Misc

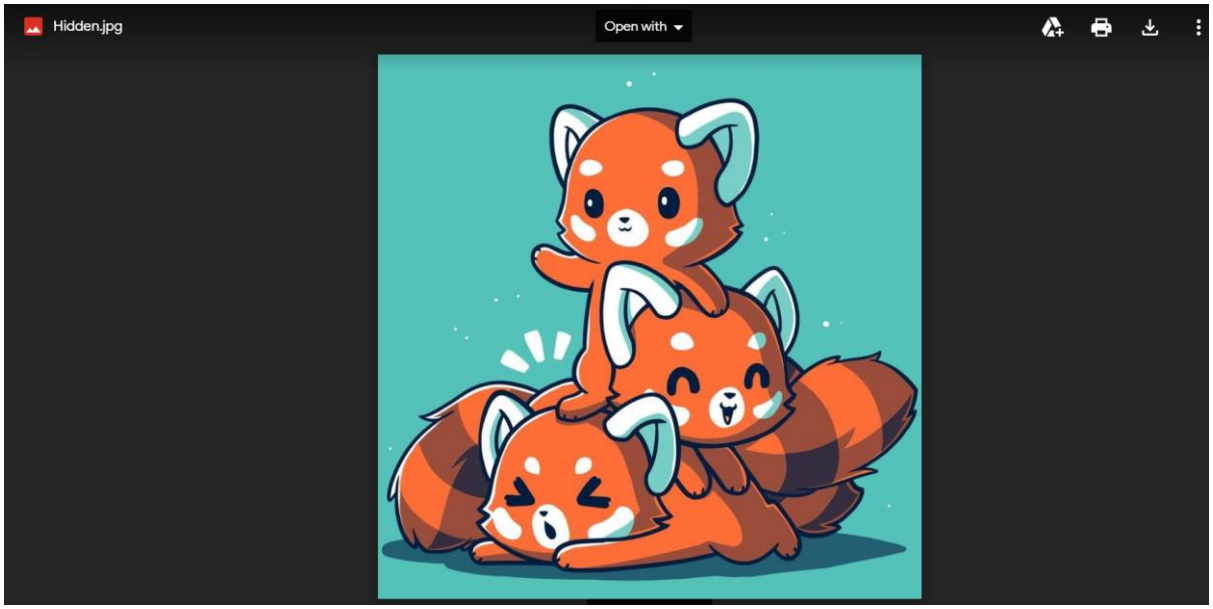
Misc

- Hidden Image – 10 points
- Mysterious Picture – 15 points
- There are plenty of flags – 15 points
- The Answer – 15 points
- Snake – 15 points
- Don’t Scan Me – 25 points
- Stegosaurus – 35 points

