INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2022-2023 – 1st Period

Digital Forensics Report

Afonso Lopes - 95526

Eduardo Claudino - 95567

Mª de Fátima Campos - 95629

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.

Artifact “1_Polaroid.jpg”: We found this artifact by analyzing “Dog.png”. A first look at this image and we can already notice the effects of banding meaning there is something hidden. With `zsteg`, we listed all the hidden files in the png and found an “Open PGP Secret Key”. However, this turned out to be a false positive. But in this list we also found a hidden jpg. We extracted this image and retrieved the “Polaroid” document.

Artifact “2_Poor_Workmanship.png”: We found this artifact by analyzing the hidden files in the artifact “Schedule.png” in the Sports folder. We used `zsteg` once again and retrieved the “Poor Workmanship” document.

Artifact “3_BuzzAldrin.mov”: We found this file while analyzing the artifact “Sports.zip”. Using `binwalk` we noticed that there was a mov file that wasn’t being extracted. In order to extract it we fixed the zip using the command `“zip -FF sports.zip –out sportsfixed.zip`” which made us able to retrieve the “BuzzAldrin” video.

Artifact “4_merged.jpg”: We found this artifact by analyzing the “Golf” file. First we tried looking at its magic numbers to check if it was corrupted and could be fixed by using an hex editor but this did not work. By using the `strings` command we could see there was some information regarding images in the beginning of the file so we suspected there could be something hidden. We then used `binwalk` like we had used on “Sports.zip” to extract the files contained in “Golf”. `Binwalk` gave us a list of JPEGs, so we knew there was indeed something relevant hidden in that file. However, `binwalk` only managed to extract some .zlib files and a text file, we did not get the images. To do so, we discovered there was a stronger `binwalk` command that ignored the file type and extracted everything: `binwalk --dd =’.*’ Golf`. This way, we managed to extract pieces of a jpg which we then pieced together thus retrieving the document “merged.jpg”.

Artifact “5_Uncorrupted.pdf”: We found this file while analyzing the artifact “Corrupted.pdf”. Our initial thoughts were that the file could indeed be a corrupted pdf, and so we tried to fix it by changing the magic numbers so that it matched those expected for a pdf file. We had no success, but when we opened the file in `hexdump` to analyze it, we realized that the file was composed entirely of ASCII characters. We then realized that it only contained characters which are used in base64 encoding, so we went ahead and used `base64` utility to decode it to “Corrupted_decoded.pdf”. We tried to open the file as a PDF again, but with no success. We then opened the file in `hexdump`, where we found that at the start of the file there was a link to a Dropbox folder. We followed this link, and downloaded another artifact, “tool”. We then ran the file command, and discovered that it was a byte-compiled python program. We tried to execute the “tool” in a safe environment, but python was exiting with an error. We then used `decompyle3` to disassemble the python file, and we managed to retrieve the source code, “tool.py”. After analyzing the source code of “tool”. we discovered that it is used to encrypt/decrypt files, presumably “Corrupted.pdf”. We also discovered that the hash of the password was located in the beginning of the file (bytes 0x40 to 0x80), but since the hash was done multiple times (25,000), we could not use a standard tool like `john the ripper` to bruteforce it. So, we created a modified version of “tool.py” to allow us to bruteforce the password using a dictionary attack. Since we hadn’t found any use for the file “Ice.mp4” up until then, we used the lyrics as a wordlist (we got the lyrics from the internet, and run `lyrics_parser.py` to get a list of used words). We then run the script `bruteforce.py`, and discovered the password to be ‘poisonous’. We promptly used it to decrypt “Corrupted.pdf”, which gave us the 5th evidence, “Uncorrupted.pdf”.

Artifact “6_Nevada.png”: We found this file while analyzing the artifact “Relativity.gif”. When analyzing this file with `binwalk` we found a corrupted zip and a png with no size. We therefore thought that we needed to somehow uncorrupt the zip in order to open it and see what was inside, however, this turned out to be fruitless as it seemed the zip had no way to be fixed. This was when we started trying new things, and when analyzing the gif with `exiftool` we found that there was a lot of data hidden in the metadata of this gif. We quickly made a python script in order to extract this hidden data and it turned out to be a zip file we named Metadata. Using `binwalk` on this zip file we were finally able to extract the “Nevada” picture.

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''.

