INSTITUTO SUPERIOR TÉCNICO
Departamento de Engenharia Informática
Forensics Cyber Security
MEIC / METI 2024-2025 – 1st Period

Digital Forensics Report Lab1

Group number:	35	Name	IST Number
Student 1:		Rodrigo Leal Saraiva Ganância	103809
Student 2:		Pedro Miguel de Melo Ribeiro	102663
Student 3:		Diogo José Almeida Rodrigues	102848

1. Acquired artifacts

Name	Type	SHA-256 Value
best-intro.pdf	pdf	c3ea6b775dd7eaecebeef00e5523483d182602118ff6de0eb3d6a41b8f43c42f
blank.pdf	pdf	55bd8016769dc421ba0c87e1c657477b00893e1194fc447cd20147b5438a39f5
galaxy_text.txt	txt	03566817f143262cd35c6c518ab303bd3127c62f2f011301fba9e227be438ecf
nmap.txt	txt	bfe6869955ed21e77bb510ea140b00ae2986cd6d08c7bf6f99c8aa2b8d20755a
tagus_extracted_image.png	png	b2e5a9075255cbd022f28fec2c04d09579ca6a96984677a303ee99e4d8ef4696
wallpaper_extracted.pdf	pdf	04c099abe319fe6dd90c420161b64523c0332905332640213eceea3f205500c8

2. Report of all findings

2.1. best-intro.pdf

During our investigation, we ran the command ‘strings best-intro.wav | less’ to examine the printable characters within the audio file ‘best-intro.wav’. Towards the end of the output, we identified content suggestive of a hidden PDF file. To further explore this, we ran the command ‘strings best-intro.wav | grep pdf’, which revealed two lines referencing a file titled "bankstatement.pdf". Based on this finding, we copied the file and renamed the file extension from .wav to .pdf to try to access the concealed data. This approach successfully uncovered a hidden PDF document, which contained sensitive financial information of a bank account under the name "Virgolino Gonçalves".

Within the statement, two notable high-value transactions were identified:

- A credit transfer of $33,000 on 05/01/2024 from an entity named CE.LTA
- A payment of $28,000 to MOBICARE for an item labeled MKU-2784

2.2. nmap.txt

Initially, the nmap file appeared to be an ELF (Executable and Linkable Format) file. Upon analyzing it using the command 'cat nmap | less', we observed text patterns, following the first few bytes, that resembled Base64 encoding. Suspecting that the file contained encoded data, we copied its content into a new file and proceeded to remove the initial non-Base64 characters which contained the ELF magic bytes. To further investigate, we decoded the content from Base64 to hexadecimal format using the command: 'hURL -b -f nmap_text.txt > nmap_hex.txt'. Next, the resulting hexadecimal data was converted to ASCII using: ' hURL -x -f nmap_hex.txt'. This process ultimately revealed text containing usernames and password credentials belonging to IST members.

2.3. thrones.pdf & myzip.zip

During our investigation, we analyzed the contents of the thrones.pdf file, which contained a translated novelette in High Valyrian—a fictional language from the "A Song of Ice and Fire" series and its television adaptation "Game of Thrones". The title of the novelette was "The Rogue Prince, or, a King's Brother". Upon reviewing the document, we noticed missing whitespaces and untranslated words, resulting in unusual and elongated terms. Suspecting these unusual words might serve as a potential password, we attempted to crack the password for myzip.zip, which was found among the student's artifacts. We began by extracting the ZIP file's hash using the command: "zip2john myzip.zip > myzip_hash". To use the strange words from thrones.pdf as a wordlist, we first converted the PDF to plain text via an online tool (https://www.pdf2go.com/pdf-to-text). Then, since the wordlist needed each word on a separate line, we formatted the extracted text by running the following command: "awk '{for (i=1; i<=NF; i++) print $i}' thrones.txt > thrones_for_john.txt". With the formatted wordlist ready, we executed the following command to use it with john the ripper: "john --wordlist=./thrones_for_john.txt myzip_hash". This process successfully cracked the ZIP file password: "zmaistangeptotlargelynaejotseda". Upon unlocking the ZIP archive, we discovered four additional files, which were then subject to further analysis.

2.4. wallpaper_extracted.pdf

Upon initial inspection of the wallpaper.png image, a noticeable banding effect was observed across the image. This visual anomaly suggested the possibility of data hidden within the Least Significant Bits (LSBs). To investigate further, we analyzed the bit planes using an online tool, Stegonline (https://georgeom.net/StegOnline/upload), and identified a distinct pattern near the top of the image, indicating potential embedded content. We then utilized zsteg, a tool designed to detect hidden data in PNG files, to search for concealed information within the LSBs. Running the following command, which tested from 1 to 7 bits, confirmed the presence of hidden data: "zsteg -b 1-7 --lsb wallpaper.png". The output revealed that a PDF file was embedded within the 3 LSBs. We extracted the hidden PDF using the command: "zsteg -E 3b,rgb,lsb,xy > wallpaper_extracted.pdf". The extracted PDF, titled "Oeira's Restaurants: Stunning Growth" (dated 05/09/2024) by Susana Santos and Ana Rita Costa, detailed the financial growth of several restaurants in Oeiras, including "A Tendinha," "O Pombalino," "A Caçoila," and "O Transmontano."

