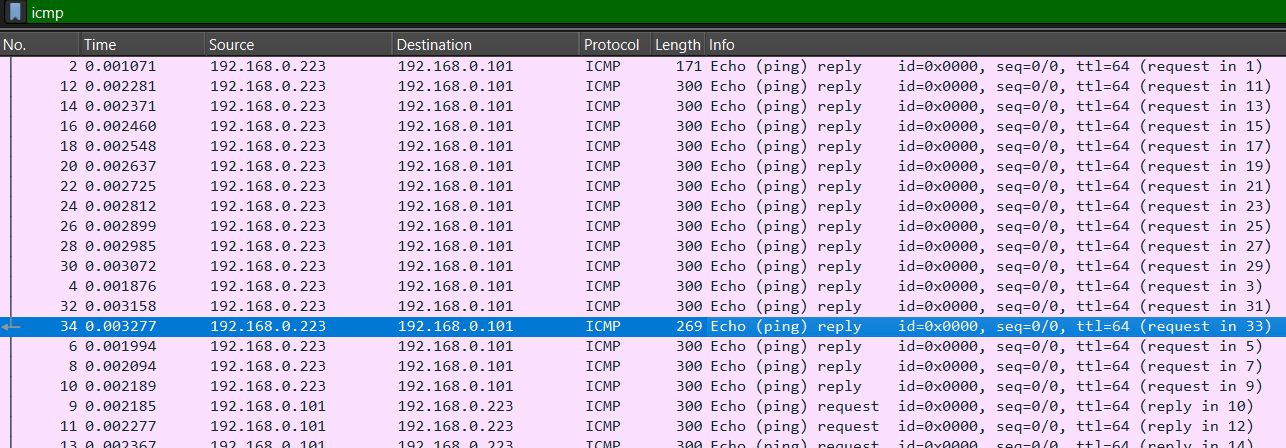
Hidden in plain write ups

Name: Zeyad Salah Mohamed Fathi Mohamed Moussa

ID: 120210297

**Discovering Abnormalities**

From the first look at the file table in Wireshark we cannot find anything abnormal about the file, but what caught my interest was the long length of the data and after investigating each reply and request we can find out that the data of the packet is changing by wide range from a packet to another so from that we can start our path for finding the hidden flag

