Challange Write Up
CTF: CSICTF
Challenge: Archenemy (forensics)

P4PA_0V3RL0RD

1 Introduction

This challenge presents the player with a picture of the Arch Linux logo and nothing else.

2 Solution steps

1. Steghide reveals zip file within image

```
steghide info arched.jpeg
"arched.jpeg":
  format: jpeg
  capacity: 30.0 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "flag.zip":
    size: 27.1 KB
    encrypted: rijndael-128, cbc
    compressed: yes
```

2. Extract zip file with steghide

```
steghide extract -sf arched.jpeg
Enter passphrase:
the file "flag.zip" does already exist. overwrite ? (y/n) y
wrote extracted data to "flag.zip".
```

3. Zip file is password protected

```
unzip flag.zip
Archive:  flag.zip
[flag.zip] meme.jpg password:
```

4. Run strings on zip file, find hint to use RockYou

```
strings flag.zip | tail
&HI:%
m`:]
k#z?
to45L
|,^#k8
1e:p:'
zj"V
;;F%>
meme.jpgUT
We will, we will, ROCKYOU!PK
```

5. Run RockYou, find password is 'kathmandu'

```
fcrackzip -v -u -D -p rockyou.txt/rockyou.txt flag.zip
found file 'meme.jpg', (size cp/uc  27553/ 27752, flags 9, chk 9ed1)


PASSWORD FOUND!!!!: pw == kathmandu
```

6. Unzip with password 'kathmandu'

```
unzip flag.zip
Archive:  flag.zip
[flag.zip] meme.jpg password:
replace meme.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: meme.jpg
```

7. Flag is in meme.jpg

3 Conclusion

Challenge presented the user to use various tools related to steganograhy and forensics. No major guessing, well constructed challange.