

## Non-traditional Sources of e-Data In Investigations

*It Pays — For All Parties — To Know Where It Is*

By David Sumner and Damon Reissman

From teenagers to retirees, the digital revolution has touched almost all aspects of our everyday lives. Widespread business use of voice mail, e-mail, instant messaging (IM), and sales-management systems, as well as use of portable devices, simplifies our work in many ways, but also makes electronic discovery much more complex.

This article describes some of the more prominent non-traditional sources of electronic data. The reader should be mindful of these sources when he or she develops a discovery work plan — and should weigh the costs and benefits of each option.

The amendments to the Federal Rules of Civil Procedure that took effect last month added electronically stored information (ESI) to the official list of items subject to production. Typical ESI sources include:

- Forensic copies of personal computers;
- Company file servers;
- e-Mail servers; and
- Backup tapes.

**David Sumner** is a manager in the Dispute Analysis & Investigations practice of PricewaterhouseCoopers' Philadelphia office. He focuses on investigations and purchase-price disputes. Sumner is a certified public accountant licensed in Pennsylvania. Reach him at david.w.sumner@us.pwc.com. **Damon Reissman** is a manager in the Forensic Technology Solutions practice of PricewaterhouseCoopers' Boston office. He focuses on computer forensics and corporate investigations. He is a certified fraud examiner and an EnCase certified examiner. Reach him at damon.reissman@us.pwc.com.

Alternative sources of ESI (whether from external data sources or from a more detailed review of forensic hard-drive images) can take many forms and can produce additional evidence. Examples of non-typical ESI, which we will examine in detail, include:

- Web-based e-mail;
- IM;
- Voice mail;
- Internal database systems;
- iPods; and
- Other portable storage devices.

### CURRENT NON-TRADITIONAL COMMUNICATIONS TOOLS

#### Web-based e-Mail

Outlook Express is one of many e-mail clients commonly available. Because it's usually installed automatically with Microsoft Windows, users often set it up to access e-mail from their personal accounts. This information is easily accessible and is frequently used in investigations.

Corporate e-mail systems often allow access to server-based company e-mail through Internet browsers. Also, countless users have turned to Web-based e-mail services (e.g., Hotmail) as a parallel personal and corporate communication method. Commonly used to communicate with friends and family, Web-based e-mail is also used to conduct company business outside normal channels. This circumvents many companies' e-mail restrictions, internal controls and retention policies. Some companies have instituted policies that filter, or restrict, attachments (or both), or prohibit personal use of corporate e-mail altogether. But these actions have the unintended consequence of forcing employees to use Web-based e-mail accounts for personal communications and workarounds when the restrictions are inconvenient for the workers.

e-Mail messages viewed through Web-based accounts are often recoverable on the user's computers via an advanced forensic review of a PC's temporary files. Fragments, and sometimes entire messages, can often be identified on a computer long after the message has been deleted from the server. e-Mail attachments downloaded to temporary folders on the local computer for viewing can remain on the PC for extended periods.

#### Instant Messaging

IM programs have become ubiquitous in corporations. Often, employees prefer IM over e-mail because of the added dimension of perceived presence that IM gives, and for the ability to get an immediate response. IM conversations are often less formal even than those conducted through e-mail, because users are generally under the impression that they are not being recorded.

Similar to the situation with e-mail, IM programs are available in corporate-enterprise versions of software, and in public versions. The most popular public networks are AOL Instant Messenger, .NET Messenger and Yahoo Messenger. All these platforms have their own programs allowing access to their network for communication and file-sharing purposes.

Enterprise IM platforms allow file transfer, and group chat and individual conversations, via centralized servers, but may not allow connectivity with public IM networks. Enterprise IM servers can also be set up to automatically log all communication. In certain regulated industries, for instance, companies may be required to retain these logs along with other data covered by their retention policy.

These logs, subsequently, may reside on the PC for a long time and, when deleted, they might also be recoverable through forensic analysis, like any other deleted file.

In a recent investigation, an IM exchange included instructions for an upcoming meeting with company auditors which, to paraphrase, said, "Remember not to show the auditors the real numbers. Show them book B."

### **Voice Mail**

Voice-mail messages have also become a growing element in investigations. In addition to a standard server that houses voice mails that a user can call into, providers are making an effort to integrate voice mail into other messaging platforms. Messages can now be attached to an e-mail as a sound file, for example, and transcribed in an e-mail or text message to a mobile device. For instance, a recovered voice-mail message was one of the primary pieces of evidence listed in the U.S. Attorney's indictment against former WorldCom CEO Bernie Ebbers.

