DIGITAL FORENSICS

A New Challenge for Accounting Professionals

By John Brozovsky and Jie Luo

Over the last several decades, accounting professionals have benefitted from the advances in Information Technology (IT). Instead of relying on hard-copy, paper-based sources, business practitioners adopted cost-effective IT to preserve and analyze information. These IT solutions have transformed the way we communicate, create data, store information, and examine evidence. An unfortunate consequence of these advances, however, is that cybercriminals now have new means to tamper with a firm's data and steal valuable information—without ever seeing or coming into contact with the victim.

In response to these challenges, methods to safeguard digital assets have been developed, spawning a new field known as digital forensics. The methods of gathering digital evidence are evolving quickly to keep pace with emerging technologies and more-skilled cybercriminals. Therefore, it's important for management accountants and other financial professionals to understand the development of digital forensics, evaluate current techniques, and assess where the technology of digital forensics is heading.

There are a number of reasons why management accountants need this information. First, they're going to be on the front lines, identifying where and when something needs to be done. Second, management accountants need to be able to talk with IT people and, as such, must have at least a basic understanding of what to instruct them to do. Third, to the extent that management accountants get involved in internal audits, it becomes even more critical that they know a bit about digital forensics. The CMA® (Certified Management Accountant) exam even includes issues that deal with internal controls and risk.

DIGITAL FORENSICS IS A POWERFUL TOOL FOR BOTH LAW ENFORCEMENT *AND* FOR BUSINESS ORGANIZATIONS IN PREVENTING AND DETECTING UNAUTHORIZED ACCESS TO A FIRM'S PRIVATE INFORMATION.

What Good Digital Forensics Tools Should Do

The main selling point of digital forensics is its capability to identify data users—legitimate or not—and what these users do with the information they access. Digital forensics has played a key role in gathering evidence for numerous court cases by allowing investigators to examine data storage devices, network servers, e-mail servers, and the like. It's therefore a powerful tool for both law enforcement *and* for business organizations in preventing and detecting unauthorized access to a firm's private information. In this article, we'll discuss many of the tools that make this evidence gathering possible and the extent to which they're useful to accounting professionals.

For digital forensics outputs to be of practical value to their users, digital forensics tools must satisfy a set of six guiding principles that experts can agree upon. First, digital forensics tools must be rigorous in reporting information about date and time. Any controversy in this regard could compromise the credibility of evidence supporting a claim.

Second, related to the first principle, digital forensics tools should be particularly competent in handling log files. As the log file describes all activities of a certain user, digital forensics tools must be able to examine them extensively as well as recover and capture images of those files, if necessary. The reasoning behind this principle is clear: If there's any trace of suspicious activities, it should be present in a log file. Therefore, the handling of this type of file should be as competent as possible.

Third, the quality of produced evidence should be high enough to avoid significant disputes in court. In short, the higher the quality of output generated by digital forensics tools, the better it will serve the party who uses that output to make its points.

Fourth, a good digital forensics tool should be able to recover deleted files whenever possible. That is, the tool should be able to recover the file when the data is still present on the hard drive, even after a user deletes it. Since criminals frequently try to cover their tracks by deleting files, the ability to recover these files is of primary importance.

Fifth, digital forensics tools should have a keyword search function to assist on file examinations. While seemingly trivial, this function makes suspicious activity detection easier while minimizing the risks of corrupting the original file under examination. A corrupted file would negatively affect potential admissibility in court.

Sixth, digital forensics tools must be able to retrieve Internet browsing history, particularly if it has been deleted or tampered with. The browsing history represents the bulk of information flows between the firm and outside parties. Because most cyberattacks are generated outside the firm, it's vital to extract and examine Internet browsing data as accurately as possible.

Commercial Products for Thwarting Criminals

There are many digital forensics tools available to accounting professionals and their organizations ranging in cost from $1,000 to $3,000—plus annual maintenance fees that run about 20% to 30% of the purchase price.

(Of course, all prices are subject to change, and vendors must be contacted for current prices.) The four key players in the commercial market are Guidance Software's EnCase, AccessData's Forensics Toolkit (FTK), Paraben's P2 Commander, and Technology Pathways' ProDiscover. Though your specific needs will depend on the type of business you're in, all four of these leading packages—especially EnCase and FTK—cover all the functions and features of digital forensics that will likely be necessary with regard to your data.