2.5. blank.pdf

We began by attempting to identify the nature of a file named "blank", which lacked any file extension. To determine its type, we executed the command: "hd blank | less". The initial analysis of the magic bytes suggested that the file might be a PNG. However, after copying the file and changing the extension to .png, an error occurred, indicating that it was not a valid PNG.

Upon further examination of the hex dump output, we noticed references to PDF structures. This led us to hypothesize that the file could be a PDF instead. After copying the file and changing it to a .pdf extension, we

successfully opened a valid document. The recovered document was the documentation for the MKULTRA Mind Control Component API (MKU-2784), which outlined methods for manipulating neural patterns and it described how the API could potentially be used to influence thoughts and issue commands on individuals.

2.6. galaxy_text.txt

By analyzing the metadata of the three images related to galaxies (andromeda.png, lactea.jpg and cartwheel.tff) with the "exiftool" command, we noticed that all of them had an unusual "User Comment" section consisting of dots and spaces. This led us to think that these patterns represented binary code, where dots (.) corresponded to binary 1s and spaces ( ) to binary 0s. We opened each file in vim and ran the commands ":%s/\./1/g" (to change the dots to 1's) and ":%s/ /0/g" (to change the spaces to 0`s). We then ran a script (text_to_bin.py) that transforms the binary words into the corresponding characters, but the resulting text for each file didn't make any sense. We thought that maybe individually the binaries didn't make any sense, but if joined could decode some type of message. Based on this assumption, we started concatenating the binaries of the files and then converting the result to text. The concatenation of order: lactea, andromeda and cartwheel resulted in a coherent text file, which we named galaxy_text.txt. This file contained logs from the MKU-2784 API and indicated that it had been used to implant ideas and encourage visits to the restaurants "A Tendinha," "O Pombalino," "A Caçoila," and "O Transmontano".

2.7. tagus_extracted_image.png

Like the wallpaper.png image, tagus.png showed a noticeable banding effect, particularly in the top left corner. To investigate further, we submitted the image to StegOnline (https://georgeom.net/StegOnline/upload) for bit plane analysis. Upon examining the Red 4, Green 4, and Blue 4 bit planes, we observed that, while the rest of the image appeared to clear up, the top left corner contained a large triangle filled with significant noise, suggesting potential hidden data in this region. After submitting the tagus.png image to the 'Extract Files/Data' section of StegOnline, no results were returned. To further investigate, we developed a custom program (lsb.py) that focused on a specific area near the noisy triangle in the top left corner. The program extracted the 5 least significant bits from the red, green, and blue components of each pixel in this region and generated a new image from the extracted data. This new image was then submitted to StegOnline in an attempt to reveal hidden information, but again, no results were obtained. We hypothesized that the order in which the pixels were read could be affecting the outcome. Initially, we had read the pixels from left to right and top to bottom, which yielded no results. Changing our approach, we read the pixels diagonally from left to right, top to bottom. This method successfully uncovered a hidden PNG file embedded within the image. The extracted PNG file contained a blueprint for what appears to be the ARIANE6 launch system along with a note indicating the location of the ISTSat-1 inside the rocket.

3. Analysis of relevant findings

3.1. Based on your analysis of the documents, did you find the stolen credentials? If so, describe how you identified them and provide details on the information you discovered.

We have successfully identified the stolen credentials hidden within the nmap file. After careful analysis of the contents of this file we noted numerous similarities with the Base64 encoding, which led us to believe that the data was encoded. By utilizing the hURL tool, we decoded the Base64 text into its hexadecimal representation and converted the hexadecimal output back into ASCII. This process revealed a series of IDs and passwords associated with IST, which supports existing rumors regarding the theft of student credentials. The information obtained from the decoded content provides compelling evidence of the unauthorized access to sensitive account information.

3.2. Did you uncover any additional concealed artifacts within the provided files? If so, explain how these artifacts were hidden and describe the methodology you used to extract them.

We uncovered several additional concealed artifacts that correlate the student with potentially unethical and dangerous activities.

- **Bank Statement:**

We identified a bank statement containing two suspicious transactions: a credit transfer from ERCE.LTA and a payment for MKU-2784, which were hidden within the intro of the “Game of Thrones” show file (best-intro.wav). To extract this information, we analyzed the printable strings using the strings command. After identifying relevant PDF data, we copied the content and changed the file extension to .pdf.

- **Restaurant Growth Report:**

A PDF document detailing the growth of various Cascais restaurants was embedded within the wallpaper.png image. We employed a steganalysis tool called zsteg to detect the hidden data and successfully extracted the document.

- **MKU-2784 API Documentation:**

We found the documentation for the MKU-2784 API, which enables the manipulation of neural patterns and the implantation of ideas into individuals. This document was concealed within a file named "blank" inside the myzip.zip archive. After successfully cracking the zip file, we analyzed its contents using the hd command, which revealed data suggesting a hidden PDF. We then copied the "blank" file and changed its extension to .pdf to access the document.

