**NYP Back to School Write-Up 2020**

**Programming**

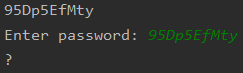
* The Bug Err
  + Step 1 : Ensure the if else statement work so that the program works normally



to



* + Step 2 : Run and Test with Debugger on and you can see that the output is obviously not the flag



* + Step 3 : Now I look at the debugger and realize there is another list call k3ys

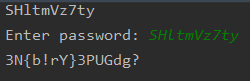


* + Step 4 : Then, I start debugging the code start by fixing the creation of the combinedflag and run the code and realize the output is still not the flag



to



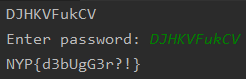


* + Step 5 : Then, I replace the current list with the new list found in the debugger earlier on and run the program again and now we found the flag



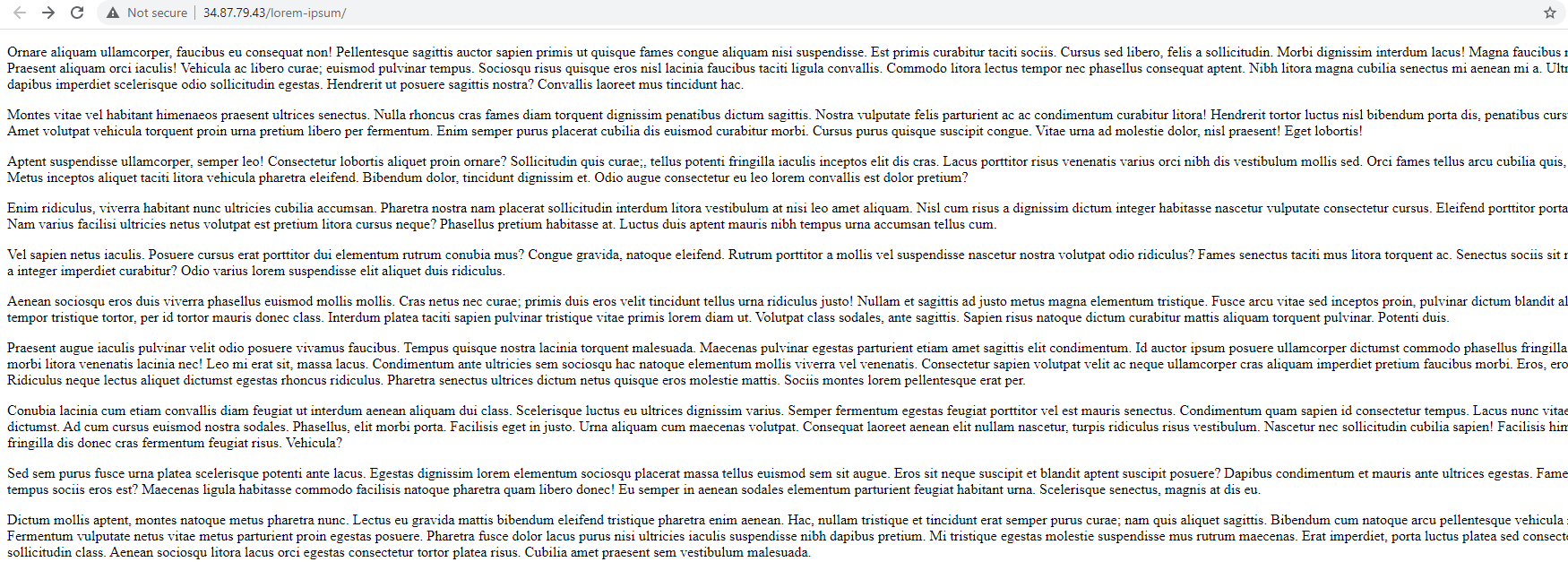
to



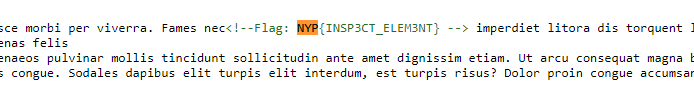


**Web**

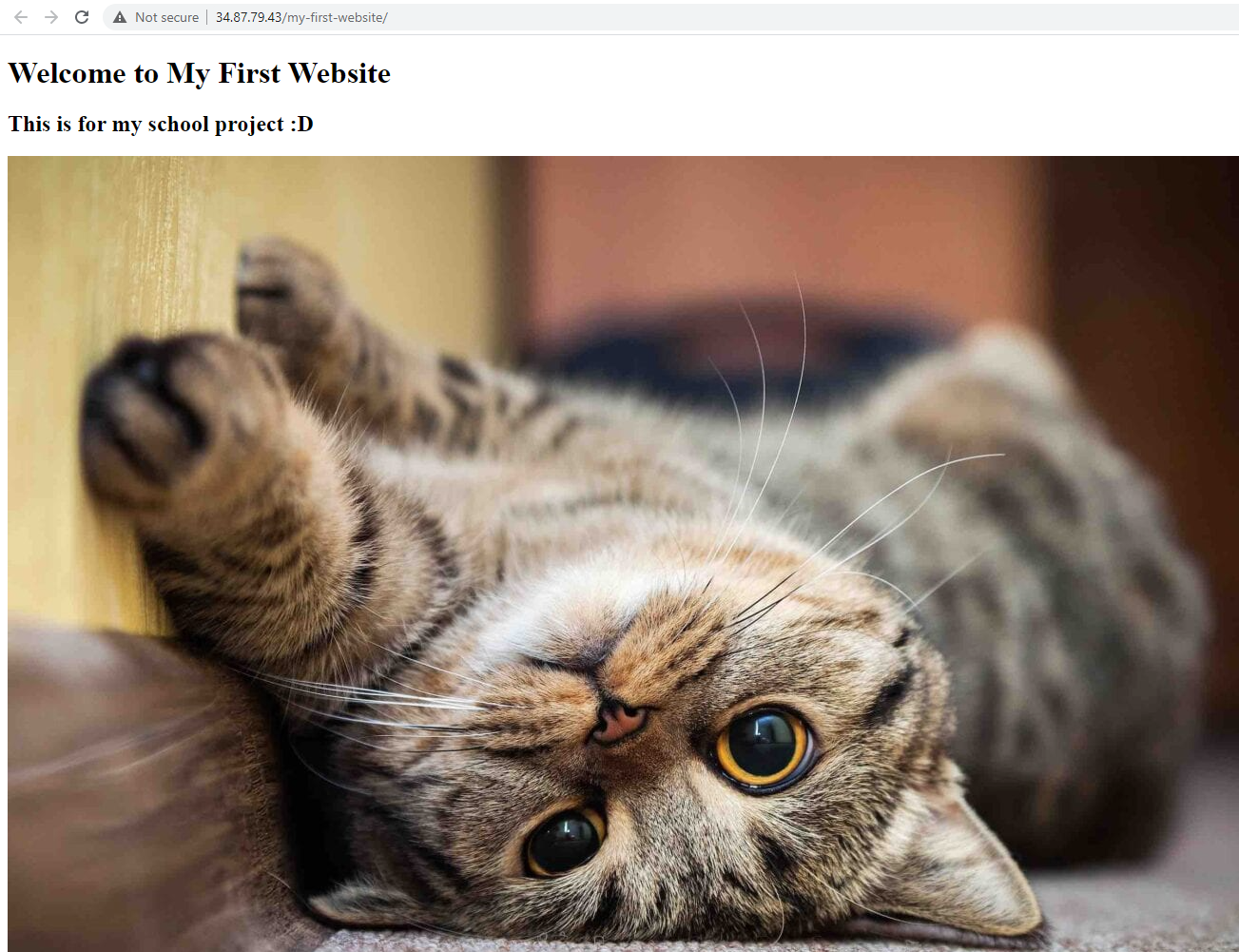
* Lorem Lpsum
  + Step 1 : Go to the link

