Project 2

Wireshark Lab: DNS

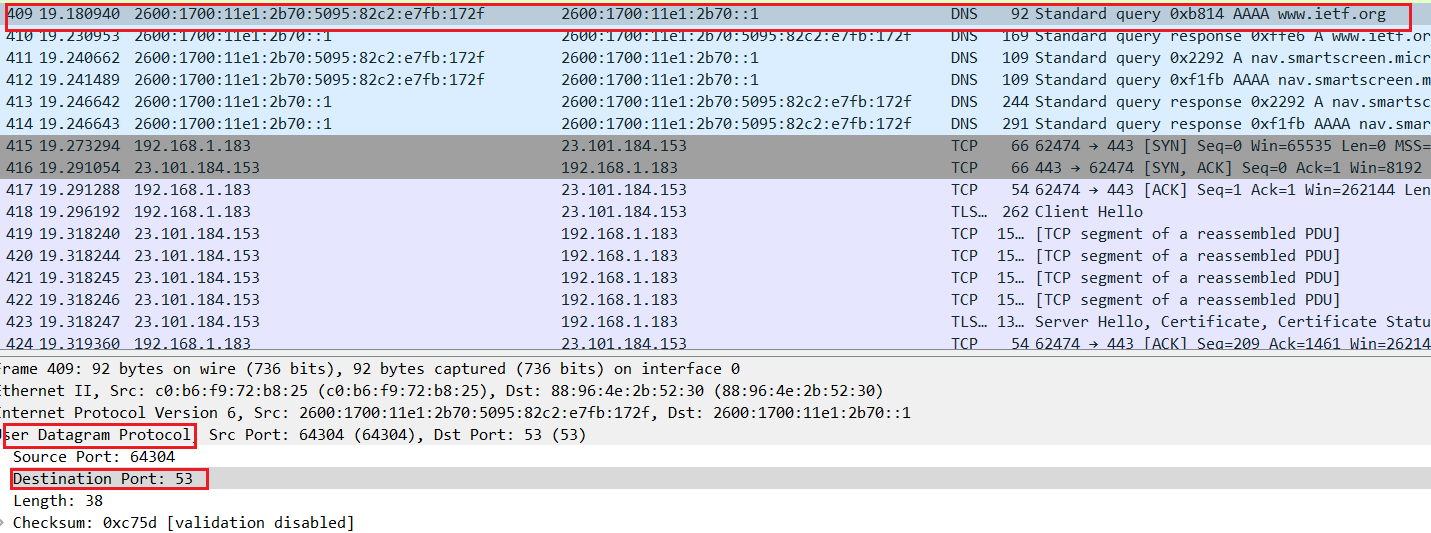
By

Shreyas Mohan

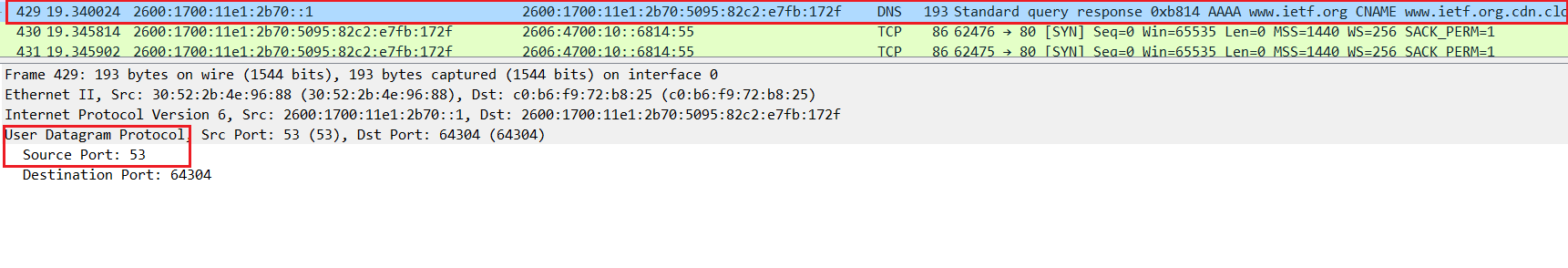
1001669806

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

***ANSWER: They are sent over UDP****.*

**

*Screenshot for DNS Query*

**

*Screenshot for DNS Response*

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

***ANSWER:***

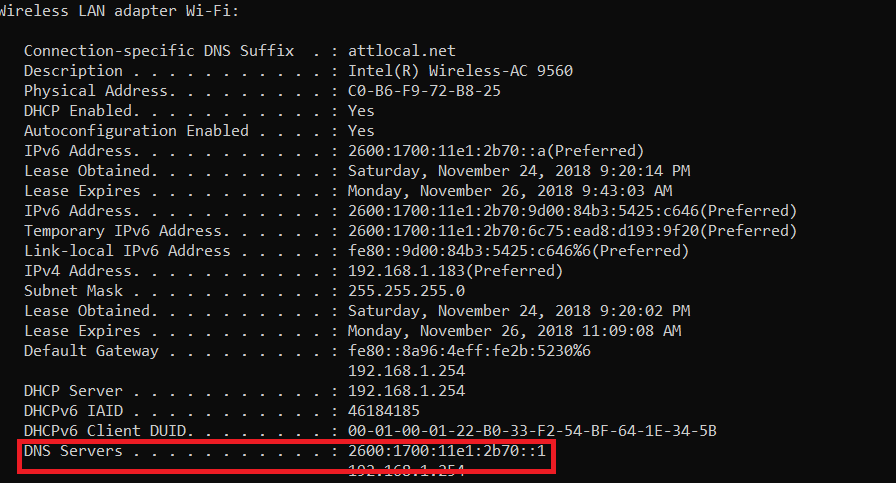
