

BLACK TECH FORENSICS

Collection and Control of Electronic Evidence

G. Stevenson Smith

Today, 30 percent of written documentation never reaches a printed format (Jessen, 1997, Johnson, 1997). It is expected this percentage will grow larger in the coming years.

Consequently, the nature and verifiability of evidence in criminal and civil procedures has drastically changed within the past ten years. At one time, only printed documents were needed for analysis, but now electronic documents must be dealt with in investigations. In many legal jurisdictions, collection of evidence is automatically assumed to mean electronic documents without requiring that "electronic documents" per se be specifically described in the information request.

In using electronic evidence, it must be remembered that an electronic document can be changed much more easily than a printed document. More frightening, a knowledgeable technician can change electronic documents and corresponding logs without leaving a trace that a change occurred. These electronic documents may be images, audio or video clips, text, magnetic tracings, and software programs. They can be found in personal computers, web servers, tapes, mainframes, pagers, personal data assistants, floppy disks, zip disks, CDs, DVDs, fax machines, wireless phones, smart cards, and even images burned into a monitor.

This column will assist readers in gaining an understanding of important new issues related to the collection and the possible seizure of electronic evidence. Additionally, readers will gain insight into how electronic collection procedures can directly affect them.¹

Legal Reasons for Seeking Electronic Evidence

Electronic evidence is collected for several reasons. Electronic evidence may be used during either civil litigation or criminal investigation. In such situations, it is important for all parties to be

¹ SAS No. 80, Evidential Matter, an amendment to SAS No. 31 on audit evidence, provides guidelines for audit engagements encountering electronic documents. It states that for a system predominately consisting of electronic audit evidence, it may not be practical or possible to reduce detection risk to an acceptable level using only substantive tests for financial statement assertions. In these cases, the auditor should perform tests of system controls to show that they are strong enough to mitigate the risks inherent with electronic audit evidence. Together with system control tests, substantive evidence should be strong enough for the auditor to issue an opinion. Such an audit may require the use of generalized audit software or a continuous audit module to test controls. Additional guidance is provided by *The Information Technology Age: Evidential Matter in The Electronic Environment* (AICPA, 1997). Of course, adhering to strong internal controls may not prevent a hacker from gaining root access on your firewalled system as has been demonstrated numerous times in recent years.

aware of the possible consequences of their actions, or the actions of others, as electronic evidence is sought under court discovery procedures.

Of course before it can be determined why or the manner in which electronic evidence will be collected, the context and the role of electronic evidence in the proceedings needs to be determined.² In making this determination, the first two questions to answer are:

How can the electronic evidence be legally seized or collected?

And, how can such evidence be collected without altering or destroying it?

Criminal Cases: In criminal investigations, many electronic devices, as those previously listed, may contain evidence needed by prosecutors.³

In order to determine if the evidence can be legally collected, the role of the electronic device in the crime needs to be ascertained. Without such a determination, the seizure of evidence and the legal seizure of evidence may become separated. For example, the Federal Rules of Criminal Procedure 41(b)(2) allow for the seizure of contraband, fruits of crime, or things

² Under criminal investigations, the electronic documents are sought with a warrant or possible subpoena. Under civil proceedings, they are sought through discovery requests such as interrogatories or dispositions. Either the Federal Rules of Evidence or Federal Rules of Civil Procedures provide legal justification for seeking such documents.

³ The Department of Justice defines a computer crime as: "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." (National Institute of Justice, U.S. Department of Justice, *Computer Crime: Criminal Justice Resource Manual 2* (1989))

criminally possessed. When a 15-year-old hacker uses stolen credit card numbers to purchase computer equipment, the equipment is contraband and it can be seized.⁴ When legitimate software, such as MS Office 2000, is downloaded from a warez site, it is contraband.⁵

On the other hand, the computer, along with other equipment, may be seized as evidence when it is not contraband, but when it played a significant role in the crime – it was an instrumentality of the crime. For example, a pornography group could have used the computer to send images through ISPs and the Internet. Such a computer is an instrumentality of the crime (as are the images themselves). From the porn dealers point of view, a legal argument could be put forth that the electronic equipment (computers, modem, PDAs, fax machines, etc.) were illegally seized because they were not contraband (they were legally purchased) and they contained other legitimate data. For example, if this evidence is mixed with newsletters or book materials published or to be published by the accused criminals, it may come under First Amendment privileges and protections that prohibit the use of search warrants against members of the press. Therefore, the legal argument would be made that any electronic evidence found on these devices should not be admitted into the court proceedings as evidence.

