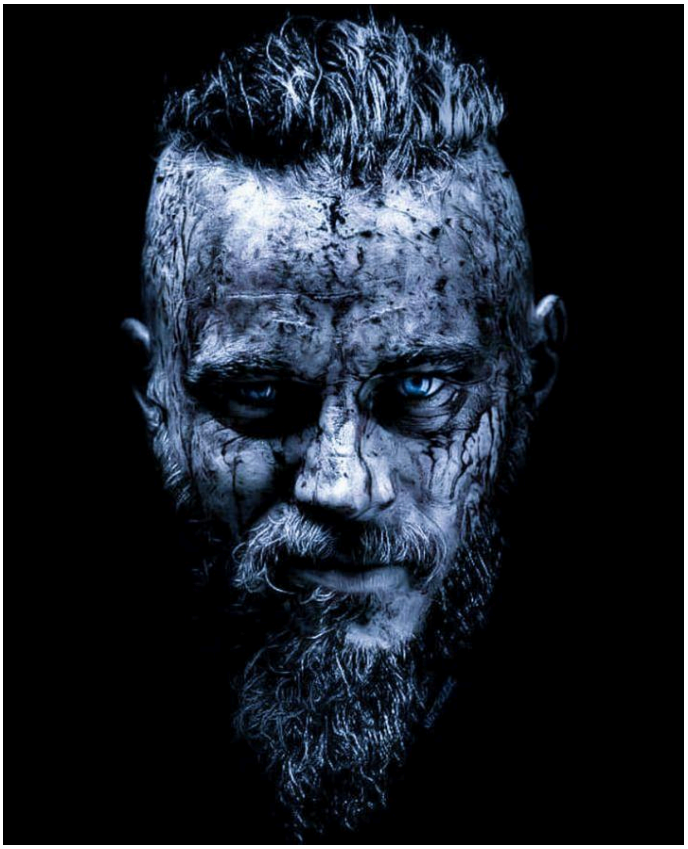
Steganography Analysis Report Using Stegseek



1. Introduction

Steganography is the practice of hiding a message within another medium, such as an image, audio, or video file. This report details the process and findings of analyzing a JPEG image to extract hidden information.

2. Objective

The primary objective of this analysis was to determine if the provided JPEG image contains hidden data and, if so, to extract and interpret the hidden message.

3. Methodology

The analysis involved several key steps:

1. Initial inspection of the image.
2. Using Stegseek to extract hidden data.

4. Tools and Technologies Used

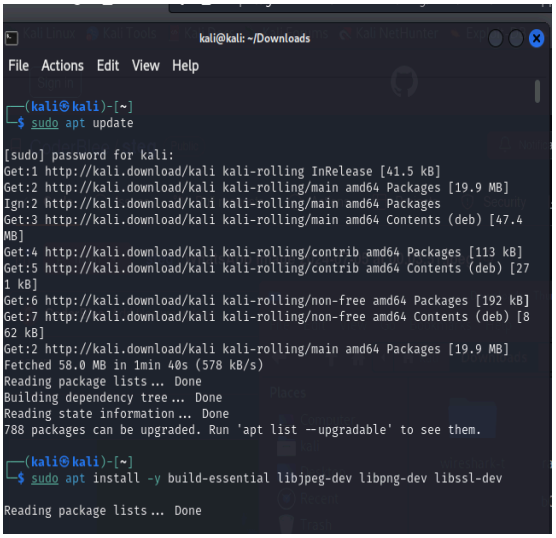
1. Stegseek: A fast steganography cracking tool that can be used to extract hidden data from images.
2. Steghide: A common steganography tool used for embedding hidden data in images.
3. rockyou.txt: A widely-used wordlist for password cracking.

