Will Barlow

81776940

Lab 06

NS Lookup

1. Run nslookup to obtain the IP address of a Web server in Asia (feel free to choose any). What is the IP address of that server? **[2 marks]**

58.229.6.225

1. Run nslookup to determine the authoritative DNS servers for a university in Europe (feel free to choose any). **[2 marks]**

85.13.132.32

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? **[2 marks]**

98.136.103.23

Tracing DNS with Wirshark

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

UDP

1. What is the destination port for the DNS query message? What is the source port of DNS response message? **[5 marks]**

Both are 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? **[5 marks]**

The query is sent to 209.90.170.72. My local DNS server has the same address

1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **[5 marks]**

It is type A. It contains no answers.

1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **[5 marks]**

There are three different answers. They contain the following attributes: name, type, class, time to live, and data length.

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? **[5 marks]**

It corresponds to the address given in the last query response message.

1. This web page contains images. Before retrieving each

image, does your host issue new DNS queries? **[5 marks]**

No it does not.

Playing with nslookup

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

What is the source port of DNS response message? **[5 marks]**

Both are 53

1. To what IP address is the DNS query message sent? Is

this the IP address of your default local DNS server? **[5 marks]**

The query is sent to 209.90.170.72. My local DNS server has the same address

1. Examine the DNS query message. What “Type” of DNS query

is it? Does the query message contain any “answers”? **[5 marks]**

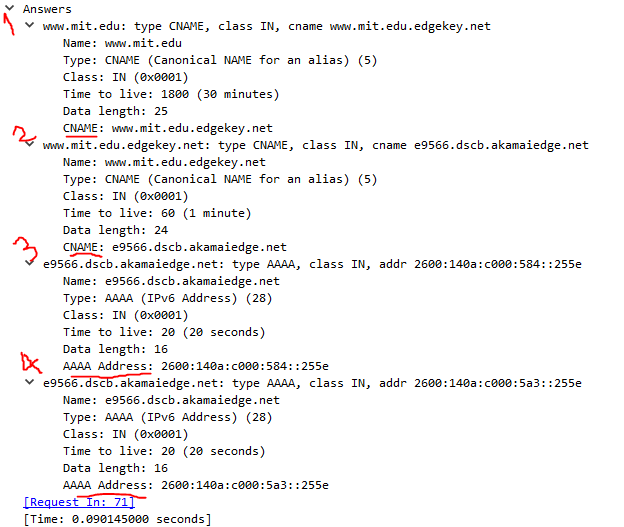
AAAA, no answers.

1. Examine the DNS response message. How many “answers”

are provided? What do each of these answers contain? **[5 marks]**

There are 4 answers. The first two contain the attributes name, type, class, TTL, data length, and CNAME. The latter two have the same attributes except the CNAME attribute is replaced with AAAA Address

1. Provide a screenshot.



Repeating previous experiment with modified command

(nslookup -type=NS mit.edu)

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? **[2 marks]**

The query is sent to 209.90.170.72. My local DNS server has the same address.

1. Examine the DNS query message. What “Type” of DNS query

is it? Does the query message contain any “answers”? **[2 marks]**

The type is NS. It does not contain any answers.

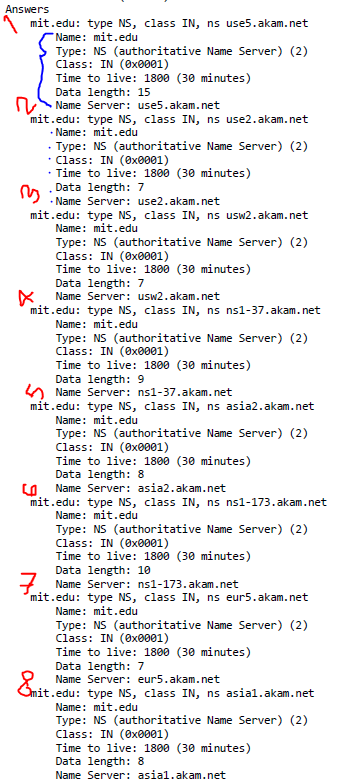
1. Examine the DNS response message. How many “answers”

are provided? What does each of these answers contain? **[2 marks]**

There are 8 answers. They each have the attributes, name, type, class, TTL, data length, and name server.

1. Provide a screenshot

*See next page*.



Repeating previous experiment with another modified command

(nslookup [www.aiit.or.kr](http://www.aiit.or.kr) bitsy.mit.edu)

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? **[2** **marks]**

The query is sent to 209.90.170.72. My local DNS server has the same address.

1. Examine the DNS query message. What “Type” of DNS query

is it? Does the query message contain any “answers”? **[2 marks]**

The Query is type A. It contains no answers.

1. Examine the DNS response message. How many “answers”

are provided? What does each of these answers contain? **[2 marks]**

There are 5 answers. The first 4 have the same attributes, name, class, TTL, data length, and CNAME. The 5th contains the same attributes except the CNAME attribute is replaced with Address.

1. Provide a screenshot

*See next page.*