EnCase is currently the market leader in digital forensics, and its technology is commonly validated in court proceedings involving data acquisition, analysis, and reporting. It features folder and deleted file recovery, automated scripting and decryption, and a timeline view of file activities. It also can perform a "signature analysis," a process of identifying files whose headers or extensions have been modified or removed to hide their true types and functions. Guidance Software offers consulting services as well as EnCase training seminars and certifications.

AccessData produces the popular FTK software. It uses wizards, which are a type of interface that provides users with a step-by-step guide to perform a task or application. Through wizards, clients are aided in "data acquisition, filtering, case management, and reporting," the company says. Compared with EnCase, FTK supports more image formats; it also provides great flexibility in reporting and powerful password recovery.

Paraben's P2 Commander offers features similar to those of EnCase and FTK, with a focus on single-workstation tools and a program that allows remote monitoring over a network. Paraben's P2 Commander differentiates itself by specializing in e-mail examination and handheld forensics, including PDAs, cell phones, and GPS devices, among others.

ProDiscover, from Technology Pathways, is known as an evidence-collecting toolset. It's capable of capturing a disk image, including those hidden in hardware-protected areas, physically and over a network. A disk image is crucial to enabling accountants, IT personnel, and other investigators to recover original files from a hardware device and to provide forensic imaging—for example, to map all contents of the hardware to a single file with a level of accuracy that's admissible in court.

Portable devices combining computer and cell phone capabilities, such as Apple's iPhone and Android-based smartphones, have become increasingly popular over the last several years. In response to this trend, several digital forensics tools, such as FTK Mobile Phone Examiner (MPE), EnCase v7, and Paraben Device Seizure, have emerged, with prices typically ranging from $1,000 to $15,000, with annual maintenance fees also required. Less-expensive alternatives, however, can be found in recent developments in the academic community, such as the iPhone forensic framework (iFF).

While large companies can't afford to be without a good detection program, law enforcement is by far one of the biggest users of digital forensics. If your organization asks the authorities to assist in a cybercrime investigation, they'll likely use Microsoft's Computer Online Forensic Evidence Extractor (COFEE). (Law enforcement organizations receive COFEE for free, and more than 2,000 agencies worldwide are using it, according to Microsoft.) COFEE, Microsoft says, is a "USB drive that allows law enforcement to run more than 150 commands on a live computer system and save the results on the portable drive for later analysis." By doing so, valuable information

FURTHER READING

Robert Vamosi, "Microsoft Serves Law Enforcement Free COFEE," *CNET*, April 30, 2008; http://news.cnet.com/8301-10789_3-9932600-57.html.

Golden G. Richard III and Vassil Roussev, "Next-Generation Digital Forensics," *Communications of the ACM*, February 2006, pp. 76-80.

Marcus K. Rogers and Kate Seigfried, "The Future of Computer Forensics: A Needs Analysis Survey," *Computers & Security*, February 2004, pp. 12-16.

Mary-Jo Kranacher, Bonnie W. Morris, Timothy A. Pearson, and Richard A. Riley, Jr., "A Model Curriculum for Education in Fraud and Forensic Accounting," *Issues in Accounting Education*, November 2008, pp. 505-519.

Mohammad Iftekhar Husain, Ibrahim Baggili, and Ramalingam Sridhar, "A Simple Cost-Effective Framework for iPhone Forensic Analysis," *Digital Forensics and Cyber Crime*, 2011, pp. 27-37.

is preserved that would be lost if the computer were shut down and transported to a lab.

Open-Source, Free Tools

If your organization is small and not yet ready to invest in an expensive commercial package, several open-source digital forensics tools are available as an alternative. Open-source tools are often free and frequently offer faster enhancements, including software updates to head off viruses. On the downside, they're more limited in their scope of coverage (meaning you might need more than one package) and have less customer support than commercial packages. Nonetheless, open-source products are certainly worth a look for businesses that don't rely extensively on computer technology yet don't want to make their data easy prey for cybercriminals.

One such open-access tool is FTimes, which is used as an "evidence collection" tool. It gathers information about directories and files in a manner "conducive to intrusion and forensic analysis," according to its producer. It logs four types of information: progress indicators, configuration settings, metrics, and errors. The program uses a command line interface, which means users need to type in commands rather than pointing and clicking with their mouse.

