CN 12 : WIRESHARK LAB :DNS

Name : Harshavardhan Anil Bamane

PRN : 22510112

Batch : S-7

Q1)

Locate the DNS query and response messages. Are then sent over UDP or TCP?

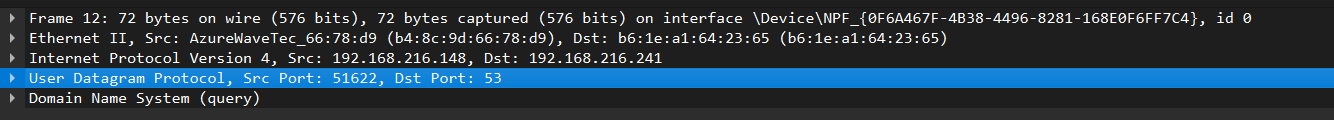
Ans. They are sent over UDP

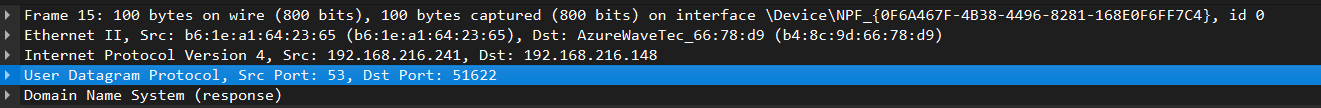




Q2)

What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans. 



The destination port for the DNS query :53

The source port of the DNS response : 53

Q3)

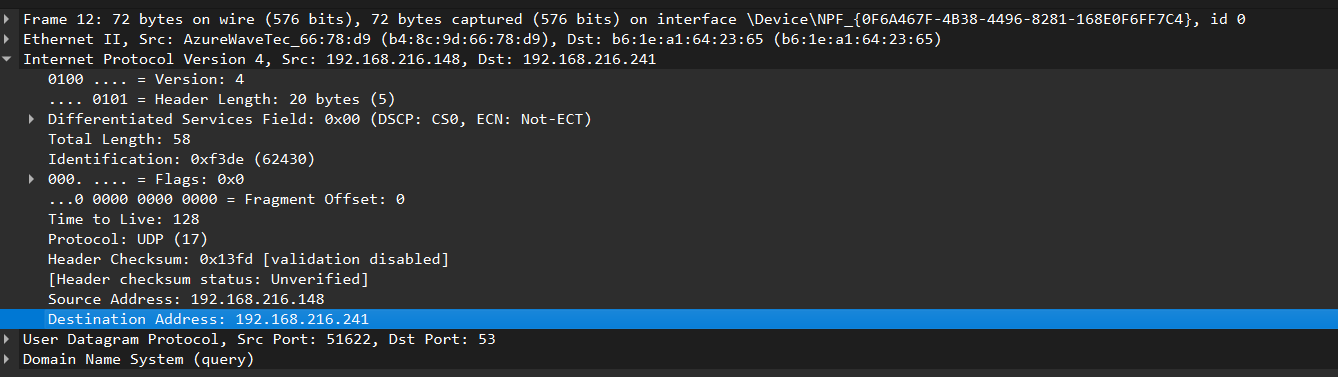
To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans. Destination in packet: 192.168.216.241

Local DNS server : 192.168.216.241

Yes, they are same.

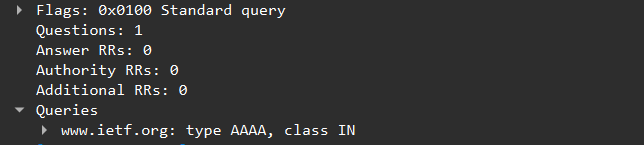




Q4)

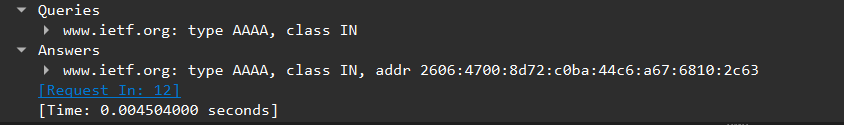
Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

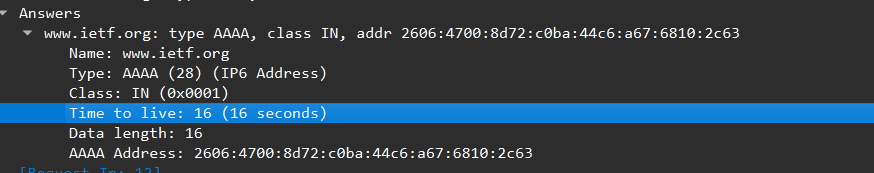
Ans. It’s a type AAAA Standard Query and it doesn’t contain any answers..



