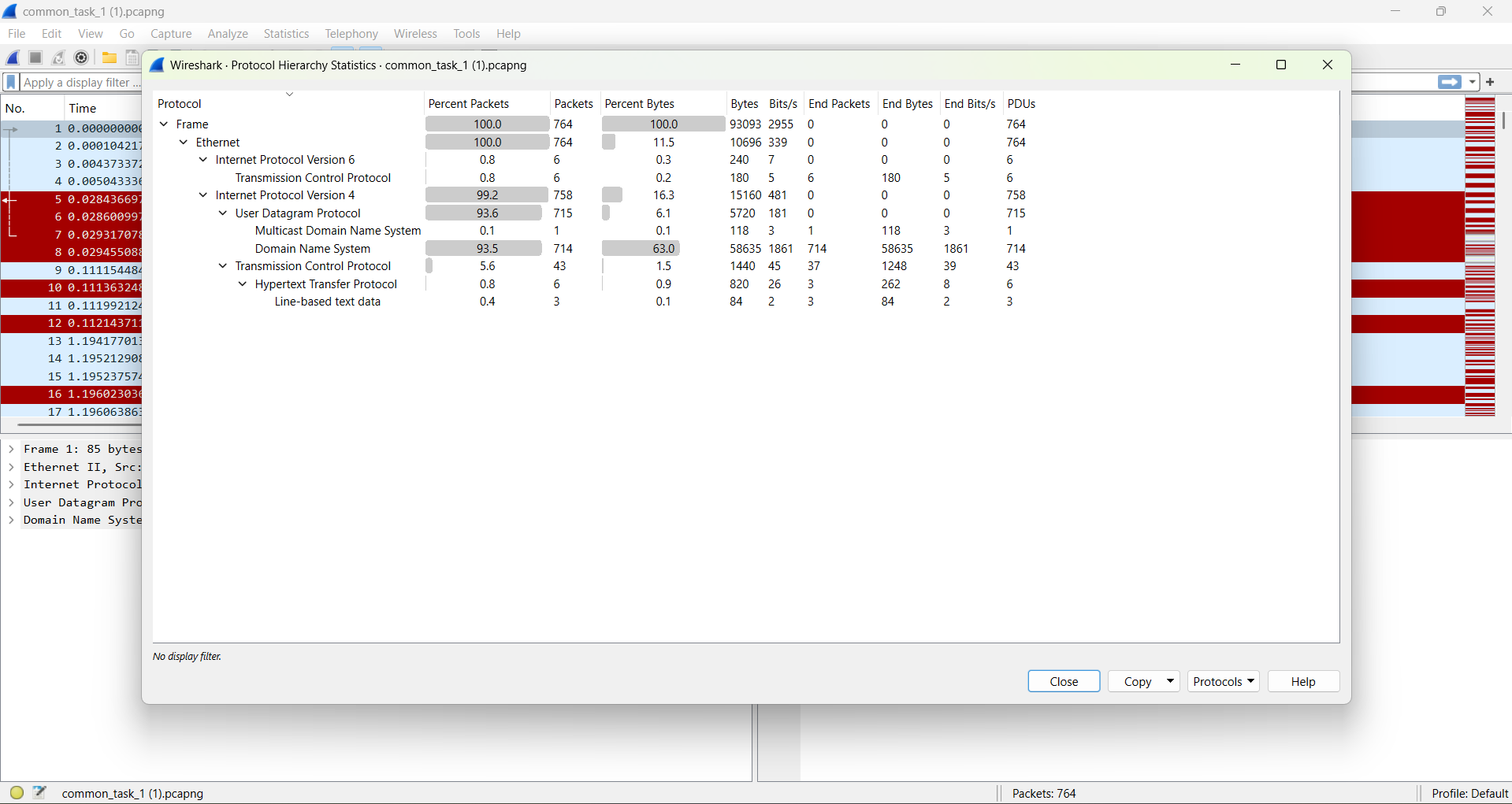
COMPUTER NETWORKING BASICS

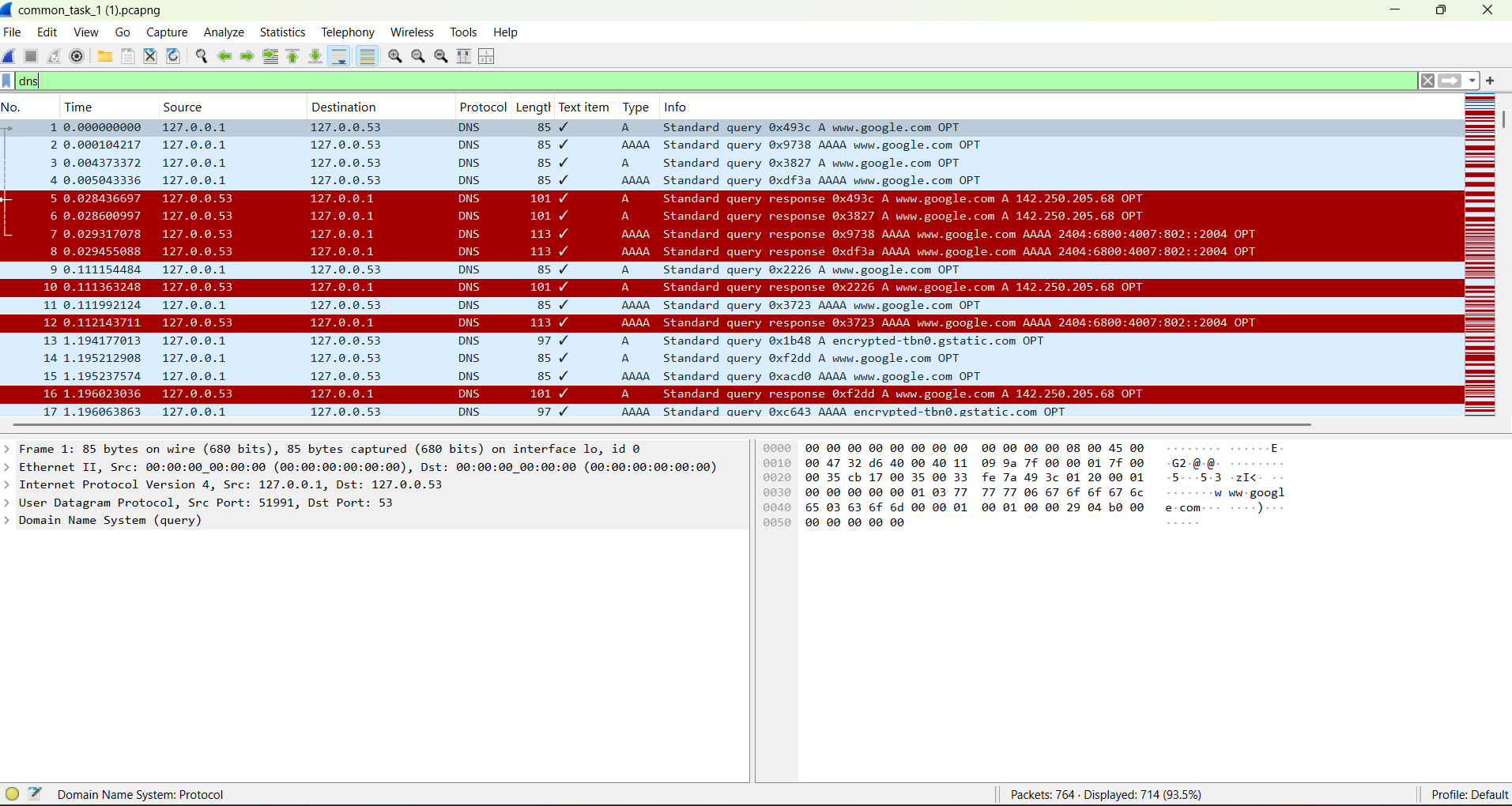
1. What types of traffic (HTTP, DNS, FTP, etc.) are present ?



