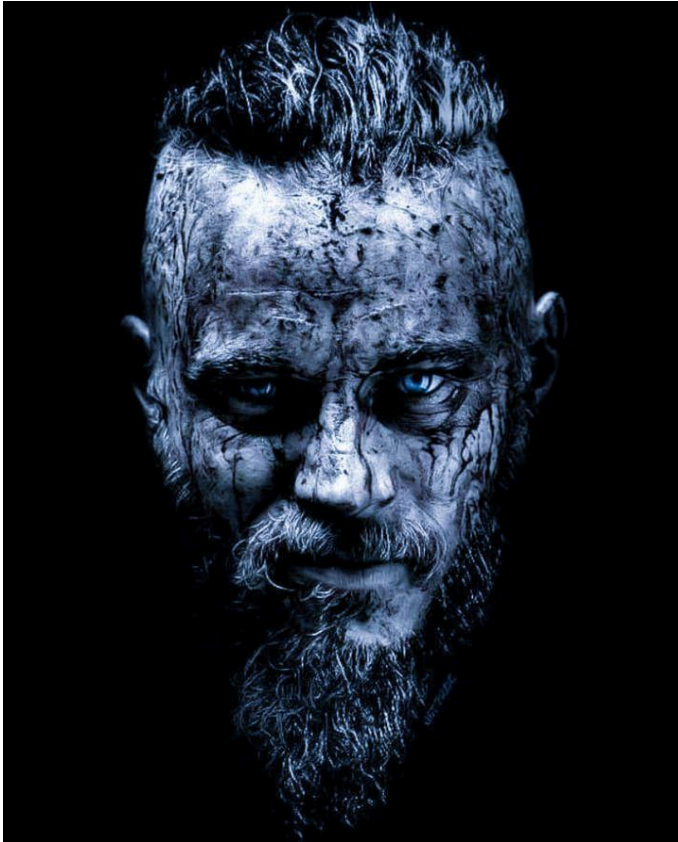


Steganography Analysis Report Using **Stegseek**



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

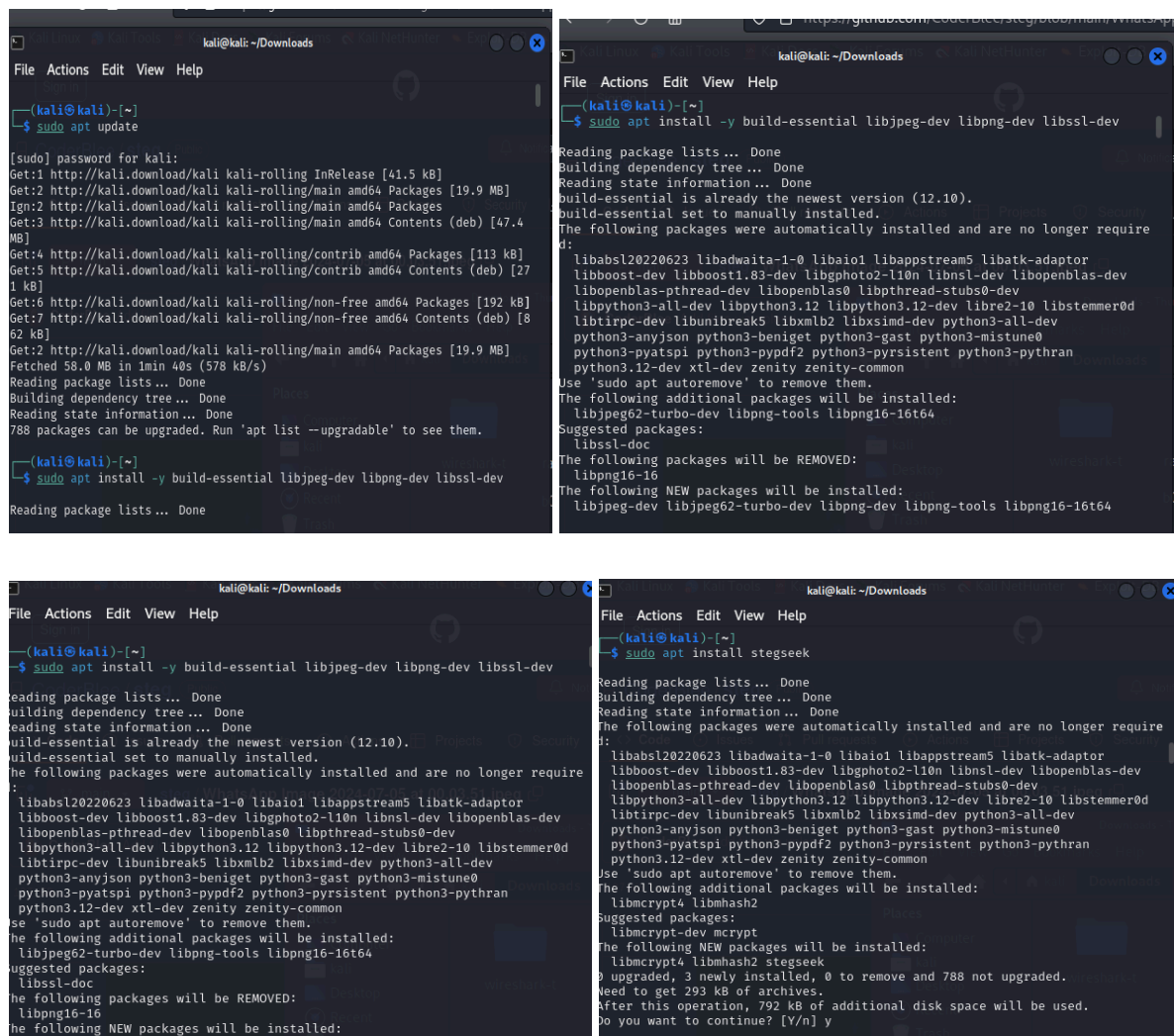
1. Stegseek: A fast steganography cracking tool that can be used to extract hidden data from images.
2. Steghide: A common steganography tool used for embedding hidden data in images.
3. rockyou.txt: A widely-used wordlist for password cracking.

