

THE CONNECTICUT LAW TRIBUNE

MARCH, 2007 • \$10.00 • WWW.CTLAWTRIBUNE.COM

ALM

Secrets Of The Computer Hard Drive

How computer forensics can help you find the smoking gun in electronic discovery

By **BRIAN C. ROCHE**
and **GERALD C. PIA, JR.**

With the enactment of the 2006 amendments to the Federal Rules of Civil Procedure, litigators are now trying to wrestle with the many significant revisions affecting the discovery of electronic data. While the potential breadth of the rules can seem daunting, some lawyers have become

pany's best customers have reported that they were recently contacted by this employee, who has offered to beat your client's special pricing arrangements on numerous products. The customers naturally expect your client to adjust its prices accordingly in order to continue their business relationship. Based on these facts, it appears that this employee took more than his favorite coffee mug when

Finding The Trail

Computer forensics can generally be defined as the analysis of digital media after a computer security issue has arisen. The goal of this analysis is to determine (1) what exactly happened, and (2) who is responsible for the conduct at issue. Whether your client chooses to utilize an outside firm capable of performing these services or an



There was little doubt that the defendant had copied [our client's trade secrets] to his and/or his new employer's computers, and that electronic discovery would reveal this.



focused on how they can best extract the "smoking gun" from an adversary's electronic materials. But finding the "smoking gun" often starts with an early forensic search of your client's own computers.

Consider the following case study: You represent a company whose primary asset is its intellectual property and trade secret material. The company has advised you that one of its key employees has recently left his position and is now working for a direct competitor. Several of the com-

he left the company—namely, the company's proprietary information and trade secrets.

As a counselor, you need to advise your client on the preliminary steps that it should take as a result of this employee's departure. Obviously, the client needs to conduct an investigation to develop additional facts related to the former employee's misconduct. One primary component of that investigation should be a forensic investigation—that is, an analysis of the former employee's desktop and laptop computers utilized during the course of the individual's employment with the company.

internal IT/security officer, any examination must be performed with eye towards recovering and preserving the integrity of the original data located on the computer or device, and ultimately presenting testimony that will withstand cross-examination.

Many of us now recognize that an individual cannot simply delete information from his computer and expect to permanently remove any trace that it ever existed. Most data that are written to a hard drive or similar media will remain there until they are actually overwritten by additional/new data. Until the "deleted" data are overwritten they will continue to

Brian C. Roche and Gerald C. Pia, Jr. are partners in the law firm of Roche Pia LLC in Shelton.

reside on the hard drive; only the “link” to that data is removed. A useful analogy is to consider the classic card catalog system utilized in your elementary school library when you were a student. If one removed an index card from the card catalog, it did not mean that the book referenced on that card ceased to exist. Only the “link” was removed. One capable of navigating his or her way through the library could still locate the book from the library shelves, unless that book was actually removed from the library and replaced with a new volume.

The benefits of an early forensic analysis can be significant. A successful examination can greatly impact the likelihood of your client’s success at a preliminary injunction hearing, alter the tenor of settlement negotiations, or justify a (sometimes intrusive) forensic analysis of a defendant’s (or even a third party’s) computer system.

Consider the following hypothetical similar to our case study. The departing employee, who had entered into a non-compete and confidentiality agreement with our client, and who indicated that he would be leaving the industry, becomes employed immediately by our client’s direct competitor.

Tell-Tale Signs

After we commenced litigation, the former employee’s attorney consistently repeated the mantra that “the defendant was a good guy” and accused our client of being the “school-yard bully.” Apparently

hoping to hide behind this line of defense, the defendant took unreasonable positions during the parties’ preliminary settlement discussions, suggesting that our client could never prove wrongdoing. Moreover, after receiving a motion for expedited discovery in connection with a preliminary injunction hearing, the defendant’s counsel responded orally that our pursuit was wasteful because “no responsive documents existed.”

Unbeknownst to the defendant at the time, our client had wisely decided to perform an early forensic analysis to assess the employee’s pre-resignation conduct. The results provided us with early signs of the proverbial “smoking gun,” as well as proof that other information – perhaps *the* “smoking gun” existed on the defendant’s and/or his new employer’s computers. The analysis revealed that the former employee had been negotiating for months with his new employer over the specifics of his new opportunity, while still employed with the company. It further demonstrated, through recovered e-mails, that the former employee had gone so far as to divert business opportunities to his potential new employer in an apparent effort to curry favor. Finally, the analysis demonstrated that the employee had connected a USB “flash drive” to his work computer and downloaded suspicious files (which he had attempted to rename and/or delete), in the format in which our client’s confidential trade secrets are kept. There was little doubt that the defendant had copied this

information to his and/or his new employer’s computers, and that electronic discovery would reveal this.

Deflating The Defense

Armed with the results of the forensic examination, we were able to deflate the defendant’s “good guy” defense, warn the defendant that we would seek examinations of the defendant’s and his new employer’s computers and media, and significantly alter the tenor of the settlement negotiations that had begun. Presented with a “taste” of the information recovered during the forensic analysis, the defendant’s counsel became better able to advise his client – and his client’s new employer (whom the attorney also represented) – on the risks posed by the litigation, as well as opine on the extent of the parties’ exposure.

Suffice it to say, this case did not proceed to trial. Indeed, it settled before the anticipated electronic discovery was formally commenced. The defendant’s counsel—like most litigators—was well aware of the potential scope of electronic discovery under the 2006 amendments, especially where, as here, the data recovered by our client would justify an examination of both the defendant’s and his new employer’s computer systems. Because our client’s demands had been reasonable, the end result was a quick and favorable resolution for our client. The moral of the story? The “smoking gun”—or at least a map to it—may be buried within your client’s own computers. Start there. ■