**EE450**

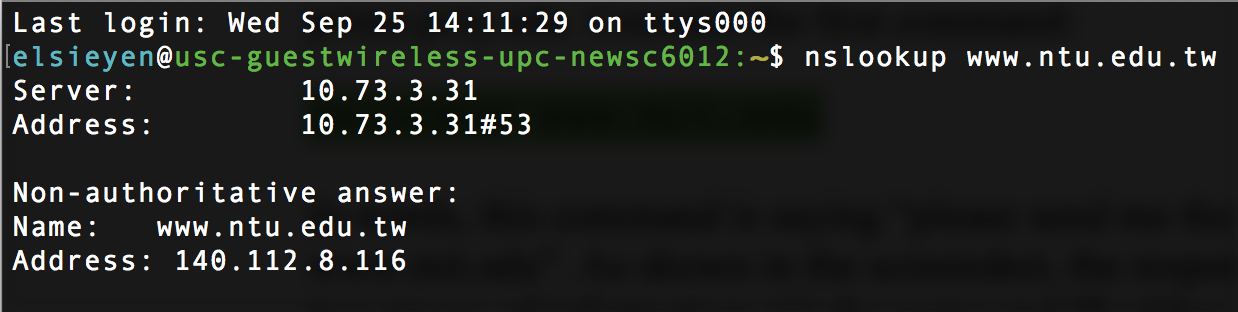
**Lab2**

**Session 2**

**Yin-Hsia Yen**

Q1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?

The IP address of [www.ntu.edu.tw](http://www.ntu.edu.tw) is 140.112.8.116



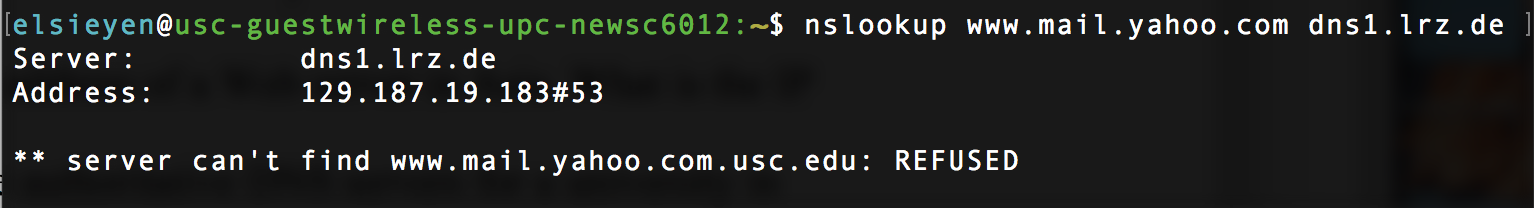
Q2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

The authoritative DNS server is dns1.lrz.de

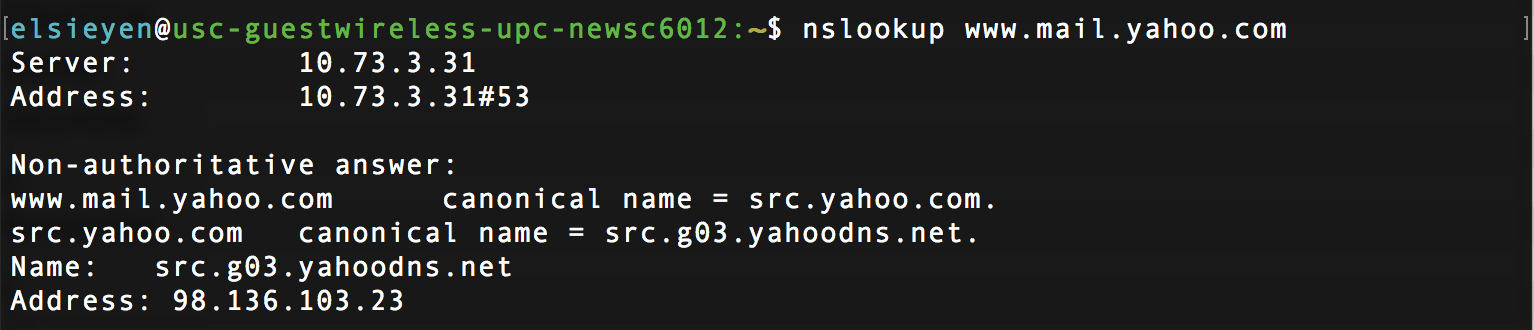


Q3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Cannot find the IP address through the authoritative DNS server (reference from Q2)