using statistics > protocol hierarchy

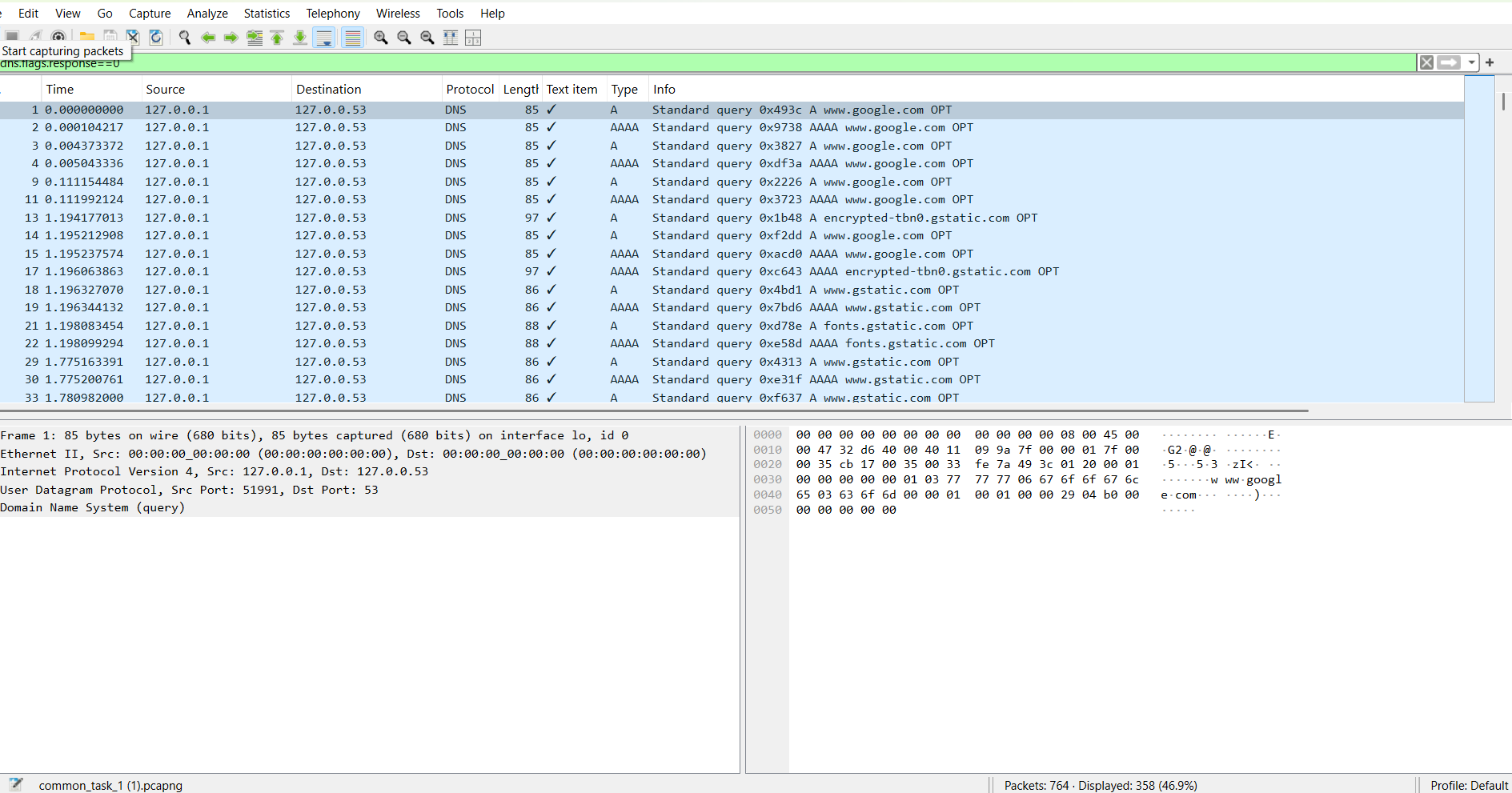
ethernet,ipv6,ipv4,udp,tcp,http,dns, mdns,line based text data

2. How many DNS queries were made in total?



filter: dns

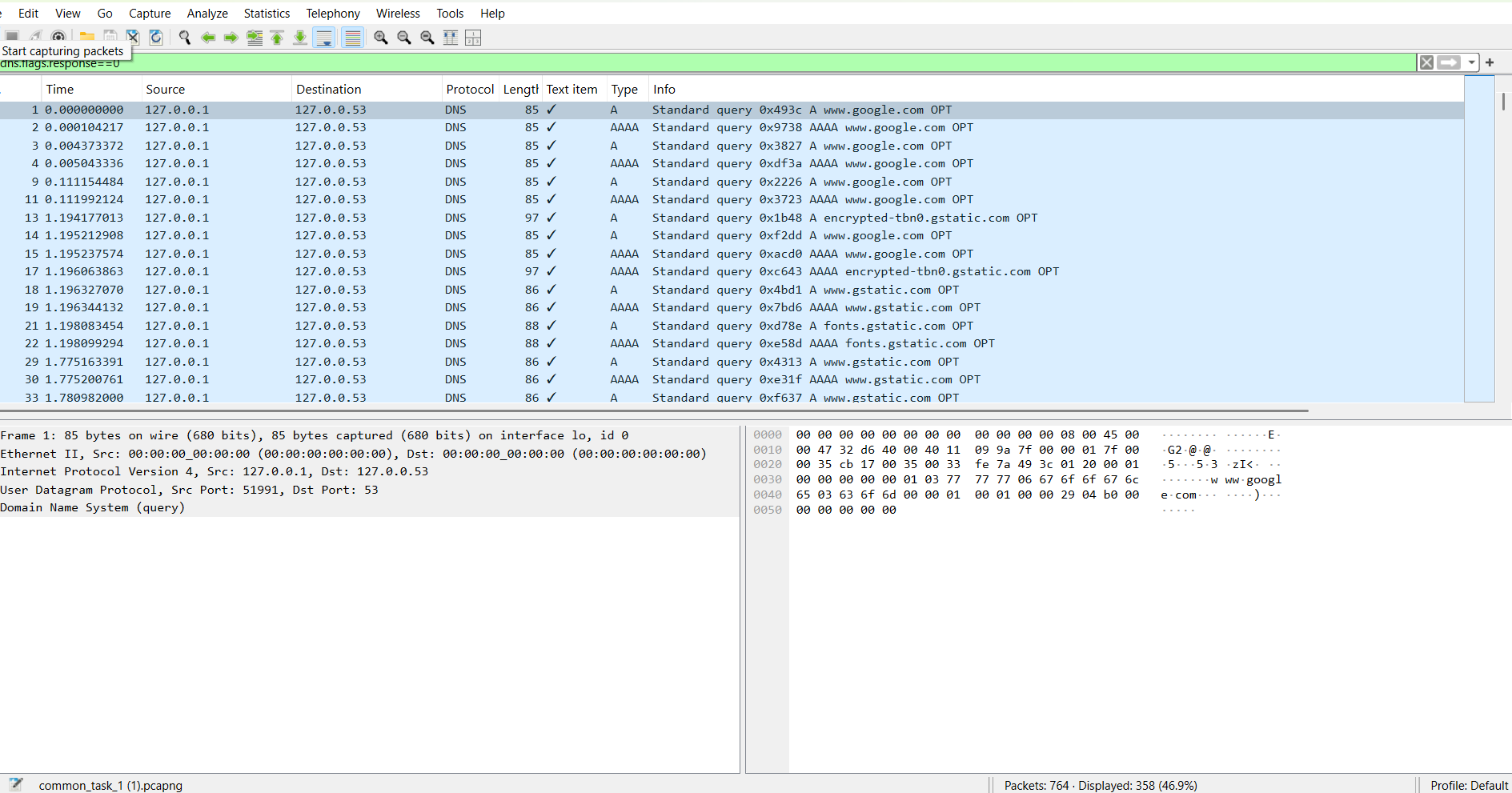
714 ( in bottom right shows packet:764 displayed:714)

