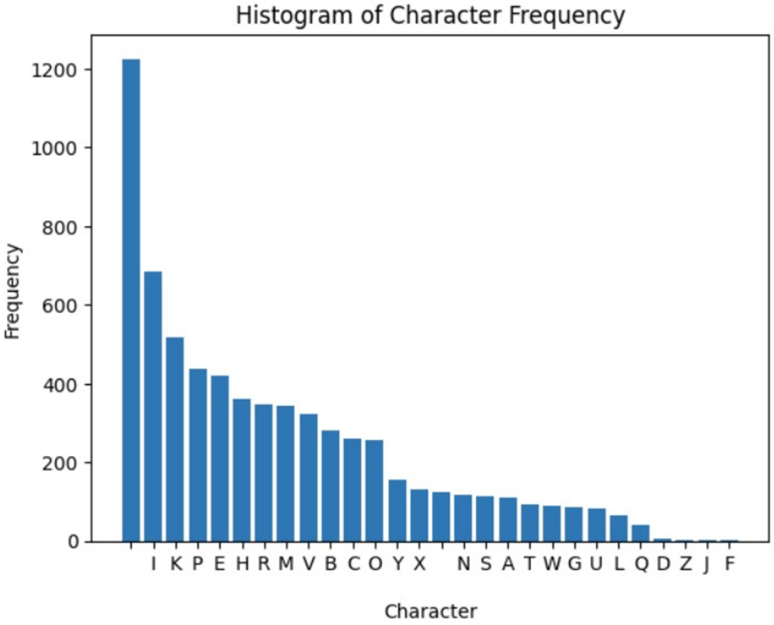
Part 2:CTF

CTF-1 :

To decrypt this text, we first analyze the cipher text by determining the frequency of each letter used within it. This involves counting how many times each letter appears in the cipher text. Next, we determine the frequency of alphabetic letters and also by observing the most common words in English like (The-He-She-It, etc..). Once we have gathered this data, we then proceed to map each letter in the cipher text to its counterpart in the alphabetic letter frequency.