***Destination Port of query message:53***

***Source Port of response message:53***

6. 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?

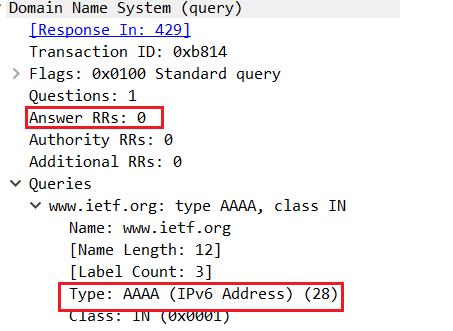
***ANSWER:***

*It is sent to 2600:1700:11e1:2b70::1(destination of query message),which is the IP address of one of my local DNS servers. Hence, both IP addresses are same.*

**

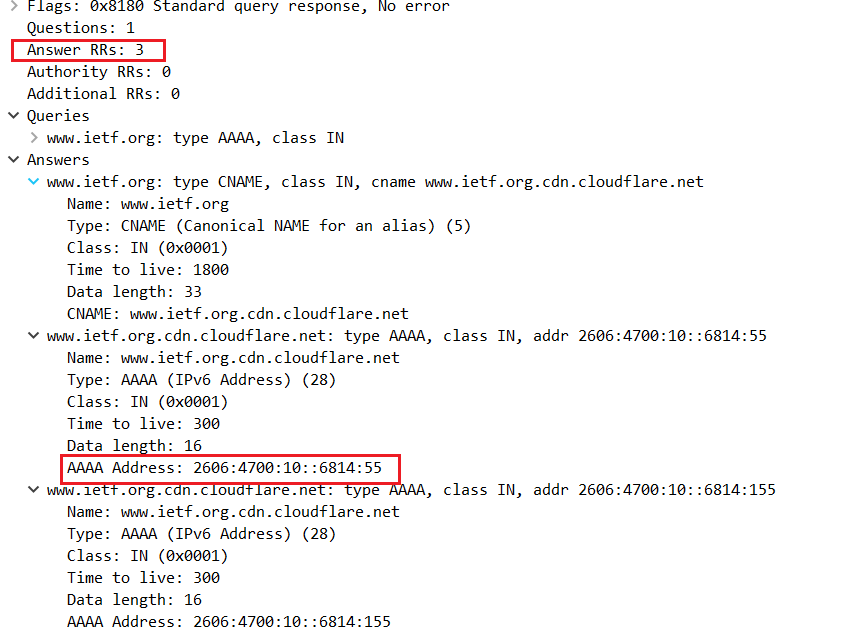
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**Answer:** Type: AAAA query (IPv6 address). The query message does not contain any answers.

