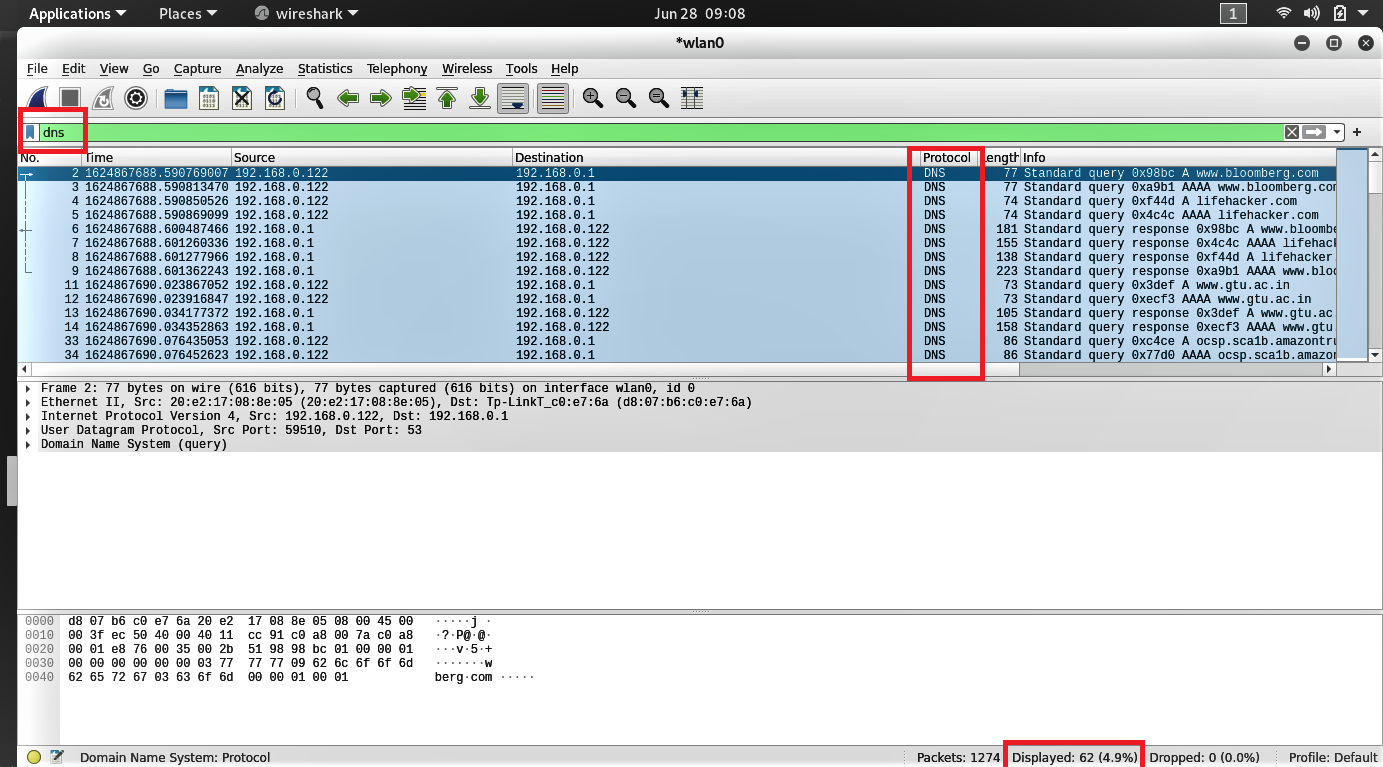
**1. Use the filtering functionality of Wireshark by typing “dns” in the filtering field, new**