plain text:

```
ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER O
BANK AND OF HAVING NOTHING TO DO ONCE OR TWICE SHE HAD PEEPED IN
BOOK HER SISTER WAS READING BUT IT HAD NO PICTURES OR CONVERSATI
IT AND WHAT IS THE USE OF A BOOK THOUGHT ALICE WITHOUT PICTURES 
CONVERSATIONS

SO SHE WAS CONSIDERING IN HER OWN MIND AS WELL AS SHE COULD FOR
```

```
DAY MADE HER FEEL VERY SLEEPY AND STUPID WHETHER THE PLEASURE O
MAKING A DAISYCHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AN
PICKING THE DAISIES WHEN SUDDENLY A WHITE RABBIT WITH PINK EYES
CLOSE BY HER

THERE WAS NOTHING SO VERY REMARKABLE IN THAT NOR DID ALICE THIN
VERY MUCH OUT OF THE WAY TO HEAR THE RABBIT SAY TO ITSELF OH DE
DEAR I SHALL BE TOO LATE BUT WHEN THE RABBIT ACTUALLY TOOK A WA
OUT OF ITS WAISTCOATPOCKET AND LOOKED AT IT AND THEN HURRIED ON
STARTED TO HER FEET FOR IT FLASHED ACROSS HER MIND THAT SHE HAD
BEFORE SEEN A RABBIT WITH EITHER A WAISTCOATPOCKET OR A WATCH T
OUT OF IT AND BURNING WITH CURIOSITY SHE RAN ACROSS THE FIELD A
IT AND WAS JUST IN TIME TO SEE IT POP DOWN A LARGE RABBITHOLE U
THE HEDGE IN ANOTHER MOMENT DOWN WENT ALICE AFTER IT

THE RABBITHOLE WENT STRAIGHT ON LIKE A TUNNEL FOR SOME WAY AND
DIPPED SUDDENLY DOWN SO SUDDENLY THAT ALICE HAD NOT A MOMENT TO
ABOUT STOPPING HERSELF BEFORE SHE FOUND HERSELF FALLING DOWN WH
TO BE A VERY DEEP WELL

EITHER THE WELL WAS VERY DEEP OR SHE FELL VERY SLOWLY FOR SHE H
PLENTY OF TIME AS SHE WENT DOWN TO LOOK ABOUT HER FIRST SHE TRI
MAKE OUT WHAT SHE WAS COMING TO BUT IT WAS TOO DARK TO SEE ANYT
THEN SHE LOOKED AT THE SIDES OF THE WELL AND NOTICED THAT THEY
FILLED WITH CUPBOARDS AND BOOKSHELVES HERE AND THERE SHE SAW MA
PICTURES HUNG UPON PEGS SHE TOOK DOWN A JAR FROM ONE OF THE SHE
SHE PASSED IT WAS LABELED ORANGE MARMALADE BUT TO HER GREAT
DISAPPOINTMENT IT WAS EMPTY SHE DID NOT LIKE TO DROP THE JAR SO
MANAGED TO PUT IT INTO ONE OF THE CUPBOARDS AS SHE FELL PAST IT

DOWN DOWN DOWN WOULD THE FALL NEVER COME TO AN END THERE WAS NO
ELSE TO DO SO ALICE SOON BEGAN TALKING TO HERSELF DINAHLL MISS
VERY MUCH TONIGHT I SHOULD THINK DINAH WAS THE CAT I HOPE
THEYLL REMEMBER HER SAUCER OF MILK AT TEATIME DINAH MY DEAR I W
YOU WERE DOWN HERE WITH ME ALICE FELT THAT SHE WAS DOZING OFF W
SUDDENLY THUMP THUMP DOWN SHE CAME UPON A HEAP OF STICKS AND DR
```

```
LEAVES AND THE FALL WAS OVER

ALICE WAS NOT A BIT HURT AND SHE JUMPED UP IN A MOMENT SHE LOOKE
BUT IT WAS ALL DARK OVERHEAD BEFORE HER WAS ANOTHER LONG PASSAGE
THE WHITE RABBIT WAS STILL IN SIGHT HURRYING DOWN IT THERE WAS N
MOMENT TO BE LOST AWAY WENT ALICE LIKE THE WIND AND WAS JUST IN
HEAR IT SAY AS IT TURNED A CORNER OH MY EARS AND WHISKERS HOW LA
ITS GETTING SHE WAS CLOSE BEHIND IT WHEN SHE TURNED THE CORNER B
THE RABBIT WAS NO LONGER TO BE SEEN

SHE FOUND HERSELF IN A LONG LOW HALL WHICH WAS LIT UP BY A ROW O
LAMPS HANGING FROM THE ROOF THERE WERE DOORS ALL ROUND THE HALL
THEY WERE ALL LOCKED AND WHEN ALICE HAD BEEN ALL THE WAY DOWN ON
AND UP THE OTHER TRYING EVERY DOOR SHE WALKED SADLY DOWN THE MID
WONDERING HOW SHE WAS EVER TO GET OUT AGAIN

SUDDENLY SHE CAME UPON A LITTLE TABLE ALL MADE OF SOLID GLASS TH
WAS NOTHING ON IT BUT A TINY GOLDEN KEY AND ALICES FIRST IDEA WA