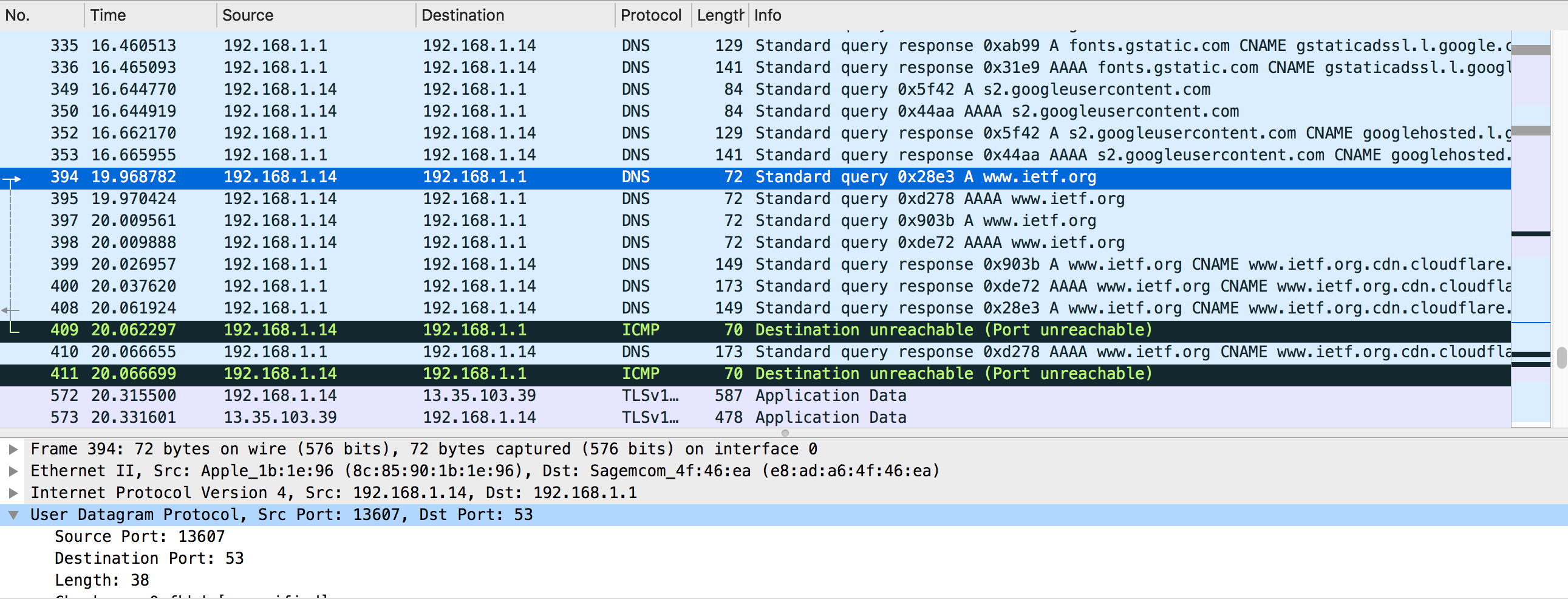


Using default DNS server instead, the IP address is 98.136.103.23



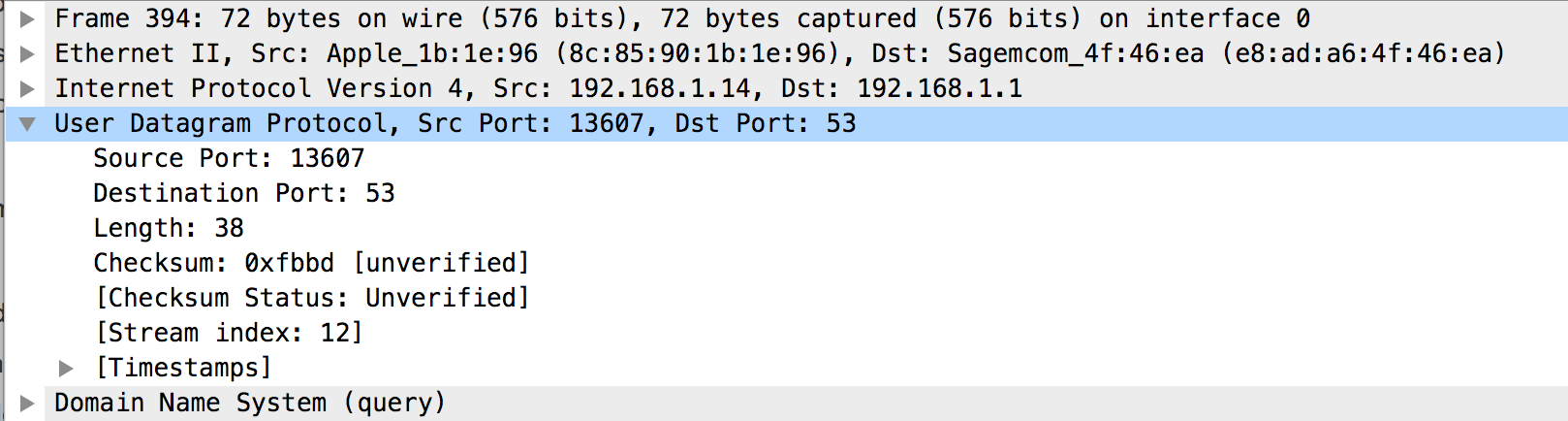
Q4. Locate the DNS query and response messages. Are they sent over UDP or TCP?

