CASE STUDY

Digital Theft of IP

A cover-up is uncovered

CAPITOL DIGITAL & Californsics

Client
Corporation

Service
Digital Forensics

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.

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
Our team forensically collected and examined the additional devices. We discovered that each device had a brand new internal drive. There was no dust or signs of wear, and the manufacture dates on the drives were very recent. Not surprisingly, the client's proprietary data was nowhere to be found. It was clear that the defendant was attempting to cover his tracks again.

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 judged ruled in our client's favor and explicitly recognized Californsics 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.

555 Capitol Mall, Suite 235 ▪ Sacramento, CA 95814 ▪ 916.449.2820 ▪ www.Capitol-Digital.com