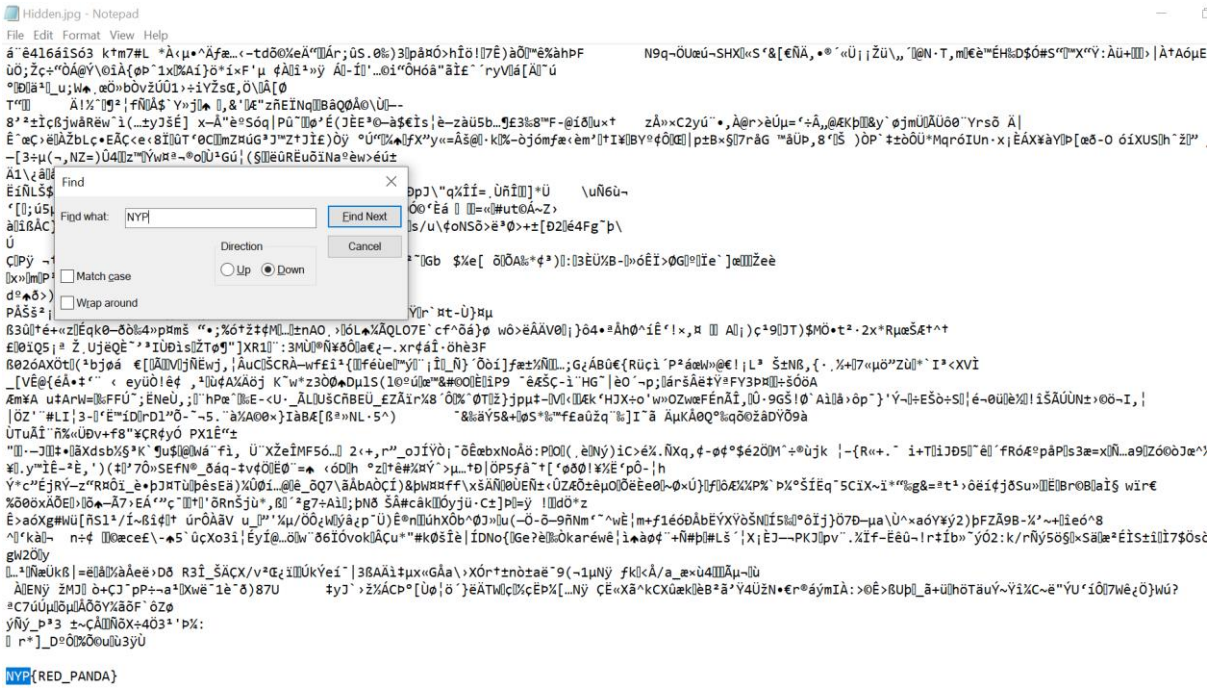
Total – 130 points

1) Hidden Image (10 points)

1. The challenge involves this image available at https://drive.google.com/file/d/1up3R9fVSBmInJAWQnlHbw68fVg4X4jyx/view



2. Download the image file. Open the image with “Notepad” and search for the flag.

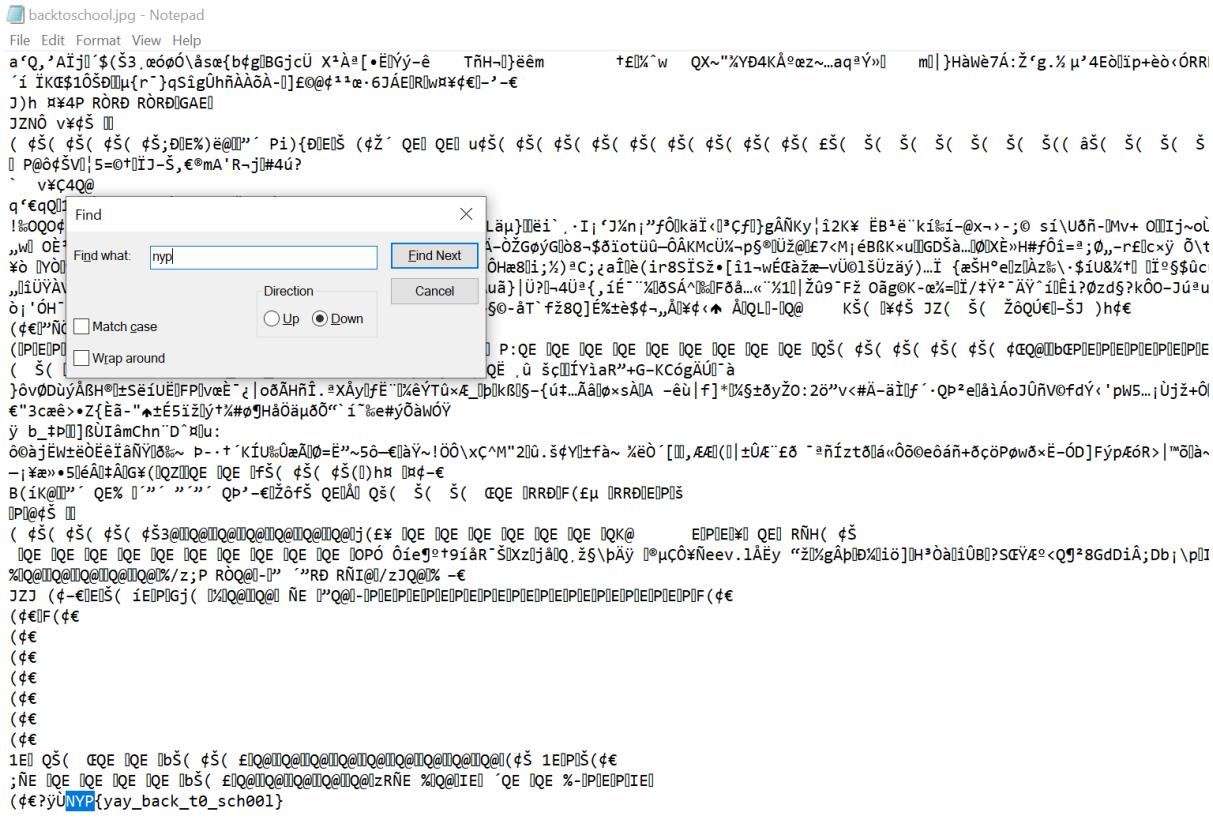


3. We got NYP{RED_PANDA} from the image file!

2) Mysterious Picture (15 points)