**window will appear:**

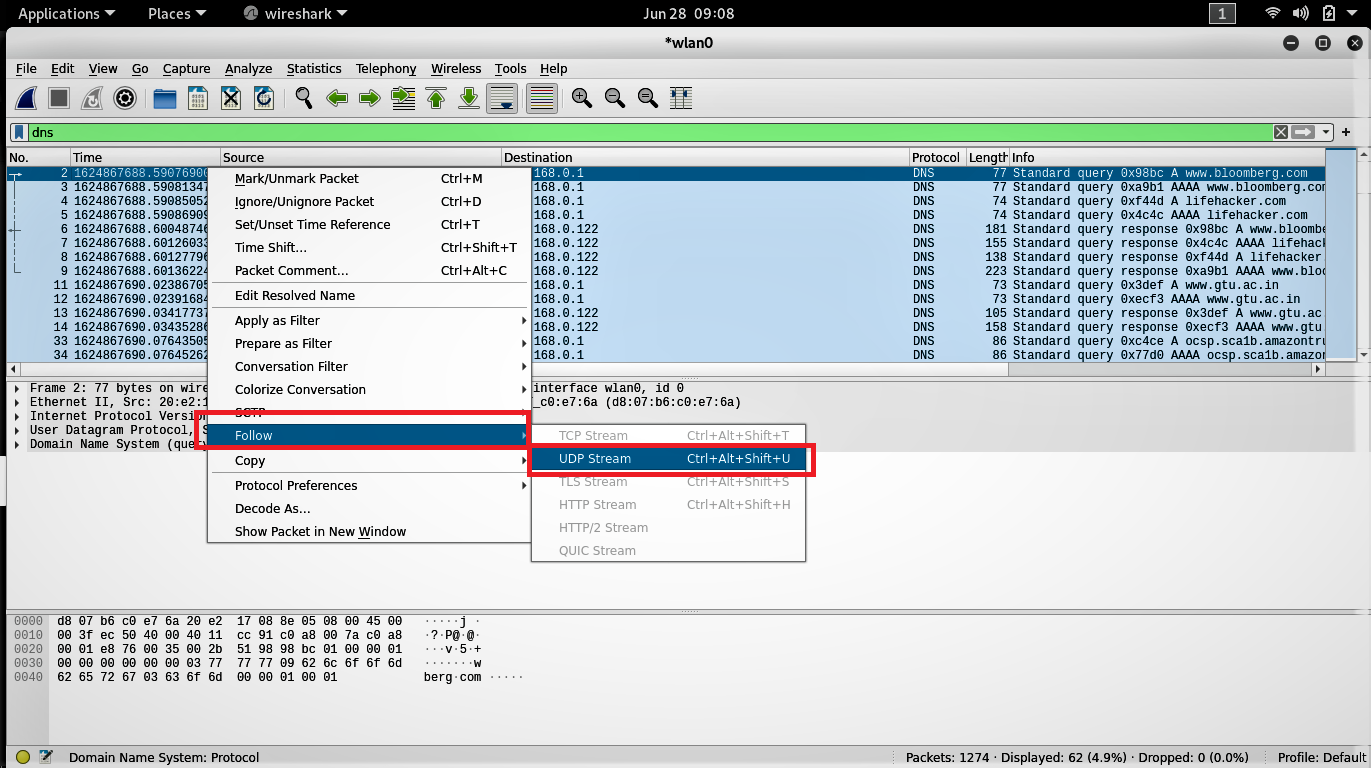
**ans🡪**Total 62 dns requests****

**2. Let’s try now to find out what are those packets contain by following one of the**