Another free alternative to consider is Galleta, an open-source tool that examines the contents of cookie files on the Internet to reconstruct a user's Web activities. The program parses each cookie file and produces field-delimited files. These files are easily imported into standard spreadsheet programs as there's a fixed item, such as a comma or a blank space, between each variable. Galleta works in Windows, Linux, or Mac systems.

Other tools, such as NetworkMiner, help monitor networks with sniffer/packet (the small bursts of data into which e-mails are divided) capturing tools to detect suspicious issues. They're used to gather information about hosts, making them popular among incident-response teams and law enforcement. Another free program, The Sleuth Kit (TSK), is open-source software that provides file extraction and forensic analysis in Windows, Linux, and Unix.

Forensics Toolkit Imager (FTK Imager) is a free software program produced by AccessData that allows users to create image files and store them in several different file formats, including those used by Guidance Software's EnCase. FTK Imager can run off of a USB thumb drive, which is particularly convenient for many users.

Digital Forensics in Action

Phishing e-mails, which attempt to deceive the recipient in order to acquire protected or personal information, have become one of the most common threats to information systems. Legitimate senders, of course, will never ask for private and confidential data via e-mail; therefore, most users are skeptical about e-mails that ask for information the sender should already know. The trick for the recipient is knowing how to verify that the e-mail really did originate from the individual or organization that the sender claims to be.

There's an easy way for you and your organization to protect against spoofing, phishing, social engineering, and other types of attacks from hackers. Consider an e-mail sent to a Google Gmail account. The user—you,

Figure 1

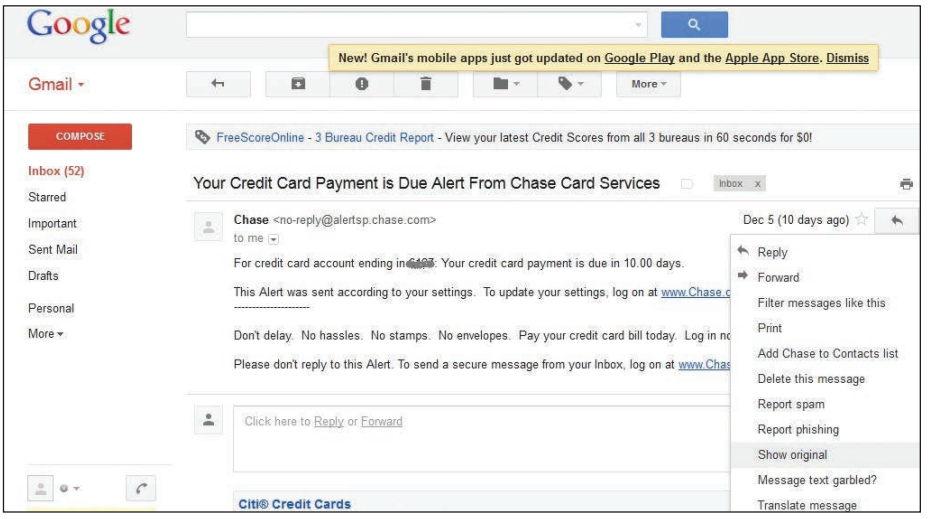
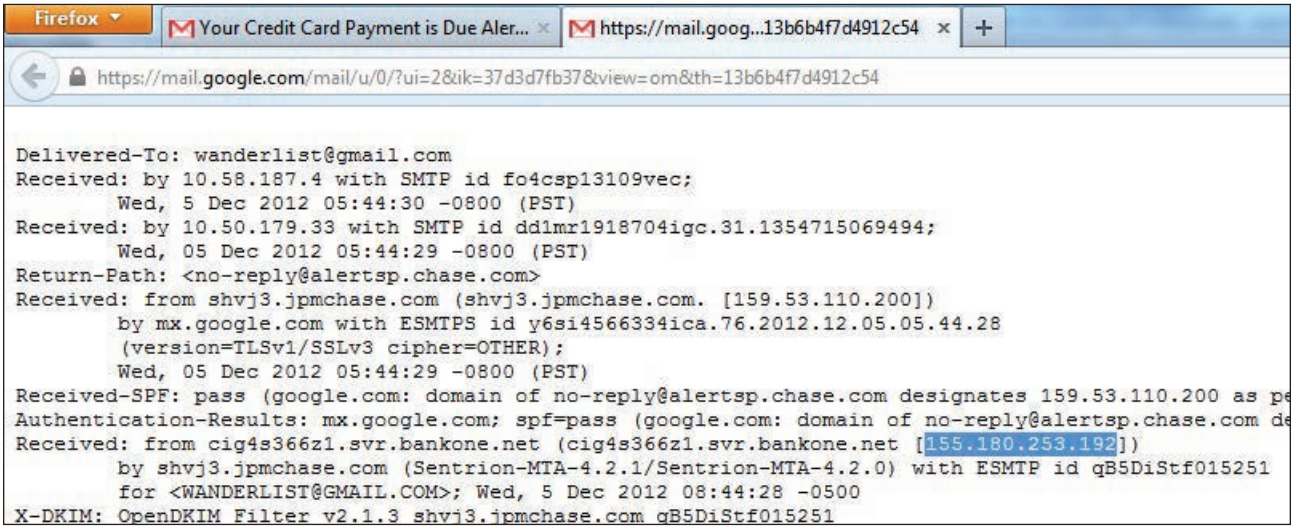


