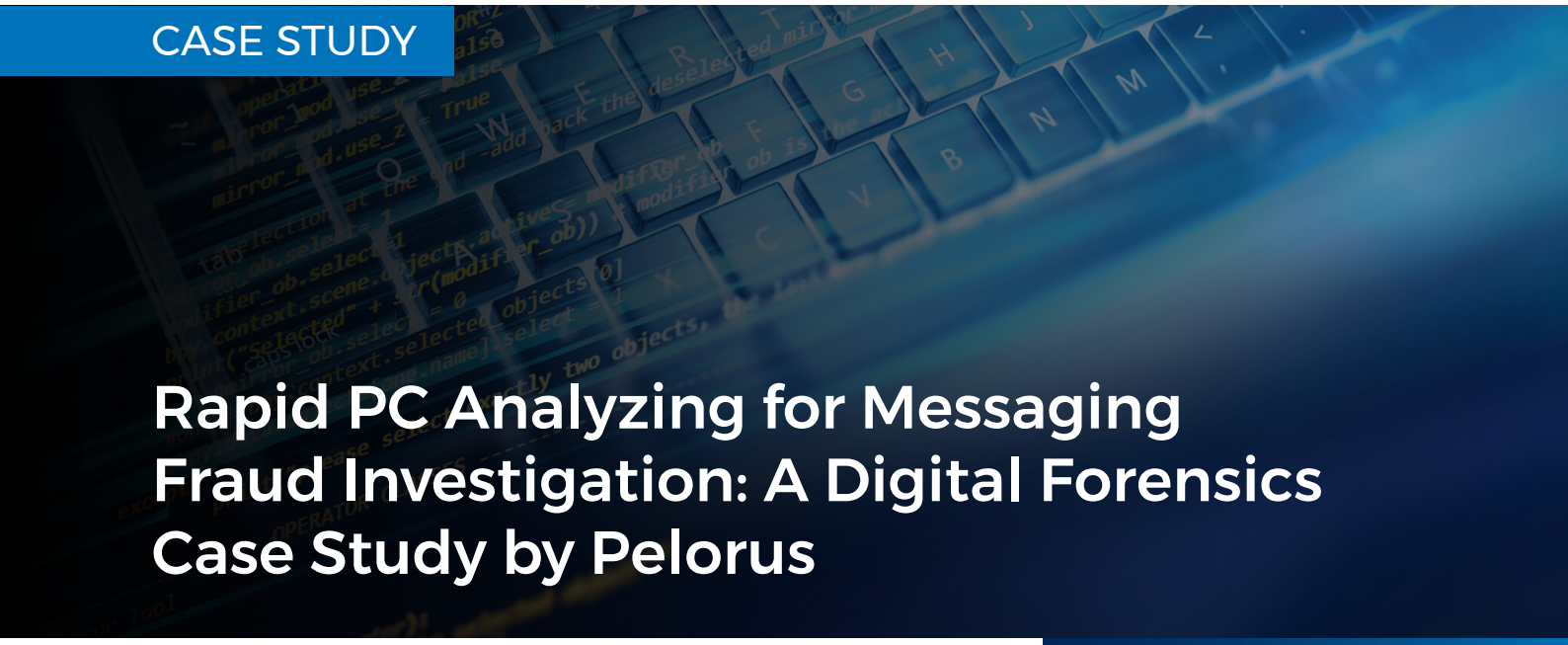
CASE STUDY



Rapid PC Analyzing for Messaging Fraud Investigation: A Digital Forensics Case Study by Pelorus

Background:

With the rise of technology, people have become more connected than ever before. Communication with people from all over the world has become simpler and more convenient. However, this has also led to an increase in messaging fraud, which has become a major concern for individuals and law enforcement agencies alike.

In this case study, the victim reported receiving regular blackmailing messages. Such messages can have a significant emotional impact on the victim, who may be left feeling vulnerable and helpless. Additionally, the victim may also face financial losses if they comply with the demands of the blackmailer.

To investigate the case, the law enforcement agency (LEA) began tracking the source of the messages. It was discovered that the messages were being sent from a cybercafé, which posed a significant challenge for the investigators. Identifying the culprit from the

Tool used:

- ADF tools

Challenges:

- Analyzing data from 32 PCs using traditional methods would have been time-consuming and complex.
- Data integrity was a significant concern as any data collected would need to be forensically sound and admissible in court.

Results:

- The use of ADF tools by Pelorus allowed for rapid analyze of all 32 PCs and efficient analysis of the massive amounts of digital data retrieved.
- The evidence obtained, combined with CCTV and an entry book, resulted in the identification and apprehension of the criminal.

32 PCs in the cybercafé would be time-consuming and require specialized tools.

The challenges faced by LEA highlight the importance of digital forensics in modern-day crime investigations. Law enforcement agencies need advanced tools and techniques to extract and analyze digital evidence, which can help them solve complex cases such as messaging fraud.

Challenges:

Analyze data from 32 PCs using traditional methods would have been a time-consuming and complex process for the digital forensic experts. It would have required taking apart each computer, attaching a hard drive to a write blocker, and copying data bit by bit. Moreover, not all 32 PCs were guaranteed to contain the relevant data, which would make the analyze process even more time-consuming.

Additionally, data integrity was a significant concern. Any data collected would need to be forensically sound and admissible in court. Collecting data improperly could result in the data being inadmissible and could even harm the investigation.

Furthermore, the investigators had to ensure that they did not disrupt any legitimate cybercafe customers' activities during the investigation.

Solution:

The ADF tools used by Pelorus is a powerful digital forensic tool that can acquire, triage, and analyze digital media. With the ADF tool, Pelorus professionals

"**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."

were able to rapidly and effectively image all 32 PCs in the cybercafe, allowing them to quickly extract the evidence required to identify the culprit. Additionally, Pelorus's professionals had the expertise to efficiently analyze and interpret the massive amounts of digital data retrieved from the PCs.

The use of CCTV and an entry book, along with the forensic evidence obtained, provided the LEA with the information necessary to locate and arrest the perpetrator. Pelorus's digital forensics expertise was critical in ensuring the successful resolution of the case, which may not have been possible with conventional investigative techniques alone.

Result:

Pelorus's use of digital forensics tools proved essential in quickly and efficiently solving the messaging fraud case. Their ability to image all 32 PCs in one day using ADF tools and analyze the data resulted in the identification and apprehension of the criminal. This case demonstrates how Pelorus's expertise in digital forensics can provide valuable assistance to law enforcement agencies in combating cybercrime.

Conclusion:

The case study demonstrates how Pelorus's digital forensics expertise can help law enforcement agencies to investigate and solve complex cases efficiently. With advanced technology and tools like ADF, Pelorus professionals can quickly gather and analyze digital evidence, ultimately leading to the successful resolution of the case.

"**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."