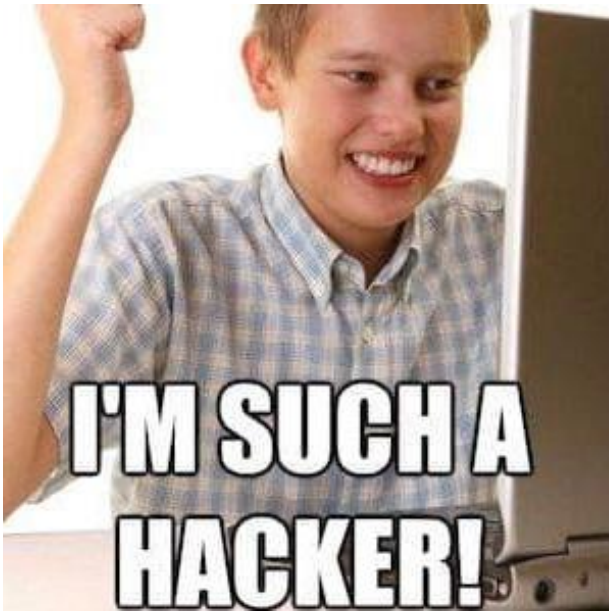
CSC-BZU

Digital Forensics Writeup

Written By: Izzdeen Al-Sayyed

Challenge 1:

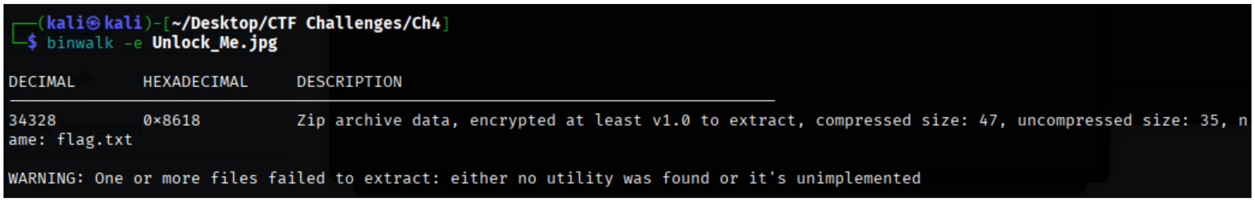
File: Unlock_Me.jpg



The flag in this picture is hidden inside a **ZIP file**, which itself contains **flag.txt**.

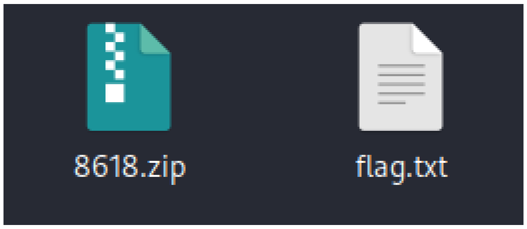
Step 1: Extract the ZIP file from the picture using:

binwalk -e Unlock_Me.jpg

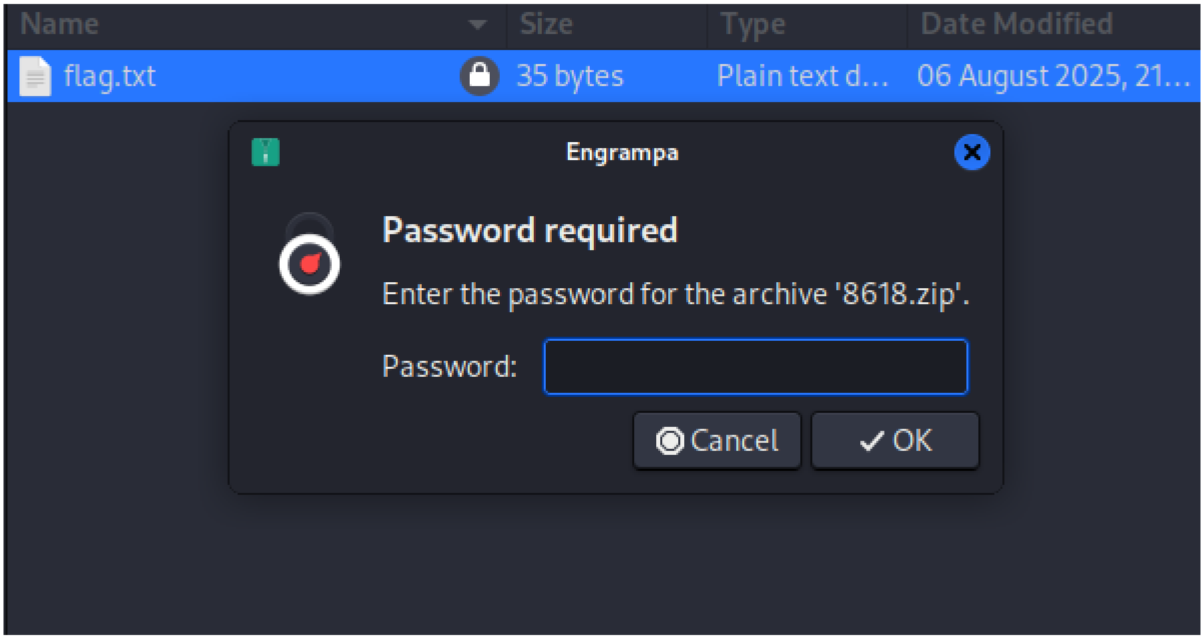


```
┌──(kali㉿kali)-[~/Desktop/CTF Challenges/Ch4]
└─$ binwalk -e Unlock_Me.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
34328         0×8618          Zip archive data, encrypted at least v1.0 to extract, compressed size: 47, uncompressed size: 35, n
ame: flag.txt

WARNING: One or more files failed to extract: either no utility was found or it's unimplemented
```