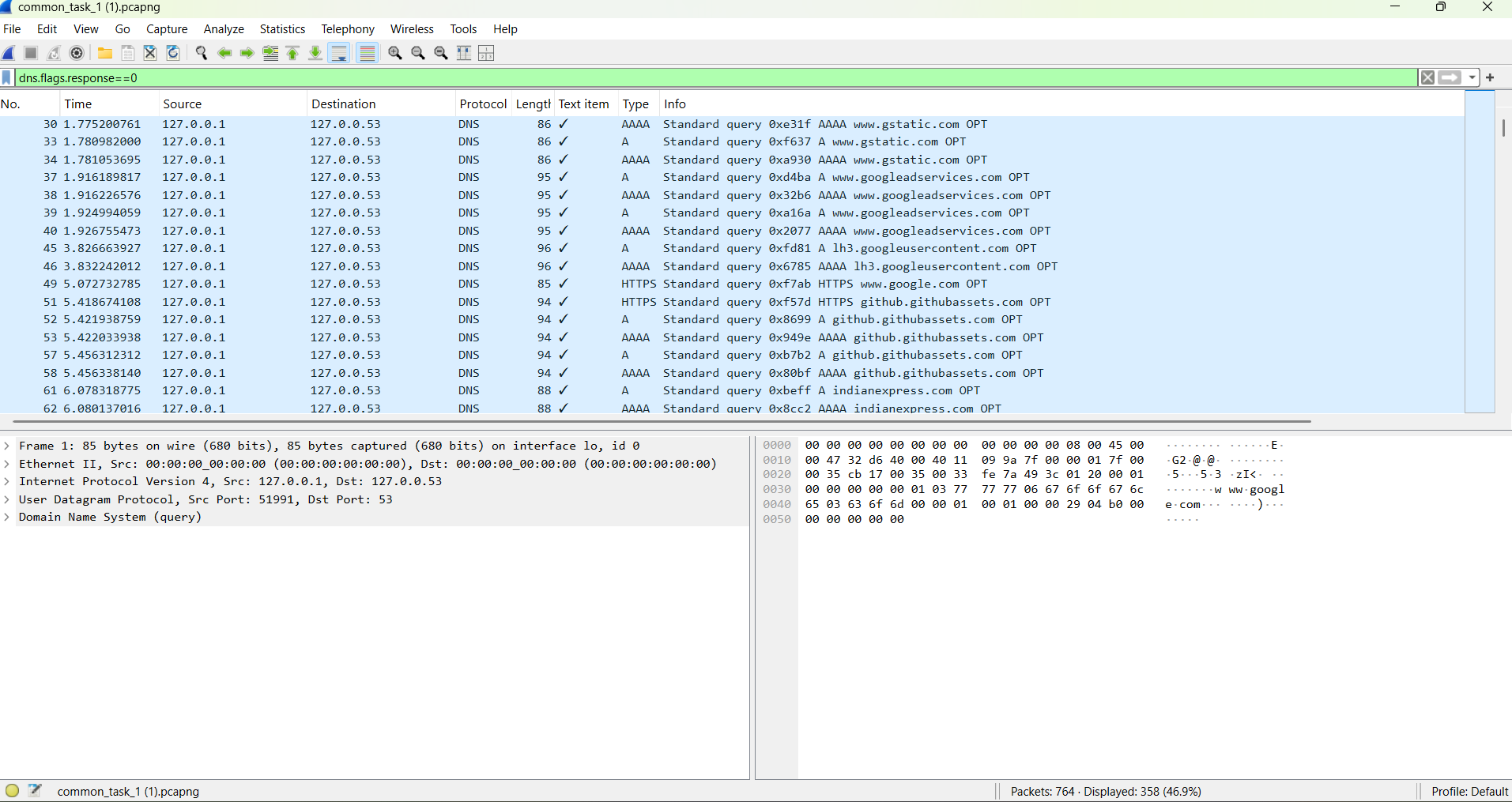


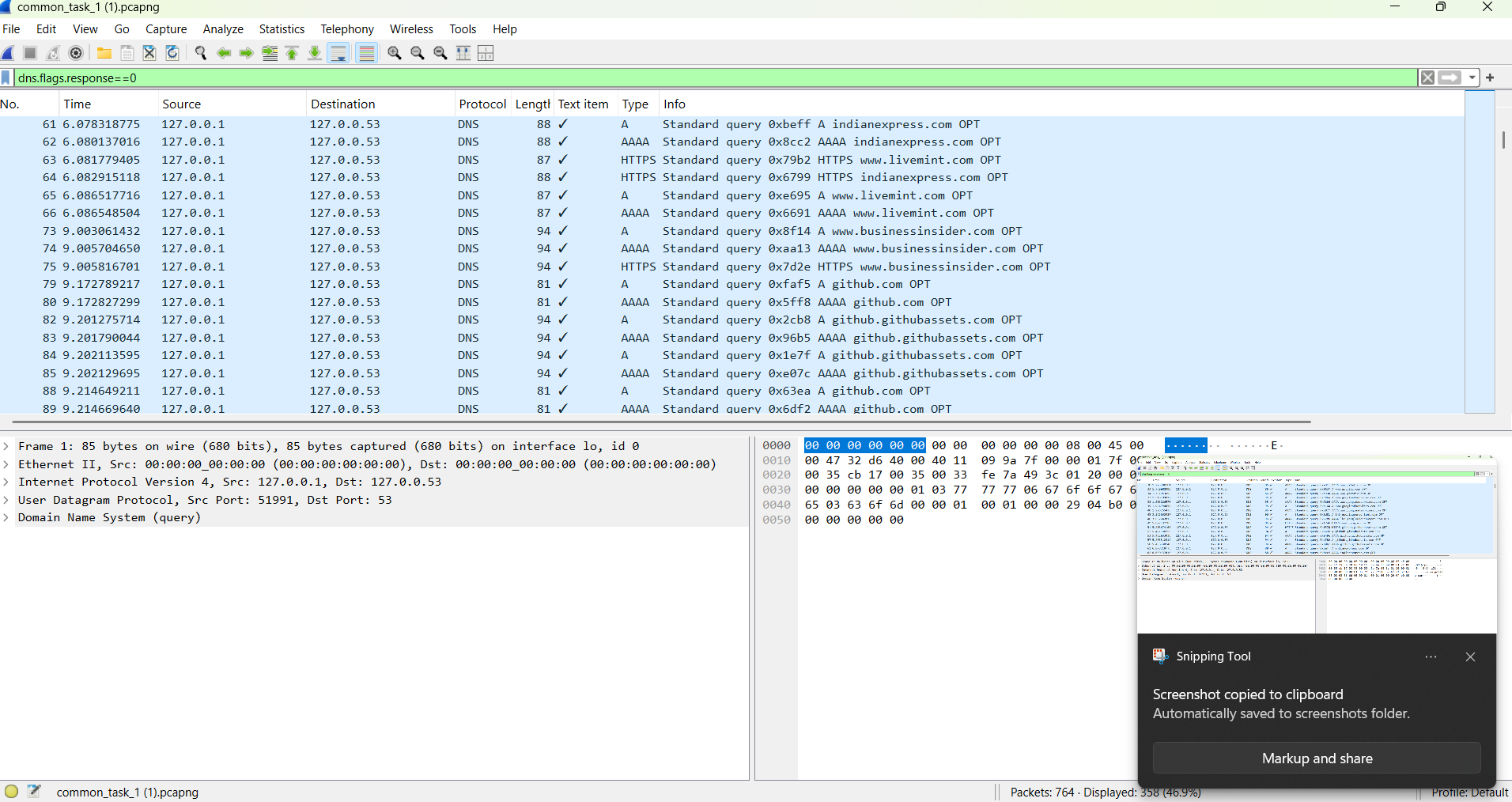
filter: dns.flags.response==0

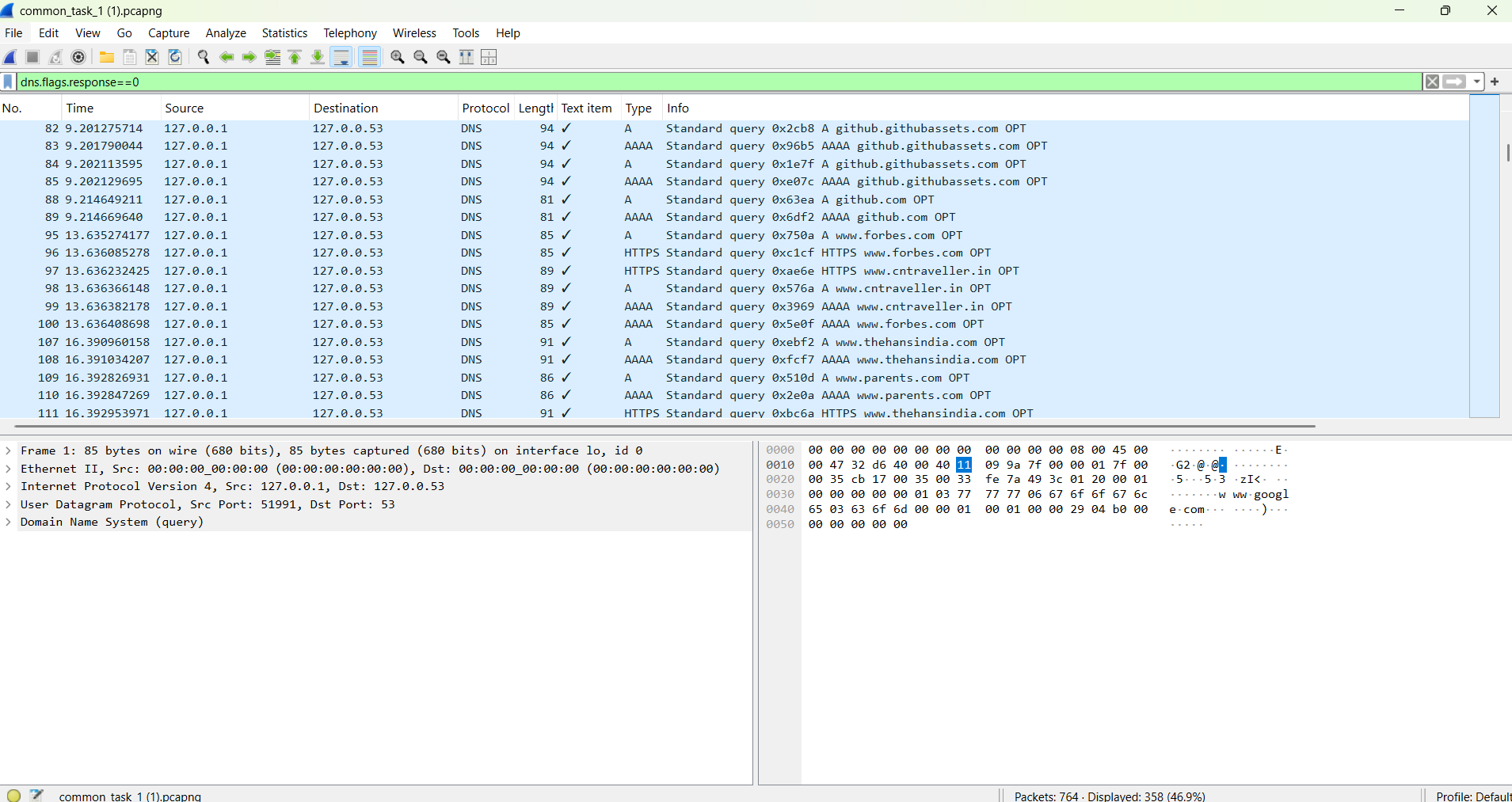
this showed that there are 358 standard query and 714-358=356 response query

3.What types of DNS queries were made?









