Bank Fraud & IT Security Report
Prepared by Southeast Consulting, Inc.
SCI
October 2006
Volume 4, Number 10

Digital Evidence in a Fraud Investigation

By Tommie W. Singleton, Ph.D., CPA, CISA, CITP, CMA, University of Alabama at Birmingham, and Kelly J. Todd, CPA/ABV, CVA, Summerford Accountancy

No one has to be reminded of the risks associated with occupational fraud and abuse in the banking industry. For decades, monies have been stolen by employees in a variety of techniques. Schemes range from simple theft of cash from teller stations, to sophisticated loan frauds by managers, and even massive financial statement frauds by executives, such as the Keating and Lincoln Savings and Loan scandal in the 1980s. But one thing has changed over the years, and that is technology.

Technology is both a boon and a bane. It is used by fraudsters to assist in perpetrating a fraud, and a tool to be used to detect or prevent frauds. But it is also practically omnipresent in personal everyday life. Who does not own a cell phone or does not use e-mail nearly every day?

In a fraud investigation, it is imperative that investigators not overlook the potential rich evidence that might be obtained from these digital sources. This article is intended to provide guidance by identifying proven sources of digital forensic evidence, as displayed in Exhibit 1.

Exhibit 1. Potential Sources of Digital Evidence in a Fraud Investigation

CATEGORY	SOURCE
Conventional	Suspect s: Computer Laptop Drives
Connected	Entity s Network Servers Internet Server/Host (backbone)
Off-Line Storage Devices	CDs DVDs Floppy Drive Flash/Jump/Thumb Drive Digital Watch
Peripherals	Printer Memory Removable Drives
Personal	Home Computer PDAs etc. iPods Digital Camera (Cards)
Communication	Cell Phone E-mail Voice Mail
Signatures	E-mailPrinter

Conventional Sources. By its nature, fraud is clandestine. Fraudsters usually take precautions to hide their activities, or cover up the fraud in some manner. But many frauds are embedded in the transactional data of the entity's computer systems. For example, loan frauds are typically on the books, but the fraudster will attempt to keep it hidden from public view. Therefore, when a fraud investigation is undertaken, investigators typically begin with what is referred to herein as conventional sources of digital evidence.

If the scheme is on the books, then evidence exists in the entity's own accounting information systems. Transactional data could be examined using data mining tools to produce forensic evidence of a fraud.

But conventional digital evidence would also include the computers and their drives that the suspect used at work. Clearly fraudsters may have some evidence in digital form on their computers related to a fraud being perpetrated. Sometimes fraudsters keep track of their frauds using spreadsheets, databases, and so forth.

However, potential evidence goes far beyond the visible, easily accessible digital files on the hard drives of the computers. Using computer forensics, an investigator can examine random access memory (RAM), and slack storage such as the free space on a hard drive that is used to temporarily store files being viewed or updated by the computer user. Even after the user closes the application, the image or data remains on the hard drive until needed by another application, whereupon it is overwritten), system data (e.g., when files were last

accessed or updated) and other means of computer use to store digital data or images.

Connected Sources. Next are technologies connected to the fraudster's computer. These sources would include technologies such as the entity's network server. It is possible that digital evidence has been erased from the suspect's own computer, but remains on the network server. Again, a cyber forensic specialist would know if such evidence existed and how to retrieve it. It is also possible that if the Internet were being used by sending attachments to an e-mail, then digital evidence may still exist on Internet servers/hosts that were used on the Internet backbone to transmit the files or images.

Offline Storage Sources. It is easy to remember to look for CDs, DVDs and floppy disks around the fraudster's desk and work area. It is also possible that such digital evidence exists on storage devices that are located at the fraudster's home. However, there are some newer technologies that should be considered in gathering digital evidence.