**

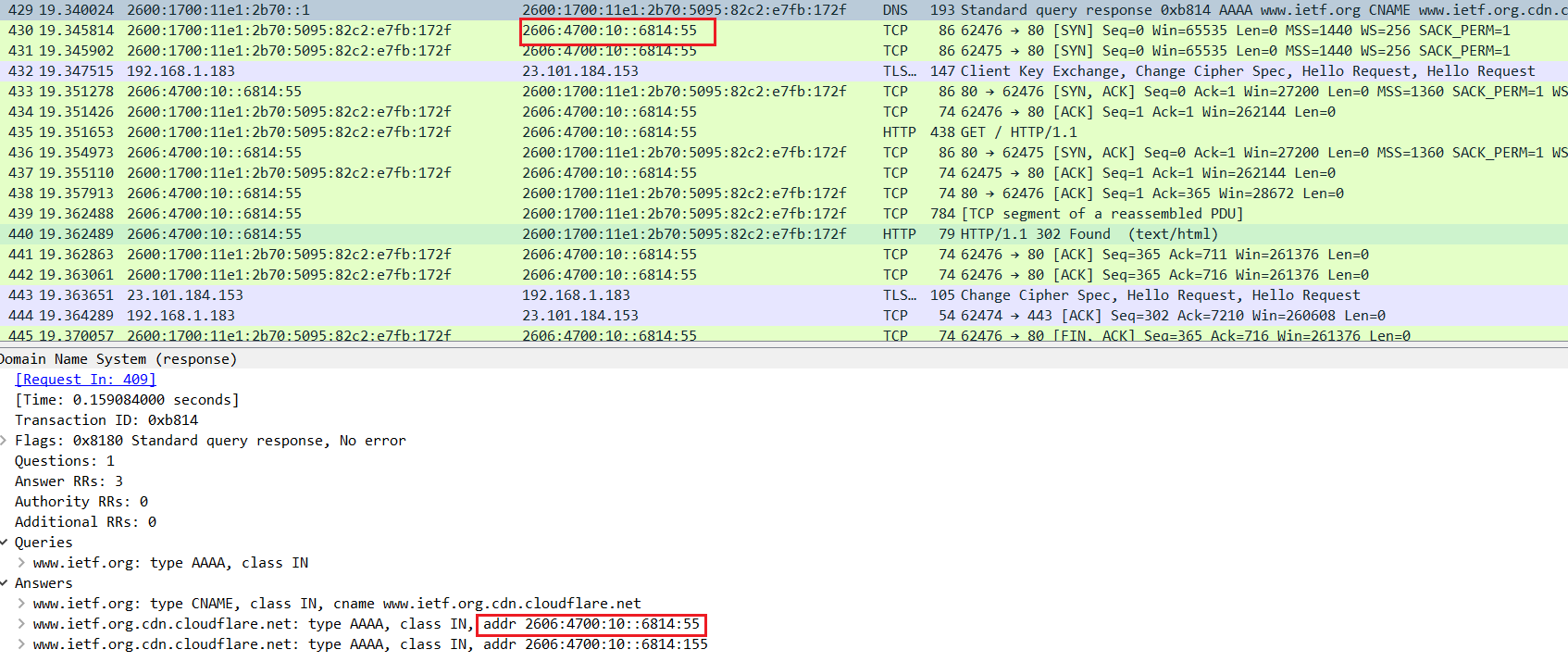
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answer: **Three answers** are provided. The answers contains **name of the host, type of the address, class, the TTL, data length and the IPv6 address.**

**

9. 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?

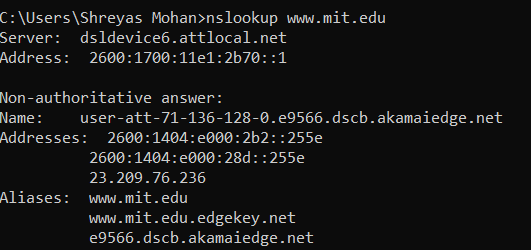
**ANSWER**: The destination IP address of the SYN packet is sent to **2606:4700:10::6814:55.** ,which **corresponds to the second IP address** in the DNS response message.

