Author : Jayesh Jaiswal; Atharva Gawas.
Title : Aaj Wednesday Hai...
Category : Miscellaneous
Git-Hub Links :
https://github.com/Jayesh-2003
https://github.com/ATHARVA-GAWAS
Category : Miscellaneous
Description : oh my god EOF.
Flag : VishwaCTF{_sinclair_addams_barclay_petropolus_walker_galpin_thornhill_weems}

Writeup

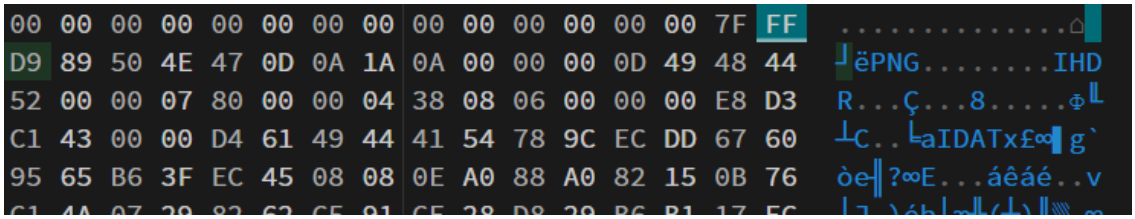
1] We can see little bit text in image soo try changing its brightness and contrast.Inorder to see the text clearly.

We can see it like this

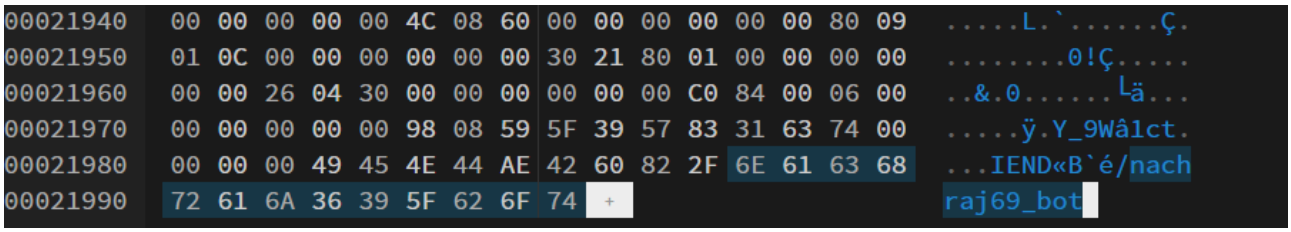
Text – "https://t.me" find other half of me also you may get 1st part of flag in image in image

soo we can get that the other half is in image, soo it is in the HEX data of image and also as the file name suggest check up to end of file soo check the ends in jepg

we can see that after the end of jepg file that is FFD9 the file dosen't end we can see a png image HEX data starts.



also scrolling to totall end we can see half bot link i.e "/nachraj69_bot"



2] Concatenating the bot parts we get link as "https://t.me/nachraj69_bot" this link will not open in browser as its a telegram link so for converting it for browser by adding telegram in place of t in t.me

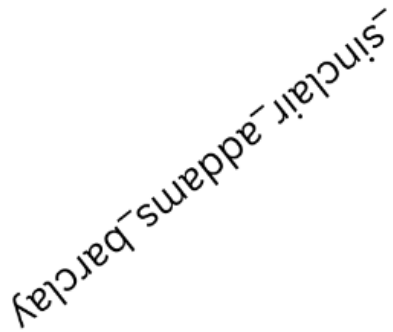
---

Soo the link becomes "https://telegram.me/nachraj69_bot"

Now we know that 1st part of falg is in image soo as we seen that at tnd of file that is FFD9 there is png file soo extracting it by writing a python code for converting HEX to image after FFD9

