

Digital Theft of IP: A cover-up is uncovered

The Challenge, Part I: Identify Stolen Data

The client wanted to compel production of the ex-employee's devices from his new employer, but first they needed to prove that data had in fact been taken. This required examination of his old desktop computer and a review of the company's server for user activity and file access.

The Solution

By reviewing the activity on the computer, our examiners determined that external drives had been attached during the period of time when the employee was suspected of stealing information. Furthermore, we identified which files had been copied to the drives, indicating which data the employee had likely taken to his new employer. Our team discovered remnants of file-wiping software which had been used to delete files only minutes after these files had been copied to the external drive. This indicated a clear attempt by the employee to cover his tracks. Over 300 files contained only zeros, meaning the data had been erased permanently. However, our examiners were able to recover other deleted files as well as email communication between the defendant and his contact at the new company. This evidence convinced the judge to compel production of the devices belonging to the defendant, his wife, and other related parties.

The Challenge, Part II: Prove Employee Took Data

The 'story' found on the app showed the Defendant sitting with a group of friends on the day of the murder with a table full of drugs. In a photo taken just 20 minutes before the murder, the Defendant can be seen pointing a gun at the camera. This evidence would have almost certainly been uncovered by the prosecution during the investigation. The defense attorney would have remained unaware of this crucial evidence, and this may have badly affected his representation of the case. ArcherHall presented this evidence to the attorney, who was then able to properly prepare and mitigate the impact of the photos.

The Solution

The defendant found out the hard way that deleting data permanently is hard. Despite his best efforts to destroy all the evidence, our team was able to recover text messages and voicemails which discussed the theft of the data, deletion from the client's systems, and subsequent efforts to wipe the data off the new systems as well.

The Outcome

Even in the face of sophisticated anti-forensics attempts, our team was able to prove which data was taken and recover the defendant's own correspondence about stealing it and covering it up. The judge ruled in our client's favor and explicitly recognized ArcherHall for providing the pivotal evidence in the case.

Key Success

Overcame defendant's efforts to hide and destroy evidence and won recognition from the judge for our work.



The Situation

Our client was a corporation investigating suspected theft of intellectual property by a former employee. The employee had left for a competitor, allegedly taking proprietary customer and technical data with him. The client suspected the defendant had attempted to cover his tracks by wiping his computer. The case ultimately involved multiple computers, external media, and mobile devices.



ARCHERHALL
AIM HIGH

We are a leading provider of computer forensics and e-discovery services for businesses and law firms nationwide. We don't take chances with your data when litigation is a possibility, and proper handling is critical.