**

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

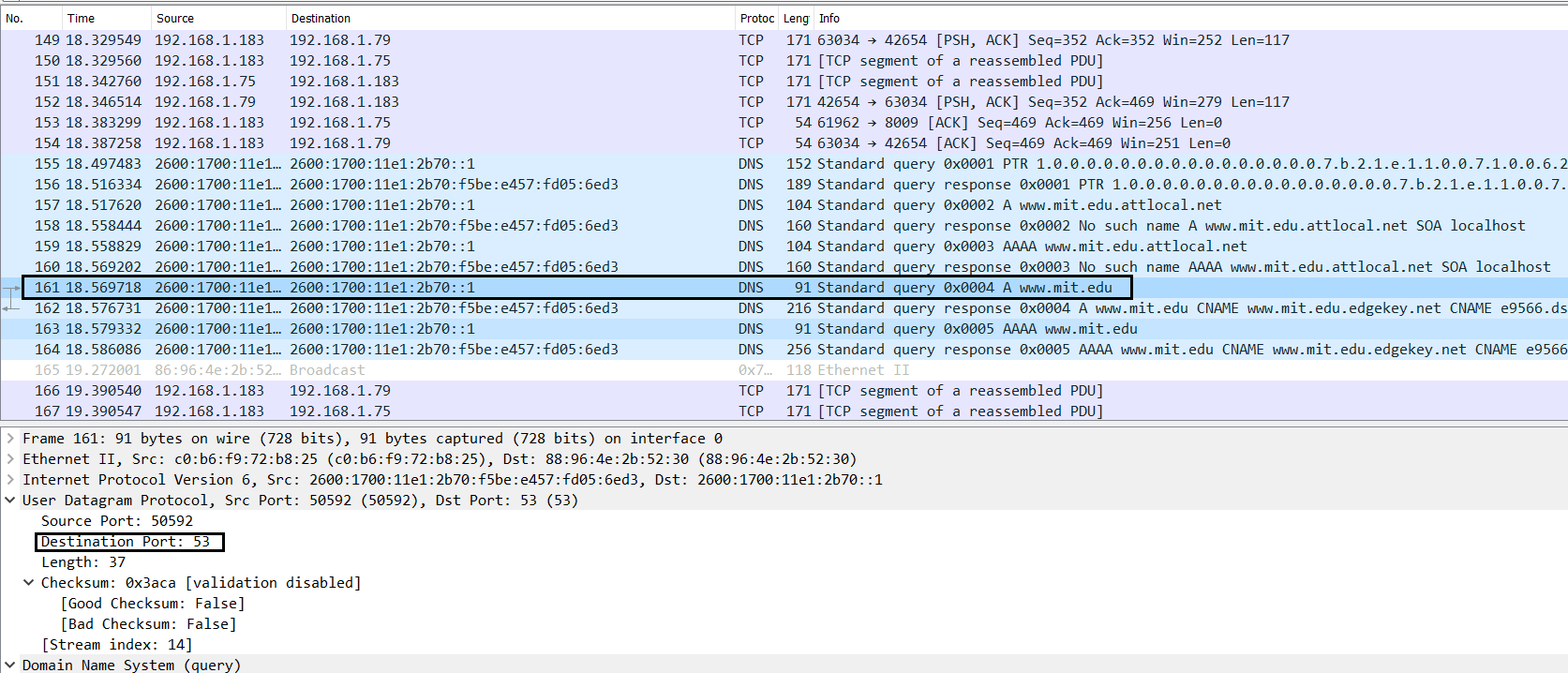
**ANSWER**: **No, no new queries are issued.**

Nslookup on [www.mit.edu](http://www.mit.edu)

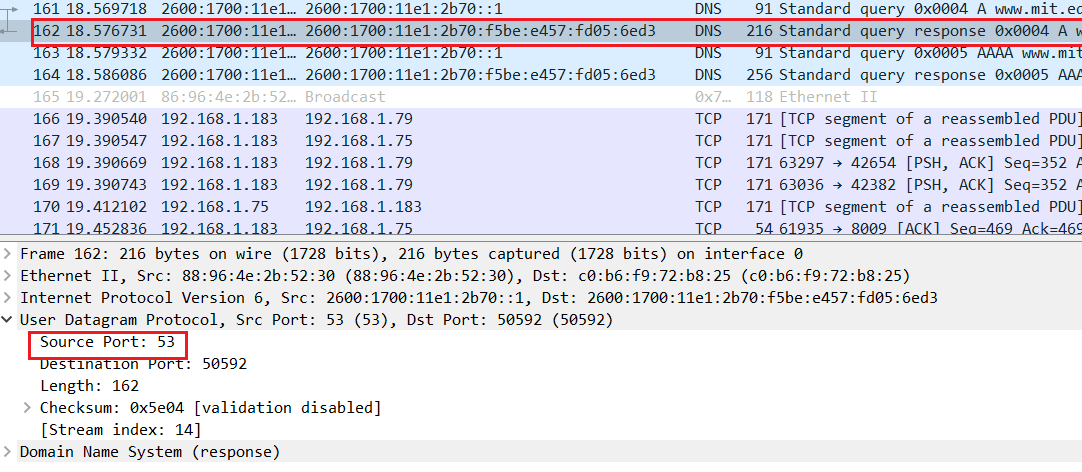


11. What is the destination port for the DNS query message? What is the source port of DNS response message?

**ANSWER**: We are supposed to pay attention to the last query fow [www.mit.edu](http://www.mit.edu) according to the lab manual. I have 4 queries,where last 2 are similar. I am paying attention to the third query. **Destination port for DNS query is 53 and Source port for DNS response is 53.**