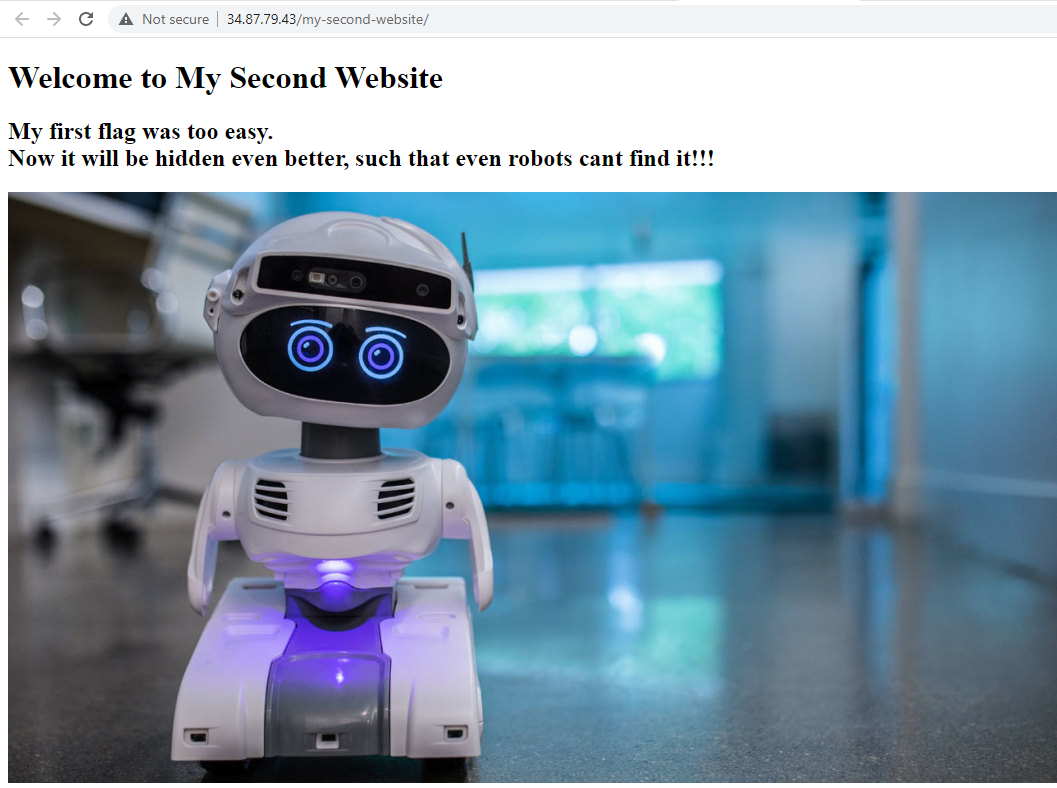


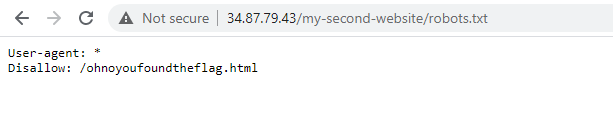
* + Step 2: view the source to find the flag



