INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

Leaky Winden

2017/2018

{danielporto, nuno.m.santos}@tecnico.ulisboa.pt

Introduction

In this guide, you will be challenged to solve a case entitled "Leaky Winden", which will help you gain hands-on experience on steganography and file forensics. This exercise requires the examination of a small number of files. These files are enclosed in the zip file `csf-lab1-artifacts.zip` which can be downloaded from the course website. To analyze these artifacts, we recommend you to use the Kali Linux distribution.

Scenario presentation

For several years now, Ed Winden has been working for a major chip manufacturer. However, motivated by suspicious changes in his behavior, this company started taking measures to investigate him. Since he had privileged access to the plans for a new revolutionary processor, Winden might have illicitly stolen those plans, perhaps to sell them to competitors. Thus, after obtaining legal counseling and authorization, an auditing team was created to look for potential evidence. Eventually, they collected the following files from a Winden's pen drive after returning from a trip to Lisbon:

File	Value
LOTR-Part1.txt	`760ff6f302a6b9132983aedc9b51af1e`
compress.py	`ee4ce345a9519d9b3f22109828f26aac`
electrico.png	`48d4eb13f4760bb18f44d425568936e0`
jeronimos.png	`a0610a1756bc34f251716ba36b5aa197`
lisbon.png	`ccd086ec7f8d450c8d091cb6b8fe0b0c`
online_banking.zip	`d6f38d287f9f8b3fa6c613503f5a1619`
rossio.png	`dacadbf11a63a09fca89da083c12ac37`

Your task is to analyze these artifacts and search for any evidence of industrial secrets that might be present in them. Write a forensic report that describes your findings. The deadline for this work is October 27^{th}. Until then, you must upload to Fenix a compressed zip file containing four deliverables:

- **Digital Forensic Report**: A document in which you present your main findings. You must identify all recovered evidence artifacts, if any, and explain how you obtained them. We recommend you to use the template that can be downloaded from the course website.
- **Evidence Artifacts:** All evidence artifacts recovered during the forensic analysis. Please make sure that the respective file names and MD5 values are indicated in the report.
- **Examination Log:** Consists of a document in which you must note down all steps that were performed during the investigation. A template of a sample examination log can be retrieved from the course website.
- **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.

TIP: There are in total four hidden secrets in the provided artifacts.

Good luck!