

I Think We Were Sabotaged!

We received a call on a Monday afternoon from an attorney whose client was preparing to go to court for a temporary injunction hearing. The scenario: A competitor had hired away a sales manager and most of his sales team. Over the weekend, the defendants had allegedly entered the office and deleted numerous relevant documents: invoices, orders, client lists and the like. We knew we had little time and a lot of work ahead of us, so we hit the road to pick up six hard drives. After imaging and processing the drives, we were shocked to see that many of the documents were alive and well on the hard drive but the metadata told us that they were all recently created. During a quick conversation with the attorney we were informed that their client's IT administrator had used consumer software to restore the deleted files.

Now let's step back and take a look at how this was possible. We knew that the files in question were deleted over the weekend and the computers had lay dormant until Monday morning. At this time the documents we restored by the IT Admin in an effort to get the remainder of the sales team back up and running. Because the computers had not been used, most of the files that had been deleted were easy for the consumer software to restore. Although this recovery enabled the sales team to resume business, it was detrimental to the looming litigation. Unfortunately, unless the proper tools and techniques are used to restore data, the metadata that allows us to identify the who, what, where and when is altered and we are left with tainted evidence.

Back to the task at hand... We are sitting with tainted evidence and a short time to come up with some value to the attorney and his clients. We were able to recover some files that the admin was unable to restore because they had been partially overwritten by the operating system. This most likely occurred when the computers were started up and the admin was installing software. We were able to corroborate some information with the files we restored. We were also able to restore additional files, which were critical to the client's case. After four days in court the case was settled in the favor of our client. At one point during the trial, opposing counsel realized we were involved and subsequently decided not to put their computer expert on the stand. As their "expert" was a member of their internal IT staff who had no experience with digital forensics, this was a wise decision.

The lesson learned is very simple: When it is possible that a computer crime has taken place, DO NOT call your IT department. Call your attorney so that he can work with digital forensic experts to ensure no spoliation takes place. In this case the admin was just doing his job, however it could have had a very negative impact in litigation. If you were to stumble across a murder scene the first thing to do would be to call the authorities. Computer crime is no different, in the civil setting call your attorney and let him/her sort it out.

The Lorenzi Group is a full service, New England based provider of Digital Forensic Services. We assist clients during the acquisition and imaging, processing, analyzing, and reporting and testifying process of digital evidence management. Born out of an expressed need by attorneys for a reliable and professional digital forensics team, we work with companies and firms across the country bringing them the evidence they need. If you would like to learn more about us, the processes and equipment we use, or how to utilize our services, we would enjoy hearing from you. Please visit our website at www.thelorenzigroup.com. We can be reached directly at 1-866-632-9880 or by email at info@thelorenzigroup.com.