vishwaCTF

CHALLENGE NAME : ANKUSH KAUDI

DEV : AMKUSH KAUDI

CATEGORY : STEGANOGRAPHY

LEVEL : HARD

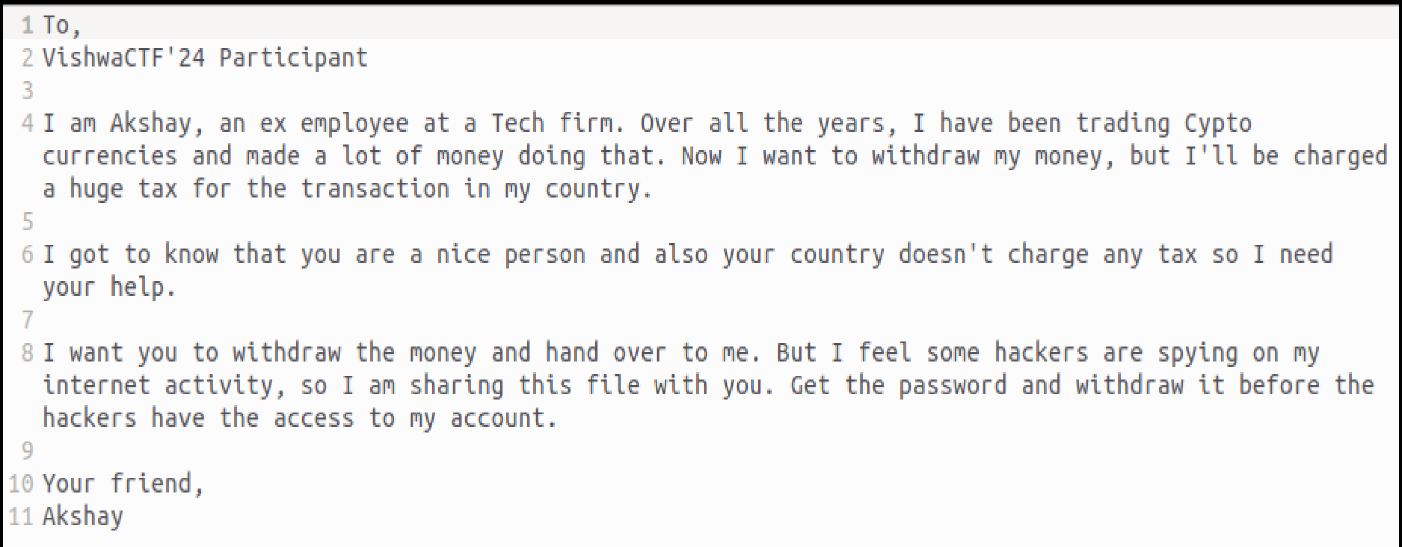
2024

vishwaCTF

Description : Akshay has a letter for you and need your help

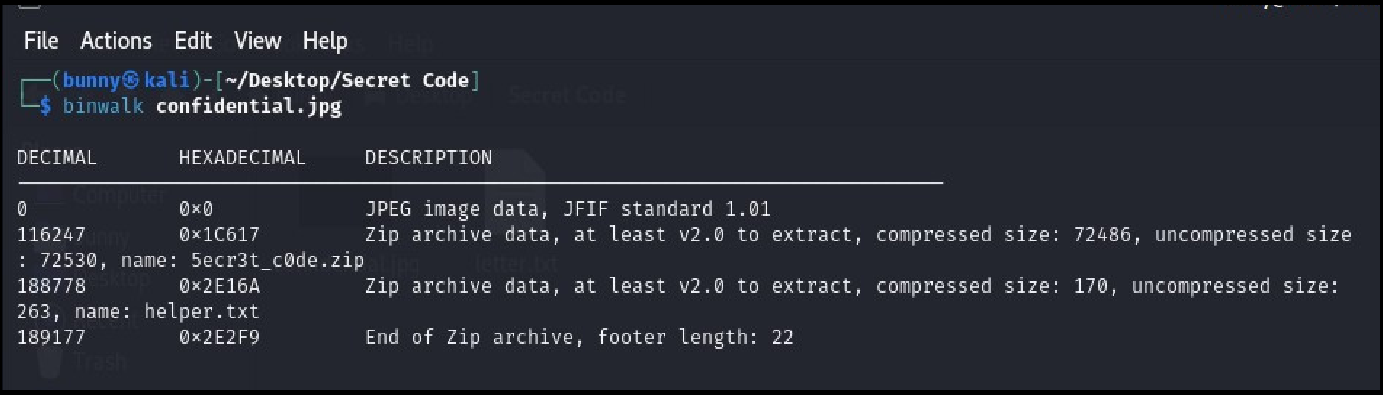
Attachments : letter.txt, confidential.jpg