since we need only query so filter: dns.flags.response==0

click any query here and go to dns and then see type and right click and give apply as column

this shows only dns query and not responses

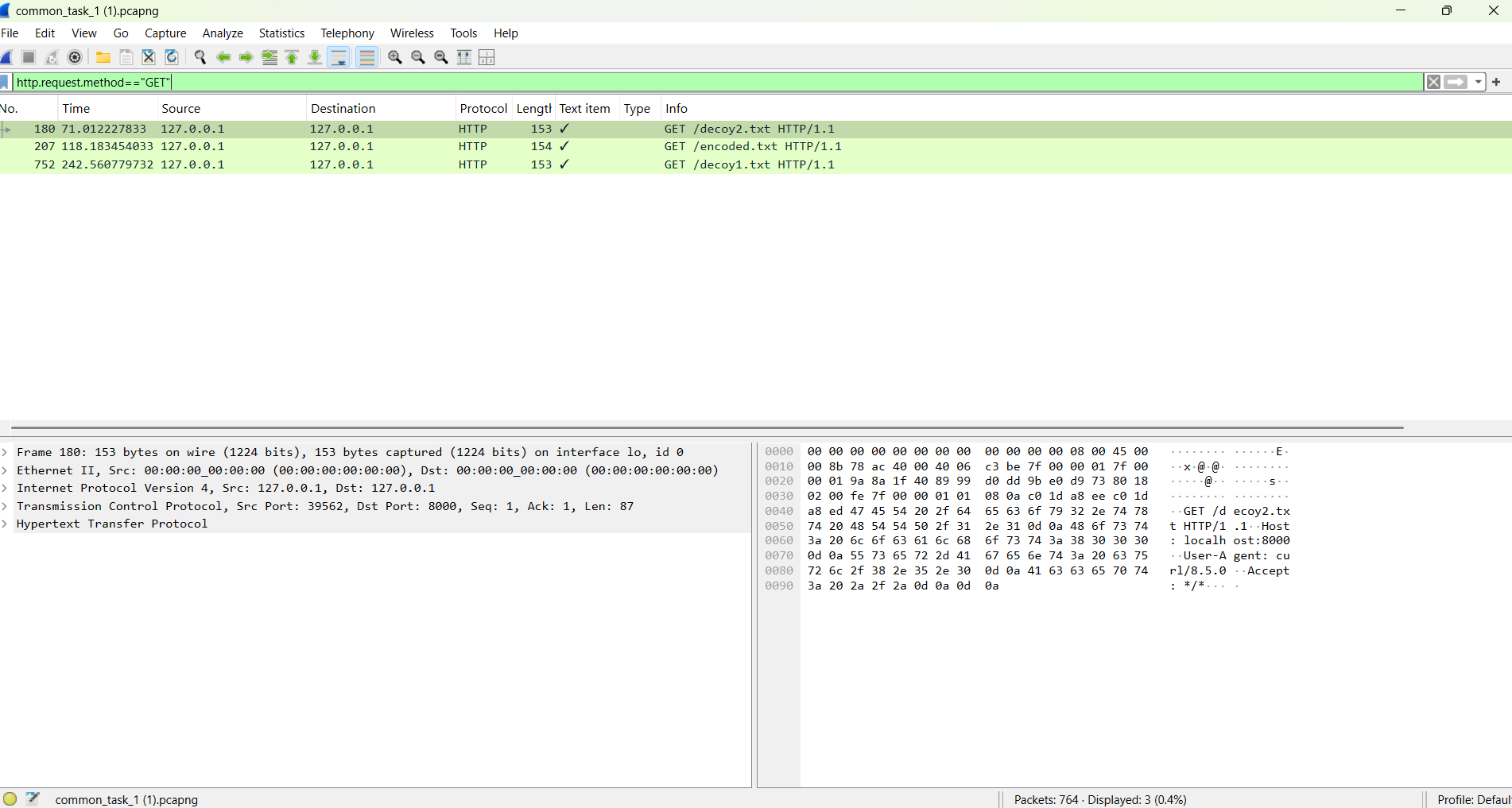
Types of dns queries found are A,AAAA,HTTPS

4.What is a Loopback Interface?

There exists special virtual network interface which is used by computer to send traffic from itself to itself

example use: ping <your ip address> . this confirms if systems network stack is working. Here loopback interface is used.

5. How many .txt files were requested? List their names.



There are 3 .txt files

filter used : http.request.method=="GET"

