CPS 706 - Wireshark DNS

1. *Run nslookup to obtain the IP address of a Web server in Asia*

[01/28/20]seed@VM:~$ nslookup nus.edu.sg
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
Name: nus.edu.sg
Address: 45.60.35.225
Name: nus.edu.sg
Address: 45.60.33.225

2. *Run nslookup to determine the authoritative DNS servers for a university in Europe*
    - *University of Oxford*

[02/08/20]seed@VM:~$ nslookup -type=NS ox.ac.uk
Server: 127.0.1.1
Address: 127.0.1.1#53

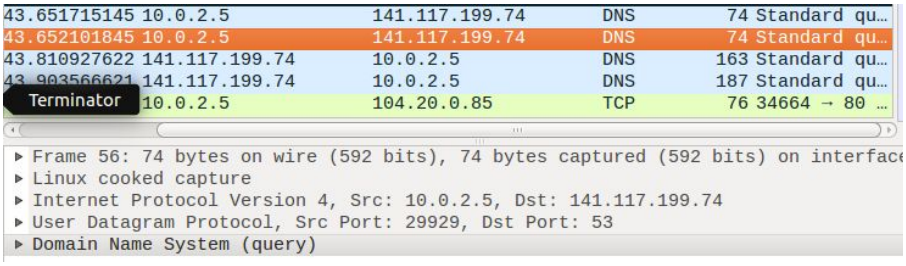
Non-authoritative answer:
ox.ac.uk nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk nameserver = dns0.ox.ac.uk.
ox.ac.uk nameserver = dns2.ox.ac.uk.
ox.ac.uk nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk nameserver = dns1.ox.ac.uk.
ox.ac.uk nameserver = ns2.ja.net.

3. *Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail.*
    - *It didn't work for Ymail. Accessed a different server (University College London)*

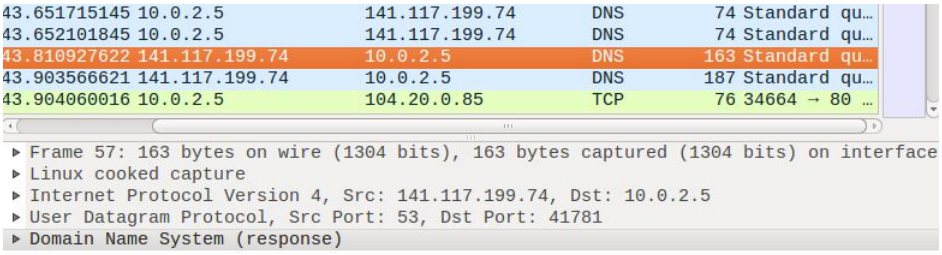
[02/03/20]seed@VM:~$ nslookup mail.yahoo.com auth6.dns.ox.ac.uk
Server: auth6.dns.ox.ac.uk
Address: 185.24.221.32#53
**** server can't find mail.yahoo.com: REFUSED**
[02/03/20]seed@VM:~$ nslookup ucl.ac.uk ns2.ja.net
Server: ns2.ja.net
Address: 193.63.105.17#53
Name: ucl.ac.uk
Address: 144.82.250.24

4. *Locate the DNS query and response messages. Are they sent over UDP or TCP?*
    - *They are sent over UDP*

5. *What is the destination port for the DNS query message? What is the source port of DNS response message?*
    - *Destination port for DNS query message: 53*



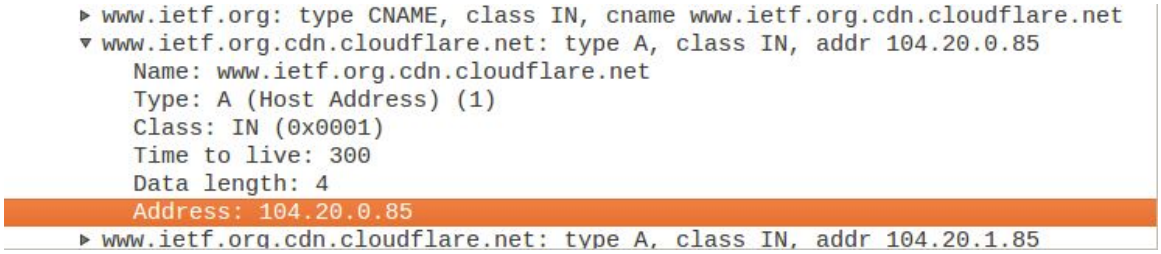
    - *Source port of DNS response message: 53*



