INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

ARIANE 6 – Stage II

2024/2025

nuno.m.santos@tecnico.ulisboa.pt

Introduction

The goal of this second assignment is to continue the investigation of the "Ariane 6" case. In the first stage (refer to Lab Assignment I), you were tasked with forensically analyzing data artifacts extracted from the private account of João Musk on the sigma cluster, a shared file storage system. This analysis uncovered stolen credentials, indicating a potential involvement in criminal activity.

In this second assignment, the objective is to further investigate the provenance and significance of these artifacts by analyzing hard disk images retrieved from João Musk's desktop and backup computers. 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 the Kali Linux distribution on a forensically sound virtual machine for your analysis.

Scenario presentation

By analyzing the collection of files extracted from João Musk's private account on the sigma cluster, your team made several significant discoveries. In particular, through the use of steganalysis techniques, your team successfully uncovered six hidden artifacts. One of these artifacts is a list of stolen credentials. Upon reporting this to your supervisor, Mr. Ricardo Prado, head of the IT department (DSI) at IST's Taguspark campus, Mr. Prado instructed your team to verify the authenticity of these credentials, which was subsequently confirmed. In response, he immediately blocked access to all affected accounts, contacted the respective owners, and requested that they change their passwords. The discovery of these credentials also corroborated an earlier phone warning. In addition to the credentials, your team identified five more hidden documents. All of these files, including the credentials, are listed in the table below. You can download these files from Course Material > Lab assignments > lab1_secrets.zip.

File	SHA-256 Value	Description
f1.pdf	`6bcaa146616cff67eb5acf9ac6a2e84e503236e86a398d9784316a76e5a5d502`	Bank Statement
f2.png	`e675e7cc9bb52fdb8eb43834395371e7dee57ab3726ff0a03099cd279c81dcaf`	Satellite Blueprint
f3.txt	`bfe6869955ed21e77bb510ea140b00ae2986cd6d08c7bf6f99c8aa2b8d20755a`	Credentials
f4.txt	`8fd0a496bcb9b687e9a363e67e7155498da1330ee87ae645a09cd84d259d4838`	Logs
f5.pdf	`75a554633a3d0a98faed4b5b1cc2e52d166fd44ee2804deb808a8f889f6ca3a5`	API Documentation
f6.pdf	`0e9aef94d7876a996be9f2fac6644e7d2258016f5409897e045501d7dfaa0625`	Deco Report

Based on these findings, particularly the confirmation of the stolen credentials, Mr. Prado reported the discovery to IST's president, Mr. Refrigério Sargaço. During their discussion, they considered whether this was a reckless, isolated action by João Musk—who recently joined Técnico's Security Team (STT) and might have decided to test his hacking skills on a live system—or if it indicated something far more serious, possibly involving an organized network of cybercriminals. While the other hidden artifacts appeared unrelated to the security breach, they raised suspicions due to their potential link to ISTSat-1, the Portuguese satellite developed by IST, which was recently launched with the Ariane 6 rocket on July 9. After careful deliberation, Prof. Sargaço decided to hand the case over to the Polícia Judiciária. The authorities believed the evidence warranted a deeper investigation, particularly the tracking of the stolen credentials, and decided to follow the primary lead: João Musk, who was residing in IST's student housing. With a warrant, the police searched his room and seized two computers: a *workstation* and a *backup server*, both connected to the Internet via the local network. Forensically sound images of the hard drives from both computers were created by the authorities, and these images are now available as two artifact files on the course website (Course Material > Lab assignments).

File	SHA-256 Value	Description
johnnyDisk.tar.gz	`7418b41704e346771b44a6545f408a64431fb31d47dabebd1a99b8e2c84121b0`	Workstation Image
backupDisk.tar.gz	`3a7d6df07f2f3435532173b7464fdb5b32d0c2ebd8b05b1418e07e86d35e7eef`	Backup Server Image

Given your team's expertise, you have been invited to collaborate with the police in analyzing these new artifacts. In this exercise, your task is to examine the provided data and answer the following four questions. Be sure to justify your answers by presenting all pertinent evidence you uncover. 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 originally discovered in João Musk's sigma account on his computers?
2. If so, can you trace the origin of these files and how they were processed over time? Construct a timeline of relevant events.
3. Did you uncover any evidence of anti-forensic activities?
4. What new discoveries can you report that might clarify the plot or identify other relevant actors?

For reference, note that the IP range of the sigma cluster's services is between 10.0.2.160-10.0.2.180.

Deliverables

Write a forensic report that describes your findings. You have until October 11^{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!