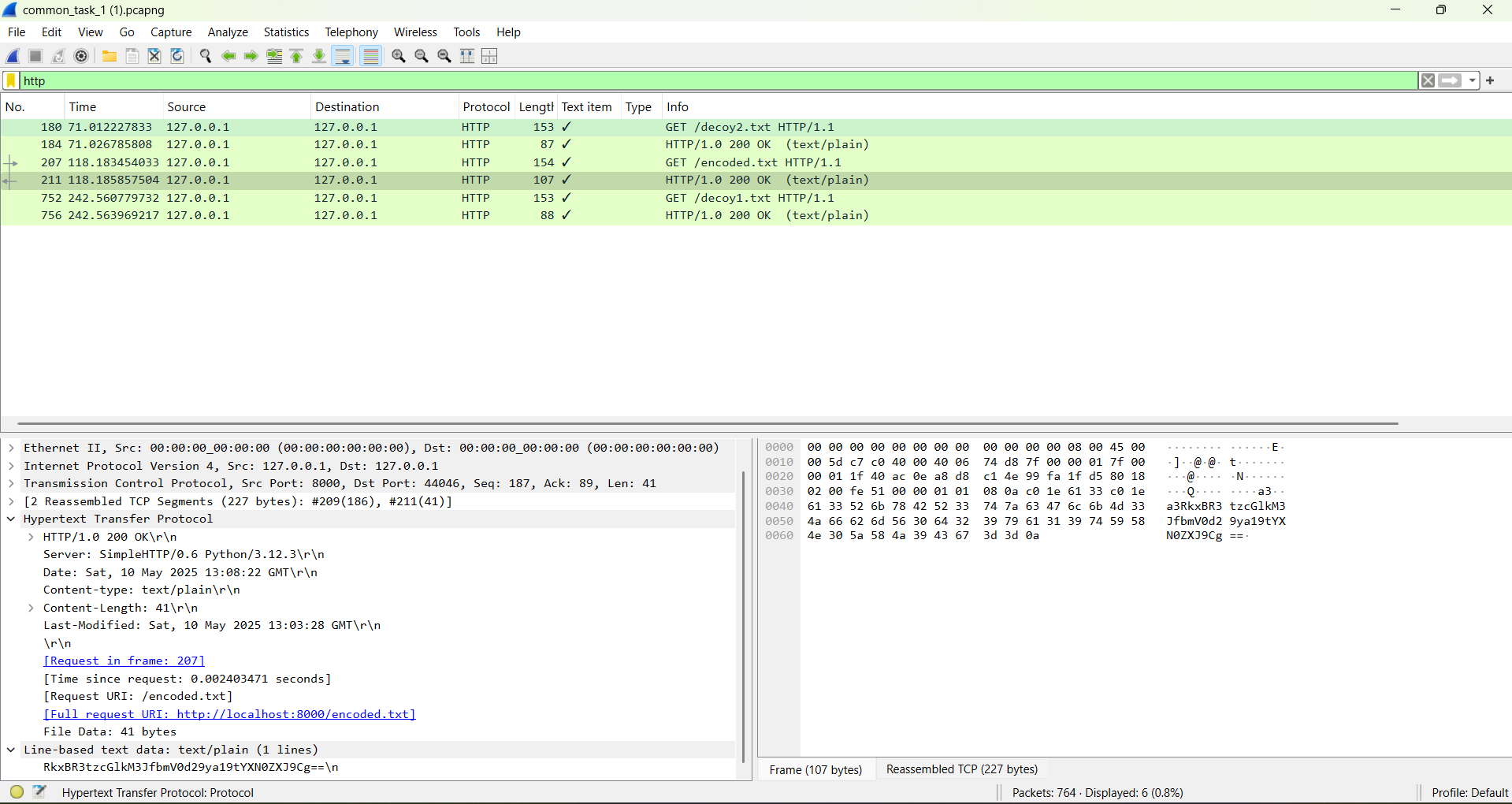
Their names are

- decoy2.txt

- decoy1.txt

- encoded.txt

6. One .txt file contains base64-encoded content. Identify and decode it. What does it contain?



filter used: http

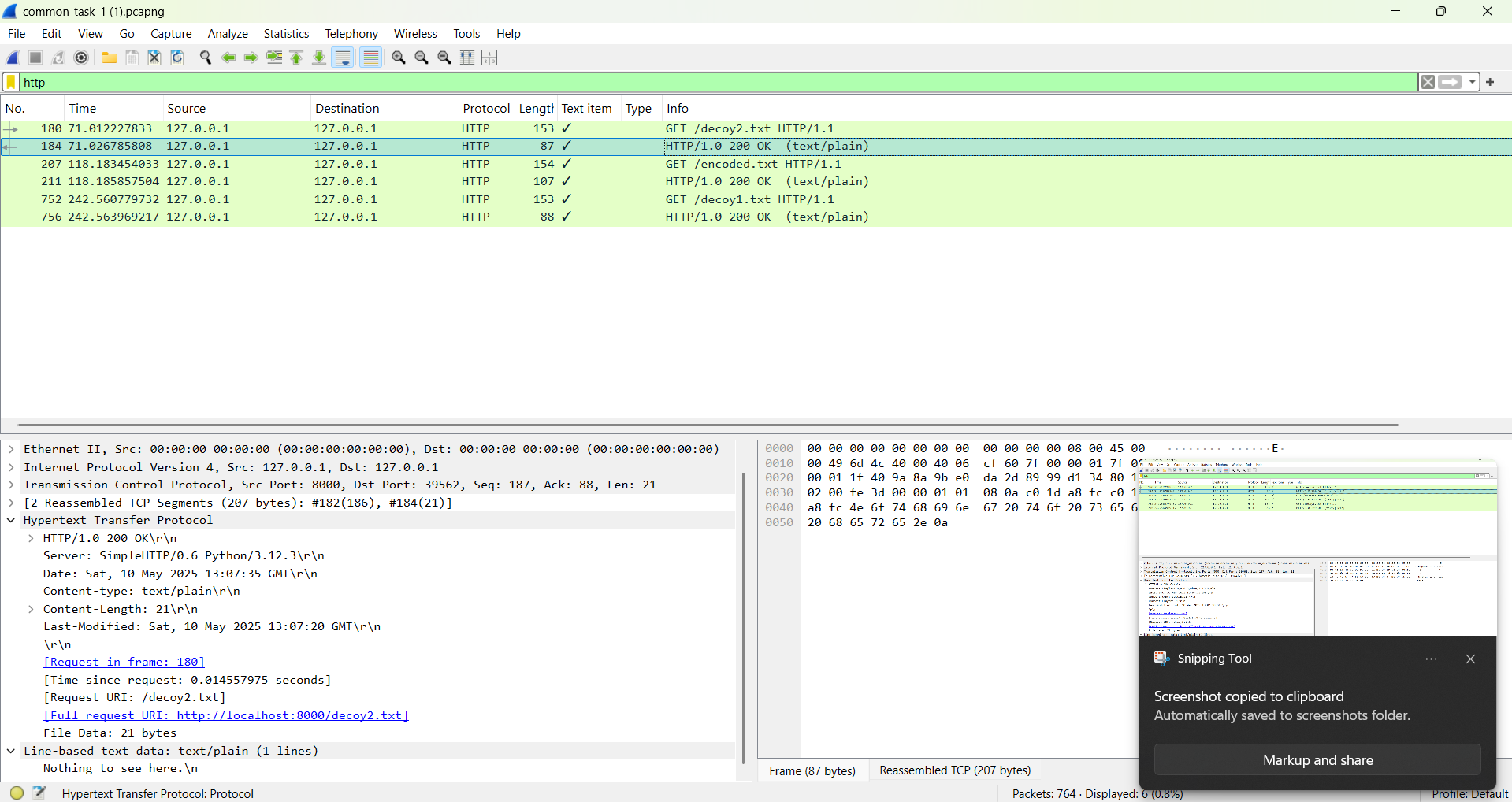
file name is encoded.txt

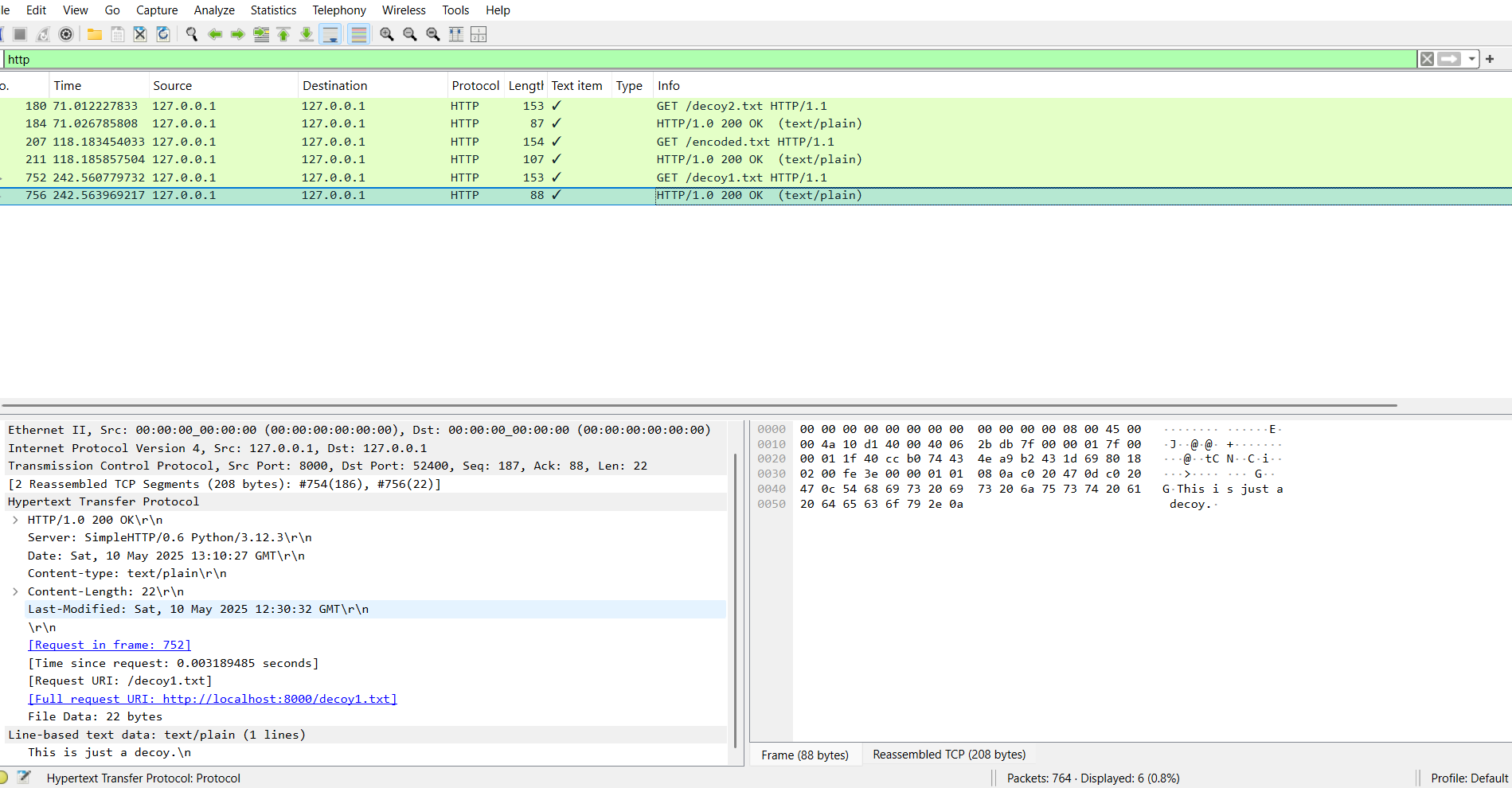
we can see line based text data

