
# INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA


## FORENSICS CYBER-SECURITY

MEIC, METI

# Lab Assignment II

## FOOTBALL LEAKS – Stage II

2021/2022


nuno.m.santos@tecnico.ulisboa.pt

# Introduction

In this second assignment, your job is to continue the investigation of the "Football Leaks" case. In the first stage (see Lab Assignment I), you were given the task to obtain evidence about potentially incriminating documents against Mr. Levy Fran Velucci by analyzing the files contained in a pen drive that was found in Mr. Charles Daniels' home. This second assignment will be focused on trying to explain how these documents have been obtained by analyzing hard disk images. To solve this exercise, you will need to develop your skills in file forensic techniques and tools. The digital artifacts required for this second assignment are available on the course website. As in the first assignment, we suggest that you analyze them using the Kali Linux distribution on a forensically sound virtual machine.

# Scenario presentation

As part of the forensic team that was responsible for locating relevant documents involving Mr. Levy Fran Velucci, your first task has been fruitful. Remember that your goal was to look for these documents by analyzing a set of files extracted from a pen drive located in Charles Daniels' home; Mr. Charles had reported on his website about being in possession of evidence of fraudulent conduct by Mr. Velucci damaging the Red Hawks Football Club. Interestingly, by analyzing the pen drive's files, the following "Football Leaks" documents have been retrieved using various steganalysis techniques (can be downloaded from Course Material > Lab assignments enclosed inside file lab1_secrets.tar.gz):

| File | MD5 Value | Description |
|---|---|---|
| f1.pdf | `33bd1f8ed5f5692c5bf1e5a87d6110b2` | Bank statement |
| f2.pdf | `e02839232a2283ac0843de8ecfc980a0` | Red Hawks FC statement |
| f3.pdf | `f0882eedb95122f39e692a9397c1f5c5` | Red Hawks FC internal document (Board of Directors) |
| f4.pdf | `2be65457105ca324381952538fc94de7` | The Hawks supporters' statement |
| f5.pdf | `44d015d11ecd0ec4ecaa6cb350032d17` | James Santos's player stats |

The authorities have then decided to further investigate i) how these documents have been obtained, and ii) who was responsible for collecting them. Unfortunately, when interrogated by the police, Mr. Daniels refused to collaborate and to disclose any meaningful information, claiming his lawful right to protect his sources. He also refused to reveal the identify of the pen drive's owner; the serial number of this pen drive is 43F34AAD. Your team was then tasked to procure additional digital evidence from Mr. Daniels' residence, where two computers were found: a *workstation* and a *backup server*. These computers were connected to the Internet via the local network. An agent seized both computers and created two forensically sound images of the hard disks, storing these images in the following two artifact files (these files can be downloaded from the course website under Course Material > Lab assignments):

| File | MD5 Value | Description |
|---|---|---|
| charlied_disk.tar.gz | `4619c51a85bcf01a0cab197d4d1192e2` | Hard disk image of Mr. Daniels's workstation |
| backup_disk.tar.gz | `0a4f41069e2aff2250536f5950b9a9f4` | Hard disk image of Mr. Daniels's backup server |

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 Football Leaks files on Mr. Daniels' computers?
2. If so, can you track the source of these files and how they have been manipulated over time? Establish a timeline of relevant events.
3. Do you find any evidence of anti-forensic activity?
4. What can you tell about the identity of the person(s) involved in the leakage of the files?

## Deliverables

Write a forensic report that describes your findings. The deadline for this work is October $29^{th}$. 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 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.

Good luck!