THIS MIGHT BELONG TO ONE OF THE DOORS OF THE HALL BUT ALAS EITHE
LOCKS WERE TOO LARGE OR THE KEY WAS TOO SMALL BUT AT ANY RATE IT
WOULD NOT OPEN ANY OF THEM HOWEVER ON THE SECOND TIME ROUND SHE
UPON A LOW CURTAIN SHE HAD NOT NOTICED BEFORE AND BEHIND IT WAS
LITTLE DOOR ABOUT FIFTEEN INCHES HIGH SHE TRIED THE LITTLE GOLDE
IN THE LOCK AND TO HER GREAT DELIGHT IT FITTED

ALICE OPENED THE DOOR AND FOUND THAT IT LED INTO A SMALL PASSAGE
MUCH LARGER THAN A RATHOLE SHE KNELT DOWN AND LOOKED ALONG THE P
INTO THE LOVELIEST GARDEN YOU EVER SAW HOW SHE LONGED TO GET OUT
THAT DARK HALL AND WANDER ABOUT AMONG THOSE BEDS OF BRIGHT FLOWE
THOSE COOL FOUNTAINS BUT SHE COULD NOT EVEN GET HER HEAD THROUGH
DOORWAY OH SAID ALICE HOW I WISH I COULD SHUT UP LIKE A TELESCOP
I THINK I COULD IF I ONLY KNEW HOW TO BEGIN

ALICE WENT BACK TO THE TABLE HALF HOPING SHE MIGHT FIND ANOTHER
IT OR AT ANY RATE A BOOK OF RULES FOR SHUTTING PEOPLE UP LIKE
TELESCOPES THIS TIME SHE FOUND A LITTLE BOTTLE ON IT WHICH CERTA
```

```
WAS NOT HERE BEFORE SAID ALICE AND TIED ROUND THE NECK OF THE
BOTTLE WAS A PAPER LABEL WITH THE WORDS DRINK ME BEAUTIFULLY PRI
ON IT IN LARGE LETTERS

NO ILL LOOK FIRST SHE SAID AND SEE WHETHER ITS MARKED POISON
OR NOT FOR SHE HAD NEVER FORGOTTEN THAT IF YOU DRINK FROM A BOTT
MARKED POISON IT IS ALMOST CERTAIN TO DISAGREE WITH YOU SOONER O
LATER HOWEVER THIS BOTTLE WAS NOT MARKED POISON SO ALICE VENTURE
TO TASTE IT AND FINDING IT VERY NICE IT HAD A SORT OF MIXED FLAV
CHERRYTART CUSTARD PINEAPPLE ROAST TURKEY TOFFY AND HOT BUTTERED
TOAST SHE VERY SOON FINISHED IT OFF

WHAT A CURIOUS FEELING SAID ALICE I MUST BE SHUTTING UP LIKE A
TELESCOPE

AND SO IT WAS INDEED SHE WAS NOW ONLY TEN INCHES HIGH AND HER FA
BRIGHTENED UP AT THE THOUGHT THAT SHE WAS NOW THE RIGHT SIZE FOR
THROUGH THE LITTLE DOOR INTO THAT LOVELY GARDEN

AFTER AWHILE FINDING THAT NOTHING MORE HAPPENED SHE DECIDED ON G
INTO THE GARDEN AT ONCE BUT ALAS FOR POOR ALICE WHEN SHE GOT TO
DOOR SHE FOUND SHE HAD FORGOTTEN THE LITTLE GOLDEN KEY AND WHEN
WENT BACK TO THE TABLE FOR IT SHE FOUND SHE COULD NOT POSSIBLY R
IT SHE COULD SEE IT QUITE PLAINLY THROUGH THE GLASS AND SHE TRIE
BEST TO CLIMB UP ONE OF THE LEGS OF THE TABLE BUT IT WAS TOO SLI
AND WHEN SHE HAD TIRED HERSELF OUT WITH TRYING THE POOR LITTLE T
SAT DOWN AND CRIED

COME THERES NO USE IN CRYING LIKE THAT SAID ALICE TO HERSELF RAT
SHARPLY I ADVISE YOU TO LEAVE OFF THIS MINUTE SHE GENERALLY GAVE
HERSELF VERY GOOD ADVICE THOUGH SHE VERY SELDOM FOLLOWED IT AND
SOMETIMES SHE SCOLDED HERSELF SO SEVERELY AS TO BRING TEARS INTO
EYES

SOON HER EYE FELL ON A LITTLE GLASS BOX THAT WAS LYING UNDER THE
SHE OPENED IT AND FOUND IN IT A VERY SMALL CAKE ON WHICH THE WOR
```

```
ME WERE BEAUTIFULLY MARKED IN CURRANTS WELL ILL EAT IT SAID
ALICE AND IF IT MAKES ME GROW LARGER I CAN REACH THE KEY AND IF
MAKES ME GROW SMALLER I CAN CREEP UNDER THE DOOR SO EITHER WAY I
GET INTO THE GARDEN AND I DONT CARE WHICH HAPPENS

SHE ATE A LITTLE BIT AND SAID ANXIOUSLY TO HERSELF WHICH WAY WHI
WAY HOLDING HER HAND ON THE TOP OF HER HEAD TO FEEL WHICH WAY SH
GROWING AND SHE WAS QUITE SURPRISED TO FIND THAT SHE REMAINED TH
SIZE SO SHE SET TO WORK AND VERY SOON FINISHED OFF THE CAKE
```

