- On this chall we have a image named `images.jpg`.
- As we know stegno is used to hide the data so to extract it i used this command

```
┌──(root㉿0xMinato)-[~/Downloads]
└─# steghide extract -sf images.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
```

- we see that its asking for passphrase and we dont know what the passphrase is, so we cant open it.
- Theres a tool called `stegcracker` to bruteforce it . I used stegcracker using rockyou.txt file to crack the passphrase of file.
- its usage is `stegcracker <file name> <path to wordlist>`

`stegcracker ~/Downloads/images.jpg /usr/share/wordlists/rockyou.txt`

```
┌──(root㉿0xMinato)-[~/Downloads]
└─# stegcracker ~/Downloads/images.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - 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 '/root/Downloads/images.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: 987654321
Tried 82 passwords
Your file has been written to: /root/Downloads/images.jpg.out
987654321
```

The passphrase is cracked, now we can use the extract command to extract the contents of file.

```
┌──(root㉿0xMinato)-[~/Downloads]
└─# steghide extract -sf images.jpg
Enter passphrase:
wrote extracted data to "secret.txt".
```

it shows tht the data has been extracted to `secret.txt` file.

i used `more` command to see the content of secret.txt file

```
┌──(root㉿0xMinato)-[~/Downloads]
└─# more secret.txt
CSCTF{TRE4SUR3_P13C3}
```

The flag was stored on secret.txt file.