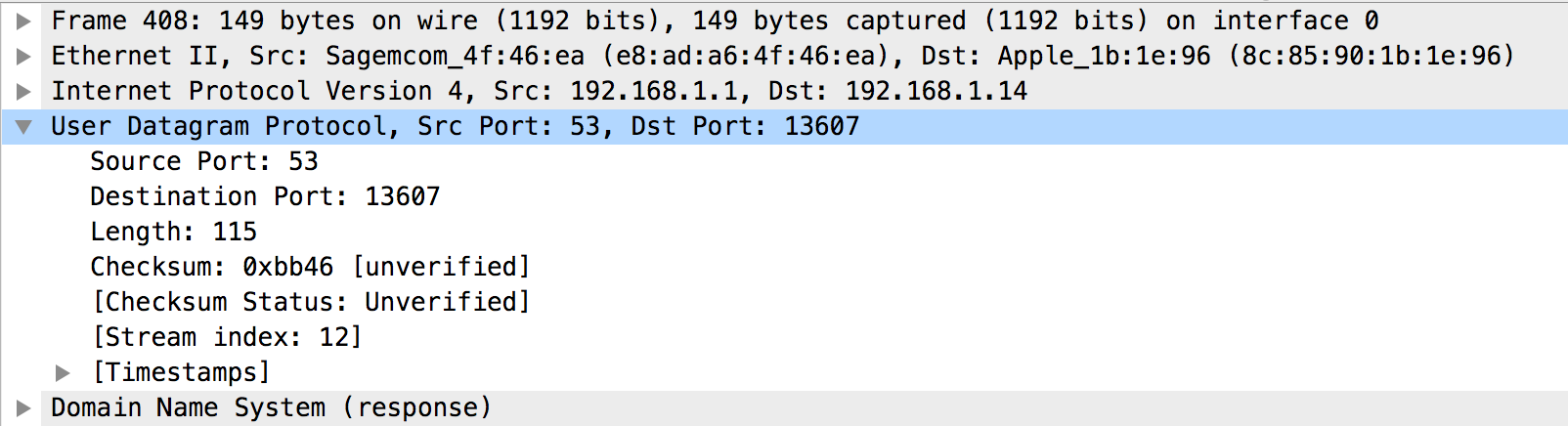
Both DNS query and response messages are sent through UDP



Q5. What is the destination port for the DNS query message? What is the source port of DNS response message?

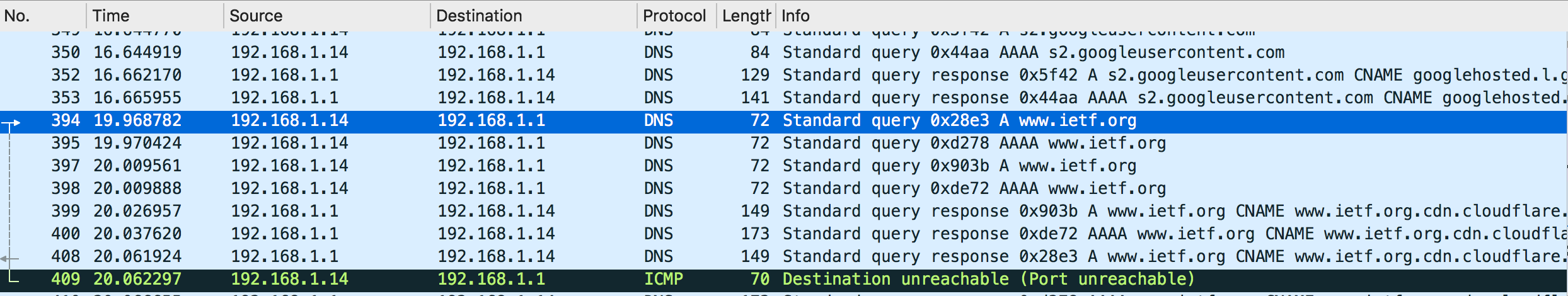
The destination port for the DNS query message is 53. And the source port of DNS response message is 53 as well.





Q6. 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?

