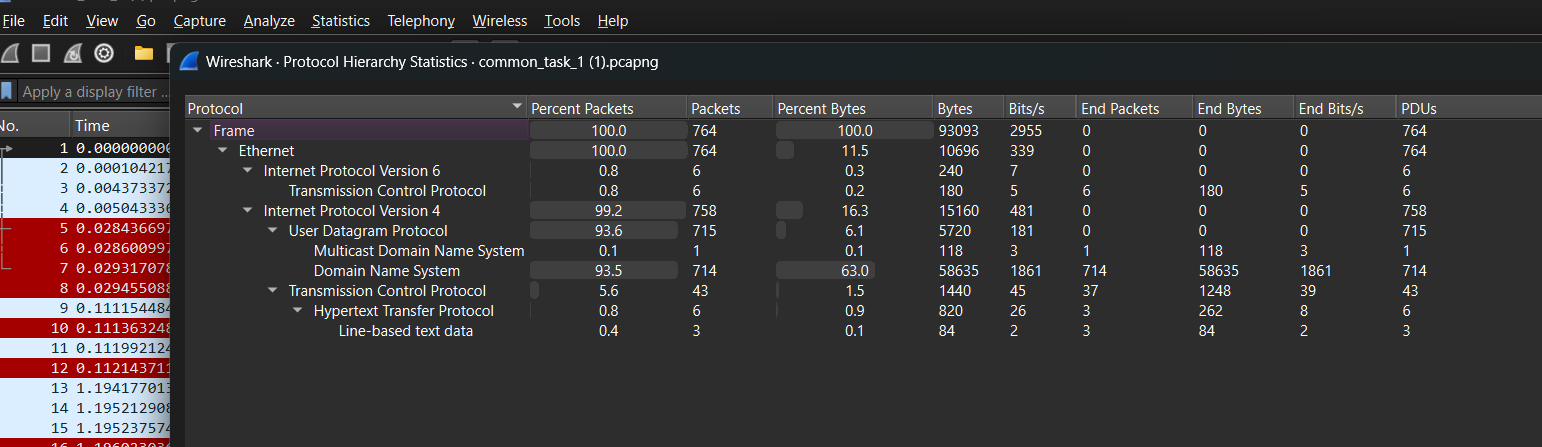
**Question-1:**

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

**🡪 While searching for the types of traffic present in the given .pcapng file ,, I saw this on Wireshark , (how do I find this whole data ) , by clicking the (statistics) 🡪(protocol hierarchy ) option in the dropdown menu .**

****

**It shows these types of traffics🡪**

1. **DNS(UDP) (domain name specific)- 714 packets-93.5%**
2. **MDNS(UDP)(Multicast domain name specific)- 1 packets-0.1%**
3. **TCP(IPv4)- 43 packets-5.6%**
4. **HTTP(hypertext transfer protocol)-0.8 % - 6 packets**
5. **TCP(IPv6)- 6 packets-0.8%**

