

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.

G. Stevenson Smith is Professor of Accounting at West Virginia University, Morgantown, WV USA.