Solution : Analysing the letter.txt we are supposed to find a password for Akshay's account for windrawing currency.



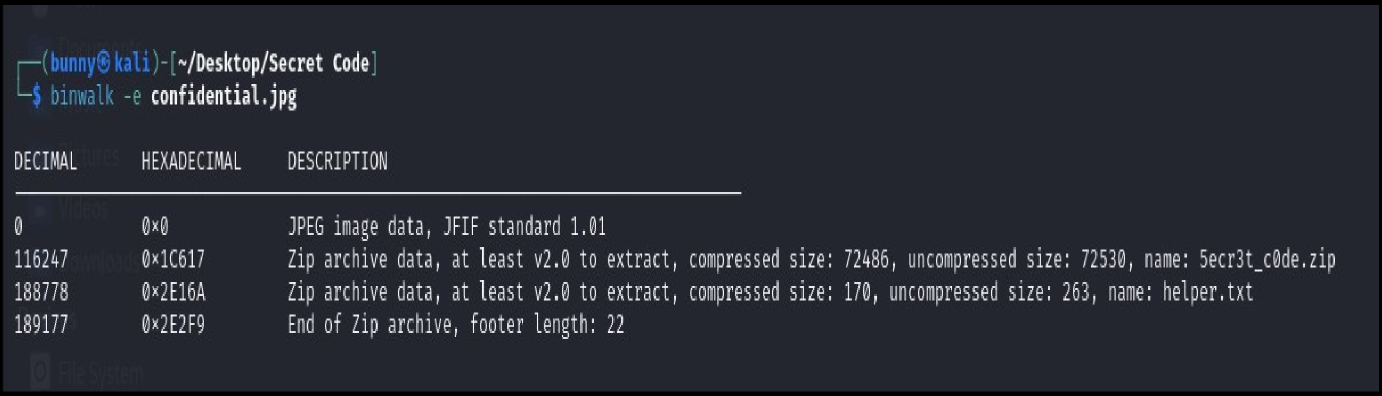
```
To,
VishwaCTF'24 Participant

I am Akshay, an ex employee at a Tech firm. Over all the years, I have been trading Cypto currencies and made a lot of money doing that. Now I want to withdraw my money, but I'll be charged a huge tax for the transaction in my country.

I got to know that you are a nice person and also your country doesn't charge any tax so I need your help.

I want you to withdraw the money and hand over to me. But I feel some hackers are spying on my internet activity, so I am sharing this file with you. Get the password and withdraw it before the hackers have the access to my account.

Your friend,
Akshay
```

The confidential.jpg is a pitch black image. Analysing this image using binwalk gives us info that it has some files in it.



```
┌──(bunny㉿kali)-[~/Desktop/Secret Code]
└─$ binwalk confidential.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
116247        0x1C617         Zip archive data, at least v2.0 to extract, compressed size: 72486, uncompressed size
: 72530, name: 5ecr3t_c0de.zip
188778        0x2E16A         Zip archive data, at least v2.0 to extract, compressed size: 170, uncompressed size:
263, name: helper.txt
189177        0x2E2F9         End of Zip archive, footer length: 22
```