**conversations (also called network flows), select one of the packets and press the right**

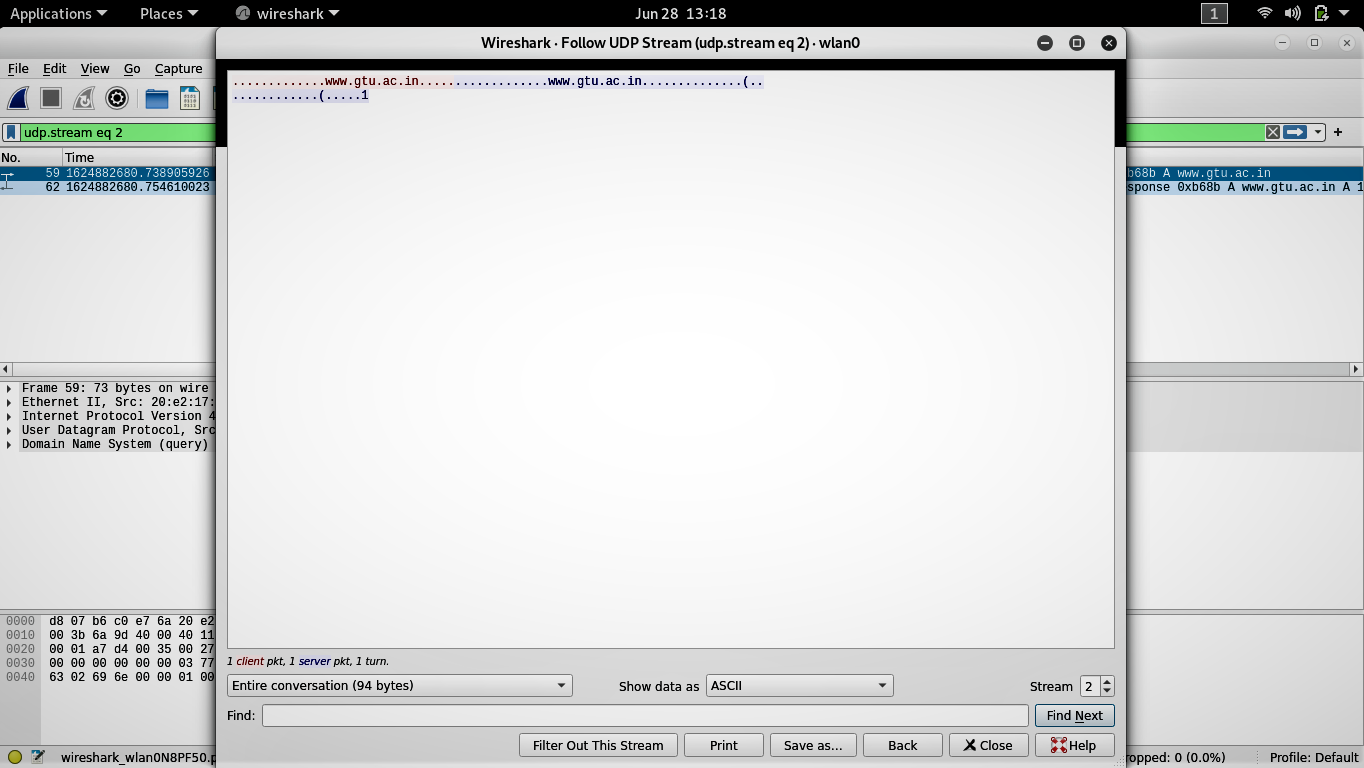
**mouse button, you should see another screen appear:**