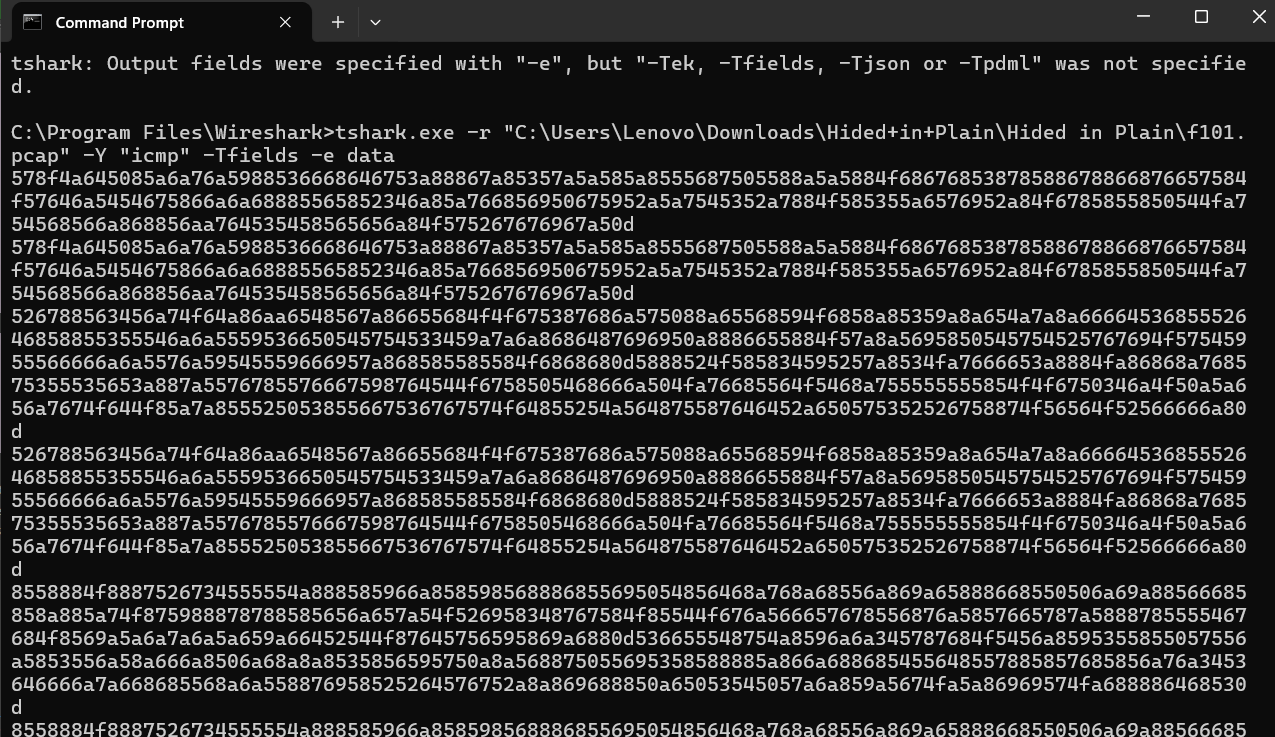


A screenshot of a computer

Description automatically generated

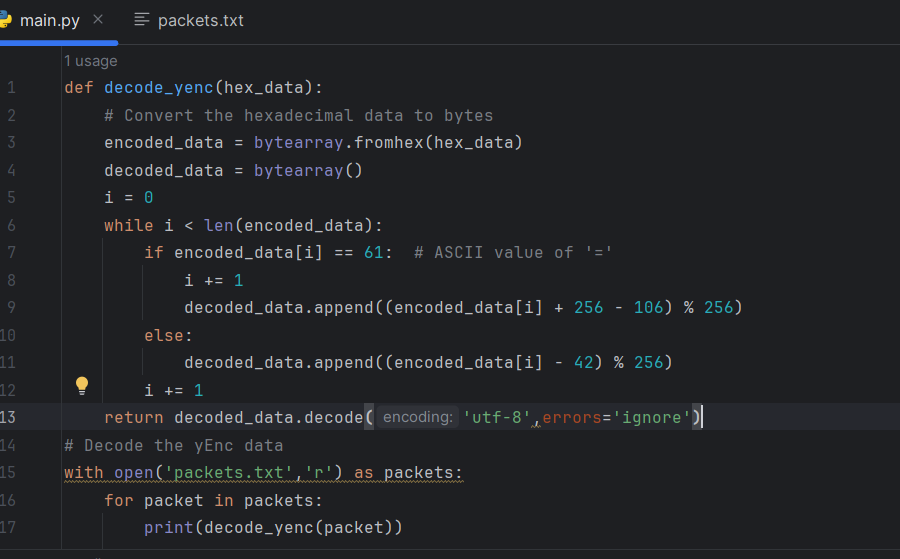
**Catching up the packets data**

Now we want to collect the packets data from each request and reply in the file and save it in a text file for investigation, we can do that using tshark in the command prompt to collect the packets data we can run the command found in the figure below then copy and paste the result in a text file.



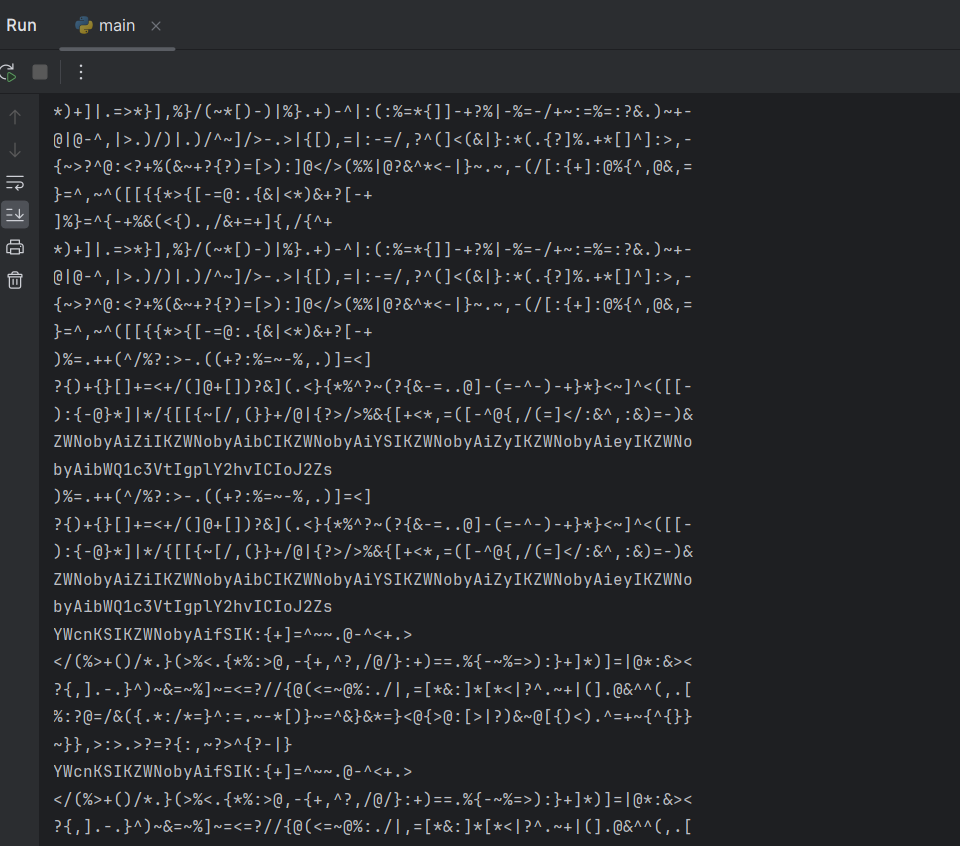
**Decoding Data**

From the output we can see that the data is encoded in some way, after using online coding analyzer we can find that the data is encoded using yEnc, so now we need to use a python code to decode that text file but installing yEnc library cannot work for python3 so we can use another way by implementing the decoding function by ourselves and decode the text file as shown in the figure below.



