

Computer Forensics for Your Firm

Decrypting e-Discovery's Up-and-Coming Science

By Christy Burke

The electronic-discovery phenomenon is here to stay — and the industry is still exploding.

The percentage of electronically stored information (“ESI”) evidence in the standard case has increased exponentially, and all signs on the Information Superhighway and on roads leading to court indicate that ESI in litigation will escalate as time goes by. Along with e-discovery, the field of computer forensics is becoming evermore central to the discovery process. The need for computer forensics analysis is appearing frequently at the state and federal level, and the field’s influence and demands are permeating civil and criminal cases, both large and small.

Attorney and e-discovery expert Tom O’Connor, with the Washington, DC-based non-profit Legal Electronic Document Institute, says that judges in the cases he consults on are ordering e-discovery and computer-forensics investigation much more frequently than ever before. O’Connor is seeing the effect of this change on all kinds of cases.

“Even a small business has a 20 GB hard drive these days,” he notes. “We can’t think of e-discovery as an issue only relevant to large or complex litigation anymore. Nearly everyone has at least one computer at work and one at home, not to mention a cell phone, PDA, GPS system and wireless Internet connection. With all these potential evidence sources for each individual, it’s no wonder that the amount of electronic evidence to be vetted is skyrocketing.”

O’Connor adds that with large criminal cases, huge amounts of electronic data must be harvested and analyzed. In many instances, suspects’ PCs are immediately seized and “imaged” — a euphemism for *cloned* or *copied* — so that their contents can be examined at a later date without the risk of tampering. This kind of work generally needs to be done by a computer-forensics expert who is trained and qualified to do a professional-caliber job.

Besides the usual information sources of hard drives, server data and e-mails, O’Connor is seeing requests for digital surveillance-camera footage and electronic audio recordings. In many cases, law enforcement provides this e-discovery to the defense on CDs or DVDs in its entirety — hundreds of hours of video consolidated on a few disks that the attorney team then watches and sifts through to find the few segments relevant to the case. Parties on both sides agree that searching for, or finding, a needle in a haystack at \$400 an hour doesn’t serve the attorneys’ or the clients’ purposes very well.

FORENSIC INVESTIGATION IS ALIVE AND WELL

For civil domestic cases such as divorce proceedings, there’s an enormous amount of forensics investigation occurring. O’Connor says that PCs are being examined to prove or refute claims by one spouse that the other has been engaging in extramarital affairs or hiding financial assets. Forensics experts are trained to search for e-mail exchanges in which the parties are setting dates and carrying on other communications. They can also:

- Uncover questionable online purchases;
- Track credit-card transactions; and
- Detect whether credit cards unknown to one spouse are being used to make illicit purchases.

Stephanie Simons Neal, litigation-support project manager in the New York office of Weil Gotshal & Manges LLP, attests to the burgeoning need for forensics expertise at her firm. Simons Neal’s caseload consists of a number of patent cases, along with other corporate-litigation matters.

“We’ve definitely noticed an increase in request for forensics, as well as requests for review and production of documents in native form as opposed to paper,” she says, adding that while the requests continue to come in, the expertise to meet those requests is lacking and there is a growing “disconnect” between what cases actually require and what the law firms are equipped to provide.

Simons Neal comments that she sees many case teams that are concerned about forensic document collection or preservation of metadata, but whose members don’t understand why they need to be concerned about it in the first place. She says that the amended Federal Rules of Civil Procedure that went into effect Dec. 1 have brought issues regarding electronic discovery to the forefront of conversation — mostly in a good way. But there are plenty of legal professionals who

still don't know what that really means — or how it affects them.

Trial attorney and certified computer forensic examiner Craig Ball of Austin, TX, has seen a marked increase in the use of forensically qualified imaging to preserve data prior to litigation rather than in reaction to it.

"Even in those matters where forensic analysis may be deferred, savvy attorneys are taking steps to preserve data of key players to the most rigorous standards," notes Ball, an author and frequent speaker on e-discovery and forensics matters.