1. The challenge involves this image available at https://drive.google.com/file/d/19Q_VqKxDWGrhZvJwAlv4bPOld8-PP05w/view

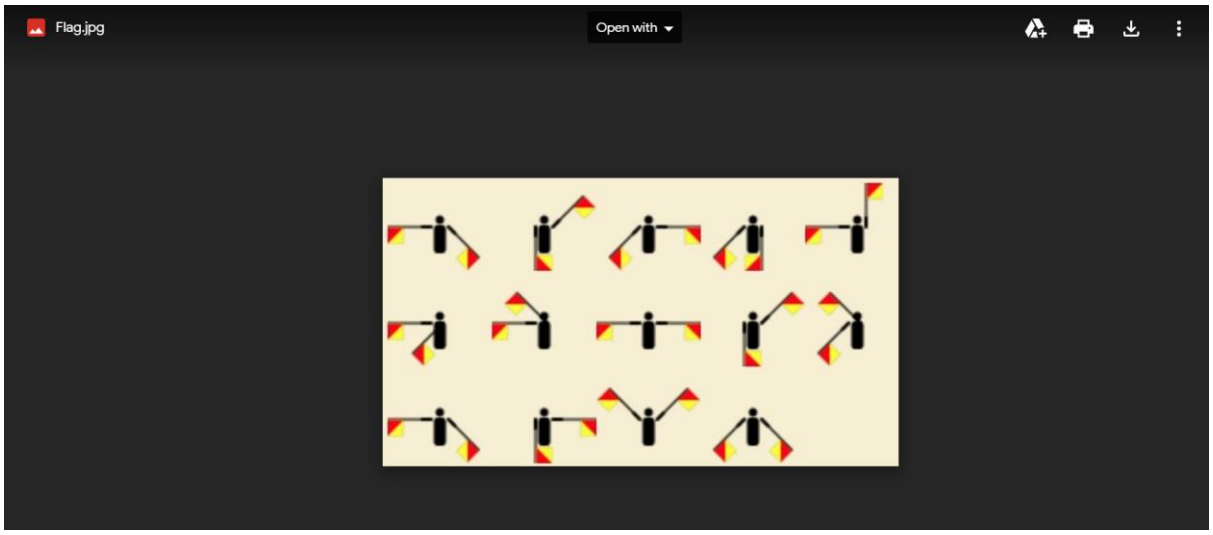
2. Download the image file. Open the image with “Notepad” and search for the flag.



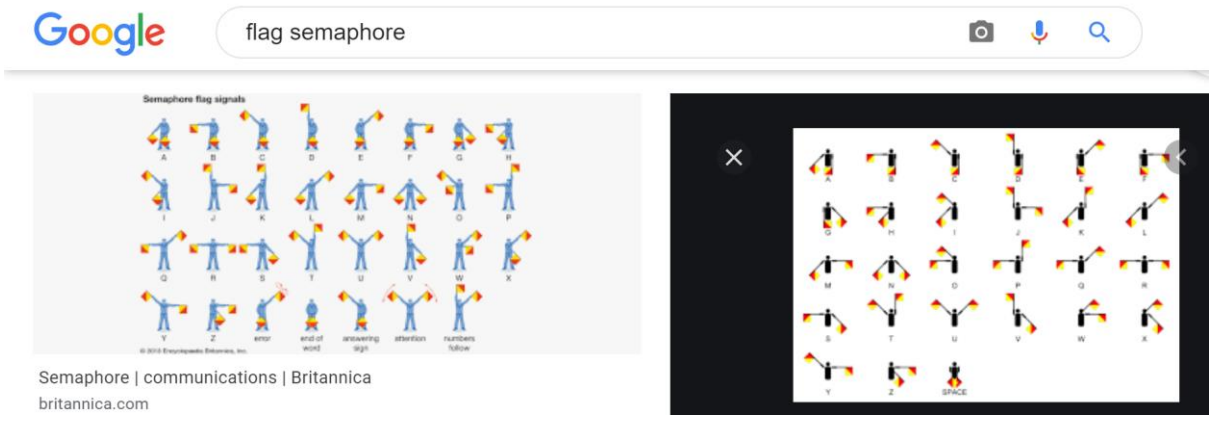
4. We got NYP{yay_back_t0_sch00l} from the image file!

