|  |  |
| --- | --- |
| 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 Porfírio 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**.

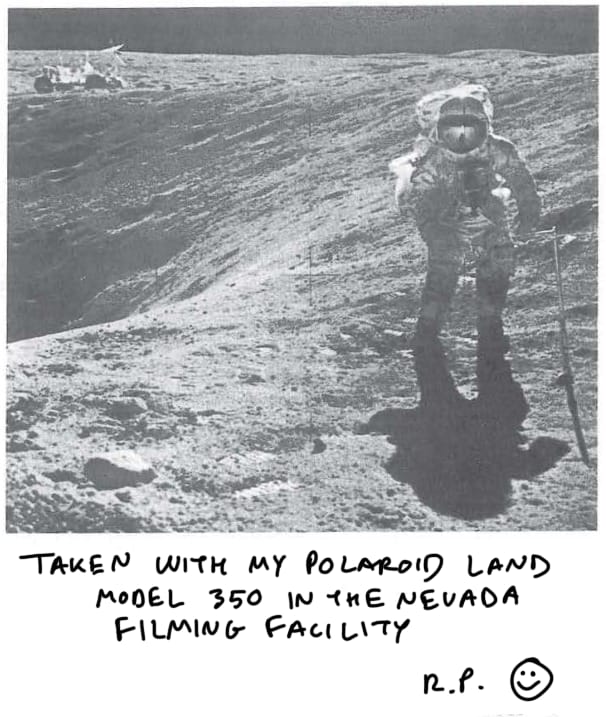
After analyzing each file, we decided to start examining each image. Doing so, **Dog.png** was visibly suspicious due to its weird sky color. This led us to believe that a file might have been hiding in the least significant bits of one of the image colors (R, G or B). With the help of https://stegonline.georgeom.net we were able to analyze the image’s bit planes and fount out that the 6 least significant bits of the image were hiding something in the top of the image.

A picture containing text

Description automatically generated

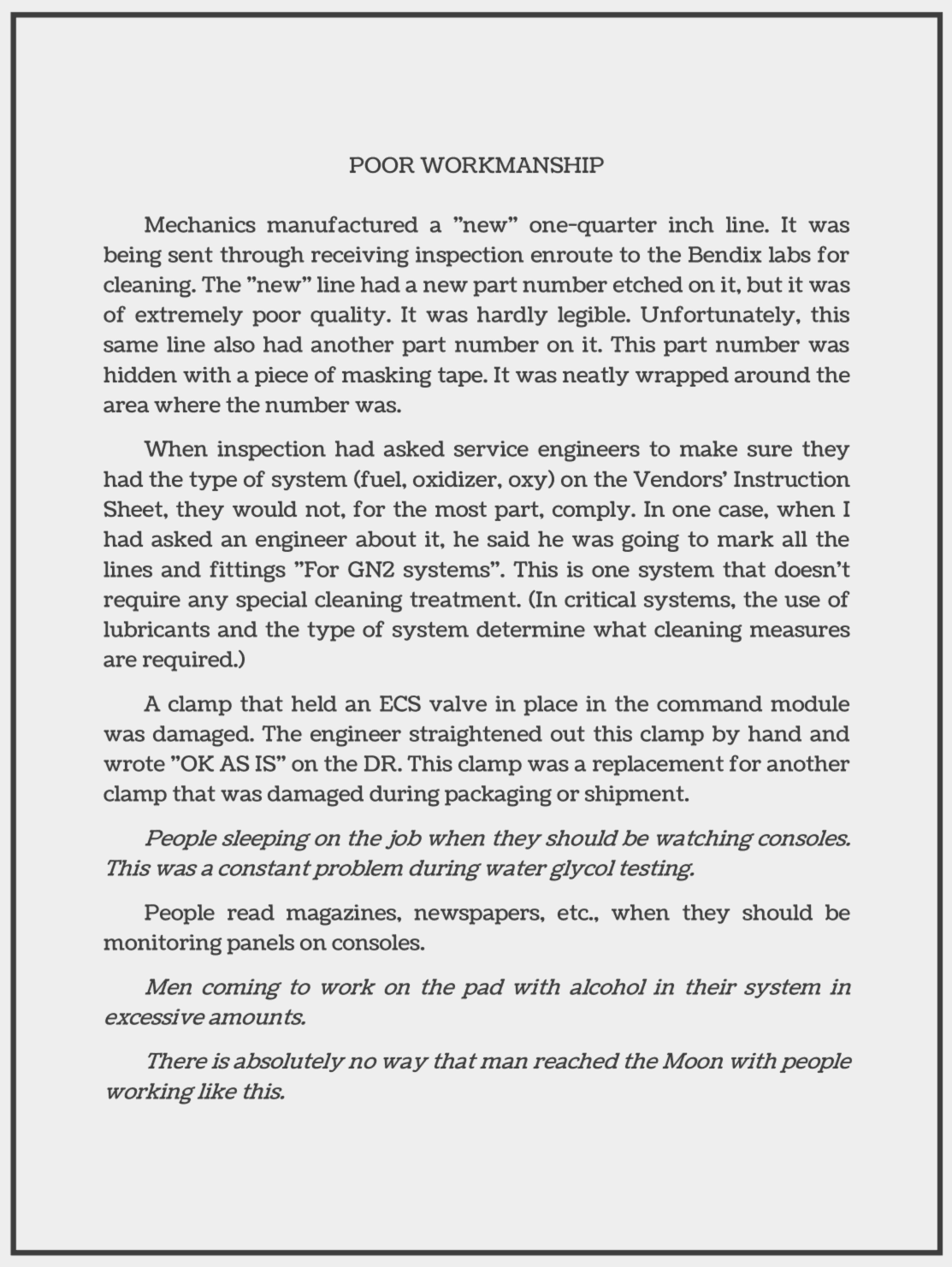
*Figure 1 - Bit Plane of the 6th least significant bit*

