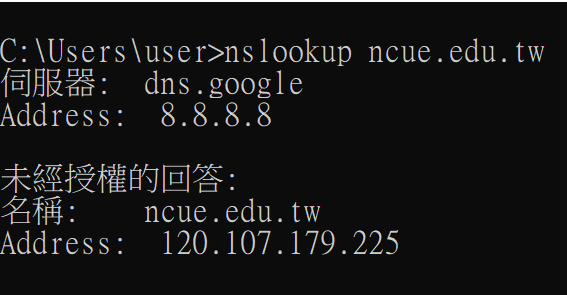
DNS Homework

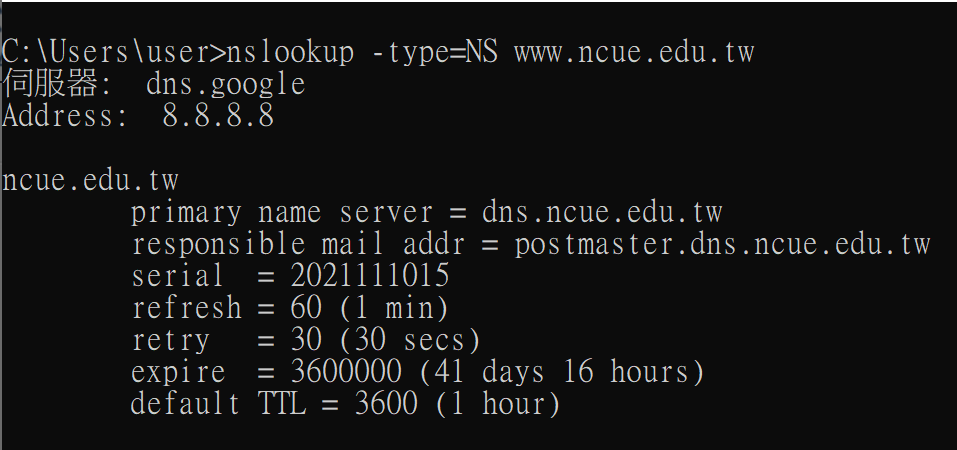
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Ans : 120.107.179.225.



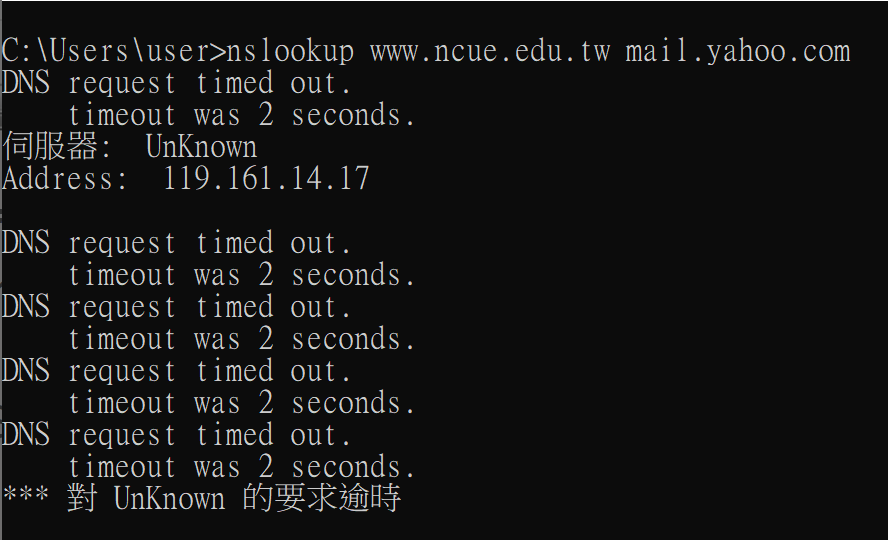
1. Run nslookup to determine the authoritative DNS servers for a university in Europe.

Ans : dns.ncue.edu.tw.



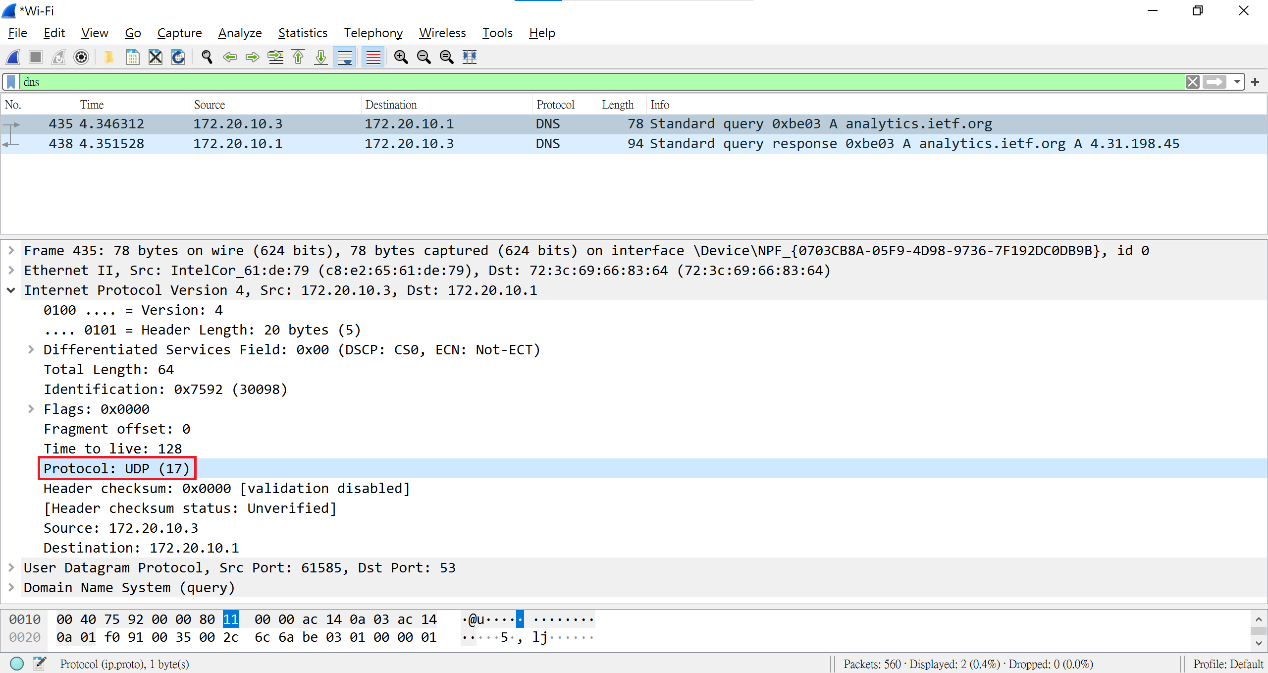
1. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Ans : The IP addreess for the DNS server if queried for the Yahoo! mail server IP address is 119.161.14.17.



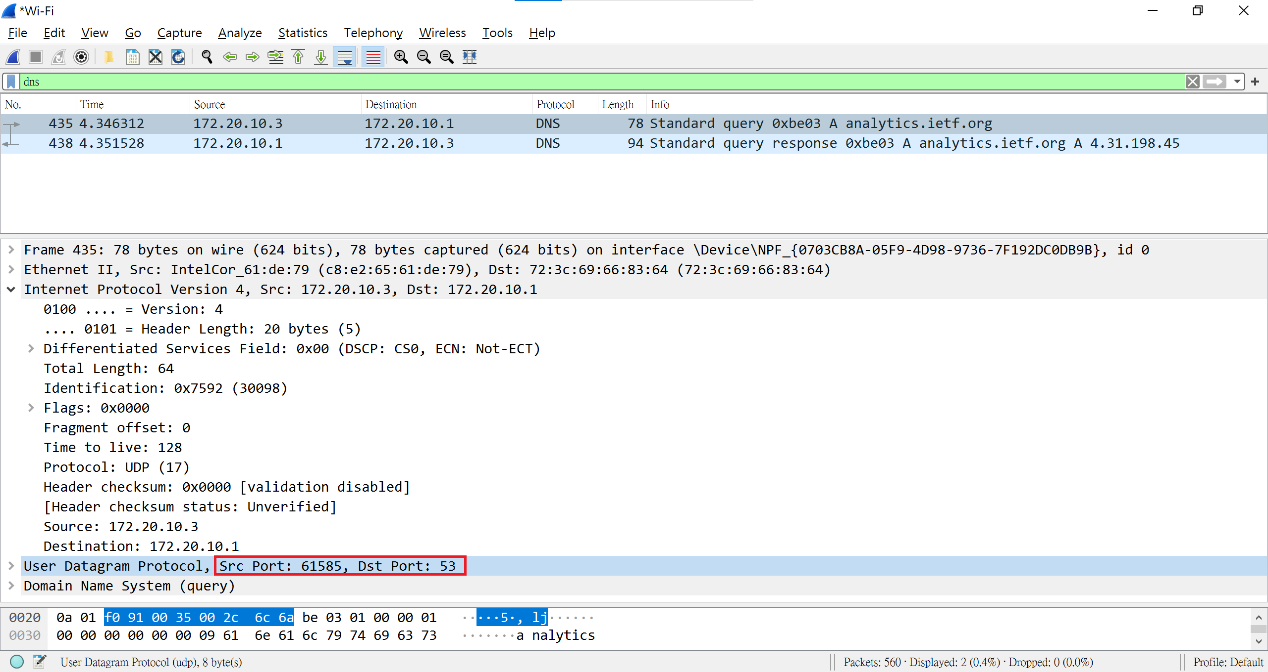
1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans : UDP.



