ACCESSDATA
an exterro company

PELORUS
Enabling Technology in the Right Direction

CASE STUDY

Using Pelorus and Advanced Digital Forensics Techniques to Investigate Tax Evasion

Background:

The suspected tax evasion involved a company under investigation for irregularities in their financial records. The whistleblower's tip provided initial leads for the investigating agency, but the lack of concrete evidence made it difficult to proceed with the case. The agency decided to enlist the help of Pelorus, a leading digital forensics company, to gather crucial evidence for the case. Pelorus experts were able to use their knowledge and experience to successfully identify and extract important data from the suspect's computer, leading to the discovery of an outside storage device used by the suspected employee.

Challenge:

The team encountered several challenges during the investigation. Firstly, they had to search for an external storage device that the suspect had been using. Additionally, they had to locate a way to bypass

Tool used:

- Tableau Disk Duplicator
- Access Data FTK

Challenges:

- Locating an external storage device and bypassing encryption on a pen drive. Required technical expertise and specialized software.

Results:

- Using Tableau Disk Duplicator and Access Data FTK, the team located the storage device and extracted evidence from the encrypted pen drive, leading to a successful prosecution.

encryption on a pen drive that contained accounting data, which the suspect denied decrypting. The team had to use their technical expertise to identify and analyze digital artifacts, such as “ShellBag” and “INK” files, to narrow down the search for the external storage device. Furthermore, they had to use specialized software and techniques to bypass the encryption on the pen drive and extract the necessary data. These challenges required a combination of technical expertise and investigative skills to overcome.

Solution:

When the team searched the suspected employee’s computer, they used a hardware device called **Tableau Disk Duplicator** to create an “image” of the computer hard drive. This process involves connecting the hard drive to the duplicator, which then copies all the data on the drive bit by bit onto a separate storage device. The resulting image contains all the files, directories, and metadata of the original hard drive.

The team then processed the image through a forensic software tool called **Access Data FTK.** This tool allows investigators to search, analyze, and recover data from the disk image in a forensically sound manner. With FTK, the team was able to conduct advanced searches and data analysis on the disk image, including the “ShellBag” and “INK” file analysis that helped them identify the external storage device used by the suspected employee.

“**Pelorus** offers LEAs a suite of powerful tools and solutions that enable them to efficiently and effectively investigate complex cases. By leveraging cutting-edge technology and streamlined processes, Pelorus helps LEAs to navigate the challenges of investigations and bring closure to even the most difficult cases.”

Overall, the use of Tableau Disk Duplicator and Access Data FTK allowed the Pelorus team to create a comprehensive digital image of the hard drive, search it for specific data, and analyze it in a way that preserved its integrity as potential evidence.

Result:

The Pelorus team's use of "ShellBag" analysis and "INK" file analysis, along with digital forensics tools like Tableau Disk Duplicator and Access Data FTK, enabled them to locate the external storage device and extract the necessary evidence from the encrypted pen drive. This evidence proved vital in proving the company's guilt and bringing the case to a successful conclusion. The case demonstrates the importance of using advanced digital forensics tools and techniques in investigating complex cases of tax evasion and other financial crimes.

Conclusion:

The successful outcome of this case is a testament to the vital role of digital forensics tools and the skills of investigators in uncovering evidence related to financial crimes. The ability to analyze digital devices and identify patterns and anomalies is a critical aspect of modern law enforcement. The use of tools such as Tableau Disk Duplicator and Access Data FTK helps investigators to image, analyze, and extract relevant data from electronic devices. In this case, the "ShellBag" analysis and "INK" file analysis techniques enabled the Pelorus team to identify the external storage device and the relevant data contained within it.

"**Pelorus** offers LEAs a suite of powerful tools and solutions that enable them to efficiently and effectively investigate complex cases. By leveraging cutting-edge technology and streamlined processes, Pelorus helps LEAs to navigate the challenges of investigations and bring closure to even the most difficult cases."

The investigation also highlights the importance of understanding encryption techniques and other data protection methods. The suspect's denial of encrypting the pen drive would have been a significant challenge for investigators without the knowledge and experience of the Pelorus team. The successful extraction of the data and the subsequent prosecution of the accused demonstrates the value of digital forensics expertise in modern-day criminal investigations.

Overall, this case serves as a powerful example of how digital forensics tools and expert investigators can work together to uncover evidence and bring criminals to justice. It underscores the importance of investing in these technologies and the skilled personnel required to use them effectively.

"**Pelorus** offers LEAs a suite of powerful tools and solutions that enable them to efficiently and effectively investigate complex cases. By leveraging cutting-edge technology and streamlined processes, Pelorus helps LEAs to navigate the challenges of investigations and bring closure to even the most difficult cases."