**Investigating the output**

The output of the code seems strange and cannot get any outcome from it but after scrolling over the output, we can see that there are some text parts present in the strange output as shown in the figure.



**Another Decoding**

After getting the part we are interested in from the output we can see that it is decoded in base64 so now we need to decode it again but this time using base64 library.

A screen shot of a computer

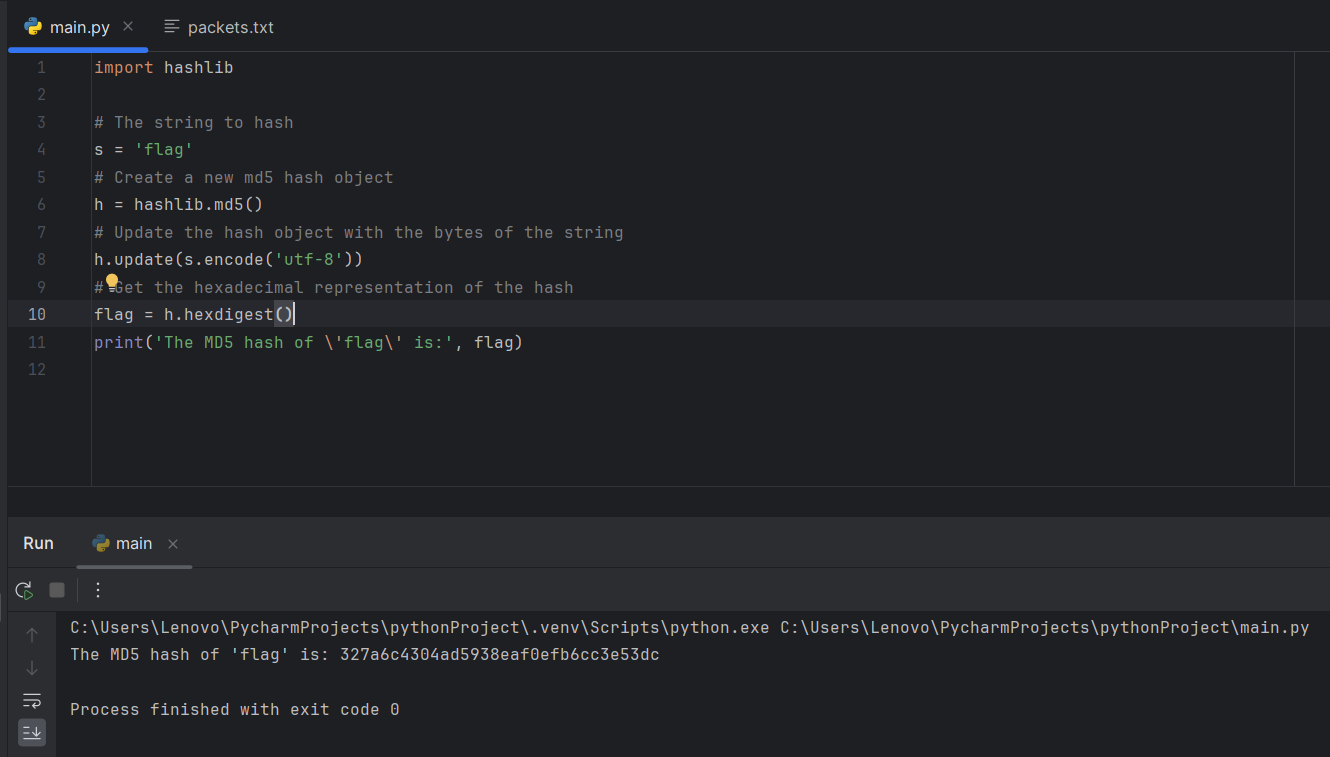
Description automatically generated

**Catching the flag**

After doing that we can take from the output is that our flag is as the following :

b’flag{md5sum(\’flag\’)}’

md5sum shows us that the flag is hashed by MD5 hash, so we need to get its actual value by running the following code.



**Submitting Flag**

Now we have got the flag which will be flag{327a6c4304ad5938eaf0efb6cc3e53dc}

A screenshot of a computer

Description automatically generated