**Q.2-** **2. How many DNS queries were made in total?**

**🡪 358 DNS queries were made**

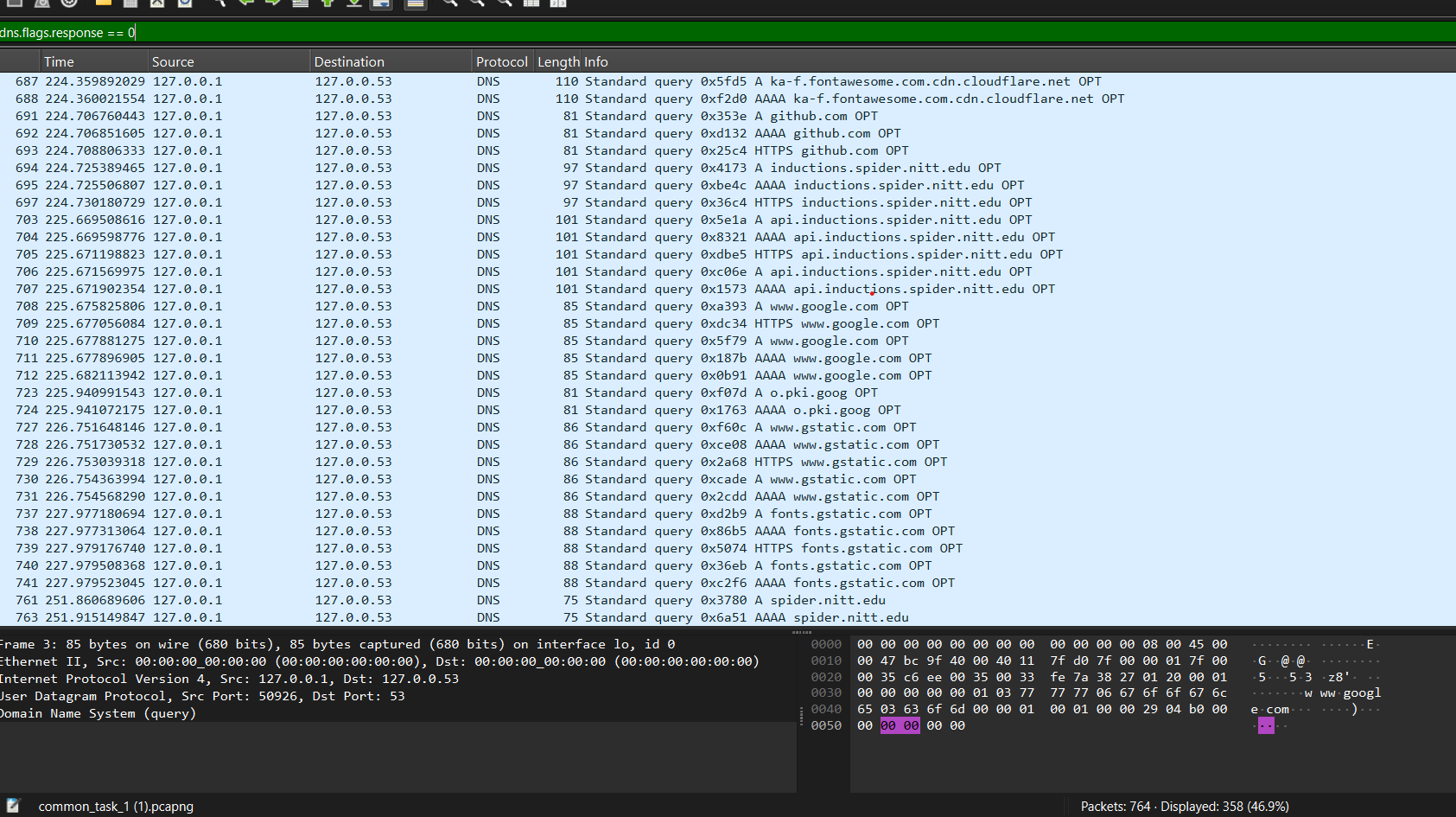
**46.9 % in total**

**By applying the filter**

**Dns.flags.response==0**

**I found something like this**

**🡪**

****

**Q.3-->**

**. What types of DNS queries were made?**

**🡪**

**Following-**

**1.A**

**2.AAAA**

**3.HTTPS**

**4.PTR**

**Q.4- 4. What is a Loopback Interface?**

**🡪**

**A loopback interface is a virtual interface that allows a computer to communicate with itself. It is mainly used for testing and internal networking purposes.**

**The most common loopback IP address is:**

**127.0.0.1**

**Q.5-**

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

**🡪3 files were requesyed through https which are .txt files->**

**decoy1.txt**

**decoy2.txt**

**encoded.txt**

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

**🡪base 64 encoded file-encoded.txt**

**After decoding->**

**It contains this message->**

**FLAG{spid3r\_network\_master}**

**Q.7 –**

**Yes, attempts were made to distract the analyst using decoy files. Two .txt files named /decoy1.txt and /decoy2.txt were requested via HTTP. Their naming and content suggest they are meant to appear relevant but contain no meaningful data. In contrast, the file /encoded.txt contains Base64-encoded data, which, when decoded, reveals the actual hidden information. This pattern indicates a deliberate attempt to mislead or distract anyone analyzing the traffic.**