⁴ Seizure occurs through the issuance of a warrant. A warrant is issued under probable cause guidelines by a judge authorizing a law enforcement officer to seize property or make a search. A warrant for a search, only, may culminate in the seizure of property. The warrant itself needs to be written as narrowly as possible yet include descriptions of property to be seized or searched.

⁵ A warez site is one that provides cracked versions of commercial software or movies. The copyright protections have been stripped.

The computers used by the ISP are also electronic evidence because of the information logged and recorded about transmissions through the site. Consequently, these computers have important evidence for the case and such evidence also needs to be collected. Unfortunately, if a small legitimate business has their Web site hosted by the ISP, this business may also be shut down along with the pornography group's operations.

Law enforcement personnel do not have the right to seize all properties, and courts exercise the "reasonable person" doctrine in determining whether seizures go beyond those boundaries. Restrictions on wide seizures of property by law enforcement are based on Fourth Amendment rights that require descriptions of the places, people, and things to be searched and seized.⁶

In many computer-related crimes, evidence will be only available from equipment that does not belong to the criminal. For example, distributed denial of service (DDOS) attacks conducted by hackers are set up so that they cannot be traced back to the attacker.⁷ In a DDOS attack, the

⁶ The Fugitive Apprehension Act of 2000 (S.2526) was passed by the Senate on July 26, 2000 (<http://www.senate.gov/~thurmond/press/000720.htm>). Its stated purpose is to "fund task forces to locate and apprehend fugitives in federal, state and local felony criminal cases and give administrative subpoena authority to the United States Marshals Service." The law extends government search authority to witnesses as well as accused criminals. Administrative subpoena power provides for the search of both witness and accused criminal's properties without disclosing that a search was conducted. If this legislation becomes law, it would likely be challenged in the courts.

⁷ In a standard denial of service attack, targeted machines are overwhelmed with a flood of transmissions that prevent legitimate users access to the system. The attack essentially creates a busy signal. Under a distributed denial of service attack, attackers use thousands of "zombie" computers to increase the attack intensity. There are freely downloadable software programs capable of orchestrating these attacks.

attacker uses computers belonging to others to assist in attacking the target computer system. These "zombie" computers, legitimate in themselves, have been compromised by the attacker. In order to solve such a crime, law enforcement needs to collect the electronic evidence that is left on the zombie computers. As a result, evidence collection by law enforcement agencies may mean the disruption of legitimate services conducted by those businesses whose computers were unknowingly involved in the crime.

Of course, the decision as to the admissibility of evidence occurs after the electronic evidence, along with the equipment in which it resides, has been seized, and evidence is collected and summarized. The process of developing electronic evidence is likely to occur both at the crime scene and at the laboratory where the equipment may be taken for analysis.

After seizure, electronic evidence must not be contaminated by mishandling or accidental destruction. Electronic documents can be contaminated or destroyed more easily than it was ever possible with paper records. For example, simply turning off or pulling the plug on a computer can destroy electronic documents that may be needed for the investigation. In addition, such actions can destroy legitimate business records owned by organizations who are not a party to the investigation. Thus, it is very important for cautions to be exercised as electronic evidence is collected.

Such cautions include:

- Closing phone line connections to the modem. Live modem connections allow for the remote removal of data to another location over a network.

- Videotaping and labeling all connections and cables so that equipment can be successfully reconnected at the lab, and possibly, later returned to legitimate businesses without damage.
- Not turning on seized electronic equipment without checking with a forensics expert. Boot up procedures may be booby trapped. Without entering the correct password or sequence of key strokes, all data may be automatically erased along with remotely stored backups.
- Reviewing all files in a bit-stream or “read only” mode to legally ensure that no testimony would indicate that alterations could have been made to the evidence and taint it. A recorded chain of custody should be kept and signed by all parties, reviewing verified copies with the original copy sealed.