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



```
kali@kali: ~/Downloads
File Actions Edit View Help
--(kali@kali)~--
$ sudo apt update

[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Ign:2 http://kali.download/kali kali-rolling/main amd64 Packages
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [47.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [113 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [271 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [862 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Fetched 58.0 MB in 1min 40s (578 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
788 packages can be upgraded. Run 'apt list --upgradable' to see them.

--(kali@kali)~--
$ sudo apt install -y build-essential libjpeg-dev libpng-dev libssl-dev

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.10).
build-essential set to manually installed.
The following packages were automatically installed and are no longer required:
  libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor
  libboost-dev libboost1.83-dev libghphoto2-110n libnsl-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpthread-stubs0-dev
  libpython3-all-dev libpython3.12 libpython3.12-dev libre2-10 libstemmer0d
  libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev python3-all-dev
  python3-anyjson python3-beniget python3-gast python3-mistune0
  python3-pyatspi python3-pydpf2 python3-pyrsistent python3-pythran
  python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjpeg62-turbo-dev libpng-tools libpng16-16t64
Suggested packages:
  libssl-doc
The following packages will be REMOVED:
  libpng16-16
The following NEW packages will be installed:
  libjpeg-dev libjpeg62-turbo-dev libpng-dev libpng-tools libpng16-16t64

kali@kali: ~/Downloads
File Actions Edit View Help
--(kali@kali)~--
$ sudo apt install -y build-essential libjpeg-dev libpng-dev libssl-dev

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor
  libboost-dev libboost1.83-dev libghphoto2-110n libnsl-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpthread-stubs0-dev
  libpython3-all-dev libpython3.12 libpython3.12-dev libre2-10 libstemmer0d
  libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev python3-all-dev
  python3-anyjson python3-beniget python3-gast python3-mistune0
  python3-pyatspi python3-pydpf2 python3-pyrsistent python3-pythran
  python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjpeg62-turbo-dev libpng-tools libpng16-16t64
Suggested packages:
  libssl-doc
The following packages will be REMOVED:
  libpng16-16
The following NEW packages will be installed:
  libjpeg-dev libjpeg62-turbo-dev libpng-dev libpng-tools libpng16-16t64

kali@kali: ~/Downloads
File Actions Edit View Help
--(kali@kali)~--
$ sudo apt install stegseek

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor
  libboost-dev libboost1.83-dev libghphoto2-110n libnsl-dev libopenblas-dev
  libopenblas-pthread-dev libopenblas0 libpthread-stubs0-dev
  libpython3-all-dev libpython3.12 libpython3.12-dev libre2-10 libstemmer0d
  libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev python3-all-dev
  python3-anyjson python3-beniget python3-gast python3-mistune0
  python3-pyatspi python3-pydpf2 python3-pyrsistent python3-pythran
  python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libmbedtls4 libmhash2
Suggested packages:
  libmbedtls-dev mcrypt
The following NEW packages will be installed:
  libmbedtls4 libmhash2 stegseek
3 upgraded, 3 newly installed, 0 to remove and 788 not upgraded.
Need to get 293 kB of archives.
After this operation, 792 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

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.

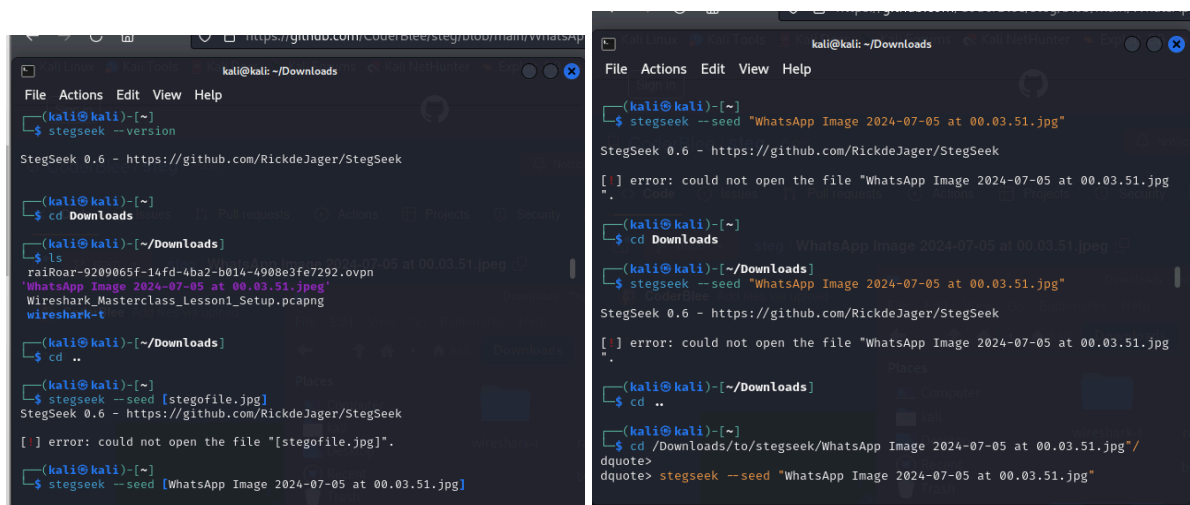
5.2 Using Stegseek for Extraction

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.