* My First Website
  + Step 1: Go to the link

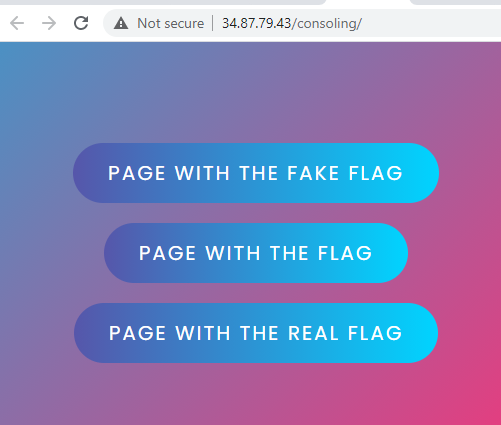
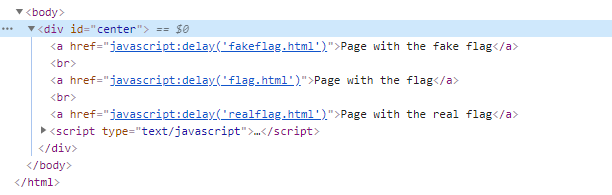
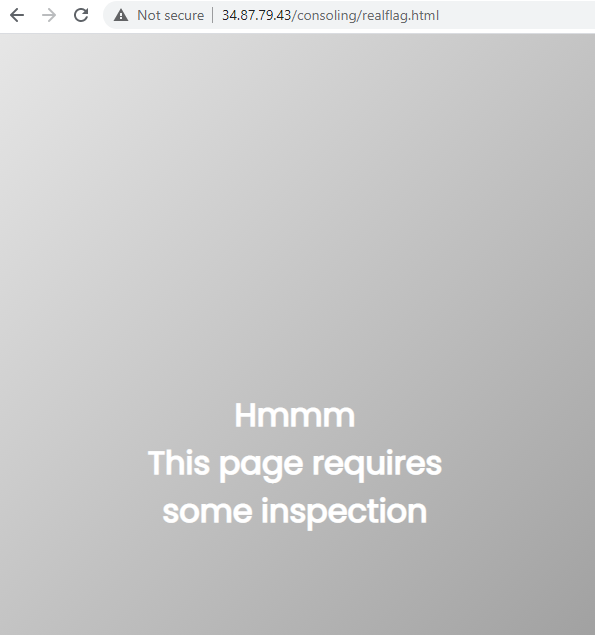
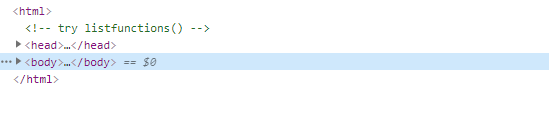
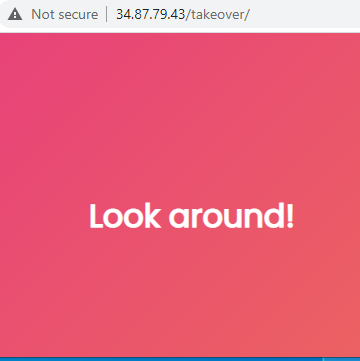
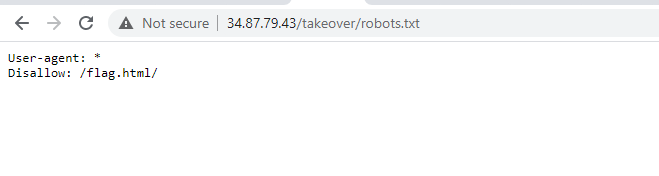


* + Step 2: Inspect element, there is a base 64 encoded string in the alt field
  + ****
  + Step 3: base 64 decode and convert from hex to get the flag
  + 
* My second website
  + Step 1: Go to the link
    - ****
  + Step 2: add robots.txt behind the url



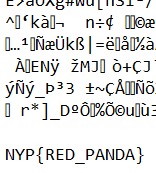
* + Step 3: GO to the html page



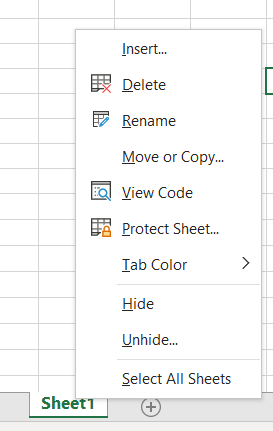
* Consoling
  + Step 1: Go to the link
    - ****
  + Step 2: looking at the source, there is 3 different html pages
    - 
  + Step 3: going to the realflag.html page
    - 
  + Step 4: viewing the source, it says to try listfunctions()
    - 
  + Step 5: try list functions in the console
    - 
  + Step 6: run the get flag and get key function to get the flag
    - 
* Takeover
  + Step 1: Go to the link
    - ****
  + Step 2: Go to robots.txt
    - 
  + Step 3: Going to the flag.html page,
    - 
  + Step 4: search for the } as there are many strings which start with NYP{
    - 
    - 
    - 

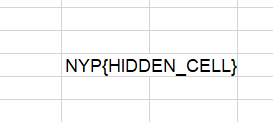
**Misc**

* Hidden Image
  + Step 1 : Change file type of hidden.png to txt and do a quick search command



* Blank Excel
  + Step 1 : Find the hidden sheet in challenge.xlsx which contain the flag by using the “unhide” option