All these practices create potential losses for legitimate businesses using servers, routers, and other electronic equipment that criminal elements may also be using. In addition, unknowingly and without their cooperation, legitimate businesses can become an integral part of an attack on a targeted organization. Consequently, legitimate businesses may find that their operations are disrupted, curtailed or closed as electronic evidence is seized, searched, and collected. Such businesses may only be able to hope that in the process their own data and systems are not destroyed or altered by law enforcement agencies. Financial losses due to such activities may or may not be recoverable.

Civil Cases: Electronic evidence also plays a key role in civil cases. Usually, parties to civil litigation are required to produce electronic docu-

ments under discovery procedures rather than having it seized by marshals.⁸ Still, financial losses for businesses can be just as great in civil cases as in criminal proceedings when discovery procedures are handled incorrectly or when attempts are made to alter or destroy electronic documents.

In civil procedures, parties to the legal action need to be put on notice that discovery procedures are underway. This is done with a letter of notice. Discovery includes depositions, requests for documents, and interrogatories, for example. It also should include a court order to prevent the spoliation of electronic evidence.⁹ If electronic evidence is destroyed or altered after notification, it can result in court sanctions, fines, and finding parties in default of discovery rules.¹⁰

For example, it is common practice for corporations to rotate their backup computer tapes. Following this practice, tapes used for backups of data are only stored for a limited time after which they are used again to record data and erase previously recorded data. Once discovery notification has been received, such normal business procedures need to be stopped and hard drives may need to be mirror imaged, otherwise the offending party is essentially destroying electronic evidence and in violation of court orders. Companies have had to pay large court fines and reached unfavorable settlements with plaintiff’s

⁸ In civil proceedings, Federal Rules of Civil Procedure 34(a) relate to the discovery of electronic evidence or “digital data.”

⁹ Spoliation is the intentional destruction or alteration of any documents requested under discovery procedures.

¹⁰ 995 F.2d 1376 (7th Cir. 1993) and 593 F. Supp. 1443 (C.D. Cal. 1984).

attorneys because of their intended or unintended actions toward such evidence (Rubenstein, 1997, Jessen 1997, and Spiva & Jacobs, 1999).

In civil proceedings, depositions of IT personnel can be used to learn about the architecture of the system from which electronic information is being sought.¹¹ When depositions, document requests, and interrogatories are considered to be produced in a defective manner, the court can order forensic computer experts to search an organization's computer systems. Most computer systems save whatever has been typed on a computer screen somewhere on the Internet, on the hard drive or within the intranet – even if the writer “deleted” the document.

Consequently, altered or supposedly deleted e-mails and documents have begun to play an important role in civil cases. Original copies of these documents are being recovered from locations on the network unknown to the individual who tried to delete the document or change it. These recovered documents are having profound effects on courtroom proceedings (Sterner, 2000).

Currently, free software is available for downloading and testing from the Internet that is advertised as having the ability to defeat forensics search software used to collect electronic evidence. It is called Evidence Eliminator, and it

¹¹ Prior to collecting electronic evidence in either civil or criminal cases, it is important to determine the structure of the network from which evidence is being sought. A network profile should be developed that includes, for example, information about hardware, software, off-site storage methods, Internet connections, web servers used, policies for duplicating and erasing electronic data, and skills of the personnel maintaining the system.

will delete sensitive information from deep within a hard drive on a daily basis. For example, it will delete the history of programs run on your computer, the network computers and files you have searched, media play files, last visited Web locations from cache, cookies, e-mail histories kept by several mail applications, Internet logs in zone alarm as well as other information (<http://www.evidence-eliminator.com/>). Such software provides an easy means of eliminating information about your computer activities and Internet use, i.e., electronic evidence. Using such software can be part of normal business operations and any activity simply based on its use should not be considered illegal.

Where is that Electronic Evidence Kept?

