files are more specific to individual applications like Microsoft Word, PowerPoint, or Excel and may contain information that a user once viewed but never saved. Many temporary files can be identified by the .TMP extension, but some lawyers think they should be marked .PTL (for “Praise the Lord!”) because temporary files are often used to recover important briefs that were . . . uhm . . . errr “lost.”

Together, swap space and temporary files can reveal screen shots of Web sites visited by the user, screen names and passwords typed in by the user, copies of spreadsheets or documents drafted by the user, and images or e-mail messages viewed but never saved to the hard drive by the user. Data in swap space and temporary files, by definition, might exist for only a short period of time; therefore, they must be captured and preserved quickly. In some situations, however, this latent data can remain on a hard drive for months or even years, especially if a computer is seldom used or used only for simple tasks like drafting short documents.

Other hidden data. There are many more types of valuable evidence that a computer forensic expert can recover. Below are explanations of some common varieties that appear in computers running Microsoft Windows operating systems.

REGISTRY KEYS: These entries list the user accounts on a computer (e.g., “guest,” “administrator,” “johndoe”), as well as the programs accessible or assigned to each user. The registry lists the sequence of programs launched whenever a person “boots” up the computer, as well as all of the software applications and hardware devices (for example, printers, scanners, thumb drives) ever installed on the computer. The registry also contains Web addresses typed in by a user.

INTERNET DATA: Temporary Internet files or “cache” files contain the source code and images from Web sites recently visited by users, and “cookie” or “history” files reveal the addresses and dates that those sites were visited. Some history files also show search terms and keywords entered into sites like MapQuest.com or Google.com. “Bookmark” or “Favorite” folders show the addresses of Web sites selected for easy access by the user. An Internet service provider (ISP), such as AOL, generates additional proprietary files on the hard drive, including e-mail folders, contact lists, buddy lists, or digital filing cabinets.

“RECENT” FILES: These files appear in the registry or separate directories and contain listings of or links to files that a user recently accessed. These files may reveal what

documents were recently opened and what general activity recently occurred on a computer (*See, e.g.*, “Documents” under the Microsoft Windows “Start” menu.) “Recent” files also may reveal what data were recently accessed using specific software programs, such as the videos most recently viewed using Microsoft’s Windows Media Player.

LOCAL “SEARCH” HISTORY: This file reveals what a user searched for on his or her own hard drive and may indicate what a suspect was trying to find, hide, or delete.

AUTOCOMPLETE MEMORY: Some users turn this function on to fill out forms and avoid retyping frequently used words. Therefore, autocomplete data can reveal a user’s name, address, and other personal information.

SHORTCUTS: These icons appear on a computer’s “desktop” or main screen every time the computer boots up. Therefore, the existence of a “shortcut” may indicate that a user intended to access a particular file or program often.

Embedded Metadata

Created:	Monday,	October 10, 2005	3:59:00 PM
Modified:	Monday,	October 10, 2005	4:40:46 PM
Accessed:	Tuesday,	October 11, 2005	12:51:26 PM
Printed:	Tuesday,	October 11, 2005	12:51:00 PM
Last saved by:	pluehr		
Revisions number:	6		
Total editing time:	53 Minutes		

PRINTER SPOOL HISTORY: This is a log of the temporary files created when printing a document from a computer hard drive or removable media like a floppy disk.

SERVER-SIDE DATA: Although not exactly “hidden,” lawyers should know that a wealth of data may be stored on company servers, separate from a user’s workstation or laptop. Server-side data may include documents posted to a user’s own “home directory” on the network, as well as collaborative work posted to a “shared” folder or directory. Server-side data also may include calendars, contact lists, and voluminous e-mail messages that have been sent, received, deleted, and/or archived. Older server-side data are often saved to backup tapes, and an experienced forensic examiner can combine this server data with individual workstation data to obtain a comprehensive view of a user’s computer activity. (*See* Beryl A. Howell & Eric Friedberg, *21st Century Forensics: Searching for the “Smoking Gun” in Computer Hard Drives*, PROSECUTOR 18 (Nov./Dec. 2003); Keith R. Gittings & Sans Institute, *Where Data Hides and Resides*, GSEC PRACTICAL REPORTS (April 30, 2004) at http://www.giac.org/practical/GSEC/Keith_Gittings_GSEC.pdf).

