INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment I

FAKE NASA – Stage I

2022/2023

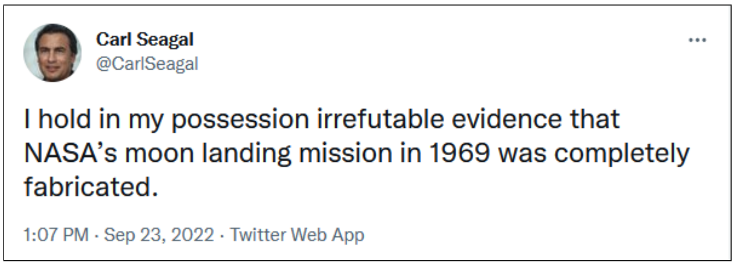
nuno.m.santos@tecnico.ulisboa.pt

Introduction

You will be helping in the investigation of a case entitled “Fake NASA”. 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 in 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

Prof. Carl Seagal is a famous astrophysicist from MIT. Recently, he made the following post on Twitter:



Carl Seagal
@CarlSeagal

I hold in my possession irrefutable evidence that NASA’s moon landing mission in 1969 was completely fabricated.

1:07 PM · Sep 23, 2022 · Twitter Web App

Figure 1: Twitter post published by Prof. Carl Seagal.

A few days later, supported by a search warrant, the FBI stormed into Prof. Seagal’s house with the purpose of determining whether he had access to classified information stolen from NASA and, if so, try to discover how it has been obtained. Prof. Seagal could face serious charges of crimes against national security. You were then hired to lead the forensic task force looking for digital evidence.

The first responding officer found several pieces of equipment in Prof. Seagal’s 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	**SHA-256 Value**
Corrupted.pdf	`e1f290cbb84a0fad81b02a7a6f5b75e33e4e3ff8cb5482b852cfb6bb38559b65`
Dog.png	`ae38b06e6b1a41ea87e5316d0c36556c18c1d225dff29e8d89cbf4d30ea273f1`
Ice.mp4	`7f7189b258d01e0f159a9288d5b988e4f609a4cca3c6ce4f7d0325be321ff758`
MIT.png	`f64ffd78760dca2c86bf890fa06d68db88de496226b0eff5a5a3c7e5d46400ec`
Relativity.gif	`79f31f1311f921237725cefb35ee3e1d8df928448a0ae6eef0af90a436cda2c9`
Sports.zip	`fbc272a65193271a7e5f62dea892890a0f9c8f9173821e4bdcb69701a29d8f4c`
Static.jpg	`6bbbf0e01bbc20af419161b00a0511bb6e130c4f25fb6a35c3e51a8953f3e545`
TCOS.txt	`777ae8a7e76068c79bdbf4119619544e1d9ac6a3a59835ea35e4dfc330af288b`

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

1. Did you find any traces of relevant documents that Prof. Seagal is probably relying on to support these claims? Present your findings explaining how you retrieved said documents.

2. If you found any relevant documents, do they support Prof. Seagal’s thesis that NASA’s moon landing was fake? Based on these documents, suggest how Prof. Seagal explains how the moon landing event occurred and why these documents constitute “irrefutable evidence”.

3. From the analysis of all provided artifacts, what else have you learned? Present additional insights that you may have gained, e.g., about other involved stakeholders.

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 7^{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 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.

TIPS: There are in total 6 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!