**ans🡪** Right click on any single line then Follow > UDP Steream

****

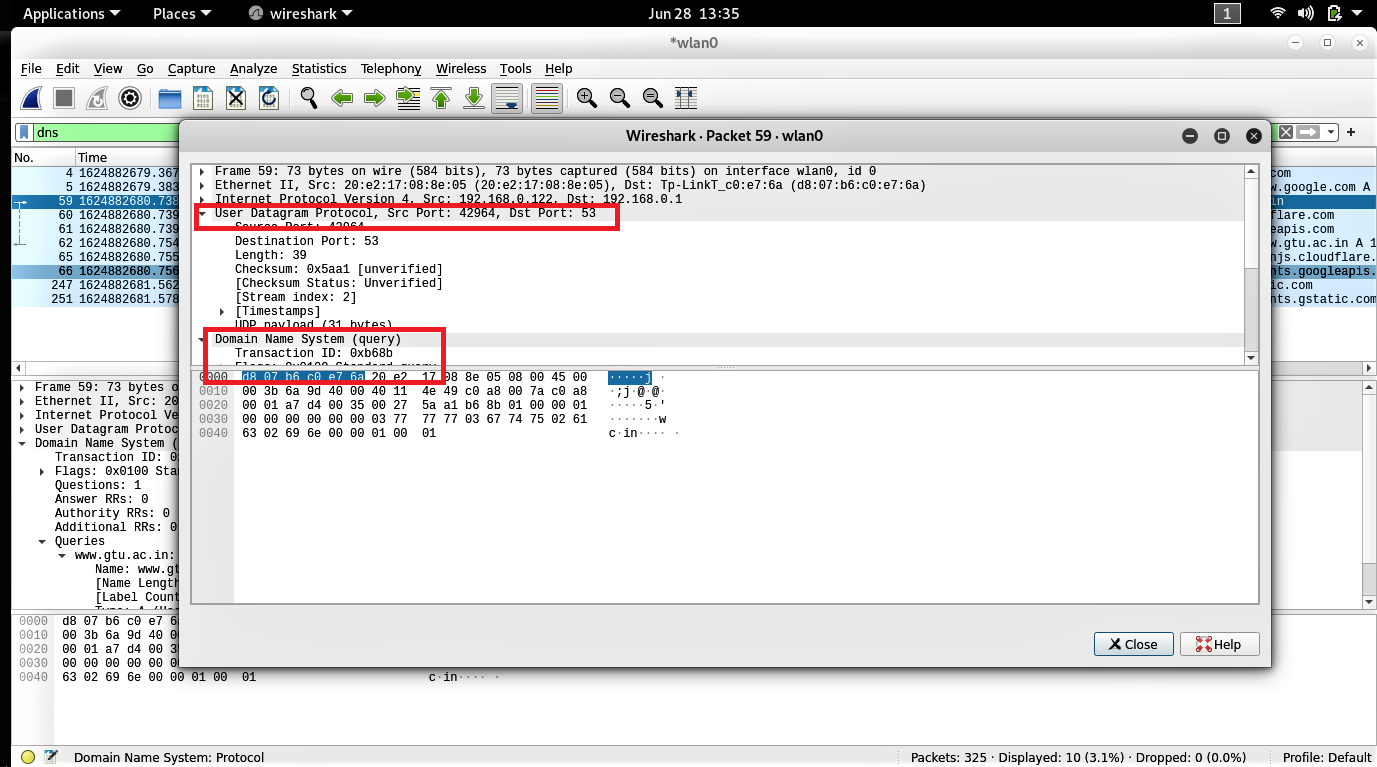
**3. Click on Follow UDP Stream, and then you will see another screen showing content**