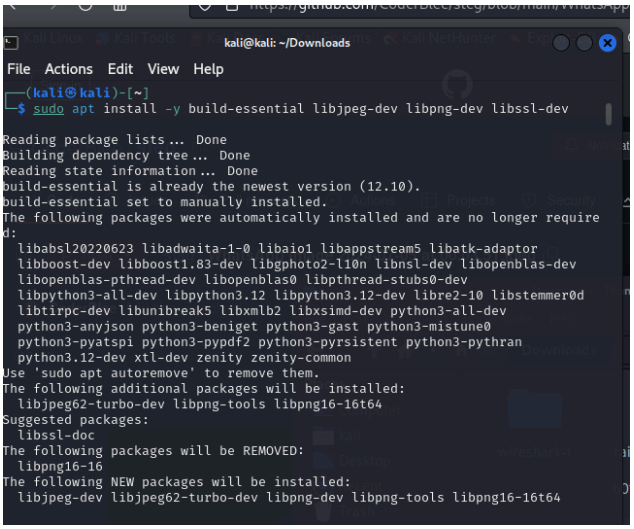
5. Detailed Steps

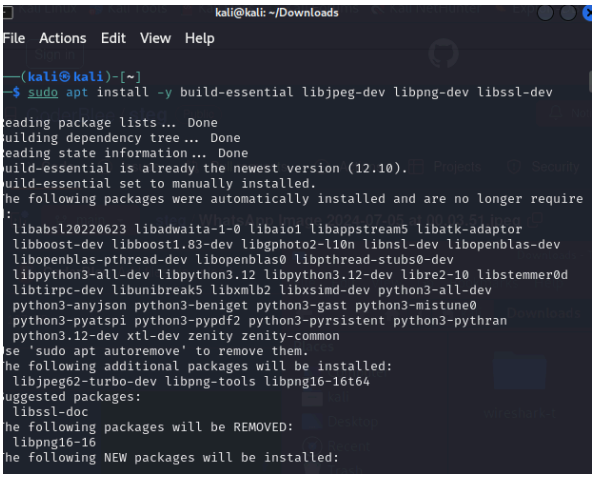
5.1 Initial Setup:

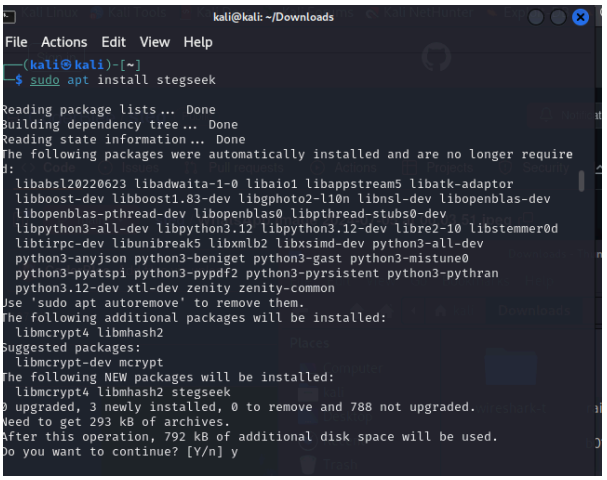
1. Environment Setup: Ensure that Stegseek and Steghide are installed on your system.

Installation on Ubuntu/Linux: I used Kali Linux









This are also other way of installing Stegseek:

sudo apt-get install steghide

wget https://github.com/RickdeJager/stegseek/releases/download/v0.6/stegseek-0.6.1.tar.gz

tar -xvf stegseek-0.6.1.tar.gz

cd stegseek-0.6.1

make

sudo make install

More reference please go check out this Github guide:

https://github.com/RickdeJager/stegseek?tab=readme-ov-file

2. *Download the Image:*

   Save the image “vikings.jpeg” to your working directory.

