



Computer Forensics & Incident Response

for One of the Largest Engineering Companies in India

Copyright MIEL e-Security Pvt Ltd

CASE STUDY

Contents

A] Why Computer Forensics?	Pg - 2
B] Objectives	Pg - 2
C] The Solution	Pg - 3
D] About MIEL	Pg - 4
E] Conclusion	Pg - 5

About The Client:

Copyright MIEL e-Security Pvt Ltd

The client, an Independently managed subsidiary of Italian Company has over 50 years of experience in designing and supplying chemical process plants worldwide. A full service engineering partner, the client has engineering, procurement and construction management expertise in man-made fibers, polymers, refining operations, petrochemical and specialty chemical facilities.

A) Why Computer Forensics? –

In response to an information security incident, the client retained the services of MIEL e-Security Pvt. Ltd to conduct a digital forensics investigation. It was observed that confidential information had leaked from an intra-departmental shared folder on the network. This confidential information was being accessed by individuals who were not authorized to view it. Further, this information was being propagated to other members of the organization using email / network sharing.

B) Objectives –

MIEL's investigation was tasked with conducting an analysis of the information systems with the following objectives:

- Perform disk based forensics to verify the information about the incident already disclosed to the client.
- Identify and isolate additional systems that contain incriminating data.

- Deploy surveillance systems across specifically chosen suspect systems that are in the network.
- Determine the extent of the movement of the incriminating data across the network.
- Identify whether confidential information has been transmitted over email.
- Determine access patterns in the incriminating data.

C) The Solution –

The client had already isolated one suspect system and provided it to MIEL's consultants to use as an initial lead for the investigation. Along with this system, a set of specifically chosen keywords and filenames from the incriminating data were provided. These keywords were used as the search criteria for the rest of the investigation.

MIEL conducted a network-wide search against these keywords and filenames with the goal of discovering other systems with the incriminating data.



Based on the results of the network search and the findings from the initial suspects system, additional systems were identified for analysis. These systems had their hard-drives replaced with copies so that the users would not discover that they were under scrutiny.

The incriminating data on the duplicate disks was corrupted so that the individuals would not be able to spread it further. The original disks were physically isolated and subjected to forensic analysis.

Mirror-images of these systems have been captured to preserve the evidence available on them. Keyword searches were made on these disks and the incriminating data was discovered. Furthermore, the email data files were extracted to analyze to determine whether the information was being spread by email.

In most cases, the individuals had not had the opportunity to delete the incriminating data as the drives were swapped while they were not in the office; however one system subjected to analysis was a laptop system where evidence was recovered. It was observed that the files on this system had recently been deleted. MIEL has recovered the deleted information.

Based on the findings of the hard-disk investigation, it was decided that a surveillance system be deployed on key suspect systems to monitor their activities and capture any attempts to move or delete the evidence. A covert surveillance system was deployed on six systems. This system is capturing all that the user of the system types and transmitting this information for analysis. It has been observed that some of the individuals are attempting to erase the evidence from their systems.

The evidence obtained from these investigations has been digitally preserved and documented as per industry best-practices.

D) About MIEL –

MIEL is a specialist information security consulting company located in Mumbai, India and offers end-to-end information security services ranging from BS7799 Consultancy to Technical Security Services to Managed Security Services. MIEL also provides the specialized services like Computer Forensics and Incident Responses.

E) Conclusion –

After completion of these activities, MIEL provided the client with 2 160 GB hard-disks containing:

1. Disk images of the suspect systems
2. Backup of the disk images

A DVD had also been burned containing the e-mail boxes of suspect systems. These information stores might be used to revisit the evidence recovered at any later stage. It was strongly recommended that they should be stored safely in a physically secure environment.



Reach us at:

MIEL e-Security Pvt Ltd: C – 611 / 612, Floral Deck Plaza
MIDC Central Road, Andheri (East), Mumbai 400 093. INDIA
Tel # General: +91 22 28215050 | Tel # Training: +91 22 39560003 / 04 | Fax #: +91 22 28215838
Email – General: feelsecure@mielesecurity.com | Email – Training: isti@mielesecurity.com
Website: www.mielesecurity.com