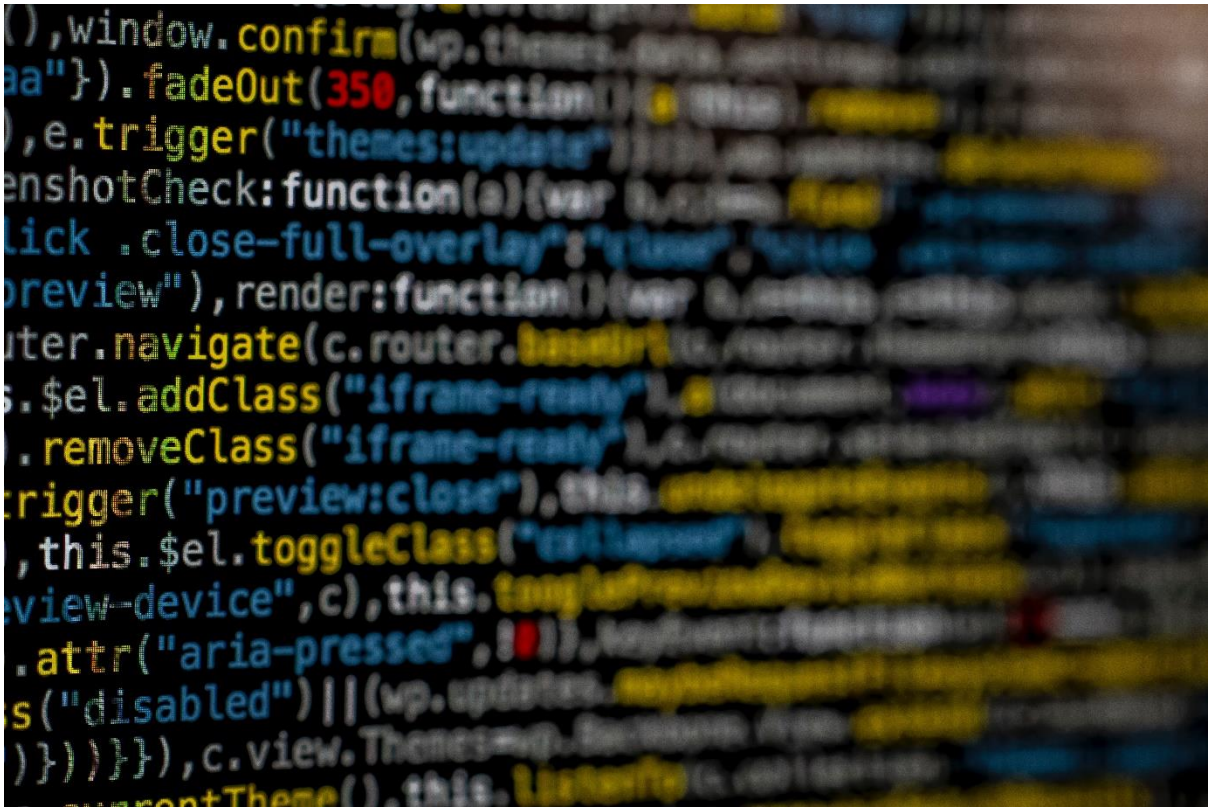
CTF Name: Cyber Defender conducted by CYSCOM (VIT Chennai)
Category: Forensics {Image Steganography}
Challenge's difficulty level: This is a beginner level CTF, if you are a beginner who wants to learn about CTF's, this room is perfect for you

We will solve and complete the given Challenge. So, let's dive in!



(This is the image (cyscom.jpg) provided for completing the challenge)

Task 1:

Deploy the machine first. Use the strings command which returns each string type of characters that are printable in the file. To extract the string from this file, execute the command as follows:

```
root@kali:~/Desktop# strings cyscom.jpg
```

This extracts all the strings present in cyscom.jpg image file.

```
JFIF
#*%%*525EE\
#*%%*525EE\
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
+)er
YD\'
en763
RMI/#
@       KIK@    E
Wn=O
"le2*
        %>y
=Bfi
+"mS!
}gWW
:}Exu
:M"tb+X
)By,
^}rl
```

```
.Bd`
=3Zk
+EP(
+(;xS
+       ?2
$qUb
lWmgn
9 {v
^ry9=
!U<c
xRC1
_P      '
R{RF
FrIQ
"[9#
q]46
{c5-
GrGZ
kz4L
W}ghN
02m4p
IR0H
I%U`
^K$`
```

At the end of the string a binary string was appended which was the passphrase for the steganographic image

