Computer Forensics Emerges as an Integral Component of an Enterprise Information Assurance Program

By Douglas Barbin, CISSP, CPA, CFE, and John Patzakis

Imagine restricting an internal company audit or investigation to allow the review of only 10 percent of all documents relevant to that investigation. As recent university studies reveal,1 more than 90 percent of all information is now created in digital form. Therefore, when company auditors ignore computer evidence, they essentially limit themselves to 10 percent of the available information. For this reason, the burgeoning practice of computer forensics has become synonymous with computer investigations and audits.

Computer forensics is the collection, preservation, analysis and court presentation of computer-related evidence. In addition to civil and criminal jury trials, computer evidence often is presented in arbitration, administrative and mediation proceedings, congressional/government hearings and presentations to corporate management. Accordingly, the proper collection and analysis of computer evidence through accepted computer forensic protocols is a critical component to any internal investigation or audit where the results have at least the potential to be presented in legal proceedings.

Computer forensics ensures the preservation and authentication of computer data, which are fragile by nature and easily can be altered, erased or subject to claims of tampering without proper handling. Improperly handled computer evidence is likely to be excluded or limited by the trial court.2 Additionally, computer forensics facilitates the recovery of deleted files and many other forms of compelling information normally invisible to the user and provides an expedient means to sift through hundreds of gigabytes of data to recover targeted information.

Computer forensics is making an important transition from a “black art,” relegated to a select few experts, to a requisite component of the information security enterprise. A major factor fueling the recent revolution in computer forensics is the latest generation of highly efficient computer forensics software. In addition to preserving and authenticating computer evidence, investigators now are able to effectively search, document and manage large volumes of computer data, allowing for the implementation of computer forensics as a feasible and standard practice.

How Computer Forensics Software Works

Computer forensics software serves as the best means to recover all available computer evidence, including the deleted files and temporary data and file fragments that are not normally visible to the user, while preserving and authenticating the evidence with a documented chain of custody. Computer forensic software performs these functions by creating a complete but non-invasive sector-by-sector physical image backup of all data contained on the target computer media. This process allows the examiner to “freeze time” through a complete snapshot of the subject drive at the time of acquisition.

After the disk image is created, the latest generation of computer forensic software will mount the disk image as a read-only drive and reconstruct the file system by reading the logical data at the disk level, instead of querying the resident operating system as other software does. This allows the examiner to search and examine the contents of the drive in a Windows GUI in a completely non-invasive manner and view the drive from a Windows Explorer-type view (with the added presentation of deleted files and folders), while drilling down to the sector level. This process is essentially the only practical means of searching and analyzing computer files without altering date stamps or other information. Often times, a file date stamp (file creation date, last modified or last accessed) is a critical piece of evidence that may weigh in the balance of a dispute.

This process also enables the effective management and analysis of large volumes of computer data. Importantly, dozens of analysis tools and functions are integrated into one application, further streamlining the investigation process and allowing the examiner to multitask, run several concurrent threads, and build a case. Additionally, several drive images, often totaling hundreds of gigabytes of data, can be concurrently searched and analyzed.

Case Examples

Computer forensics has played a central role in many recent cases and investigations. The following are some notable case studies that drive home the critical objectives of computer forensics.

Cooking the Books

A business unit of a Fortune 500 conglomerate had been accused of fraudulent financial reporting. Forensic accountants, the masters of transaction reconstruction and accounting analytics, were brought in.

Their investigation hit a roadblock when a trip to the controller’s office yielded worksheets, journals and ledgers that were all in electronic form and were created over a two-year...
period. Enter the computer forensic specialists.

Tasked with identifying all documents and spreadsheets that would help the accountants reconstruct the events, a targeted search with automated forensic analysis software made the computer forensic experts’ job much easier. As it later turned out, an order was given by managers within the company to erase such materials. Upon examination of all the computers in the finance department, two things were clear: not everyone deleted the files as instructed and most of the deleted files were easily recoverable by the computer forensic experts, using tools such as EnCase. In addition, the investigators were able to preview noninvasively the machines of division managers to see if duplicate copies of the documents in question were on the machines.

In the end, the recovered computer information enabled the forensic accountants to reconstruct the events leading to termination and criminal charges against several high-level officials in the organization. The matter was settled prior to trial.

Foiled Corporate Espionage

After a senior member of a company’s sales team accepted a lucrative offer from a competitor, he began plotting his transition. In violation of noncompete and nondisclosure provisions in his employment contract, the manager transmitted copies of customer lists, marketing plans and other trade secret information to his home e-mail account. A computer forensic analysis of the work hard drive by outside experts enabled an expedient reconstruction of the events, while maintaining the integrity of the data. The examination particularly focused on the systems security logs, the Windows 2000 profiles, file access times and other metadata associated with the files in question.

The manager’s aggressive defense lawyers raised several defenses, including claims that evidence may have been planted or that other employees may have accessed the subject’s computer.

It was discovered that the director of human resources had accessed the employee’s machine, an action which could bring into question the integrity of the evidence. Unfortunately, this occurs quite often in organizations that do not understand the legal risks involved in such actions.

However, forensic analysis was able to assist on this front as well. The investigators were able to retrace and establish what the rogue director did, while successfully identifying and isolating all of the files that the HR director had accessed.

Floppy Disk Ballistics

The case of United States v. Dean is a notable and publicly reported case where the defendant, accused of possessing child pornography on floppy disks, denied accessing the illegal images in question. However, a forensic examination of the defendant’s hard drive (which the defendant did admit using) by a federal agent revealed several temporary and normally invisible link files pointing to the exact floppy disk image files in question. This information was among other key evidence resulting in the defendant’s conviction. Link files are only one of many types of hidden temporary files generated by the operating system that skilled computer forensic examiners focus on as important clues, which often are determinative evidence in many investigations.

