Computer Forensics—From Cottage Industry to Standard Practice

By John M. Patzakis

The scenario is all too common. Corporate security, suspecting that an employee is misappropriating company trade secrets, summons one of the resident computer experts to scour the employee’s hard drive for the smoking gun without regard to proper computer forensic protocol. Internal investigations involving the examination of computer media for evidence relevant to an intrusion, intellectual property theft or other insider misconduct are frequent within the information systems security field. However, the recruited investigators do not always conduct such investigations in a completely non-invasive and forensically proper manner. The resident computer expert may well find the evidence, but will likely trample all over the electronic crime scene in the process.

If an intrusion or internal computer investigation leads to litigation or a referral to law enforcement, the evidence likely will not hold up in court unless proper computer forensic tools and procedures are employed. Further, if the company’s IS team or hired consultant who initially responds to a computer incident cannot establish the integrity of computer evidence at issue, law enforcement likely will decline any request for prosecution. For these reasons, employing proper computer forensic tools and procedures is essential.

Computer forensics is commonly defined as the collection, preservation, analysis and court presentation of computer-related evidence. The proper seizure and analysis of computer evidence is important in any investigation where a computer is the means or an instrument of a crime or other offense or may contain evidence relevant to an investigation.

The US Federal Bureau of Investigation reports that incidents of computer-related security breaches have increased by almost 250 percent in the last two years. Financial losses stemming from intellectual property theft and assorted computer crimes are estimated at US $250 billion for 1997 alone.

Further, while distributed denial-of-service attacks and other intrusions from the cracker community grab headlines, industry surveys reveal that over 70 percent of intrusion incidents are actually the work of an insider. This statistic does not include the purely internal incidents involving various forms of employee theft and malfeasance. The rising tide of computer-related intellectual property theft, security breaches and associated financial losses mandates that IS administrators conduct or oversee proper computer forensic investigations when responding to these incidents.

The most important tool for a computer forensic investigator is the software used to perform the investigation. Without specially designed computer forensic software, there cannot be a true forensic analysis. In general, there are three primary reasons why specialized computer forensic software must be employed in order to conduct a proper computer investigation:

1) To preserve and properly acquire the evidence

Electronic evidence is fragile by nature and easily can be altered or erased without proper handling. Merely booting a subject computer to a Windows environment will alter critical date stamps and erase data contained in temporary files. Specialized computer forensic software, such as EnCase, employs a boot process that ensures the data on the subject computer are not altered in any way.

After the boot procedure is initiated, the examiner utilizes the forensic software to create a complete mirror image copy or exact snapshot of the target hard drive and all other external media, such as floppy or zip disks, which are subject to the investigation. This evidentiary image must be a complete, but non-invasive, sector-by-sector copy of all data contained on the target media in order to recover all active, deleted and otherwise unallocated data, including often critical file slack, clipboards, printer spooler information, swap files and data contained or even hidden in bad sectors or clusters. This process allows the examiner to freeze time by having a complete snapshot of the subject drive at the time of acquisition.

After the mirror image copy is created, computer forensic software will mount the mirror image as a read-only drive, thus allowing the examiner to
2) To authenticate the data for presentation in court

Computer forensics is based largely on the premise that the data recovered from computer systems ultimately will be presented in a court of law. As such, another important feature of computer forensic software is a verification process that establishes that the examiner did not corrupt or tamper with the subject evidence at any time in the course of the investigation. This is a particularly important step, as courts will accept duplicated computer data only if the data are demonstrated to be an accurate copy of the original computer data. Gathering computer evidence by employing proper forensic tools and techniques is the best means to establish the integrity of the recovered data.

Computer forensic examiners rely upon software that utilizes a standard algorithm to generate a hash value, which calculates a unique numerical value based upon the exact contents contained in the evidentiary mirror image copy. If one bit of datum on the acquired evidentiary bit-stream image changes, even by adding a single space of text or changing the case of a single character, this value changes.

The most common hashing process utilized is the MD5 (Message Digest Number 5), which is based on a publicly available algorithm developed by RSA Security. The MD5 value for a file is a 128-bit value similar to a checksum. Its additional length (conventional checksums usually are either 16 or 32 bits) means that the possibility of a different file having the same MD5 value is drastically reduced. In fact, the odds of two computer files or two mirror images of drives with different contents having the same MD5 hash value is roughly ten raised to the 38th power. If one were to write that number, it would be a one followed by 38 zeros. By contrast, one trillion is one followed by only twelve zeros. The MD5 hash function allows the examiner to effectively and confidently stand by the integrity of the data in court.