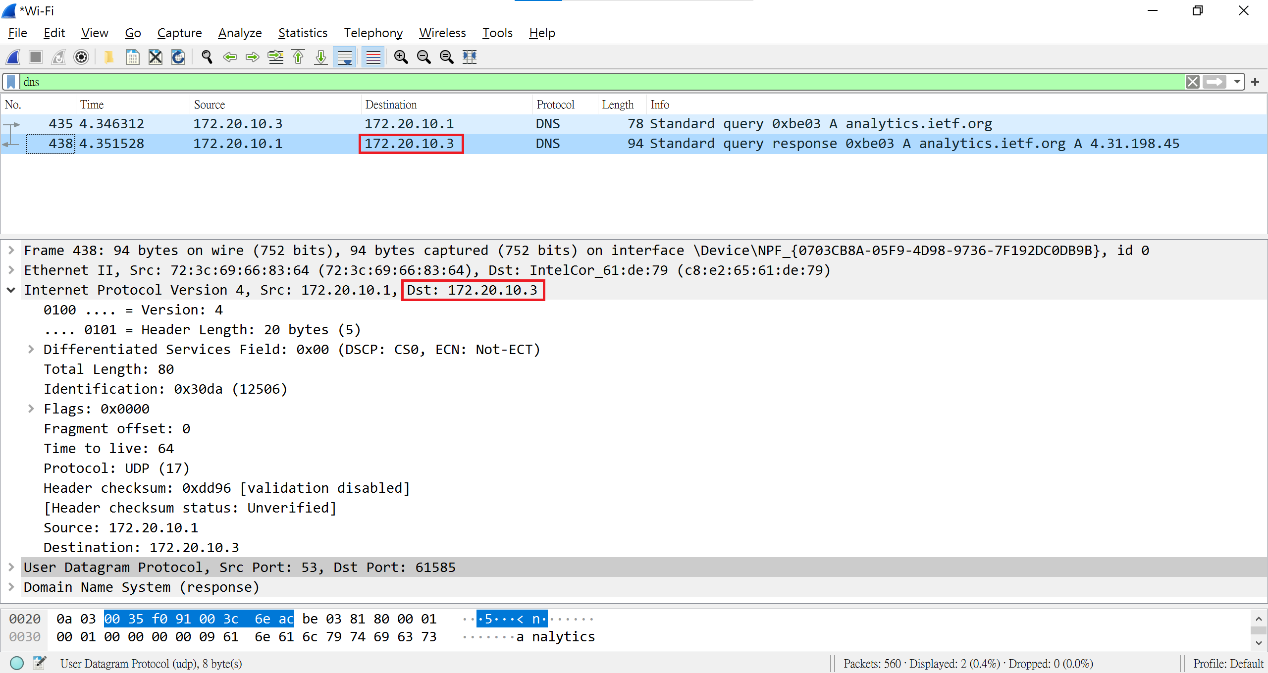
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans : Source port: 61585, Destination port: 53.



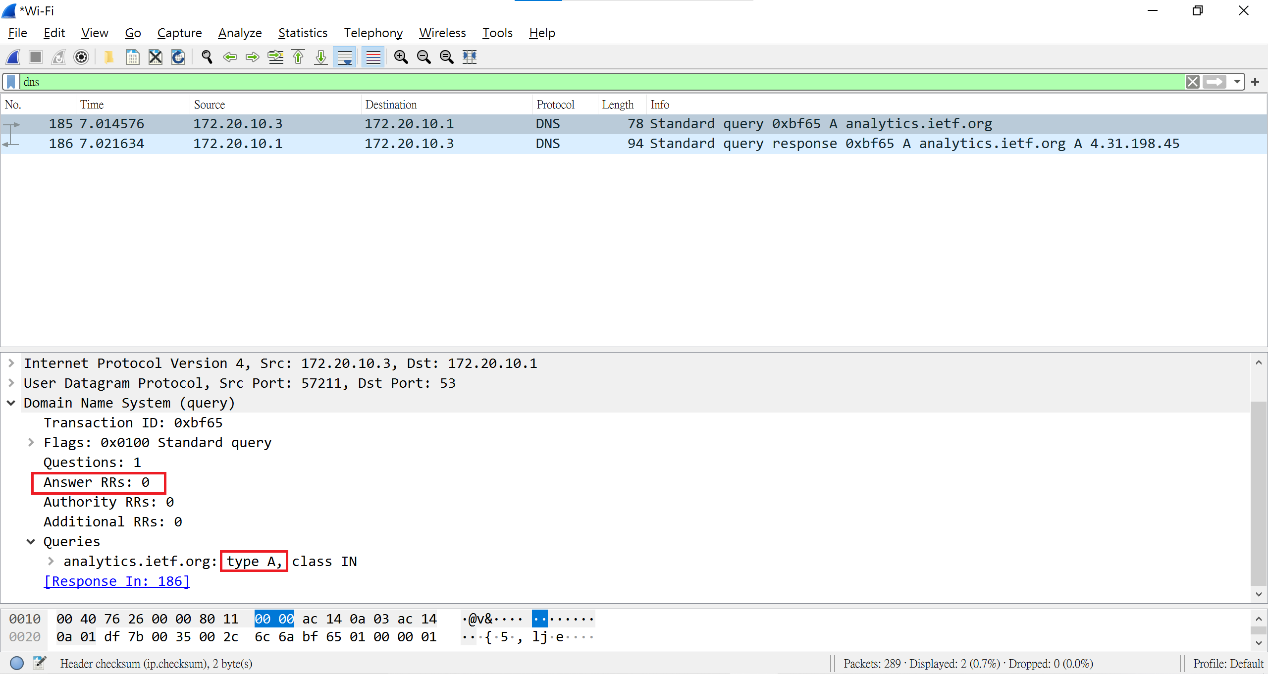
1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans : First IP address is 172.20.10.3 the other is 172.20.10.1.



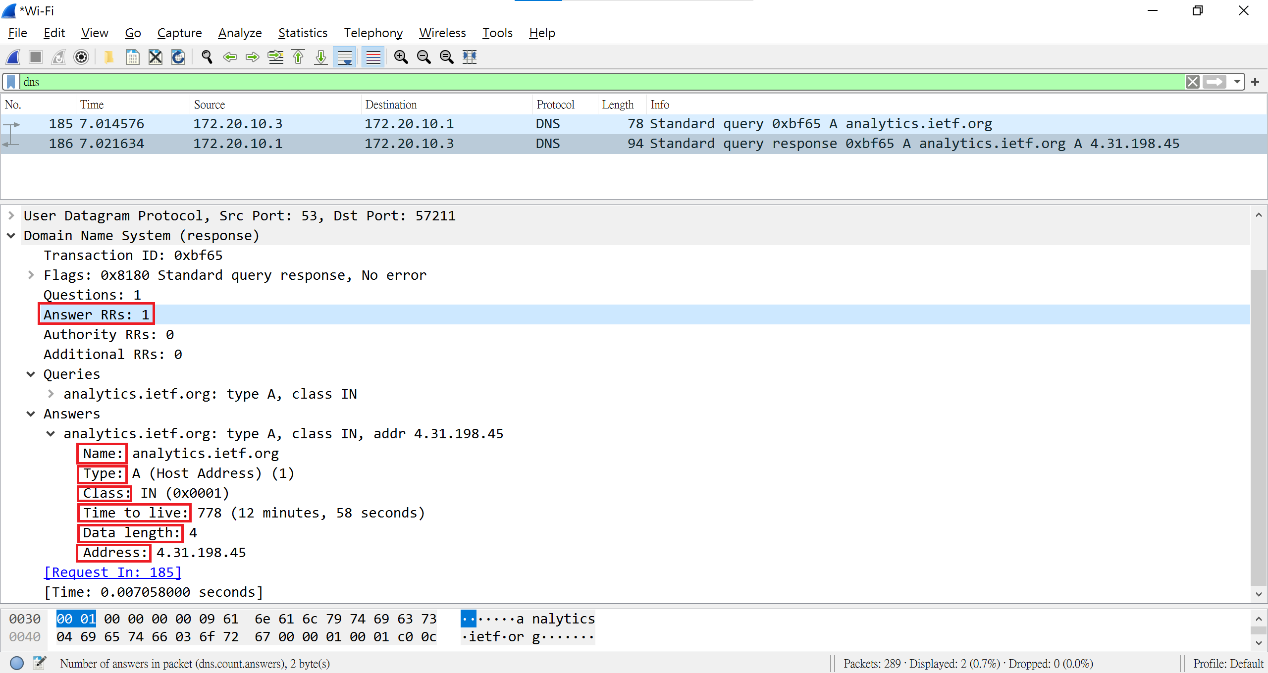
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans : Type A, no answers.



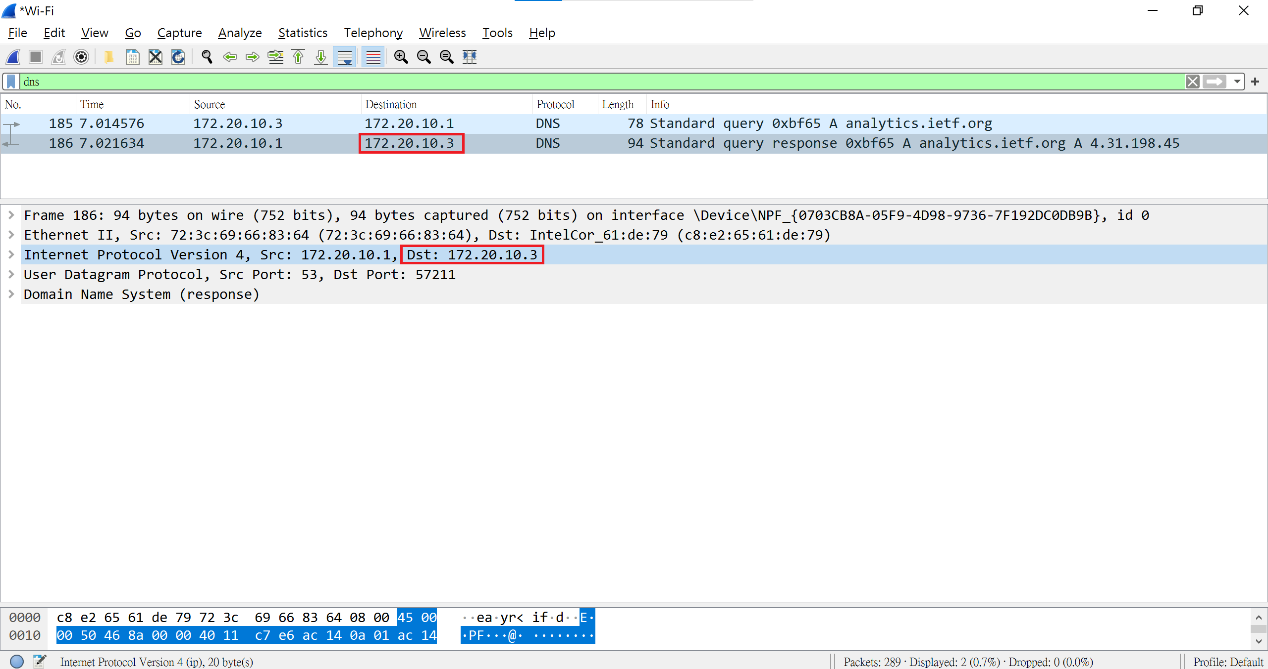
1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans : 1, Contain: Name, Type, Class, TTL(Time To Live) , Data Length , Address.