- **Log File on MKU-2784 API Usage:**

A log file provided evidence of the MKU-2784 API being used to influence individuals to visit restaurants in Cascais. To access this file, we examined the metadata of the images andromeda.png, lactea.jpg, and cartwheel.tff using exiftool and extracted the "User Comment" section. We transformed the spaces into 0s and the dots into 1s to construct binary data. After concatenating the binary sequences in the order of lactea, andromeda, and cartwheel, we utilized a Python program to convert the resulting binary data into readable text.

- **ARIANE6 blueprint:**

We extracted a blueprint that mentioned the launcher “ARIANE6”, along with the satellite "IST SAT-1." To uncover this information, we analyzed the bit planes of the image file and wrote a Python program that read the pixel data diagonally, extracting the four least significant bits from each pixel to create a new image. We then submitted this new image to StegOnline, which allowed us to successfully extract the hidden file.

These artifacts collectively suggest a connection to a range of illicit activities and suggest further investigations.

3.3. With a focus on the additional concealed secrets you recovered, analyze their content and relationships, and propose a possible interpretation of their meaning. Formulate a hypothesis regarding their significance and support it with the content of the recovered secrets. Additionally, prepare a timeline of the events as indicated by the recovered secrets.

The recovered secrets suggest that the student, possibly in collaboration with Virgolino Gonçalves, was involved in a scheme that led several people to be brainwashed into visiting specific Restaurants. Evidence includes the purchase of the MKU-2784 API through Virgolino Gonçalves’ account, as well as a log file documenting the

implantation of ideas, such as "I feel like going tonight to the restaurant 'O Pombalino' to have dinner." Additionally, a report found among the student's artifacts confirms the financial growth of these restaurants. All this points to the involvement of these two individuals in the illegal use of dangerous mental manipulation technology. The discovery of stolen credentials, combined with the ARIANE6 rocket and IST-SAT1 satellite blueprints, suggests that this scheme could be part of a much larger operation. The use of the MKU-2784 API to influence people's choices, such as dining preferences, may represent only the initial phase of a broader experiment or conspiracy, potentially aimed at testing or refining this technology for more far-reaching applications. The link between the ARIANE6 rocket and IST-SAT1 satellite raises the possibility that the student and their accomplices were preparing to deploy this manipulation technology on a larger scale, with potentially global ramifications.

3.4. Based on your findings, what recommendations would you make for the next steps in the investigation? Advise Mr. Ricardo Prado on the best course of action moving forward.

Based on our findings, we highly suggest Mr. Ricardo Prado to contact the competent authorities and recommend the following next steps:

- **Verify IST IDs and Passwords:**

It is crucial to investigate the validity of the stolen IST IDs and passwords. Mr. Prado should confirm whether these credentials correspond to actual users and, if so, determine how the student obtained this information. If the credentials are valid, the affected users should be immediately notified and urged to change their passwords. Additionally, a thorough investigation into how this security breach occurred should be conducted to prevent future incidents.

- **Determine the Purpose of the Stolen Credentials:**

It is essential to understand why the student had access to the stolen credentials and what they were intended for. Mr. Prado should investigate whether these credentials were used for unauthorized access to institutional systems, financial manipulation, or other malicious activities. This will help determine the extent of the breach and uncover any potential damage caused by the misuse of these credentials.

- **Investigate the Acquisition of the MKU-2784 API:**

Given the powerful capabilities of the MKU-2784 API, which can manipulate neural patterns and implant ideas, it is a priority to determine how Virgolino Gonçalves and João Musk obtained access to such technology. Efforts should be made to trace the origin of the API, understand its functionality, and deactivate any ongoing activities related to its use. Investigating the history and potential distribution of the MKU-2784 API is essential to curbing its misuse.

- **Investigate the Purpose of ARIANE6 and IST-SAT1 Blueprint:**

It is essential to investigate the specific role of the ARIANE6 rocket and the IST-SAT1 satellite mentioned in the blueprint. This includes determining whether these references relate to legitimate aerospace projects or if they have been repurposed for illicit activities. Mr. Prado should verify if the blueprint reflects real technical details about the ARIANE6 rocket or IST-SAT1 satellite, and assess whether the involvement of these technologies indicates a larger scheme connected to the student's actions.

- **Examine the Student's Personal Computer:**

A comprehensive forensic analysis of the student's personal computer is necessary to uncover more information about their involvement in the scheme to influence people to visit specific restaurants in Oeiras. This analysis may reveal further details about the student's role in the operation and provide insight into any additional parties involved.

- **Investigate the Restaurants' Involvement:**

Lastly, it is important to determine whether the restaurants mentioned—"A Tendinha," "O Pombalino," "A Caçoila," and "O Transmontano"—were complicit in the scheme. Investigating their involvement will help clarify whether they were aware of, or played an active role in, the illicit use of the MKU-2784 API to attract customers.

These steps will help ensure a thorough investigation and address the potential security risks posed by the stolen credentials and the misuse of the MKU-2784 API.