We can extract the data using binwalk as follows :

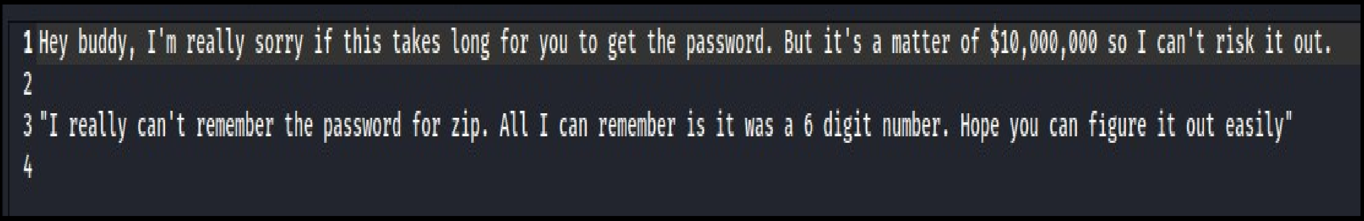


```
┌──(bunny㉿kali)-[~/Desktop/Secret Code]
└─$ binwalk -e confidential.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
116247        0x1C617         Zip archive data, at least v2.0 to extract, compressed size: 72486, uncompressed size: 72530, name: 5ecr3t_c0de.zip
188778        0x2E16A         Zip archive data, at least v2.0 to extract, compressed size: 170, uncompressed size: 263, name: helper.txt
189177        0x2E2F9         End of Zip archive, footer length: 22
```

We can see 2 files after extracting data using binwalk,

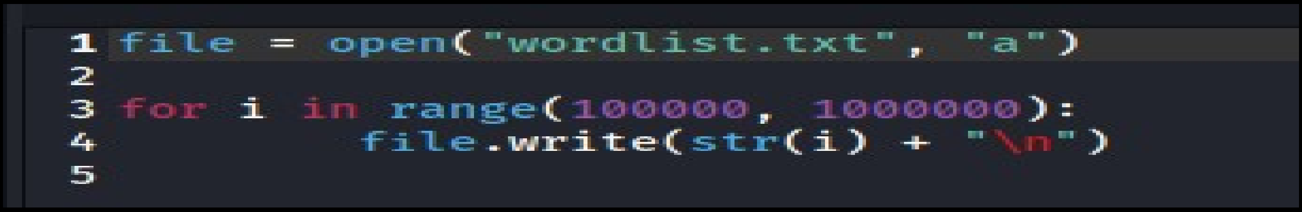
1. 5ecr3t_c0de.zip
2. helper.txt

5ecr3t_c0de.zip is password protected file and helper.txt is as follows :



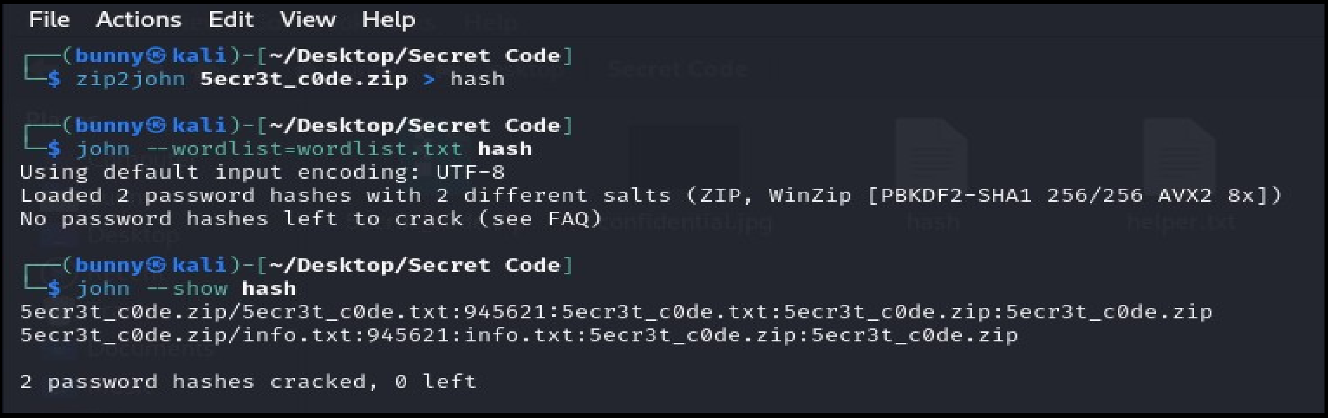
```
Hey buddy, I'm really sorry if this takes long for you to get the password. But it's a matter of $10,000,000 so I can't risk it out.

"I really can't remember the password for zip. All I can remember is it was a 6 digit number. Hope you can figure it out easily"

