INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

MEMELGATE – Stage II

2025/2026

nuno.m.santos@tecnico.ulisboa.pt

Introduction

The goal of this second assignment is to continue the investigation of the "MEMELgate" case. In Lab Assignment I, you were tasked with forensically analyzing the suspicious Zyra promotional flyers and the website they referenced. Your analysis confirmed that the Zyra site was hosting a phishing campaign designed to capture user credentials and also revealed a set of hidden files that suggest a larger scheme may be unfolding. Both the phishing website and the extracted hidden files are downloadable from: Course Material > Lab assignments > lab1_artifacts.zip.

In this second assignment, the objective is to further investigate the provenance and significance of these artifacts by analyzing hard disk images retrieved from the desktop and backup computers of the main suspect of this crime: João Musk. To solve this exercise, you will need to develop your skills in file system forensics. All the required digital artifacts are available on the course website. As in the first assignment, we recommend using Kali Linux on a forensically sound virtual machine for your analysis.

Scenario presentation

When you followed the flyer's QR code in Lab 1 you were redirected to a cloned Zyra website. This site mimicked Zyra's official login page and was configured to harvest credentials submitted by unsuspecting users. Any passwords entered were captured by the server and logged for later retrieval, while users were presented with misleading error messages to mask the fraud. This confirmed the presence of a phishing campaign targeting IST students and staff. In addition to uncovering the phishing scam, your team also recovered a hidden bundle of suspicious files embedded within the Zyra site. These artifacts hinted at deeper irregularities and manipulated pricing data at MEMEL. The complete set of artifacts comprising the six hidden files and a snapshot of the Zyra website is summarized below:

File	SHA-256 Value	Description
f1.db	`23108d6552bbd633ed80c3de50449e0698294c0da3a049a61bbaed41e0edcea0`	Partial database extract.
f2.txt	`80373bc7994731717f3fe753685848541bb81cbf906a85c3f42415e5ed05bd86`	Algorithm diff file.
f3.png	`ff56d339f5affe0279530214dec0ef01950828beb4af6bfa83fe8465a71da7d8`	Reddit thread.
f4.pdf	`748e7358ccbba0b769b94ecb3c96c161fd8366454acf076a6f95b5f404515e1d`	Invoice Futuro Inteligente, Lda.
f5.pdf	`fde6e8582b5b4763e4e574c5eb293876f5894339215d12bffd224f929e559cc9`	Internal financial report.
f6.png	`c938a05b84f2d749fc6ac65a88f57ccc0c860d4169577947425cc01aa1bbd1c3`	Whatsapp conversation.
website.zip	`02cea7249de8242bd2319b543e463f5164da213420c04f2f0f2a8ef128dec1fb`	Zyra website snapshot.

Since phishing constitutes a criminal offense, and the presence of these hidden files suggested the possibility of a larger fraudulent scheme, the investigation escalated with a focus on attribution. During the forensic analysis of the site and the hosting VM, the team discovered evidence linking the malicious VM to resources administered by an INESC-ID account. Furthermore, a publicly visible GitHub (`https://github.com/MuskyBoi`) repository owned by `MuskyBoi` contained source code and deployment scripts that matched artifacts on the hosting VM. The GitHub profile claimed the owner was João Musk, verified to be an IST MSc student and former intern in Prof. Nuno Santos' team at INESC-ID. Log entries further suggested the phishing VM was launched from a VM instance controlled by that account.

Following these findings, João was contacted at IST and questioned about his possible involvement. He denied any responsibility and refused to cooperate. In light of the phishing attack and the possibility of a larger fraud, the case was formally referred to the Polícia Judiciária. With judicial authorization, the authorities executed a search warrant at João's residence and seized two devices: a *workstation* and a *backup server*, both connected to the Internet via the local network. Forensic images of the hard drives from both computers are now available on the course website (Course Material > Lab assignments):

File	SHA-256 Value	Description
johnny.tar.gz	`dca5f990988c1b07ec71e533b75c19611de91b4446c54dce60946a573f564576`	Workstation image.
backup.tar.gz	`95c2ee81f7302191eae16eea3a1e6fc68ba73abf87e03fc83b11f57aed5cbc60`	Backup server image.

Your team has been invited to collaborate with the Polícia Judiciária in analyzing these new artifacts. Based on your analysis of the provided disk images and the previously recovered artifacts, answer the following questions. Justify your answers and provide evidence supporting your conclusions.

1. Do the seized disk images contain traces of the phishing website (source code, deployment scripts, logs) and/or the hidden artifacts discovered in Lab 1? If so, identify them, their locations on disk, and their SHA-256 values as recovered from the images.

2. Can you reconstruct the provenance and handling of these files? Provide a timeline of relevant events that shows how the phishing site was built and operated, and how the hidden artifacts were managed on the seized machines.

3. Did you find any evidence of anti-forensic activity? If so, describe the techniques observed and the evidence that supports your claim.

4. What new discoveries emerge from the seized images that were not visible in Lab 1? Do these findings strengthen the attribution of the phishing attack to João Musk, or point to other relevant actors (collaborators, external servers)? Based on your analysis, what hypotheses can you form about the larger scheme hinted at by the hidden artifacts, and what recommendations would you make for further investigative steps by Prof. Alexandre Magno and the Polícia Judiciária?

Note: The forensic images provided in this exercise were produced in an emulated environment. The acquisition metadata records the creation of the workstation and backup forensic images as *2025-09-23*. However, for the purposes of this exercise you must treat the images as if they were created on *2025-09-09*. Concretely, when reconstructing timelines from timestamps, *adjust all observed absolute timestamps by subtracting 14 days* (i.e., 23 - 09 = 14 days). For example, a file with a recorded timestamp "2025-09-21 14:10" in the image should be reported as "2025-09-07 14:10" in your reconstructed timeline.

Deliverables

Write a forensic report that describes your findings. You have until October 8^{th} to solve this exercise and upload to Fenix a compressed zip file containing four pieces:

- **Digital Forensic Report**: A document in which you answer the aforementioned questions. You must identify all relevant evidentiary items that support your claims. We recommend you to 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!