He adds the observation that judges are increasingly attuned to forensic issues, and the existence of electronic evidence has made them more likely to entertain requests for forensic preservation and compulsory examination. For instance, law-enforcement personnel often are adept at preserving the chain of custody and other forensic methodologies, but their experience is generally more oriented toward criminal rather than civil cases. Unless they can find a law-enforcement expert with the proper qualifications, lawyers must look elsewhere for resources to preserve pre-litigation data.

Ball cites as an example a recent case that focused on pre-litigation data preservation.

"I promulgated a forensic preservation protocol which was then applied to over 100 machines linked with other key players involved in events giving rise to a contemplated litigation," he explains.

Ball says that this was a preemptive measure, that the images gathered may never be examined, but that their being "locked down" was an effective insurance policy against litigation-compliance errors.

"The imaging was not a stand-alone effort," he continues, "but was part of a broad, concerted effort to preserve potentially relevant data, including server storage areas, e-mail, archival media, voicemail, portable media and, of course, paper."

Christy Burke is a New York City writer who covers law and technology. Reach her at cburke@burke-company.com.

CALLING ALL COMPUTER

FORENSIC EXPERTS

As the demand for computer-forensics examiners goes through the roof, everyone wants a piece of the action — and its business. Law firms and corporate counsel are taking many approaches to tackle the issue, with varying degrees of success. The fact remains that there is still no standardized or official certification process for computer-forensics experts in the United States. Simons Neal, for example, has seen many formerly paper-based vendors (copy shops) hanging out shingles saying that they do computer forensics. She regards these qualifications with some suspicion — any company can claim to do the examinations, but how do you determine which ones actually deliver quality, defensible results?

"They're getting to be a dime a dozen, though that doesn't mean that they know what they're doing or that they have much experience," she says. "It's up to us to figure out the difference between the true experts and the impostors."

That takes some old-fashioned common sense, determination to ask questions and get answers, and follow through on the answers found.

Speaking from his expertise as an attorney and certified computer-forensics specialist, Ball acknowledges the scarcity of qualified vendors from which one can choose. He agrees that when it comes to computer forensics, "lawyers are looking for help anywhere they can find it." Ball cautions that because it's difficult to gauge the qualifications of service providers, lawyers are being poorly served in many cases and need to be on guard. So, the question remains: How can you find a qualified computer-forensics analyst who will provide the thorough and accurate assistance that you need for your case?

Ball recommends looking for a computer-forensics expert that provides formal training and meaningful certification — something with substantial components of practice examination, peer review and experience, like CCE (certified computer examiner) or EnCe (EnCase certified examiner). He also suggests that your expert have:

- A record of published work;
- Respect from peers;
- Considerable court experience;
- Report-writing skills; and
- Extensive focus on the discipline.

Ball emphasizes that forensics is too important and complicated to be a part-time job for an IT person.

Many different approaches exist for meeting the computer-forensics requirements. Also, many EDD vendors claim to have computer-forensics experts on staff, and Ball concedes that a few of these vendors do provide quality service, but that they often enlist the assistance of subcontracted "partners" to do so. He has seen some vendors do little to verify the abilities, experience and other qualifications of these "silent" partners. As the customer, law firms and corporate counsel are well within their rights to ask for the credentials of the person who will actually be doing the examination; otherwise, they are leaving quality control completely to chance.

Ball adds that corporate counsel and law firms sometimes assign forensics projects to their IT staff, ostensibly to save costs and to reduce the exposure risk of hiring an external provider, but these staffers rarely have the proper training to guard the chain of custody.

"Often they use methodologies that have untoward anti-forensic consequences," he says. "Further, when the IT staff is among those implicated in the case, they are basically wolves chosen to guard the hen house."

(For more on e-discovery processes, see, "e-Discovery Best Practices: How Good Is Good Enough?", on page 3.)