Evidence Eliminator may be a useful product for ensuring that possible sources of electronic evidence are removed from an individual PC, but it cannot be assumed that all such evidence has been eliminated because of duplication that occurs when a computer is part of a larger network. Electronic messages are sent through an expanse of routers and servers. Along this path information such as access times, who wrote and who last modified a file, the computer used to access the system, the message itself, sequence numbers and IP addresses are logged, along with any digital signatures.¹² Electronic evidence is collected on servers and routers through which information passes before reaching the designat-

¹² A server is used for storing programs and files that may be shared across the network. Viewed essentially as a remote disk drive, geographically it can be located anywhere. A router forwards data between two different networks. A digital signature is a means to sign a digital document using encryption. While the message can be opened with the sender's publicly available key, the identity of the sender is verified since only the sender could encrypt the original message.

ed recipient. If this information is unencrypted, anyone can read it. All transmission information and copies of messages and documents may be retained long after the recipient deleted the message from their PC.¹³

Other sources of electronic information are chat rooms and bulletin boards. These sites are places for groups to meet and exchange information. Information such as documents, executable programs, and photographs may be stored at a bulletin board site. Bulletin boards can be located in any jurisdiction in the world where there are phone lines. Investigations have used scanning software to search chat room logs and bulletin board discussions for leads in recent DDOS investigations. Without encryption, these messages are open for anyone to read.

Additionally, information can be stored on devices connected to a PC. For example, a laser printer may retain copies of the last page printed in its internal memory or the laser printer may have software that uses the hard drive within the PC for storage and the message is retained there. E-mails printed on such peripheral devices may be obtainable even though the printed copy has been destroyed and the hard drive completely swiped clean.

¹³ Recently, SafeMessage (www.safemessage.com), Disappearing E-mail (www.disappearing.com), and Hush Mail (www.hushmail.com) have begun providing a direct messaging service that transmits encrypted e-mail directly between parties without a central server to help ensure that servers at intermediate locations are not keeping copies of the e-mail message. Some of these new applications also allow e-mail to "self-destruct" after a set time with no record being kept on the receiver's hard drive. These applications have the potential to frustrate or avoid the conventional audit trail that exists in most standard networked systems.

Johnson (1997) identifies electronic data as available in either active, inactive, archival, or residual formats. Active data is data that is used and changed on a daily basis such as calendaring applications. Inactive data is electronic data that PC users may not be aware is stored on the hard drives such as timed backups that have not been removed. Some word processing programs will automatically make and retain timed back ups of files. Archival data is data that has been purposefully backed up. This data may be on tapes or CDs stored in a safe location with additional backups stored off-site. Backups may be made two or three times on one IT shift. The policy for retaining such data can vary, but it could exist for several years as off-site information held as a CD. Individuals may use a zip drive to store archival data. Archival data can contain rich sources of information for discovery purposes and in criminal cases. Residual data is data that is in the swap files or "deleted files" on a PC that has not been overwritten or in the buffer memory on peripherals such as faxes and printers. A computer user working on one document usually creates various versions of the same document within the same PC and its peripherals so that the deletion of one version does not delete the older versions. When discovery motions are begun in civil proceedings, all the normal deletion procedures for all the various backups of requested information must be curtailed to prevent electronic evidence from being destroyed. In criminal proceedings, attempts will be made to seize this information and possibly the equipment on which it is stored.

Even when electronic tapes are reused or hard drives are overwritten, the information may still be available for collection. Magnetic force microscopy is an expensive technique that can be

used to recover information on a magnetic tape or hard drive that has been overwritten (Gutmann, 1996). The use of this recovery technique makes it difficult to ever delete information from a magnetic tape. For example, deviations of the drive head from the original track made in recording the information on the disk may make portions of the previous track of information recoverable. Inconsistent circuit frequencies used in rewriting the disk may also result in recoverable information. To prevent recovery of information on a magnetic medium, the rewrite has to be performed using lower than normal circuit frequencies, deep drive head penetration on the disk, and random passes before and after the erasure process to confound the reconstruction. Circumventing recovery from magnetic media can also be attempted with costly magnetic equipment that will neutralize the magnetic field on the disks or tapes.