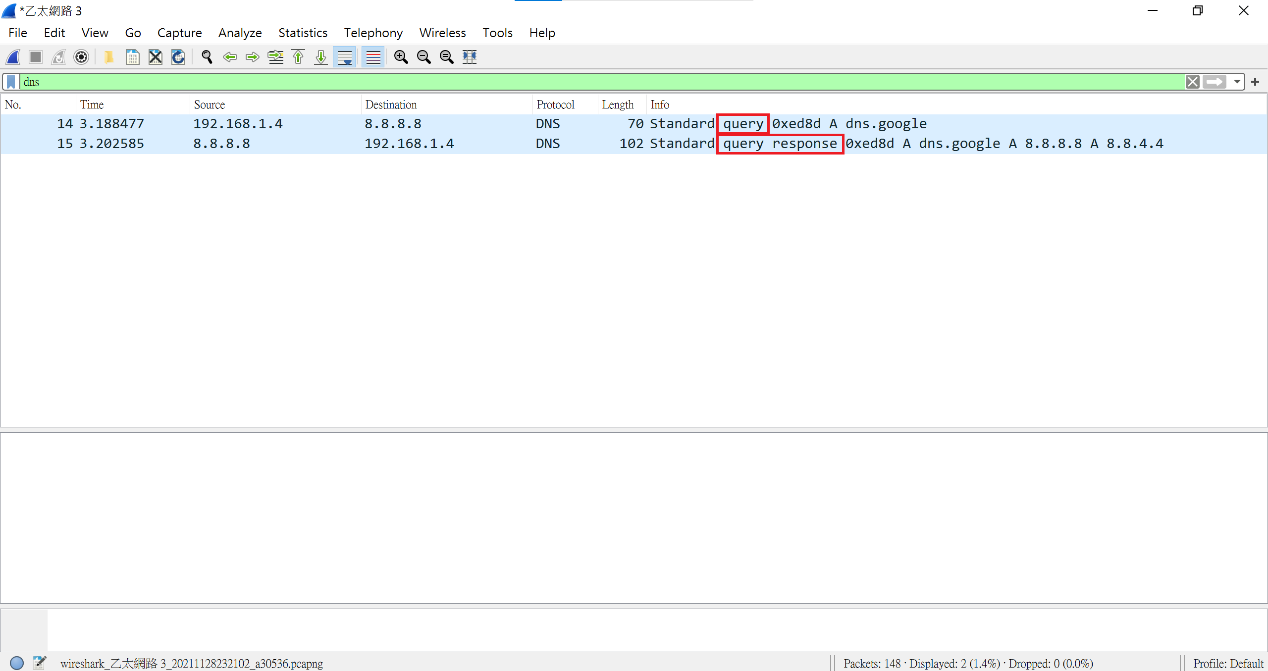
1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans : 172.20.10.3.



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

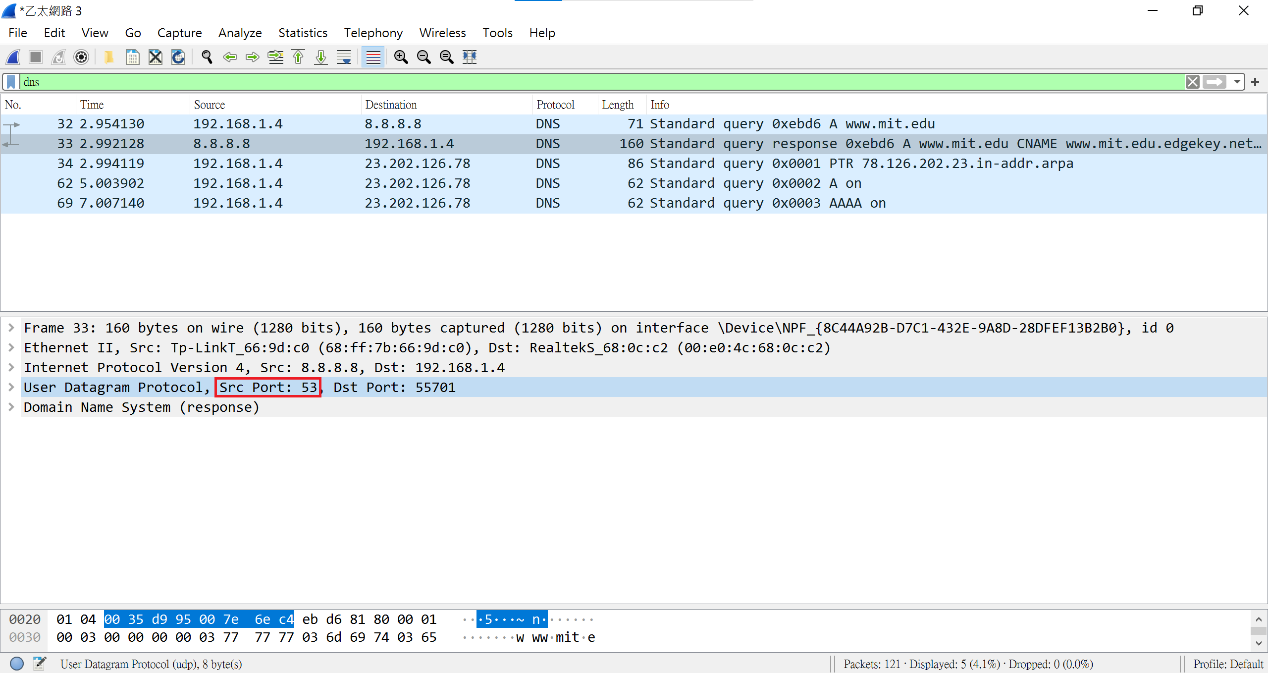
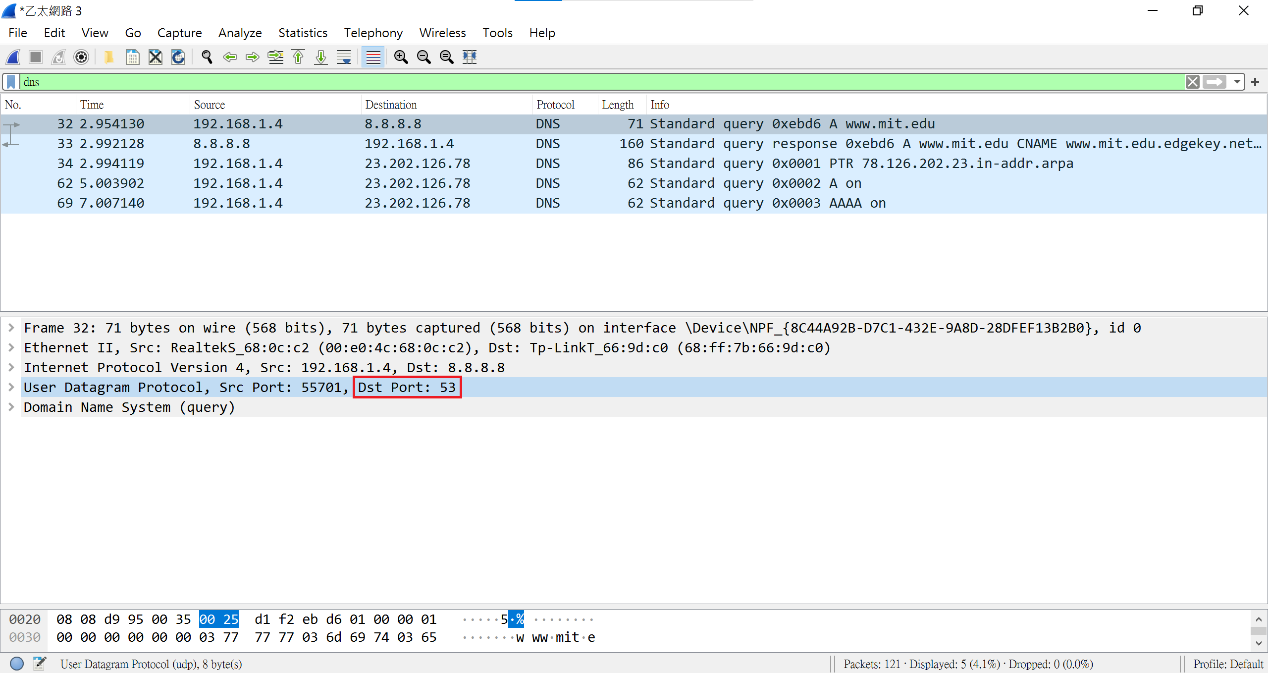
Ans : No, only one queries. (注:此處我有換網路故DNS server不同)