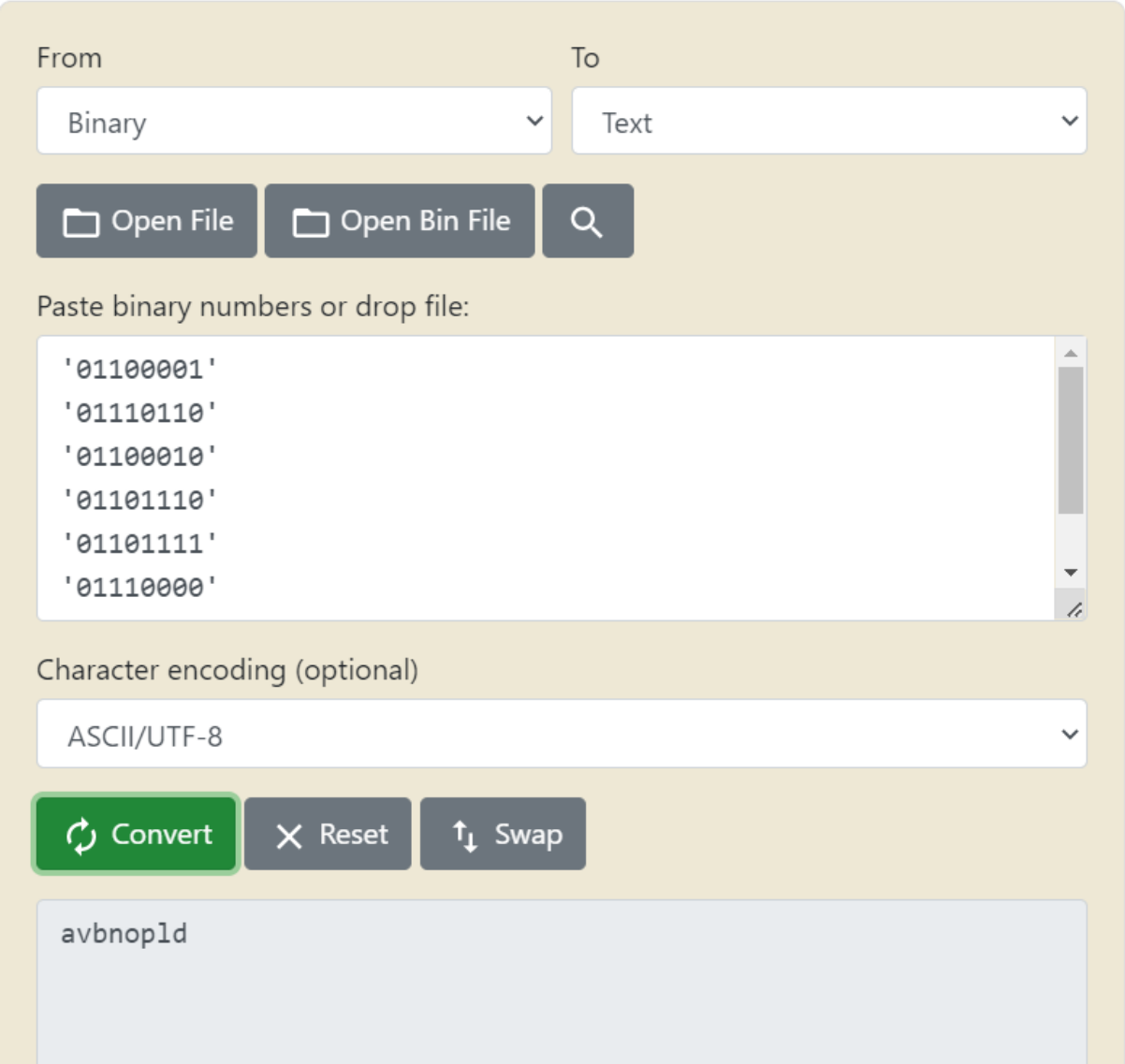
```
r0NI
oN:z
w#pc
        cocVc
v*xm
.2Ku
gh#*wc'>
"#9E
py?t
{RKQ
9 gv1
=r0+
}ENs
TXW'
7 7Q
#c#qC
Ed\yyn
FFx8
?5Vq
jFc>
NG9z
pjP:c
01100001011101100110001001101110011011110111000001101100011001 00
```

Task 2:

Convert this binary string into ASCII characters. Since each letter is made of 8 binary strings and length of the whole string is 64 which means the passphrase has 8 letters. Using python and performing string operation we acquired the binary string of each letter of passphrase separately.

```
root@kali:~/Desktop# python
Python 2.7.18 (default, Jan 27 2022, 02:05:20)
[GCC 11.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> s="0110000101110110011000100110111001101111011100000110110001100100"
>>> len(s)
64
>>> for i in range(0,8):
...     s[0:8]
...     s=s[8:]
...
'01100001'
'01110110'
'01100010'
'01101110'
'01101111'
'01110000'
'01101100'
'01100100'
```

After operating the above commands we used an online Binary to ASCII converter tool to convert the above binary string to ASCII.



