

LinkedIn: [Kelvin Kimotho](#)

Challenge



# Hidden in Images

## 0

How many have been added?

The flag should be submitted as: cyber{\_\_\_\_\_}



Flag

Submit

### Solution

I first downloaded the image using **wget** tool.

```
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ wget https://practice.ctfcyber.org/files/c5c5e376053cd9782a42345a31c87731/Chicken.jpg
--2025-02-10 12:47:25-- https://practice.ctfcyber.org/files/c5c5e376053cd9782a42345a31c87731/Chicken.jpg
Resolving practice.ctfcyber.org (practice.ctfcyber.org)... 54.144.139.50
Connecting to practice.ctfcyber.org (practice.ctfcyber.org)[54.144.139.50]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 115959 (113K) [image/jpeg]
Saving to: 'Chicken.jpg'

Chicken.jpg           100%[=====] 113.24K  58.0KB/s  in 2.0s
2025-02-10 12:47:28 (58.0 KB/s) - 'Chicken.jpg' saved [115959/115959]

(kali@kali)-[~/Desktop]
$ ls
Chicken.jpg

(kali@kali)-[~/Desktop]
$
```

I went ahead and used tools like **exiftool** for metadata analysis and **strings** tool that prints out strings that have been added into a file. The metadata revealed nothing very suspicious.

```
(kali@kali)-[~/Desktop]
$ exiftool Chicken.jpg
ExifTool Version Number      : 12.76
File Name                    : Chicken.jpg
Directory                    : .
File Size                    : 116 kB
File Modification Date/Time   : 2023:04:27 18:53:35+00:00
File Access Date/Time        : 2025:02:10 12:47:28+00:00
File Inode Change Date/Time   : 2025:02:10 12:47:28+00:00
File Permissions              : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                  : 1.01
Resolution Unit               : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                   : 1100
Image Height                  : 818
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                   : 1100x818
Megapixels                   : 0.900

(kali@kali)-[~/Desktop]
$
```

I went ahead and used strings tool looking for embedded strings in the image file.

```
(kali@kali)-[~/Desktop]
$ strings Chicken.jpg
JFIF
, #0'*)
-0-(0%)(
((((((((((((((((((((((((((((((((((((
$3br
%0'*)*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
#3R
0'*)*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
ZWGdp

] ex
;QEc
6_pWK
Salt
Thyme
Basil
Oregano
Celery Salt
Black Pepper
Dried Mustard
Paprika
Garlic Salt
Ground Ginger
White Pepper

(kali@kali)-[~/Desktop]
$
```

I found 11 lines of embedded strings. The flag was **cyber{11}**.