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

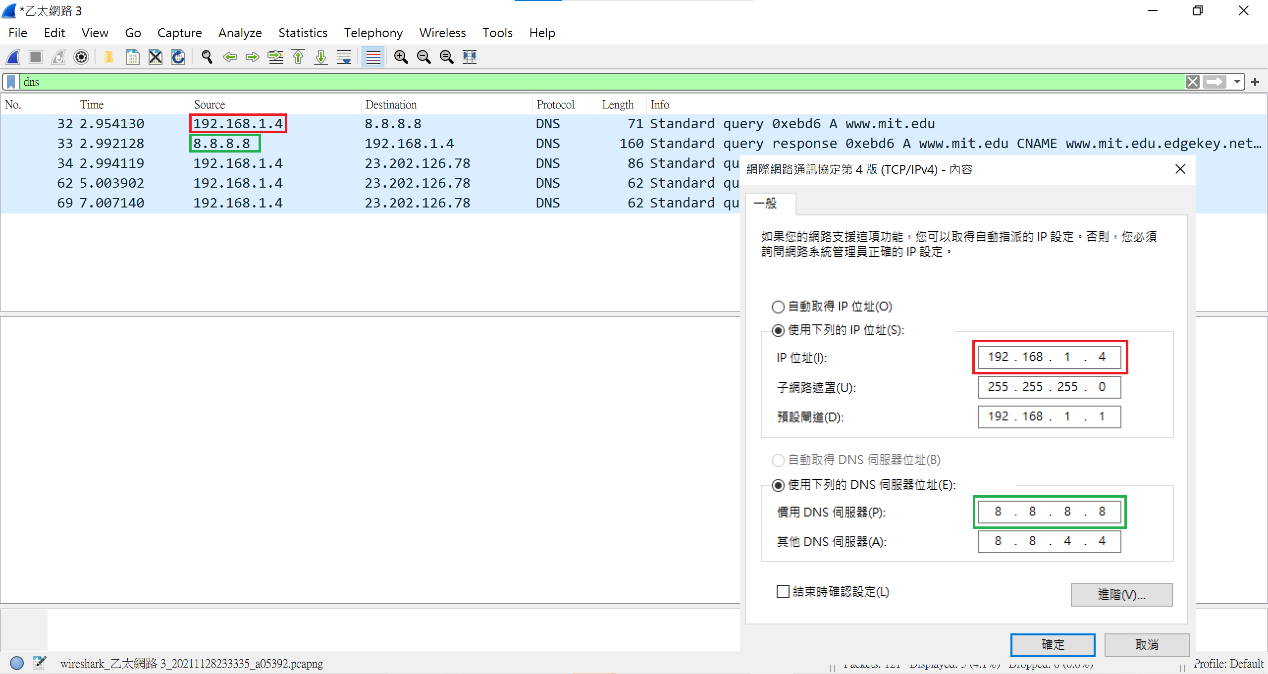
Ans : Destination port “53” for the DNS query message.

Source port “53” of DNS response message.



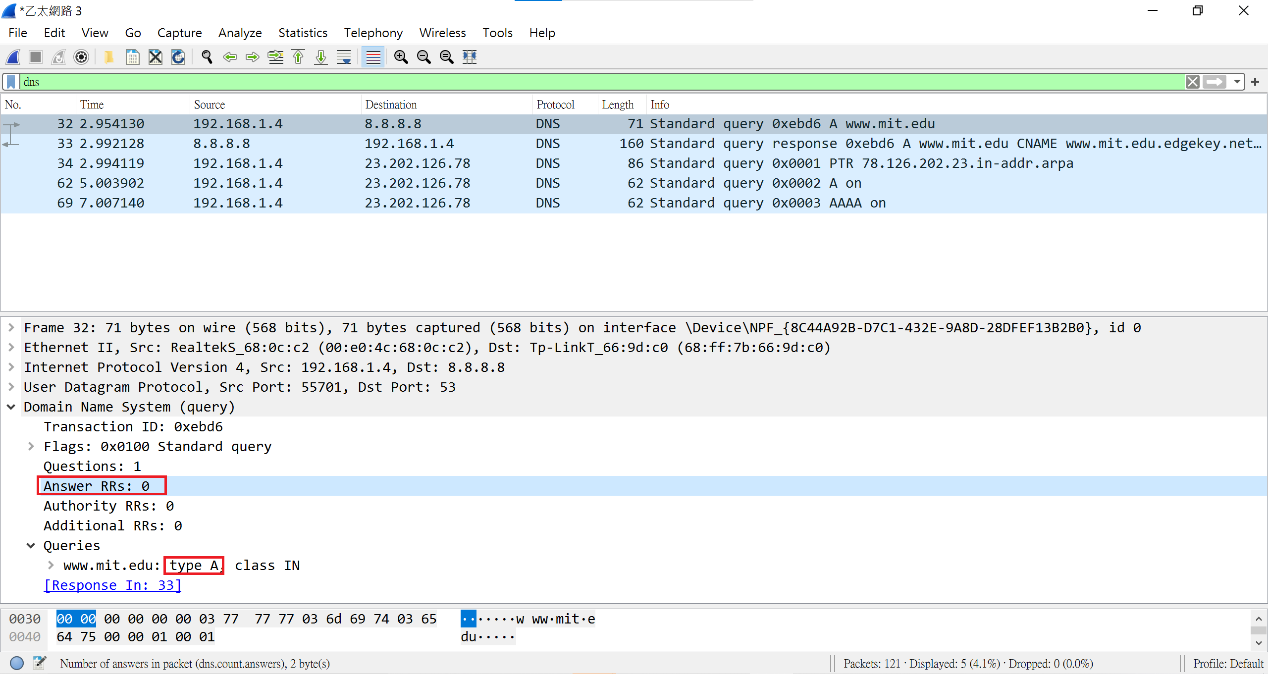
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans : 192.168.1.4, yes.



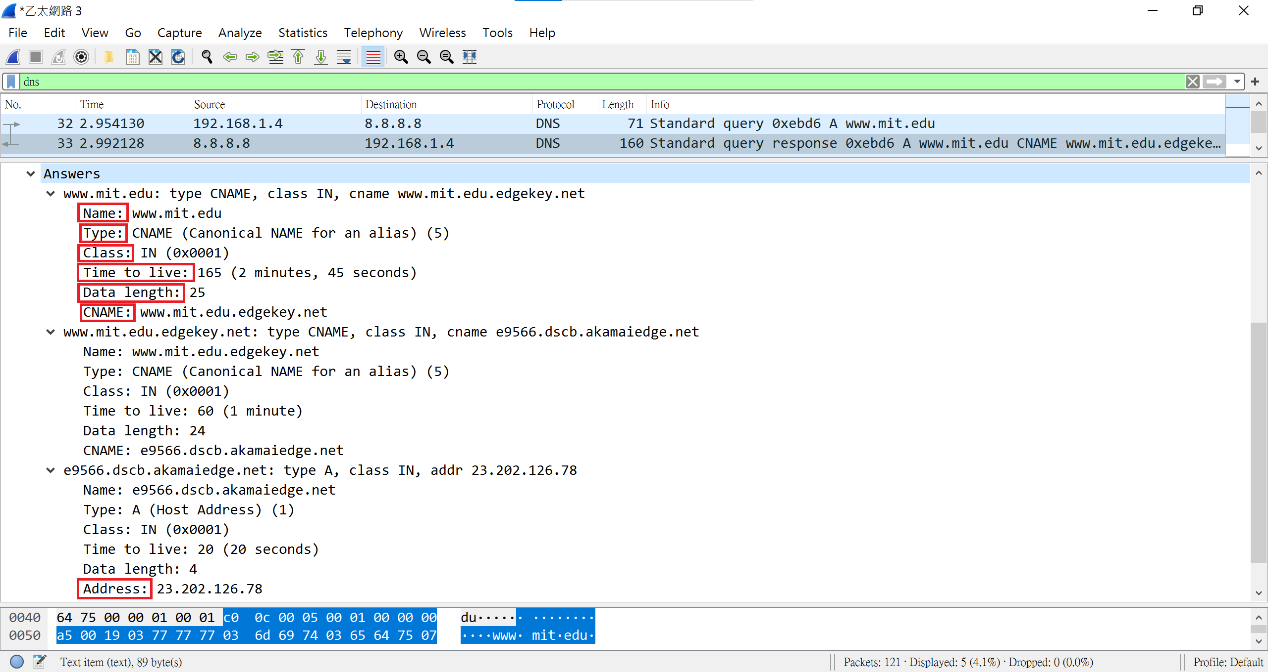
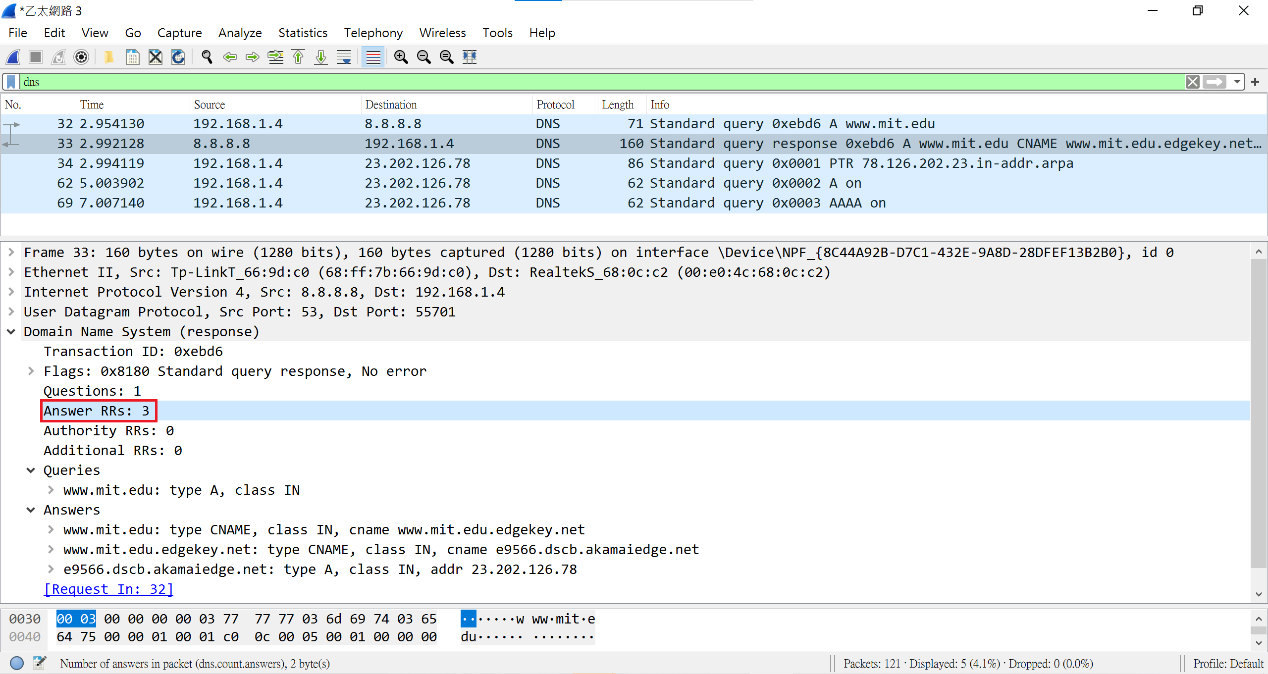
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans : Type A, no answer.



