INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

# FORENSICS CYBER-SECURITY

MEIC, METI

# Lab Assignment II

## ARCO UNDERGROUND – Stage II

2023/2024

nuno.m.santos@tecnico.ulisboa.pt

# Introduction

The goal of this second assignment is to continue the investigation of the “Arco Underground” case. In the first stage (refer to Lab Assignment I), you were given the task of forensically analyzing a lost pen drive. This analysis revealed hidden artifacts that suggest a crime is unfolding. In this second assignment, the objective is to further track the provenance and significance of these artifacts by analyzing hard disk images. 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 suggest that you analyze them using the Kali Linux distribution on a forensically sound virtual machine.

# Scenario presentation

By analyzing the collection of files extracted from the forensic image of the lost pen drive, your team made several relevant findings. First, the analysis of the content and metadata of these documents suggests that the possible owner of this pen drive is César Silva Ferro, a student from IST enrolled in the MEIC master’s program. Moreover, by employing various steganalysis techniques, your team managed to retrieve six hidden artifacts. One of these artifacts is a number (1683461) that was secretly embedded inside a WAV file. The remaining five are part of the set of files listed in the table below. These files can be downloaded from Course Material > Lab assignments > lab1_secrets.tar.gz.

| File | SHA-256 Value | Description |
|---|---|---|
| f1.pdf | a6a005c97a758f04220fe161c269a2ac229d7fe3b6fbfc88e40d6d8675be8fd6 | Anonymous letter |
| f2.png | 1f70fc60e1c23b842e3278846e29c5fb66ed43c1d6ac3ccfe408f53acf005edb | Bank statement |
| f3.jpeg | dca0850ab895e45808235d32e9591d4ec08b09be89727760878cdd17963990bb | Underground photo |
| f4.jpeg | 131e54681ae4abca1d677384b3765bbc92c873eff252baec713196c2b696adeb | Tunnel blueprint |
| f5.mp4 | 8f9a03d13221bf0477f8c7d178bcfbdd94c3ef22df05dcee05cc3962c82ff11c | Video footage |

In addition to securing these hidden artifacts, Mr. Golias Matos, as the head of IT, knew what to do and decided to be proactive, following the standard procedure for evidence collection. As part of the procedure, he filled in a chain of custody form, in which he noted the serial number of the pen drive, knowing that it could prove to be crucial for further investigations. The serial number that was registered was **YLBE5FV0**. Based on the findings you presented Mr. Matos then decided to escalate the investigation and contacted the president of IST. During their conversation, Mr. Matos recounted the events that led to this investigation and reported that the hidden artifacts suggest a plot to build an underground tunnel connecting the new Arco do Cego building to Casa da Moeda. The full plan remains unclear, but if true, it suggests that a major heist might be in the works. "Who might be behind this? The construction firm?", inquired the IST president, Prof. Rodrigo Cabaço. Mr. Matos replied that he was uncertain, as there wasn’t much evidence aside from a bank statement linked to Prof. Eva Rocha and some clues pointing to the potential owner of the pen drive. After lengthy deliberation, Prof. Cabaço decided to hand the investigation over to Polícia Judiciária. The authorities believed the presented material warranted further investigation and chose to follow the primary lead: César Silva Ferro, who resided in IST’s student housing. After obtaining a warrant, the police entered his room and discovered two computers: a *workstation* and a *backup server*. Both computers had connections to the Internet via the local network. An agent confiscated both computers and created forensically sound images of their hard drives, storing these images in two artifact files available on the course website (Course Material > Lab assignments).

| File | SHA-256 Value | Description |
|---|---|---|
| caesarDisk.tar.gz | dab4cb12116ab978c7c1cf62678878277398bee4d0a82c690133029ce2dd8494 | Workstation image |
| backupDisk.tar.gz | e8a0e8c70c9a37baa5eb89578f064ff2a9254d33069ca7528d08bd31b69e4f21 | Backup server image |

Given your team's expertise, you were invited to collaborate with the police to analyze these new artifacts. In this exercise, your task is to examine them and answer the following four questions. Please justify your answers by presenting all pertinent evidence you uncover. Ensure that you clearly articulate your hypotheses and describe the steps you took to validate them.

1. Did you find any traces of the hidden artifacts and/or the files from the lost pen drive on César Silva Ferro's computers?
2. If so, can you trace the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.
3. Do you find any evidence of anti-forensic activity?
4. What new discoveries can you report that clarify the plot or identify other relevant actors?

## Deliverables

Write a forensic report that describes your findings. You have until October 13*th* to solve this exercise and upload to Fenix a compressed zip file containing three 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.

Good luck!