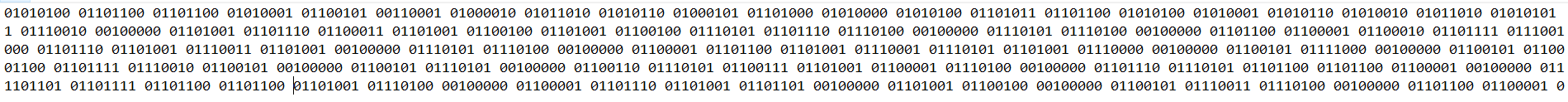




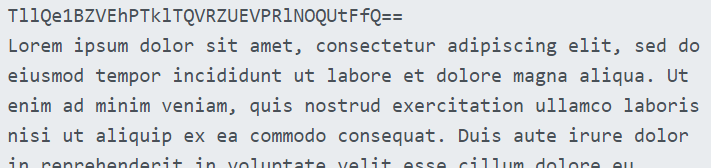
* The Hardest Challenge
  + Step 1 : Complete survey provided by NYP Infosec
* Mysterious Picture
  + Step 1 : Change file type of backtoschool.png to txt and do a quick search command



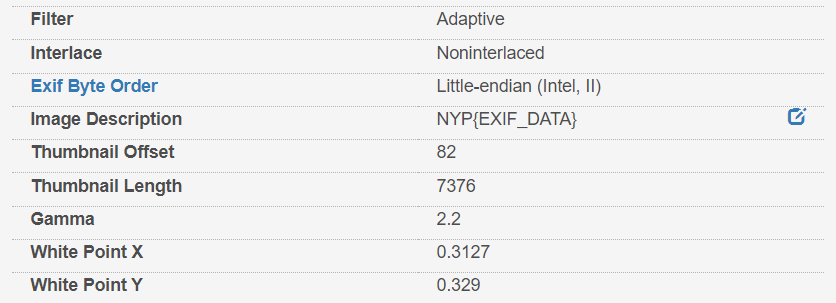
* There are plenty of flags
  + Step 1 : Flag Semaphore
* The answer
  + Step 1 : Extract The Answer.zip and run this command on linux
    - grep -rnw '/path\_of\_zip/' -e 'NYP{'
* Snake
  + Step 1 : Change the filetype of Snake.exe to text file



* + Step 2 : Convert the binary to ASCII/UTF-8 character on a online converter and you will see a base64 encoded string on the header



* + Step 3 : Decode the base64 character for the flag : NYP{PYTHONISATYPEOFSNAKE}
* Don’t Scan Me
  + Step 1 : Check the metadata of Don’t Scan Me.png on [www.metadata2go.com](http://www.metadata2go.com)



* Musically Inclined
  + Step 1 : Decode it on <https://www.dcode.fr/music-sheet-cipher> with the character on BTS\_MusicallyInclined.png
* Stegosaurus
  + Step 1 : Go to <https://futureboy.us/stegano/decinput.html>
  + Step 2 : Find the password by taking the first character of each word from the challenge description



* + Step 3 : Select Stego.jpg and enter Password as Ze3cAC

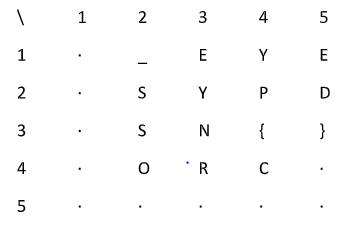


* + Step 4 : Convert the binaries to ASCII/UTF-8 for the flag : NYP{ST3GAN0GRAPHY}
* What’s my Password
  + Step 1 : Brute force the zip file by using rockyou.txt and frcrackzip to find the password

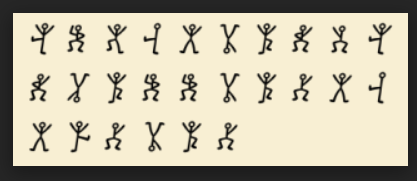
**$fcrackzip -v -u -D -p rockyou.txt secret.zip**

**Crypto**

* 13
  + Step 1 : https://rot13.com/
* Caesar Salad
  + Step 1 : <https://cryptii.com/pipes/caesar-cipher> with key of 3
* Breath Of The Wild
  + Step 1 : https://www.dcode.fr/hylian-language-breath-of-the-wild
* ZIG ZAG
  + Step 1 : <https://www.dcode.fr/rail-fence-cipher>, with keep punctuation and spaces checkbox checked
* Black and White
  + Step 1 : Reverse the QR Code Colour and Scan it
* Beep Beep Beep dun
  + Step 1 : https://morsecode.world/international/decoder/audio-decoder-adaptive.html
* Sing a Song
  + Step 1 : https://www.dcode.fr/bacon-cipher
* XOR
  + Step 1 : <https://www.dcode.fr/xor-cipher> with WHAT as the key
* Spirals