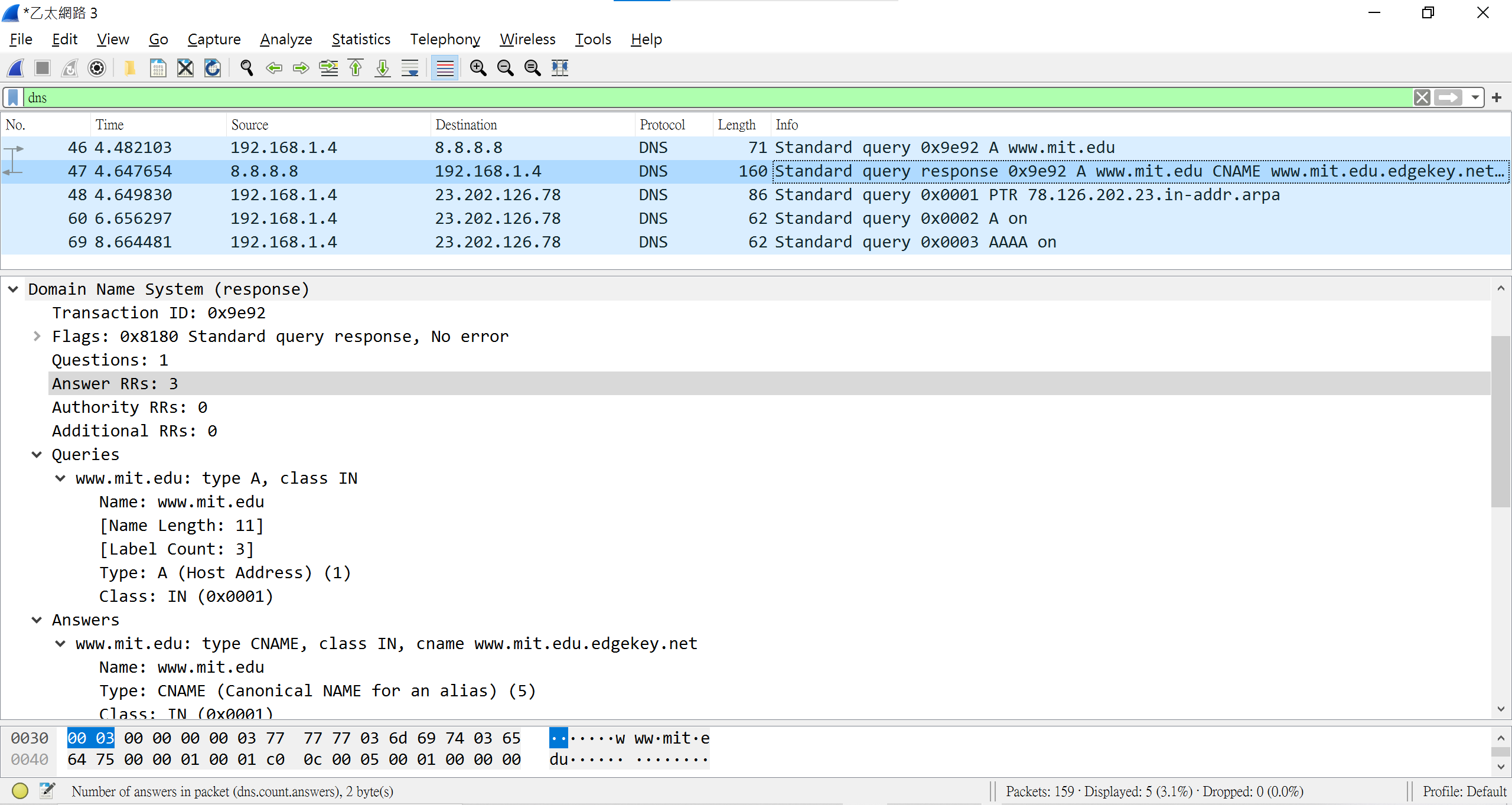
1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans : 3, Contain: Type, Class, TTL(Time To Live), Data Length, (Address or CNAME).



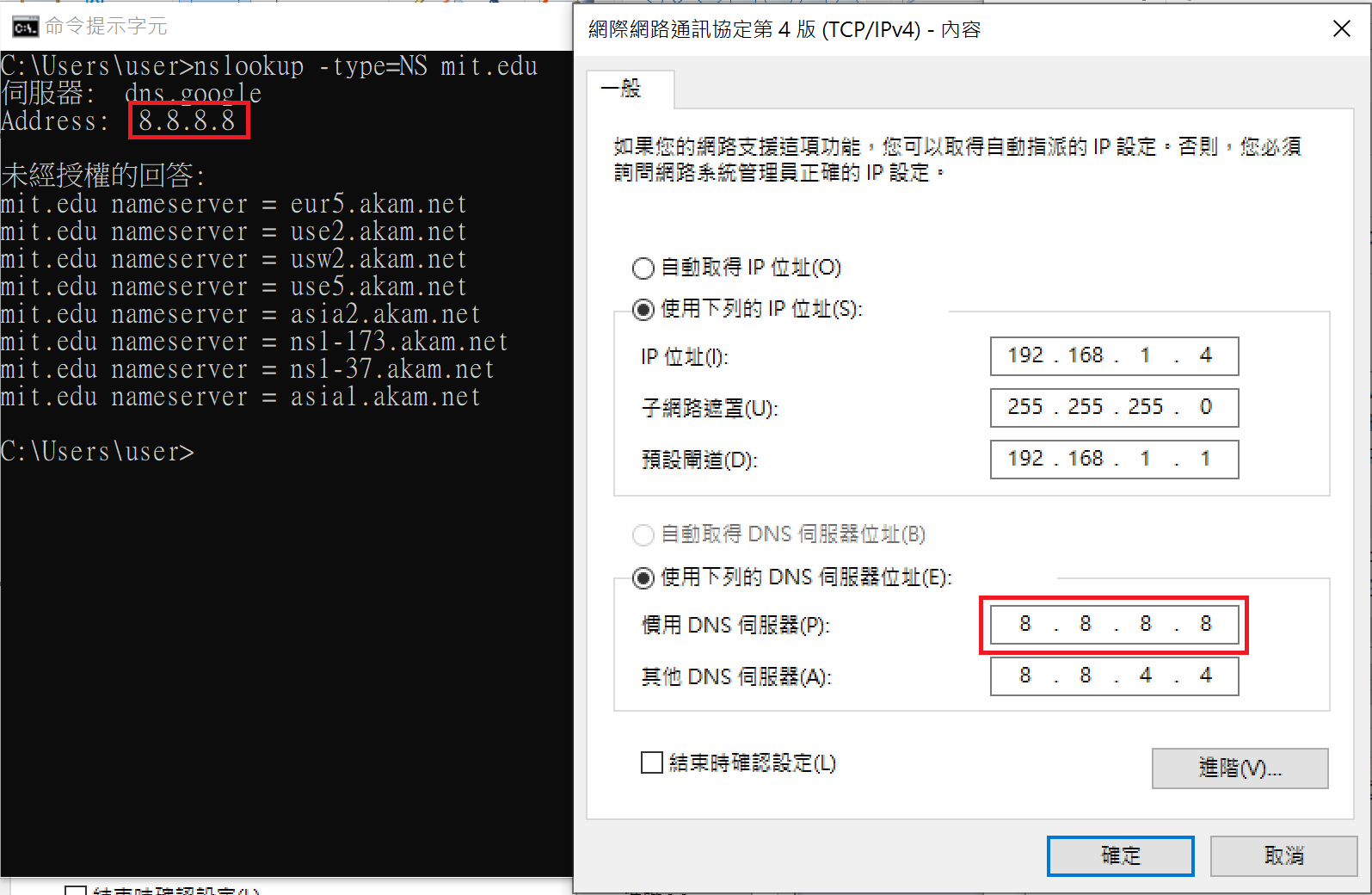
1. Provide a screenshot.

Ans : As following.



