

Computer Forensic Investigations Require The Skills Of Trained E-Discovery Specialists

By Stephen P. Tarr

When it comes to white-collar crime these days, the answer to the age-old question, “Whodunit?” is frequently being discovered in a series of zeroes and ones. E-mail correspondence, computer documentation, and electronic files of all sorts leave an indelible trail of clues that—more often than not—tip the balance in contentious corporate lawsuits.

This means that the emerging field of computer forensics—the collection, preservation, analysis and presentation of computer-related evidence—will only grow in importance. Without exception, investigations involving the search for electronic evidence demand that companies rely upon sophisticated techniques employed by experts with specialized IT training because evidence retrieved or collected in an inappropriate manner may have highly adverse effects on the outcome of litigation. Data that appear to have been altered or damaged, for instance, may be ruled inadmissible—thereby undercutting a company’s defense against wrongdoing, or rendering useless vital information that might lead to judgments against guilty parties. In fact, to ensure they produce documents of unimpeachable integrity, most companies turn to technology partners that specialize in computer forensics.

E-Discovery Mistakes Can Be Costly

One doesn’t have to look far to see proof of the importance of irreplaceable e-discovery. There have been a number of cases in the past few years where the methods used to produce evidence were called into question and, ultimately, had a dramatic effect on the outcome of the litigation:

- ▲ *Zubulake v. UBS Warburg LLC*—a failure to preserve relevant e-mails led, in part, to a \$29 million wrongful termination verdict;
- ▲ *United States v. Philip Morris*—improper handling of electronic documents contributed to a \$2.75 million judgment against Philip Morris;
- ▲ *Coleman Holdings v. Morgan Stanley Co.*—a failure to properly handle electronic documents subject to disclosure proved damaging and led to \$1.5 billion jury verdict;

Electronic technology has forever changed how evidence is produced and viewed by the legal system. Computers make it easy for companies to document, duplicate and distribute great volumes of information. Plus, for good or ill, these systems leave a permanent electronic “paper trail,” so to speak. Even after e-mail correspondence or documents are deleted, they can nonetheless be reconstructed—or, at the very least, experts can uncover indications that they existed at an earlier time. Likewise, today’s technology produces metadata to record information like the date a document was created, modified or deleted, as well as e-mail tracking information like the contents of the to/from/subject lines.

Courts recognize that electronic evidence can be searched easily and so require that it be introduced whenever possible. At the same time, attorneys savvy in computer forensics can spot indications that data has been altered or deleted—and can use such information to discredit evidence. The result: companies have learned to rely upon only the most expert IT professionals to conduct computer forensic investigations.

When conducting such an investigation, experts must consider a multitude of factors: operating and network systems; application and backup software; and data sources that include file servers, storage devices, desktop computers, laptops, PDAs, cache files, temporary files, deleted files, unallocated space, slack space, swap files, system logs, and internet cookies.

Spoilation Of Data Is Major Risk

The very complexity of these searches compounds the risk of error or mishandling of data. The most common hazard affecting computer forensics, for instance, is spoliation of evidence. The legal system holds that individuals and corporations have a duty to preserve evidence that relates to ongoing or imminent litigation. Simply put, this means parties named in lawsuits must be extraordinarily careful not to misplace or destroy relevant information—either intentionally or through negligence—not only during litigation, but from the very moment the party suspects a suit might be brought.

While it seems straightforward enough, corporations are often shocked to learn how easy it is to violate this dictum. The very act of searching a computer, server or network to uncover electronic evidence can alter data unless proper forensic techniques are used. The damage can range from total erasure of critical files, to alteration of metadata that establishes the credibility of the information itself. Even accidental spoliation can occur throughout the e-discovery process—while accessing, copying or compressing files, for example, or while information is being burned to CDs and DVDs.

No matter how innocent, alterations to electronic evidence call the veracity of the data into question. The credibility of the evidence is tainted and, ultimately, it may be ruled inadmissible—which means litigants could be prohibited from producing information that favors or defends their position, or which contributes to a level of suspicion regarding their integrity.