```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ stegseek --version
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
raIRoar-9209065f-14fd-4ba2-b014-4908e3fe7292.ovpn  WhatsApp Image 2024-07-05 at 00.03.51.jpg
Wireshark_Masterclass_Lesson1_Setup.pcapng        wireshark-t
(kali@kali)-[~/Downloads]
$ cd ..
(kali@kali)-[~]
$ stegseek --seed [stegofile.jpg]
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[.] error: could not open the file "[stegofile.jpg]".
(kali@kali)-[~]
$ stegseek --seed "WhatsApp Image 2024-07-05 at 00.03.51.jpg"

kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ stegseek --seed "WhatsApp Image 2024-07-05 at 00.03.51.jpg"
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[.] error: could not open the file "WhatsApp Image 2024-07-05 at 00.03.51.jpg"

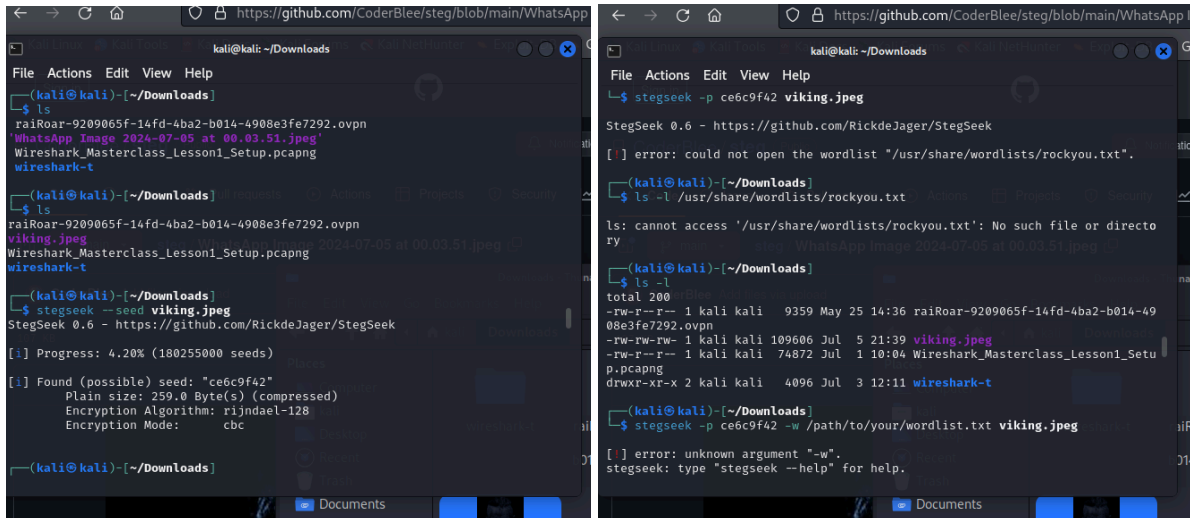
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ stegseek --seed "WhatsApp Image 2024-07-05 at 00.03.51.jpg"
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[.] error: could not open the file "WhatsApp Image 2024-07-05 at 00.03.51.jpg"

(kali@kali)-[~/Downloads]
$ cd ..
(kali@kali)-[~]
$ cd /Downloads/to/stegseek/WhatsApp Image 2024-07-05 at 00.03.51.jpg/"
dquote> stegseek --seed "WhatsApp Image 2024-07-05 at 00.03.51.jpg"
```

--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.



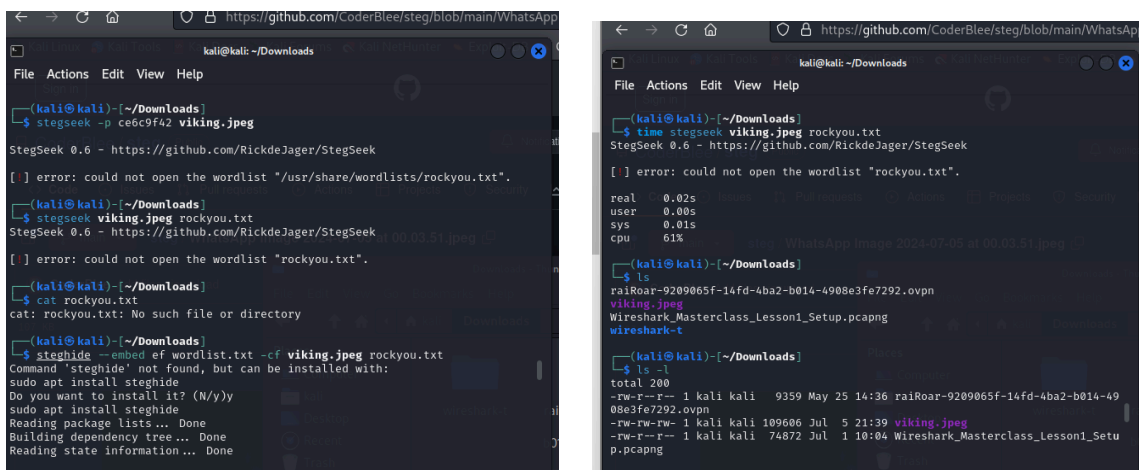
```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~/Downloads
$ ls
raiRoar-9209065f-14fd-4ba2-b014-4908e3fe7292.ovpn
WhatsApp_Image_2024-07-05_at_00.03.51.jpeg
Wireshark_Masterclass_Lesson1_Setup.pcapng
wireshark-t
(kali@kali)~/Downloads
$ stegseek --seed viking.jpeg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] Progress: 4.20% (180255000 seeds)
[!] Found (possible) seed: "ce6c9f42"
    Plain size: 259.0 Byte(s) (compressed)
    Encryption Algorithm: rijndael-128
    Encryption Mode: cbc
(kali@kali)~/Downloads

