Case Study

legal

RICOH
imagine. change.

A Resourceful Analysis by Ricoh's Forensic Expert Solves a Software Piracy Case

The advanced forensic techniques employed by Ricoh's expert discovered the document that turned out to be the 'smoking gun' of the software piracy that the search team was hoping to find.

ABOUT THE CUSTOMER

The customer is a global computer software manufacturer.

CHALLENGE

The customer spent approximately seven months investigating the source of compact discs containing counterfeit versions of its software products. An individual was identified as a suspect in the course of the investigation and the company worked with authorities to obtain an ex-parte civil search order to raid the suspect's residence. Anticipating that critical evidence might be stored on computers at the location, the company enlisted the seasoned expertise of the licensed investigators from Ricoh Forensics to accompany the search team.

Holding the distinction of being the first private computer forensics lab accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board, Ricoh Forensics has a host of forensic experts and licensed private investigators with more than 60 years combined industry experience. It offers corporate counsel and law firms a full suite of capabilities for the identification, collection, verification, logging and analysis of electronically stored information (ESI).

SOLUTION

A Ricoh forensic expert joined law enforcement and the client's own investigators who served the search order and gained entry into the suspect's residence. A computer was quickly located in the course of the search. The Ricoh expert acquired a forensic image of the ESI on the computer and began an analysis of it while the search continued through the rest of the residence.

CHALLENGE

- Find critical evidence of software piracy during a raid of the suspect's residence

SOLUTION

- A thorough forensic analysis of the suspect's computer that traced down a USB device containing definitive evidence of the counterfeit transactions

RESULTS

- Recovery of more than 30 million dollars of lost revenue

Case Study

RICOH
imagine. change.

The analysis recovered Internet history that revealed evidence of online banking transactions with an account in a country with a well-known history of money laundering and corruption in its banking system. The expert also recovered deleted emails reflecting correspondence with a realtor in Spain concerning the purchase of a three million dollar property in one of Spain's exclusive resorts.

Additionally, the analysis showed activity involving the transfer of data to a USB storage device. However, the codes the operating system recorded related to the device were not any of those used with major USB memory devices.

Using his laptop, the expert went online and researched the code, tracing it to a brand of watch that had USB capabilities. When the expert showed a picture of the watch to the search team, one of the members of the team stated that he had seen the watch in the kitchen. The watch was recovered and Ricoh's expert acquired a forensic image of it. Initial analysis of the forensic image of the watch revealed that it contained a password-protected spreadsheet. While the expert was confident that the encryption could eventually be broken if the forensic image was taken back to Ricoh's forensic lab, he did not have the tools on-site to accomplish that task.

Not stopping there, Ricoh's expert wrote a script on-site to automate the process of recovering all of the more than 1 million words contained in the forensic image of the computer attained earlier, de-duplicating them and then running them against the encrypted spreadsheet to see if any of them were the password. After approximately twenty minutes of processing, the script revealed the password and opened the spreadsheet. The advanced forensic techniques employed by Ricoh's expert discovered the document that turned out to be the 'smoking gun' of the software piracy that the search team was hoping to find.

The spreadsheet contained a list of assets, including bank accounts, their balances and associated passwords. Moreover, the document contained information on all of the transactions related to selling the counterfeit CDs, including the identity of the purchasers, as well as additional information concerning the purchase of the property in Spain.

In the course of performing all of these resourceful investigative steps, Ricoh's expert strictly observed forensic processes with respect to the forensic imaging and preservation of ESI, using industry standard forensic tools.

RESULTS

As a result of the ESI obtained in the raid, the software company was able to assert that the purchasers of the software CDs should have known that the software was counterfeit as it was sold for one-third of the normal price. Threatening legal action against these purchasers, the company was able to recover the full retail license fee from each, resulting in a recovery of more than 17 million dollars. The settlement with the defendant also involved the recovery of millions of dollars from the bank accounts Ricoh's expert uncovered.

Needless to say, the software company was extremely satisfied with the work of Ricoh's forensic expert and the results that the single-day forensic investigation achieved.

www.ricoh-usa.com