Steganography Challenge

Objective

Thepurposeofthisexercise was to analyze a suspicious JPEG image (challenge.jpg) and determine whether it contained hidden data. The goal was to extract the hidden content and obtain the final flag.

Steganography Challenge

Name:	Praveen Kumar
Instructor:	Nitish Agrawal 18-
Date:	11-2025

Tools Used

- **Kali Linux**
- **stegcracker**
- **rockyou.txt** wordlist
- **steghide**

Task Steps =

Password Discovery (Dictionary Attack)

The creator typically uses weak or common passwords, so I attempted a **dictionary attack**.

Command - stegcracker challenge.jpg /usr/share/wordlists/rockyou.txt

Output:

Successfully cracked file with password: **thursday**

Extraction of Hidden File

Used the recovered passphrase to extract the actual embedded file:

Command - steghide extract -sf challenge.jpg

Result:

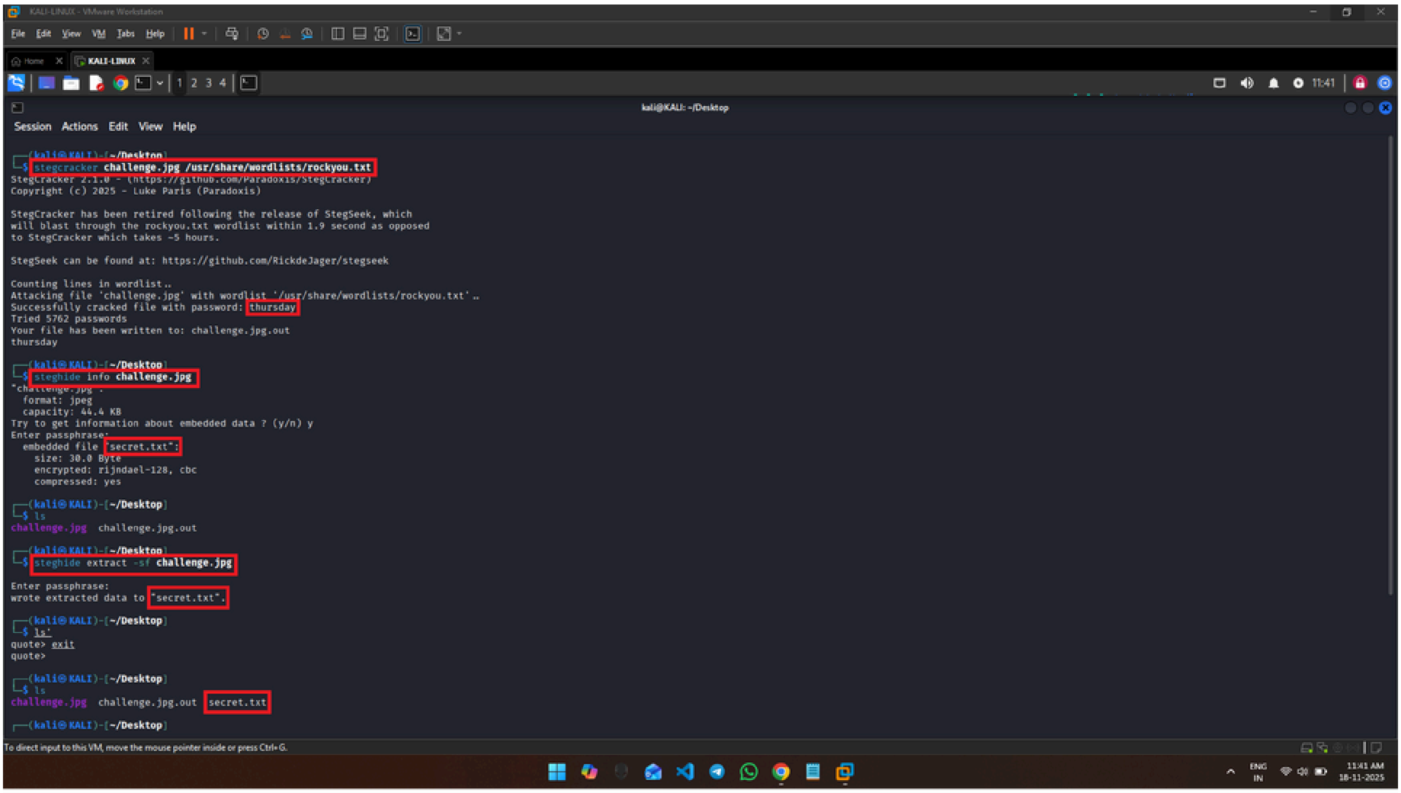
wrote extracted data to "**secret.txt**"