**

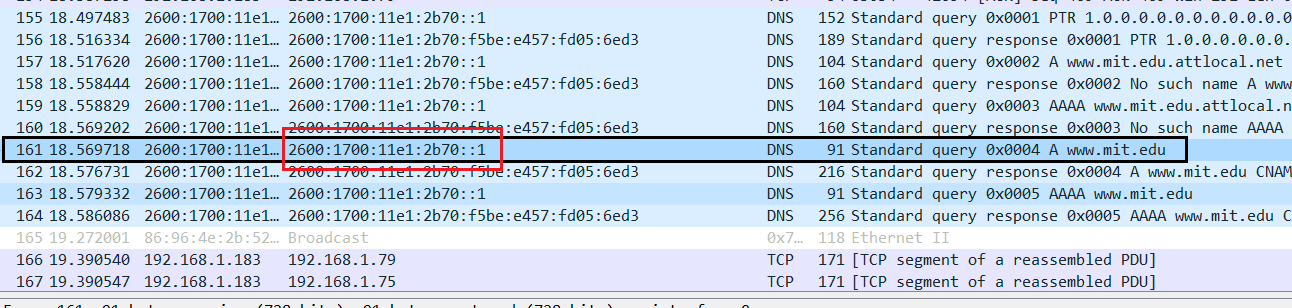
*Screenshot for DNS Query Message*

**

*Screenshot for DNS Response Message*

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

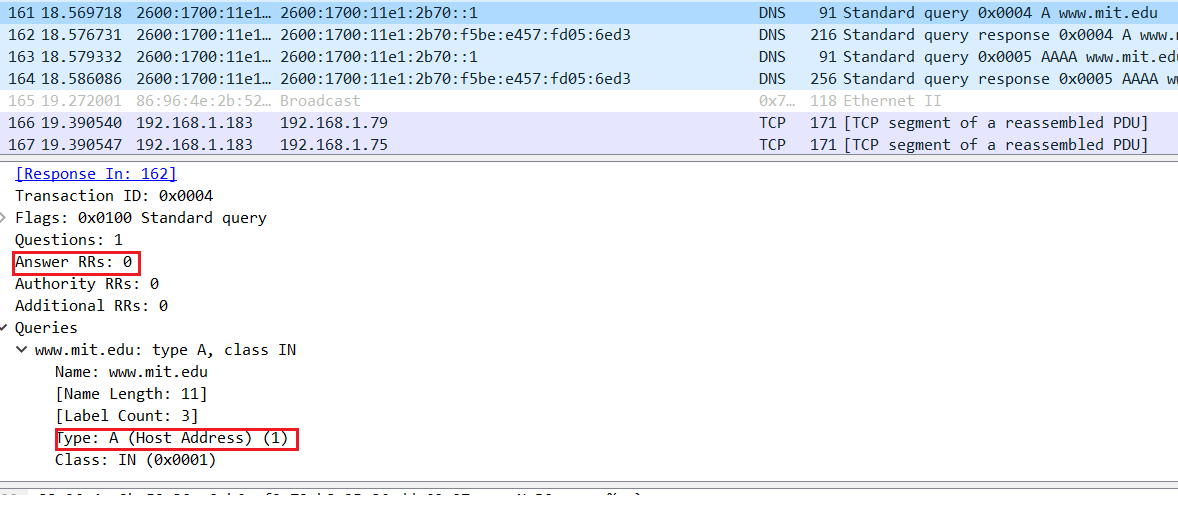
**ANSWER:** It is sent to **2600:1700:11e1:2b70::1**(destination of query message),which is the IP address of one of my local DNS servers. The screenshot of ipconfig is already provided in the previous answers.

******

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

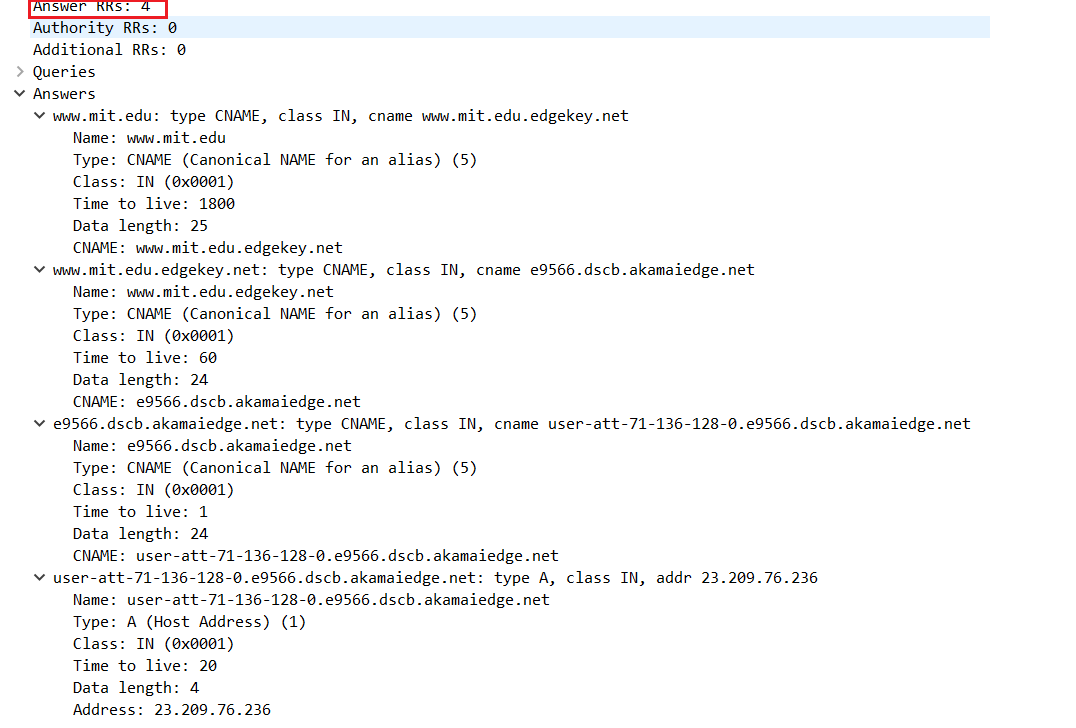
**ANSWER**:

Type: A standard query (Host address). The query message does not contain any answers.



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

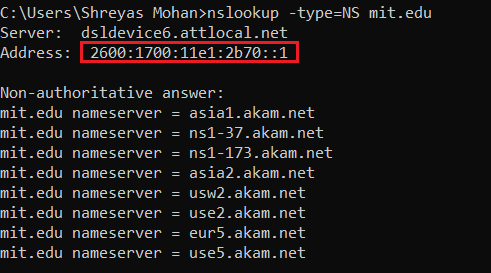
Answer: **Four answers** are provided. The answers contains **name of the host, type of the address, class, the TTL, data length and the IP address.**



15. Provide a screenshot.

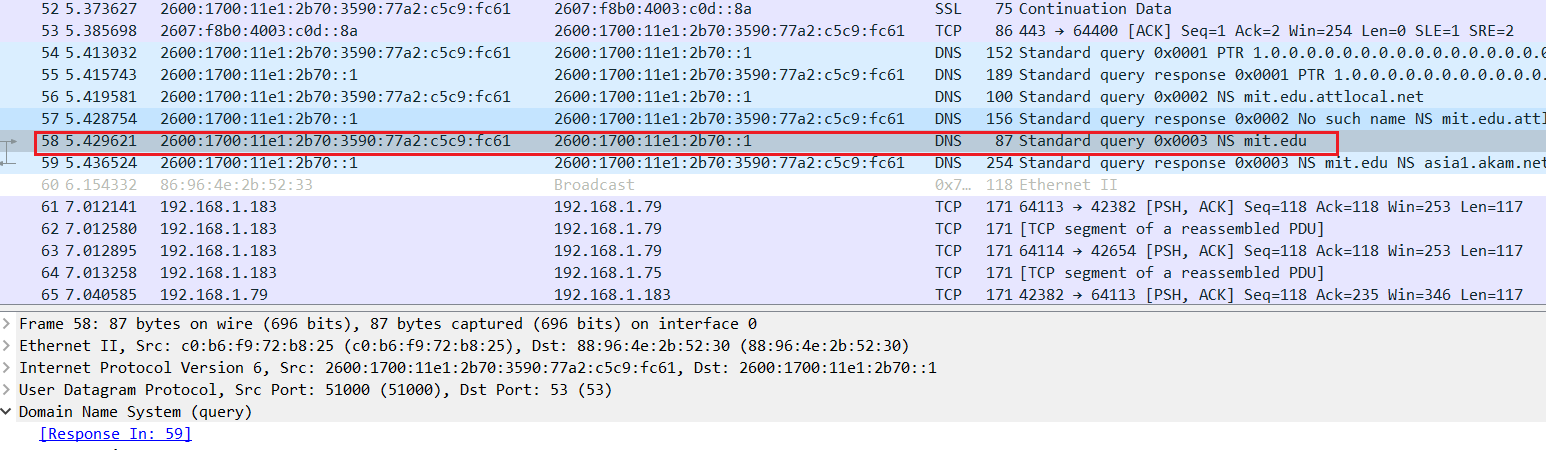
I have already provided it.

------------------------------------------------------------------------------------------------------------------------------