**gtu.ac.in**

**ans🡪 **

**5. Locate the DNS Query and Response message, Are they sent on UDP or TCP**

**Ans🡪**  The DNS query and response messages are sent over UDP.

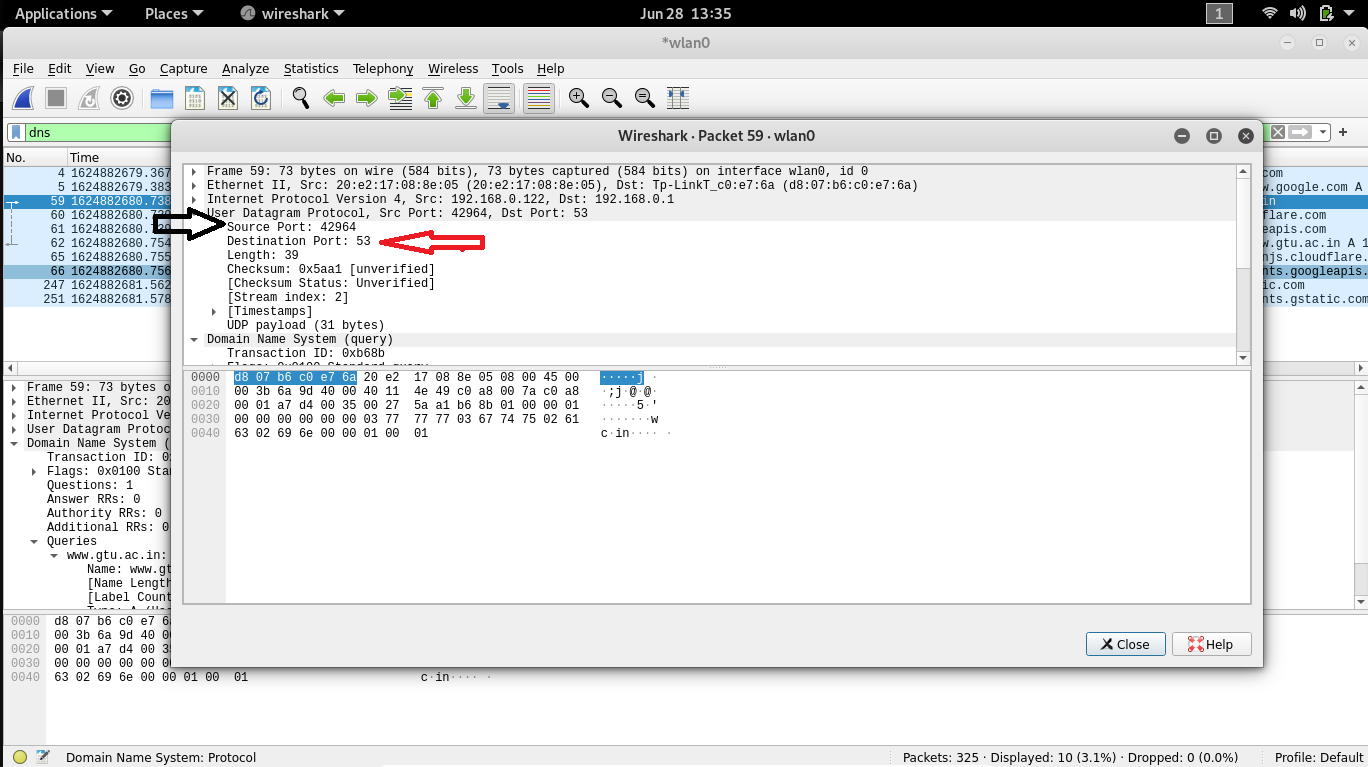


**6. What is the destination port for the DNS query message ? What is the source port of of**

**DNS response message?