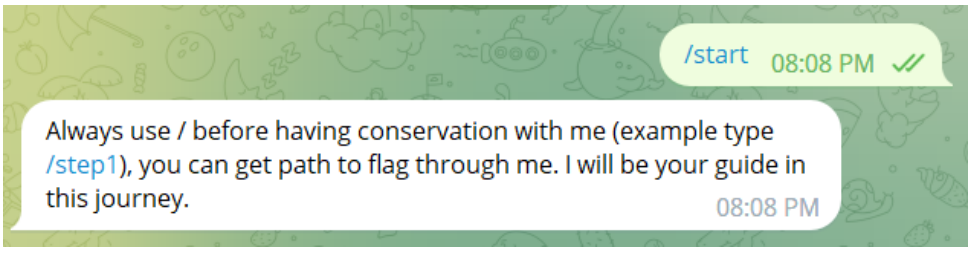
```
import PIL.Image
import io
with open("ki.jpeg","rb") as f:
    content=f.read()
    offset=content.index(bytes.fromhex('FFD9'))

    f.seek(offset+2)
    new_img = PIL.Image.open(io.BytesIO(f.read()))
    new_img.save("new_image.png")
```

Congracts we got first part of flag "_sinclair_addams_barclay"

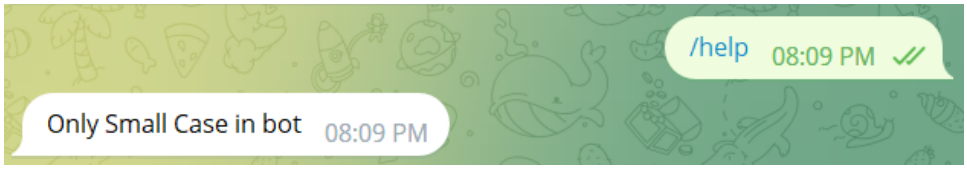


3] Now moving towards Telegram bot

As we now basic commands that work on Telegram bots like /start and /help

we get 

after using /start

and this 

after using /help

4] as given after /start "Always use / before having conservation with me (example type /step1), you can get path to flag through me. I will be your

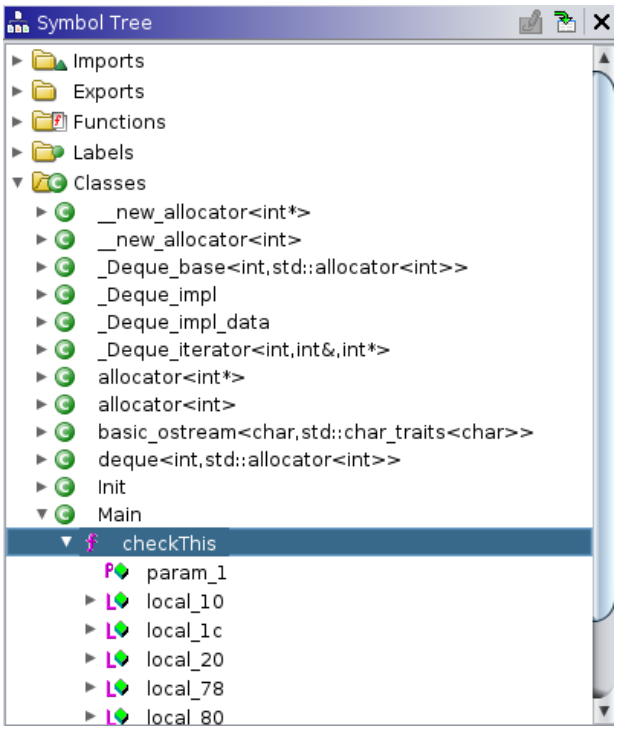
guide in this journey.”

soo typing /step1 we get 

opening this link “https://shorturl.at/guEFY”

we will get a CPP output excutable, after running it we get “This is a coding question and Guess Its Name from Leetcode website,which concepts from english it checks? Type name of concept in bot.1”