Assurances that it is impossible to recover information from magnetic media is important to legitimate businesses that discard their old PCs, servers, and routers to the trash heap and later find that business secrets and confidential information have not been deleted from their discarded equipment.

Summary

Organizations need policies in place to determine how their electronic data is to be handled. These electronic management plans need to be written before discovery motions are issued in civil proceedings or before a company's legitimate activities become indirectly swept into a criminal investigation. Without clear policies and procedures in place regarding data destruction, data retention, and data recovery, these organizations

are placing their organizational assets in jeopardy. In developing such plans, it is necessary to know or quickly identify the type and location of active, inactive, archival, or residual data so that current policies and procedures for storing sensitive information may be implemented.¹⁴

Furthermore, electronic management plans need to provide training for employees so that there is a clear understanding about the underlying nature of electronic documents, especially e-mail. Employees need to grasp the basic dynamics of recovery procedures for electronic data. They need to realize that such data may exist long after they have deleted it from their PC's applications.

¹⁴The strong need for recovery of data from corporate files without disrupting business operations, and the need to show the court that proper and good faith discovery procedures are followed, has led to the development of new software programs. CaptureIt, a product of Ontrack (www.ontrack.com), for example, allows organizations to capture and save electronic evidence to meet discovery requirements without incurring the high costs involved in shutting down parts of the company's IT operations.

REFERENCES

- Computer Crime: Criminal Justice Resources Manual 2*. (1989). United States Department of Justice, Washington, DC.
- Gutmann, P. (1996). *Secure Deletion of Data from Magnetic and Solid-State Memory. Sixth USENIX Security Symposium Proceedings*. San Jose, CA.
- The Information Technology Age: Evidential Matter in the Electronic Environment*. (1997). AICPA, NY.

- Jessen, J. (1997). The perils of disk-covery. *Electronic Perspectives*, 22(6), 48.
- Johnson, G. (1997/1998). Symposium: Emerging Technologies and the Law: Practitioner's Overview of Digital Discovery. *Gonzaga Law Review*, 33,347-363.
- SAS No. 80, Amendment to SAS No. 31, Evidential Matter (1996). AICPA, NY.
- Rubenstein, B. (1997). Somebody Destroyed the Evidence. *Corporate Legal Times*, 7(70), 6.
- Spiva B. and Jacobs, J. (1999). Reducing Risks Posed by Electronic Records. *Association Management*, 51(5), 111.
- Stern, T. (2000). Computer Forensics – a Trail of Evidence. *Business Credit*, 102(1), 8.

OTHER SUGGESTED READINGS:

- Best Practices for Seizing Electronic Evidence. (2000). http://www.treas.gov/usss/index.htm?electronic_evidence.htm&1 United States Secret Service, Washington, DC.
- *Conducting Searches in a Computer Environment*. (1997). Federal Bureau of Investigation, Washington, DC.
- *Federal Guidelines for Searching and Seizing Computers*. (1994). United States Department of Justice, Washington, DC
- *Supplement to Federal Guidelines for Searching and Seizing Computers*. (1997). United States Department of Justice, Washington, DC.

Reprinted with permission from:

***Journal of Forensic Accounting* ISSN 1524-5586**

A semiannual publication with approximately 125 pages per issue

- Please send sample copy for subscription consideration (enclose \$10.00 S & H)
- Please enter our institutional subscription (enclose \$239.00 per volume year)
- Please enter my individual subscription (enclose \$119.00 per volume year; payable by personal check and dispatched to personal residence only)

Name: _____

Address: _____

Prepayment required for all orders. Send to: R.T. Edwards, Inc., P.O. Box 27388, Philadelphia, PA 19118

For questions, comments, or customers desiring to use a credit card, please call 215.233.5046.

Visit the *Journal of Forensic Accounting* website: <http://www.rtedwards.com/journals/JFA/>

Disclaimer: The work contained within this reprint is not an attempt to render accounting, legal, or other professional services and must not be relied upon as such. If such services are required, the assistance of an appropriate professional should be sought.