

CYBER-CRIME FIGHTER

Kelly J. Todd, CPA, *Summerford Accountancy, PC*

Using Digital Evidence to Nail Dishonest Employees



The business world's inescapable dependency on digital technology has given rise to a groundswell of such high-tech frauds as cyber-extortion, theft of company trade secrets, computer sabotage, identity theft, embezzlement and more.

Result: Desperate to deter, detect and support the prosecution of today's technology-savvy internal fraudsters, corporations are creating huge demand for the relatively new specialty of computer forensic investigation.

DAUNTING CHALLENGES

That's partly because simply locating, searching and managing digital evidence requires a special understanding of technology that the majority of computer users lack.

Moreover, because of the fragile nature of digital evidence, contamination (known in the legal field as "spoliation") must be avoided at all costs in order to preserve its admissibility in court. Only trained computer forensics experts can ensure that the chain of custody is preserved in fraud investigations that rely heavily on incriminating digital evidence.

KNOW WHAT TO LOOK FOR

Key to effective digital investigation: Determine what types of evidence are essential for proving a suspected fraud incident, and share this list with your forensic specialist before he or she begins the data collection process.

Helpful guidelines:

✓**Know the objective of the investigation.** Are you looking for data to prove your suspicions about a particular crime or a specific employee? Is your objective to stop the fraud...apprehend the suspect...or just to show your employees that you take fraud seriously and will investigate suspicious

activity even if nothing turns up?

✓**Specify relevant time periods when you suspect fraud to have occurred.**

✓**Provide the investigator with search terms,** including important keywords, names, phrases, locations, hobbies or assets that may be helpful to the forensic examiner.

✓**Provide known E-mail addresses, screen names, passwords or log-in names that may have been used by suspects.**

✓**Determine whether there are other computers or devices that may contain key evidence,** such as home PCs or removable storage devices owned by the suspect(s).

Starting point: To prepare for the examination, the forensic specialist must be informed about your organization's operating and backup systems...as well as all company-owned mobile devices that employees are using.

Caution: While cooperation from your IT manager(s) can be invaluable to outside forensics experts, most IT bosses are protective of their "digital domains." Be prepared to manage this potential obstacle at the outset of the investigation.

WHAT IS DIGITAL EVIDENCE?

The good news is that while gathering, preserving and analyzing digital evidence in fraud cases requires unique skills, the mere existence of such evidence has in many cases made catching internal fraudsters easier.

Key reason: Any information stored and/or used with computer technology is considered digital evidence. Such evidence can reside on a multitude of storage devices, starting with a suspect's computer hard drive and potentially including...

•Compact discs or diskettes.

Continued on page 6

- Backup tapes.
- Personal digital assistants, such as PalmPilot or iPAQ.
- “Thumb” drives or other removable USB storage drives.
- Internet-ready cell phones.
- Digital watches.
- Digital cameras.
- Fax machines.

MOBILE EVIDENCE

While your in-house or outside investigator must examine all of these media when internal fraud is suspected, removable media—such as CDs, cell phones, USB storage devices, etc.—are often the ones storing the most incriminating evidence.

Reason: They contain data the fraudster either does not want to keep on a company computer or has deleted from the hard drive.

COMPUTER FORENSICS: THE COVERT OPERATION

When gathering digital evidence to ferret out a dishonest employee, your computer forensic specialist will likely conduct the examination covertly to avoid tipping off suspects. In the process, the investigator will search for different kinds of data in numerous storage locations.

Examples:

✓**Active data.** This is information readily available and accessible by the organization’s users. It can easily be viewed through file manager programs, and includes spreadsheets, databases, word processing files, business application files, E-mail, electronic calendars and address books.

✓**Deleted files.** When a file or E-mail message is deleted with a computer operating system, the data itself is not removed. Rather, the process of deleting simply indicates to the computer operating system that the physical space belonging to the deleted file is available for new data to be stored.

Result: The data that makes up the file remains on the hard drive until it is overwritten by new data or “wiped” with special software.

Important: Don’t overlook or dismiss partially recoverable files. Partial files often reveal motive or intent, as well as passwords, addresses, assets or other information that may shed light on the investigation.

✓**Hidden files.** Data that is relevant to internal fraud cases is often hidden, encrypted or password-protected.

Examples: Incriminating data can be concealed by labeling files with a common name that makes them appear to be part of the operating system, such as files containing the file extension “.com” or “.sys.” Trained specialists will examine an element of the file known as the file header which contains the true identity of the file.

✓**Automatically stored data.** Many software manufacturers build in automatic backup features that create and periodically save copies of files being worked on.

Typically, the file copies are not stored in the same directory as the active file. Additionally, on most networked systems, copies are saved to the user’s hard drive rather than to the network file server.

Result: A document (or a version of it) that was deleted from the file server may exist as a copy on the user’s hard drive. In addition, if an employee deletes a file from his or her hard drive, another version of it may still exist there, having been earlier backed up by the automatic backup function.

✓**E-mail.** As has been reported in previous issues of *White-Collar Crime Fighter*, most computer users treat E-mail more like a convenient way to conduct casual conversation and less like a form of business correspondence.

Trap: Not only does E-mail create a more permanent record than most users realize, the computer maintains records of when messages were sent and opened in multiple locations.

✓**Computer logs.** More and more employers are installing special software designed to monitor employees’ use of company computers and create digital logs that track network usage, screening for such key information as who, when, where and how long a user was on the system.

✓**Backup data.** Networks are normally backed up manually on a routine schedule set by the IT department.

Typically, however, network backups capture only the data saved on the centralized network file server.

Still, backup tapes can provide a useful historical snapshot of data stored on a system on the particular day the backup was made.

Result: Reviewing a series of backup tapes can turn up information about how a particular fraud progressed. ☞

White-Collar Crime Fighter source:

Kelly J. Todd, CPA, CVA, is a Senior Manager at Summerford Accountancy, PC, Birmingham, AL-based fraud and forensic accountants. Kelly’s experience as a forensic accountant and fraud examiner includes work for defense and plaintiff attorneys, audit committees, corporate boards and government inspector generals. She can be reached at kelly@summerfordcpa.com.