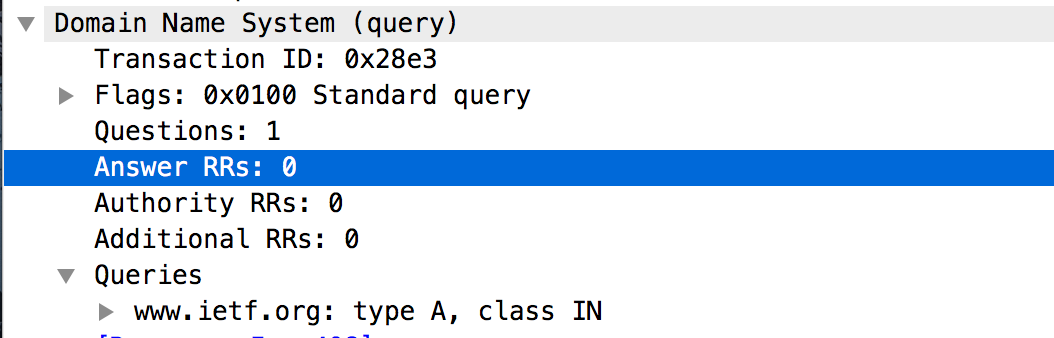
Both are 192.168.1.1





Q7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

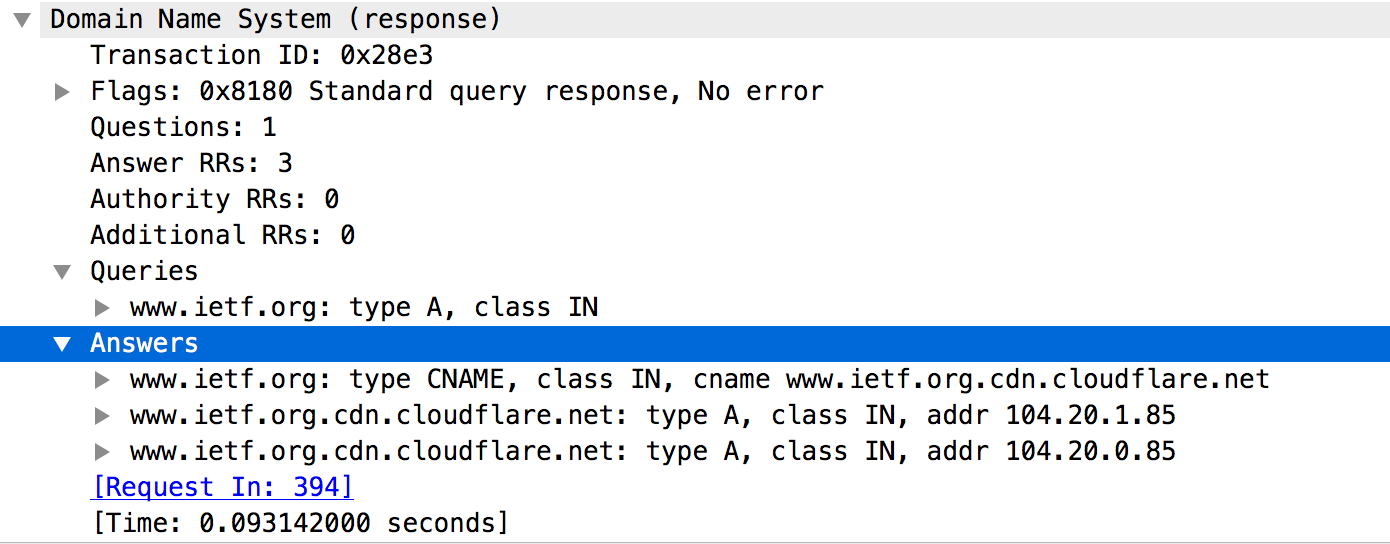
Type A, and the query message doesn’t contain any answers.



Q8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

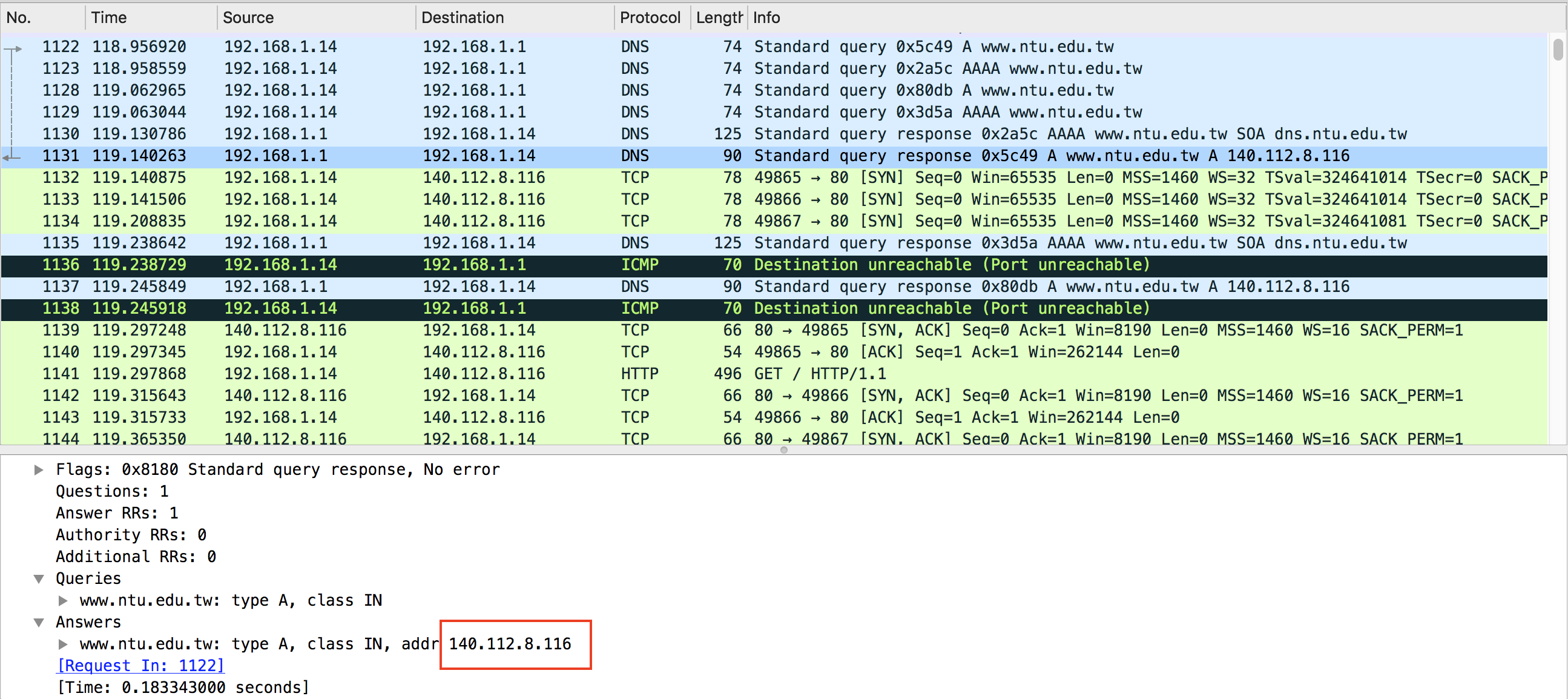
There are three answers in the DNS response messages

One answer has type = CNAME (Canonical domain name for and alias); others has type = A (32-Bit IP Address of host or domain)



Q9. 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?