3) There are plenty of flags (15 points)

1. The challenge involves this image available at https://drive.google.com/file/d/1i0p_vxQAlORvBTB_2jTVffwTHXLbZhjz/view

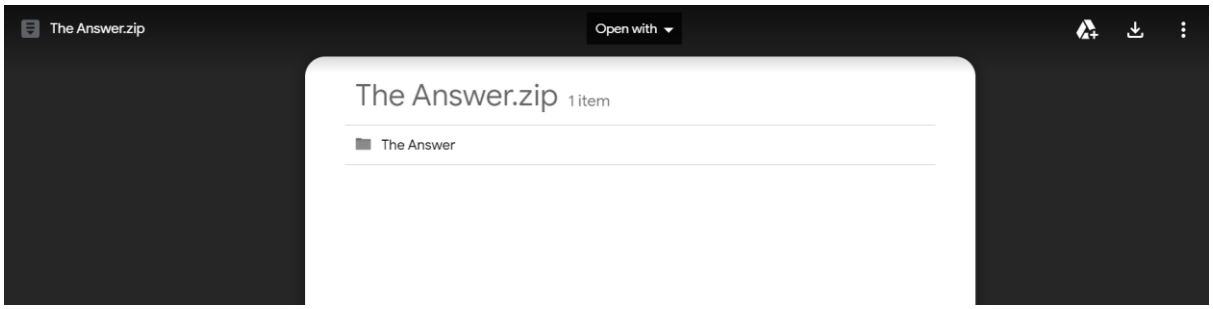


2. This image depicts a flag semaphore. A quick Google Search would give us the message of the image.



4) The Answer (15 points)