5] Analyzing it with ghidra, opening main class and a function made in it




```
/* Main::checkThis(int) */

undefined8 __thiscall Main::checkThis(Main *this,int param_1)

{
  int iVar1;
  int *piVar2;
  undefined8 uVar3;
  int local_84;
  stack<int,std::deque<int,std::allocator<int>>> local_78 [88];
  int local_20;
  int local_1c;

  std::stack<int,std::deque<int,std::allocator<int>>>::
  stack<std::deque<int,std::allocator<int>>,void>(local_78);
  local_84 = param_1;
  iVar1 = param_1;
  if (param_1 < 0) {
    uVar3 = 0;
  }
  else {
    for (; local_1c = iVar1, local_84 != 0; local_84 = local_84 / 10) {
      local_20 = local_84 % 10;
                    /* try { // try from 00101383 to 00101387 has its CatchHandler @ 0010143b */
      std::stack<int,std::deque<int,std::allocator<int>>>::push(local_78,&local_20);
      iVar1 = local_1c;
    }
    for (; local_1c != 0; local_1c = local_1c / 10) {
      piVar2 = (int *)std::stack<int,std::deque<int,std::allocator<int>>>::top();
      if (*piVar2 != local_1c % 10) {
        uVar3 = 0;
        goto LAB_0010142b;
      }
      std::stack<int,std::deque<int,std::allocator<int>>>::pop(local_78);
    }
    uVar3 = 1;
  }
LAB_0010142b:
  std::stack<int,std::deque<int,std::allocator<int>>>::~stack(local_78);
  return uVar3;
}
```

Doing some reversing techniques and analysing what is hapening with variables we can get that function is used to check the concept of palindrome from english. typing that concept in bot gives

we get a link "http://shorturl.at/HKLOY"

6] Opening this link we get a music file in which voice says "who is she, type her name in the bot once you find her also the second part of flag is in the picture also their are many secrets in audio"

---

using string we can get that something is in its metadata

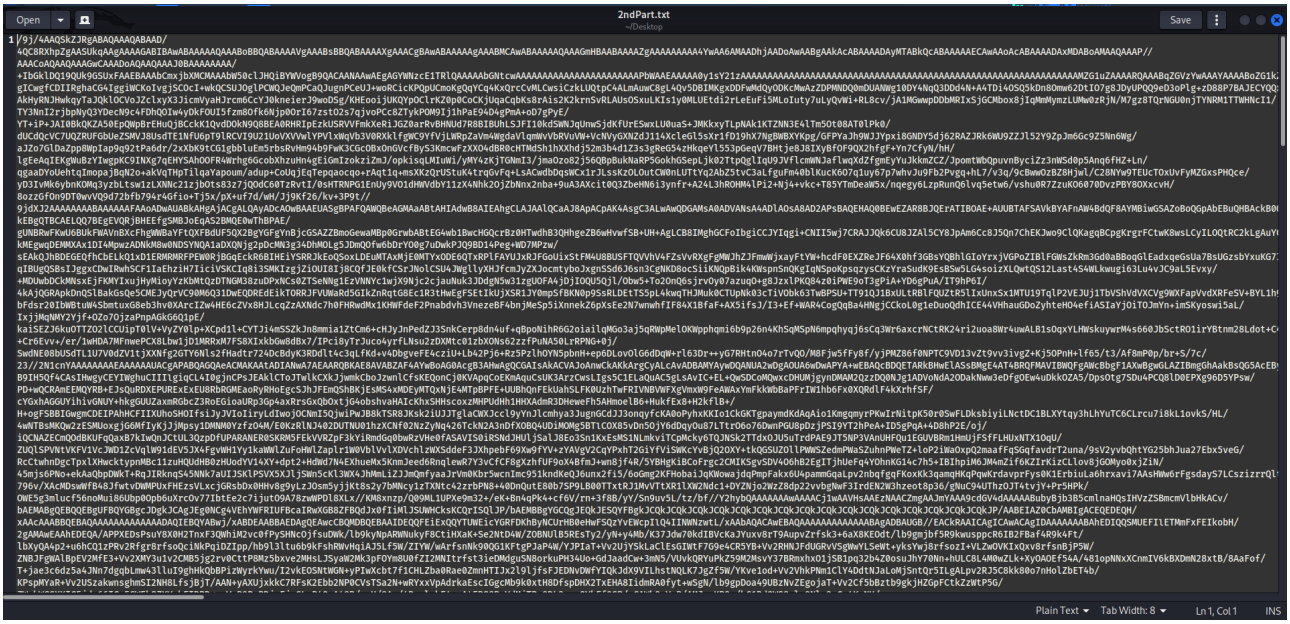
```
LIST
INFOINAM"
Wednesday's child is full of woe
ICMTz
first name of persone who is hyde in the Show
one of dialogue of show is given as title or track name is the passphrase
ID3
vCOMM
TIT2
WXXX
https://youtu.be/z4t2_6SFiPo
```