Forensic preservation of computer evidence

In cybercrime cases and other types of cases involving digital evidence, a computer forensic examiner can potentially collect all of the data described above and can do so with a high degree of assurance that the data will be captured in an unaltered state and preserved for evidentiary purposes. Without this assurance, much of the data described above might be lost. For example, if a layperson or in-house information technology (IT) staffer simply turns on an evidence-laden computer, it could change the computer’s registry values, reset the dates on several documents, wipe out temporary files, or overwrite previously “deleted” data. Even worse, if an unwitting person begins to open and copy different files on that machine, crucial metadata like the “created” dates and “last accessed” dates can change, and embedded metadata or file contents may be irretrievably altered.

The forensic examiner avoids these problems and captures both the visible and the latent data from a computer by making a bit-stream copy of the entire hard drive, also known as a “mirror image.” During and after the imaging process, the forensic examiner who follows best practices ensures the integrity of the collected data in several ways. First, the examiner uses special software or hardware to “write block” the original source drive so that no data can be written back to it. Data flow in a one-way path away from the source drive to the duplicate disk drive, thereby preventing any original data from being altered during the imaging process. In addition, a conscientious forensic examiner creates a second backup or working copy of the original hard drive and stores the first “sacred” copy in a fireproof safe. From that point on, the examiner typically keeps a meticulous chain-of-custody log on the first drive copy and records if and when it is removed from the safe, who removed the drive, and for what purpose.

Finally, the computer forensic examiner usually authenticates his or her data by running them through a mathematical program known as a “hashing” algorithm. The most popular is the MD5 program created by Professor Ronald L. Rivest at MIT. (*See* MD5 Homepage (unofficial) at <http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html>). The program creates an electronic “fingerprint” of a data set, and the computer forensic examiner uses it to create a string of letters and numbers that is unique to the volume of data pulled from the original hard drive. Later in an investigation, an examiner can verify that he or she is working with an authentic copy of the original hard drive by matching a new “hash” value against the original one, as seen below.

Acquisition Hash:
3E781F09522E12C2B467C050278A2832
Verify Hash:
3E781F09522E12C2B467C050278A2832

In addition to verifying the contents of a hard drive, MD5 and other “hashing” programs can be used to “fingerprint” individual files. Therefore, forensic examiners can use “hash” values to look for “smoking guns” such as an identifiable hacker code, specific child porn images, and documents known to contain trade secrets. Forensic experts also can use “hash” values to speed up their examinations by sorting out common software programs and system files from unique event logs and user-created files.

Theoretically, there is a one in “340 billion billion billion” chance of randomly generating two identical hash values; therefore, an MD5 match is considered even more accurate than a DNA match. (See Loren Mercer, *Computer Forensics: Characteristics and Preservation of Digital Evidence*, FBI LAW ENFORCEMENT BULL. 29 (March 2004), available at http://www.fbi.gov/publications/leb/2004/mar2004/march2004.htm#page_29). Last year some computer scientists successfully attacked the MD5 program and produced identical hash values from slightly different data sets; however, the attack took 80,000 computing hours to launch and involved artificial data sets created in the lab, not real data from laptops or computers in the field. Therefore, the MD5 algorithm will see continued use in computer forensics, but over time even more robust hashing programs likely will replace it. (See NAT’L SOFTWARE REFERENCE LIBRARY, *NLSR and Recent Cryptographic News*, (Aug. 19, 2004), <http://www.nslr.nist.gov/collision.html>).

Selecting and hiring a computer forensic expert

The benefits of an early consult. Because so much turns on the evidence inside the computer in a cybercrime case, it is important to choose an expert early and wisely. If you are a prosecutor, chatting with a forensic examiner early in a case can help you develop an effective investigative plan. For example, in a child pornography case, a forensic examiner first might propose tracing e-mail messages and ISP account information back to a suspect’s residence. Once a suspect’s hard drive has been seized pursuant to a warrant, a forensic examiner then might propose looking through an electronic “buddy list” for potential victims or looking in Internet history files for search terms like “Lolita” or “preteen sex” that indicate an intent to collect child pornography.

