Matryoshka Doll Write Up

By: Achid*on

>be me

>me wanna do CTF

>me sucks

>me do forensics

>me look at picoCTF

>me see challenge

>me do challenge until me get stuck and me peek other’s WU

>challenge turns out to be doable

>me get flag

>me make writeup

Anyway look at this funny dolls.jpg from the challenge

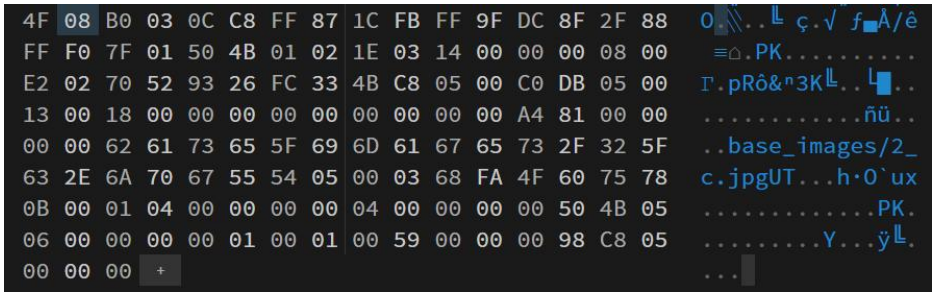
Pretty simple eh? WRONG! The flag is here

>me check metadata

>found nothing

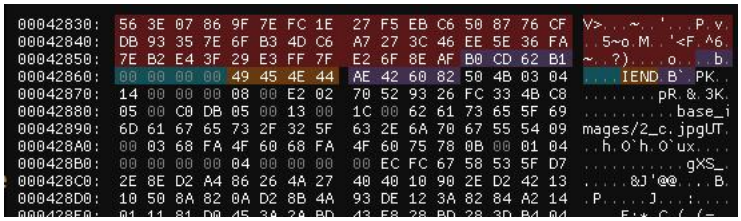
>me check hex code

>PKZip file signature



Pepega

>opens imhex at linux to check where the hexcode of the png stops before the zip hex

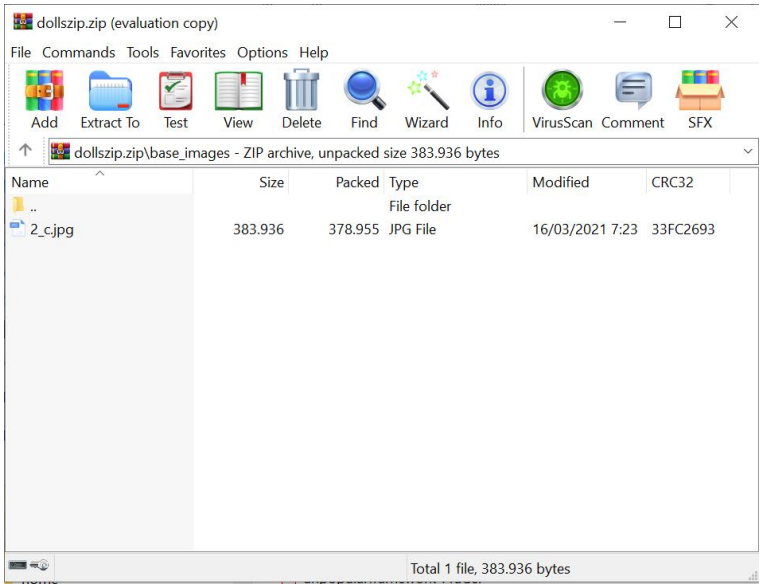


“oh it ends here, omaga”

