INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

FOOTBALL LEAKS – Stage I

2021/2022

nuno.m.santos@tecnico.ulisboa.pt

Introduction

You will be helping in the investigation of a case entitled “Football Leaks”. This investigation will be conducted in three progressive stages, each of them guided by an independent lab assignment. This document provides an overview of the case and describes the first assignment. This exercise will help you gain hands-on experience on 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

Charles Daniels is an investigative reporter that is famous for breaking controversial stories on sports. Recently, he made a post on his blog claiming that Levy Fran Velucci has been involved in a fraudulent transaction of James Santos, a rising star football player that was transferred to Red Hawks Football Club in the last season. Mr. Velucci has been the president of the club for nearly 20 years. In his blog post, Mr. Daniels claims to have documentation in his possession proving that Mr. Velucci has financially damaged the club in said transfer by diverting 3 million euro worth into his bank account.

This blog post caught the attention of a prosecuting attorney (ministério público) who has been investigating Mr. Velucci for several years now as a suspect for several crimes of embezzlement against the club. In an attempt to follow this new lead, the prosecuting attorney obtained a warrant and instructed the police authorities to search Mr. Daniels’ household to look for potentially incriminating documents and tracing their source. The police authorities followed suit and started an investigation. You were hired to lead the forensic task force looking for relevant digital evidence.

The first responding officer found several pieces of equipment in Mr. Daniels’ residence, amongst which a pen drive. The following files were extracted from this pen drive (these files can be downloaded from the course website in Course Material > Lab assignments):

File	MD5 Value
SNA_Football_Lyrics.mp4	`7083c363444daa3b0eb391443320ecd8`
chants.zip	`1b78c24f64322c51f181e6ac5ec97bc6`
daft_punk.gif	`5305480b1832ad42698bdf91f8c2c8e1`
discovery.jpg	`8331798d0e376a5336fe6838174e74e8`
hbfs.wav	`ab7ad5f3427854429ac3a4574197ae0b`
homework.jpg	`8963c92d2f964492ed1c7e9138849ad9`
ram.jpg	`5c766ce1155a907627355633a9f61340`
ticket.jpg	`d8bdf6c05594548670f5cceda02fded2`

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

1. Do you find any traces of the documents that Mr. Daniels claims to have in his possession? Present your findings explaining the procedure you followed to retrieve these documents.

2. In case you found any relevant documents, what can you learn from them at this point? Do they support the original hypothesis of Mr. Velucci’s fraudulent actions put forth by Mr. Daniels?

3. From the analysis of all provided artifacts, what else have you learned? Present every interesting insight you may have gained, e.g., about the potential identity of involved stakeholders, sources of leakage, skill level of the individuals responsible for the leakage, etc.

4. Based on your findings, suggest the next steps you would take to pursue this investigation.

Deliverables

Write a forensic report that describes your findings. The deadline for this work is October 15^{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 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 5 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.

Good luck!