On defense counsel’s side, hiring a forensic examiner early may allow you to view the same computer evidence seized by the government, without having to wait for an indictment or the start of the formal discovery process. In cases involving alleged corporate fraud, a forensic examiner can help identify if and when financial information may have been altered. A forensic examiner also can help a company respond faster to a government subpoena for e-mail and electronic documents. At times, a forensic examiner can even help narrow the scope of a government sub-

poena by presenting a reasonable, alternative method of identifying, harvesting, and producing relevant data. Also, by preserving a snapshot of important company data *the first time* a company receives a subpoena, a forensic examiner can help reduce the time and expense of responding to the government’s inevitable second and third requests for documents. At the same time, a forensic examiner can assist corporate lawyers in many internal investigations, especially when computer forensic evidence may help counsel determine how to interview specific employees.

The risks of nonpreservation. When an attorney consults with a computer forensic examiner at the beginning of a case, it also minimizes the risk that key evidence will be destroyed or altered. Today, this is a risk that lawyers and corporate officers ignore at their peril, as Frank Quattrone learned. He was head of the Technology Group for the high-flying IPO (initial public offering) bank CSFB. After being notified that CSFB had received subpoenas from both the Security and Exchange Commission (SEC) and a federal grand jury, Quattrone authorized an employee to send out an e-mail in December 2000 that stated, “We strongly suggest that before you leave for the holidays, you should catch up on file cleaning.” Quattrone followed up with his own message saying, “[H]aving been a key witness in a securities litigation case in south texas i [sic] strongly advise you to follow these procedures.” Quattrone was indicted on obstruction of justice and witness tampering charges. He pled guilty and is currently serving 18 months in federal prison. (See *United States v. Frank Quattrone*, (S.D.N.Y. 2003); indictment available at <http://news.findlaw.com/hdocs/docs/csfb/usquattrone51203ind.pdf>).

The duty to preserve evidence may be triggered even before the government issues a subpoena or an indictment, especially under the Sarbanes-Oxley Act, which codifies two new document destruction crimes at 18 U.S.C. §§ 1512(c) and 1519. Together, these laws prohibit the destruction, concealment, falsification, or alteration of any record or document for the purpose of obstructing or influencing “any official proceeding” of a federal agency (18 U.S.C. § 1512(c)), or “in relation or contemplation of any such matter.” (18 U.S.C. § 1519) (emphasis added.)

In *United States v. Arthur Andersen*, 125 S. Ct. 2129 (2005), the U.S. Supreme Court recently clarified when a failure to preserve documents rises to the level of criminal obstruction. In that case, the Arthur Andersen accounting firm was convicted at trial of destroying paper and electronic documents during the Enron collapse. The firm was found guilty under the pre-Sarbanes Oxley statute, 18 U.S.C. § 1512(b), which prohibited “knowingly . . . corruptly persuading” others to “withhold” or “alter” documents for use in an “official proceeding.” The Supreme Court unanimously overturned the conviction

and held that the jury should have been instructed to find “a ‘nexus’ between the obstructive act and the proceeding.” (*Id.* at 2137.) The Court explained, “It is . . . one thing to say that a proceeding ‘need not be pending or about to be instituted at the time of the offense,’ and quite another to say a proceeding need not even be foreseen.” (*Id.*) Under this reasoning attorneys need not be pre-scient, but if they know of a government investigation or anticipate a lawsuit, they should issue a litigation hold and preserve relevant evidence with the help of a qualified forensic examiner.

Too many attorneys and corporate officers initially call upon their trusted IT personnel to “poke around” in a computer and see what evidence can be viewed or recovered. Yet, as described above, each time a file is highlighted, opened, copied, moved, or otherwise “poked” without the appropriate forensic tools, the system dates on important files can change and the likelihood of tainting the evidence increases. By consulting with a computer forensic expert early in a case, the attorney can preserve the quantity and quality of valuable evidence, avoid spoliation charges, and minimize the risk of facing civil or criminal sanctions.

Looking for experience.

Even after deciding that a computer forensic expert is needed in a case, the process of choosing one can be confusing because the field is littered with certifications and titles. Although many certificates are issued based on formal training and testing, others can be purchased if an examiner simply completes the right paperwork. There is no certificate that offers a silver bullet to the attorney seeking a computer forensics expert; however, the following programs and certifications are generally respected in the field.

