Andrew Morrison

Lab 2

Computer Networks

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

210.86.125.59

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

Google-public-dns-a.google.com

3. 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?

131.111.150.25

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

UDP

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

Destination port: 53. Source port: 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?

Sent to: 8.8.8.8 IP address of local DNS server: 8.8.8.8 Yes, they are the same.

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

Type: A. It does not contain any answers.

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

There is one answer. It contains name, type, class, time to live, data length, and 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?

The destination IP address is 35.227.255.136 and it corresponds to the IP address contained in the answer.

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

No.

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

Destination port: 53. Source port: 53.

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

Sent to IP address: 8.8.8.8

Yes this is the IP address of my local DNS server.

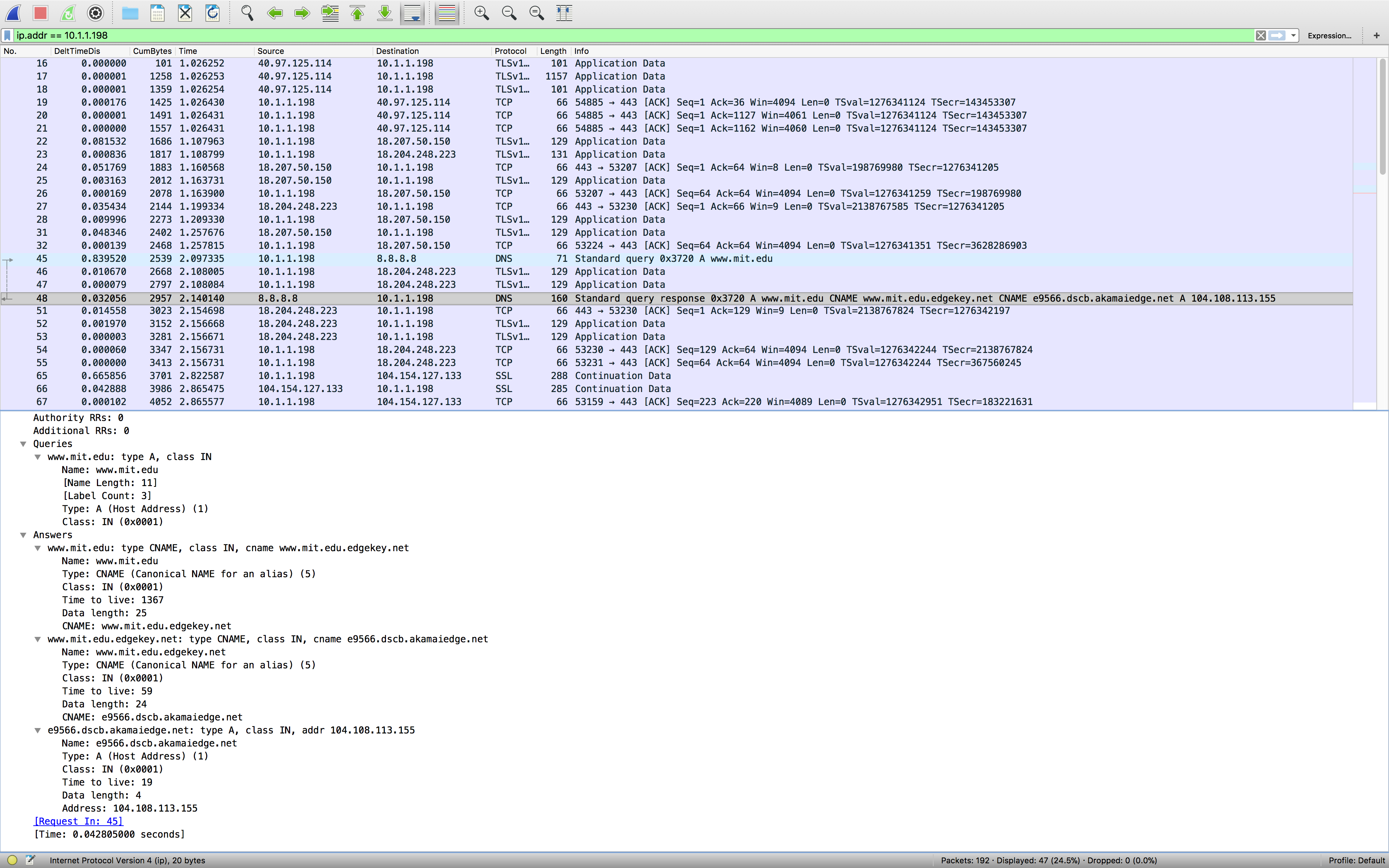
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A. It does not contain any answers.

