

Challenge 2 Day 2 – Harambe

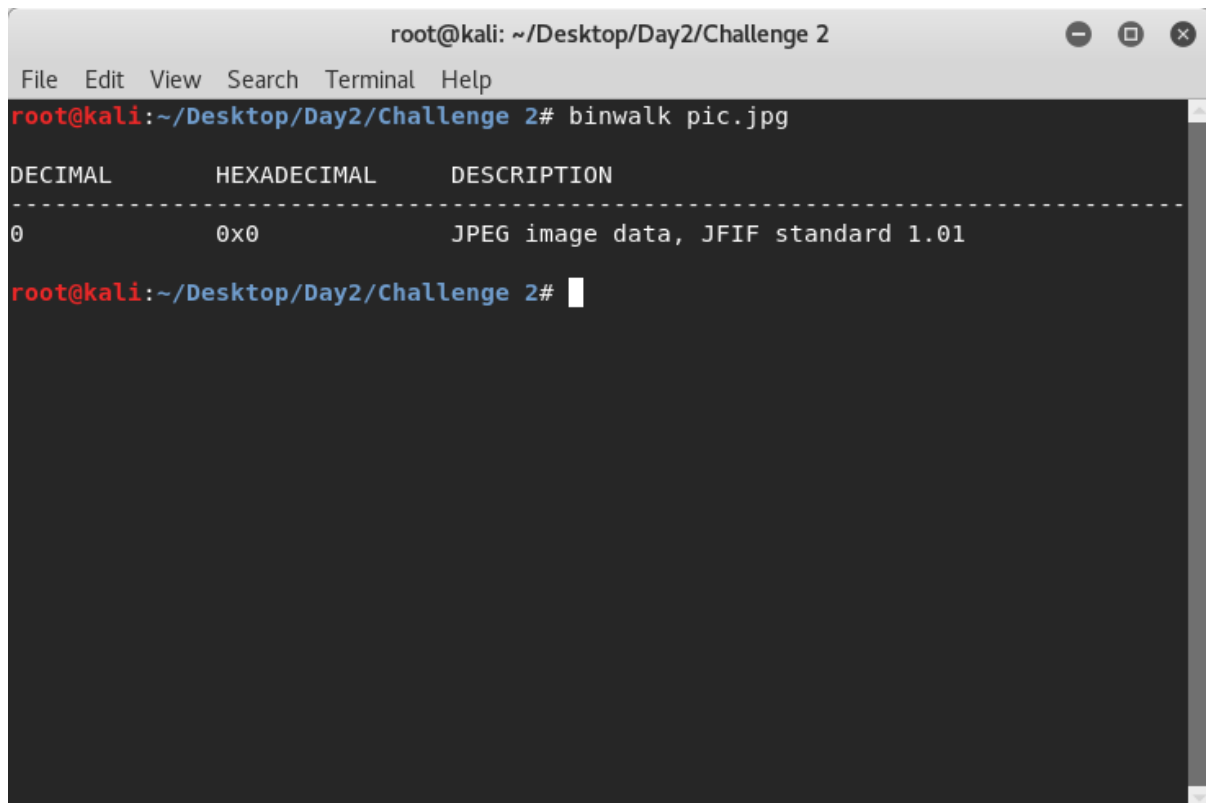
By team Bingsu Strawberry from IIUM

Step 1:

We received a picture of type .jpg which mean this is definitely going to be easier than the first challenge which involved a .png file. Whew. We zoomed in to check for any hidden text and found nothing. Moving onto the more complex stages.

Step 2:

Moving onto the next step, we tried using binwalk on the image to check for any hidden zip file.



```
root@kali: ~/Desktop/Day2/Challenge 2
File Edit View Search Terminal Help
root@kali:~/Desktop/Day2/Challenge 2# binwalk pic.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
root@kali:~/Desktop/Day2/Challenge 2#
```

Nothing hidden here inside the image.