Hidden Content Analysis

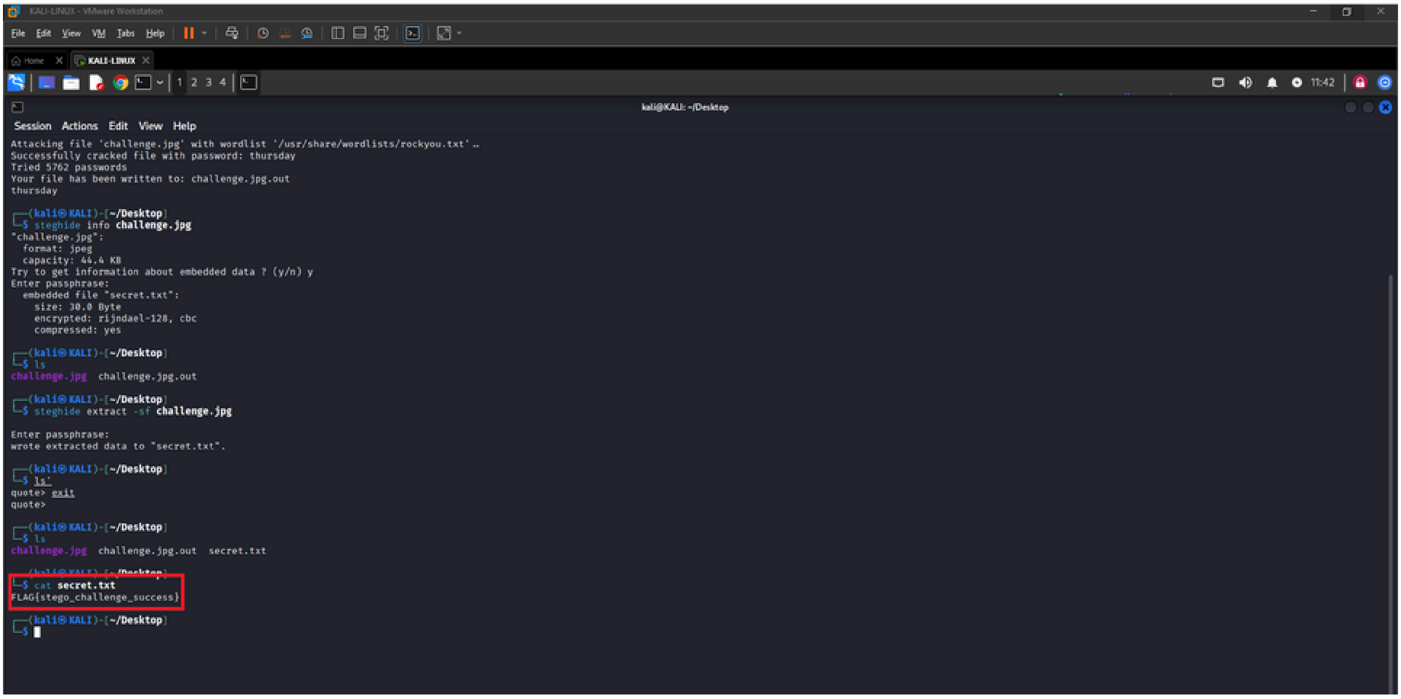
Finally, viewed the extracted text file:

Command - cat secret.txt

The file contained the hidden **flag (FLAG{stego_challenge_success})**,proving the steganography operation successful.


KALI-LINUX - VMware Workstation
File Edit View VM Tabs Help
Home
KALI-LINUX
1 2 3 4
11:41
kali@KALI: ~/Desktop
Session Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
IN
11:41 AM
18-11-2025

```
┌──(kali㉿KALI)-[~/Desktop]
└─$ stegcracker challenge.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'challenge.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: thursday
Tried 5762 passwords
Your file has been written to: challenge.jpg.out
thursday

┌──(kali㉿KALI)-[~/Desktop]
└─$ steghide info challenge.jpg
"challenge.jpg":
  format: jpeg
  capacity: 44.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 30.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls
challenge.jpg  challenge.jpg.out

┌──(kali㉿KALI)-[~/Desktop]
└─$ steghide extract -sf challenge.jpg

Enter passphrase:
wrote extracted data to "secret.txt".

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls'
quote> exit
quote>

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls
challenge.jpg  challenge.jpg.out  secret.txt

┌──(kali㉿KALI)-[~/Desktop]
```


KALI-LINUX - VMware Workstation
File Edit View VM Tabs Help
Home
KALI-LINUX
1 2 3 4
11:42
kali@KALI: ~/Desktop
Session Actions Edit View Help

```
Attacking file 'challenge.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: thursday
Tried 5762 passwords
Your file has been written to: challenge.jpg.out
thursday

┌──(kali㉿KALI)-[~/Desktop]
└─$ steghide info challenge.jpg
"challenge.jpg":
  format: jpeg
  capacity: 44.4 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 30.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls
challenge.jpg  challenge.jpg.out

┌──(kali㉿KALI)-[~/Desktop]
└─$ steghide extract -sf challenge.jpg

Enter passphrase:
wrote extracted data to "secret.txt".

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls'
quote> exit
quote>

┌──(kali㉿KALI)-[~/Desktop]
└─$ ls
challenge.jpg  challenge.jpg.out  secret.txt

┌──(kali㉿KALI)-[~/Desktop]
└─$ cat secret.txt
FLAG{stego_challenge_success}

┌──(kali㉿KALI)-[~/Desktop]
└─$ 
```