California State University, Monterey Bay

Week 3 – Lab 3
Group 10

Clarence Mitchell

CST331

Introduction to Computer Networks

SUMMER 2015

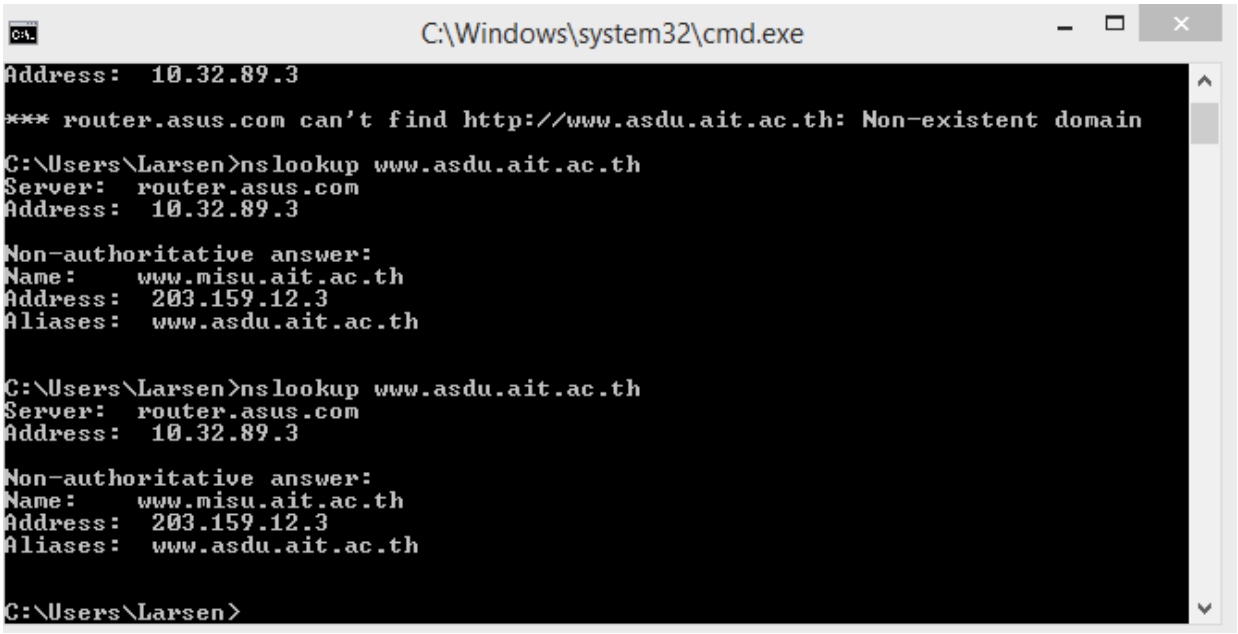
Instructor: Dr. Anand Seetharam

Questions and Answers

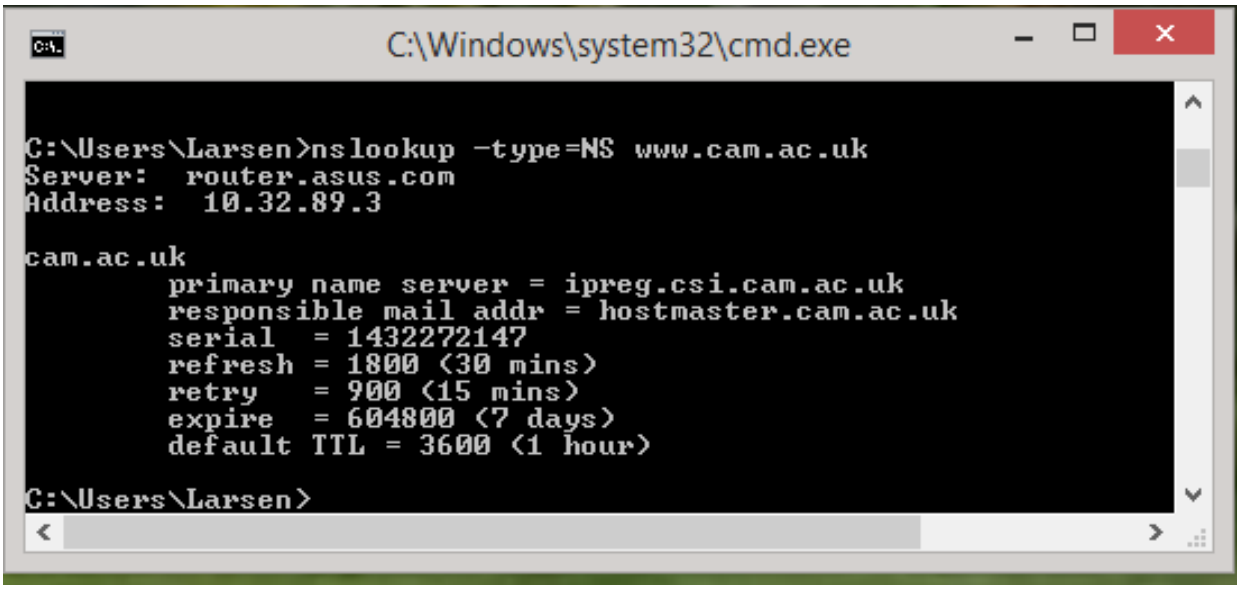
The following are the list of questions and related answers for this lab.

1. nslookup

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
   - I used google to find a webserver that I think is located in Asia, which is the server for AIT Asian Institute of Technology.(http://www.asdu.ait.ac.th/)
