INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

The Mole Affair

2018/2019

nuno.m.santos@tecnico.ulisboa.pt

Introduction

In this guide, you will be challenged to solve a case entitled "The Mole Affair", which will help you gain hands-on experience on file forensics and steganalysis. This exercise requires the examination of a small number of files. These files are enclosed inside 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 on a forensically sound virtual machine.

Scenario presentation

For several years now, John Mole has been working for DroneX, a major manufacturer of drone technology. In the past few months, motivated by suspicious changes in John's behavior, DroneX started taking measures to investigate him. Since he had privileged access to the design plans of their new revolutionary drones, the fear was that he might be illicitly stealing those plans in order to sell them to competitors. To dissipate such fears, after obtaining legal counseling and authorization, DroneX assembled an auditing team to look for potential evidence of industrial espionage. Eventually, this team collected the following files from a pen drive that John was carrying along after returning from a trip to Germany:

File	Value
munich.txt	`c6596b360ac97889c4f2d68ba6787f92`
compress.py	`72eab63334dcd0f73418e32999b71f05`
cathedral.png	`55fd5b1d42072955e15769b55a390400`
oktoberfest.png	`deb345aea6cdb82ca4636c0811c292df`
street.png	`f1ea1beaa6a838d16b4d457c6fe68fd0`
wursten.png	`13c85b20b6b1e481a32700f26818333e`
snow.bmp	`a6e56c4d34d9a541b622b74c954c3fc9`
online_banking.zip	`b3baa737b818db4f52a681f0cf8d440c`

Your task is to analyze these artifacts and search for 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 26^{th}. Until then, you must upload to Fenix a compressed zip file containing three 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.
- **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 five hidden secrets in the provided artifacts. The secrets were hidden using some of the techniques that were introduced in the theory classes about file forensics and steganography. You can begin your examination by applying the "strings" tool to the collected files.

Good luck!