1. Download the file at https://drive.google.com/file/d/1oHStdJSF2x9sBJFKGVCEljwr3gRBMflj/view

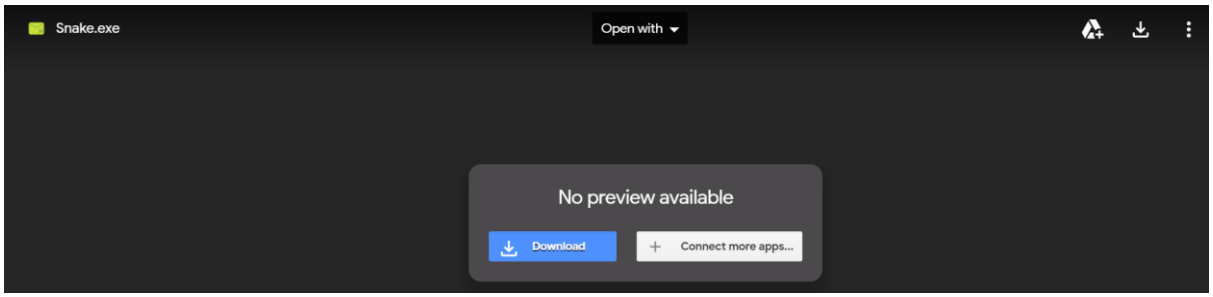


2. Extract the file and do a GREP search for the flag.

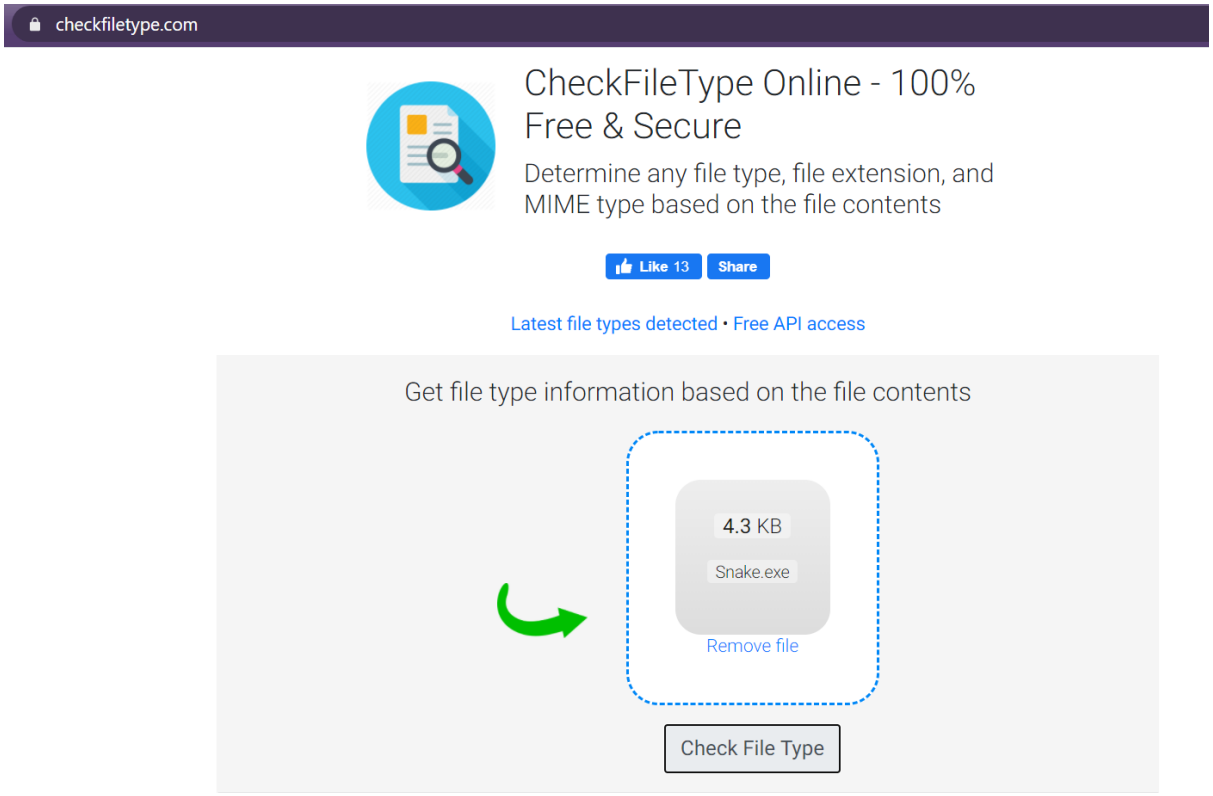
```
root@kali:~/ctf# grep -r "NYP" The\ Answer
The Answer/4/2.txt:NYP{Y0U_F0UND_THE_FLAG}
```

5) Snake (15 points)

1. Download the file at
   https://drive.google.com/file/d/1rov4uayJqcAHuy55BAx0kcWzrJ5AKQ0D/view



2. Goto http://checkfiletype.com and upload the executable file.



3. File Type is an ASCII text.

CheckFileType - SUCCESS

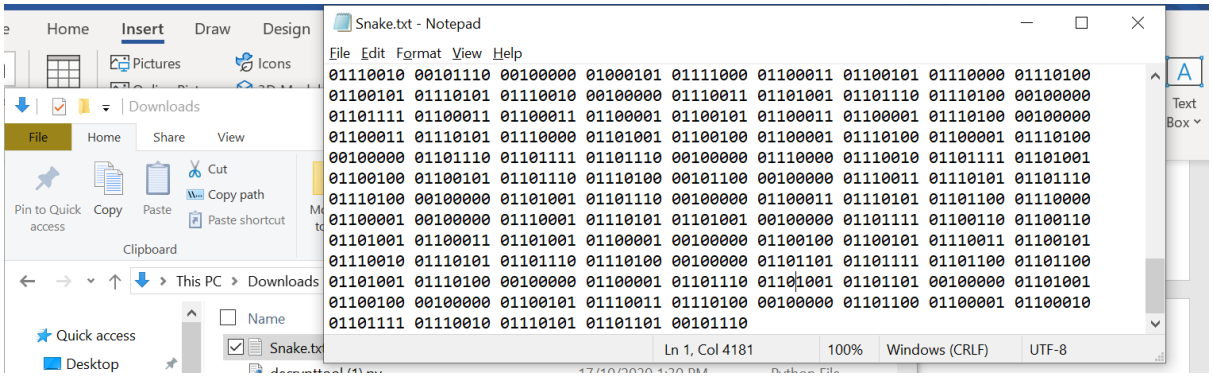
See the Latest Unit 42 Research Report on IAM Misconfigurations and How to Avoid Them.