**They don’t contain 64 bit encodd data**

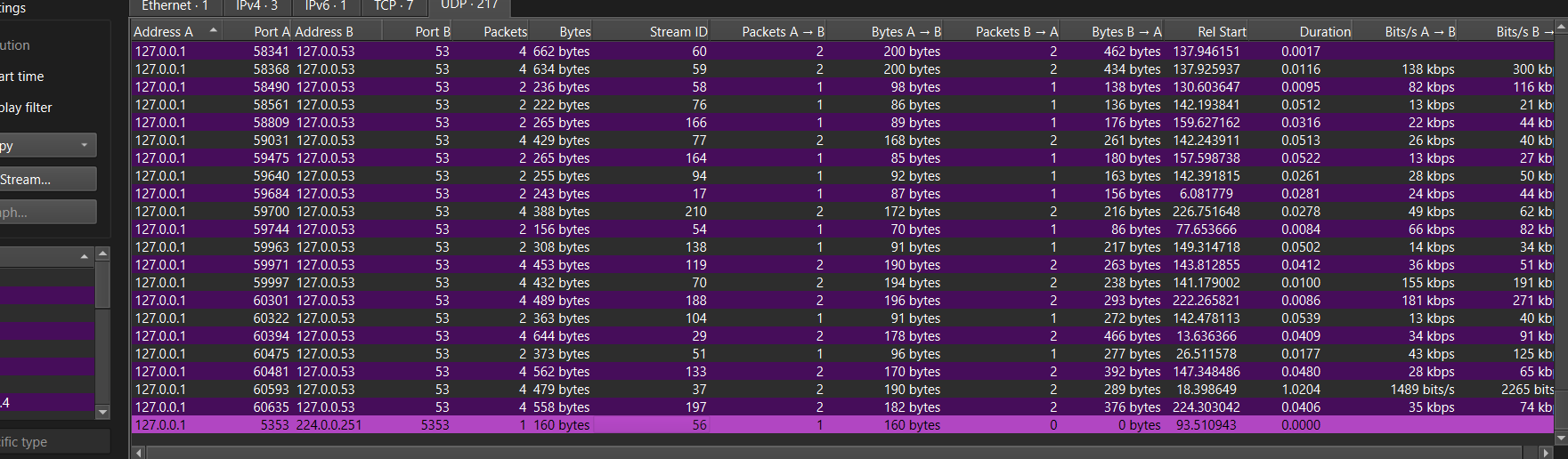
**They just contain messages like->**

**Nothing to see here**

**This is just a decoy**

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

**Soln->**

**Yes , UDP port **

**As it is shown that the transfer to the port in the last communication have destination port numbered as 5353 which is different from the other udp port comunation destination ports so I think they might be used for uncommon service .**

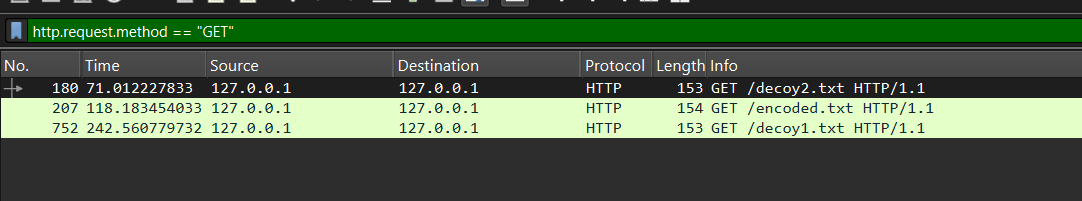
**Q.9 How many HTTP GET requests are visible in the capture?**

**Soln - > using the filter http.request.method==”GET”**

**We can filter out the http get requests in wireshark as you can see in the ss**

**There are 3 http get requests**

**---🡪**

****

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

Soln🡪from this ss,, I have applied filter http.request

Then clicking on one of the request get me this page where user agent is given as curl/8.5.0\r\n and checking all 3 http request shows there are same user agent in all of them