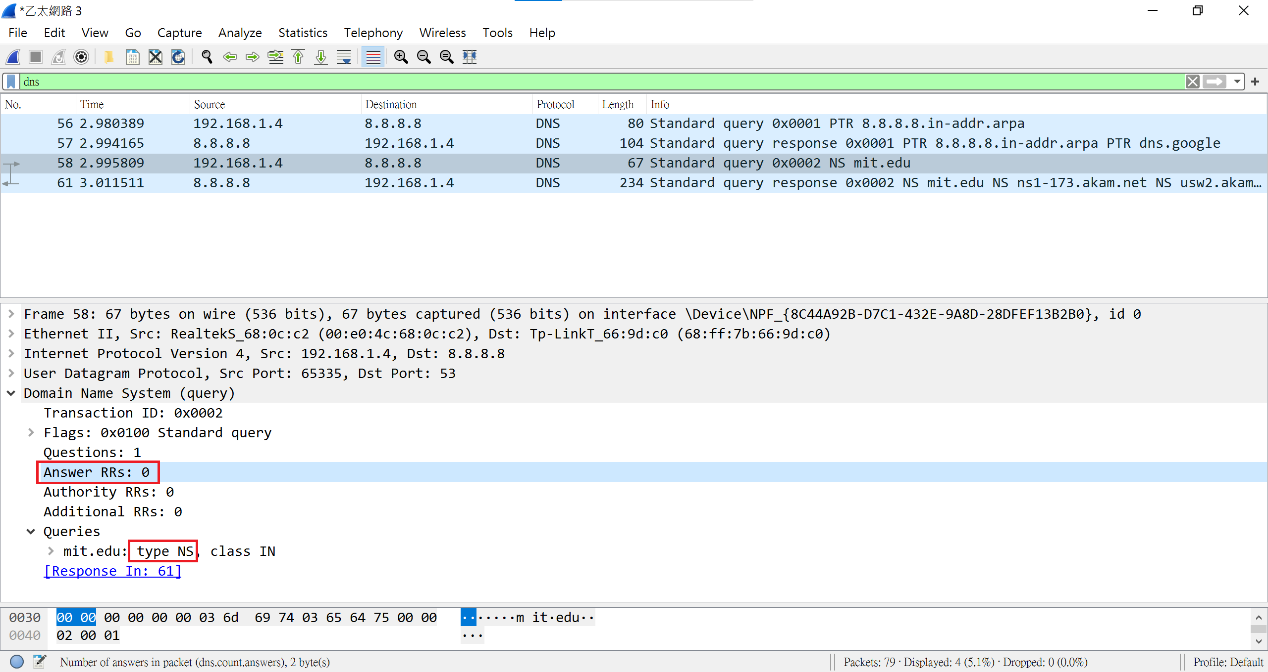
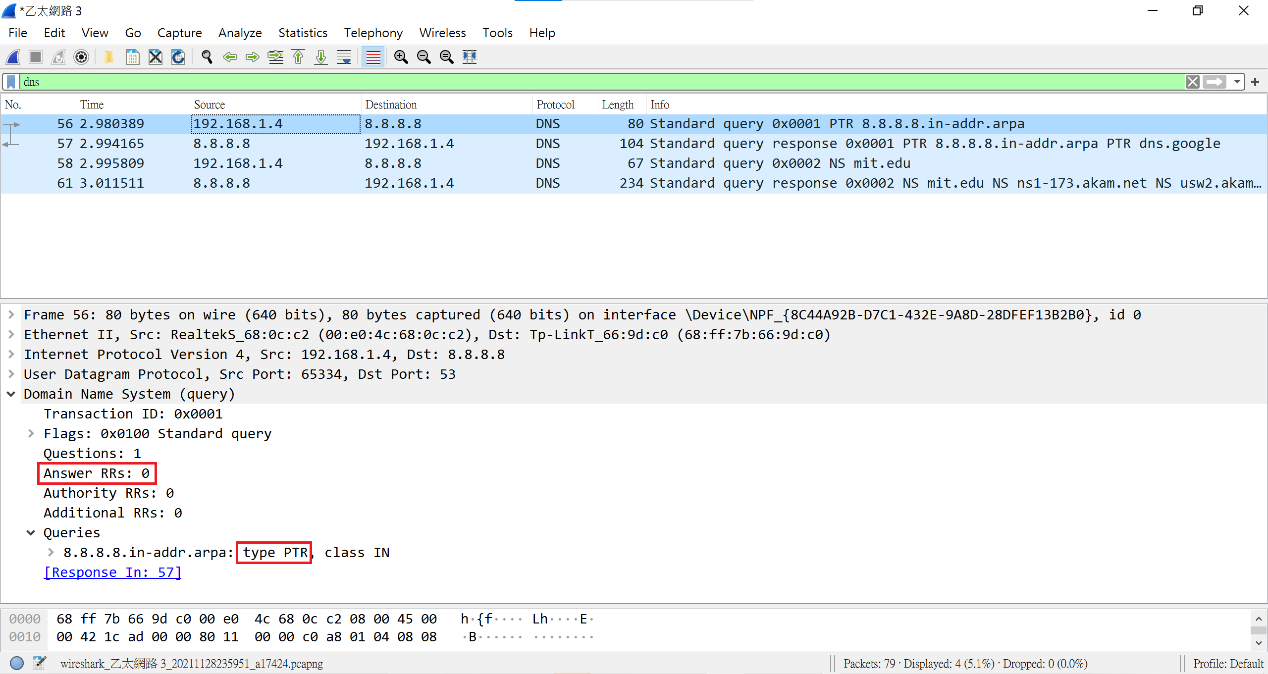
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans : 8.8.8.8, Yes.



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

Ans : Respectively Type PTR and Type NS, then the two query messages are not answer.



1. 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 namesers?

Ans :

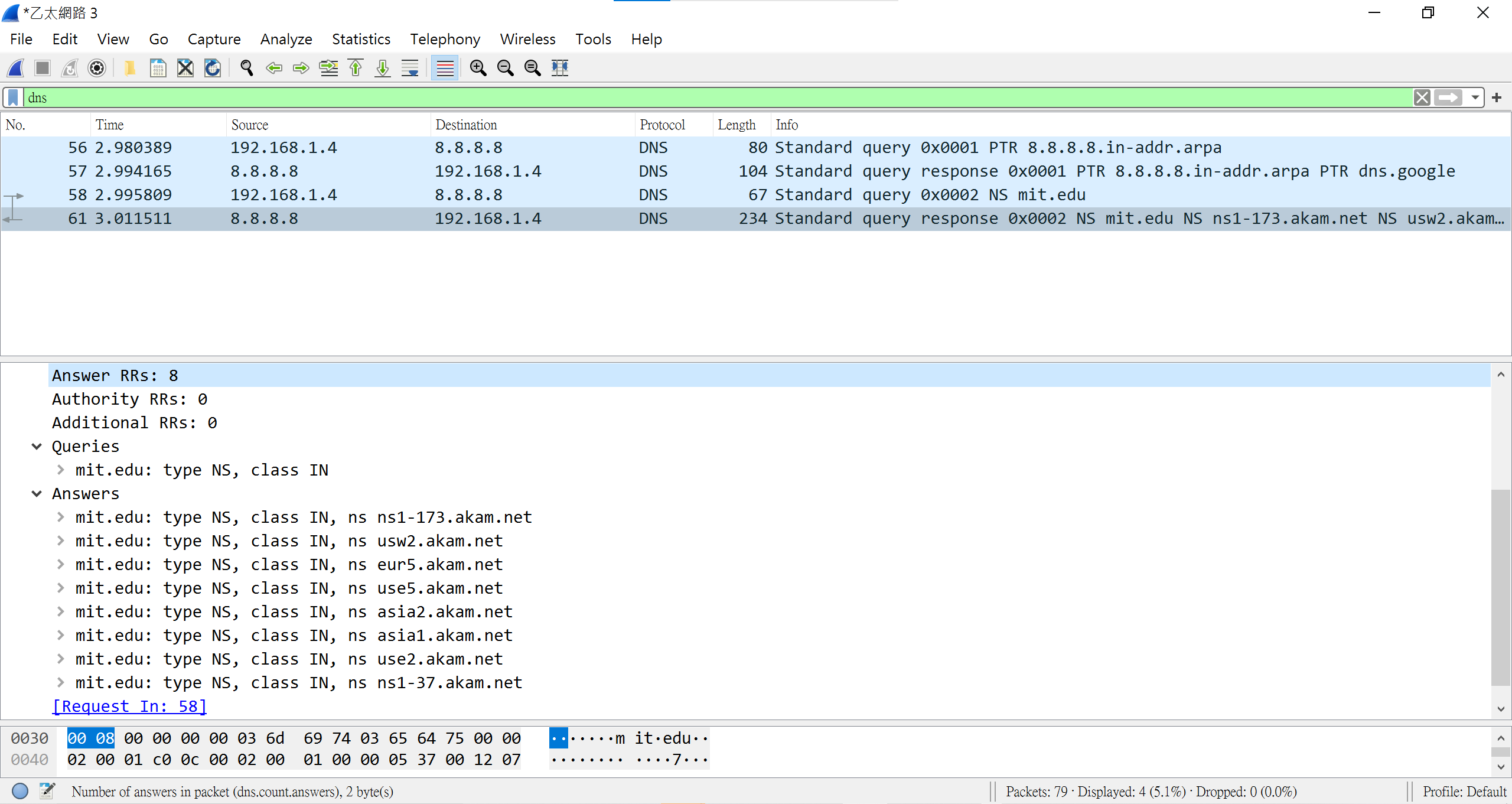
1. ns1-173.akam.net, 2. usw2.akam.net, 3. eur5.akam.net.