   - I got the IP address 203.159.12.3



2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
   - Again, I used google to find a webserver of a university that is located in Eurpose, which is the server for University of Cambridge.(http://www.cam.ac.uk)
   - To determine the authoritative DNS servers, I used -type=NS to get ipreg.csi.cam.ac.uk



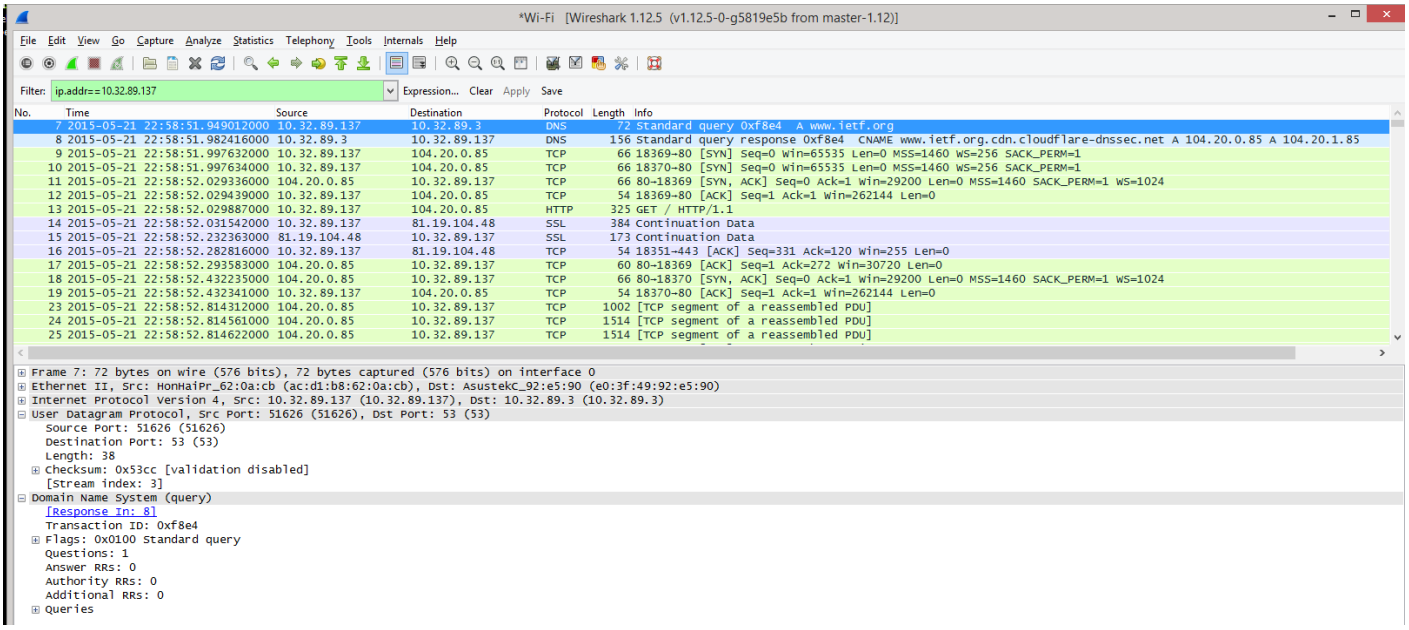
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?
   - IP Address is 98.136.189.41