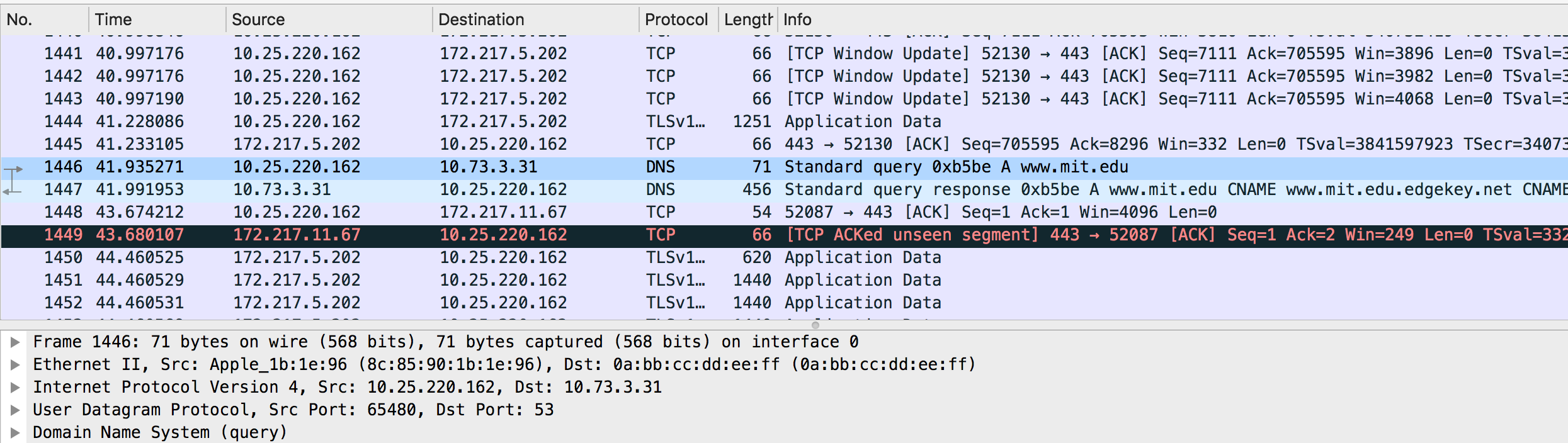
Yes. The IP address is 140.112.8.116

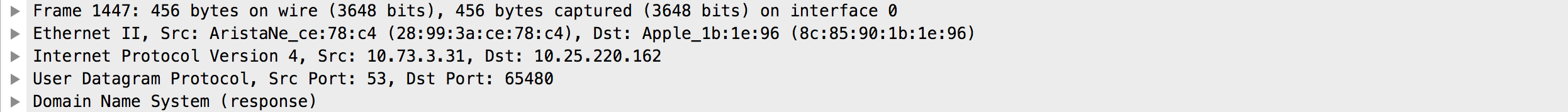


Q10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?  No

Q11. What is the destination port for the DNS query message? What is the source port of DNS response message?

The destination port for the DNS query message is 53. And the source port of DNS response message is 53 as well.





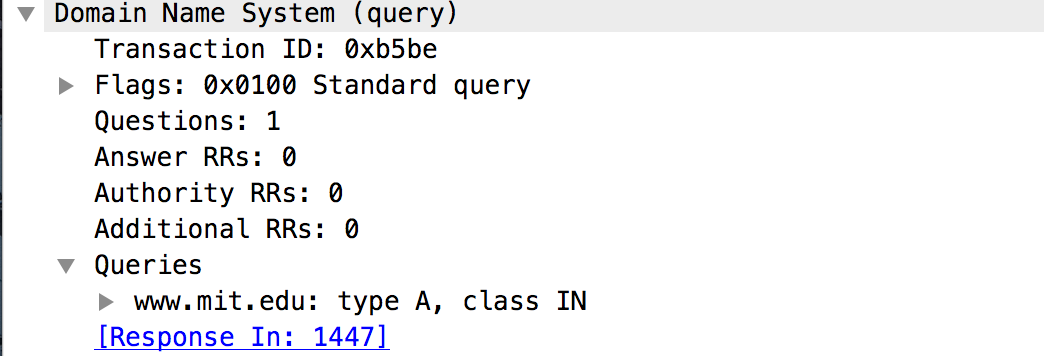
Q12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

(Reference picture from Q11)

The destination IP address of DNS query message is 10.73.3.31 which is the IP address of my local DNS server as well.

Q13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a type A query (32-Bit IP Address of host or domain) and it does not contain any answer.