CTF-2 :

We used a packet analyzer and noticed the ciphered ion GET request:

`Gur synt vf cvpbPGS{c33xno00_1_f33_h_qrnqorrs}`

using Caesar cipher with key = *39*

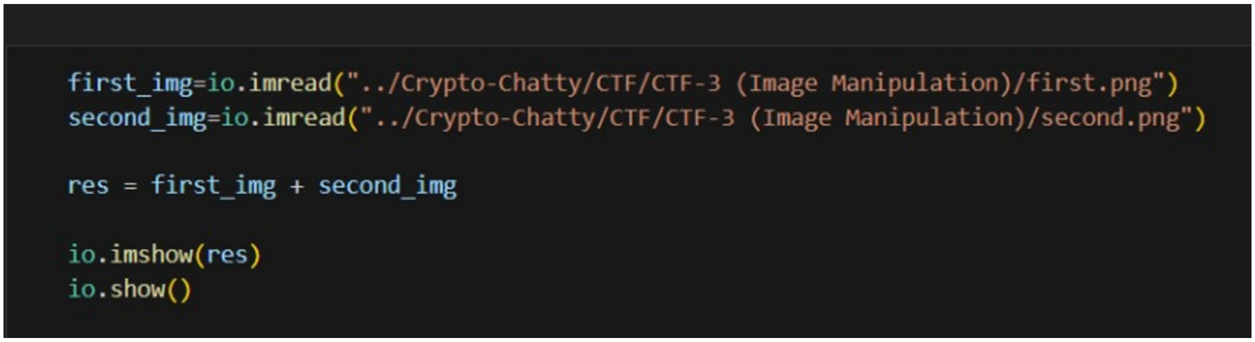
`Flag is picoCTF{p33kab00_1_s33_u_deadbeef}`

CTF-3 :

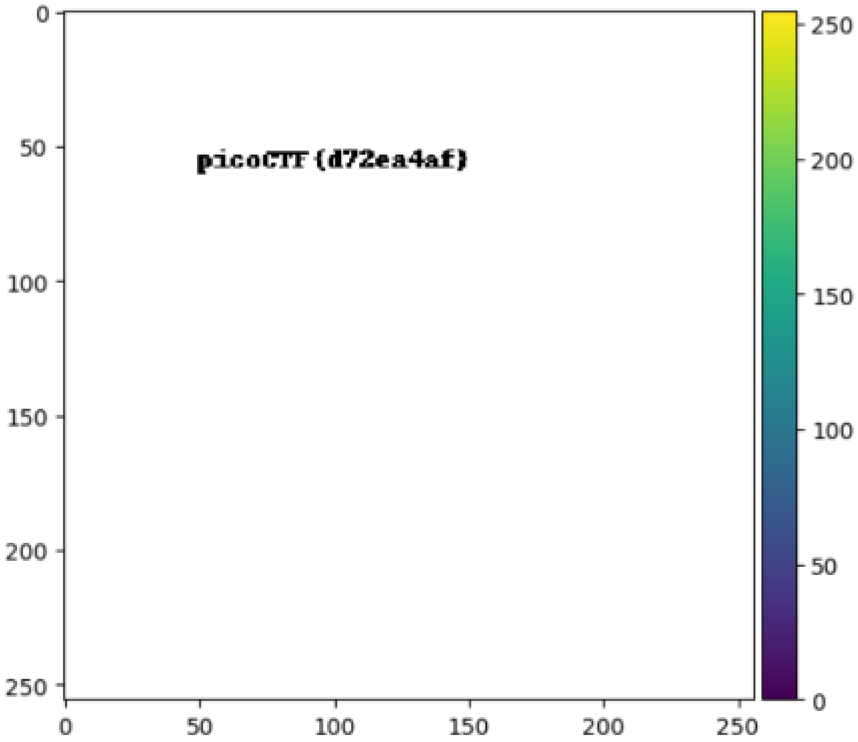
To get the flag from the two images :

Result = first image + second image

`Flag is pico`*`CTF`*`{d72ea4af}`



```
first_img=io.imread("../Crypto-Chatty/CTF/CTF-3 (Image Manipulation)/first.png")
second_img=io.imread("../Crypto-Chatty/CTF/CTF-3 (Image Manipulation)/second.png")

res = first_img + second_img

io.imshow(res)
io.show()
```