```

From the above text, we come to know that the password to the zip file is a 6 digit number. We can create a wordlist of all the 6 digits numbers. The following script creates the wordlist.



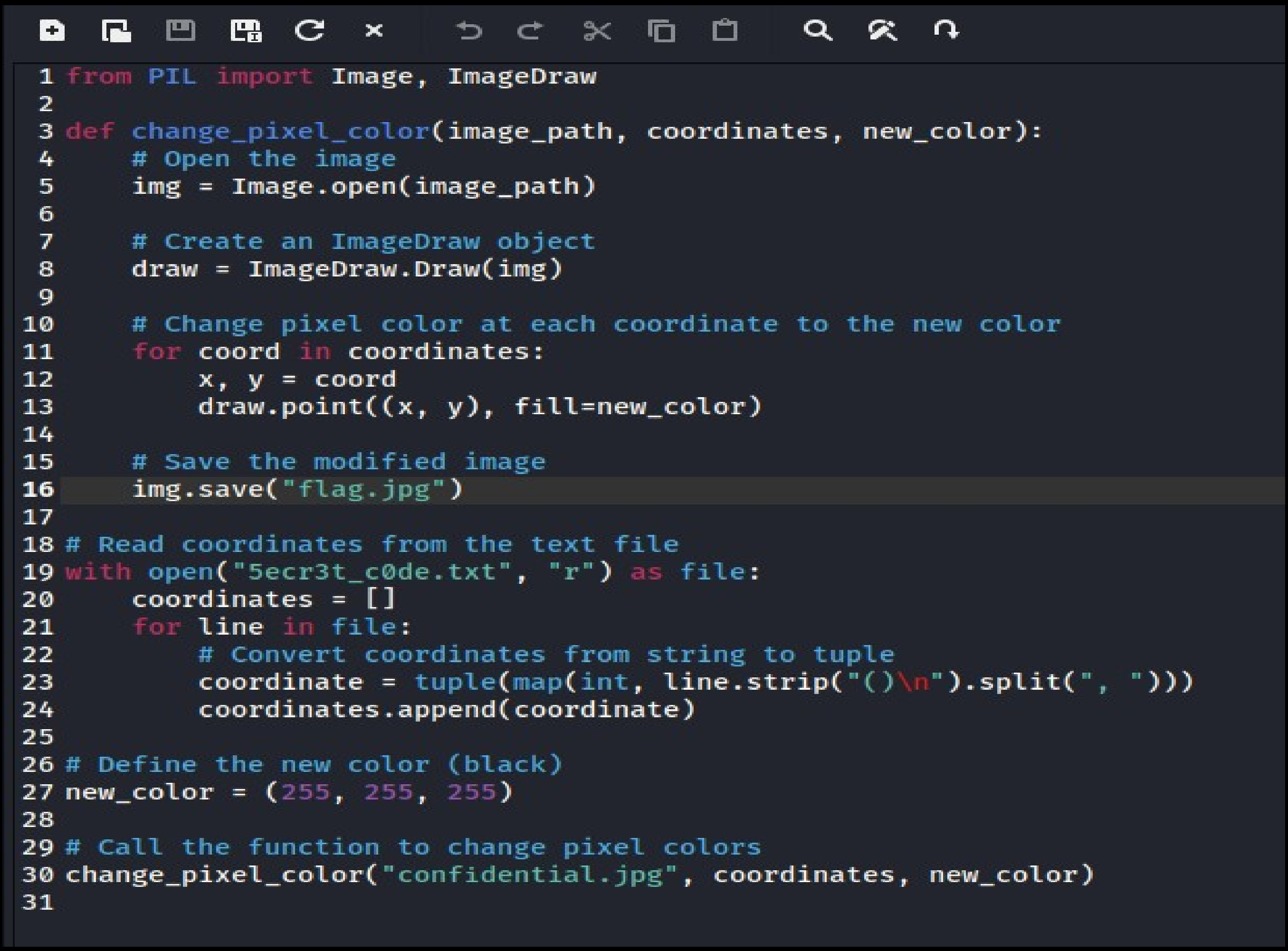
```python
file = open("wordlist.txt", "a")

for i in range(100000, 1000000):
        file.write(str(i) + "\n")

