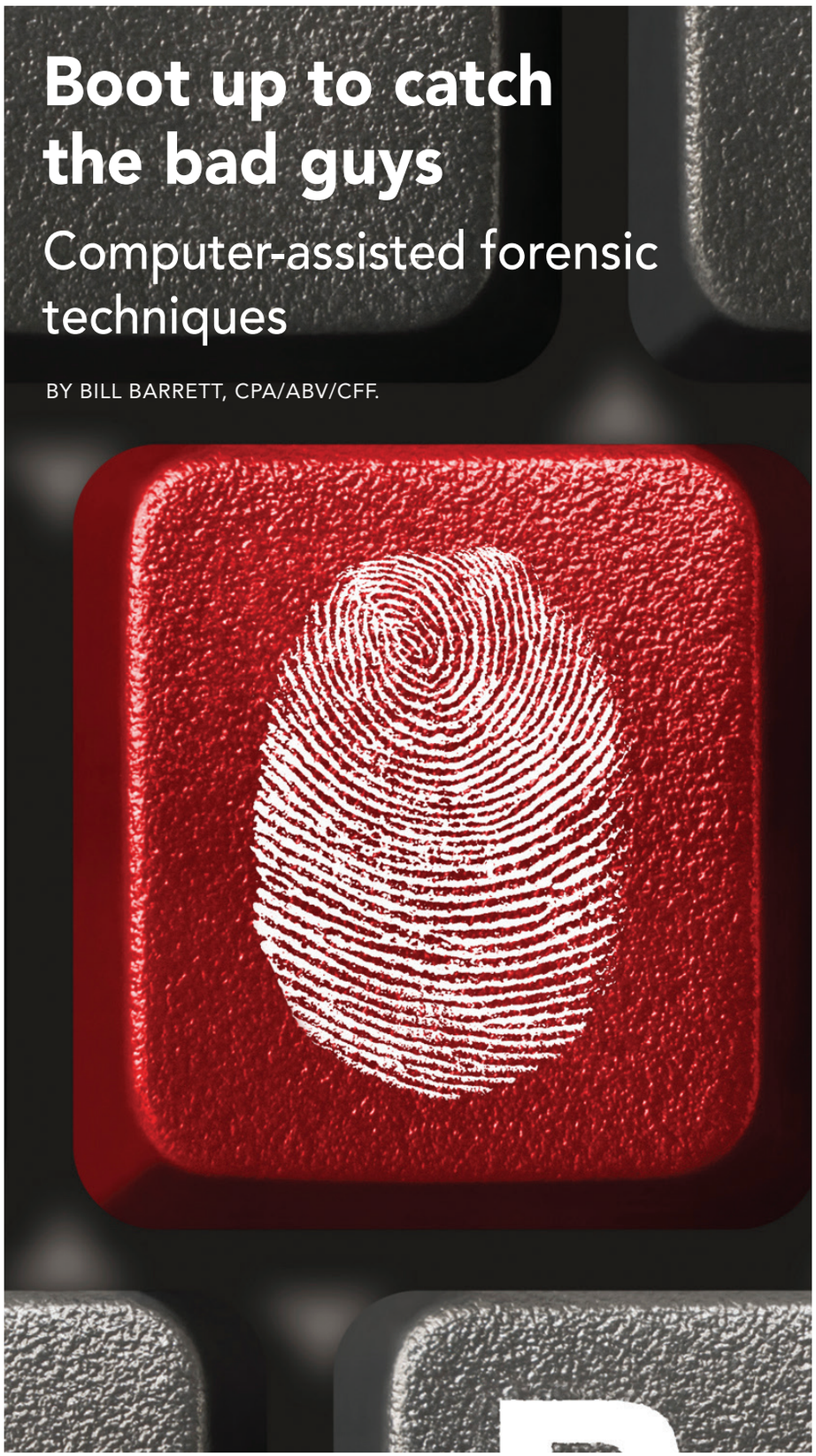
Boot up to catch the bad guys

Computer-assisted forensic techniques

BY BILL BARRETT, CPA/ABV/CFF.