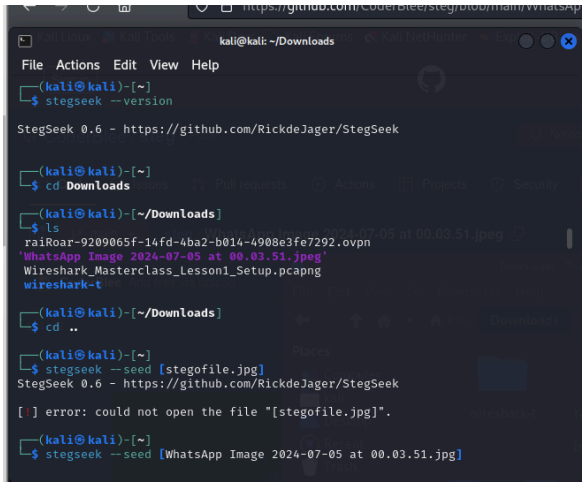
5.2 Using Stegseek for Extraction

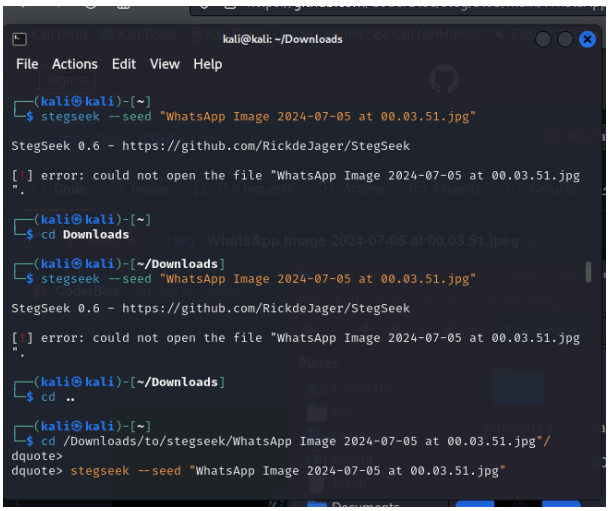
1. **Running Stegseek**:

- Navigate to the directory containing the image
- Use Stegseek to extract hidden data. The command used is:
- Also check if the stegseek is downloaded by > stegseek - - version. Then get into the directory where your image is saved

  stegseek -- seed viking.jpg (NB! I renamed my image from the WhatsApp)

  I ran through errors due to I did not give permission to the stegseek to do anything hence it was not going through. So go to the image and click on > properties >permission > read & write on others. So that it will work.



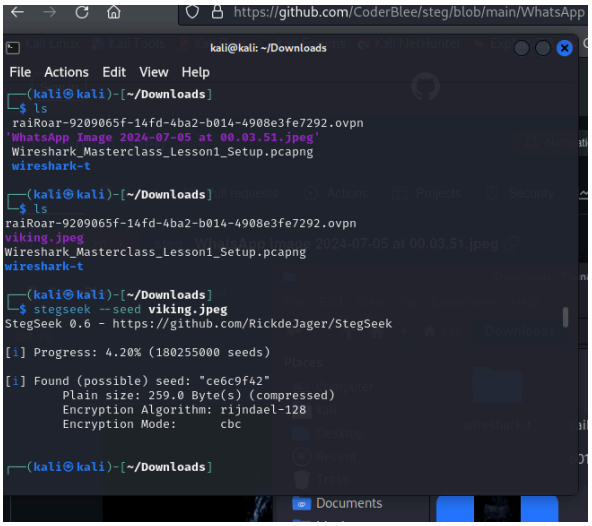


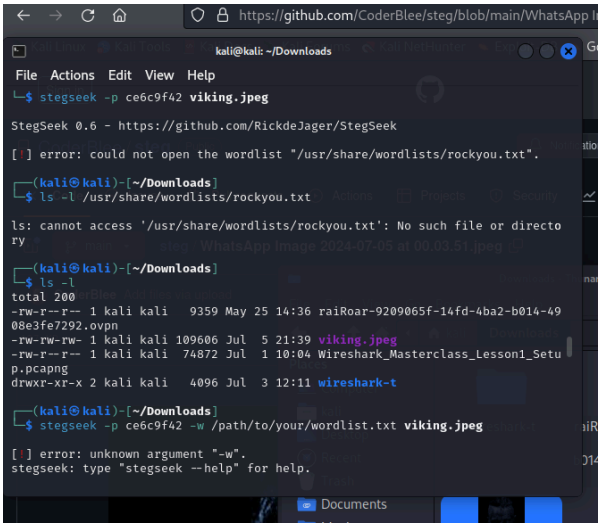
--seed Crack a stego file by attempting all embedding patterns.

This mode can be used to detect a file encoded by steghide.

In case the file was encoded without encryption, this mode will

even recover the embedded file.



