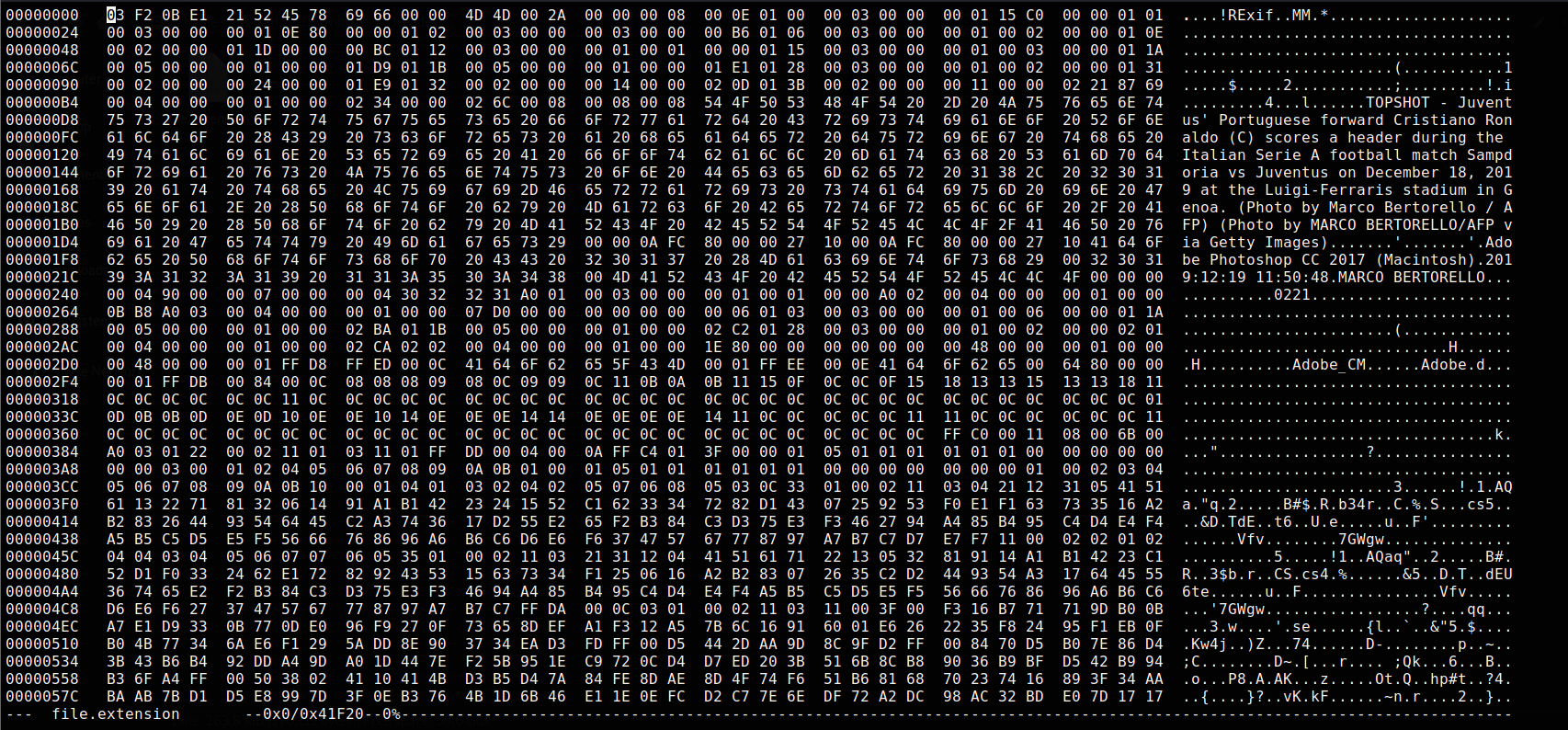
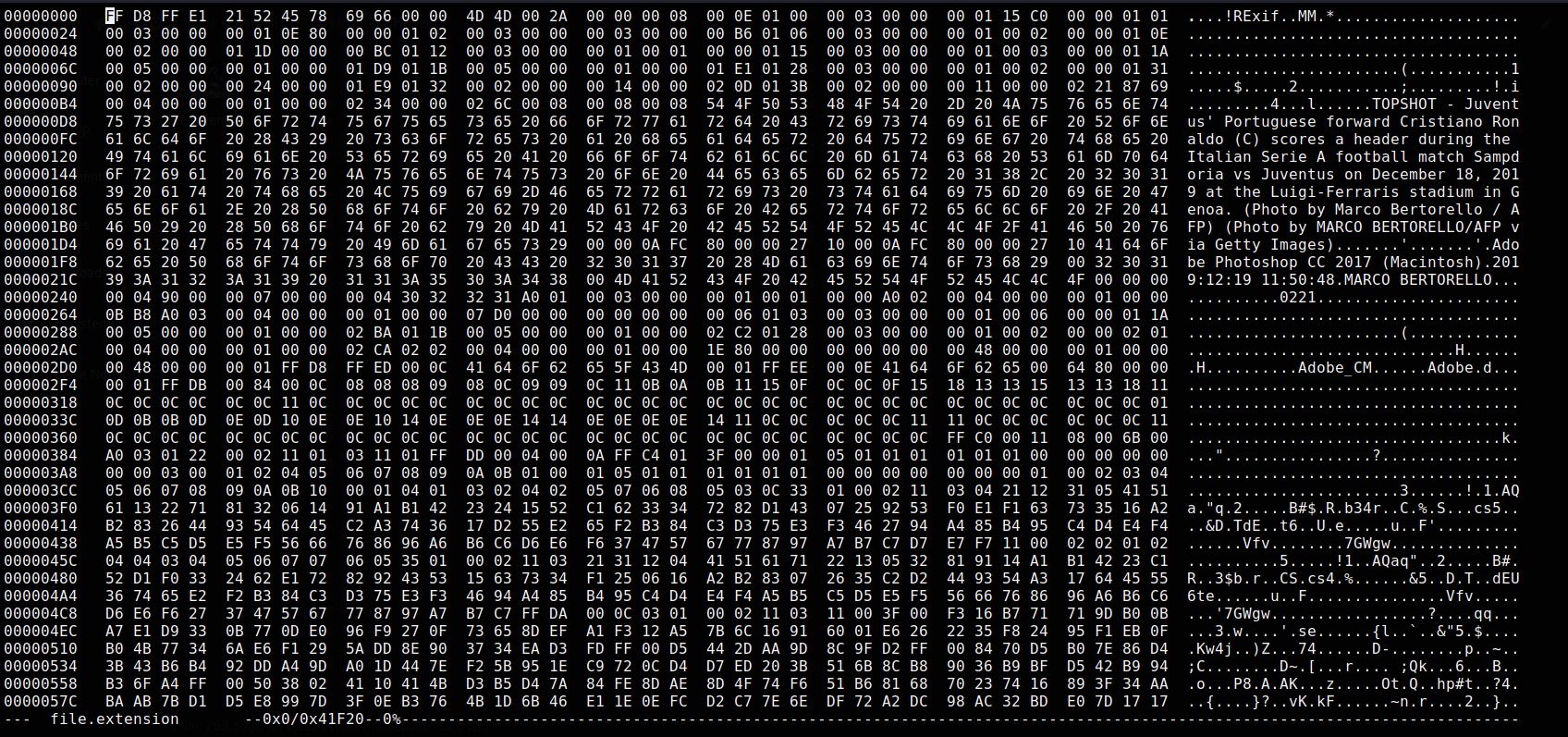
**Writeup for Tallest Header:**