Within the last 10 years, the world of electronic or digital evidence has evolved to become a vital part of practically every case a forensic accountant handles. Most cases require an inquiry into all forms of communications and records of every nature — especially those that are in digital form or were created electronically.

Businesses typically generate hundreds or thousands of documents related to various areas of operations: sales invoices, purchase orders, checks, etc. So there could be thousands of documents related to an area being investigated for fraud.

Computers can be used to perform investigative procedures on accounts payable and payroll fraud, such as printing out all unauthorized check numbers or checks over a specified amount, printing out a list of all employees not electing insurance or other employee benefits (as this might signal a fictitious employee scheme) or identifying vendors who always submit the latest bid or obtain a disproportionate share of contracts.

An accountant sniffing out accounts payable fraud might examine payments to vendors for certain attributes. They may look at vendor names on checks written to an approved vendor list and search for checks with different addresses for the same vendor names.

Other examples of investigative procedures that can be performed using computers include:

- Recomputing items on documents for mathematical accuracy.
- Searching for fictitious names or addresses by comparing data on documents to known fictitious names or addresses, for multiple names to the same address or for multiple addresses for the same name.
- Searching for payments made or inventory shipped to a vendor or customer with the same address as an employee.
- Searching for duplicate vendor payments. (The suspect intercepts and retains the duplicate payment.)
- Searching for unusual patterns on purchase orders or contracts, such as unusually large numbers or amounts.
- Searching for unusual accounting entries, for example, debit entries to accounts that normally receive credit entries (such as accounts payable or long-term debt) or credit entries to accounts that normally receive debit entries (such as loans receivable or inventory).
- Analyzing entries to suspense, clearing and inter-unit accounts.

The company's general ledger software package generally includes transaction reports that can be used to identify all transactions affecting an account during a specified period. These reports can be scanned to help identify unusual items.

Also, much of the publicly available information exists in databases that can be accessed by computer, which can make the data-gathering process more efficient.

What distinguishes computer-based evidence from traditional paper documents in discovery? "Electronic" documents thought to be lost or destroyed can be recovered. Valuable information such as the time, date and author's name may be embedded in the electronic version of a document. Comparisons of computer backups to existing documents can be used to show that a critical document was altered and when the event occurred. In the case of email, casual and candid correspondence may be frozen in time like insects in amber.

Computer-based evidence exists in many forms and locations within any computer system. The key to finding and using this information is in understanding the kinds of information that may exist and where to look within the system for each type of information.

DATA FILES

The primary function of most computer systems is to process and store information. Information processed and stored electronically can be divided into four basic categories: active data, file clones, backup data and residual data.

ACTIVE DATA

Active data is the information readily available and accessible to users. Active data includes word-processing documents, spreadsheets, databases, email messages, electronic ▶

More companies are installing software designed to monitor employees' use of company computers: programs used, files accessed, email sent and received and websites visited.

calendars and contact managers. A list of active data files can be easily viewed through file manager programs such as Windows Explorer or through "list file" commands in DOS.

FILE CLONES

Many operating systems build in automatic backup features that create, and periodically save, copies of the file being worked on by a user. These files are created and saved to help users recover data lost due to a computer malfunction (e.g., system crash or power loss); usually, the file clones are not stored in the same directory as the active file.

File clones are useful because they create a copy, or multiple copies, of a document that the users can't erase and may not be aware exists. On most networked systems, file clones are saved to the user's hard drive rather than to a centralized network file server. As a result, a document (or some version of it) that was purged from the file server may exist as a file clone on a user's hard drive.

Data contained in buffer memory (RAM) is usually limited to recently created and stored information. Cache files are temporary files of work in progress, and once these files are saved to a permanent file, the cache file buffer is "emptied" and ready for refilling of more temporary files.

BACKUP DATA

Backup data is information copied to removable media in order to provide users with access to data in the event of a system failure. Networks are normally backed up on a routine schedule, while individual users tend to back up (or not) on an informal basis. Network backups normally capture only the data saved on the centralized storage media (e.g., the file server) and do not capture all the data stored on individual users' hard drives.