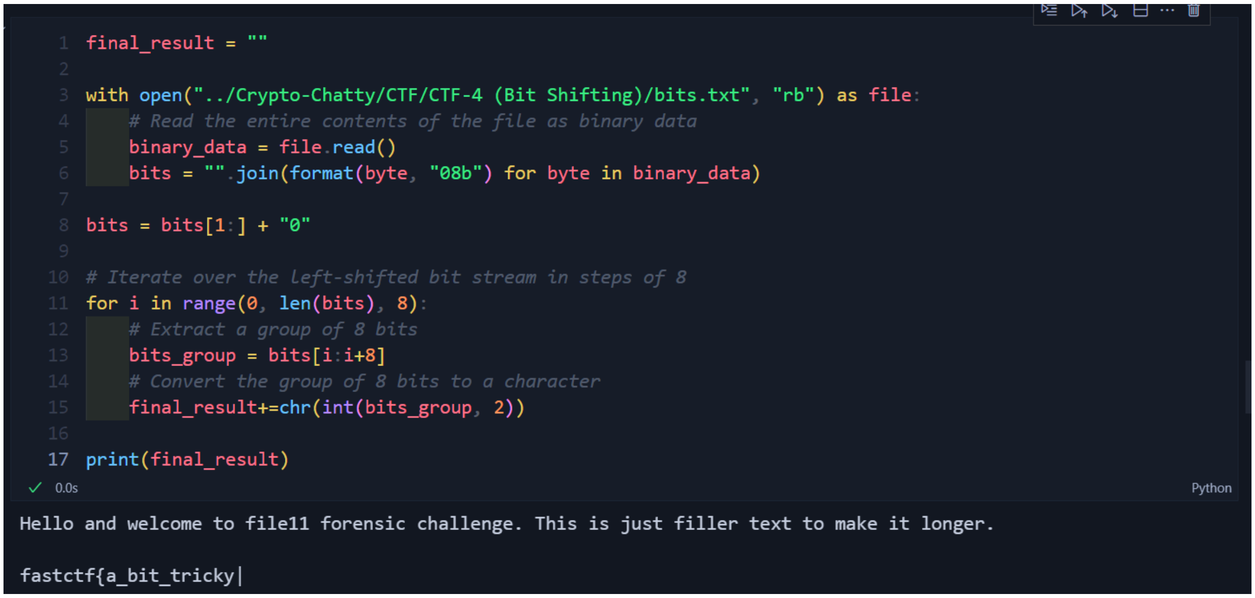
CTF-4

We read binary data from bits.txt, convert it into a string of bits, and then perform a left shift operation on these bits. After this shift, we convert groups of 8 bits back into ASCII characters. We displayed the result and we got:

Hello and welcome to file11 forensic challenge. This is just filler text to make it longer.

fastctf{a_bit_tricky

`The Flag is: fastctf{a_bit_tricky}`



```python
final_result = ""

with open("../Crypto-Chatty/CTF/CTF-4 (Bit Shifting)/bits.txt", "rb") as file:
    # Read the entire contents of the file as binary data
    binary_data = file.read()
    bits = "".join(format(byte, "08b") for byte in binary_data)

bits = bits[1:] + "0"

# Iterate over the left-shifted bit stream in steps of 8
for i in range(0, len(bits), 8):
    # Extract a group of 8 bits
    bits_group = bits[i:i+8]
    # Convert the group of 8 bits to a character
    final_result+=chr(int(bits_group, 2))

print(final_result)
```

