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]**
2. Run nslookup to determine the authoritative DNS servers for a university in Europe (feel free to choose any). **[2 marks]**
3. 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]**

Tracing DNS with Wirshark

1. Locate the DNS query and response messages. Are then sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message? **[5 marks]**
3. 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]**
4. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? **[5 marks]**
5. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain? **[5 marks]**
6. 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]**
7. This web page contains images. Before retrieving each

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

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

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

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

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

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

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

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

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

1. Provide a screenshot.
2. 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]**

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

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

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

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

1. Provide a screenshot.
2. 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]**

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

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

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

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

1. Provide a screenshot.