INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

ARIANE 6 – Stage I

2024/2025

nuno.m.santos@tecnico.ulisboa.pt

Introduction

Your team will be leading the investigation of the "Ariane 6" 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. Through this assignment, you will gain practical experience in file forensics and steganalysis, requiring you to examine a select set of files available for download from the course website (`csf-lab1-artifacts.zip`). To analyze these artifacts, we suggest you to utilize the Kali Linux distribution on a forensically sound virtual machine.

Scenario presentation

Mr. Ricardo Prado, the head of the IT department (DSI) at IST's Taguspark campus, received an urgent phone call. A credible source reported that a student in the Computer Science and Engineering program was suspected of engaging in cybercriminal activities, specifically the theft of user credentials from Fenix, the university's information system. These stolen credentials, if misused, could pose a significant security threat to IST, particularly if they belong to high-ranking professors with the authority to make critical decisions and override operations within Fenix.

The source not only provided this alarming information but also identified the suspect: João Musk, a fourth-year master's student. The source suggested that Musk had likely stored the stolen credentials in his private account on the sigma cluster, the file storage system used by all students to manage their data. While a broad response, such as forcing all Fenix users to reset their credentials, might seem wise, this could seriously disrupt the university's operations and create widespread concern within the IST community. Instead, Mr. Prado opted for a more targeted approach: to investigate Musk's private files and discreetly retrieve the stolen credentials so that only the affected users would be contacted.

However, accessing a student's private data is no small matter, given the strict data protection regulations in place. Before proceeding, Mr. Prado needed to secure legal authorization. Acting swiftly, he contacted IST's president, Mr. Refrigério Sargaço, who promptly issued an official mandate granting Mr. Prado and his team permission to access João Musk's files on the file server.

With the legalities in order, Mr. Prado's team initiated the investigation by creating a forensic copy of all files from Musk's account and carefully documenting the chain of custody. To ensure a thorough examination, he has now turned to your group, currently working for the DSI, to analyze these files. The files are listed below and are available at course website under "Course Material > Lab assignments":

File	SHA-256 Value
andromeda.png	`fcdd6ce7ae9a8f02c2ba3b2693d49848606b1ca5d332a076fe63013fcaa55ab2`
best-intro.wav	`c3ea6b775dd7eaecebeef00e5523483d182602118ff6de0eb3d6a41b8f43c42f`
cartwheel.tiff	`f6861a315acb49b9c8ac18e9d6e92ed366e78f43bd2850d0f2a8f30f695aad45`
lactea.jpg	`326f3601ab7ad66fff2c43b3c5d4465d820dbf7381be65ab20c6adac2d1c10bb`
myzip.zip	`b7debe08f1b030f608a9ca34a091f09c1b7d3758beae453123a53250893645c4`
nmap	`33da582bf8705b3a6818fa25d1f61ee339d46f58b8aedfdd951e1d4a915d582d`
poster.pdf	`e34595b1f3761d6d4f23a50db8fdec01396f1b725ed8cf5af4f8cdaf58008603`
tagus.png	`0b916d4d246372e07b1a6901585b632d8426a07b611fa4b1058341ef2a59f7b2`
thrones.pdf	`0d61083587e9e6ba5c4a66c9d4ced247d5d0d78da9cdfce86d306c0fcdc8a336`

In this exercise, your task is to analyze the provided digital artifacts and respond to the four questions listed below. Be sure to justify your answers by presenting all relevant evidence you uncover. Clearly explain your hypotheses and how you validated them.

1. Based on your analysis of the documents, did you find the stolen credentials? If so, describe how you identified them and provide details on the information you discovered.

2. Did you uncover any additional concealed artifacts within the provided files? 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 as indicated by the recovered secrets.

4. Based on your findings, what recommendations would you make for the next steps in the investigation? Advise Mr. Ricardo Prado on the best course of action moving forward.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is September 27th. 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!