so checking mediainfo we get

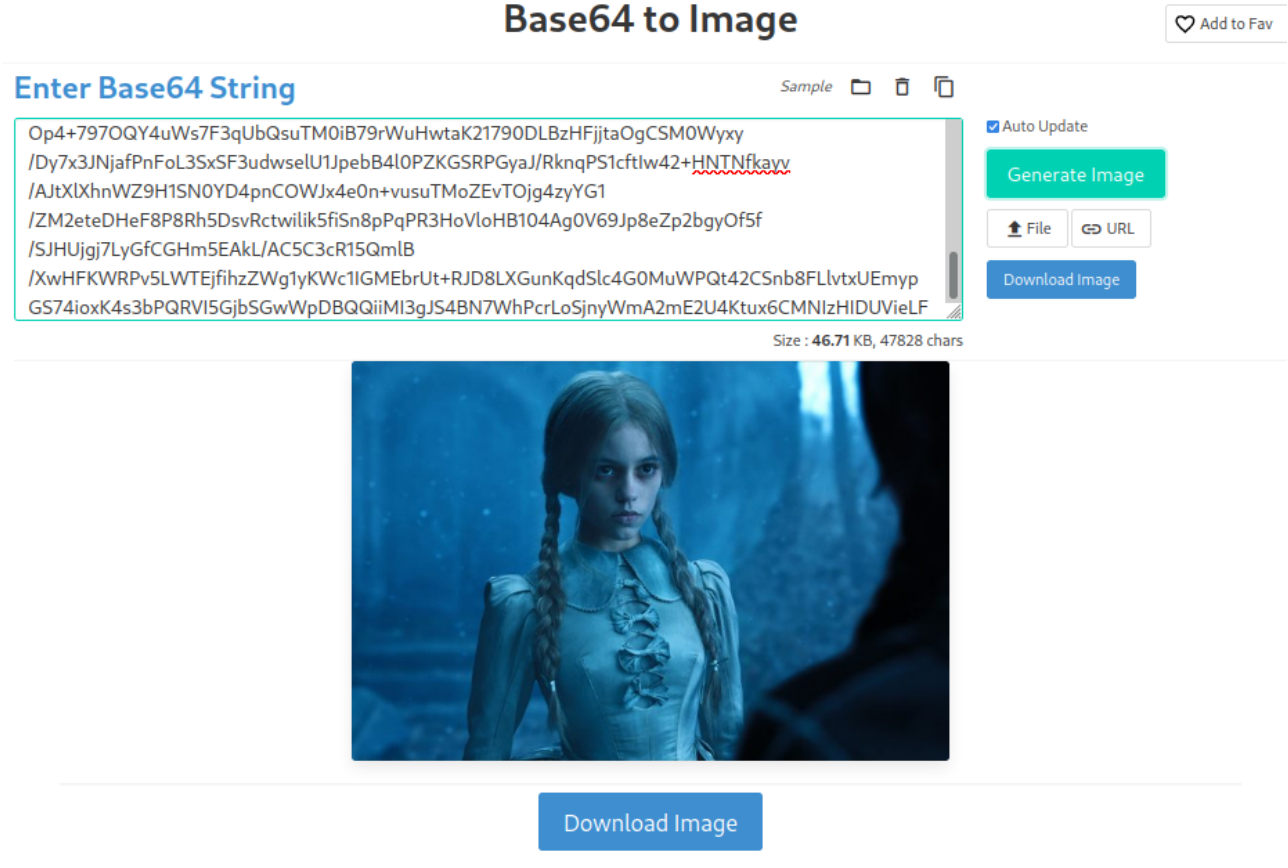
as we can see in comment

“first name of person who is hyde in the Show / one of dialogue of show is given as title or track name is the passphrase”
soo the title which is “Wednesday’s child is full of woe” is dialogue of Wednesday Webseries and the first name of hyde is tyler and using steghide extract the hidden text.

```
┌──(krish㉿kali)-[~/Desktop]
└─$ steghide extract -sf you_suck.wav
Enter passphrase:
the file "2ndPart.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "2ndPart.txt".
```



7] After doing some research about text we can get its a base64 form of image(also as indicated that there is a image in audio somewhere) so after converting it we get