Thumb drives, also called flash drives or jump drives, now have rather large capacity, often exceeding 1 GB, and extremely small, approximating the size of a thumb. Thus a fraudster trying to offload digital data, files or images that contain evidence of the fraud could easily download them to a thumb drive, hang it on the neck chain usually provided with these small drives, underneath clothing, and have an excellent chance of successfully hiding the evidence. Meanwhile, the fraudster either deletes the files from his or her work computer, or never used it in the first place but recorded it directly to the thumb drive. These thumb drives can not only be easily hidden but can come in the form of an actual ink pen, cleverly disguising the data storage device.

Other tiny devices can be used to store digital files, data or images. For example, camera flash cards have large capacities for storing images. A fraud investigator should look for these devices that can be hidden underneath a postage stamp! Other traditional personal items that can be used to store digital files include digital watches.

Peripheral Sources. In addition to offline storage sources, there are other sources of potential digital evidence. Printers use memory to store digital data as it prints to free up computer resources to go on to other processes while the printer while printing. The computer has a print spool process that will store the printed image to cooperate with the printer in printing *in the background.* That image usually remains in the slack area of the computer's hard drive after being printed and *erased.* It also may remain in the printer's memory.

Moreover, there are external hard drives that can be easily removed, like a thumb drive. It is more difficult to hide, being both larger than a thumb drive and having the obvious appearance of a drive.

Personal Sources. Obviously, the fraudster may have used a personal computer at home in connection with a fraud. But digital evidence may be more than transactional data or fraud tracking data stored on that computer. Fraudsters have been caught due to the fact that the most significant forensic evidence was a document, such as action steps or a *to do* list, created by a word processor on the fraudster's home computer that detailed the fraud. Thus, fraud investigators should consider searching a suspect's home computer, looking for this type of evidence.

However, there are other personal sources of potential digital evidence. Fraudsters may own a personal digital assistant (PDA) such as a Palm Pilot or iPaq, digital camera, specifically, the flash cards, or iPod. The latter is known for its ability to store and play a large number of music files. However, because it is a mass storage device, it could contain files or images that contain digital evidence associated with a fraud; that is, the iPod is used just like a thumb drive to offload digital files or documents. Because they are associated with music, iPods can be overlooked as a source of digital evidence. Again, these types of devices may contain more than transactional data or direct evidence of the fraud, but might also contain communications or other casual and personal documents that refer to the fraud.

Communications Sources. This category contains sources that do not necessarily contain direct digital evidence associated with the fraud scheme and transactional data but rather contain information, or evidence, that the fraud is being perpetrated while incriminating the suspect. These sources include e-mail, voice mail and cell phones. People tend to let their guards down when communicating with these forms of communications. In fact, the attorney general of New York has made a number of successful prosecutions of fraudsters relating to securities and insurance frauds. Most of the cases were won based on forensic evidence gathered from e-mail! In the e-mails, fraudsters talked freely about the fraud, how it was being done and specific details. Since it is e-mail, that digital e-mail file is contained on several computers including the fraudster's, the entity's e-mail server, and an Internet host server.

Parties interested in conducting fraud investigations should not forget that voice mail is digitized. A fraudster may have messages that contain information that could be used as evidence. Cell phones contain saved messages, and the cell phone provider may have copies of erased messages. But cell phones also contain phone numbers, notes and other information saved on the chip that might contain evidence.

Signature Sources. Some new and emerging technological advances create *signatures* that can be used as forensic evidence. E-mail has always contained a *header* that contains information about the sender and where the e-mail originated. Cyber forensic experts can already usually trace an e-mail back to the sender. But new technology has the ability to provide an invisible signature on a paper document from a printer with this capability. Thus a paper document can be forensically shown to have been printed on a certain printer.

Conclusion. When a fraud investigation turns up some evidence from conventional means, but not enough to be competent sufficient evidence to win a court case, then investigators should consider extending the scope of digital evidence beyond the suspect's and entity's computer drives. There could be evidence of the fraud in devices connected to the suspect's computers, offline storage, other peripherals, personal devices, communication devices and signature-enabled devices. Together, these additional sources can provide a wealth of sources not only in direct digital evidence from the fraud scheme, but indirect evidence about the fraud that sufficiently incriminates the suspect.