INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment II

FAKE NASA – Stage II

2022/2023

nuno.m.santos@tecnico.ulisboa.pt

Introduction

The goal of this second assignment is to continue the investigation of the "Fake NASA" case. In the first stage (see Lab Assignment I), you were given the task of looking for evidence of classified documents stolen from NASA by analyzing the contents of a pen drive in possession of Prof. Carl Seagal. In this second assignment, the objective is to investigate how these documents have been obtained by analyzing hard disk images. To solve this exercise, you will need to develop your skills in file system forensics. The required digital artifacts 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 analyzing the contents of the pen drive located in Prof. Seagal's residence, your first task has been fruitful. By analyzing the pen drive's files, your team has managed to retrieve several relevant documents (listed below) using various steganalysis techniques (you can download these documents from Course Material > Lab assignments > lab1_secrets.tar.gz). Remember that this raid was originally motivated by a Twitter post where Prof. Seagal had claimed to be in possession of "irrefutable evidence" that NASA's moon landing mission was a hoax.

File	SHA-256 Value	Description
f1.jpeg	15d41c98cba533dd7c9703409109d72c53bec3d85b20e687fe86c464caebf6b5	Raymond Polanski's Polaroid
f2.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da	Nevada site blueprint
f3.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480	Buzz Aldrin interview
f4.png	d330090e25b709aa1a9cdb28d60b103218aeeb470ecaa2df461157297a4a6444	Poor workmanship report
f5.pdf	73a6b01845a1365e3f9a6f48fdf93651f0efc07575ce1a89c5f32e01babf20ec	Top Secret document
f6.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872	Nixon's letter

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, Prof. Seagal refused to collaborate and to disclose any meaningful information, claiming his lawful right to protect his sources. He also refused to reveal the identity of the pen drive's owner; the serial number of this pen drive is 14C0F244AF16F6. Your team was then instructed to procure more digital evidence from Mr. Seagal's 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	SHA-256 Value	Description
carl_disk.tar.gz	0efab63905dabf98ffeeb7f4e26ff1607250de2e622286081d82255232f91adc	Workstation image
backup_disk.tar.gz	753906aa979443e2702bef31c65528ce95bf0c86fafc6c8468a85fcf3254087c	Backup server image

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 Fake NASA files on Prof. Seagal's 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. You have until October 21st to solve this exercise and upload to Fenix a compressed zip file containing three pieces:

- **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.

Good luck!