* + Step 1 : Since we know the format of the first 3 character of NYP{, just follow Spiral orders and get the flag
* What the JS!!!
  + Step 1 : It is JSFuck so we will use <http://codertab.com/JsUnFuck> to obtain the flag
* Dancing Men



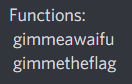
* + Step 1 : Use https://www.dcode.fr/dancing-men-cipher

**OSINT**

* There’s an I in every flag 1
  + Step 1 : Go to Instagram of NYP Infosec and look at the comments



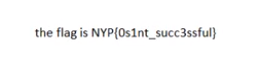
* What a bot
  + Step 1 : Run a ~help command on the NYP InfoSec discord channel



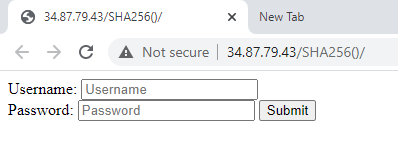
* + Step 2 : Run a ~gimmetheflag command on the same channel

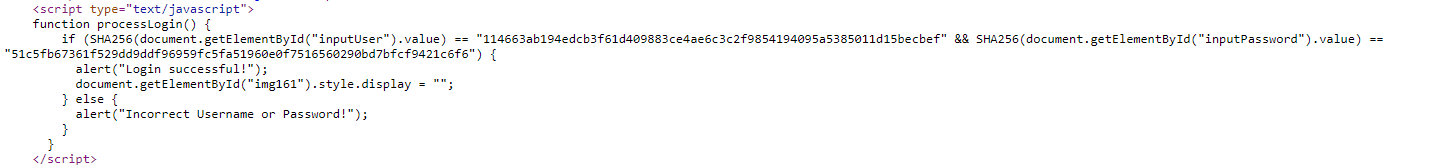


* Susan Wojcicki
  + Step 1 : Go Youtube and search for NYP BTS CTF 2020



**RE**

* APK
  + Step 1 :
* SHA256()
  + Step 1 : Go to the URL
  + 
  + Step 2: View the page source
    - In the page source there is this js function