encoded is RkxBR3tzcGlkM3JfbmV0d29ya19tYXN0ZXJ9Cg==\n

decoded is FLAG{spid3r\_network\_master}

7.Was any attempt made to distract the analyst using decoy files? Explain.



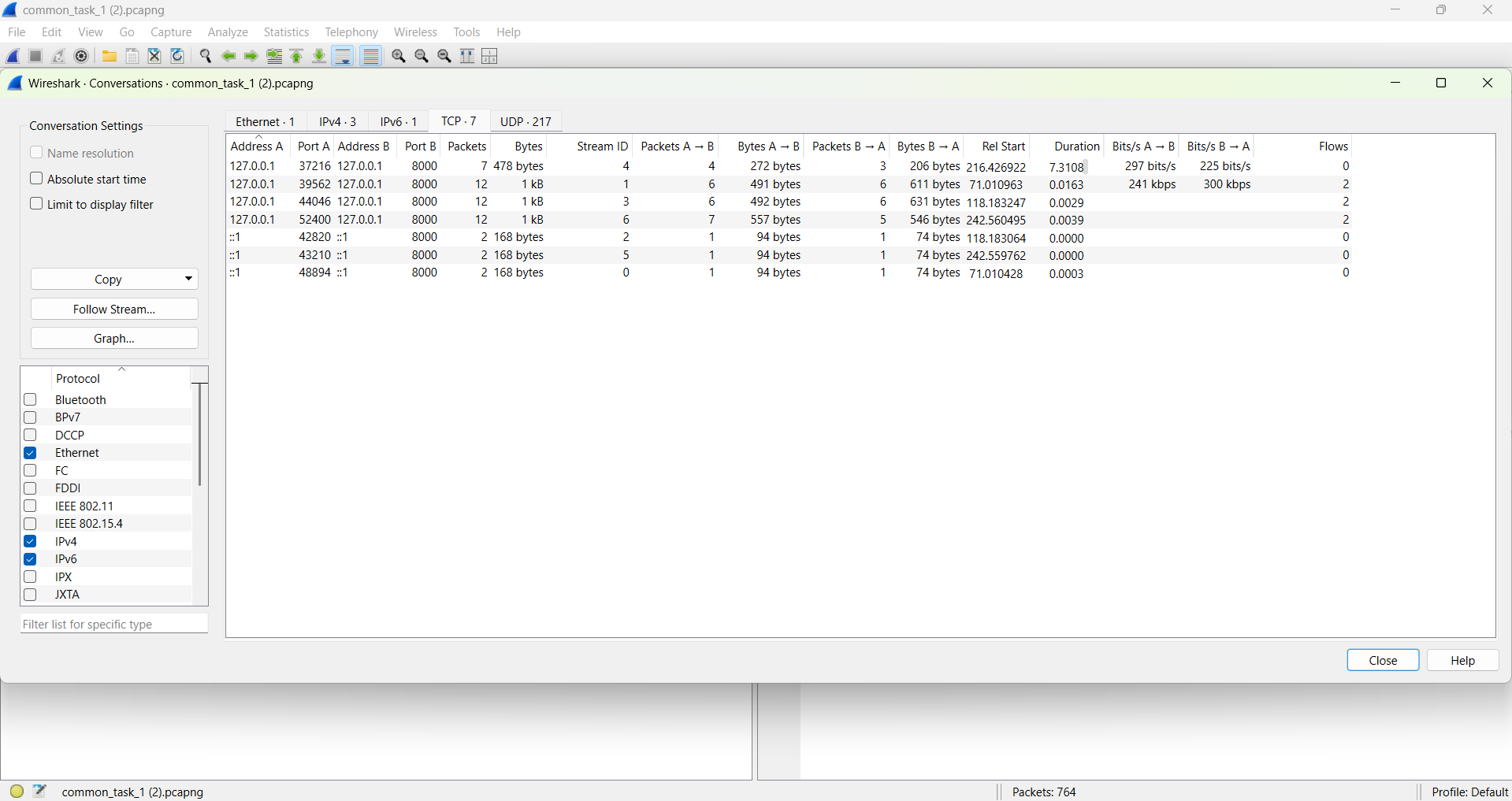


yes, there are two http files named decoy1.txt and decoy2.txt which have contents "this is just a decoy.\n' and "nothing to see here.\n" .