Inside the government, many examiners have “A+” and “Network+” certifications from the Computing Technology Industry Association (CompTIA) (*see* <http://www.computia.org>), and within the FBI, examiners also must qualify as computer analysis and response team (CART) members. Some private companies offer certifications related to their proprietary forensic tools, but only those tools. For example, Guidance Software sells a popular forensic tool called EnCase and qualifies a person as an EnCase-certified examiner (EnCE) if he or she passes a CompTIA written test and a “hands-on” exam using the EnCase software. (*See* <http://www.guidancesoftware.com/training/EnCE/>). AccessData offers its own program suite called Forensic Toolkit (FTK) and issues certificates to examiners who

attend “boot camp” or more advanced FTK training. (*See* <http://www.accessdata.com/training>). More broadly, many network administrators and computer security officers are certified information systems security professionals (CISSP) under the standards of the International Information Systems Security Certification Consortium (*see* <http://www.isc2.org>) or certified information security managers (CISM) under the standards issued by the Information Systems Audit and Control Association (ISACA) (*see* <http://www.isaca.org>). Finally, many examiners belong to organizations like Infragard, the High Technology Crime Investigation Association (HTCIA), and ASIS. These groups provide industry news and training to examiners, but mere membership in these organizations does not qualify a person as a computer forensics expert.

In short, there is no substitute for experience, and lawyers should always inquire about the depth and breadth

of a potential expert’s background. Lawyers should avoid the one-trick examiner who has only imaged and analyzed one type of computer using a single forensic tool. Rather, an attorney should look for a forensic examiner who has analyzed a number of different machines or systems, in a number of different settings, in a wide variety of legal cases. Attorneys should ask: Where and when did you start working as a computer forensic examiner? What

types of cases have you been involved in? Do you work out of a lab or out of your basement? How do you store your digital evidence and maintain a chain of custody? Do you make a duplicate working copy of your evidence? Have you ever written an expert report or testified at trial? Have you ever collected evidence from a network server or backup tapes? Have you worked on (Apple) Mac, Linux, or Unix machines, in addition to Microsoft Windows machines? Have you ever harvested e-mail and attachments from Lotus Notes, Groupwise, or other e-mail clients beside Microsoft’s Outlook and Exchange? What forensic tools do you typically use?

Experienced examiners can be found within both the government and the private sector. Government computer forensic agents often have considerable experience because they must image or review scores of hard drives every year and must work on issues ranging from possession of child pornography to computer intrusions and counterintelligence surveillance. In the wake of 9/11 and fears about cyberterrorism, the government has moved to expand its computer forensic capabilities, and the FBI is in the process of constructing 14 regional computer forensic labs

The duty to preserve evidence may be triggered before a subpoena.

(RCFLs) around the country. (See <http://www.rcfl.gov>). Seven such labs are already operational in San Diego, Silicon Valley, Dallas, Houston, Kansas City (Missouri), Chicago, and central New Jersey. Seven more labs will be added by the end of 2006 in Buffalo, Philadelphia, Dayton, Louisville, Denver, Salt Lake City, and Portland (Oregon). In the private sector, the talents and experience of private examiners can match those of government agents, precisely because some of those examiners got their start in government. In addition, many private forensic examiners have honed their skills, not just on criminal cases, but also on complex civil litigation matters.

Presenting the testimony of computer forensic experts

As trial approaches, an attorney needs to think about qualifying a computer forensic examiner as an expert and having his or her testimony admitted at trial. The well-known Federal Rules of Evidence (FRE) 702-03, 803, 901, and 1001-03 govern this process.

Qualifying the forensic expert. Under FRE 702, if there is “scientific, technical or other specialized knowledge” that will assist the judge or jury, “a witness qualified as an expert by knowledge, skill, experience, training or education may testify thereto. . . .”

Courts do not expect a computer forensic expert to rip apart the code of a forensic software tool any more than they would expect a radiologist to be able to disassemble and rebuild an X-ray machine. (See *People v. Lugashi*, 205 Cal. App. 3d 632, 640 (1988).) The focus is on whether the expert can understand and effectively use the array of specialized hardware and software tools within the forensic trade. Thus, one federal court noted that computer forensic experts did not need computer science degrees or “the expertise . . . to develop sophisticated software programs. The question is whether they have the skill to find out what’s on a hard drive” (*U.S. v. Scott-Emuakpor*, 2000 U.S. Dist. LEXIS 3118, 33 (W.D. Mich., Jan. 25, 2000).)