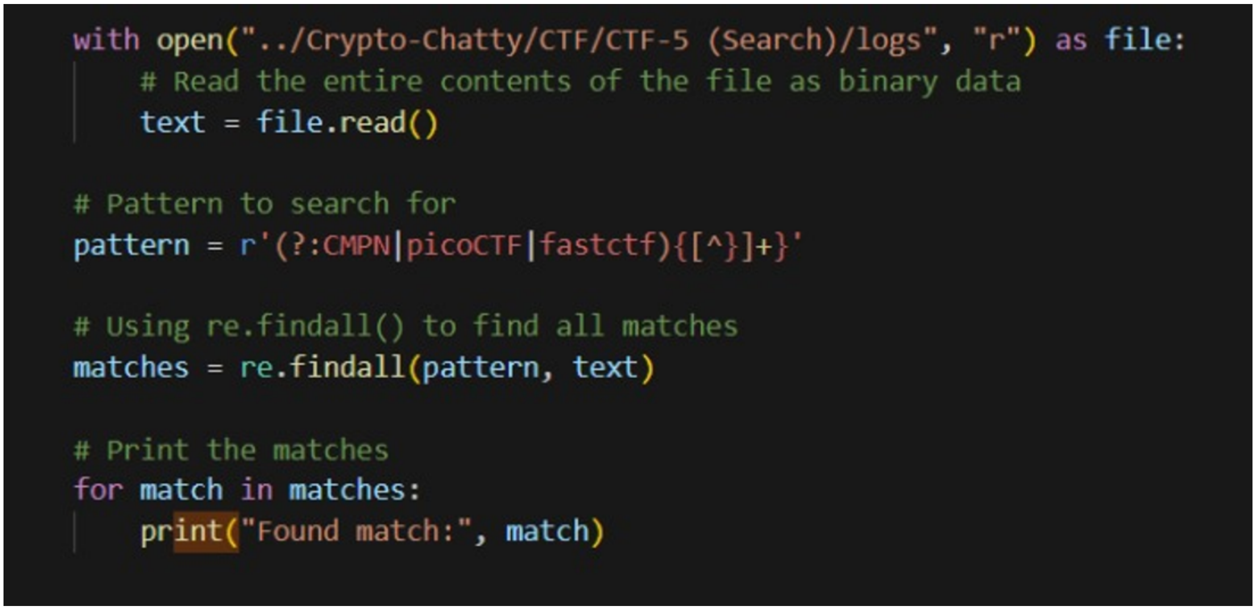
```
Hello and welcome to file11 forensic challenge. This is just filler text to make it longer.

fastctf{a_bit_tricky|
```

CTF-5

We interpret the contents of "logs" as text data. Then, we use a regular expression pattern to find specific substrings in this text.

Our goal is to identify any substring that begins with "CMPN", "picoCTF", or "fastctf", followed by a pair of curly braces that contain any characters except "}".

`Flag is: picoCTF{grep_is_good_to_find_things_dba08a45}`



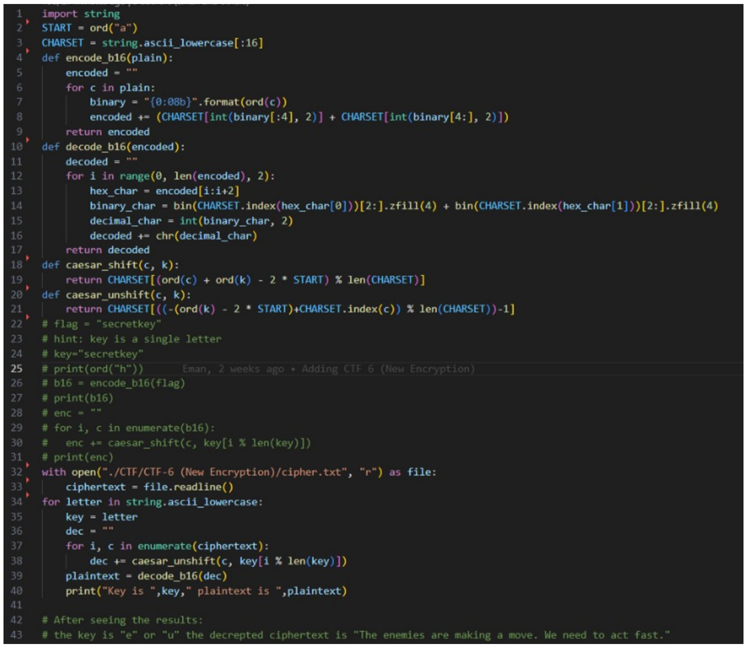
```python
with open("../Crypto-Chatty/CTF/CTF-5 (Search)/logs", "r") as file:
    # Read the entire contents of the file as binary data
    text = file.read()

# Pattern to search for
pattern = r'(?:CMPN|picoCTF|fastctf){[^}]+}'

# Using re.findall() to find all matches
matches = re.findall(pattern, text)

# Print the matches
for match in matches:
    print("Found match:", match)
```

CTF-6

We used the reverse of the Caesar shift and then decoded it, trying all possible keys. Since the hint mentioned that the key is a single letter, we continued until we obtained an intelligible sentence.

