CASE STUDY

Anti-Forensics

Investigating attempts to hide IP theft using anti-forensic software

CAPITOL DIGITAL & Californsics

Client
Global Market Research Firm

Service
Investigating theft of IP

The Situation
Our client asked us to investigate a suspected theft of IP. Two employees had recently left the company for competitors and were suspected of misappropriating intellectual property and proprietary information. Californsics was given their work laptops to search for unusual activity and build evidence of the IP theft, including file transfers to USB, files sent to personal email addresses, correspondences with rival companies, and mass deletion of files.

The Challenge
Our team quickly determined that anti-forensics had been used in an attempt to hide suspicious activity on the laptops. The ex-employees had utilized different methods for copying IP, such as Google Drive and Dropbox. They had attempted to hide their activity using drive wiping software, which we could see had been used, and subsequently uninstalled, close to the time of termination of employment. Anti-forensics software makes it more difficult to find the evidence of IP theft, but our team was determined to continue.

The Solution
We expanded the scope of our investigation in order to examine not only traces of IP theft, but also evidence of data wiping and anti-forensic activity. Using the latest forensic software, we examined restore points and shadow copies to identify items and activity that had been deliberately hidden or obscured. This allowed us to collect evidence of data tampering that points towards theft of IP.

The Outcome
Californsics found evidence that data had been accessed, copied and deleted, and that anti-forensic software had been used in an attempt to hide the tracks of unusual digital activity. This evidence was compiled and reported to our client to support their case. Alongside other evidence, the signs of anti-forensic activity may allow for further investigation into the suspect's personal devices, eventually leading to the recovery of IP and mitigation of losses.

Key Success

Awareness of anti-forensic activity lead to an expansion of the scope of the investigation. Our forensic team uncovered signs of IP theft, and circumnavigated attempts to cover up unusual activity.

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