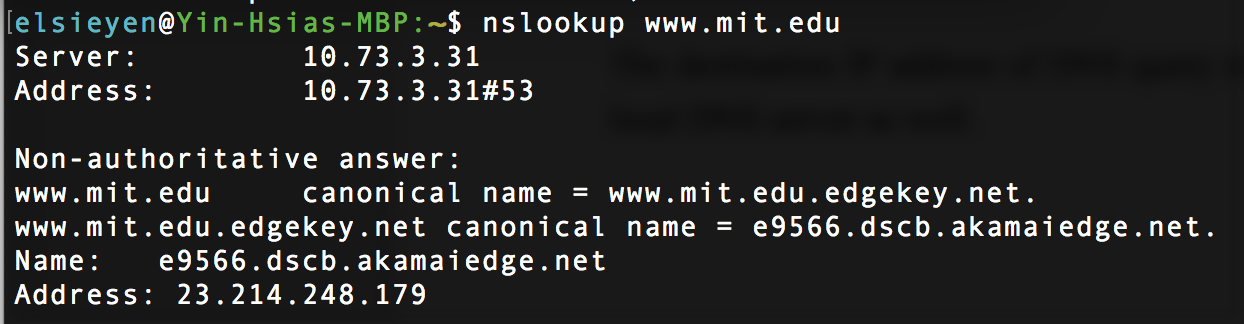


Q14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There are three answers in this DNS response message. Two answers with type = CNAME (Canonical domain name for and alias) and one with type = A (32-Bit IP Address of host or domain)

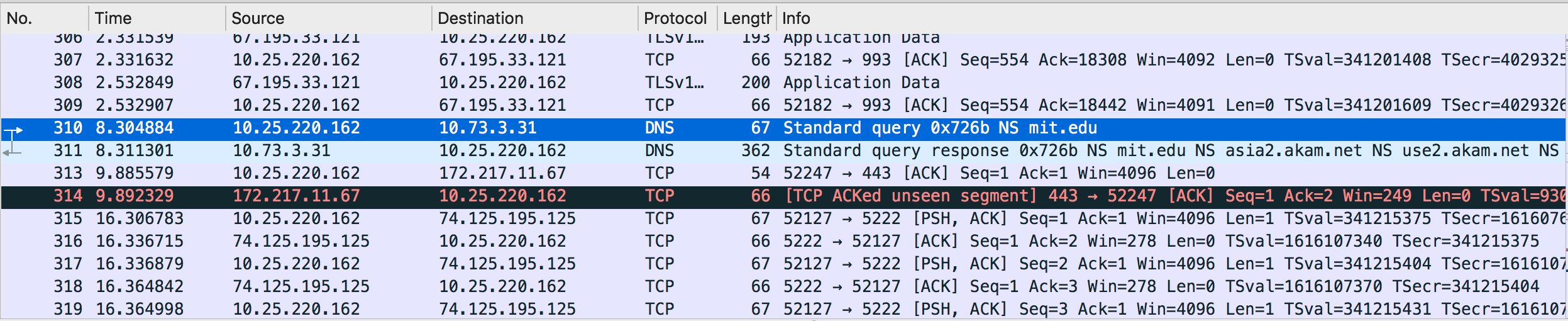


Q15. Provide a screenshot



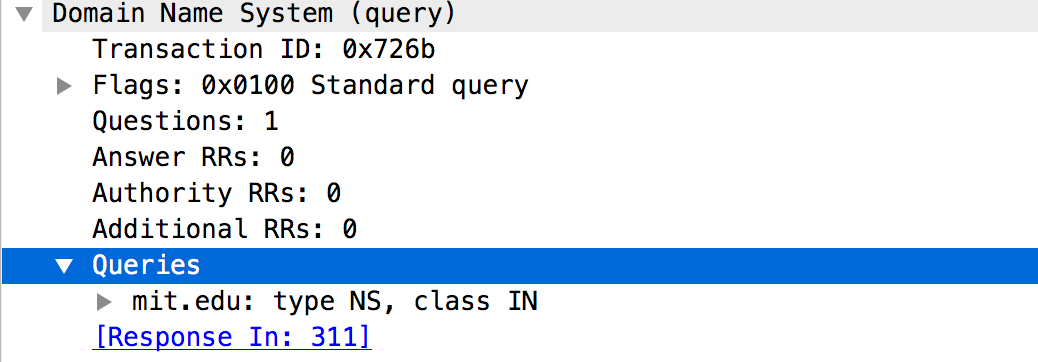
Q16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The destination IP address of DNS query message is 10.73.3.31 which is the IP address of my local DNS server as well.



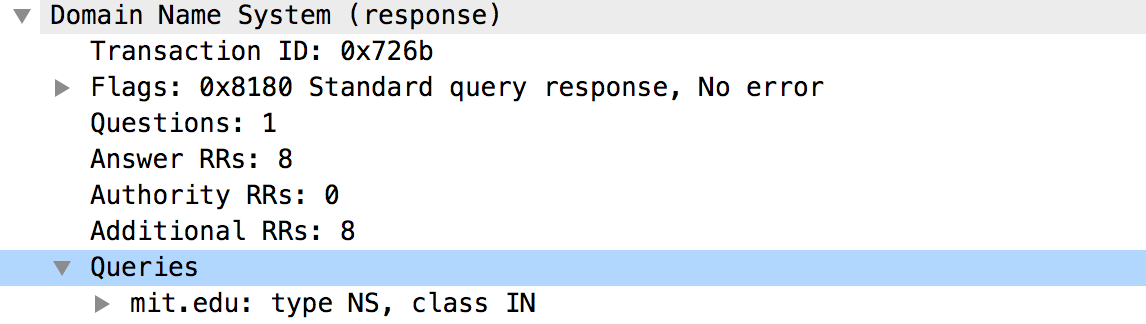
Q17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

