Data Communications Laboratory
Domain Name System

Exercise 1: nslookup

1. Run nslookup to obtain the IP address of the Macquarie University Web server. What is the IP address of that server?

ANS:_____121.127.32.19_____

2. Run nslookup to determine the authoritative DNS servers for Macquarie University.

ANS:_____
adcampprod001.mqauth.uni.mq.edu.au_____

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the IP address of the Macquarie University Web server. Is there any difference in the output when compared to the first time you did the query in task 1 above?

ANS:_____Yes_____

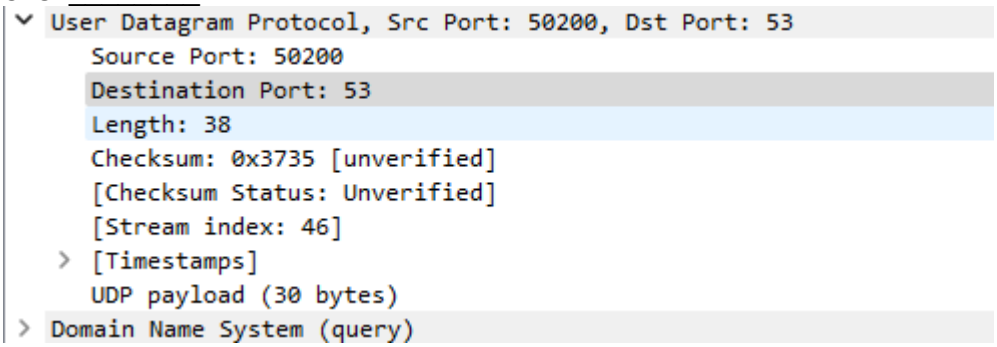
```
C:\Users\46392459>nslookup -type=NS ilearn-macquarie.catalyst-au.net
Server:  adcampprod001.mqauth.uni.mq.edu.au
Address:  10.127.5.17

catalyst-au.net
        primary name server = ns-1312.awsdns-36.org
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
```

Exercise 3: Tracing DNS with Wireshark

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

ANS:__They are sent over as UDP (User diagram protocol) this is shown in packet 528. _____



_____

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

ANS:___Destination port is 50200 and the Source port is 50200_____

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?

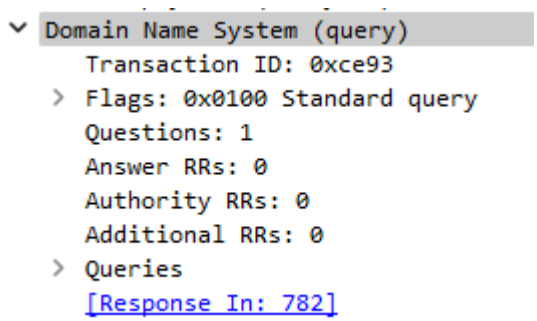
ANS:___10.127.5.21 yes both IP addresses they are the same

_____

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

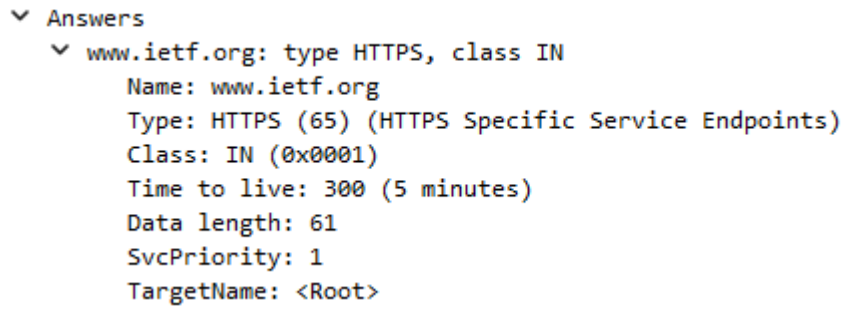
ANS:_____

It is a standard query the query message contains 0 answers



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

ANS:___1 answer is provided, as you can see in the screenshot these answers contains the Name, Type, Class, Time to live, Data length, SvcPriority, and TargetName.



You

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

ANS:

The destination port of the query message is shown in packet number 355 is 53

the source port of the query message is shown in packet number 356 is 53

_____

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

ANS:___in packet 355 the IP address in the DNS query message is sent to 10.127.5.17 which is the same IP address of my default local DNS server

11. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANS:__In packet 355 it is a standard query and the message doesn't contain any answers_____

12. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

ANS:_____In packet 356 there are 0 answers provided_(I made a typo sorry)_____

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

ANS:__ The IP address is sent to 10.127.5.17 my local DNS server. Yes it is the default local DNS
sever._____

14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

ANS:___it is a standard query the query doesn't contain any answers._____

15. 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?

ANS:____The MIT nameservers provides a standard query response. It doesn't provide the IP addresses of the MIT
nameservers._____
__

16. How many different types of DNS records can you see?

ANS:__3 different types

17. Looking at your Wireshark window, what is the most significant difference between a normal DNS query and a zone transfer?

ANS: