INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

ARCO UNDERGROUND – Stage I

2023/2024

nuno.m.santos@tecnico.ulisboa.pt

Introduction

Your team will be leading the investigation of the "Arco Underground" case. This investigation will be conducted in three progressive stages, each of them to be steered by an independent lab assignment. This document provides an overview of the case and presents the first assignment. This assignment will help you gain hands-on experience in file forensics and steganalysis, and it requires the examination of a small number of files which can be downloaded from the course website (`csf-lab1-artifacts.zip`). To analyze these artifacts, you may use the Kali Linux distribution on a forensically sound virtual machine.

Scenario presentation

At the Instituto Superior Técnico (IST), University of Lisbon – Portugal's premier computer engineering school — a noteworthy incident has recently occurred. Mr. Golias Matos, the head of the IT staff, stumbled upon a lost pen drive in Lab 5 of the computer science department (DEI). In line with DEI's stringent internal regulations, any unclaimed or misplaced storage device on the premises must be subject to an in-depth forensic analysis. This protocol primarily serves two objectives: first, to identify the device's owner with the intention of its safe return, provided no malicious activity is detected. Secondly, it ensures a thorough digital inspection to safeguard against potential threats, whether that be malware distribution or data theft attempts from unsuspecting users connecting the device to their machines. Should the forensic analysis reveal malicious content or intent, not only is the device withheld from return, but the situation may escalate. Specifically, a formal process could be initiated against the involved parties, even involving police authorities if the evidence suggests criminal activity.

Mr. Matos himself initiated the forensic analysis by creating a forensic image of the pen drive and completing the chain of custody form. He then requested the assistance of your group to analyze the following files that he extracted from the pen drive's forensic image (these files can be downloaded from the course website in Course Material > Lab assignments):

File	SHA-256 Value
BdC_on_the_beat	`d8028eb28c6aa2b94607df770515368e0d2c0488279328599ca51fe1bdbced6c`
Cool_stuff.mp4	`240cb4494b4a4e0e367f67afa80bd7287dda09755e3eaa66af1994a03ea3e316`
logo.png	`d25a8d99bccc3e176b2852acb72b92f3d40c8f7e4b6501d2145101929de637fb`
report.docx	`30bb4ca7580bd331d3334bf4bba6b9e45165d1f51960eb7ee345a631aee90f70`
Rialva.png	`8873a7055c9838ef8847424306f6997c3eb0d0aa6373acd65206ede85bfe8ec8`
Social.png	`50011896abe7f70e9e8b00b4d3ccc25acf6a2272f11b343b2758be01355d21f4`
sporting_anthem	`7d4e8b5d0d8d127fdf31f097a208a511847872884c2e11db662279292a0969cd`
Tagus.png	`ec54db5e6df2093573548d685ce72f3c4ffa548032e6a26ac2cc3f544bd3c283`
waste-of-time	`941b69160a7c4d6e3483c54c43a9a8fd52ff12b65af77b770d879cace846bce4`

In this exercise, your job is to analyze these digital artifacts and answer the four questions presented below. Justify your answers by presenting all the relevant evidence you can find. Make sure to explain your hypotheses and how you have validated them.

1. Based on your analysis of the documents, can you deduce the likely identity of the owner of this pen drive? Justify your answer with relevant findings.

2. Were there any concealed artifacts within the provided files? If so, detail how these artifacts were embedded and your methodology to extract them.

3. Based on the secrets you recovered, is there any indication that the pen drive was intended to spread malware or present a specific security threat? If there's no direct evidence of malicious intent, how would you interpret the data? Formulate a hypothesis regarding their purpose and justify it using the content of the recovered secrets.

4. Given your discoveries, what would be your recommendations for the subsequent course of action? Advise Mr. Golias Matos on how best to proceed with this investigation.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is September 29^{th}. Until then, you must upload to Fenix a compressed zip file containing three 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.

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

Good luck!