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

It contains three answers. They contain name, type, class, time to live, data length, and CNAME.

15. Provide a screenshot.



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

8.8.8.8

Yes this is the IP address of my local DNS server.

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

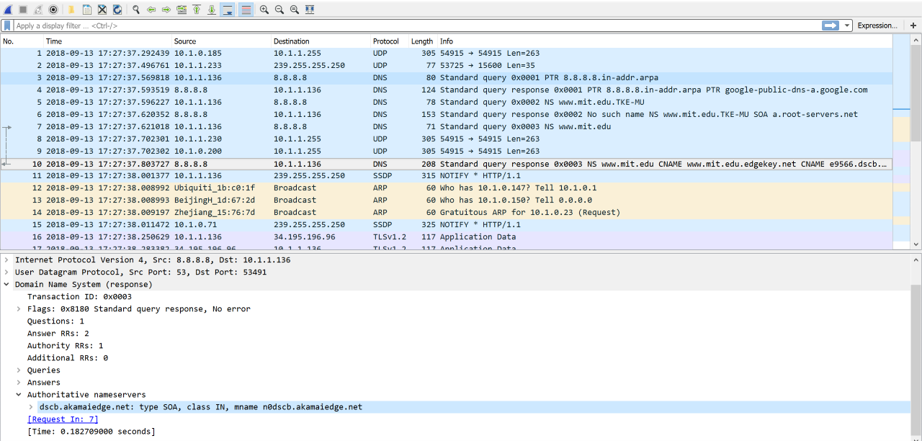
Type NS. There is no answers.

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 namesers?

(this wouldn’t work on mac for me so I used a friend’s Windows laptop)

It provides dscb.akamaiedge.net. No, it doe not provide any IP addresses.

19. Provide a screenshot.



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?

18.72.0.3

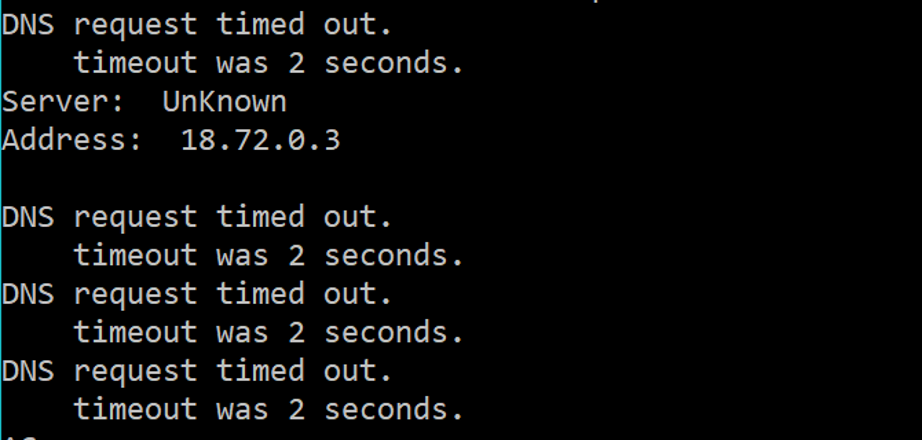
No it is the IP address of the MIT server.

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

Type: PTR. It contains no answers.

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

No DNS response message was captured.



23. Provide a screenshot.

