Digging for the Truth: Computer Forensics and Employment Law

by Peter Coons

When I was a lad, I distinctly recall dismantling more than a few household items. Once I took apart my parent's clock radio because I wanted to see how it worked. My parents were less than thrilled as it turned out I was deficient in the putting back together department. Instead of grounding me, my Dad accompanied me to Radio Shack and purchased me a kit that could be used to build a real AM radio. It was very cool and I am thankful my Dad fostered my fervor. I retained that interest and passion for tinkering and channel it daily in my work as a computer forensic examiner.

Computer forensics differs from the traditional eDiscovery process that typically involves the collection and processing of hundreds of gigabytes of electronically stored information ("ESI"). Utilizing forensics allows for the recovery of deleted chat logs or temporary Internet files, items that may prove very useful in an investigation, but not normally accessible through the traditional e-Discovery approach. How are these items useful, you ask? Below I outline two actual employment matters I worked on where the use of computer forensics was instrumental.

Case #1

D4's client, a large chemical company, believed that one of its employees was moonlighting and engaged in trade secret misappropriation. I was asked to forensically image the individual's work laptop and search for any nefarious activities or evidence the individual was running a side business.

Through the use of computer forensics, I uncovered the fact that the individual was indeed running a side business in addition to stealing and selling proprietary technology. I was able to provide information surrounding the individual's use of a third party document collaboration website that hosted our client's proprietary and confidential trade secrets. The individual was also communicating with his co-conspirator and the company he was selling secrets to via Yahoo mail. I was able to recover deleted emails that openly discuss the fact that he knew this information was stolen and emails providing login credentials for the third party collaboration site to the company purchasing the trade secrets.

Once presented with this evidence our client was able to obtain a TRO, which enjoined the individual from purging any potential evidence of his scheme. That same court also permitted for the imaging and review of the individual's home computer, where it was expected we would find additional incriminating evidence.

The forensic examination of the individual's home computer proved even more fruitful. We uncovered hundreds of other e-mails, in addition to attempts by the individual to delete over

2,000 files related to the matter within minutes of his receiving the TRO via an electronic faxing system. That fact was uncovered by recovering deleted temporary Internet files that depicted the individuals Yahoo inbox clearly showing the electronic fax being received.

What was the outcome of this case? The individual was fired of course, and our client, the plaintiff, won a judgment to the tune of $152.7 million.

All of this evidence could only have been identified through the use of specialized software and the right know-how. Without the initial evidence uncovered by computer forensics, there may have been no way to secure a TRO and the ultimate discovery of the extent of the scheme employed by the individual and his co-conspirator.

Case #2

D4 was hired by a small company that had a big problem. Its owner was being accused of sexual harassment by one of its former employees. The owner claimed he was completely innocent and being framed. The company's attorney suggested the owner engage D4 to forensically examine the accuser's work computer. The owner agreed but wasn't much help to us when we wanted to know what we were supposed to look for. He said he wanted us to find something that could prove his innocence.

Since we don't conjure evidence, we proceeded to examine the computer's hard drive. What we found, to the delight of the owner, was very revealing.

Through the use of computer forensics, we were able to uncover portions of deleted "MySpace" chat logs between the accuser and their employees. The accuser not only openly discussed her disdain for the owner, but how she was going to "get him". The accuser was also having an affair with two other people in the office, one of whom was married. We found out all of this information by recovering deleted chat logs. The accuser openly asked for gifts from the individuals she was carrying on with and even threatened the married individual that she would reveal the tryst to the man's wife if he did not buy her an expensive piece of jewelry. This evidence certainly did not speak well of the accuser's character. When confronted with his evidence, the accuser decided to drop the suit immediately.

Without the use of computer forensics, there was a strong possibility this case could have gone much further and ruined the lives of the owner and possibly everyone at the company. Traditional discovery would not have uncovered the deleted chat logs and without computer forensics, no one would have been aware of the accuser's shenanigans.

When to consider using computer forensics in an employment matter: If you can answer YES to any of these questions, then you may want to consider going the forensic route in addition to traditional eDiscovery.

1. Is someone being accused of harassment (sexual or other) in the workplace?
2. Has a key employee left and shown up the next day/week/month at a direct competitor?
3. Is there a belief that an employee is engaged in trade secret misappropriation?
4. Has an employee been accused of violating the company's usage policy (viewing pornography at work, etc.) and you want to verify the accusations prior to taking action?
5. Do you think any useful evidence can be garnered by recovering deleted items or recreating a computer timeline?
6. Is the reputation of the company on the line?
7. Can you call D4 and speak to someone about your situation for some FREE advice? (hint: the answer is YES)