Data Communications Laboratory
Domain Name System

Jai Carey

45188416

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?

```
C:\Users\JAI_CAREY>nslookup ilearn.mq.edu.au
Server:  ADCAMPPROD001.mqauth.uni.mq.edu.au
Address:  10.127.5.17

Non-authoritative answer:
Name:    ilearn-macquarie.catalyst-au.net
Addresses:  76.223.72.246
          13.248.216.85
Aliases:  ilearn.mq.edu.au
```

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

```
Authoritative answers can be found from:
goza.science.mq.edu.au  internet address = 137.111.92.36
netdnsprod1.mq.edu.au   internet address = 137.111.226.226
netdnsprod2.mq.edu.au   internet address = 137.111.226.228
zoul.science.mq.edu.au  internet address = 137.111.92.14
dcutildr02.mq.edu.au    internet address = 137.111.225.138
```

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?

```
C:\Users\JAI_CAREY>nslookup netdnsprod1.mq.edu.au
Server:  ADCAMPPROD001.mqauth.uni.mq.edu.au
Address:  10.127.5.17

Non-authoritative answer:
Name:    netdnsprod1.mq.edu.au
Address:  137.111.226.226
```

Exercise 3: Tracing DNS with Wireshark

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

The DNS packets are sent over UDP (User Datagram Protocol).

```
> Frame 8: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
> Ethernet II, Src: IBM_10:60:99 (00:09:6b:10:60:99), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
> Internet Protocol Version 4, Src: 128.238.38.160, Dst: 128.238.29.23
> User Datagram Protocol, Src Port: 3163, Dst Port: 53
> Domain Name System (query)
```

5. 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.
The source port for the DNS RESPONSE message is 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 destination address is 128.238.29.23.
The local DNS server is also 128.238.29.23.

7. 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 answers.

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

In the DNS RESPONSE message, there are 2 answers provided. Each answer contains a different IP address that is linked to the same requested DNS.

```
> Queries
v Answers
  > www.ietf.org: type A, class IN, addr 132.151.6.75
  > www.ietf.org: type A, class IN, addr 65.246.255.51
  [Request In: 8]
  [Time: 0.000844000 seconds]
```

9. 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.
The source port for the DNS RESPONSE message is 53.

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

The DNS QUERY destination address is 10.127.5.17
The local DNS server is also 10.127.5.17

11. 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 answers.

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

1 Answer and 1 address. The answers contain the address.

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

The DNS QUERY destination address is 10.127.5.17
The local DNS server is also 10.127.5.17

14. 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 NS.
The query message does not 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?

The IP Addresses are provided of the MIT servers.

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

ANS:_____

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

ANS:_____