

## Hidden whispers:

1. Attached was wall.jpg.gz file as an attachment
2. Extract the file with `gunzip wall.jpg.gz` to `wall.jpg`
3. Using `steghide info wall.jpg`, it is asking for passphrase.

```
(kali㉿kali)-[~/Downloads]
└─$ steghide info wall.jpg
"wall.jpg":
  format: jpeg
  capacity: 7.1 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase: █
```

4. Since it is asking for passphrase, let's try if bruteforce can crack it!!
5. Run command to bruteforce password:

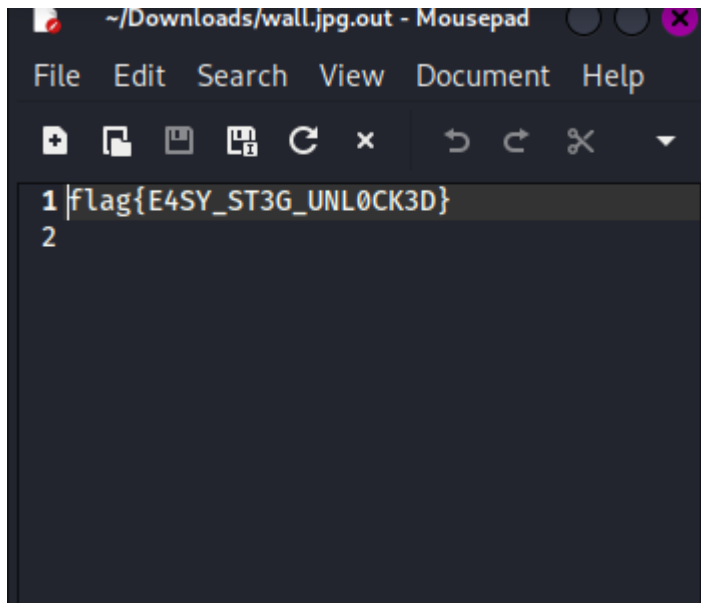
`stegcracker wall.jpg /usr/share/wordlists/rockyou.txt`

```
(kali㉿kali)-[~/Downloads]
└─$ stegcracker wall.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2025 - Luke Paris (Paradoxis)
bytecodevm.ko esp_blob.bin rev1 challenge(1).txt challenge.txt
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
WhatsApp Image wall.jpg og image_final.jpeg webp
Counting lines in wordlist..
Attacking file 'wall.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: 123456
Tried 1 passwords
Your file has been written to: wall.jpg.out
123456
```

Password found: **123456**

```
(kali㉿kali)-[~/Downloads]
└─$ ls | grep wall
RSA.pem Exp4'.docx java_oops.png SIH2025-
network-firewall-icon-illustration-vector-on-white-background.jpg Presenta
wall.jpg Format(2
wall.jpg.out
```

6. Run it and it downloads another file named `wall.jpg.out`



7.

Found flag:

flag{E4SY\_ST3G\_UNL0CK3D}