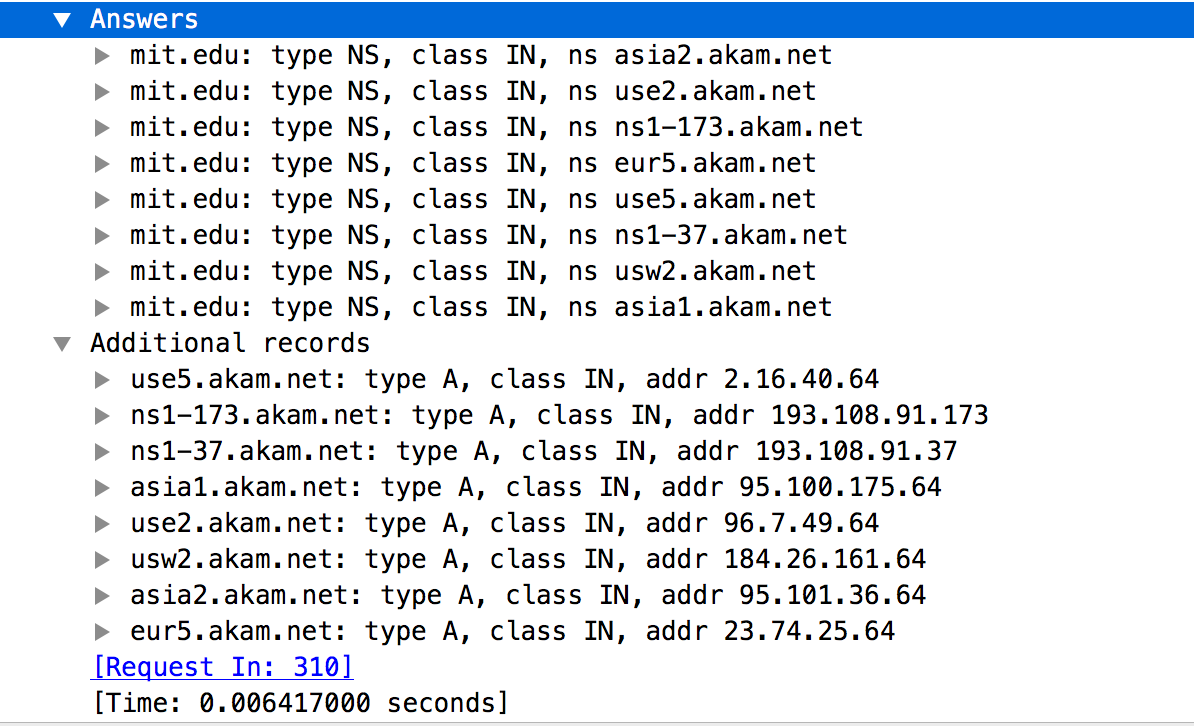
The DNS query is type NS (Name server record) and it does not contain any answer.



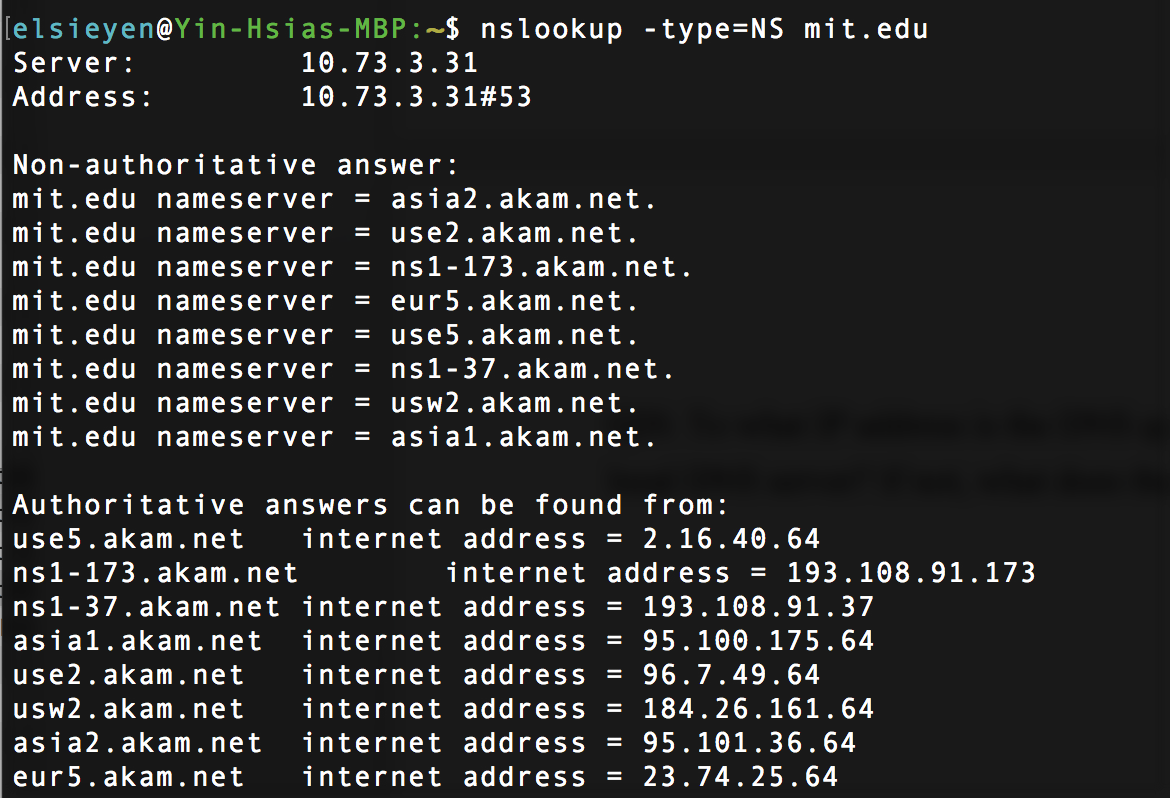
Q18. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name severs?