OPEN

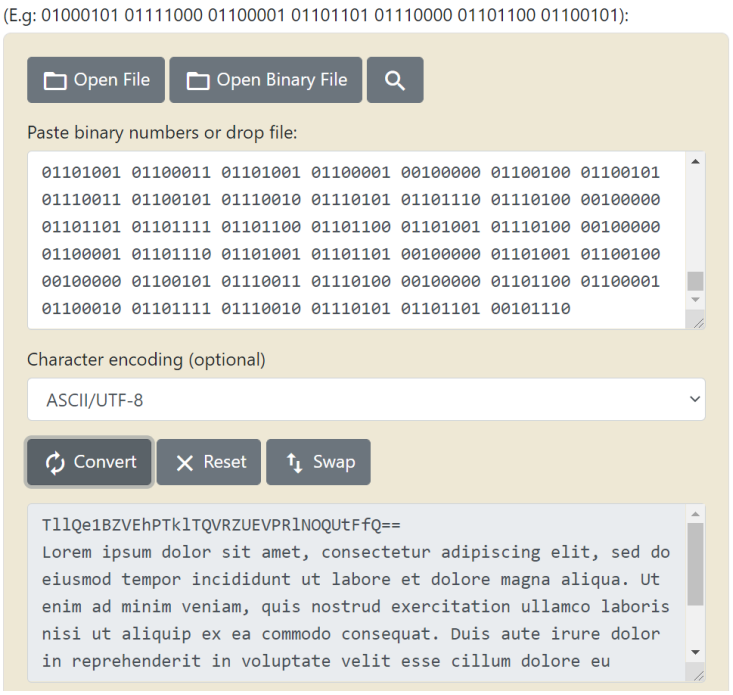
File Type: ASCII text, with very long lines, with no line terminators

How did we do?

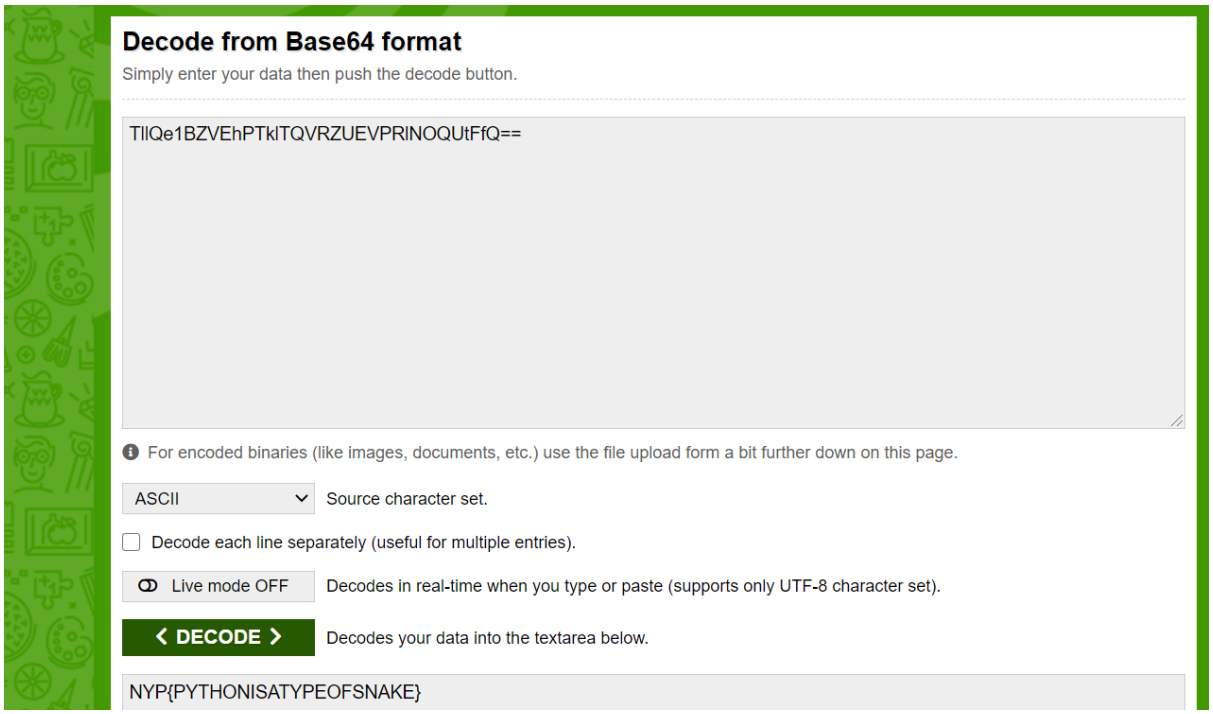
4. Change the executable file from ".exe" to ".txt" and open the file.