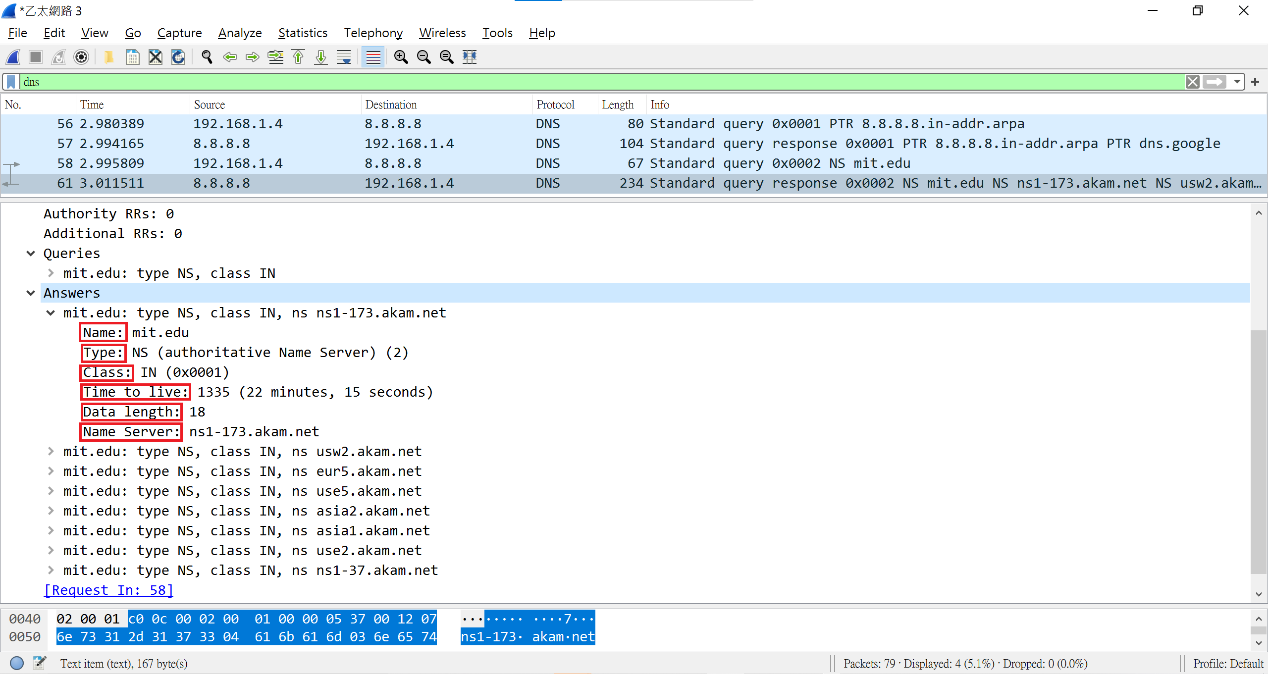
4. use5.akam.net, 5. asia2.akam.net, 6. asia1.akam.net

7. use2.akam.net, 8. ns1-37.akam.net

No, I can’t seeing IP address of the MIT namesers.

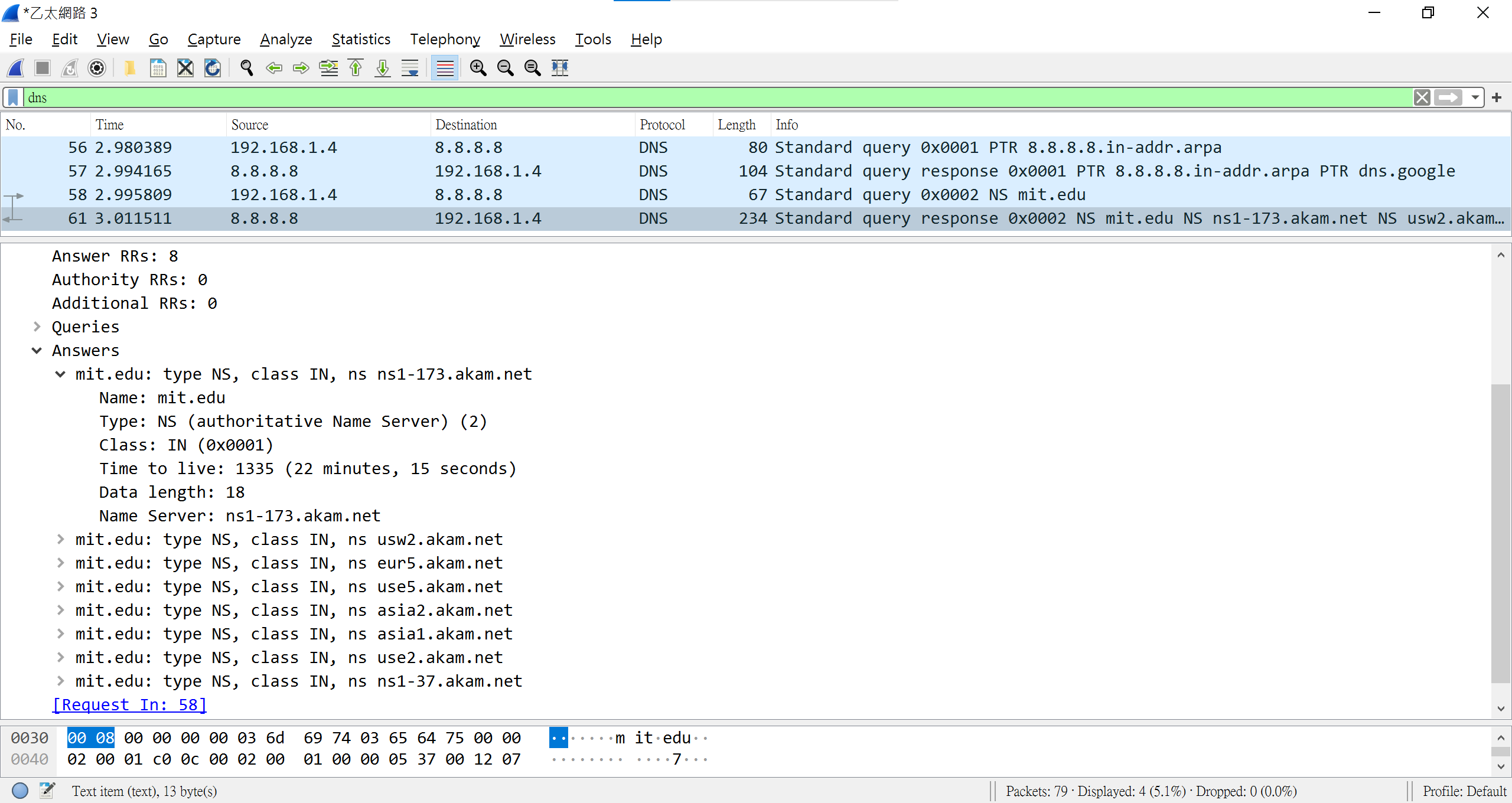
I only can seeing: Name, Type, Class, TTL(Time To Live), Data Length, Name Server.





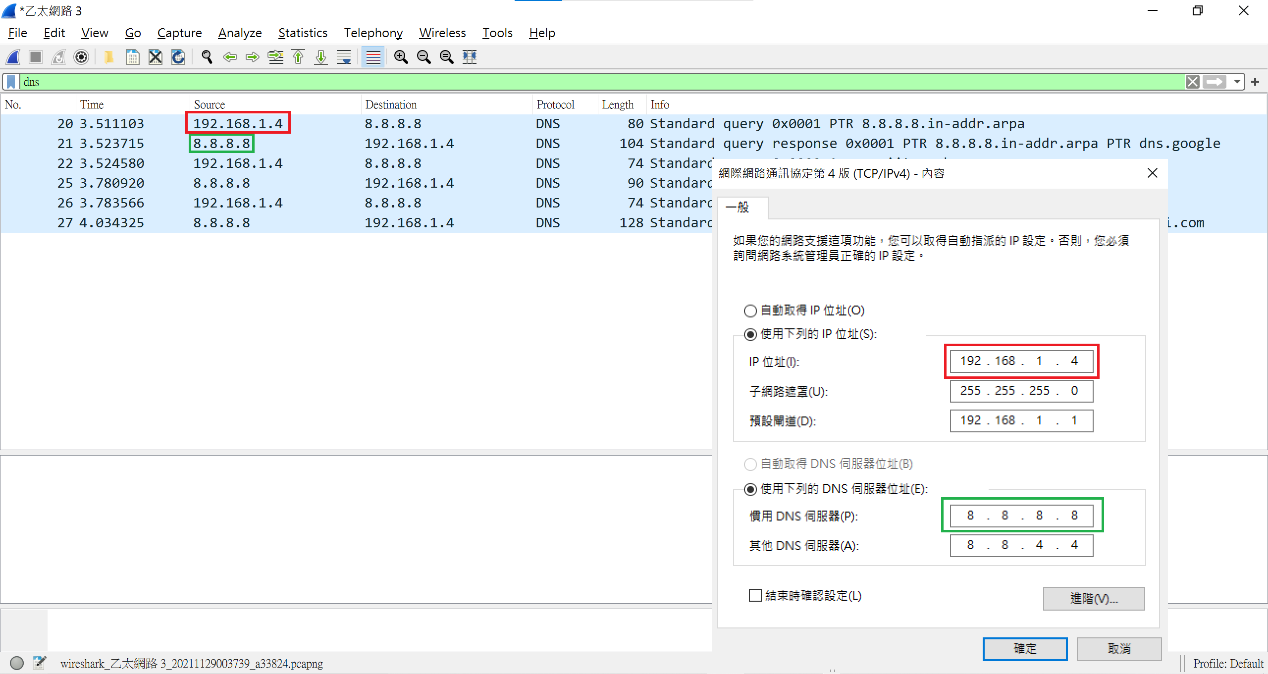
1. Provide a screenshot.

Ans : As following.