The Internal Hacker

An employee hacked into the company e-mail system and erased the accounts of key executives. In addition, an anonymous note had been sent to the entire company with passwords of key individuals. A computer forensics team was dispatched to the client site. Network forensic analysis and event-correlation of e-mail and VPN logs pointed towards an unsuspected (and unsuspecting) employee.

The employee initially stated that he had no idea how such activity could have occurred. A computer forensics analysis of this systems administrator’s hard drive uncovered hacking tools, evidence of hacker web site browsing, and a deleted 10PHL password cracking output file with password lists for the company. Those passwords matched the list of passwords sent anonymously via e-mail. Upon being presented with this evidence, the employee confessed to the attacks.

Lessons Learned

There Almost Always Is a Clue Somewhere

Distributed computing environments are just that. They are designed to facilitate information sharing. Accordingly, what is thought to have been stored on a central file server often is stored in various forms on employee hard drives and other locations. In addition, conventional file deletion techniques often leave vast amounts of ambient data, if not the entire file for reconstruction. In the case of “Cooking the Books,” investigators found key files on multiple machines in the finance department. Some were active, some were deleted, but most were recoverable.

“Floppy Disk Ballistics” showed that even accessing files not resident on the hard drive can leave traces of data, and that such traces are often critical clues. Finally, “The Internal Hacker” showed us that deleted data, output files and Internet usage data are very much recoverable.

The Devil Is in the Detail

It can be said that an investigation is not “closed” by the establishment of the facts, but in the disproving of the defenses asserted against such facts. When confronted with the incriminating computer evidence implicating an investigation subject, claims of ignorance of such activity are not uncommon. A proper computer forensics analysis often is essential to refute such claims.

In the case of “Foiled Corporate Espionage,” opposing counsel raised several defenses to the facts raised. Forensics was used once again to counter these defenses and further strengthen the case. “Floppy Disk Ballistics” tied images on floppy disks to the employee’s machine, virtually sealing a conviction. Finally, in the case of “The Internal Hacker,” the suspect employee was identified through system log analysis,
but it was the system forensics that closed the case and forced the employee’s confession.

As computer technology advances, it is important that computer forensic tools and techniques keep pace. Many software applications now feature advanced analytical functions that help extract the finest points of information from very large volumes of computer data. Newer techniques include the ability to conduct powerful forensic examinations over a local or even a wide area network.

Efficiency Matters

Computer investigations in some form routinely take place at any typical Fortune 1000 company. Law enforcement is often afforded (or perceived to be afforded) the luxury of unlimited time and extended deadlines. In the private sector, investigations cost money and the law of diminishing returns applies in full. Accordingly, forensic examiners must aim to work smarter without compromising quality and integrity.

Fortunately, with the advent of a new generation of computer forensic software, the implementation of proper forensic investigation practice and protocol is technically feasible and cost efficient:

In the case of “Cooking the Books,” investigators had approximately 40 machines in which the key documents could be located. Using computer forensic tools enabled an expedient yet noninvasive examination that quickly identified the key files in question, many of which had been deleted. In the case of “The Internal Hacker,” the investigators had to address the reality that the longer they investigated the longer the organization faced an additional security risk. In both cases, the team used modern forensic tools that provided a substantially automated process—in contrast to what was previously done manually with numerous nonintegrated command-line tools—thus saving countless hours and costs.

A Matter of Policy and Awareness

Many corporate legal counsels are working with the IT staff and auditors to implement policies that take advantage of new computer forensics capabilities. At one Fortune 500 company, for instance, an employee’s hard drive is imaged upon resignation, termination or internal transfer as a matter of standard procedure. The images then are archived to CD-ROM disks should an examination need to take place at a later date. Preserving and archiving these images is important, as issues such as theft of trade secrets or intellectual property, harassment and wrongful termination claims often do not surface until months after an employee leaves his or her position, at which point the critical computer evidence has been overwritten.

Future Directions

With supporting technology becoming increasingly powerful and efficient, coupled with increased emphasis on information assurance and security, computer forensics quickly is becoming standard protocol in corporate internal investigations by expanding beyond the realm of specialized, computer incident response teams. As the overwhelming majority of documents are now stored electronically and the completely paperless office seems only a few years away, it is difficult to imagine any type of investigation that does not warrant a computer forensic investigation.

In addition, forensic tools and techniques are being used for many noninvestigative purposes. Examples include data mapping for security and privacy risk assessment, and the search for intellectual property for data protection. Computer forensics is therefore transitioning from an investigation and response mechanism to one of prevention, compliance and assurance.

With organizations incurring excessive losses of intellectual property and other trade secrets, advancements in computer forensics technology are meeting the compelling need to counter this threat. With this improved technology and infrastructure, ongoing and proactive computer investigations are now a mandatory component of the information assurance enterprise.

Endnotes

1 A recent University of California, Berkeley (USA) study indicates that “[o]ver 93 percent of the information produced in 1999 was in digital format,” and “[c]omputer forensics is necessary to address the reality that the longer they investigated the longer the organization faced an additional security risk” (The Internal Hacker).


Douglas Barbin, CISSP, CPA, CFE
is a principal consultant and service leader for Incident Management and Forensics with Guardent Inc., a managed security services and consulting firm. He can be reached at doug.barbin@guardent.com.

John M. Patzakis
is president and general counsel to Guidance Software, Inc. (www.encase.com), the developer of the computer forensic software tool, EnCase. He can be reached at john.patzakis@encase.com.

© 2002 Guidance Software Inc.