After extracting, you will find a ZIP file. When you open flag.txt inside it, the content looks unreadable because the file is password-protected.



Step 2: Perform a dictionary attack on the ZIP file using the **rockyou.txt** wordlist, since the password is included there.



Name	Size	Type	Date Modified
flag.txt	35 bytes	Plain text d…	06 August 2025, 21…

Engrampa

Password required

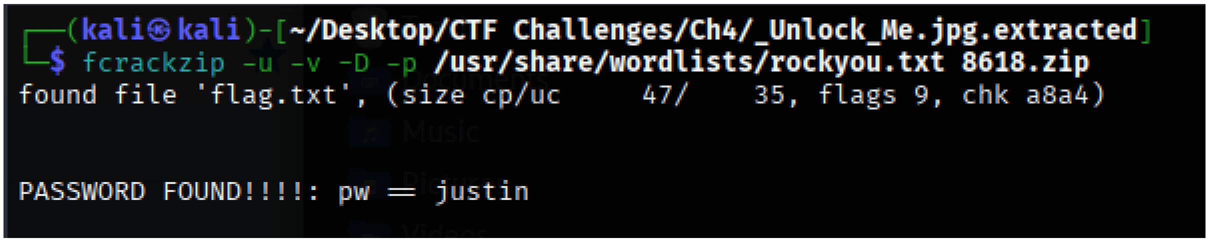
Enter the password for the archive '8618.zip'.

Password:

Step 2: Perform a dictionary attack on the ZIP file using the rockyou.txt wordlist, since the password is included there.

Command:

fcrackzip -u -v -D -p /usr/share/wordlists/rockyou.txt 8618.zip



```
┌──(kali㉿kali)-[~/Desktop/CTF Challenges/Ch4/_Unlock_Me.jpg.extracted]
└─$ fcrackzip -u -v -D -p /usr/share/wordlists/rockyou.txt 8618.zip
found file 'flag.txt', (size cp/uc     47/    35, flags 9, chk a8a4)


PASSWORD FOUND!!!!: pw == justin
```

The Password is: justin

Explanation:

- **fcrackzip** → Tool to crack ZIP file passwords.
- **-u** → Test-unzip the file after each guess to verify correctness.
- **-v** → Verbose mode, shows detailed progress.
- **-D** → Dictionary attack.
- **-p** /usr/share/wordlists/rockyou.txt → The wordlist used for guessing.
- **8618.zip** → The target ZIP file.

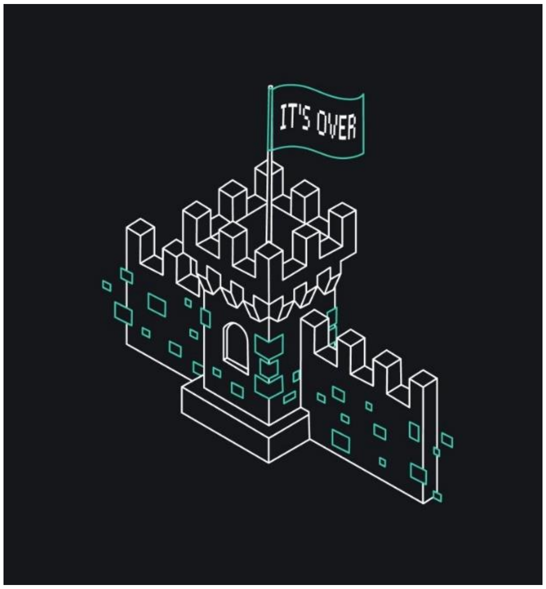
Once cracked, open the ZIP and read “ flag.txt “ to obtain the flag.

