|  |  |
| --- | --- |
| C:\user-pjpf\Briefcase-SO\so\so-12-13\slides\logo-IST-Tecnico.JPG | INSTITUTO SUPERIOR TÉCNICO  Departamento de Engenharia Informática  Forensics Cyber Security  MEIC / METI 2022-2023 – 1st Period |

Digital Forensics Report

**Authors**

**Francisco Sousa ist**

**Miguel Porfirio ist**

**Sara Aguincha ist195674**

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

Going through the files extracted from the pen drive, **we found 6 relevant documents**.

![A picture containing text, outdoor

Description automatically generated]()After analyzing each file the pen had, we decided to start examining each image. Doing so, the **Dog.png** was visibly suspicious due to its weird sky color saturation. Assuming it were a LSB type of steganography we ran the **lsb.py** script. After some tries we ended up finding that the 6 Least-Significant green bits were hiding a jpg image.

Text, letter

Description automatically generatedThere was also other image we thought it had a weird pigmentation. In fact, the **Schedule.png** also had something hidden in itself. After extracting the 6 Least-Significant red bits (using the same script) we recovered a png image.

Diagram, engineering drawing

Description automatically generatedAfter all the images were carefully inspected we moved to the other files. When investigating the **Relativity.gif**, we noticed that it had something on it's metadata (comment). Running the command “*exiftool -b -comment Relativity.gif > Relativity.zip*” on the terminal we obtained a zip that when extracted had the following image.

Text, letter

Description automatically generatedWe then moved to the Golf file. When using the exiftool, it said that was a JPG file with a **163 byte** unknown header. Since the problem was the header we decided that we should inspect it further, and by using the <https://hexed.it/> (a website that is a hex editor) we could finally see the header. With the first (ver os hexadecimals e colocar aqui) part of the header we concluded that instead of a JPG with extra unknown header it was a PDF file with some part of its header missing. When complete, the PDF was repaired.

# 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''.

We have found 6 different documents (provided in the zip file).

In the artifact obtained from the Golf file, the obtained PDF appears to be a classified document from February 1st 1969 (about 5 months before the Moon Landing). This document accuses Raymond Polanski and President Richard Nixon of being involved in the staging of the Moon Landing.

In the artifact obtained from Dog.png, a jpeg image showing off what appears to be a polaroid photograph of the first Moon Landing was obtained , with the caption “Taken with my Polaroid Land Model 350 in the Nevada Filming Facility” handwritten.

In the artifact obtained from the Relativity.gif, we acquired a png that seems to be a map of the “Nevada Filming Facility” referenced before.

In the artifact obtained from Schedule.png, yet another png was discovered. This one had a thorough report about how useless and careless all the staff was. It mentioned “people sleeping on the job...” and “...coming to work…with alcohol in their system in excessive amounts”. The author then concludes that there was no way that man reached the moon with people working like that.

In the artifact obtained from Sports.zip, we found a video file, which shows an interview with astronaut Buzz Aldrin where he states that “...it didn’t happen, it could have been scary…” when supposedly referring to the moon landing, which further supports Prof. Seagal’s thesis.

In the artifact obtained from Corrupted.pdf, there was an encrypted pdf that shows a handwritten letter by President Richard Nixon to his grandson in August 9th 1990. In the letter, the president confesses to his grandson his biggest secret, “...the falsification of the Moon landing …” “... film fake but believable footage in the Nevada Desert”. He then proceeds to ask his grandson to “...please consider burning it so that no traces of this get left behind”.

The Falsification plan (TOP SECRET file), combined with the polaroid photo, the Nevada Filming Facility, the report of someone who was not involved in the plan, the Buzz Aldrin statement and the confession on the President Richard letter seemingly points to the fact that the moon landing was fake, as stated by Prof. Seagal.

# 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.

- nao algo assim muito grande

-quem sao as partes envolvidas, e como estao envolvidas

- 1 ou duas frases para cada pessoa

- se tinha capacidade para conseguir os ficheiros (prof seagal)

- a validade dos artifactos em tribunal

- se ha algum caminho para validar os artifacts

- legal network of each one

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

-> assumir que temos a lead

-> por que caminho seguiamos (tipo validar provas/invalidar) (((FOI O QUE O STOR QUE SUGERIU)))

-> mandatos etc (maybe, se acharmos necessario ig)

Can also attach appendices, e.g., displaying relevant evidence, timelines, etc.