kali@kali: ~/Downloads
File Actions Edit View Help
$ stegseek -p ce6c9f42 viking.jpeg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] error: could not open the wordlist "/usr/share/wordlists/rockyou.txt".
(kali@kali)~/Downloads
$ ls -l /usr/share/wordlists/rockyou.txt
ls: cannot access '/usr/share/wordlists/rockyou.txt': No such file or directory
(kali@kali)~/Downloads
$ stegseek -p ce6c9f42 -w /path/to/your/wordlist.txt viking.jpeg
[!] error: unknown argument "-w".
stegseek: type "stegseek --help" for help.
```

- 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.



```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~/Downloads
$ stegseek -p ce6c9f42 viking.jpeg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] error: could not open the wordlist "/usr/share/wordlists/rockyou.txt".
(kali@kali)~/Downloads
$ stegseek viking.jpeg rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] error: could not open the wordlist "rockyou.txt".
(kali@kali)~/Downloads
$ cat rockyou.txt
cat: rockyou.txt: No such file or directory
(kali@kali)~/Downloads
$ steghide --embed ef wordlist.txt -cf viking.jpeg rockyou.txt
command 'steghide' not found, but can be installed with:
sudo apt install steghide
Do you want to install it? (N/y/y)
sudo apt install steghide
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