```

We have the wordlist, so we can brute force the zip using this wordlist with John The Ripper as follows and obtain the password for the zip file.



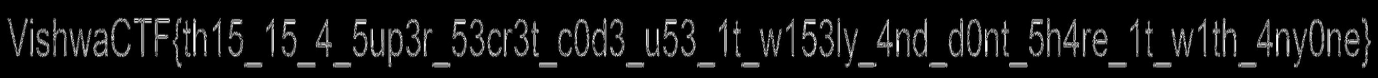
```
┌──(bunny㉿kali)-[~/Desktop/Secret Code]
└─$ zip2john 5ecr3t_c0de.zip > hash

┌──(bunny㉿kali)-[~/Desktop/Secret Code]
└─$ john --wordlist=wordlist.txt hash
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)

┌──(bunny㉿kali)-[~/Desktop/Secret Code]
└─$ john --show hash
5ecr3t_c0de.zip/5ecr3t_c0de.txt:945621:5ecr3t_c0de.txt:5ecr3t_c0de.zip:5ecr3t_c0de.zip
5ecr3t_c0de.zip/info.txt:945621:info.txt:5ecr3t_c0de.zip:5ecr3t_c0de.zip

2 password hashes cracked, 0 left
```

The password for the zip is 945621. After extracting the zip, we can see a text file named 5ecr3t_c0de.txt with some co-ordinates. We can think of plotting this co-ordinates on the given image. Following is the script which changes the pixel colour for the given co-ordinates.



```python
from PIL import Image, ImageDraw

def change_pixel_color(image_path, coordinates, new_color):
    # Open the image
    img = Image.open(image_path)

    # Create an ImageDraw object
    draw = ImageDraw.Draw(img)

    # Change pixel color at each coordinate to the new color
    for coord in coordinates:
        x, y = coord
        draw.point((x, y), fill=new_color)

    # Save the modified image
    img.save("flag.jpg")

# Read coordinates from the text file
with open("5ecr3t_c0de.txt", "r") as file:
    coordinates = []
    for line in file:
        # Convert coordinates from string to tuple
        coordinate = tuple(map(int, line.strip("()\n").split(", ")))
        coordinates.append(coordinate)

# Define the new color (black)
new_color = (255, 255, 255)

# Call the function to change pixel colors
change_pixel_color("confidential.jpg", coordinates, new_color)
```

This script will change the pixels at given co-ordinates and saved as flag.txt



VishwaCTF{th15_15_4_5up3r_53cr3t_c0d3_u53_1t_w153ly_4nd_d0nt_5h4re_1t_w1th_4ny0ne}

Flag :

VishwaCTF{th15_15_4_5up3r_53cr3t_c0d3_u53_1t_w153ly_4nd_d0nt_5h4re_1t_w1th_4ny0ne}