The documents found do indeed support Prof. Seagal’s hypothesis that the moon landing was fabricated. According to these documents, the Americans were losing the Space Race amidst the Cold War in the eyes of the public (despite the recent successes on Apollo 8 and Apollo 10 mission) so the solution for this problem was to assert american dominance over the soviets by stepping on a celestial body like the Moon. However, the technology needed to accomplish such a feat was at least 5 years away from being developed. So, the shooting of the moon landing on Earth was approved. The production was conducted in a filming facility in the Nevada desert as it is supported by the polaroid and the map of said filming facility. The workmanship during production was also very poor, having people sleeping on the job instead of watching consoles, men coming to work with alcohol in their system, and even valves which were damaged. These working conditions would make it impossible for man to reach the Moon, given how accurate and disciplined space exploration needs to be. There is also a video of apparently Buzz Aldrin, the second man to land on the Moon, saying “It could have been scary, but it didn’t happen”. Prof Seagal assumes he was talking about the Moon, meaning the astronaut denies ever having landed on it. The final piece that ties it all together is the letter of Richard Nixon, the President of the United States at time of the Moon landing, to his grandson Christopher admitting he gave the order to film the Moon landing in the Nevada filming facility and also explaining how he did it for the sake of his country, which was losing the Space Race. With all this information, Professor Seagal concludes the Moon Landing must have been fake, and that these documents constitute “irrefutable evidence”, since some of them are signed by the people involved and are allegedly classified documents that were not meant to be disclosed to the public.

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.

We have learned that, according to these artifacts, President Richard Nixon was the one who orchestrated and approved the filming of the Moon landing due to the insights provided by the Pentagon analysts. We also discovered that Raymond Polanski was the film director, in collaboration with NASA experts, and that Buzz Aldrin appears to admit that the Moon landing was faked. We have also learned about the reason behind this alleged faked Moon landing: that it was due to the tensions between the USA and the Soviet Union during the Cold War, in which the Space Race was a main factor, the location of the filming was in Nevada and there were poor work conditions with people sleeping and drinking on the job, the polaroid was taken with a model 350 camera, the document issuing the fake Moon Landing was written in 1st of february 1969 and Richard Nixon's letter was written in august 9th 1990.

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

After extracting all the evidence (both inculpatory and exculpatory), we should perform the temporal, relational and functional event reconstitution (if we're following the Kruse model). Then we should document the case. We should start with general case documentation, presenting contact information and legal authorizations and compile all the first response documents. Then move on to procedural documentation in which we explain every task performed, the steps taken, the tools we used to extract the files and an analysis in detail of the data. We also need to make sure to make a record with all external documentation used in the process (like user manuals for the tools we used) and to create a case timeline, to have an idea of the times the events took place (in this case in particular we don't have any specific dates except for the letter in 1990 and the moon landing in 1969 but we can have a general idea of the times in our case timeline).

Assuming the steps before were correctly done, we now have in our possession admissible evidence. The next step is to report back to the authorities responsible for the investigation and wait for trial to present our findings and give an expert testimony in which we explain the concepts of forensics in a simple manner for the judge/jury to understand the results of the investigation we conducted.

Throughout these steps (and the whole investigation) we should not make any assertions of innocence or guilt because this is the judge/jury's job, not ours.

Appendix A - Evidence Artifacts

Artifact	SHA-256 sum
1_Polaroid.jpg	4d10bcbe31a17c866b305750685d87878bb58fa68dc934440b528f9796642a65
2_Poor_Workmanship.png	4bfd97afe8a1d510e84a52094d888bc8907f643f5793b6d259260505d33920f4
3_BuzzAldrin.mov	bc8a2d12aa1e8f280294a7b413612e739927b789181c826c30cbe2b460513480
4_1_12DAF8.jpg	241ed2062371ea8459024a4e3428f37566c128700d282c63f1bcc143a853faf0
4_2_F0D0C.jpg	862520a510711ee671ae2c943cbe6ebe2ad3a75c21c9af65e44e62a798396924
4_3_A5DEF.jpg	f65e6b8147411b75eb4c4b043bfa1fe812f7b33b6d6a3c41ead9d154facda790
4_4_58221.jpg	83744c406105e6ec230257e4fdae751034f2b12f9c2115f0010b35ab4e986a00
4_5_1B86D.jpg	37fb55e63272b7f7e8db0f2cc9ccfcfce28c3055795cb77bfbc725bead6847a7
4_6_A3.jpg	20dca4c7746f6bbcf687d25d2a464b35435107827307ba4b884164c57c6d7c12
4_merged.jpg	c89f6c029e721e01521c746aa600024581cc1a1f9ca681f3164f9a7177a27307
5_Uncorrupted.pdf	631fb4c4aadc6ca3f46310466974c85d9ab226e6617096eb0206a22b6fbd5872
6_Nevada.png	4ec286d1b6fbb9466d1f68dcdd6d248441645be85be6f4bf0365f068060486da