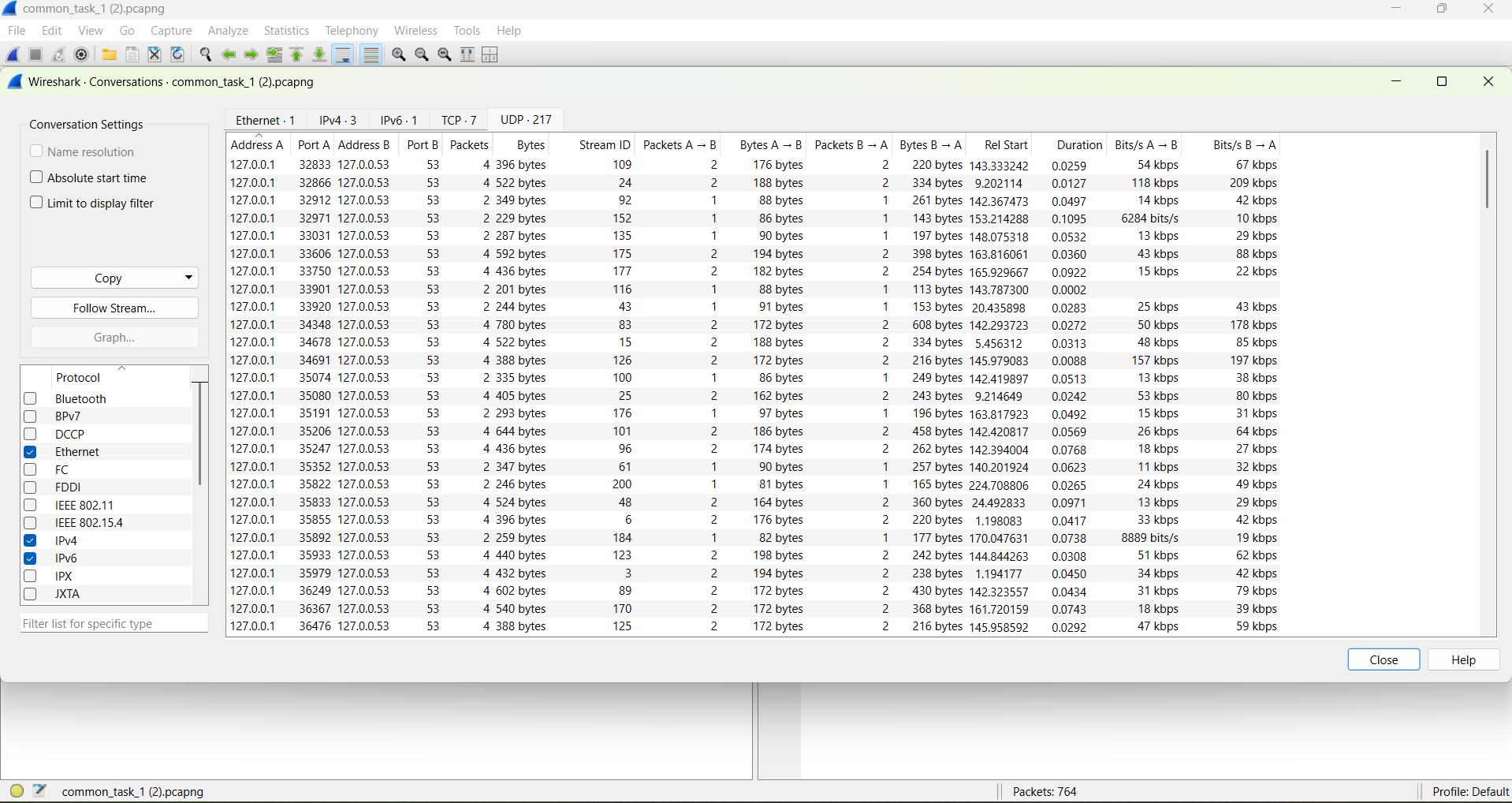
these contents are just to time waste the analyst

8.Are there any known ports being used for uncommon services?

In statistics -> conversations

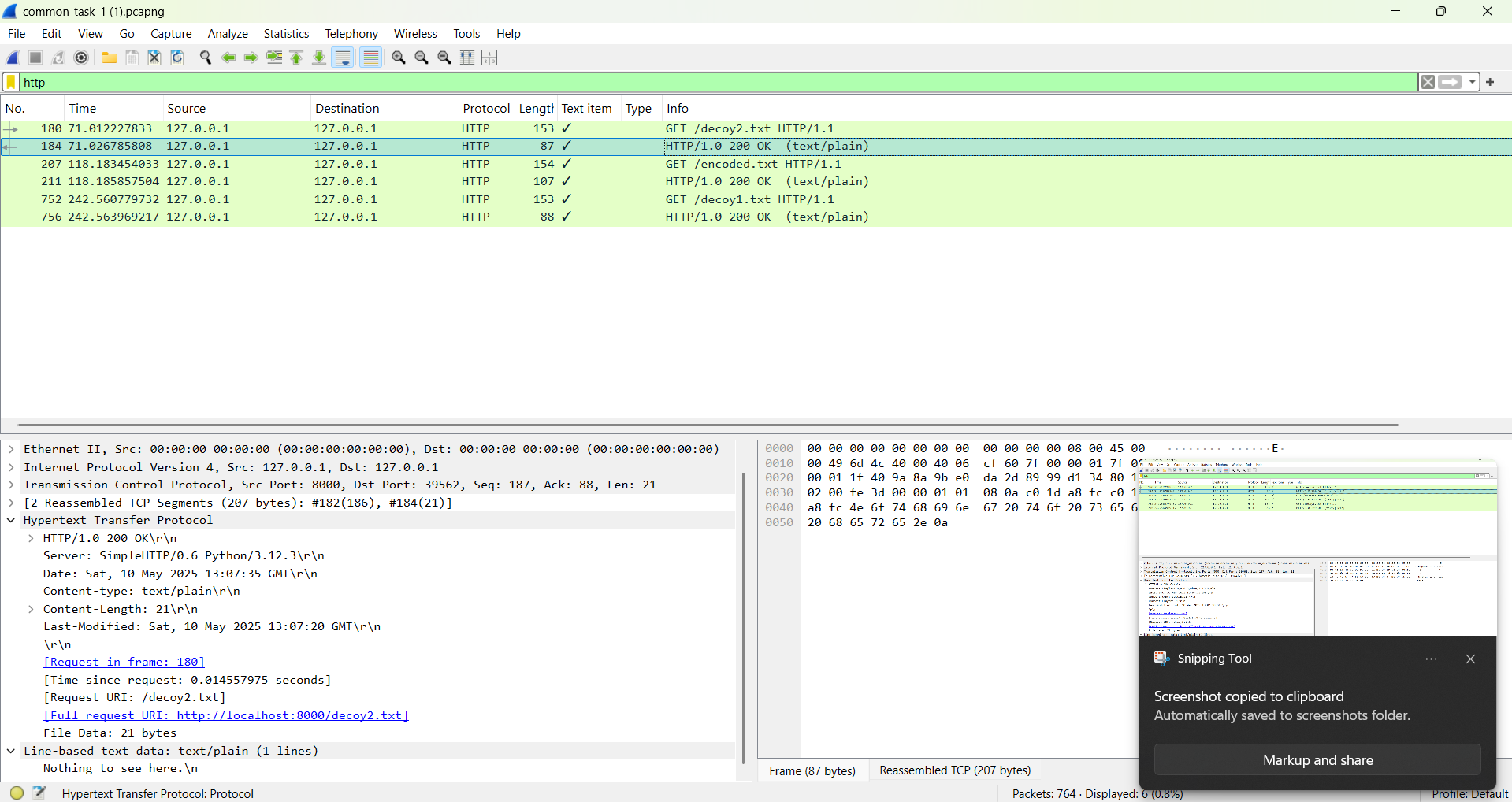


TCP WE SEE PORT 8000 WAS USED



IN UDP WE SEE PORT 53 USED

9.How many HTTP GET requests are visible in the capture?



3 HTTP GET request are visible

10.What User-Agent was used to make the HTTP requests?

to find filter:http then right click get request then give follow http request

file decoy1.txt user agent: curl/8.5.0

file decoy2.txt user agent : curl/8.5.0

file encoded.txt user agent: curl/8.5.0

so user agent for all was curl/8.5.0

