

Computer Forensics: Helping to Achieve the Auditor's Fraud Mission?

G. Stevenson Smith

West Virginia University, Morgantown, WV USA

Auditors are more responsible for detecting fraud today than they ever have been in the recent past, and many fraudulent transactions are found hidden in the recesses of a computer or network. Therefore, it is important for the auditing profession to consider the roles of the computer forensic specialist so digital data is not destroyed for forensic purposes. Without a doubt, collecting digital data can help in performing today's more fraud-oriented audit. As a fraud investigation can hinge on electronic evidence, it is important for these two professions – auditing and computer forensics – to assist one another in collecting and using digital evidence. Without such cooperation, digital data tested during an audit may be forensically unusable. This article reviews the relationship between the use of digital data by auditors and computer forensics specialists. There is a conflict in the use of such electronic data, and the article suggests how training can be used to improve this problem.

Today, almost every financial fraud incorporates the use of a computer and digital documents whether the fraud is falsifying invoices or electronic money laundering. Consequently, electronic evidence of the crime is contained on employer-owned personal computers (PC) and mainframes, employee's personal PCs, the company's network, personal data assistants, disk sticks, floppy disks, smart cards, and on web servers in external networks.¹ Such electronic evidence easily and unintentionally can be destroyed or made inadmissible as courtroom evidence by the actions of those who first find the evidence and are uninformed as to how such data should be handled. Further, electronic evidence is likely to vanish more quickly than any paper evidence. For example, original paper documents can be copied and used in court, but when original digital files are copied, they are essentially destroyed for evidentiary purposes.²

¹ In 2002, Ernst & Young's fraud survey of directors and managers of large organizations across the world found that slightly more than half the respondents to the survey were concerned with computer crime and corruption. Yet in only 5% of reported frauds was electronic evidence used in the investigation. It is surmised that one possible reason for the low level use of digital evidence is because "investigation competencies have not yet moved to match this new source of evidence." (Savage 2002, p. 12)