5. Convert the binary to string at https://www.rapidtables.com/convert/number/binary-to-ascii.html. We get Base64 encoded TllQe1BZVEhPTklTQVRZUEVPRlNOQUtFfQ==



6. Goto https://www.base64decode.org/ and decode the Base64 encoded text, and we get the flag!



6) Don’t Scan Me (25 points)

1. Download the file from
   https://drive.google.com/file/d/19zeVfRaNKx83ZDXnyJHSExPGbReEZw9t/view

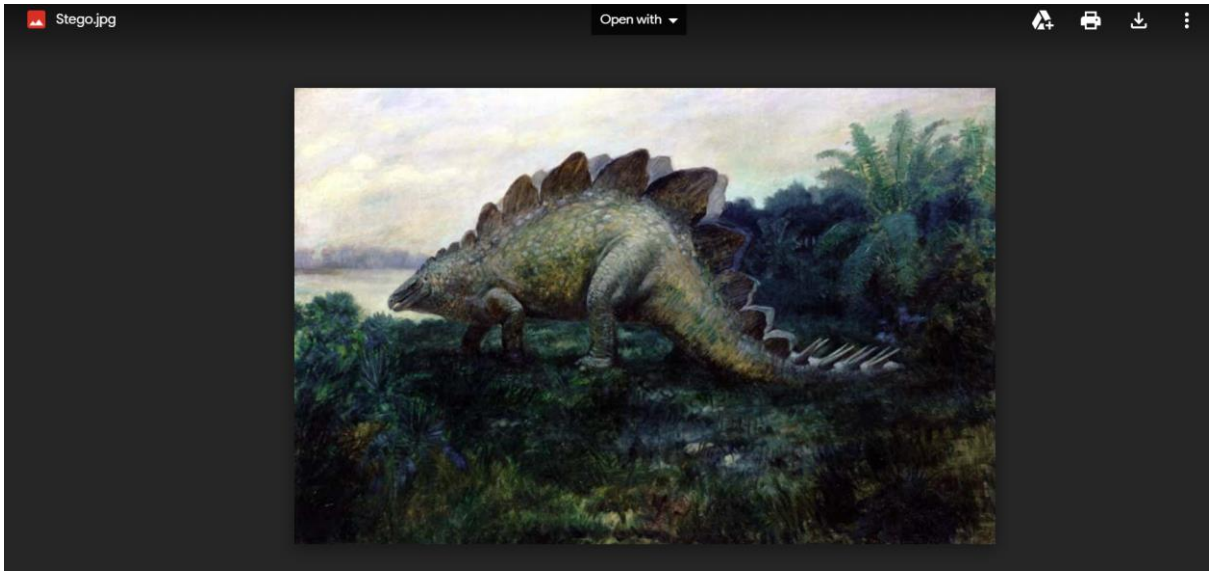
2. Scanning the QR codes leads me to nowhere.