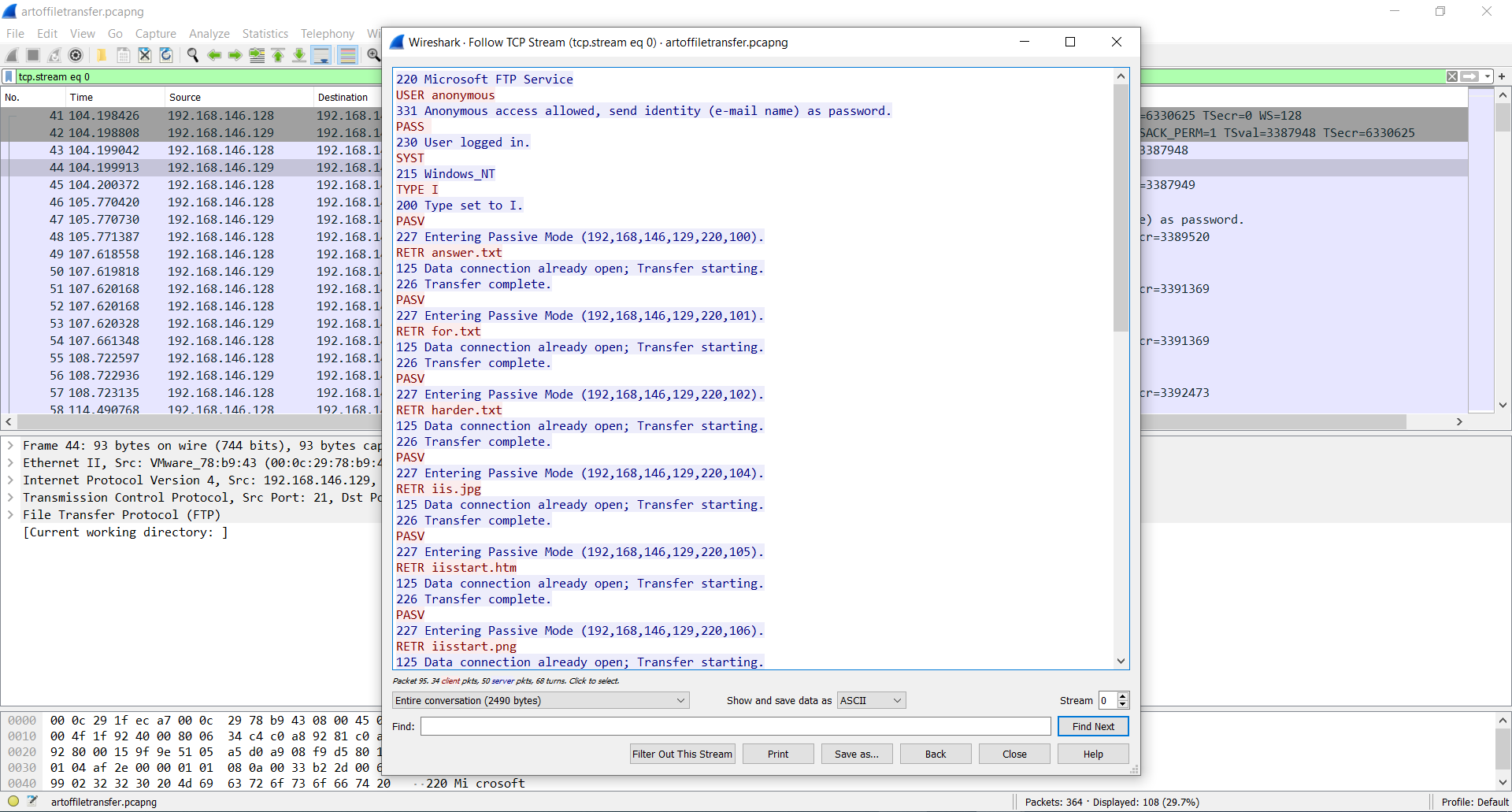
* + - And a lot of links to imgs



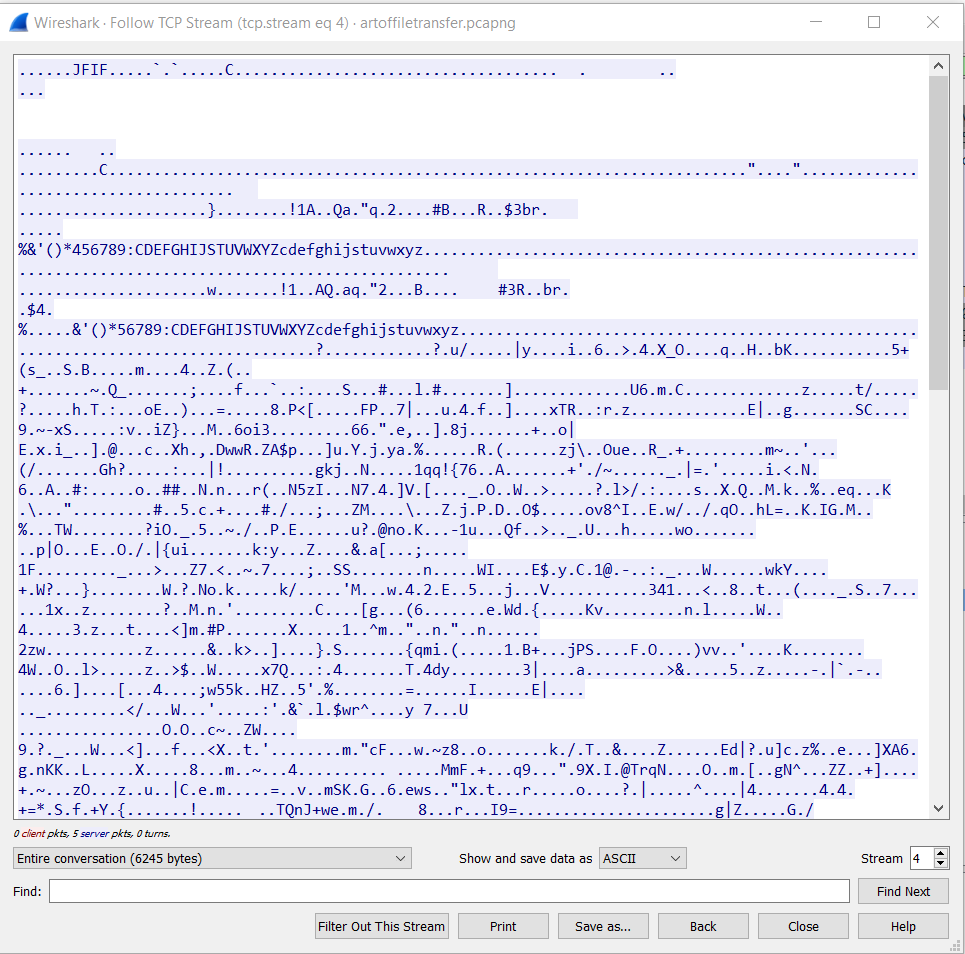
* + Step 3:from the js function, if the login is successful, it will display image 161
  + Step 4: opening image 161, we get the flag
  + 