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?*
    - *The DNS query message is sent to IP address: 141.117.199.74*
    - *This IP address is the same as one of the local DNS server*

7. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*
    - *It's a Type A standard DNS query*
    - *The query message doesn't contain any answers*

8. *Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?*
    - *3 answers are provided.*
    - *The answers contain information such as Name, Type, Class, TTL, datalength and address (one CNAME and two Type A answers)*



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 correspond to the IP address provided by the "answer" in the DNS response message*

10. *This web page contains images. Before retrieving each image, does your host issue new DNS queries?*
    - *No, the host doesn't issue any new DNS queries*

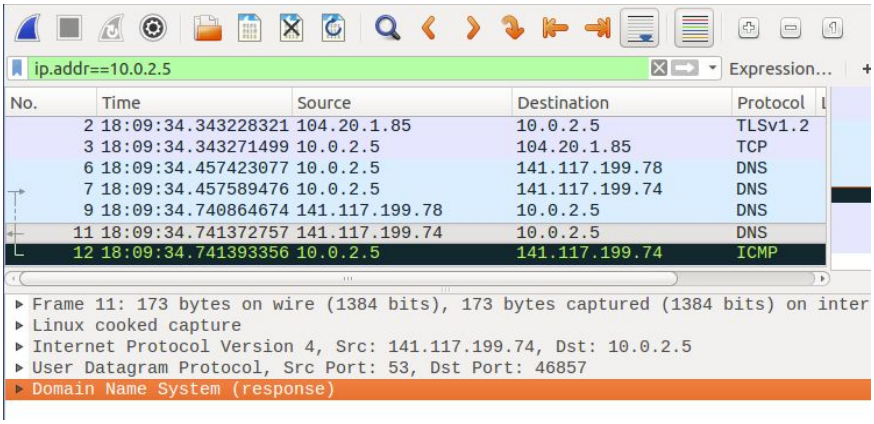
11. *What is the dst port for the DNS query message? What is the src port of DNS response message?*
    - *Destination port for DNS query message: 53*
    - *Source port of DNS response message: 53*

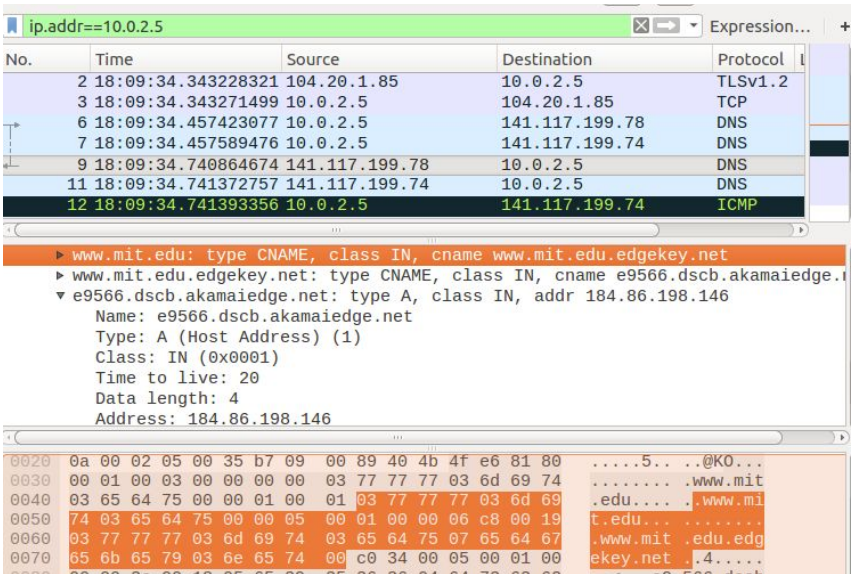
12. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*
    - *IP address of where it's sent: 141.117.199.74*
    - *Yes it's the IP address of the local DNS server*

13. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*
    - *It's a Type A DNS query*
    - *It does not contain any answers*

14. *Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?*
    - *3 answers are provided*
    - *Each of them contain information such as Name, Type, Class, TTL, datalength and address (two CNAME and one Type A answers)*