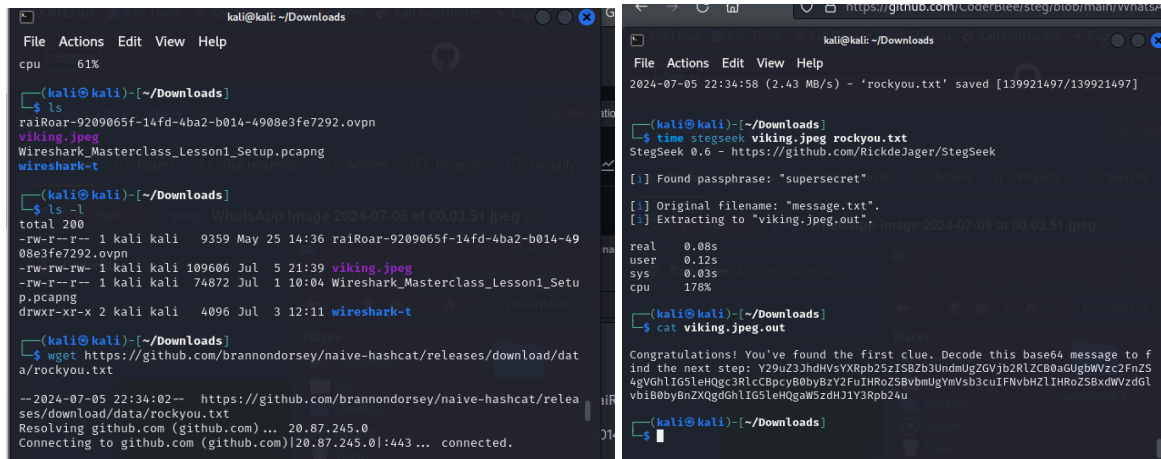
kali@kali: ~/Downloads
File Actions Edit View Help
$ time stegseek viking.jpeg rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
[!] error: could not open the wordlist "rockyou.txt".
real    0.02s
user    0.00s
sys     0.01s
cpu     61%
(kali@kali)~/Downloads
$ ls
raiRoar-9209065f-14fd-4ba2-b014-4908e3fe7292.ovpn
viking.jpeg
Wireshark_Masterclass_Lesson1_Setup.pcapng
wireshark-t
(kali@kali)~/Downloads