**

**Ans🡪**  The destination port is 53

The Source port is 42964

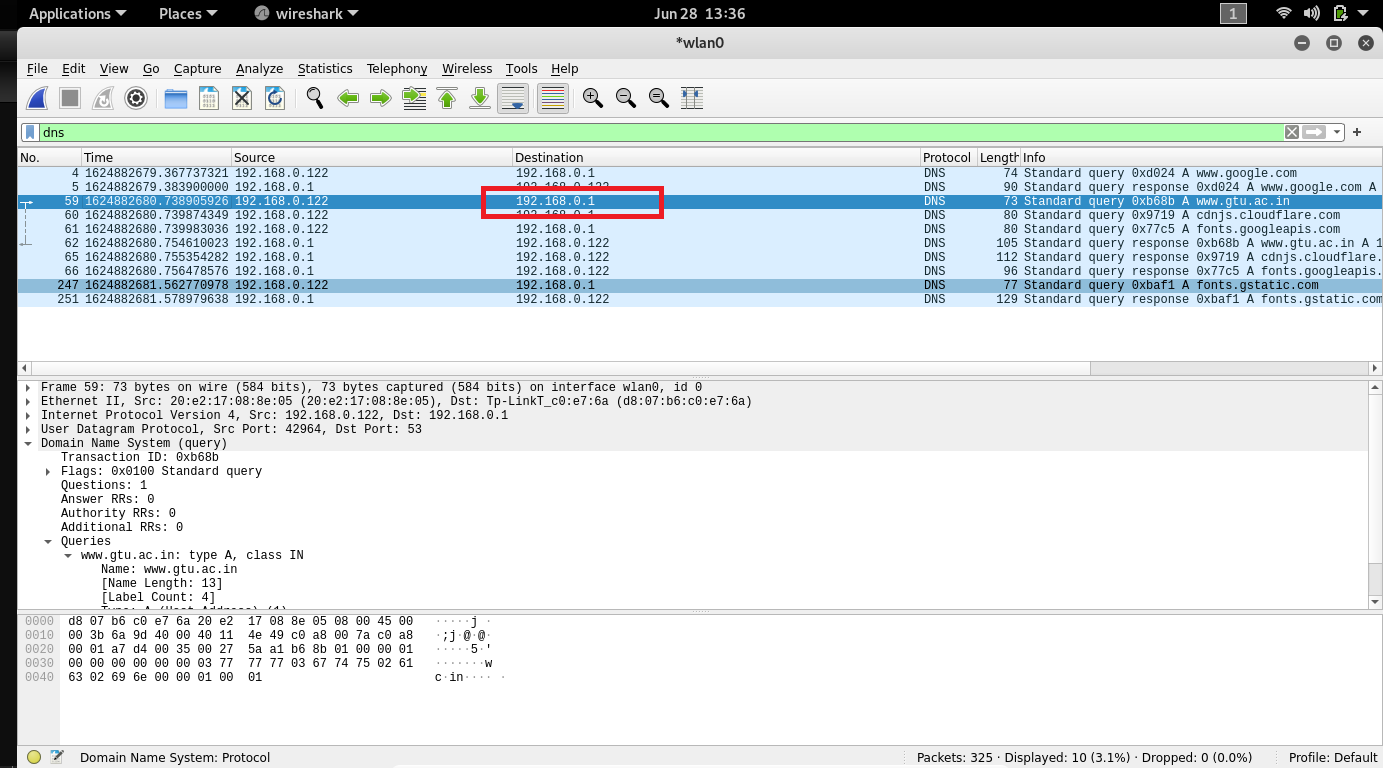


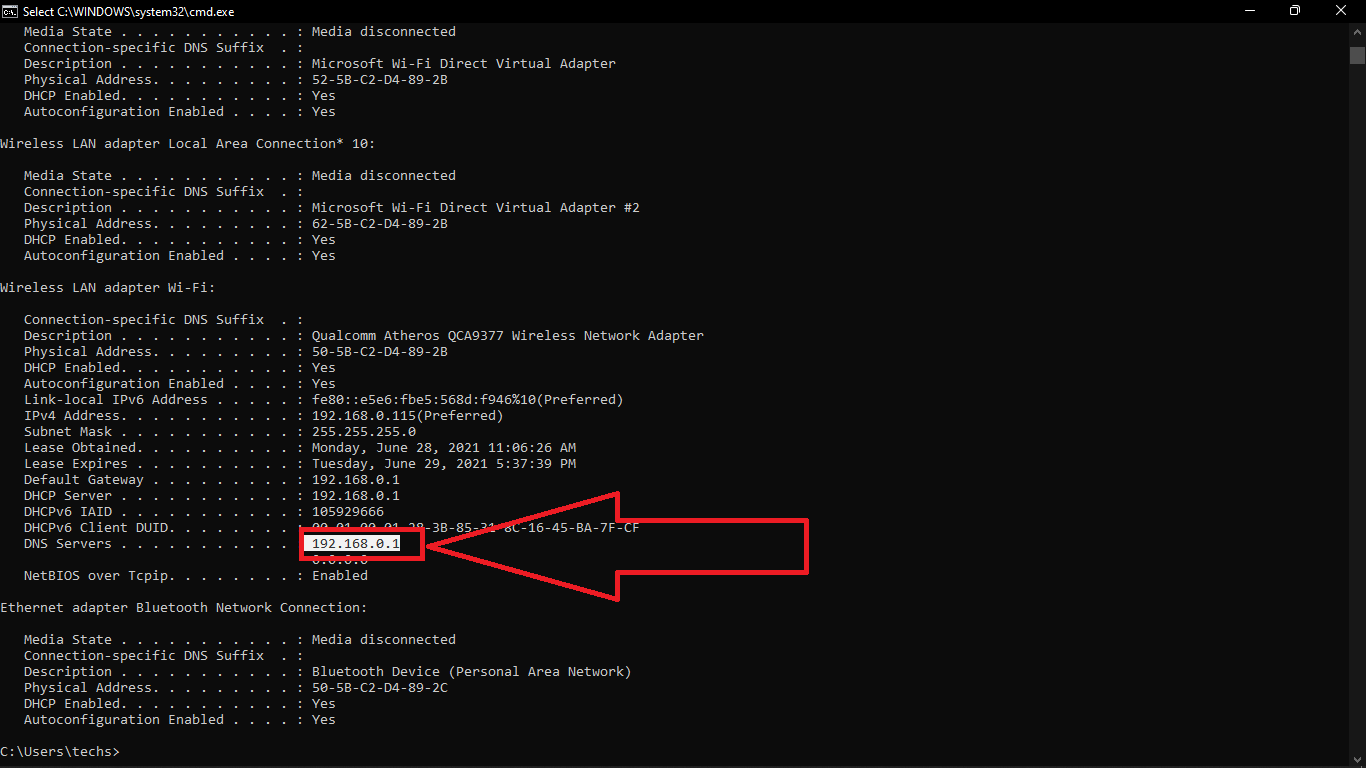
**7. To what IP address is the DNS query message sent ? is this the IP address of your default**