In addition to considering an expert’s background, the court will inquire into the expert’s techniques to determine if they are reliable under FRE 703. *Frye v. United States*, 293 F. 1013, 1014 (D.C. Cir. 1923) established the traditional methodology test still followed by some state courts and asked whether an expert’s technique has been “sufficiently established to have gained general acceptance in the particular field in which it belongs.” *Daubert v.*

Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 593-95 (1993), set forth the more detailed and modern standard of review in federal court regarding the soundness of an expert’s methods and asked: 1) whether the expert’s theory or technique has been tested; 2) whether it has been subjected to peer review and publication; 3) whether there is a high known or potential error rate, and 4) whether the theory or technique is generally accepted within a specialized field. Although *Daubert* itself applied to medicine and traditional science, the same test was extended by *Kumho Tire Co., Ltd. v. Carmichael*, 119 S. Ct. 1167 (1999) to engineers and other nonscientific experts. Thus, criminal attorneys and their forensic examiners should be prepared for a pretrial *Daubert/Frye* hearing. They can take some comfort in knowing that some forensic tools have already been tested by the Computer Forensic Tool Testing Program of the National Institute of Standards and Technology (see <http://www.cftt.nist.gov/>) and that some

forensic tool manufacturers publish their own *Daubert/Frye* guides. (See, e.g., Guidance Software, ENCASE LEGAL J., (May 2005) at <http://www.guidancesoftware.com/products/legalresources.asp>).

Attorneys also can rely on cases that have upheld the validity of specific forensic tools in the face of a *Daubert/Frye* challenge. For example, in *Williford v. State*,

127 S.W.3d, 309, 312-13 (Tex. App., 2004), a state court of appeals reviewed the admission of computer data in a child pornography case. The data had been recovered using the EnCase tool, and the court evaluated the tool in light of seven evidentiary factors, including those outlined by *Daubert*. The court concluded that the testifying forensic examiner had addressed all seven factors and had “established EnCase’s reliability.” (See also *State of Washington v. Leavell*, No. 00-1-0026-8 (Okanogan County, Wash. Superior Ct., Oct. 20, 2000); *People v. Rodriguez*, No. SCR-28424 (Sonoma County, Cal. Superior Ct., Jan. 9-11, 2001), *Frye* hearing transcripts at <http://www.guidancesoftware.com/corporate/downloads/whitepapers/peoplevrodriquez.pdf>; *accord United States v. Crim. Triumph Capital Group*, 211 F.R.D. 31, 48-49 (D. Conn. 2002) (recognizing the validity of the SafeBack tool used to restore a seized hard drive).)

Authenticating computer evidence. If a computer forensic expert “write blocks” his or her original hard drive, creates bit-stream copies of the drive, “hashes” drive images, and maintains a solid chain of custody as described above, the expert’s methodology should pass

The field is
littered with
certifications
and licenses.

muster under *Daubert*. Moreover, the expert's evidence should be deemed "authentic" under FRE 901(9) because the evidence was created using a "process or system [that] produces an accurate result." It does not matter if a computer forensic expert only possesses a copy of the original hard drive. Even if the data are offered to "prove the content of a writing" under the Best Evidence Rule at FRE 1002, a forensic "duplicate" should be admissible "to the same extent as an original" because it was produced by "techniques which accurately reproduces the original." (See FRE 1001(1)(4); FRE 1003; *Broderick v. State*, 35 S.W.3d 67, 69 (Tex. App. 2000).)

Overcoming hearsay objections. At trial, as the computer forensic expert moves from background and methods into the substance of his or her testimony, a lawyer can expect hearsay objections from opposing counsel. Most of these objections can be overcome with a little forethought, research, and planning. If the forensic examiner is merely testifying about time stamps or other system data on the defendant's hard drive, the hearsay rule should not apply because such computer-generated files are not out-of-court "statements" by a person. On the other hand, if the examiner finds compilations of data input by one or more users (even simple telephone lists), many courts will rule that these compilations *are* hearsay statements, but may admit them as reliable business records under Fed. R. Evid. 803(6) as long as the proper foundation is laid by a company custodian, not the expert. (Compare *United States v. Vela*, 673 F.2d 86, 89-91 (5th Cir. 1982) and *Harveston v. State*, 798 So. 2d 638, 641 (Miss. Ct. App. 2001).) Offering old e-mails into evidence is likely to provoke the most vocal hearsay objections because they are pure out-of-court communications. Yet, even some of these objections can be overcome if the messages were written by the party-opponent or forwarded by that person with a note of approval. In those instances, the messages should be admissible as nonhearsay admissions or adopted admissions under Fed. R. Evid. 801(d)(2). (See *Sea-Land Serv., Inc. v. Lozen Int'l*, 285 F.3d 808, 821 (9th Cir. 2002).)

