Darrel Chang

Professor Ibrahim

CS 3800

3/8/24

Homework 4 Wireshark Lab 3

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

address of that server?

**47.264.131.55**

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

Europe.

**Oxford University**

**IP: 151.101.194.216**

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?

**IP: 151.101.2.216**

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

**They are sent over UDP**

1. 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 of the DNS response message is also 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?

**The DNS query message is sent to 172.20.1.1. My local dns server is also 172.20.1.1**

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

**It’s Type a standard query and it contains no answers**

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

**It contains 2 answers. They contain name, type, class, time to live, data length, and address**

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?

**The first TCP SYN packet sent by my host corresponds with one of addresses in the DNS response message**

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

**No**

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

**The destination port fo the DNS query message is 53 and the source port of the DNS response message is also 53**

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

**The IP address is sent to 172.20.1.1 which is my local DNS server**

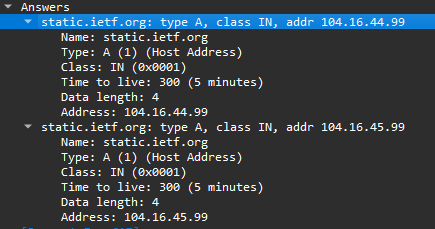
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**It is type A, and contains no answers**

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

**It contains 2 answers, which contain name, type, class, time to live, data length, and address**

1. Provide a screenshot.



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

**It is sent to 172.20.1.1, which is my default local DNS server**

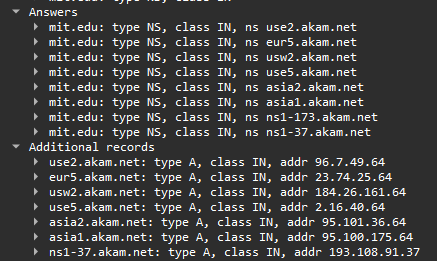
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

**It is type NS and does not contain answers**

1. 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?

**It provides many nameservers such as use2, eur5, usw2, use5, asia2, asia1, ns1, ns1**

1. Provide a screenshot.



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?

**It is sent to 18.072.3, which corresponds to bitsys address**

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

**It is type A and does not contain answers**

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

**One answers is provided which contains name, type, class, time to live, data length, and address**

1. Provide a screenshot.