Figure 2



we'll assume—has a credit card account with Chase Bank. If you receive an e-mail that appears as if it were sent from Chase, open the e-mail, click on the inverted triangle next to the sender's e-mail address, and then select "Show Original" from the dropdown menu (see Figure 1). A new window opens (see Figure 2). In this new window, locate the sender's IP address (a four-part number, set off by periods, that's frequently 12 digits).

Once you find the IP address, copy and paste it into the search bar at www.whatsmyip.org (see Figure 3). Whatsmyip.org is a website that allows you to trace the originating IP address of the sender to pinpoint the location from which the e-mail was sent (arin.net and domaintools.com are two other examples). Using the IP address/domain name, the Whois & DNS link on Whatsmyip.org can provide more detailed identification information, such as the organization's name, geographical location, and domain server (see Figure 4). Therefore, using Chase as our example, if the IP location and the organization identification indicate a different location from where Chase Bank is headquartered and/or have a different organization identification, the e-mail could be phishing for private information. This technique also allows the courts to trace e-mail communications between disputing parties. This is a simple example, of course. More-complicated situations may require downloading packages and possibly purchasing complex forensic software.

So what's the current state of forensic software, and where is it headed? To answer those questions, let's discuss the trends for these tools from the perspective of accounting professionals.

Where Things Must Improve

To understand where this expanding technology is headed, we examined the current environment and found four factors that should markedly affect the present and future of digital forensics tools:

1. Technological progress. Despite good efforts, digital forensics has been unable to keep pace with the rapid advances of computer technology. These advances have increased the complexities involved in analyzing IT devices, and it takes time for digital forensics to catch up. To facilitate the work of digital forensics, data that's deemed important should be stored in hardware that most digital forensics tools have proven qualified to operate with. This is especially important when your organization is considering a new technology touting some security advantage as an alternative to data storage.

2. Lack of collaboration. Most of the digital forensics community (government departments, corporations, business organizations, and academia) rarely coordinate their efforts to find solutions to improve tools and procedures. Pooling knowledge from their collective experience would be invaluable to improve forensic analysis. Since there's currently no solution to this, our perspective is that accounting and IT professionals should clearly identify what type of digital forensics fits the particular needs of their businesses and refer to the most up-to-date tools—either commercial or open-source.

3. Forensic education. Most university programs on digital forensics follow their own path. This means that individuals who graduate with a degree in the field have widely varying amounts of knowledge and understanding