To avoid these problems and ensure that litigants aren’t exposed to additional risk because of faulty computer forensic techniques, leading corporate executives frequently turn to trained professionals to assist. In doing so, they have benefited from three distinct advantages:

1. Computer forensic specialists can actually help avert lawsuits that may have been brought because important data, documents or exculpatory evidence had been destroyed or overlooked during previous litigation.

2. Professionals trained in the intricacies of computer forensics can prevent the loss, destruction or inadvertent alteration of computer evidence (accidental overwriting of a hard drive, for example) during data searches—and, by doing so, can insure the admissibility of this information in court, or at hearings and other proceedings.
3. Experts can ensure that all potential electronic evidence is uncovered. Because of their comprehensive training, they are well versed not only in examining likely data sources (e.g., hard drives and backup systems), but also the less obvious repositories (e.g., internet cookies, cache files and unallocated space).


Trained Specialists Preserve Integrity Of Data

Computer forensics specialists have developed a meticulous set of standards and procedures they employ to insure the integrity of all electronic files they produce. With the specific objective of finding all relevant material, but altering none of it, these professionals typically follow a number of steps:

1. Specialists ensure that the examination in no way violates the integrity of the original media. To this end, computer forensic specialists almost never conduct discovery activities on the original media, but instead image the data, duplicating it to forensically sterile media. If there is indication of residual data on the media to which the original is copied, opposing attorneys can question whether or not the residue could have contaminated the evidence presented.
2. All potentially relevant hardware systems and software applications are examined and the process is thoroughly documented. All examinations are conducted using licensed software. During e-discovery, computer forensic specialists will ensure they have investigated the following elements –
 - ▼ data from original storage device sources
 - ▼ boot record data, and user defined system configuration and operation command files, such as the CONFIG.SYS file and the AUTOEXEC.BAT file
 - ▼ password protected files
 - ▼ user data files in the root directory and each sub-directory (if present)
 - ▼ executable programs of specific interest
3. Besides investigating data currently in existence, experts dig deeper to ensure that all recoverable deleted files have been restored. In addition, they will examine unallocated and slack space for lost or hidden data, if appropriate. They will also check the contents of CMOS and the internal clock for the accuracy of the system date.
4. A listing of all the files contained on the examined media is constructed, and a printout or copy of all apparent evidentiary data is produced. The file or location where any apparent evidentiary data was obtained is noted on each printout. The specialist confirms that all exhibits are marked and sequentially numbered—and that they have been properly secured.
5. The computer forensic professional is also expected to certify the discovery process. A final report, including findings and comments, is produced and properly documented.

Although no corporation looks forward to involvement in litigation or e-discovery activities, it is nonetheless a possibility it must be prepared for. If the situation arises when the skills of a computer forensics examiner are required, companies would be well served to ask the following questions when reviewing a vendor's level of expertise:

- A. Have investigators received specialized and comprehensive computer forensic training from a recognized training school?
- B. Did that training include the use of sound forensic procedures, like those described earlier?
- C. Do the vendor and individual investigators understand "chain of custody" and how to maintain it as it relates to a specific e-discovery project? A legal concept, chain of custody relates to the process used during the handling of all evidence—where it was stored at all times, who had access to it, and if it was kept in a secure environment, for instance. If there are gaps in this chain, opposing attorneys have reason to attack the credibility of the evidence.
- D. Have the investigators assigned to the computer forensic examination received up-to-date training in the use of the most advanced forensic tools, as well as instruction in current techniques for data recovery?

Unfortunately, we operate in a highly litigious society—and the odds are great that most corporations will someday be involved in a lawsuit. In many instances, the field of computer forensics will have an impact on the outcome of these cases. If produced properly, electronic evidence can lead to a successful outcome but, if mishandled, it can have an equally adverse effect. It makes sense for IT leadership to recognize the specialized skills that are required and to be prepared to seek out expert assistance if—and when—the need for computer forensics arises. 

Stephen P. Tarr is a Solutions Analyst with Atlanta-based eMag Solutions, an electronic discovery company specializing in accessing data from a variety of archived sources.