The key is e or u (This is because they are identical when considered modulo 16).

`Flag is : The enemies are making a move. We need to act fast.`



```python
import string
START = ord("a")
CHARSET = string.ascii_lowercase[:16]
def encode_b16(plain):
    encoded = ""
    for c in plain:
        binary = "{0:08b}".format(ord(c))
        encoded += (CHARSET[int(binary[:4], 2)] + CHARSET[int(binary[4:], 2)])
    return encoded
def decode_b16(encoded):
    decoded = ""
    for i in range(0, len(encoded), 2):
        hex_char = encoded[i:i+2]
        binary_char = bin(CHARSET.index(hex_char[0]))[2:].zfill(4) + bin(CHARSET.index(hex_char[1]))[2:].zfill(4)
        decimal_char = int(binary_char, 2)
        decoded += chr(decimal_char)
    return decoded
def caesar_shift(c, k):
    return CHARSET[(ord(c) + ord(k) - 2 * START) % len(CHARSET)]
def caesar_unshift(c, k):
    return CHARSET[((-(ord(k) - 2 * START)+CHARSET.index(c)) % len(CHARSET))-1]
# flag = "secretkey"
# hint: key is a single letter
# key="secretkey"
# print(ord("h"))
# b16 = encode_b16(flag)
# print(b16)
# enc = ""
# for i, c in enumerate(b16):
#   enc += caesar_shift(c, key[i % len(key)])
# print(enc)
with open("./CTF/CTF-6 (New Encryption)/cipher.txt", "r") as file:
    ciphertext = file.readline()
for letter in string.ascii_lowercase:
    key = letter
    dec = ""
    for i, c in enumerate(ciphertext):
        dec += caesar_unshift(c, key[i % len(key)])
    plaintext = decode_b16(dec)
    print("Key is ",key," plaintext is ",plaintext)

# After seeing the results:
# the key is "e" or "u" the decrepted ciphertext is "The enemies are making a move. We need to act fast."
```

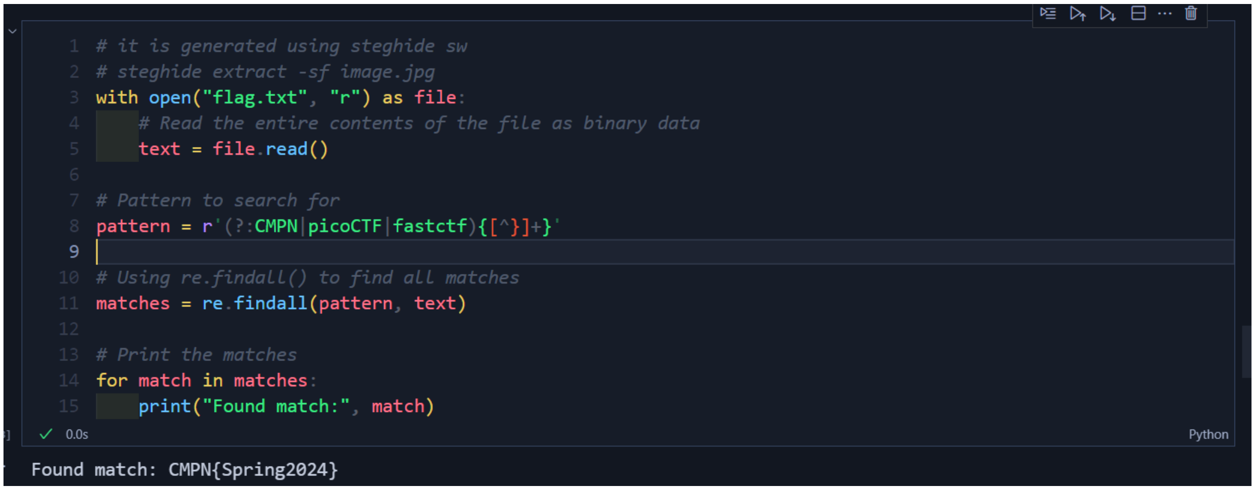
CTF-7

We used a command `steghide extract -sf pepo_evil.jpg` with password `HIDING`

to extract the flag.txt which contains: "Hello, the flag is CMPN{Spring2024}"

Then, we searched for a pattern, either CMPN, picoCTF, or fastctf.