Common expert battles in cybercrime cases

If a full cybercrime trial ensues, computer forensic experts are apt to debate the following fundamental questions: 1) Who committed the criminal acts that can be traced to a specific computer? 2) When did these acts occur? 3) What was the defendant thinking at the time, and did he or she act with criminal intent? 4) How much injury did the cybercrime cause?

Attribution. Proving that a crime is attributable to one particular person is always a challenge. In cybercrime cases, this challenge is magnified because the Internet crosses geographic and jurisdictional boundaries and

shrouds perpetrators in relative anonymity. Also, many computer security features can be circumvented by a technically savvy hacker; therefore, it's little wonder that computer forensic experts are usually locked in a real "whodunit."

Many accused criminals raise the SODDI defense—short for "Some Other Dude Did It"—but in cybercrime cases the defense takes on multiple meanings. On the one hand, the defendant may use the SODDI defense to argue that no criminal activity even occurred on his or her computer. On the other hand, the defendant may concede that his or her computer was the source of criminal activity, but will use the SODDI defense to argue that an unknown hacker was responsible for the crime. Some scholars refer to this second argument as a "Trojan horse defense." (See Susan W. Brenner, Brian D. Carrier, Jeff Henninger, *The Trojan Horse Defense in Cybercrime Cases*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (2004).)

Although a government forensic expert could easily defeat the first version of the SODDI defense by uncovering child pornography or incriminating e-mail on a defendant's computer, overcoming a Trojan horse defense is more difficult, as seen in the trial of Aaron Caffrey. He was a 19-year-old British citizen, charged with launching a denial-of-service attack on the computers of the port of Houston, Texas, less than two weeks after the 9/11 attacks. At his trial in the United Kingdom in 2003, Caffrey testified as his own expert and stated that he was part of a hacker group called Allied Haxor Elite. He claimed that hacker rivals must have remotely controlled his computer using a Trojan horse program, deposited incriminating evidence there, and then erased any sign of their actions. The government could find no trace of the purported Trojan horse program, only evidence of the Houston attack. Still, the prosecution could not overcome the jury's doubt, and Caffrey was acquitted. (*Id.* at 2-4).

Part of the difficulty in defeating a Trojan horse defense is the technical nature of the defense and cybercrime itself. The language of computers—with its binary 1s and 0s, FATs and floppies, Megs and Gigs—does not exactly lend itself to soaring prose. Thus, an unwary trial attorney could easily lose the jury to sheer boredom. According to one reporter, this is exactly what happened to the prosecution in the *Caffrey* case. He writes,

I spent most of the first week of the trial in the public gallery and found it didn't take long before the jury's eyes glazed over because the technical arguments sounded like a Russian version of *Moby Dick* that had been translated into English using Babelfish. By the third day, one of the jury members had to be discharged because of a severe migraine, which was indubitably brought on by the jargon.

(Munir Kotadia, *The Case of the Trojan Wookie*, ZDNET (UK) (Oct. 27, 2003), at http://news.zdnet.com/2100-9595_22-5096128.html).

To overcome the tedium of computer tech-talk, attorneys need to encourage their experts to KISS (“Keep It Simple Stupid”). Overall, attorneys and experts need to think more strategically about how to present technical evidence. (See sidebar at left.)

Procedurally, prosecutors may try to counter a Trojan horse defense by asking the court to apply the advanced notice provisions related to traditional alibis. (See Fed. R. Crim. Proc. 12.1.) A Trojan horse defense parallels a traditional alibi defense because it has the element of surprise and, if true, provides a complete defense to any criminal charges. Like the assertion of a traditional alibi, a Trojan horse defense also may delay trial if the prosecution needs more time to investigate the defendant’s claim. Thus, a court may find it prudent to apply the procedural rules related to traditional alibis when a Trojan horse defense is raised. (See Brenner et al., *supra*, at 19-21.)