$
```

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:

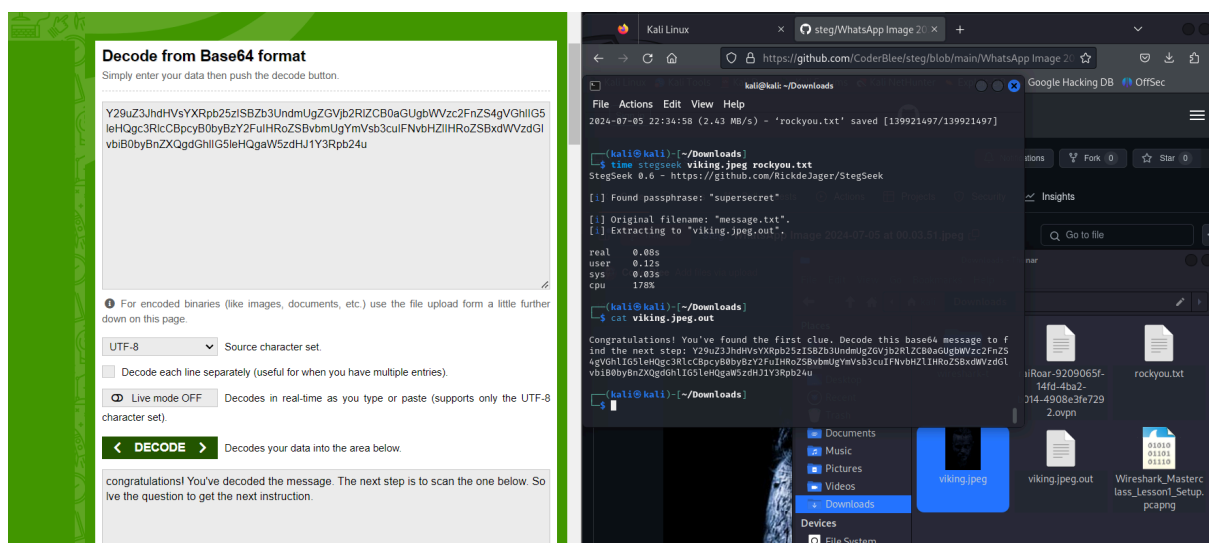


[i] The password is: "password123"

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

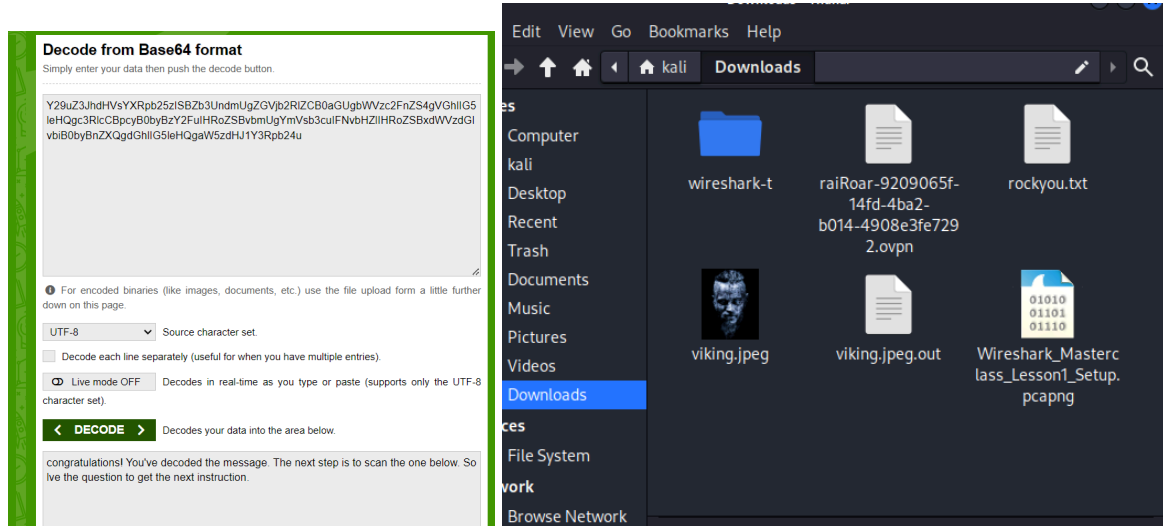
In this example, `password123` is the password used to hide the data, and the hidden message or file is extracted to `vikings.jpeg.out`.

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.