INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

MEMELGATE – Stage III

2025/2026

nuno.m.santos@tecnico.ulisboa.pt

Introduction

This assignment concludes the investigation into the "MEMELgate" case. In the previous stage, you analyzed the hard disk images from two computers belonging to João Musk, the main suspect behind the phishing campaign discovered in Lab 1. The investigation now shifts its focus to the computer network of MEMEL, the company at the center of the alleged fraud scheme. Evidence discovered on João Musk's computers suggests the existence of a broader criminal operation involving information leaks from MEMEL and the circulation of confidential documents that may expose internal corruption. This assignment aims to investigate this new lead by examining forensic material collected from MEMEL's infrastructure. Your objectives are to assess the authenticity of the leaked documents, determine how they were exfiltrated, and identify those responsible for the leak. As in previous assignments, we recommend conducting all analyses within a forensically sound virtual machine running the Kali Linux distribution.

Scenario presentation

The forensic analysis of João Musk's workstation and backup server provided decisive evidence confirming his authorship of the phishing campaign against the Zyra platform. His computers contained the complete source code of the fake website, local clones of the GitHub repository referenced in the `.git` configuration file recovered from the phishing server, and logs of commits that matched those on the public repository. Deployment scripts and SSH configuration files showed that the fake site had been uploaded to a virtual machine hosted on INESC-ID's servers. INESC-ID later confirmed that João was solely responsible for managing that VM and was the only person with administrative access credentials.

Confronted with this evidence, João was interviewed a second time. He admitted to being the author of the phishing campaign, claiming his motivation was personal revenge after suffering an accident with one of Zyra's bikes that left him temporarily incapacitated. The phishing campaign, according to his statement, was intended merely to discredit the company.

However, the investigation also uncovered new elements unrelated to the phishing attack. Among the data stored on João's backup server were duplicates of the covert documents hidden within the Zyra website. Analysis of file metadata showed that these documents had been copied from his workstation to the backup server, and previously imported from a USB drive. Further inspection of João's email and chat logs revealed that the USB drive had been left in a public locker by an unidentified individual, who sent an anonymous email with instructions for retrieval. Chat conversations recovered from an IRC client showed exchanges between João and a contact using the nickname `CatDucky`. João identified `CatDucky` as Catarina Pato, another IST Computer Engineering student and a senior member of IST's STT.

Because the content of these documents appeared to implicate MEMEL in potentially serious financial crimes, the IST investigation team escalated the matter to the Polícia Judiciária. Catarina was questioned and acknowledged having received an anonymous email from an unknown sender containing instructions to retrieve a USB drive but denied any involvement in MEMEL's internal affairs. She explained that she had recently been interning at MEMEL, contributing to the development of its management platform, but claimed to be unaware of any illegal activity.

Given these circumstances, the Polícia Judiciária opened a new investigation to determine whether the leaked documents were authentic and to identify how they were exfiltrated from MEMEL's network. A judicial warrant was issued authorizing a forensic inspection of MEMEL's IT infrastructure, with particular focus on the systems most likely to contain traces of data leakage. The search centered on network communications of the workstation of Duarte Calado, MEMEL's Director of IT and Digital Transformation, as well as other machines within the same internal subnet.

You have been enlisted once again to assist the Polícia Judiciária in this investigation. With the support of Miguel Pontes, an intern from MEMEL's gateway security division, you were briefed on the network topology and provided access to relevant forensic material. The figure below depicts a simplified reconstruction of MEMEL's internal network. The topology includes a gateway acting as both a router and an HTTPS proxy, assigned the IP 194.210.63.254. Three key workstations operate within the subnet:

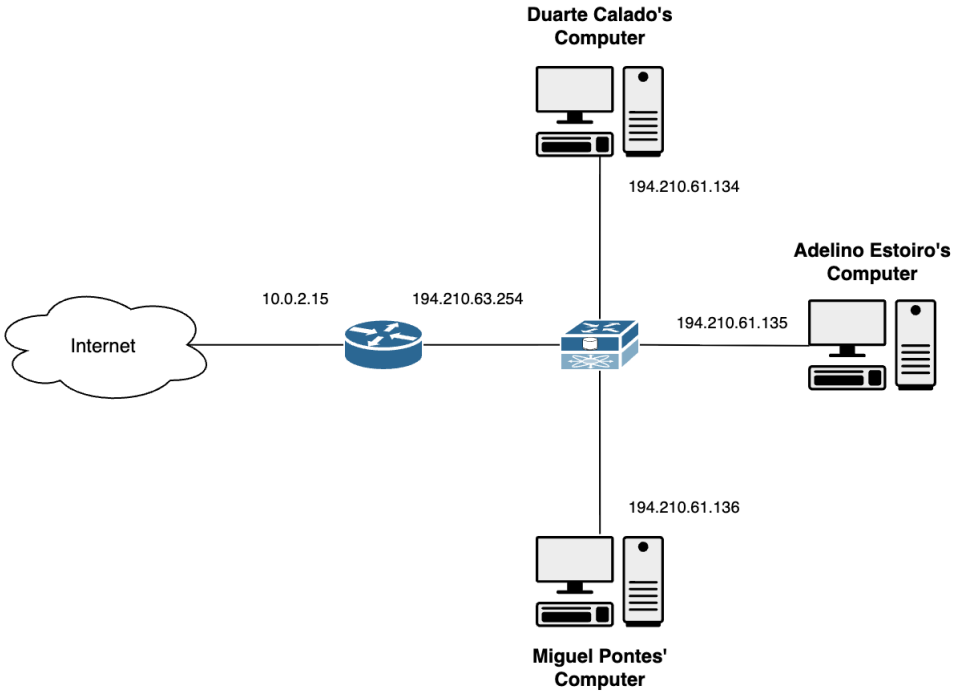

Figure 1: Diagram of the simplified network topology at MEMEL's premises.

- **Duarte Calado** — IT Director (IP: 194.210.61.134)
- **Adelino Estoiro** — Financial Director (IP: 194.210.61.135)
- **Miguel Pontes** — Gateway Security Intern (IP: 194.210.61.136)

Due to MEMEL's internal security policy, the HTTPS proxy periodically captures network traffic for auditing purposes. You were provided with three distinct network traces, each recorded at different times, along with an SSL key log file secured prior to the events analyzed in earlier assignments. The SSL key log enables forensic experts to decrypt HTTPS traffic captured by the proxy. It is compatible with Wireshark and can be loaded directly within the tool. All relevant files for this assignment are available on the course website under *Course Material* > *Lab Assignments*.

File	SHA-256 Value	Description
trace1.pcapng	`188f74388ed7d58b3faf28674856669e900603a8131ebbc405dc6069a69c63fd`	Network trace 1
trace2.pcapng	`421163eb2eef55dd63697eb607cefe212fedb756696fed2bd78732aad005d4f2`	Network trace 2
trace3.pcapng	`9e1a5f25ea2a07f4400f8cba98a37010acf4166281a45ba16f50b6b0215c4aa6`	Network trace 3
sslkeylogfile.txt	`1e88bdeedc28986dc98bdc708a30153edba29d506884a9ac38c658db5a83f471`	HTTPS proxy key

In this exercise, your task is to analyze the provided digital artifacts and answer the following questions. Justify all your conclusions by presenting the evidence that supports them, clearly stating your hypotheses and describing the steps you took to validate each one.

1. Do the analyzed network traces contain evidence of transfers involving any of the six hidden documents identified in previous assignments? What can you infer about the source and origin of these documents within MEMEL's network?

2. Based on the observed network activity, what can you deduce about the identity of the person or persons responsible for transferring the documents?

3. Can you reconstruct a timeline of key events that explains how the data exfiltration took place and how the documents ultimately reached João Musk's possession? Present your reasoning clearly and reference all timestamps used to establish the chronology.

4. Considering all the evidence collected throughout the MEMELgate investigation, what can you now conclude about the hypothesis of fraudulent activity within MEMEL that initiated this inquiry? Did you uncover additional evidence supporting the existence of fraud? Identify the actors who may be involved and outline your recommendations for the next phase of the investigation.

Note: Given that this exercise was emulated in a virtual environment, please consider that:

1. The analyzed network was implemented using virtual machines connected through a simplified virtual topology running on a single host. In a real deployment, MEMEL's network would include many more active users and systems.
2. The trace collection started really on **October 7th**. Therefore, the absolute timestamps recorded within the provided digital artifacts are skewed by about **32 days** in comparison to the timestamps of Lab Assignment I. For the purpose of your timeline, you must adjust the times of this trace to match those of the first assignment (go to the Time Shift, as in Tutorial 3, and apply: **-768:0:0**).

Deliverables

Write a forensic report that describes your findings. The deadline for this work is October 22nd. Until then, you must upload to Fénix a compressed zip file containing three deliverables:

- **Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend that you use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All relevant evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and SHA-256 values are indicated in the report.
- **Auxiliary Items:** Programs, scripts, and additional documents that you have produced during the investigation which are important to justify your results must also be included.
- **Timeline:** A timeline of the most relevant events. You must identify all relevant events that support your claims. We recommend you use the template that can be downloaded from the course website.

Good luck!