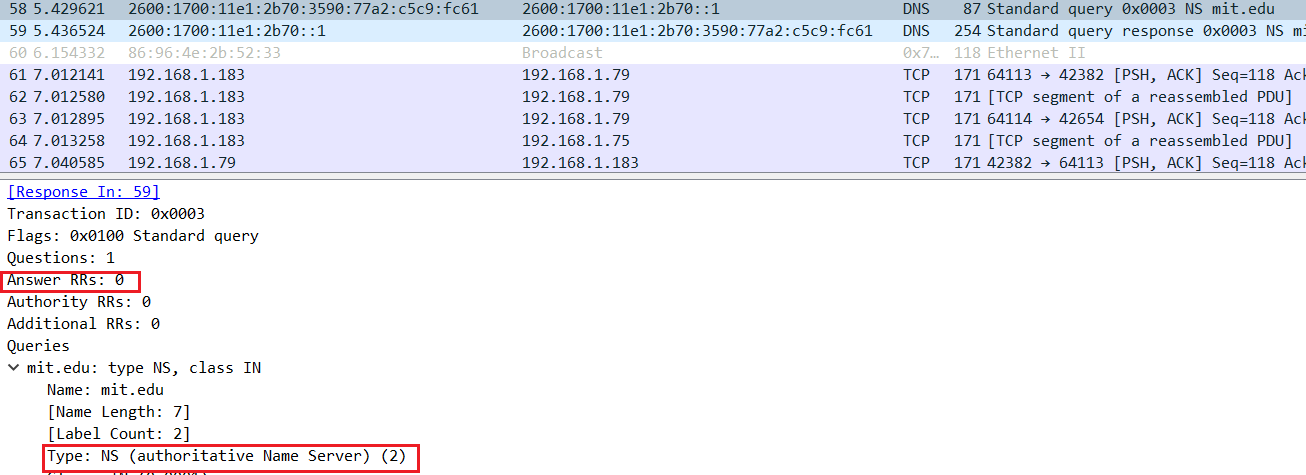
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

**ANSWER**: It is sent to **2600:1700:11e1:2b70::1**(destination of query message),which matches the IP address of my local DNS server (already shown in the screenshot of ipconfig -all).



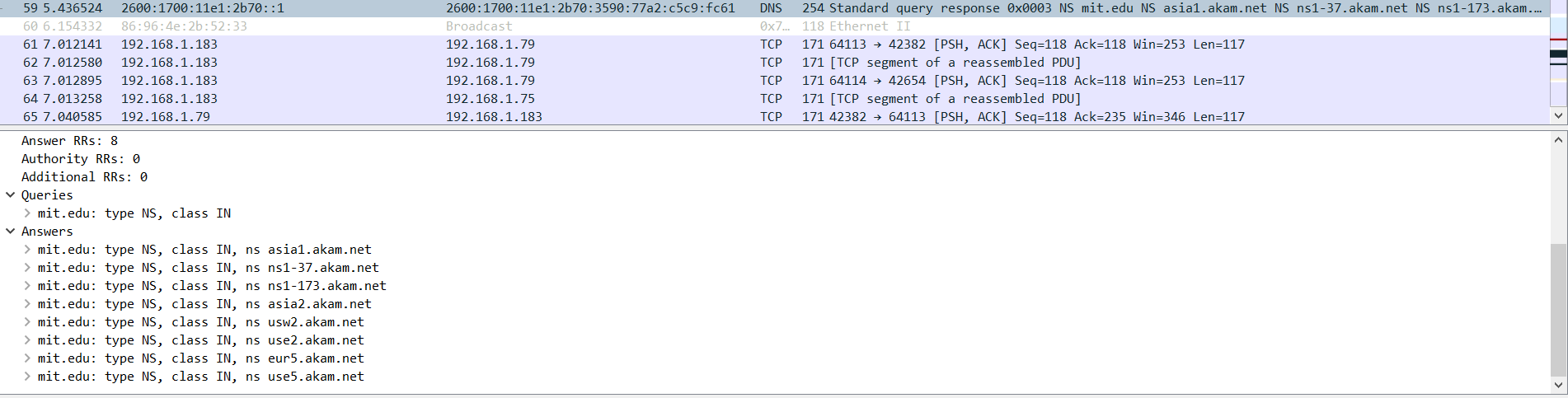
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**ANSWER**: This is a **standard type NS query** and it contains no answers.



18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers?

**ANSWER:** The response message **does not contain any nameservers**. If they contained, it would be under additional records right under answers, but there is nothing below answers.