After finding the LSB where a secret file could be hiding, we ran **lsb.py** in order to extract the hidden information, this gave us the hexadecimal values of the file and after reverse hexdumping the file, we found out it was a jpg file because of its header.



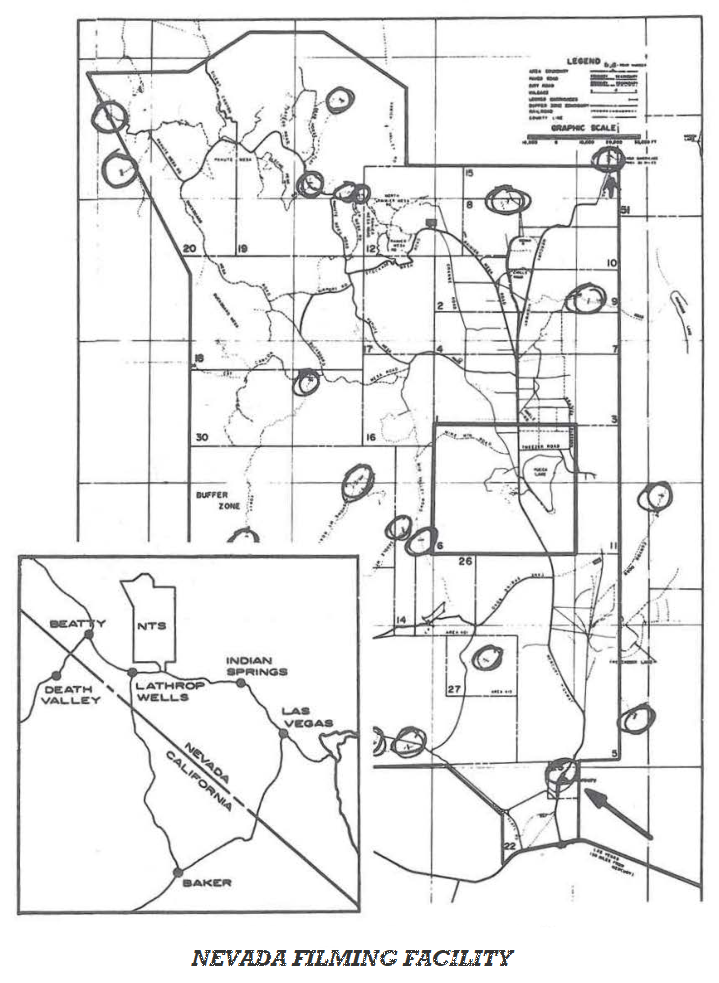
*Figure 2 - First hidden artifact*

**Schedule.png** was also another image that had some weird artifacts. Using the same process as **Dog.png**, we were able to find out that there was some hidden data in the 6 LSB of the red color space. Using the same script as before, we were able to retrieve the file, though this time its signature pointed to it being a png file.



*Figure 3 - Second hidden artifact*

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



*Figure 4 - Third hidden artifact*

Then we moved to the Golf file. When using exiftool, it showed a JPG file with a **163 byte** unknown header. Since the problem was the header, we decided that we should inspect it further, by using <https://hexed.it/> (hex editor) we could finally see its header. With what we had of the header we concluded that instead of a JPG with an extra unknown header, it was a PDF file with some part of its header missing. When completing the header, the PDF was repaired.

Text, letter

Description automatically generated

*Figure 5 - Fourth hidden artifact (screenshot of pdf)*

We also ran exiftool on **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. After hexdumping the zip file, we also found out more references to **BuzzAldrin.mov.** We thought that the zip file might be corrupted. In order to repair it we used a repair tool within **WinRar**. After repairing it, the video **BuzzAldrin.mov** was found among the other files.

A person wearing a suit and tie

Description automatically generated with medium confidence

*Figure 6 - Fifth hidden artifact (screenshot of video)*

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, the file has the appearance of a text file with only ASCII characters. There was nothing we could get from the header so we looked for some clue on the footer. The only clue was that there was a “**==**” at the end, this two symbols together made us recall a popular encoding method, **base64**. Using the command *less Corrupted.pdf | base64 --decode > Corrupted.bin* we obtained the decoded version (binary file).

We ran hexdump 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 *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 decompiled the file with the command *decompyle3 tool.pyc > tool.py*.

We then made our own script **tool\_bruteforce.py** which iterates through every word in a text file and checks if any of them is the password needed to decrypt the Corrupted.pdf file. After having it 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 revealed the last hidden document.

Text, letter

Description automatically generated

*Figure 7 – Sixth hidden artifact (screenshot of pdf)*

# 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.