|  |  |
| --- | --- |
| 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 ist195579**

**Miguel Porfirio ist195641**

**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.

A person wearing a suit and tie

Description automatically generatedBefore discovering the artifact in the Golf file we also ran the exiftool on the **Sports.zip**. While doing so we found a weird comment that stated “ …**BuzzAldrin.mov**…”, but there were no file with that name when the zip was extracted. We thought that the zip file might be somewhat corrupted and to try to repair it we used a repair tool from **WinRar**. After the repair the video **BuzzAldrin.mov** was found among the other files.

Lastly we tried to understand how to decrypt the **Corrupted.pdf.** We ran the exiftool but we didn’t find anything out of ordinary. We then opted to see what the data looked like, doing an hexdump we found ourselves with a string (and encrypted). There was nothing we could get from the header so we looked for some clue on the footer. The only clue was that instead of an EOF there was a “**==**”, this two symbols together made us recall a well-known encrypt method, **base64**. Using the command “*less Corrupted.pdf| base64 --decode > Corrupted.bin*” on the terminal we obtained the decoded version (binary).

We hexdumped once again to see what was in the new evidence. The header of the file had a **tiny url** (<http://tiny.cc/7o2d6LuDVNSd>) that lead us to a dropbox file called **tool.** We ran the file tool, and got the output tool: **python 3.7 byte-compiled** which led us to know that this was a compiled python file (**.pyc** extension). As we needed the actual script we created a new file named **tool.py** and decompiled with the command “*decompyle3 tool.pyc > tool.py*”.

Finally we only had to make a script to test out every word as a password, [**tool\_bruteforce.py**](https://github.com/franciscomcsousa/CSF2223/blob/main/csf-project1-artifacts-altered/tool_bruteforce.py). After having tested on the **TCOS.txt** file without any hits, we copied the lyrics of **Ice.mp4** onto a text file and then ran the script on it. By doing so, we found that the word '**poisonous**' was the key to decrypting the pdf file, which upon being decrypted revealed the last hidden document, a pdf file [**Corrupted\_Decrypted.pdf**](https://github.com/franciscomcsousa/CSF2223/blob/main/csf-project1-artifacts-altered/Flags/Corrupted_Decrypted.pdf).

Text, letter

Description automatically generated

# 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.

We have found that there were some involved parties in this theory. The first and most important one is former US President Richard Nixon (president at the time of the moon landing) from whom we have gathered a letter to his grandson pertaining to the fact that the moon landing was fake. The other one is Raymond Polanski who, according to the artifacts we found, directed the moon landing footage in the Nevada Filming Facility and took a picture of the event during the filming.

As to whether Prof. Seagal had the ability to obtain and possess such files or not, it is our belief that it’s highly unlikely he had the permission to get said files. We don’t know how he obtained these files and have no means to prove their authenticity, so whether or not they are valid in court is up to the Judge of this case.

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

The first thing that should be done after obtaining these hidden artifacts is to analyze them in order to understand if they contain classified information or not.

After analyzing these artifacts, the forensics team should meet up and decide whether or not it’s justified to ask a Judge for another search warrant in order to obtain more information that might be classified and is in the hands of Professor Seagal.

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