Step 3:

We tried using the strings tool to check whether its hidden there.

```
root@kali: ~/Desktop/Day2/Challenge 2
File Edit View Search Terminal Help
root@kali:~/Desktop/Day2/Challenge 2# binwalk pic.jpg

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0           JPEG image data, JFIF standard 1.01

root@kali:~/Desktop/Day2/Challenge 2# strings pic.jpg >out.txt
root@kali:~/Desktop/Day2/Challenge 2#
```

out.txt

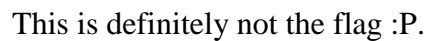
penny_8c388e74e82fd...5f7b41c507faf157.ps1

out.txt

```
w.{V
b0;t
lc5r/
J$F#$
yA[
rwp=
XsV2
@So5J{
*5+b
1' *MH
Hf `
Etz>
z{Ta
j\UU
0?.+
/,zn
Jy'<-2
1V`B
=MA,
sQ#n
=rEi
E##Q
Br0j
h\ (n
0+m|9
<U$I
k]2.
qM2Y
Bylt
pzzP
z+?k
h'oJ
pr+7T
fi$D
FhT7
n6Ff(
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

We tried decoding it using a base64 decoder online

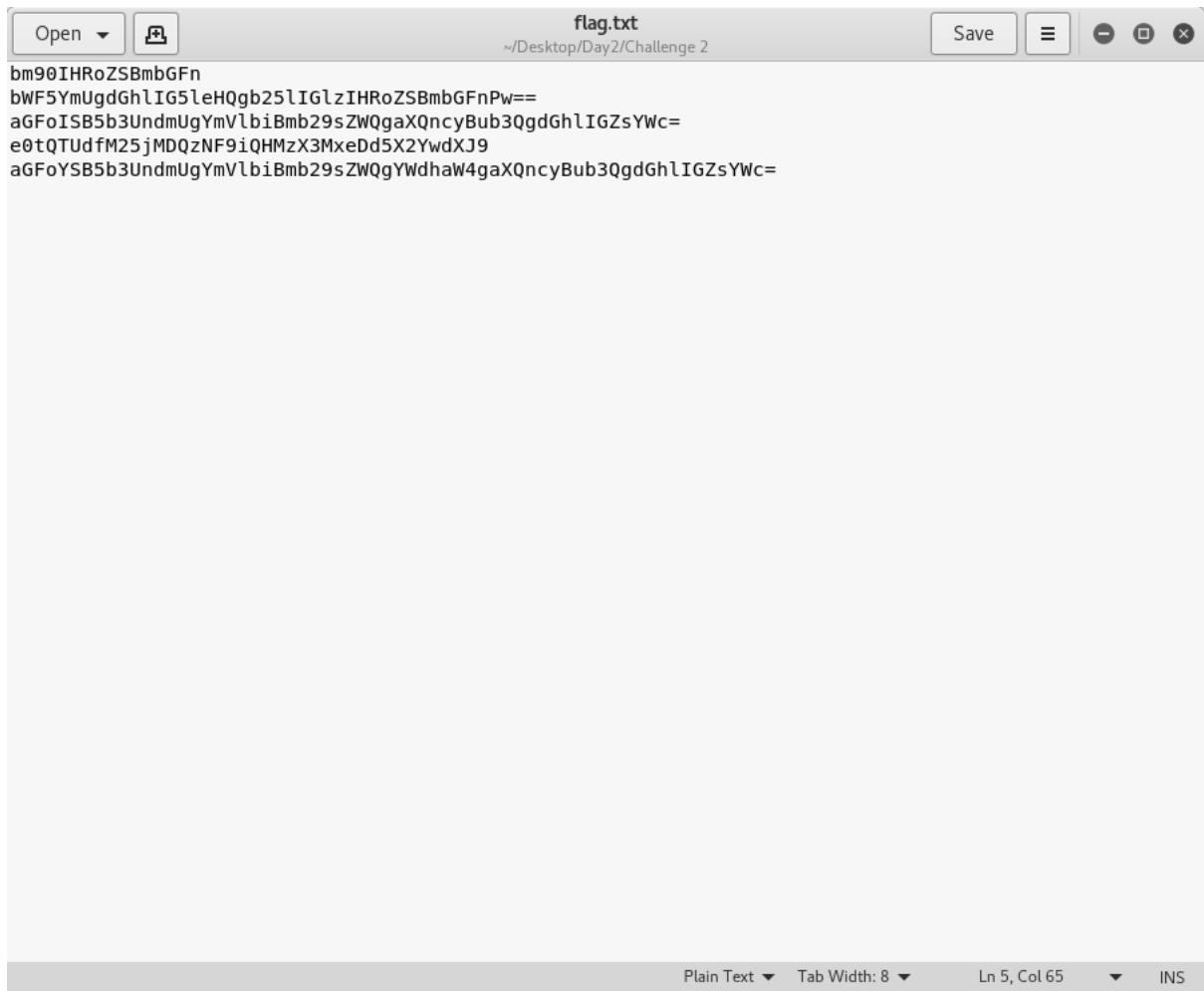


Time to use some common steganography tools we can find. First up, steghide!

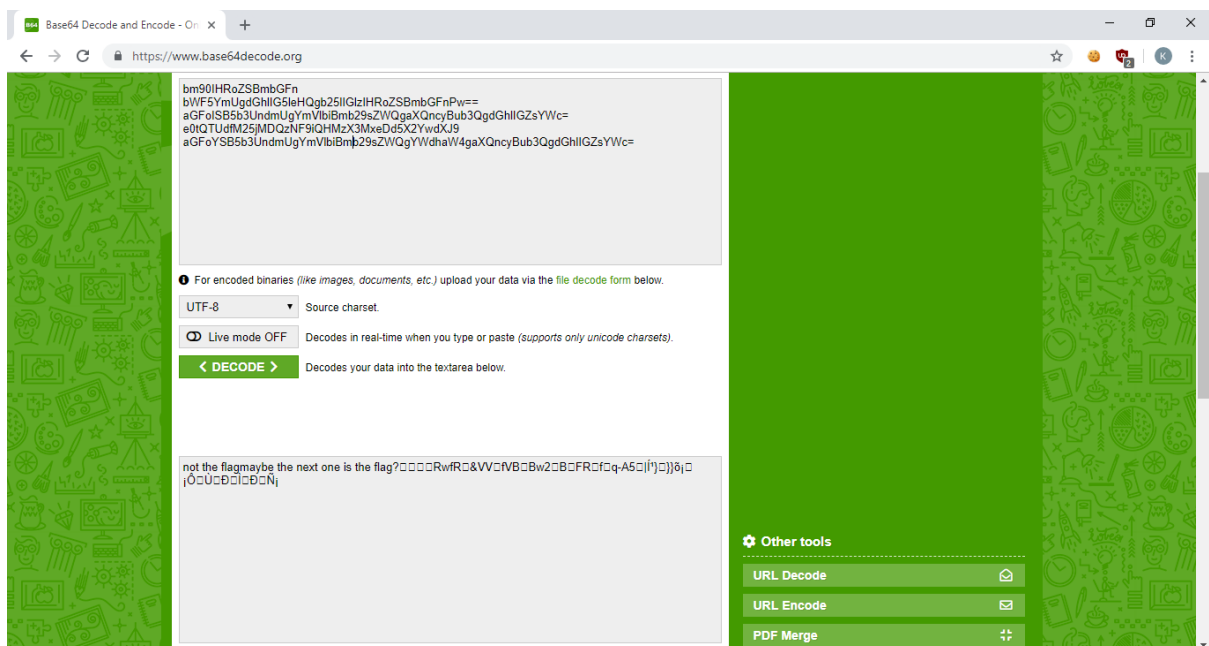
```
root@kali: ~/Desktop/Day2/Challenge 2
File Edit View Search Terminal Help
root@kali:~/Desktop/Day2/Challenge 2# steghide info pic.jpg
"pic.jpg":
  format: jpeg
  capacity: 658.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "flag.txt":
    size: 228.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
root@kali:~/Desktop/Day2/Challenge 2#
```

Bingo! We found the flag! We can now go to class peacefully :D . We extract the file out.

```
root@kali: ~/Desktop/Day2/Challenge 2
File Edit View Search Terminal Help
root@kali:~/Desktop/Day2/Challenge 2# steghide extract -sf pic.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
root@kali:~/Desktop/Day2/Challenge 2#
```



Now this definitely encoded using base64 . Run it through a base64 decoder and we should find the flag I hope.



Running it all at once doesn't provide us the flag but it gave us a hint. Maybe we should run it one by one.

The fourth line gave us the flag! e0tQTUdfM25jMDQzNF9iQHMzX3MxeDd5X2YwdXJ9 decoded to {KPMG_3nc0434_b@s3_s1x7y_f0ur} and this is our flag!

Flag = {KPMG_3nc0434_b@s3_s1x7y_f0ur}