We got the passphrase for the image.

Task 3:

Using steghide function extract the file hidden in cyscom.jpg image. Use the command as follows and enter the passphrase to know the name of the file hidden.

```
root@kali:~/Desktop# steghide extract -sf cyscom.jpg
Enter passphrase:
the file "cyscomctf.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "cyscomctf.txt".
```

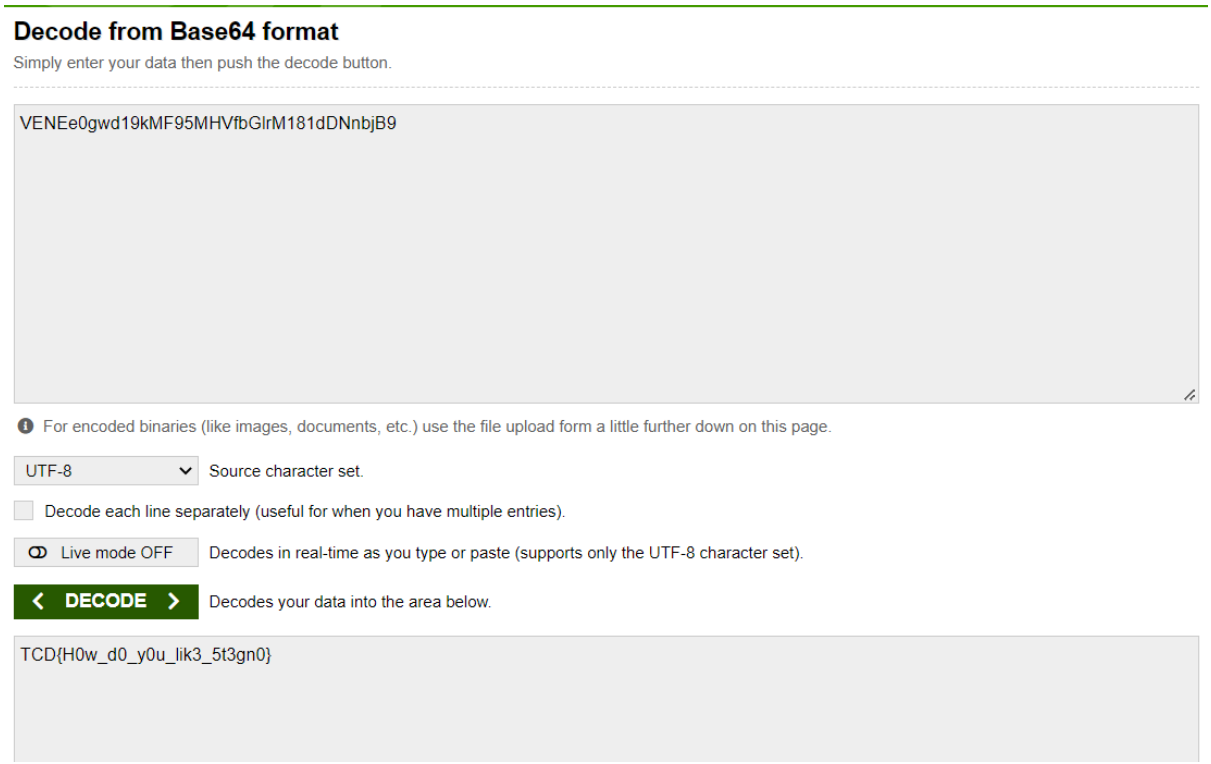
The hidden file is now extracted.

Task 4:

Use the cat command to extract the flag from the cyscomctf.txt file .

```
root@kali:~/Desktop# cat cyscomctf.txt
VENEe0gwd19kMF95MHVfbGlrM181dDNnbjB9root@kali:~/Desktop#
```

Though we got the flag the flag is in Base64 format which need to be converted to the ASCII format. Use online Base64 to ASCII converter tool to capture the flag.



“TCD{H0w_d0_y0u_lik3_5t3gn0} “. This is the flag we captured and completed steganographic challenge.