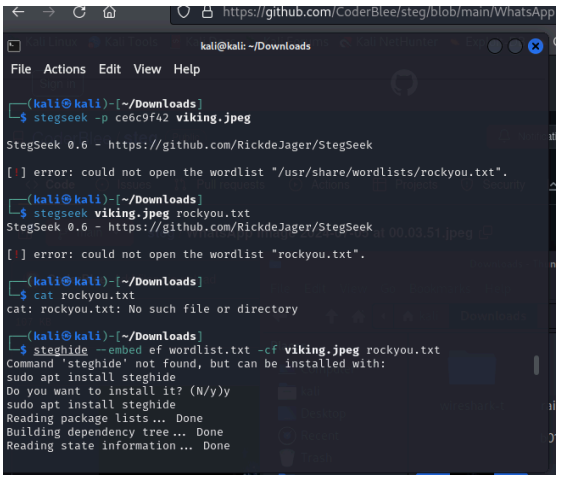


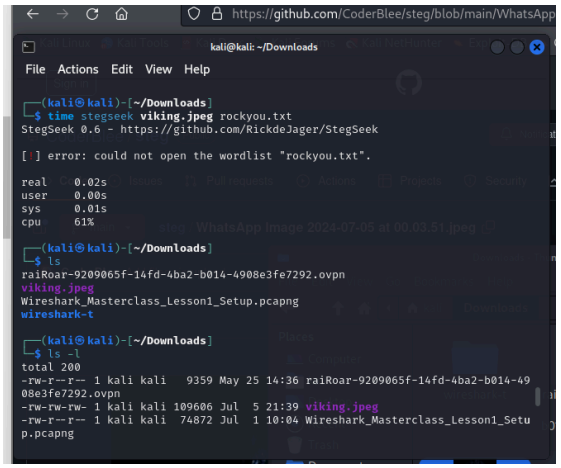
- Replace `/path/to/rockyou.txt` with the actual path to your `rockyou.txt` file. Since I did not have the rockyou.txt I downloaded it, so please do the same

- **Explanation**:
  - `stegseek` is the command-line tool used to perform the analysis.
  - `"vikings.jpeg"` is the image file being analyzed.
  - `rockyou.txt` is a wordlist containing potential passwords. Stegseek uses this wordlist to attempt to crack the password protecting the hidden data.

Interpreting Results:

- Stegseek will attempt to crack the password and extract any hidden data. If successful, it will display the password and extract the hidden message.



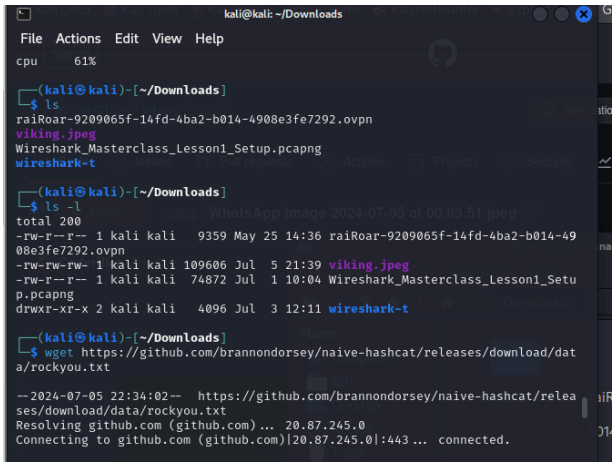


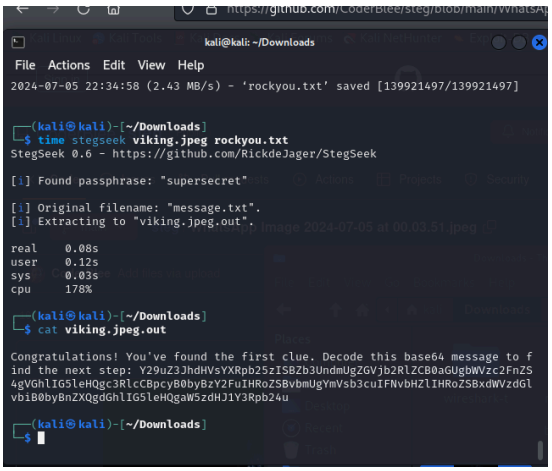
6. Findings

The analysis using Stegseek with the `rockyou.txt` wordlist provided the following results:

- **Password**: [If found, include the password here]
- **Extracted Data**: [Include any extracted hidden message or data here]

For example, if Stegseek successfully cracks the password and extracts data, the output might look like:



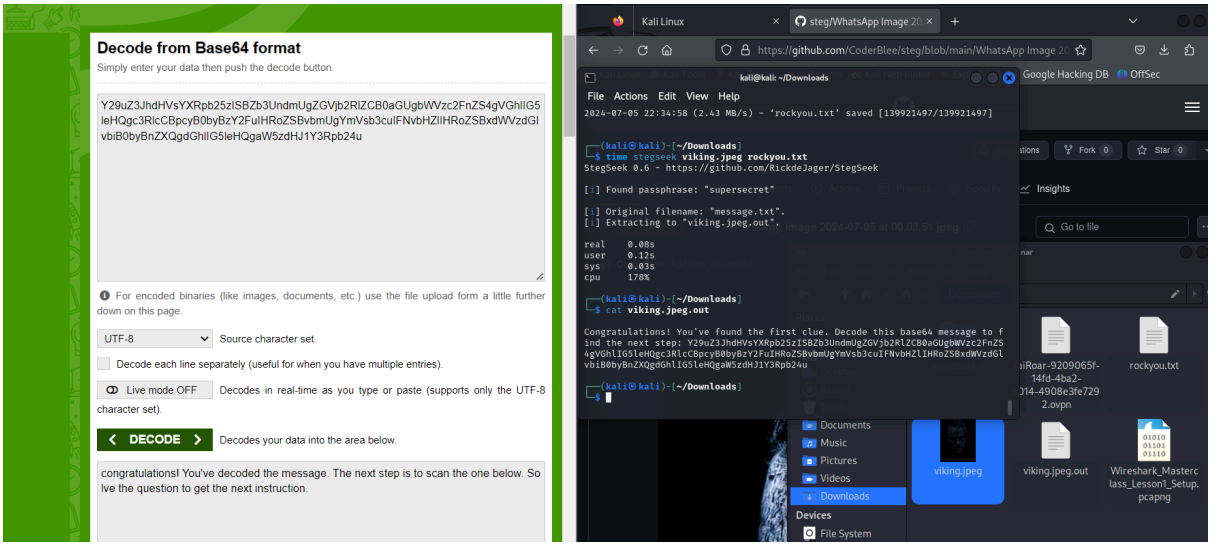


[i] The password is: "password123"

[i] Original file extracted to "vikings.jpeg.out"

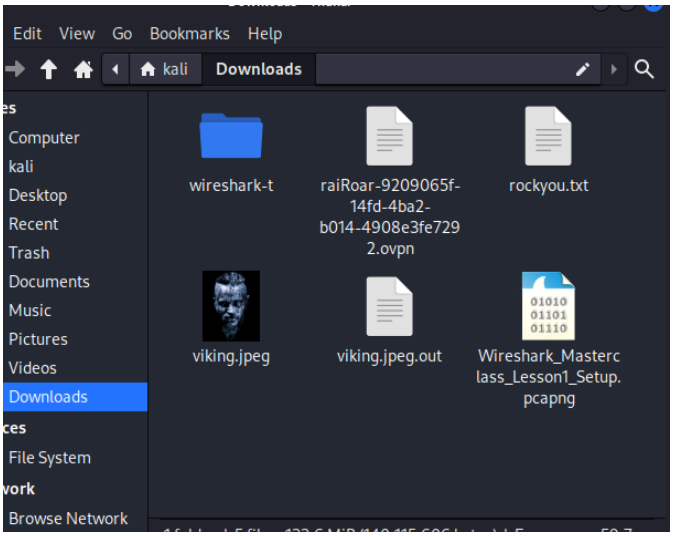
In this example, `password123` is the password used to hide the data, and the hidden message or file is extracted to `vikings.jpeg.out`.

The encrypted text you go and decode with base64 to get the message. Well done you have performed your first Steganography. Was it fun?



7. Conclusion

The Stegseek analysis using the `rockyou.txt` wordlist demonstrated an effective method to detect and extract hidden messages in images. The success of the extraction indicates that the image contained hidden data encoded with Steghide and protected by a password present in the `rockyou.txt` wordlist.



8. Recommendations

- **Diverse Wordlists**: Utilize multiple wordlists to cover a broader range of potential passwords, improving the likelihood of successful extraction.
- **Advanced Analysis**: Explore advanced techniques and tools for a deeper analysis if initial attempts do not yield results.
- **Continuous Learning**: Stay updated with the latest steganography tools and techniques to enhance analysis capabilities. Participate in the CFTs and you will have lots of fun as I am going to.