INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

MEMELGATE – Stage I

2025/2026

nuno.m.santos@tecnico.ulisboa.pt

Introduction

Your team will be leading the investigation of the "MEMELgate" case. This investigation will unfold in three progressive stages, each guided by a separate lab assignment. This document offers an overview of the case and introduces the first assignment. In this stage, you will gain practical experience in digital file forensics, potentially including steganalysis, by examining a set of artifacts accessible through the scenario presentation. To carry out your work in a controlled and forensically sound environment, we suggest the use of the Kali Linux distribution running on a virtual machine.

Scenario presentation

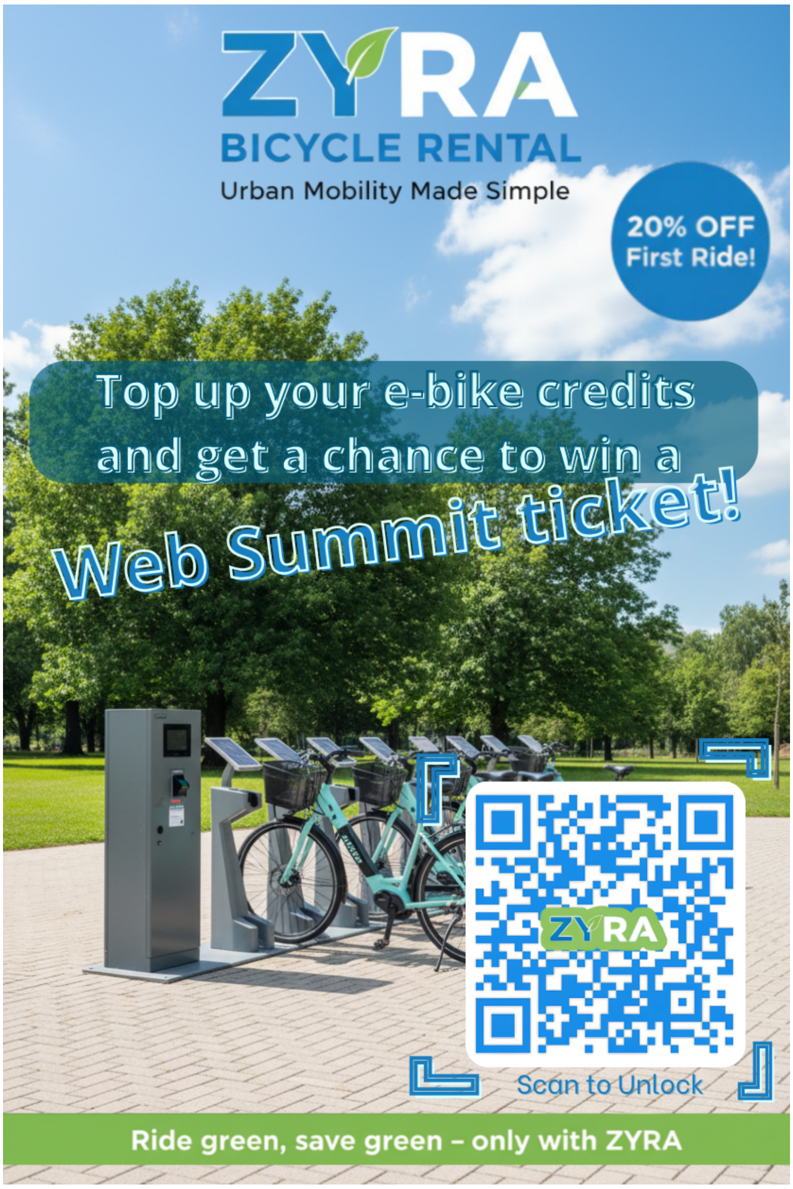
ZYRA
BICYCLE RENTAL
Urban Mobility Made Simple
20% OFF First Ride!
Top up your e-bike credits and get a chance to win a
Web Summit ticket!
ZYRA
Scan to Unlock
Ride green, save green – only with ZYRA

Figure 1: Suspicious flyer promoting a Zyra e-bike campaign, found posted across IST premises.

The suspicious flyers shown in Figure 1 were found posted in multiple locations across the Alameda and Taguspark campuses of Instituto Superior Técnico. The flyers promote a campaign of the bicycle rental company *Zyra*, a well-known operator of bike sharing services in the Lisbon metropolitan area. The promotion promises a discount on the first ride and even a chance to win tickets for the Web Summit, directing users to scan a QR code that supposedly unlocks the service.

Shortly after the flyers appeared, several IST students reported that scanning the QR code led to errors when attempting to log in. Some expressed suspicion that the destination website might be fraudulent or malicious. These concerns reached the attention of Prof. Alexandre Magno, Vice-President for Digital Technologies at IST, who decided to initiate a formal investigation. After consultation with Prof. Refrigério Sargaço, President of IST, an official mandate was issued granting Prof. Magno full authority to conduct a thorough forensic inquiry into the case.

Your group has been hired to act as the forensic investigation team supporting Prof. Magno. Your mission is to determine whether these flyers are indeed part of a scam, to characterize the nature of the attack if one exists, and to attempt attribution of responsibility. The investigation should begin directly from the flyer itself, in particular by analyzing the digital references it contains (such as the QR code) and carefully following all leads that emerge from it.

As the case unfolds, you may come across additional digital materials such as websites or files hosted online. These artifacts must be treated as potential evidence and analyzed thoroughly to support your conclusions. If suspicions arise regarding the use of steganography or other obfuscation techniques, your team should be prepared to analyze and retrieve any hidden secrets.

In summary, your task in this first assignment is to treat the flyer as the entry point to the investigation, pursue the evidence trail it opens, and assemble answers to the questions listed below. Be sure to justify your conclusions by presenting all relevant evidence you uncover, and clearly explain your hypotheses and how you validated them.

1. Based on your analysis, did you find evidence of this being a scam? If so, describe the nature of this scam and provide technical details on how it was conducted.

2. Did you uncover any additional concealed artifacts during your investigation? If so, explain how these artifacts were hidden and describe the methodology you used to extract them.

3. With a focus on the additional concealed secrets you recovered, analyze their content and relationships, and propose a possible interpretation of their meaning. Formulate a hypothesis regarding their significance and support it with the content of the recovered secrets. Additionally, prepare a timeline of the events suggested by these recovered materials.

4. Did you find evidence of the identity of those responsible for this scam? Based on your findings, what recommendations would you make for the next steps in the investigation? Advise Prof. Alexandre Magno on the best course of action moving forward.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is September 24^{th}. Until then, you must upload to Fenix a compressed zip file containing four deliverables:

- **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.

TIPS: There are in total 6 hidden secrets in the provided artifacts.

Good luck!