The DNS response message contains 8 answers and it also provide the IP address of the MIT name servers.



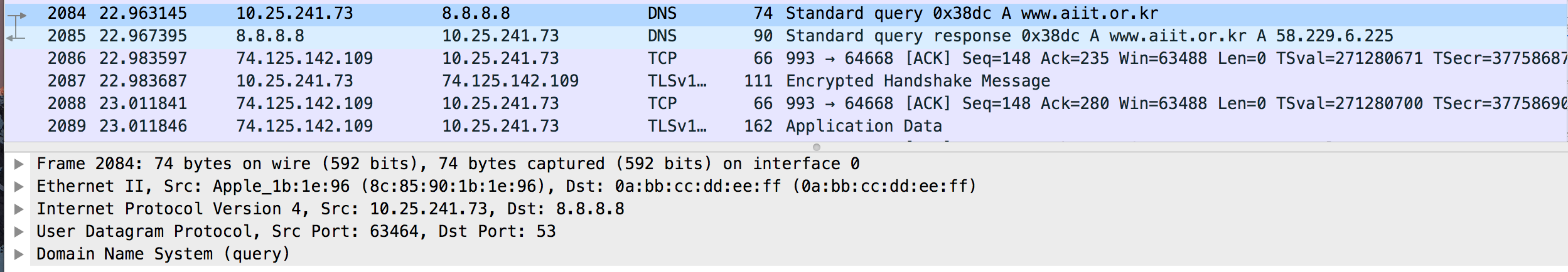


Q19. Provide a screenshot



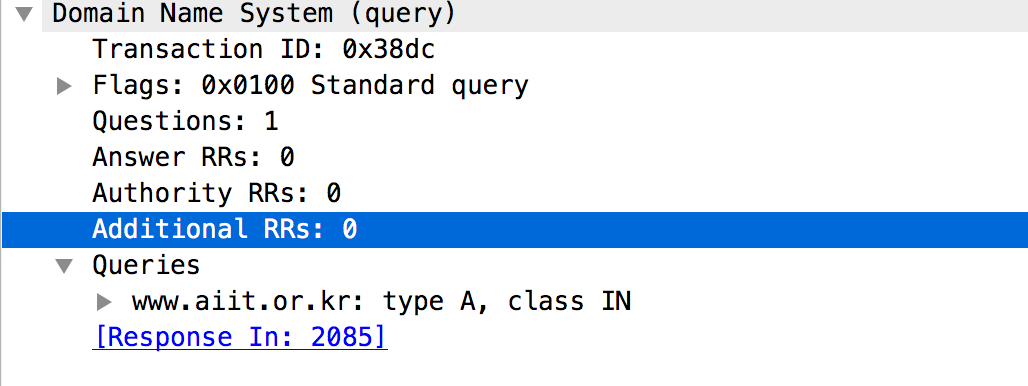
Q20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

The DNS query message is sent to Google Public DNS server 8.8.8.8 to get the IP address of [www.aiit.or.kr](http://www.aiit.or.kr)



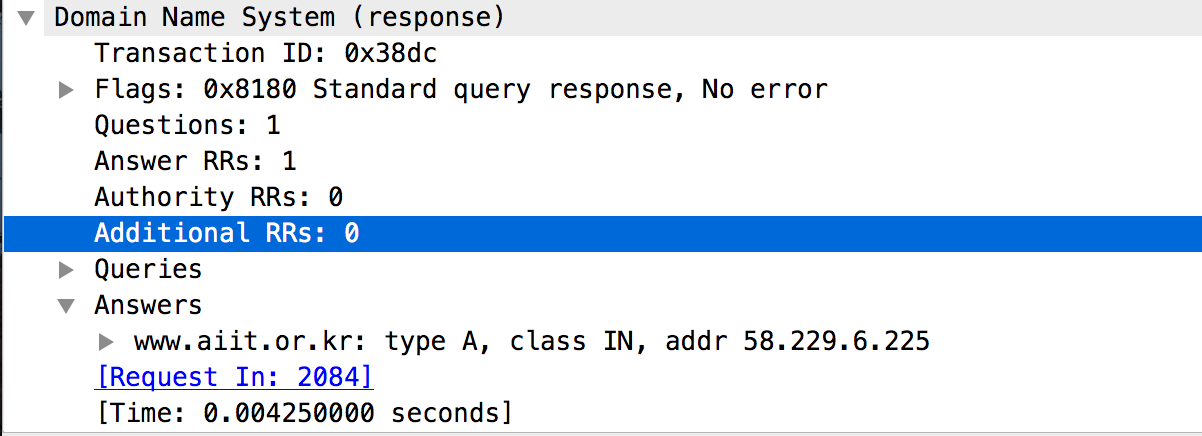
Q21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

It is a type A query and no answer is included.



Q22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

One answer is included and it returns the IP address of [www.aiit.or.kr](http://www.aiit.or.kr) (58.229.6.225)



Q23. Provide a screenshot