Backups provide a historical snapshot of the data stored on a system on the particular day the backup was made. Reviewing a series of backup sessions can provide a wealth of information about how a particular matter progressed over several weeks or months.

Backup data is loosely organized, so finding relevant data requires restoring a tape, viewing its directories and searching within the directories for specific files. If the file an investigator seeks is not on the tape, the process must be repeated for each backup tape. Searching through a large number of backup tapes can be an expensive, time-consuming process.

RESIDUAL DATA

Residual data is information that appears to be gone but is still recoverable from the computer system. It includes "deleted" files still extant on a disk surface and data existing in other system hardware such as buffer memories of cell phones, digital tape recorders, dictation recorders, printers, copiers and fax machines. In most operating systems, the term "deleted" does not mean destroyed. Rather, when a file is deleted, the computer makes the space occupied by that file available for new data.

Reference to the "deleted" file is removed from directory listings and from the file allocation table (FAT); but the bits and bytes that make up the file remain on the hard drive until they are "overwritten" by new data or "wiped" through use of utility

software. If a file appears to have been deleted, it may still be recovered from the disk surface.

Until data is overwritten or wiped, it can be restored through use of "undelete" or "restore" commands contained in many systems' operating software. In the case of a partially overwritten file, pieces of the file or "file fragments" may also be recovered.

Residual data can be buried in a number of other places on disks and drives. Forensic specialists have tools that allow them to examine the entirety of a drive for residual data.

METADATA

Metadata, which means "data about the data," can provide key pieces of relevant evidence and information about a particular email, spreadsheet or other electronic document in a computer forensic investigation. Metadata includes information about a document, such as who created a file, when it was created and when it was last modified.

The availability of metadata depends on the properties of the file type. Depending on the type of application, a single document has the potential of having hundreds of metadata fields. Two primary types of file metadata can prove useful during a forensic investigation:

> SYSTEM METADATA: Data stored externally from the file and used to track file locations. System metadata is usually operating-system dependent and contains information about the file (e.g., file names, dates, path locations, sizes, etc.).

> APPLICATION METADATA: Information embedded within the file itself (i.e., tracked changes, document author, document version, macros, email "to," "from," "subject," etc.). Application metadata moves with the file when it is copied and varies depending on the type of file.

In the case of email, casual and candid correspondence may be frozen in time like insects in amber.

Like other forms of electronic evidence, metadata can be easily altered if proper preservation precautions are not taken. To avoid altering metadata during a forensic investigation, an expert should work off of an exact, bit-by-bit copy of the media at issue.

Metadata can provide a number of telltale clues. In most cases, computer users are not aware of the computer's metadata "log," which documents the date and time a file is created, accessed and modified. This trail of evidence can help tell the story about a computer user's conduct or the history of a particular file. Even after the data itself has been wiped, directory entries, pointers or other metadata related to the deleted data may remain on the computer.

Without this documentation, an electronic document is incomplete, and courts may refuse to admit a key piece of evidence if it finds the data unreliable. Once a forensic investigation is completed, an expert can testify about how metadata verifies the credibility of an electronic document. The expert also can help the judge or jury understand, interpret and evaluate the relationship between a piece of evidence and its associated metadata.

EMAIL

Email has several characteristics that make it an excellent source of evidence:

- Most people use email informally and candidly.
- Many people believe that email messages are impermanent.
- Email is more difficult to get rid of than most users believe. Permanently deleting messages on most email systems is usually a two-step process and many users only complete the first step.
- Email is easily copied and forwarded, thus making distribution of a message nearly impossible to control.
- Undeleted email may be captured on system backups.

Though business use of email is skyrocketing, guidelines for its use are lacking. A recent survey conducted by the Cohasset Associates revealed that 59 percent of organizations using email did not provide policies concerning either content control or retention periods for saving messages. ▶

Computer systems can provide a wealth of background material: audit trails, access lists, date and time stamps and more.

BACKGROUND INFORMATION

While data files and email are often targeted for evidence, they are not the only information that can be gleaned from a computer system. Computer systems can provide a wealth of background information, which may be valuable evidence or can be used to further develop the facts of a case.

