SWISS FTS
Forensic Technology Solutions

A PRACTICAL CASE – IT FORENSICS

EMPLOYEE MISCONDUCT

IT forensics primarily deals with searching, securing and analyzing digital traces and evidence. If there are suspicious incidents regarding computer systems and IT infrastructure then a potential violation might have occurred, and further investigations are actioned through deeper data analysis and forensically acquiring new evidence.

Fraudsters are often disgruntled employees. There are different reasons for unsatisfied staff, but if they have the necessary knowledge of internal processes, sufficient rights and access authorization, and have a certain criminal energy then they may seek to acquire illicit gains at the company's expense.

THE SITUATION

In the presented case, suspicions were initially raised by a suppliers' fixed prices being artificially inflated, and having family ties to a member of staff. A detailed analysis of the employee's computers by an IT forensics expert was requested to verify the suspicion.

The forensic expert investigated three local workstations and a hard disk that was removed from a laptop. During the investigation, the suspicion of illicit activities was confirmed based on the analysis of recovered files, and the fact that the removed hard disk was not the original part the laptop. It was apparent that the suspect had been informed about the imminent seizure of its devices, and had tried to cover its tracks through file deletion and switching its laptop hard drive. These circumstances led to a far-reaching extension of the investigation and 2TB of data was ultimately analyzed.

THE SWISS FTS APPROACH

IT forensics requires in-depth expert knowledge to properly secure and analyze digital evidence. Swiss FTS has a team of certified experts with many years of experience to ensure that evidence is professionally acquired and analyzed.

After the acquisition of potentially relevant data sources, the data was analyzed with specialized forensic software allowing deliberately or accidentally deleted data to be recovered.

Suspects often try to remove incriminatory data from storage devices. If secure deletion software was used for irrevocable deletion, traces of it can be found which can indicate that the suspect is trying to hide something.

If a suspect attempts to destroy a hard drive or other storage device in order to prevent accessing the data on them, it can still be possible to retrieve fractions of the data by applying special procedures in a clean room and using professional software tools. ■

IMPORTANT ASPECTS

SECURING DEVICES

As soon as a suspected misconduct arises, data carriers, computers and other electronic devices have to be secured.

KEEPING TRACES

Devices which are seized should not be used any further, manipulated or analyzed by yourself. Vital information can be destroyed, and the integrity of the evidence might be compromised.

DOCUMENTATION

When devices are seized and data acquired due to suspected misconduct, the procedure has to be thoroughly documented to initiate potential legal proceedings.

ABOUT SWISS FTS
Founded: 2010
Specialties: IT Forensics, eDiscovery, Information Governance
www.swiss-fts.com

SWISS FTS
Forensic Technology Solutions

SWISS FTS AG
Europa-Strasse 19 | 8152 Glattbrugg | Switzerland
Phone +41 43 266 78 50 | info@swiss-fts.com

SWISS FTS (SINGAPORE) PTE LTD
55 Market Street | #10-01 | Singapore 048941
Phone +65 6950 1370 | singapore@swiss-fts.com