### **Internal Systems and Productivity Tools**

An important aspect of any investigation is identifying the company's programs and databases, and designing a plan for effective analysis of relevant information stored in these materials. If the scope spans several years, data can be found in multiple versions of a system, and in legacy systems.

Many organizations also use sales force automation tools. These tools might be as simple as a contact manager, or may involve a more robust system used by the sales force to track opportunities and individual notes on each meeting with a potential customer. This type of data can be valuable in any investigation involving sales practices (e.g., Foreign Corrupt Practices Act, or anti-trust), but they also have unique challenges. Corporate retention policies might not include the sales force automation system that could be located on a separate corporate or third-party server, which could present some trying compliance challenges.

### **Portable Devices and Other Storage Media**

Portable productivity tools, such as Blackberrys, Palms and Windows CE-based personal digital assistants (PDAs) are mainstream. These devices provide users with e-mail and Internet access separate from their company networks and policies. People can use standard cell phones for minor scheduling and note-taking, and for text-messaging. While this information might be synchronized or backed up to the user's computer and the company's server, that's not always the case. Many of these devices have the ability to synchronize not just with the corporate system but also with Web-based e-mail accounts, which is another avenue used to circumvent internal controls.

The physical dimension and cost of external storage devices (including thumb drives) have shrunk while their capacity continues to grow. A consumer external hard drive can have more capacity than some small business servers, and the newest iPod can hold as much data as common PCs used by most businesses. The ease of installation and use also presents benefits and challenges. And, as though that weren't enough data-harboring devices with which to contend, document servers and fax machines can contain information in memory and, as with voice mail, faxes can be sent directly to e-mail accounts. All this information boils down to this: Investigators should not ignore these devices, because they all might hold critically useful information.

In a recent case, important non-photo documents were located on the memory card inside a digital camera. In another case, computerized cash registers were acquired to search for payments on a transactional basis and then compared to what was posted in the accounting system. This involved analyzing data from two very different types of sources, one of which is not commonly examined.

### **OBSTRUCTIONIST ACTS**

It's a standard, and because of that, a given: In investigations, suspects try to hide or delete important information. These attempts can range from simply deleting documents and e-mail to installing wiping software and reinstalling operating systems. With the right expertise, it's possible to recover much of this evidence, as well as provide proof of this obfuscation as evidence itself. In a recent case involving an executive at a prominent software firm, a PC was completely "wiped," and then the Linux operating system was installed. Use of sophisticated forensics analysis led investigators to the conclusion that the installation of Linux took place after government subpoenas had been issued; these actions were identified and factored into the case as evidence detrimental to the defendant.

A particularly useful option (from an investigator's perspective) in Outlook is the "Journal" feature, which, if turned on, logs activity associated with Microsoft Office applications, including Outlook e-mail activity. The logs track when e-mails are viewed and for how long, including any activity involving attachments. This was very useful to a recent investigation in which an interviewee denied having reviewed an attachment to a certain critical e-mail. While the interview was still in progress, we were able to access the Journal logs for the interviewee's mail file and sent

the proof to the interviewers that not only had the interviewee opened the e-mail but that the interviewee had opened the attachment for six minutes at 2:54 p.m. on the day in question.

### **SUMMARY**

Investigations and electronic discovery have unique challenges. We suggest that an inventory of the systems a person of interest to an investigation uses on a daily basis be compiled through a method such as interviewing a peer. More often than not, one will encounter a system or process wholly separate from the standard corporate e-mail and shared-file networks that could provide critical data.

When devising an electronic-discovery plan, litigators and investigators need to consider the following questions, and weigh the costs and benefits of each data source, in addition to the traditional corporate e-mail and file-sharing network-discovery procedures:

- Are legacy systems involved?
- If a link between individuals is being sought, or confirmation that an individual had knowledge of an occurrence is a goal, which of the multitude of communications channels should be considered?
- To establish who possessed an important document, what devices should be searched?
- Is anything this company or person uses not common?
- What are the company's policies re-garding personal use of non-standard programs or peripherals?
- What other types of data would advance the inquiry?

These are the questions that might need to be answered in today's investigations. Tomorrow's technological advances will add their own complexity with new operating-system features like increased data volume, automatic file encryption and built-in "secure deletion." It's easy to be overwhelmed by the multitude of data sources in today's corporate environment, and just as important as identifying all of these sources is deciding which sources will yield the best and most cost-efficient answers to address the matter at hand.