LAWYERS TAKING ON THE COMPUTER FORENSICS CHALLENGE

O'Connor chimes in on the danger of lawyers not pursuing e-discovery knowledge: "Lawyers cannot afford to ignore the importance of electronic discovery and computer forensics any more," he warns. "Those who do are bordering on malpractice, especially for cases which involve any digital data component."

Although a small handful of attorneys have accepted the challenge and have chosen to educate themselves on

the technology, Ball says the number of such e-discovery lawyers is tiny.

“We can hold our conventions in a phone booth, so we can make only the tiniest dent in solving the problem,” he says.

He adds, however, that this is changing — that he is seeing more lawyers embrace their responsibility to master e-discovery obligations, and to understand the forensics piece, too.

But Ball concedes that, while some lawyers have developed this in-depth expertise, for all lawyers to take on a computer-forensics role is hardly cost-effective for the client. As a general rule, paying lawyers to do the forensics work for every case is simply not economically feasible. Because the divergent nature of many forensics examinations can lead to upwardly spiraling hours, having an attorney do the work can be cost-prohibitive.

Still, these experts say, this does not absolve the attorney of his or her responsibility to become familiar with the technology; indeed, if for nothing else, legal professionals must inform themselves about the technology so that they can provide competent counsel to clients in the modern courtroom environment. That means that attorneys must understand at least enough about technology, electronic discovery and the computer-forensics process to represent their client’s interests zealously, to evaluate expert-witness testimony and to develop case strategy. They must also be able to explain coherently these forensic search techniques and methods to a judge or jury, or both, because much of today’s evidence is virtual rather than physical.

“Lawyers are still looking for the shortcut to avoid the full brunt of EDD, or they err on the side of unrealistic, oversimplified advice (*i.e.*, “save everything”),” Ball says. “Lawyers need to buckle down and learn to do it right, in a balanced manner where potential relevance is the touchstone.”

PREDICTIONS FOR THE FUTURE

Like it or not, computer forensics is a new but permanent fixture in the world of electronic discovery, but the precise future of this science is uncertain at the moment. For now, many players are boldly planting their flags in the ground to stake their claim to a part of the business.

Simons Neal sums up the vendor situation as she sees it.

“The fever pitch of vendors jumping into the EDD game will probably get more chaotic in the short-term until the cream rises to the top and others fall away,” she notes. “Given the heavy demand for this expertise, the marketplace will be able to sustain a large number of computer forensic providers, but the vendors will have to prove themselves in order to keep the business. They will have ample incentive to control the quality of their forensics product since this is where their future lies.”

O’Connor stresses that legal counsel and corporate America alike need to figure out forensics now. On the high end of the market, this has begun: Big corporations and law firms are aware of it, with some hiring ex-FBI and ex-military personnel trained in the technology to be their in-house security gurus. At the mid-sized and smaller end of the scale, the evolution of forensics will be determined by how different states handle e-discovery cases. O’Connor

predicts that there will be a vast disparity between states — some will be on the forefront and others will lag behind.

Ball sees a common nomenclature (and shortcuts) emerging to describe e-discovery scope and production. Litigants will come to have common expectations regarding preservation and production. Ball also thinks that lawyers will realize that the technologies relied on now — such as keyword searches — are flawed and will remain that way until lawyers improve framing the searches and applying multidimensional search techniques. They will be forced to learn more about the computer-forensics realm so that they can evaluate the information, services, performance and results that they are getting. He adds that attorneys must appreciate that discovery and e-discovery are not disparate undertakings, and to see that case evidence is so ESI-dominated that there truly is no going back now.

Computer forensics is still a young science that is being shaped by the electronic-discovery rules as they continue to evolve and change. This expanding industry simultaneously presents huge opportunities and great responsibility. Lawyers who choose to face the importance of e-discovery and computer forensics sooner rather than later will have a distinct advantage over those who prefer to ignore them or to underestimate their impact.



The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.