AUDIT TRAILS AND COMPUTER LOGS

Audit trails and computer logs create an electronic trail regarding network usage. Typically, an audit trail contains information about who, when, where and how long a user was on the system. Information about who last modified a file and when the modification was made may also be available. An audit trail may also indicate when and by whom files were downloaded to a particular location, copied, printed or purged.

In addition to using a network's audit trail, an increasing number of companies are also installing software designed to monitor employees' use of company computers. This software records information such as programs used, files accessed, email sent and received and Internet sites visited.

ACCESS CONTROL LISTS

Access control lists limit users' rights to access, view and edit various files. Access rights often depend on the employee's particular job duties and position.

The access rights for a company's billing files may be limited to the accounting department and senior management. Additionally, different personnel may have different access rights. For example, the accounting department may have read and write access, whereas managers may have read-only access. If an investigation centers on a particular file or group of files, identifying who had access rights to the files and the type of access each person was allowed can establish data ownership/authenticity of files. Network security systems allow system administrators to set and maintain varying level of access to users on the system.

NON-PRINTING INFORMATION

The non-printing information carried by most data files is another excellent source of information. The most common example is the date and time stamp the operating system puts on every file. Some word-processing programs store revisions to documents, allowing a viewer to follow

the thought process of the author as a document is edited.

Some word-processing packages allow users to insert "hidden" or non-printing comments. Many schedule programs track who made changes to a calendar and when the changes were made. This information may never appear in hard copy form, but may be found in the electronic version.

CASE STUDY: THE APPS-5 CORPORATION

Computer-based evidence, in all its incarnations, can be scattered throughout a company's computer system. Consider the following case study as an example. See if you can identify where the five "smoking gun" documents were found.

To remain in business, APPs-5 Corporation needed to launch a new version of their software. The announcement of a June 2012 ship date for the new release gave a welcome boost to shareholders. Stock prices soared and optimism was high. APPs-5 principals and directors did well. The June 2012 date came and went, and APPs-5's software was still only in beta-stage.

Gayle Turner, principal and CEO of APPs-5, wrote a memo to Virginia Armstrong, APPs-5's public relations director, encouraging her to accelerate work on the May media campaign regarding the June ship date. Using the hidden text feature of his word-processor, Turner wrote this side note to his secretary: "delivering smoke and mirrors to the press is like carrying coals to Newcastle." He gave his secretary the memo on his thumb drive. The edited copy, generated by his secretary and emailed to Armstrong, did not contain the side note.

In May, Brian, in Research and Development, was sending his own messages to fellow staff members, making use of APPs-5's email system: "Even if we triple our staff (which you know we won't), we're never going to make it." This email message, sent at 11:00 p.m., was swept into the monthly backup created at midnight.

Gayle Turner automatically received electronic status reports generated using project manager software. Project reports included Gantt charts showing critical path, as well as resource, cost and project status. The project manager software and data was stored on R&D's file server and backed up weekly.

Virginia Armstrong then wrote a memo to Turner expressing her growing alarm that APPs-5's promises to the press were untrue. Before printing the memo, she had second thoughts and deleted it from her hard drive.

When stock prices plummeted, shareholders filed suit. Aggressive attorneys for the plaintiffs incorporated requests for computer-based files in their discovery strategy. Five computer-based documents provided the jury with a compelling picture of investment security fraud.

So, which five documents found during the e-discovery process helped the case?

- Hidden text was revealed when the memo to the secretary, found in the file on the thumb drive, was reviewed.
- Brian's email message was discovered on the monthly backup tape.
- Gayle Turner's hard drive contained saved status reports.
- Files from the project manager software were stored in weekly backup tapes.
- The deleted file on Virginia Armstrong's hard drive was recovered.

If figuring out these clues was interesting to you, you may want to consider a CPA specialty in forensic accounting and fraud. ■

BILL BARRETT, CPA/ABV/CFF, a sole practitioner in Richmond, has investigated fraud in business and professional entities, and has directed federal teams investigating multi-defendant money laundering, illegal income, tax evasion and white-collar fraud.

billbarrett@barrettpc.com

This article was developed from Bill Barrett's course, "Forensic Accounting in Non-Audit Engagements."