We have been given a file named file.extension, whose file type is not visible in file command in Linux. So, analyzing the file using Hexedit we can get a hint that file is JPG image.

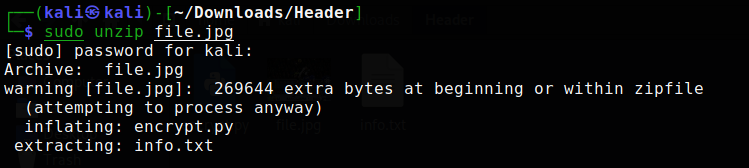


Header of this JPG image is changed; hence image was not recognized as JPG. Changing the starting HEX to the original format of JPG which is FF D8 FF we can make file detectable as Image.



But after opening Image file we can see that there’s nothing but Tallest Header Goal by Ronaldo.

Now if someone thought that image will get you to Flag, they are fallen for Rabbit Hole.

There something behind this image hidden using Steganography, which zip file and can be extracted by using command unzip on terminal.

From that zip we got two new files, i.e., encrypt.py and info.txt.

encrypt.py contain a python script for encryption of Flag using simple Permutation Cipher Algorithm.

We must write decrypt function for the same and pass parameters from info.txt in decrypt function.

In decryption function we just must inverse the key and pass inversed key and ciphertext to encrypt function to decrypt the original Flag.

decrypt.py

def inverse\_key(key):

inverse = []

for position in range(min(key),max(key)+1,1):

inverse.append(key.index(position)+1)

return inverse

def decrypt(key, ciphertext):

return encrypt(inverse\_key(key), ciphertext)

print(decrypt(key, ciphertext)

after decrypting we get a flag as output

vishwaCTF{tr1cky\_h34d3r\_w1th\_p3rmu7at10n}