A IS administrator should approach every computer investigation with the assumption that the mirror image of the target-computers ultimately will be turned over to company lawyers or law enforcement for civil litigation or criminal prosecution purposes. The creation of a mirror image that is verified and authenticated pursuant to proper computer forensic protocol is essential to ensure a smooth transition from the response stage of the investigation to the enforcement or litigation process.

3) To recover all available data, including deleted files

In addition to the active data normally seen by the computer user, computer forensic software allows the examiner to recover all deleted files that have not been completely overwritten, as well as other forms of unallocated or temporary data. Information contained in swap files, printer spooler files, file slack and other temporary or buffer files are examples of data residing on a computer drive that are not normally visible to the user. As noted previously, this information must be recovered non-invasively.

Additionally, successful computer forensic investigations often depend on advanced techniques, such as recovering temporary files from unallocated clusters or locating and decoding Windows artifacts such as recycle bin info files, metafiles and base64 files. Advanced computer forensic tools are designed to extract this information, allowing the investigator to conduct a complete and thorough investigation. Perhaps more importantly, more advanced computer forensic software will identify and document the exact location on the original drive from which the investigator recovered the evidence.

Recent Advancements in Computer Forensic Tools

The latest generation of Windows-based tools has redefined the field of computer forensics. Prior to the recent development of integrated tools with a graphic user interface, forensic investigators toiled with various procedures that required numerous non-integrated DOS-based utilities in a process that was inefficient, costly, burdensome and often incomplete and inaccurate. Under the old methodology, examiners often spent weeks examining a standard FAT 16, 600 MB hard drive, while missing critical pieces of evidence in the process or, in the case of law enforcement, failing to meet warrant time limitations in searching and seizing computers, resulting in the exclusion of evidence in some situations. One industry expert in 1998 suggested that companies consider not bothering with the process, noting, "When people hear about computer forensics, they think it sounds like fun... In fact, it is a lot of work." So much work, in fact, that any benefit gained from a proper forensic investigation often could not justify the extensive time and resources burned in the process.

Viewed by many CIOs and other IS managers as impractical and costly, market forces relegated the practice of computer forensics in the private sector to a relatively small group of consultants. However, with the advent of improved, integrated and more automated software, the private sector is now widely adopting computer forensics, as there now exists a mechanism to conduct effective and efficient computer forensic examinations.

Previous methodologies required extensive training and overall mastery of the DOS operating system. Since the examiner performed the bulk of the examination from the DOS command prompt, the process mandated proficiency in crafting hundreds of arcane DOS commands and switches. The early pioneers of computer forensics believed that forensic examinations should never take place in a Windows environment, as Windows routinely alters data and writes to the hard drive whenever it is used.

However, the latest generation of computer software tools resolves this problem by acquiring the evidence in DOS and then mounting the resulting bit-stream mirror image as a read-only drive. The forensic software, not the operating system, then reconstructs the file system of the acquired drive by reading the logical data on the mirror image backup, thus allowing the examiner to view, sort and analyze the data through a
Windows graphic user interface in a completely non-invasive manner.

Additionally, all the necessary tools and functions are integrated into one application, further streamlining the investigation process and allowing the examiner to multitask, manage the evidence more effectively and build a case. The new generation of forensic software is expanding the practice of computer forensics by providing a powerful yet user-friendly solution that allows for comprehensive and dramatically more efficient investigations by reasonably skilled IS professionals.

Computer investigations in some form routinely take place at any typical Fortune 1000 company. As such, it is incumbent upon IS managers to ensure that their auditors employ proper forensic tools and techniques in the course of these investigations. Fortunately, with the advent of a new generation of computer forensic software, the implementation of proper forensic investigation practice and protocol is both technically feasible and cost-efficient.

Endnotes

1 Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90 (D.C. Col., 1996) is a particularly important published court decision in this area, in which the court ruled that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."

2 "Evidence Compromised in Credit Card Theft Case," by Mike Brunker and Bob Sullivan, MSNBC.COM, 8 June, 2000, reports on a recent high-profile case where a law enforcement agency declined to pursue an investigation due to a failure to protect the integrity of the electronic evidence in question.


5 Federal Rule of Evidence 1001(3), (28 U.S.C.A. section 1001(3))


John M. Patzakis

is general counsel to Guidance Software, Inc., developer of a computer forensic software tool, EnCase (www.encase.com). Patzakis is a member of the High Technology Crime Investigators Association (HTCIA) and California State Bar. He regularly presents and publishes articles on legal issues pertaining to computer forensics and EnCase software.