3. Goto https://www.metadata2go.com/ and upload the file, and we get the flag.

File Name	Dont Scan Me (1).png
File Size	15 kB
File Type	PNG
File Type Extension	png
Mime Type	image/png
Image Width	300
Image Height	300
Bit Depth	8
Color Type	RGB with Alpha
Compression	Deflate/Inflate
Filter	Adaptive
Interlace	Noninterlaced
Exif Byte Order	Little-endian (Intel, II)
Image Description	NYP{EXIF_DATA}

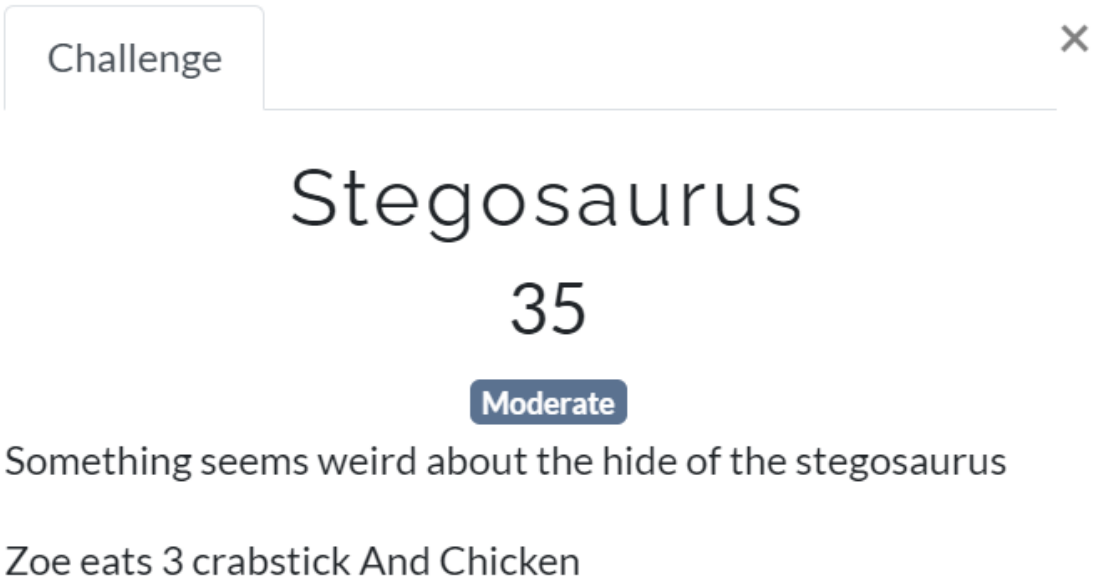
7) Stegosaurus (35 points)

1. Download the file from https://drive.google.com/file/d/1WAFK1NsQVcDeFzKnDt-LgmtKmFiQOhdu/view

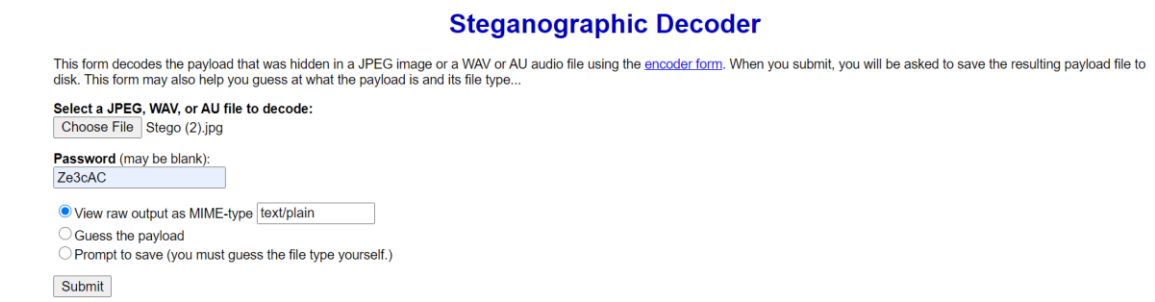


2. Upon opening the file with Notepad and checking the file's metadata, I was led to nowhere.

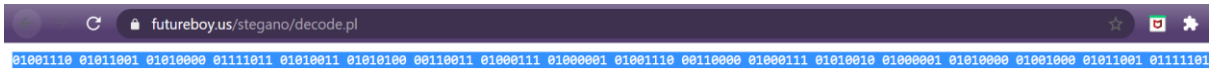
3. Notice the statement "Zoe eats 3 crabstick And Chicken". Taking the first letter of each word, we get "Ze3cAC"



4. Goto https://futureboy.us/stegano/decinput.html. Upload the file and enter the password.



5. We got a binary string!



6. Convert the binary to text at https://www.rapidtables.com/convert/number/binary-to-ascii.html and we get the flag!