Flag: CSC-BZU{rR0ocK_yo0u_d4sa30sk6fA59}

Challenge 2:

File: hmmm.jpg

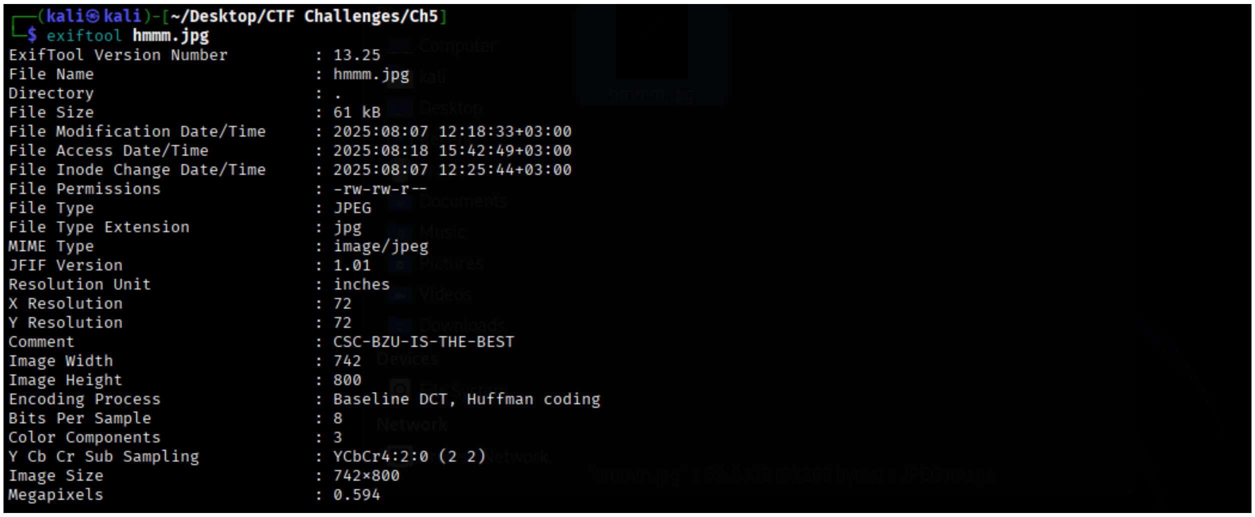
This image contains a hidden flag.txt.



In this challenge there is a (flag.txt) file hidden in this picture ,

Step 1: Check the metadata of the picture using:

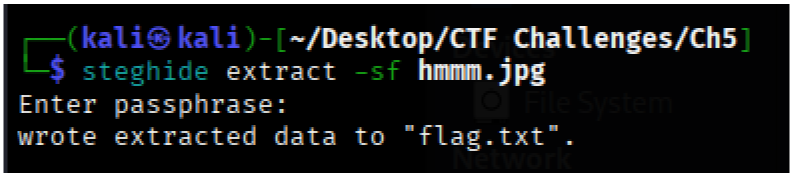
exiftool hmmm.jpg



```
┌──(kali㉿kali)-[~/Desktop/CTF Challenges/Ch5]
└─$ exiftool hmmm.jpg
ExifTool Version Number         : 13.25
File Name                       : hmmm.jpg
Directory                       : .
File Size                       : 61 kB
File Modification Date/Time     : 2025:08:07 12:18:33+03:00
File Access Date/Time           : 2025:08:18 15:42:49+03:00
File Inode Change Date/Time     : 2025:08:07 12:25:44+03:00
File Permissions                : -rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Comment                         : CSC-BZU-IS-THE-BEST
Image Width                     : 742
Image Height                    : 800
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 742x800
Megapixels                      : 0.594
```