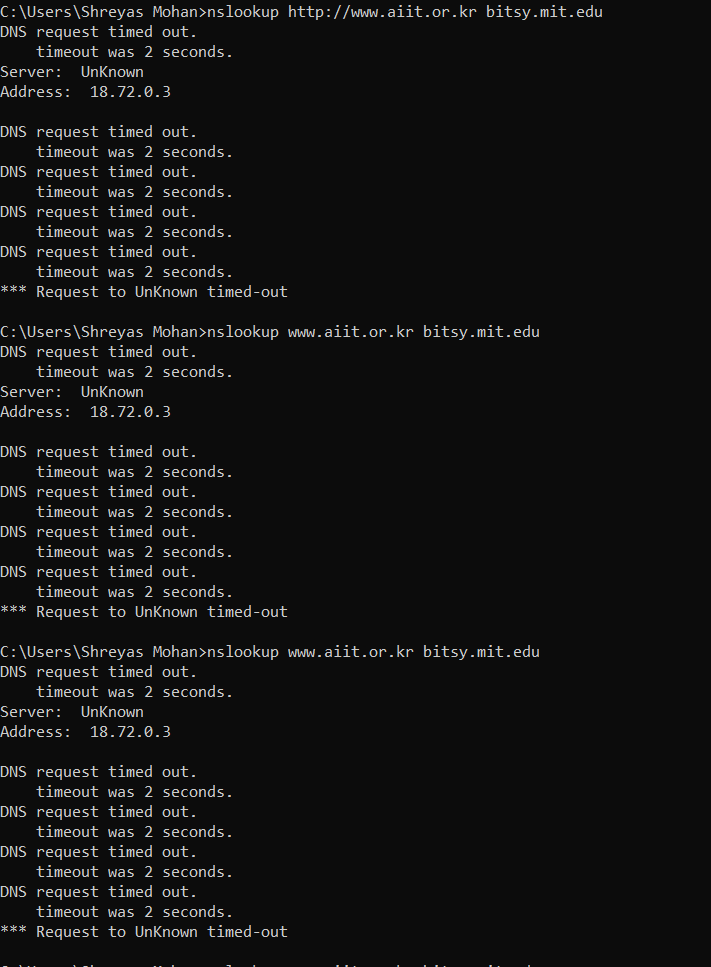


19. Provide a screenshot.

Screenshots provided in the answers of each question*.*

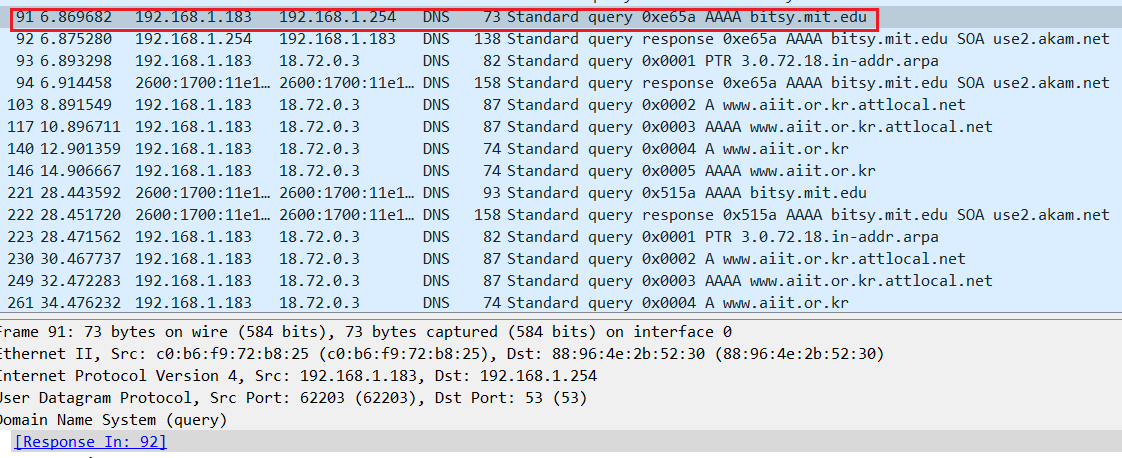
Now repeat the previous experiment, but instead issue the command:

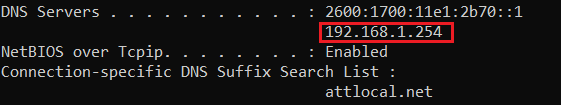
nslookup www.aiit.or.kr bitsy.mit.edu



20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

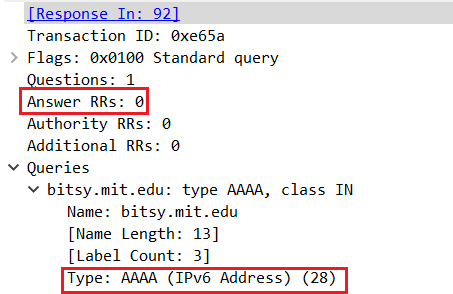
**ANSWER** I tried doing the nslookup 3 times and all of them timed out. The query is sent to **192.168.1.254** . Yes, it is same as of default local DNS server.





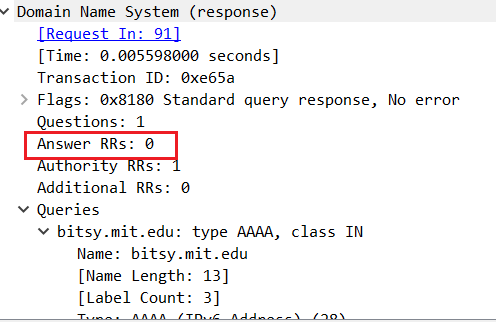
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**ANSWER**: This is a **IPv6 type AAAA query** and it contains no answers.



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

ANSWER: The response message does not contain any answers.



23. Provide a screenshot.

Screenshots are provided in the answers of each question