>copy the hex code

>go to hexed.it cuz idk how to build a file locally

>create dollszip.zip from zip hexcode



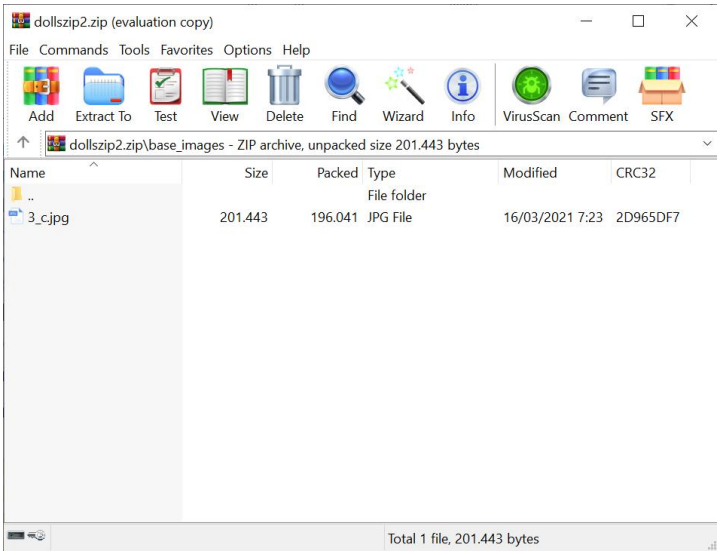
>another jpg file

>apparently it’ s a matryoshka photo again

>it’ s the same method as before

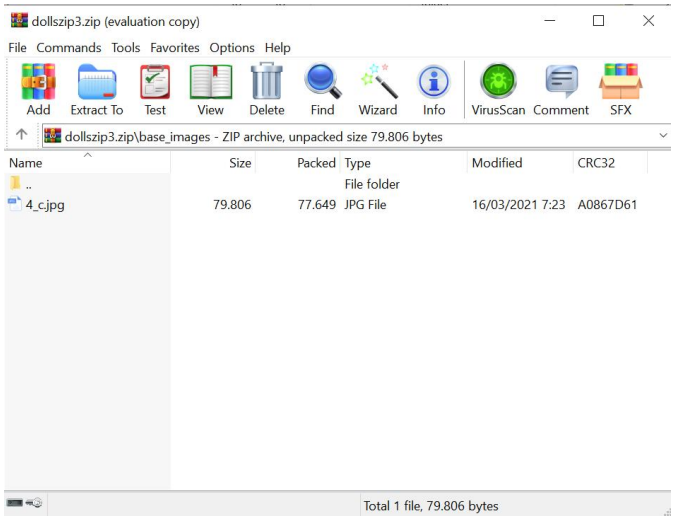
>repeat method

>3_c.jpg



>it’ s the same photo

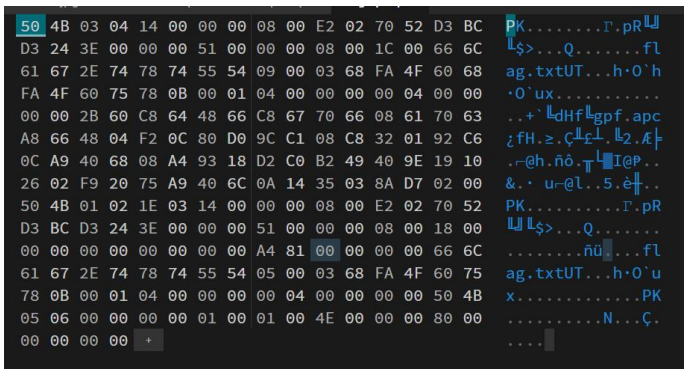
>repeat method



itsnotending.jpg

>repeat the same method AGAIN

>" hold on"

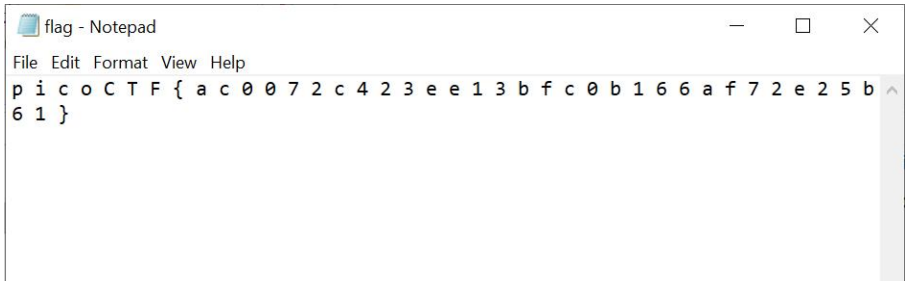


"YAY!"

>create flagzip.zip

>look into zip

>flag



Flag:

picoCTF{ac0072c423ee13bfc0b166af72e25b61}

get real