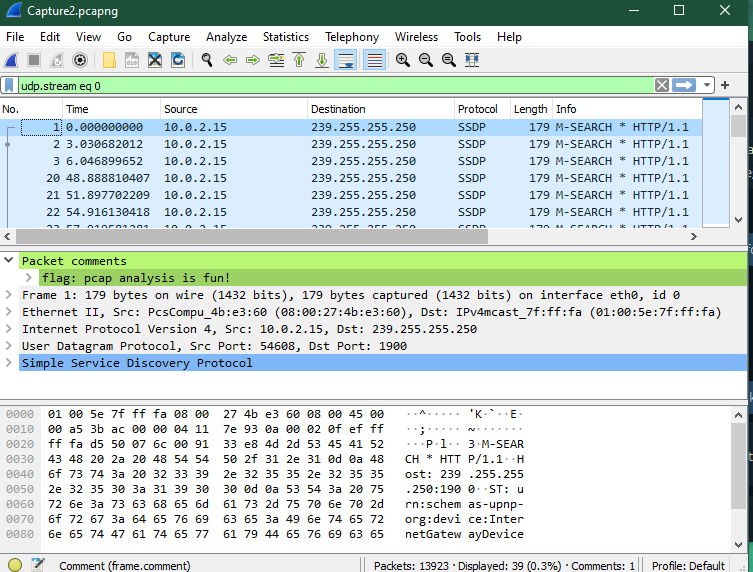
QUESTION 1

**“H!DD3N C0MM3NTS"**

-open the pcap file on wirehark and follow the Packet Comments

FLAG- **FLAG{pcap analysis is fun!}**



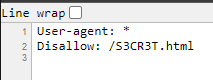
Question 2

**Suspecious**

- Navigate to given link [Welcome](http://51.89.5.222/challenge1/)(51.89.5.222/challenge1/)

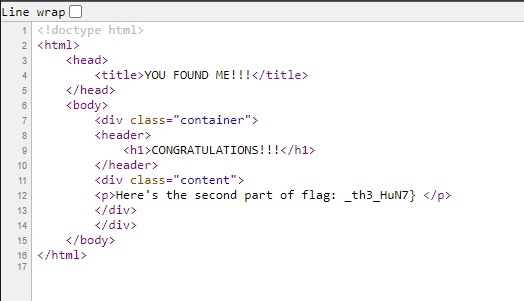
-look the source code

-go to /challenges/robots.txt



-navigate to

|  |
| --- |
|  |
| /S3CR3T.html |
|  |

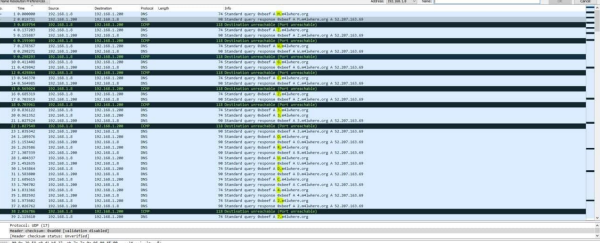


**Flag= \_FLAG{ S3CR3T\_th3\_HuN7}**

Question3

**DNS-QUERIES**

-Open the pcap file on wire shark and look on every DNS query h, it has a string.

-The first letter/number is the pattern, copy them all

-The output is MZWGCZ33ORUDC427NFZV65BQOVTWQX3XNF2GQMDVG5PXI43IGRZGWIL5

-This is base 32 so decode it and you will the your flag

**FLAG{th1s\_is\_t0ugh\_with0u7\_tsh4rk!}**