

Destruction of Data

Our team at The Lorenzi Group was arriving onsite at the defendants' place of business to perform a routine collection of evidence from their computer hard drives. The plaintiff's attorney had retained us for what was to be a very typical case: Employee leaves Company A starts working for Company B, bringing with him/her proprietary information such as pricing, client lists, new product ideas, etc. Going in we knew that we would be forensically imaging four hard drives so that we could then perform an analysis of machines. What we did not know was that the defendants were VERY busy deleting everything they didn't want us to see.

What does it mean to "create a forensic image of a hard drive"? A forensic image of a hard drive, or any digital media for that matter, is a bit by bit copy of every 1 and 0 contained on the hard drive. Utilizing specialized hardware and software tools we are able to reconstruct all the data, even data that has been deleted or partially overwritten.

As we walked in, our team was greeted by a nervous employee who escorted us to a room that was out of sight from the rest of the office. He proceeded to tell us that our work was going to be redundant as they had already had their "computer guy" perform this work. NOTE: The employee was mis-informed. A typical computer consultant has neither the correct tools or training to forensically image hard drives or other digital media. It was a typical scenario in many ways until the owner showed up. We had removed the hard drive from the first machine and setup our equipment to image the hard drive. While we were monitoring the image, the owner of the company came in and wasted no time in expressing his displeasure at what we were doing and demanded that we leave. The fact remained that we were there under a court order and after a short conversation with both attorneys involved with this case his animosity subsided rather quickly.

With disaster averted we proceeded to image all of the drives in question and brought them back to our lab to be processed. Once the drives were processed we began to analyze them. Before long we discovered that a gargantuan amount of data had been deleted following the date that the litigation hold was put in place. Not only had the defendants been deleting information as we were walking through the door they continued to do so while we were imaging other drives just down the hall. In fact one of the defendants had run a disk defragmenter, a program that is used to consolidate files, often overwriting information contained on the hard drive.

Unfortunately for the defendants we were able to reconstruct most of the deleted data, including the smoking gun emails that the plaintiffs were looking for. Just as powerful was the fact that for approximately a week the defendants were deleting roughly 500 times the average amount of files than that of their normal habits for the previous months. When this information was presented in a graph it was devastating to their defense as the judge was very perturbed at the deliberate destruction of digital information and the blatant disregard for the litigation hold.

THE LORENZI GROUP

Although the defendants had refused to settle prior to discovery, our findings enabled the plaintiff's attorney to hit a towering home run and recover a substantial sum of money for his clients while shutting down their competitor.

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.