In terms of evidence, a Trojan horse defense can be countered with antivirus and antispyware scans and a review of registry keys that would indicate whether files have been added to or altered on the defendant’s computer. A forensic examiner also can look at start-up configuration files to see if a malicious program is set to launch every time a computer is turned on. Looking at Internet logs and history files might indicate whether the defendant’s computer has made an unusual connection to an outside entity or hacker. In addition, the defendant’s prior or real-world activities may help corroborate any forensic analysis. For example, in the *Ray* case, the government offered FRE 404(b) evidence that the defendant had made extortion threats before.

Apart from showing whether “some other dude did it,” computer forensics may reveal whether “lots of other dudes did it.” In short, when a case involves more than one potential defendant, computer forensics can provide valuable evidence about the existence and scope of an alleged conspiracy and the roles played by different individuals. In a “carding” case like the one brought against Shadowcrew.com, alleging that its 4,000 members trafficked in at least 1.7 million stolen credit cards, computer forensics might help confirm the nicknames or “nics” of certain individuals and their roles in acquiring, testing, trading, and using stolen credit cards. (See *First Operation Site Down Indictment* (press release), U.S. Dep’t. of

Justice (Oct. 28, 2004), <http://www.cybercrime.gov/mantovaniIndict.htm>). Similarly, in cases against movie and software pirates, computer forensics can help determine how many titles have been uploaded and downloaded and who served as an administrator, “cracker,” “scripter,” “encoder,” or “broker” for an underground “warez” site. Even violent crime cases can have a cyber flavor, and computer forensics might show whether a violent offender acted alone or in concert with others. Thus, it is not surprising that after the tragic Red Lake school shootings, the FBI began reviewing records of students’ online communications and reportedly seized 30 to 40 computers for examination. (See Dana Hedgpeth and Dan Eggen, *Others Aware of Red Lake Plans, Officials Say*, WASH. POST (Apr. 2, 2005), at <http://www.washingtonpost.com/wp-dyn/articles/A19704-2005Apr1.html>).

Timing. Criminal liability may rise and fall, not just on whether specific acts occurred, but when they took place. Thus, Frank Quattrone was indicted, primarily because he encouraged CFSB employees to clean up their IPO files after he was made aware of SEC and U.S. Justice Department investigations. Similarly, Martha Stewart was indicted, in part, because her

trading activity closely coincided with an insider’s tip.

Computer forensic examiners can present a wide array of evidence that bears on the timing of key events in a case. Examiners often estimate when a computer was purchased or given to a new user. They can help determine whether a document has been forged or backdated based on surrounding metadata or system files. “Last accessed” dates uncovered by an examiner also can reveal if certain programs, like a CD burner, were run on an employee’s last day of work. If a CD burner was activated, a forensic expert can look to see if numerous sensitive files were rapidly accessed and copied during that same time period.

While some computer dates and time stamps will be conclusive, others may be open to interpretation by competing experts. Created, modified, and accessed dates may be viewed differently depending on whether a file remained in one place or whether it was copied and saved to several locations. In addition, log files may vary by time zone, and metadata are generally only as accurate as the underlying computer clock time.

Intent. Even when real-world events line up with the computer data to incriminate just one person—the defendant—computer forensic experts are asked to examine whether that person acted with the requisite level of crimi-

Many accused criminals raise the SODDI defense.

TEN TECHNOLOGY TIPS FOR THE COURTROOM

1. Get organized.	Write a trial script with technical cues. Practice using new equipment or software. Disable your screen saver for trial.
2. Keep it simple.	Use laymen's terms, simple graphics, and time lines to explain complex data.
3. Get to the point.	Move quickly to your expert's findings. Don't get bogged down in technical procedures, especially if they're not challenged.
4. Tone it down.	Mark topic changes with simple slide transitions (e.g., "Cover Down"). Avoid schmaltzy sound effects and flashy text.
5. Make it readable.	Use large, simple fonts in your slides. Minimize glare with light text on a solid dark background. Enlarge or highlight key phrases.
6. Keep it "real."	Demystify "virtual" evidence by showing the physical location and computer equipment from which data were recovered.
7. Don't get ahead of yourself.	Publish evidence to the jury only after it has been admitted. Until then, make sure the jury's monitors are blank.
8. Know your judge.	Some judges encourage digital presentations. Others still like exhibit binders. Inquire about your judge's likes and dislikes.
9. Know your courtroom.	Test outlets and equipment before trial. Scale back your technology if the courtroom looks like the original set from <i>Inherit the Wind</i> .
10. Prepare for the worst.	If the lights dim and your laptop dies, be ready with hard copies of your exhibits.

nal intent. This is especially true in child pornography cases where the definition of illegal images has been shifting, possession of such images must be "knowing," and the law provides an affirmative defense to people who possess less than three images and take reasonable steps to destroy them. (See 18 U.S.C. § 2252(a)(4)(B) and (c); 18 U.S.C. § 2252A(a)(4)(B) and (c); *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).)