**local DNS server ? use ipconfig to determine the IP address of your local DNS server. Are**

**these two IP address the same ?**

**ans🡪** The DNS query was sent t oIP address 192.168.0.1 Yes it is the same IP address as that of my local DNS Server

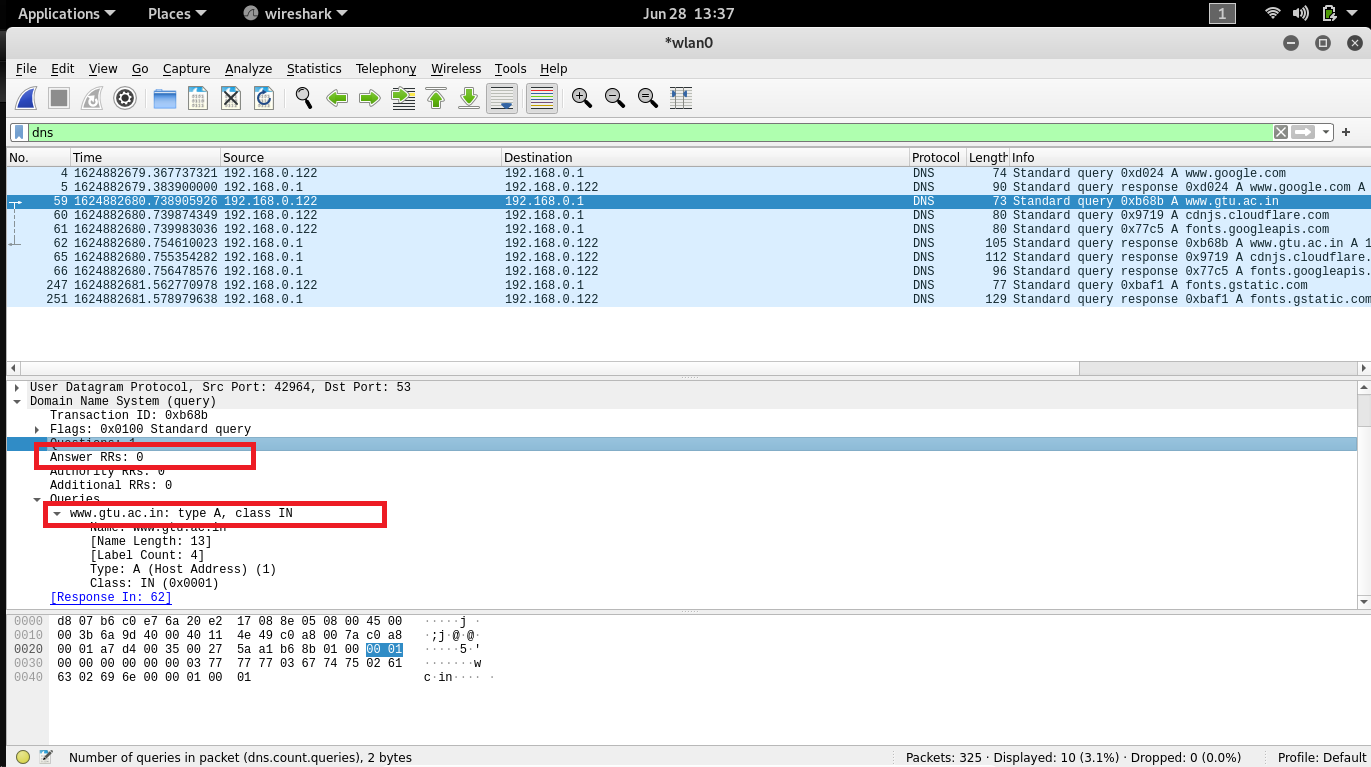


Also same as local dns server ip mentioned in below image

**8. Examine the DNS query message. What “Type” of DNS query is it? Does the query**

**message contain any “answers”?**

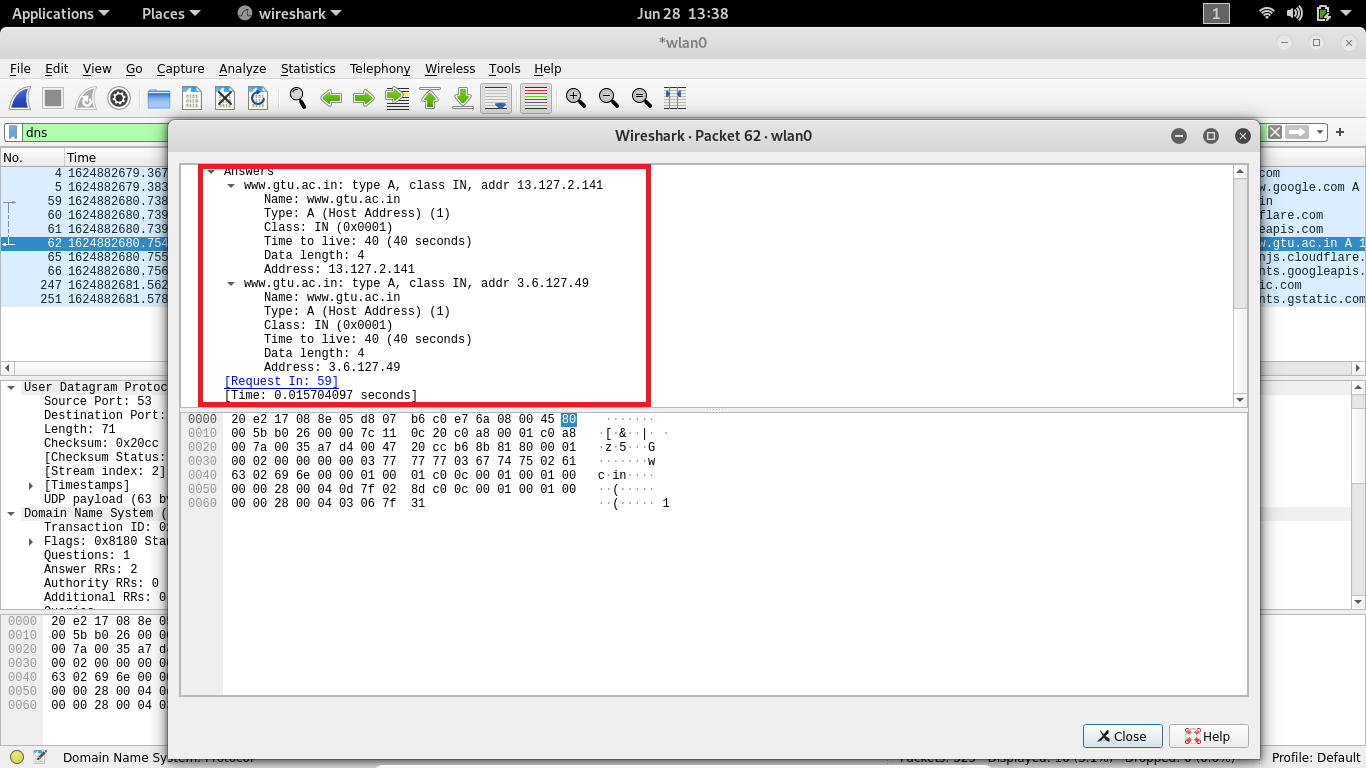
**ans🡪**  The Query message was a type “A” Query, but the message didn’t contain any “answer”



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

**these answers contain?**

**Ans🡪** The response message contained two answers to the query which was the sites address [13.127.2.141] and second is [3.6.127.49]. Although it also provided type of host address, time to live also data length.



**10. 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🡪** The destination of the SYN packet is 13.127.2.141, the same address that was provided in the DNS response message as the type “A” address of the webpage

**11. Why does DNS uses UDP ?**

**Ans🡪 UDP** can be **used** to exchange small information whereas **TCP** must be **used** to exchange information larger than 512 bytes. ... To make this, **DNS** always transfers Zone data **using TCP** because **TCP** is reliable and make sure zone data is consistent by transferring the full zone to other **DNS** servers who has requested the data.