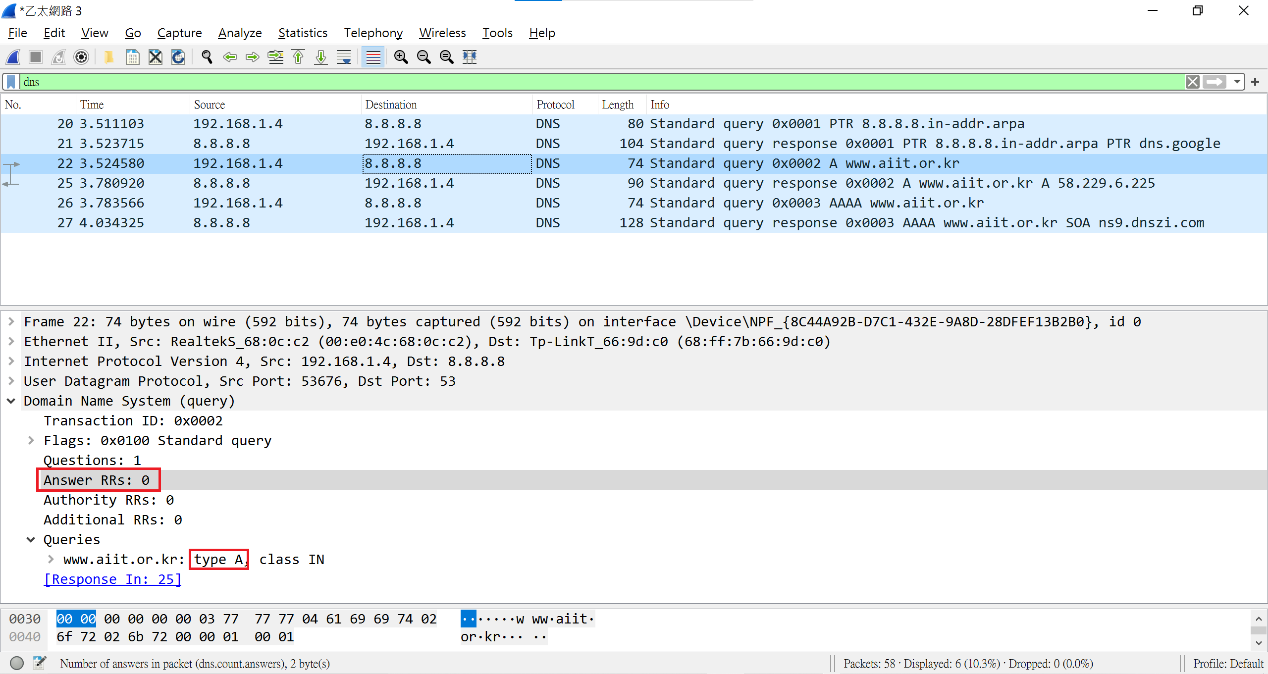
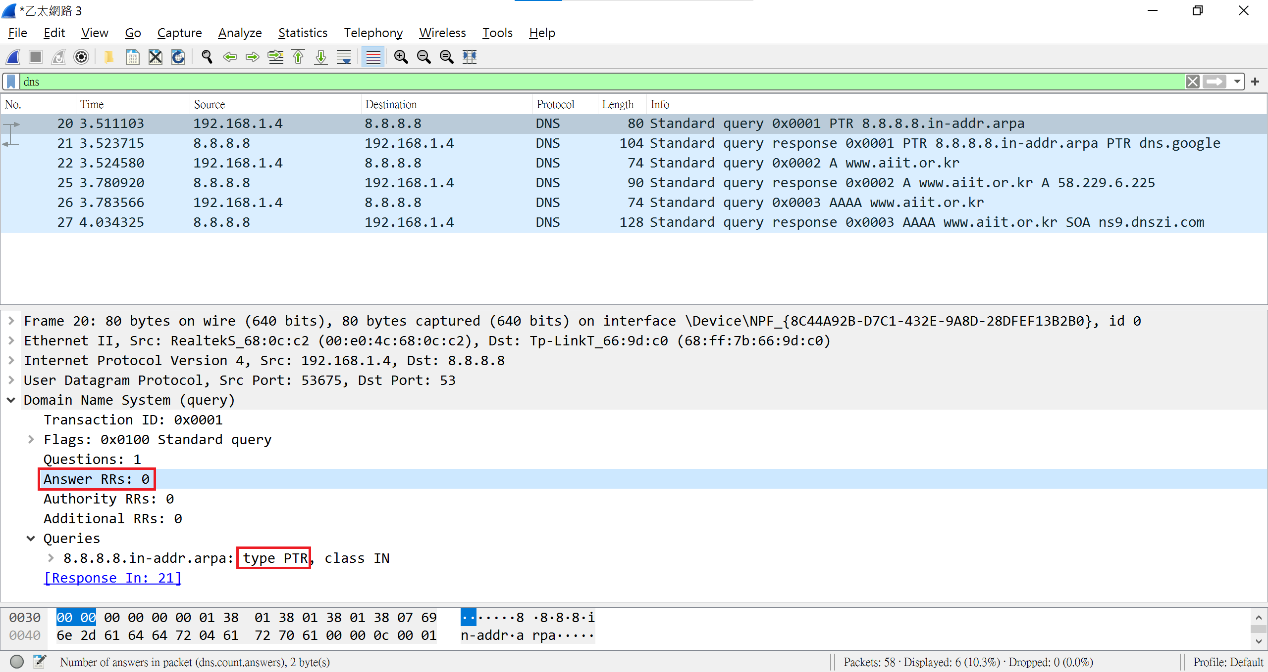
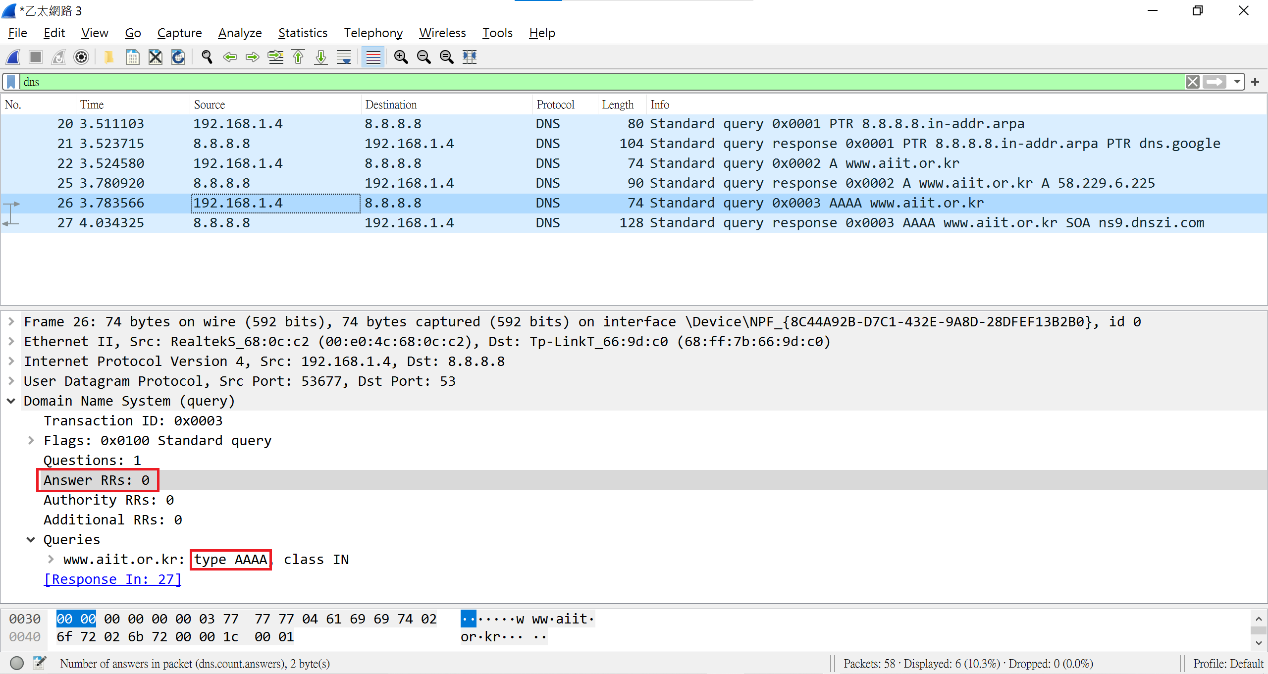
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Ans : 192.168.1.4, Yes, because I’m not specify my DNS server, the server always are default.



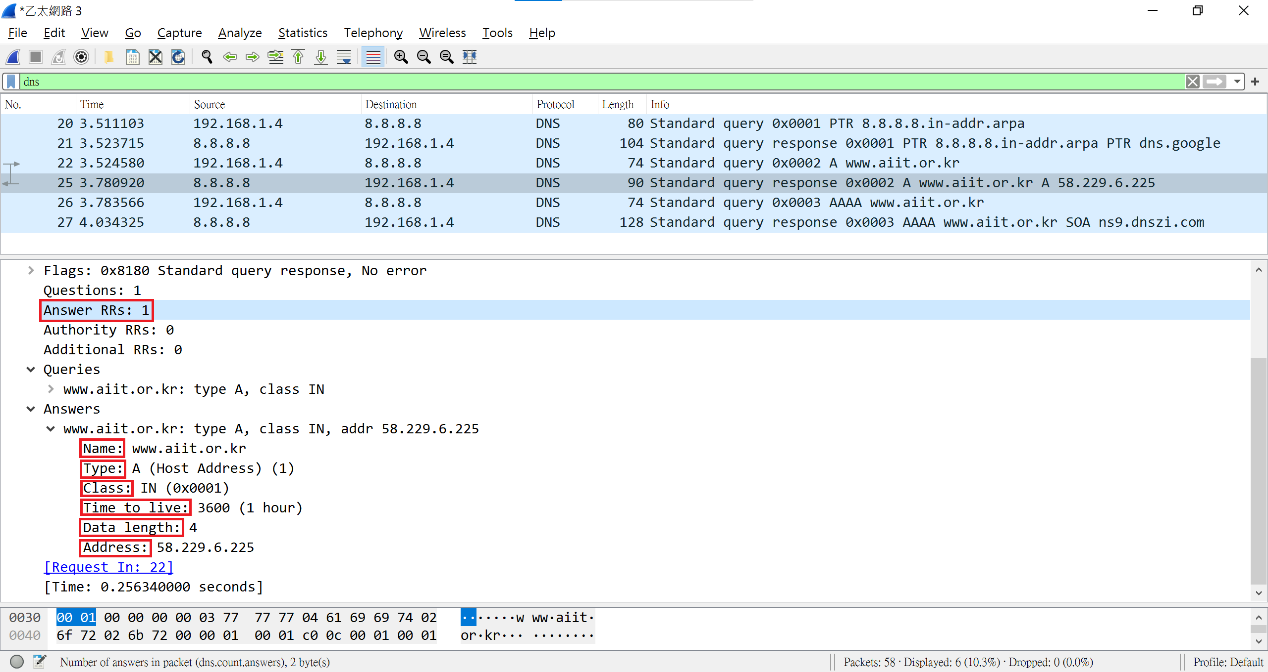
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Ans : Respectively Type PTR、Type A and Type AAAA, then the three query messages are not answer.

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

Ans : 1, Contain: Name Type, Class, TTL(Time To Live), Data Length, Address.



1. Provide a screenshot.

Ans : As following.

