The CPA Journal

Forensic Computing: A Review of a Growing Technical Field

By Yigal Rechtman

JULY 2006 - Forensic computing is a science that can have many definitions. For example, the Australian Institute of Criminology defines it as: "the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable." For a CPA engaged in litigation support services, this area of work increasingly requires the use of specialists. Having a general knowledge of this process can help accountants respond to client inquiries and can make consultation with forensic computer specialists more effective.

As with other litigation support services, the objectives of a forensic computing engagement change for each case. For example, financial fraud cases may require delivery of all correspondence related to a person with access to a sensitive Web server, while matrimonial cases may require only specific financial information from a home computer. The devices under scrutiny—such as mass computer storage disks, memory sticks and their variations, digital cameras, cellphones, and copiers— will also vary with the engagement and advances in technology.

Types of Engagements

There are two types of forensic computing engagements, based upon the use of the device as it pertains to a case. The first type of engagement is when a device, such as a computer, has been the tool with which an activity was carried out. This engagement will center on retrieval of the evidence from that device. For example, a text message may have legal implications: The June 2004 case of athlete Kobe Bryant revolved around a text message that was sent from his accuser to a third party. The content of the text message was subpoenaed and presented as evidence.

The second type of forensic computing engagement focuses on an electronic device that has been the target of a crime. This engagement entails other devices and other types of evidence. For example, consider a Web server that has been breached for the purpose of identity theft. Evidence for such an engagement would include the electronic traces of the perpetrators, but also an analysis of the use of the stolen information, such as whether the stolen identities were sold.

Types of Perpetrators

In a generic way, forensic computing engagements involve three types of perpetrators. This classification helps a forensic computer specialist know where to effectively search for evidence.

First, individuals with a high level of technical knowledge can often conceal their steps. Their technical knowledge about the activity or devices utilized also facilitates their illicit use in a manner that is challenging to prove.

The second type of perpetrator is one with low-level technical skills who will attempt, with varying success, to

perpetrate and conceal his activity. Obviously, the lower the technical skill of the person, the easier it is to find and prove the suspected activity.

A third type of possible perpetrator is an everyday authorized user. For example, a manager who is about to leave a professional firm to start his own company would have the basic technical skills through his everyday work to search the client relation management (CRM) database for prospective clients. Such an activity would likely not breach any security measures in the computer system, nor would the user need to conceal the activity. Ethical and legal considerations aside, such activity is technically not a breach of security, because the manager is an authorized user of the CRM.

Forensic Process

The forensic computing process includes identification of evidence, preservation of that evidence, and analysis of the results. To be legally valid, a proper documentation and reporting of the results must be performed and delivered to a client or their legal counsel.

A forensic computing specialist must be familiar with the rules of evidence as well as the technical skills necessary to identify and retrieve electronic evidence. For example, in a matrimonial case revolving around financial information in an electronic worksheet, a technician may not just start up the computer and save the worksheet to a diskette. First, a full duplication, in several copies, of the entire hard disk must be made in a manner that will allow both sides in the case to apply their own procedures to the data while maintaining the integrity of the underlying electronic image of the memory. Second, retrieval from the copy of the source disk must be done in such a way that changes to the original cannot be made. For example, in a corporate application, software packages such as Encase or Ontrack scan large amounts of unprocessed data. Utilizing an intelligent filter, meaningless and random bits of information are removed and screened out, while meaningful text or keywords are delivered to the investigator.

Finally, a strict documentation of the entire process, complete with names, dates, locations, and procedures applied must accompany the device in question. In the legal vernacular, the technical expert must "bag and tag" all the evidence that comes under their purview.

Technical Issues

From a technical and legal perspective, there are three types of electronic evidence that can be retrieved, based on their completeness and ease of retrieval.

First, there is active data. In the example above, an electronic worksheet with financial information that did not experience any loss of integrity is an active-data type of evidence.

The legal area involving discovery and delivery of data is complex and beyond the scope of this article. The Federal Rules of Civil Procedures mandate certain restriction on "electronically stored information," which cannot be considered "reasonably accessible" under certain circumstances, such as backup or latent data, discussed below. This and other legal tests must be considered in all engagements.

Second, archival data is information that cannot be retrieved by the user but otherwise has no loss of integrity. For example, in certain operating systems several versions of the same file are maintained automatically. The last version represents active data, but an older archival version may still exist, without being compromised but

typically hidden from the user.

Last, latent data are purposely hidden from the user and may be incomplete or unreadable. For example, an area of a disk drive that has been marked as a "deleted file" in fact may still contain some information from that file that has not been overwritten. Specialized software can retrieve such data and provide evidence of its existence that is otherwise obscured from the user.

To further understand the electronic environment, it is imperative to discuss the concept of abstraction. In an electronic environment, activity is performed in abstraction of underlying devices using a driver. Modern computer users, for example, are familiar with a "device driver" required for the use of certain hardware. The driver is one instance of an abstraction: it provides translation between the requests of the user and the commands that the underlying unit understands. For example, a printer driver can receive the request "print in *italics*" and translate it into the corresponding command that a printer's hardware can understand. Abstraction occurs in many instances in an electronic environment. It may start with the chip that computes the command, then continue to the hardware driver, the software driver, the operating system, applications, and so on.

Because of abstraction, evidence that may appear to have been no longer active in one layer may continue to be active in another. For example, a hardware driver may contain information of the last piece of a file that was read. Although the file itself may be deleted and overwritten, retrieval of that portion of the memory from a disk driver may allow data to be retrieved and presented as evidence.

Data analysis and its usefulness vary depending on the engagement at hand. A series of webpage visits, for example, may be required whereby the sequence of the pages is of import to the legal process. In other instances, versions of the same file containing revised financial information may have significance to the evidentiary matter. In all cases, the application of the rules of evidence is of the utmost consequence, as it not only provides a sound basis for any conclusion but also protects the technical expert and his clients from claims against the merits of the evidence provided.

The Role of CPAs

CPAs, who increasingly provide litigation services and technical expertise to businesses, are well suited to forensic computing engagements in several ways. Understanding the requirements of the forensic computing, accountants can help prevent tampering with electronic evidence. Although consultation with an attorney is typically required, many companies often turn first to their auditors or accountants when fraud, a computer breach, or employee misconduct has been discovered. Understanding the possible issues facing a business may allow accountants to provide the most help to such requests.

Yigal Rechtman, CPA, CFE, CISM, CITP, is the president of Person Consulting Organization, Inc., of New York City. He is also vice-chair of the NYSSCPA's Technology Assurance Committee.
Disclaimer: *The author is not an attorney and does not provide a legal opinion. Computer hacking techniques lie outside the scope of this article.*