Many defendants may claim they never meant to possess any child pornography and simply stumbled across it when surfing the Internet; however, computer forensics may show otherwise. In *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002), a state forensics examiner recovered approximately 27,000 images from the computer of Jeffrey Tucker, the defendant, and estimated that 90 to 95 percent of the viewable files contained child pornography. Many images were small "thumbnails" while others were larger versions of the same images. The files had not been saved to Tucker's "My Documents" directory or other user folders; instead, the images were located in a Web browser cache file, the Recycle Bin, and in unallocated space. Nevertheless, the Internet history files on Tucker's machine showed repeated visits to Web sites containing child pornography, and one saved e-mail to a Web site operator showed that Tucker had requested access to pictures of "naked young girls." (*Id.* at 1198.) The defendant claimed that his Web browser "saved the images against his will," *id.* at 1205, but both the trial court and appellate court rejected this argument. They noted that Tucker admitted he knew how his computer worked, and the courts relied on the government's computer forensic data to find that Tucker intentionally surfed to child porn sites, clicked on various thumbnails to enlarge them, and then affirmatively deleted his cache files, thereby exercising sufficient control over the images to "knowingly possess" child pornography within the meaning of federal law.

Harm. A computer forensic expert can play an important role, not just in determining a defendant's guilt or innocence, but also in determining the amount of harm caused by a cybercrime and the restitution, fine, and term of imprisonment that are proper under advisory sentencing guidelines.

In a federal case involving Internet auction fraud, a forensic examiner may be able to recover Web postings or spreadsheets that list the names, street addresses, and e-mail addresses of potential victims and the amount of money lost by each of them. This information can be combined with bank data, auction house information, and records from PayPal (the popular online payment service) in order to compile final loss figures and a comprehensive list of victims. Computer forensics also may show whether sentencing enhancements should apply, depending on whether computer records show that more than 10,

50, or 250 people were victimized or “sophisticated means” were used to carry out a fraudulent scheme. (See U.S.S.G. § 2B1.1(b)(1), (2) & (8).)

Forensic data also may be crucial to the calculation of damage caused by a virus or computer intrusion under the federal Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030. If given access to networks or servers of a victim company, a computer forensic examiner may be able to determine how a hacker or virus accessed the network, whether any threat remains, and how many users or systems have been affected. In many situations, the computer forensic expert’s own expenses can be added to the loss amount being considered by the court for sentencing purposes. (See U.S.S.G. § 2B1.1, comment, (n.3(A)(v)(III).) More fundamentally, computer forensic experts can help determine the threshold question regarding whether the government can file *felony* charges or whether a private victim can seek *civil damages* for offenses under the Computer Fraud and Abuse Act. (See Nick Ackerman, *CFAA’S \$5,000 Threshold*, NAT’L L.J. (Oct. 18, 2004) (discussing the civil requirements of the Act).) In either situation, the Act requires the complaining party prove that the alleged offense caused “loss . . . during any 1-year period . . . aggregating at least \$5,000 in value.” (18 U.S.C. § 1030(a)(B)(i)). This loss figure can include the cost of hiring a forensic examiner plus

his or her assessment of the damage caused to the victim’s computer or business. In the language of the statute, “loss” is defined as:

[A]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service. (18 U.S.C. 1030 (e)(11).)

Conclusion

Computer forensic examiners are not the only experts involved in cybercrime cases, but they are among the most valuable. Using trusted tools and methods, they can recover the visible data that normally appear on a computer monitor as well as the important latent data that lie buried in a hard drive. By consulting with an experienced forensic examiner at the beginning of a case, an attorney can secure an expert who can preserve and authenticate important evidence, provide focus to an investigation, and give crucial insight into the ultimate questions about who committed an offense, when it occurred, the intent of the accused, and the extent of the injury caused by a cybercrime. ■