**Network**

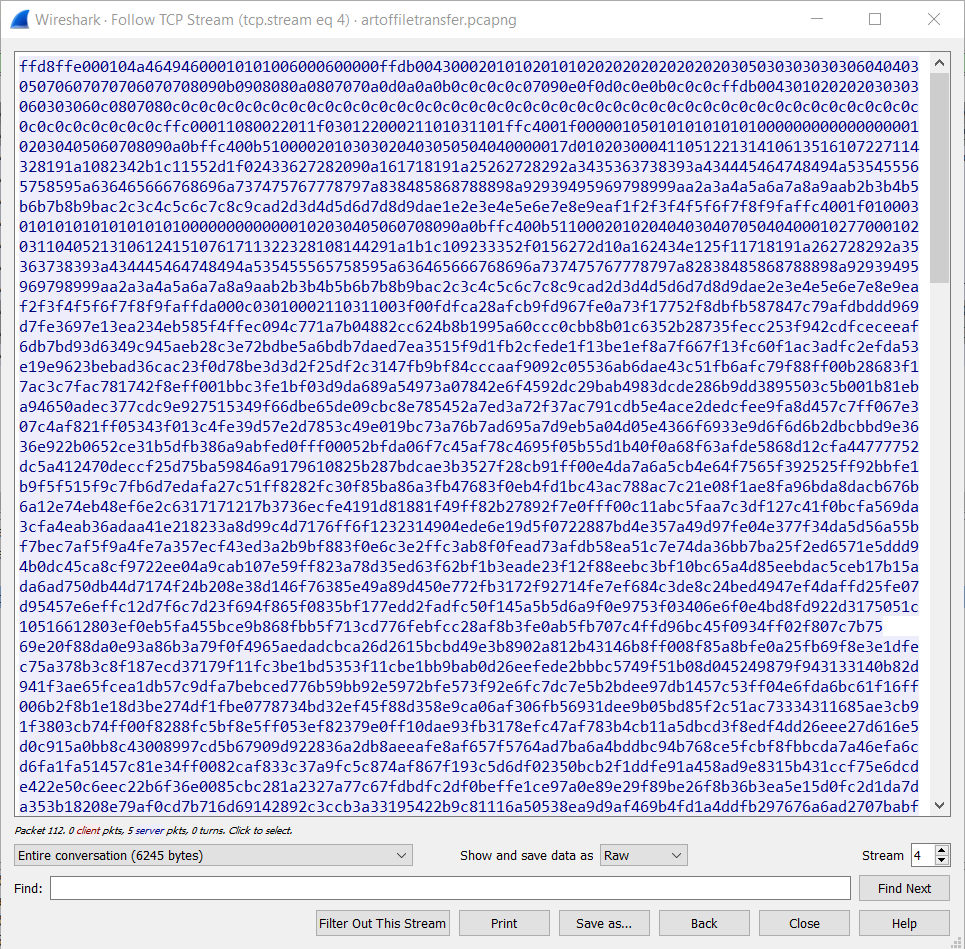
* Art of File Transfer
  + Step 1 : Follow the TCP Stream



* + Step 2: Go to tcp stream 4



* + Show and save data as Raw



* + Save it as a file with .JFIF