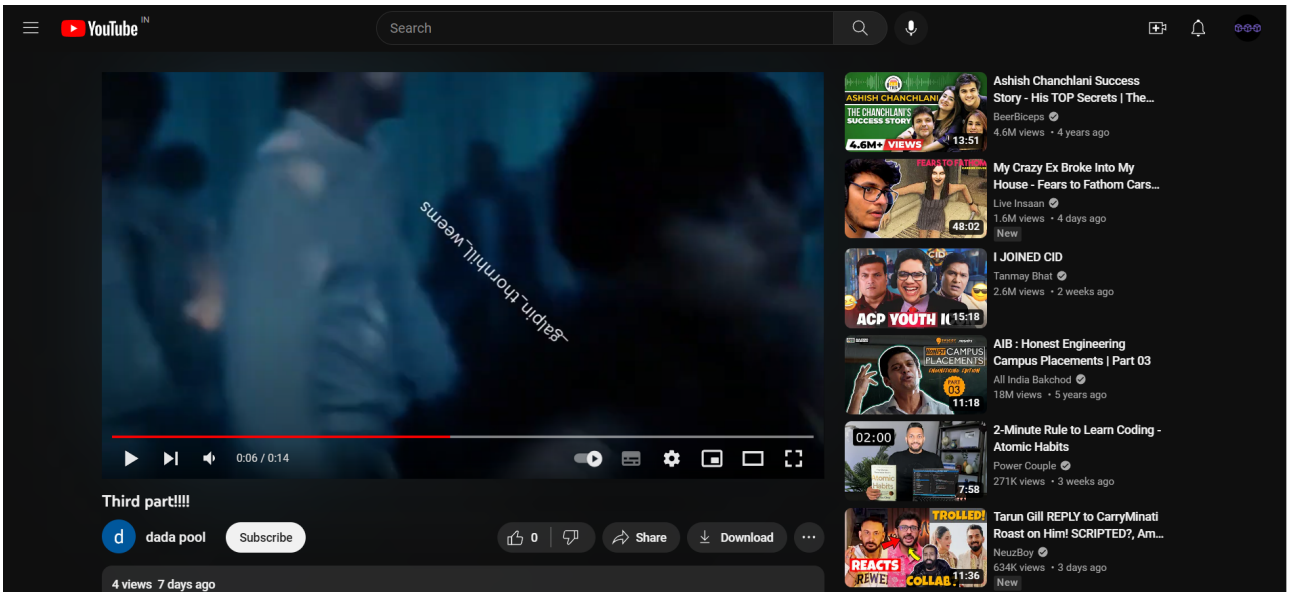
Download Image

After some research we can find that her name is goody

Soo typing that in bot we get 2nd part of flag “_petropolus_walker”

8] Now also as said in audio contain many secrets and we can see a link in mediainfo which is "https://youtu.be/z4t2_6SFiPo"

going on that link we get a video whose name is 3rd part and in that for a fraction of second we get the 3rd flag as "_galpin_thornhill_weems"



9] Finally Concatenating part of flag we get flag as VishwaCTF{_sinclair_addams_barclay_petropolus_walker_galpin_thornhill_weems}