`Flag is CMPN{Spring2024}`



```python
# it is generated using steghide sw
# steghide extract -sf image.jpg
with open("flag.txt", "r") as file:
    # Read the entire contents of the file as binary data
    text = file.read()

# Pattern to search for
pattern = r'(?:CMPN|picoCTF|fastctf){[^}]+}'

# Using re.findall() to find all matches
matches = re.findall(pattern, text)

# Print the matches
for match in matches:
    print("Found match:", match)
```

```
Found match: CMPN{Spring2024}
```

CTF-8

1. We used an online tool to convert the Morse code audio into text. The text we received was:

   THE RUSSIAN TERRORISTS ARE THE ONES WHO STARTED THIS, THEY ARE THE KEY. PLEASE YOU MUST EXTRACT ME

2. We used an online steganography tool and extracted ciphertext and a Wikipedia link from the audio:

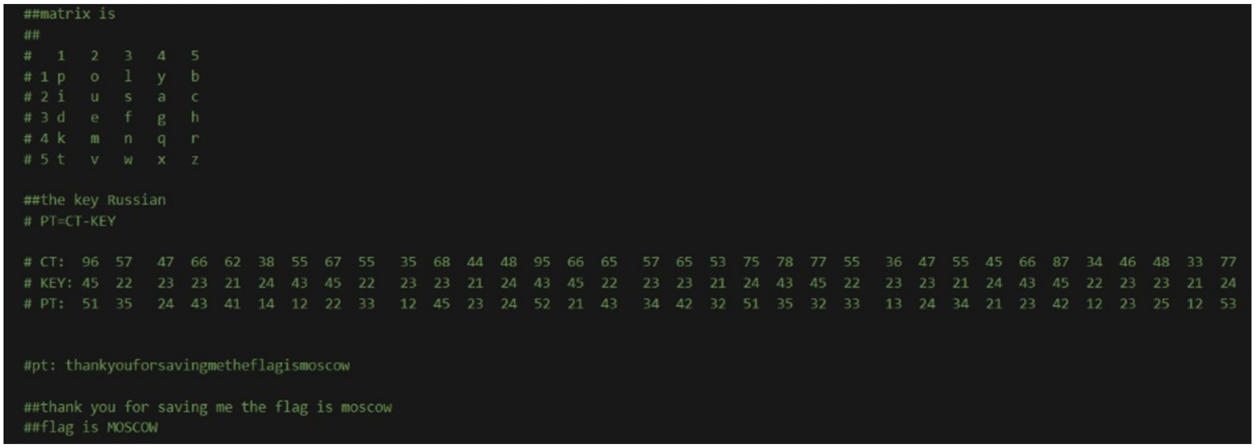
   https://en.wikipedia.org/wiki/Nihilist_cipher?keyword=polybius

   96 57 47 66 62 38 55 67 55 35 68 44 48 95 66 65 57 65 53 75 78 77 55 36 47 55 45 66 87 34 46 48 33 77

3. We used the Nihilist cipher with keyword=polybius and key = Russian.

plain text: thank you for saving me the flag is Moscow

`Flag is MOSCOW`



```
##matrix is
##
#   1   2   3   4   5
# 1 p   o   l   y   b
# 2 i   u   s   a   c
# 3 d   e   f   g   h
# 4 k   m   n   q   r
# 5 t   v   w   x   z

##the key Russian
# PT=CT-KEY

# CT:  96  57   47  66  62  38  55  67  55   35  68  44  48  95  66  65   57  65  53  75  78  77  55   36  47  55  45  66  87  34  46  48  33  77
# KEY: 45  22   23  23  21  24  43  45  22   23  23  21  24  43  45  22   23  23  21  24  43  45  22   23  23  21  24  43  45  22  23  23  21  24
# PT:  51  35   24  43  41  14  12  22  33   12  45  23  24  52  21  43   34  42  32  51  35  32  33   13  24  34  21  23  42  12  23  25  12  53


#pt: thankyouforsavingmetheflagismoscow

##thank you for saving me the flag is moscow
##flag is MOSCOW
```