Figure 3

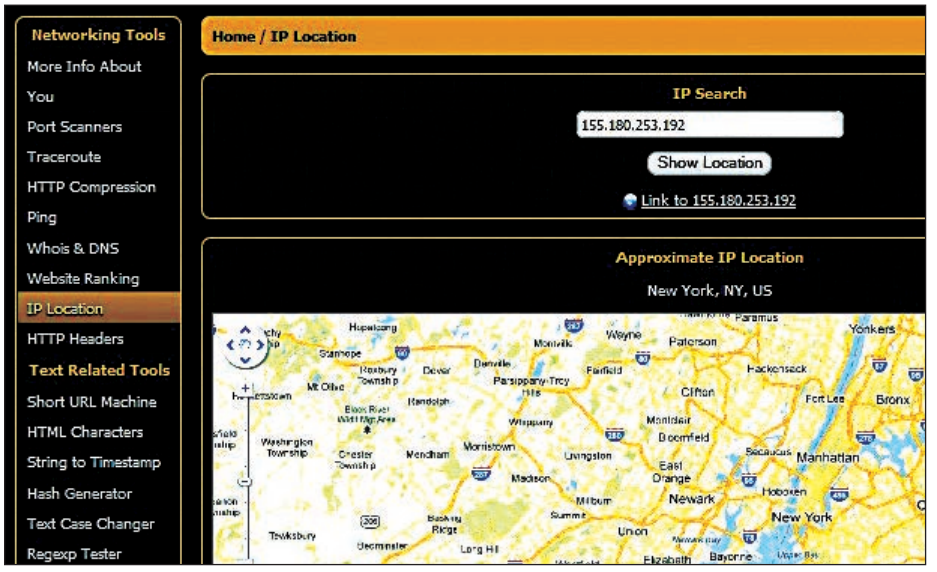
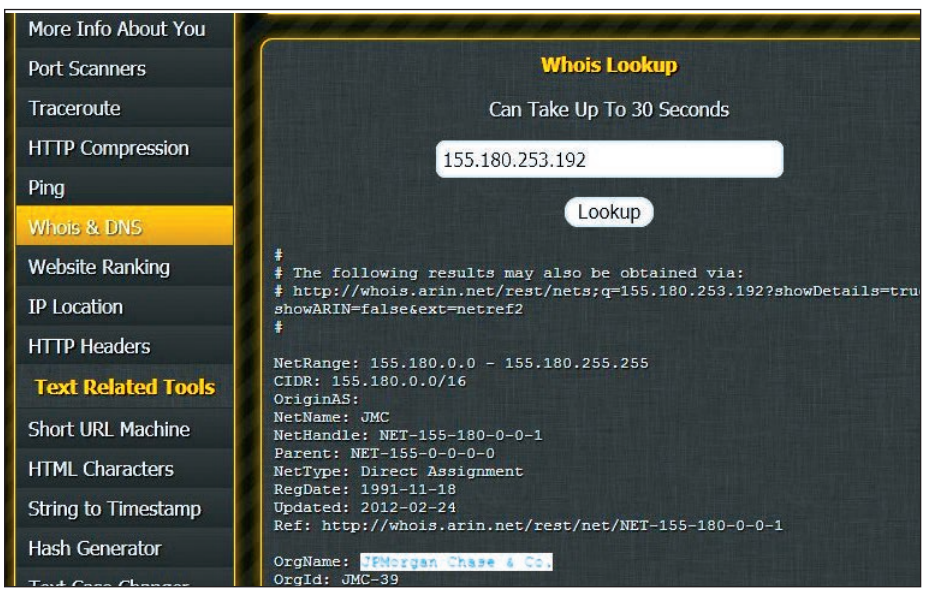


Figure 4



of the subject. In addition, as the field of digital forensics continues to evolve rapidly, many instructors aren't acquainted with the latest developments. A proposed curriculum in forensics has been developed, but it isn't digital specific.

4. Lack of well-established standards. The lack of formal standards provided by an overseeing body creates an issue with defining limits for forensic evidence, such as quality levels, ethical boundaries, and technically valid methods. Fuzzy concepts and unclear rules in the world of digital forensics are currently an unfortunate reality for which there's no immediate solution. Some guidance on the "rules," however, is available by examining recent court decisions. But if you're looking for advice about concrete issues of interest to your particular business, consult only with professionals familiar with the world of digital forensics.

Despite these shortcomings, organizations shouldn't simply dismiss these tools based on their current limitations. Management accountants have a unique knowledge about their firms and understand which information is valuable enough to be at risk of tampering, theft, or unauthorized access. IT experts generally don't have this information, and their technical skill may not be enough to spot distortions that would be obvious to an accountant.

Clearly, management accountants can use basic knowledge of digital forensics to help prevent such situations, avoid escalating damages in cases where security has been breached, and lend help to the IT experts in spotting tampered data. As businesses rely more and more on technological gadgets, getting acquainted with the methods used to track cybercriminals—and implementing tools to thwart them—will prove invaluable in efforts to keep business data safe. **SF**

John Brozovsky, Ph.D., is an associate professor of accounting and information systems in the Pamplin College of Business at Virginia Tech University in Blacksburg, Va. You can contact him at jbrozovs@vt.edu or (540) 231-5971.

Jie Luo, Ph.D., is an assistant professor of accounting in the Division of Business at Concord University, in Athens, W.Va. You can reach her at jluo@exchange.concord.edu or (304) 384-5397.