Looks like we have some hints here? **CSC-BZU-IS-THE-BEST**

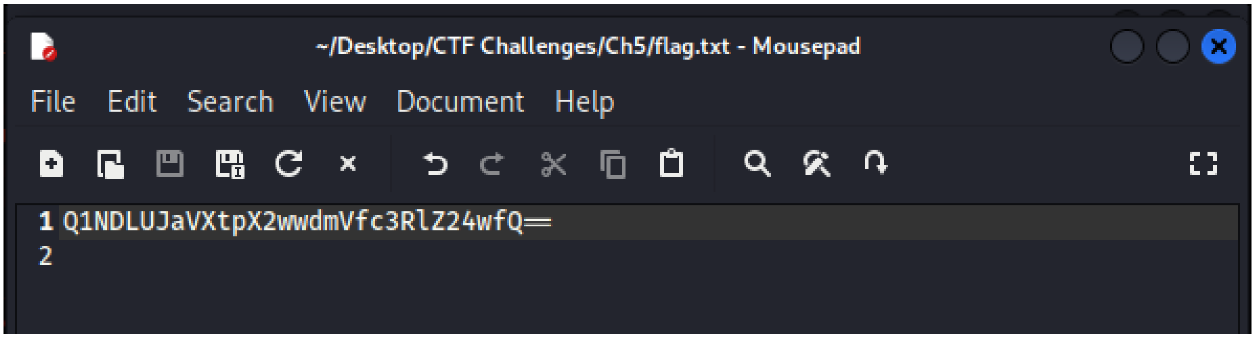
Step 2: Use steghide to check if hidden files exist:



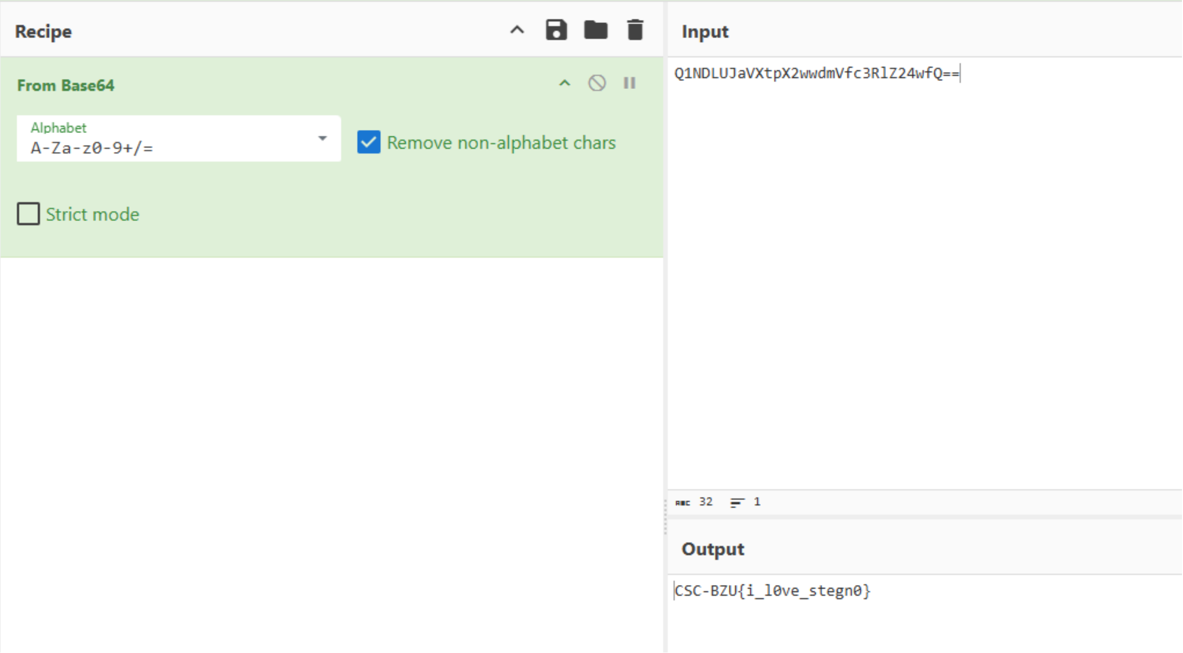
```
┌──(kali㉿kali)-[~/Desktop/CTF Challenges/Ch5]
└─$ steghide extract -sf hmmm.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
```

It will ask for a password. The correct one is the hint .

After extraction, open flag.txt. The text looks encrypted, so use CyberChef to decode it.



```
Q1NDLUJaVXtpX2wwdmVfc3RlZ24wfQ==
```



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

```
Q1NDLUJaVXtpX2wwdmVfc3RlZ24wfQ==
```

32 1

```
CSC-BZU{i_l0ve_stegn0}
```

Flag: CSC-BZU{i_l0ve_stegn0}

“Behind every byte, there’s a story waiting to be uncovered. Keep digging, keep learning.”