15. *Provide a screenshot.*



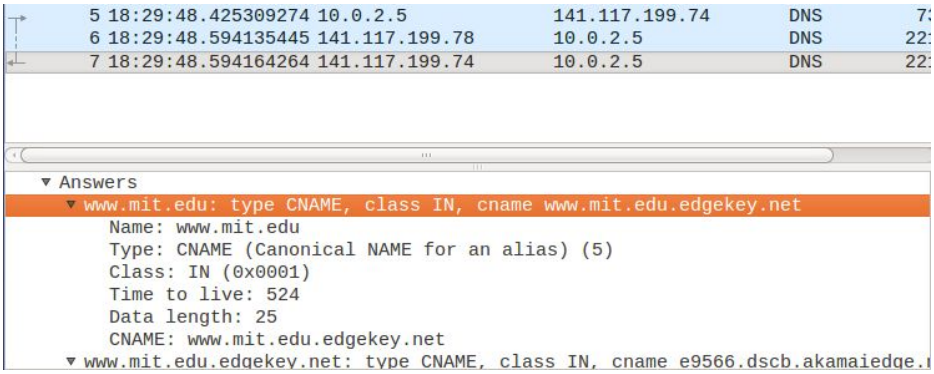


16. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*
    - *DNS query message is sent to IP address: 141.117.199.74*
    - *This is the IP address of the local DNS server*

17. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*
    - *The DNS query is of Type NS*
    - *It does not contain any answer*

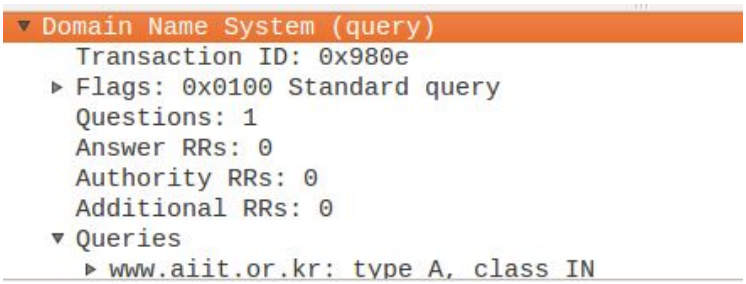
18. *Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?*
    - *MIT name servers provided are www.mit.edu and www.mit.edu.edgekey.net*
    - *The response message does not provide IP addresses the MIT name servers*

19. *Provide a screenshot.*



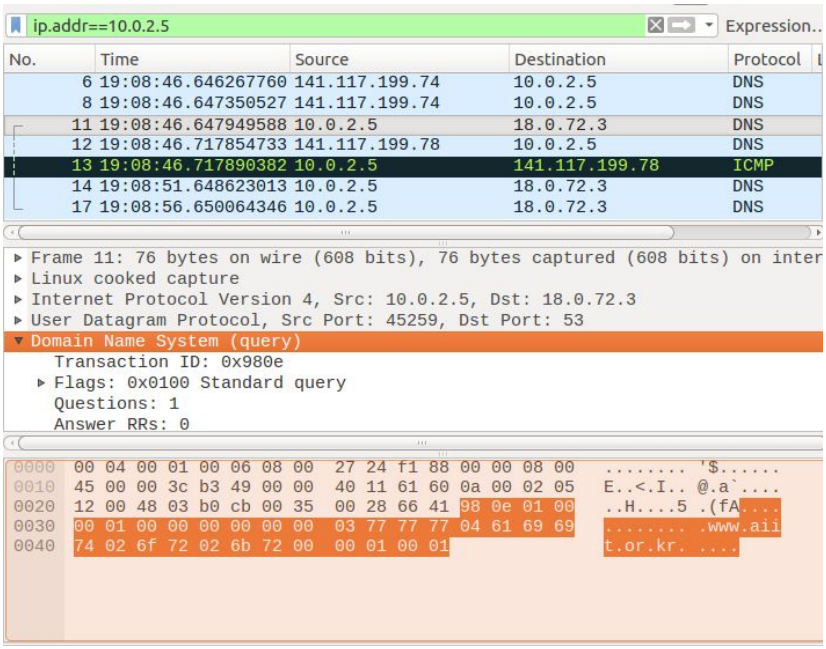
20. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?*
    - *The DNS query message is sent to IP address: 18.0.2.73*
    - *The IP corresponds to the address of bitsy.mit.edu*

21. *Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?*
    - *The DNS query message is of Type A*
    - *The query message does not contain any answer*



22. *Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?*
    - *There is no response message received*

23. *Provide a screenshot.*




```
[02/04/20]seed@VM:~$ nslookup aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached
```