Q5)

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans. Yes 1 answers, it contains TTL,type,class,address,name. 

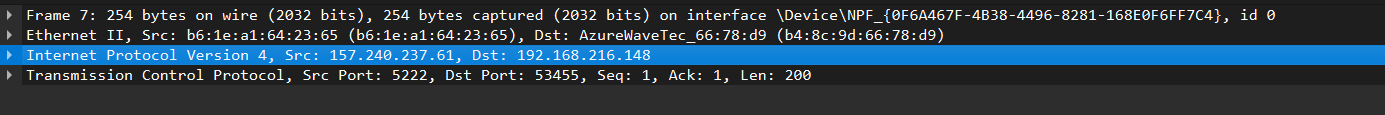


Q6)

Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans.

TCP Packet



The first SYN packet was sent to 192.168.216.148which corresponding to the first IP address provided in the DNS response message.

Q7)

This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Ans. No.

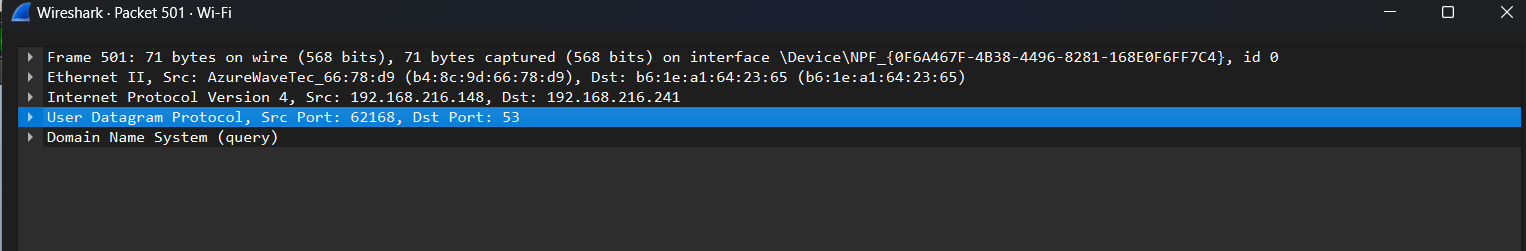
Q8)

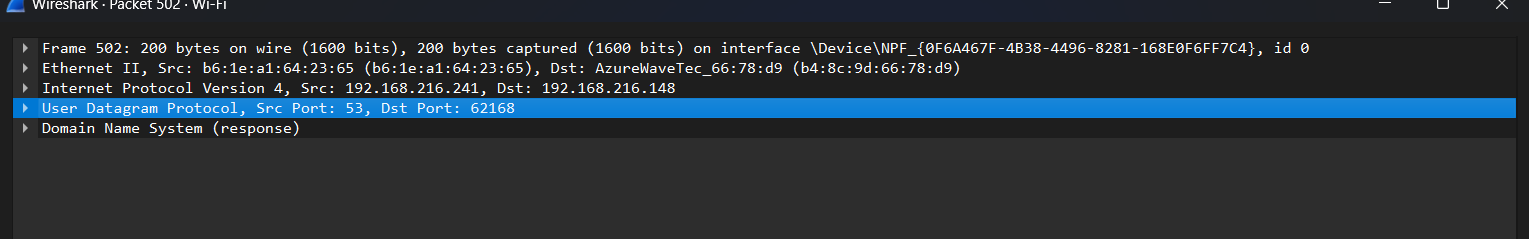


What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans.

Both are 53.





Q9)

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans.

Destination: 192.168.216.241.Yes, it is of the DNS server to which

request was sent.