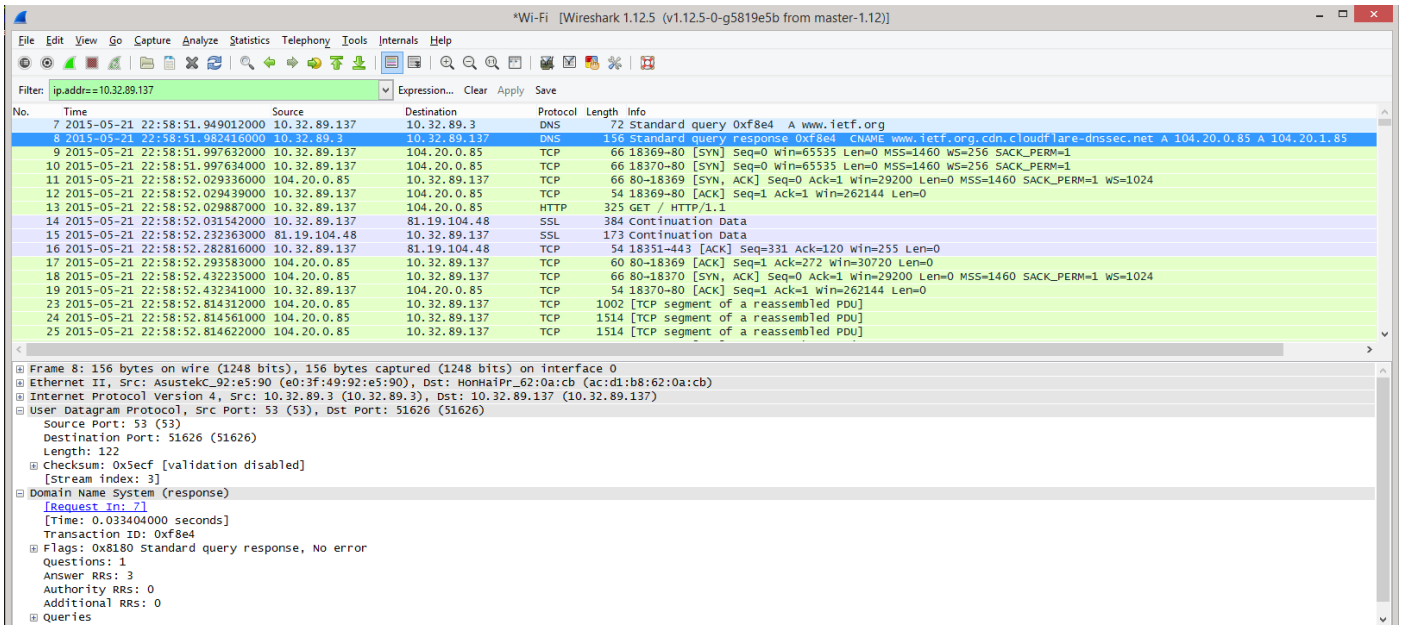
```
C:\Users\Larsen>nslookup ipreg.csi.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  98.136.189.41

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\Larsen>
```

2. ipconfig

- This is ALL of the DNS information about my host. ipconfig/displaydns and ipconfig/flushdns can be used to show and clear DNS records obtained by the host..

3. Tracing DNS with Wireshark





4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
    - They are sent over UDP.
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
    - The destination port is port 53, and the source port is port 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?

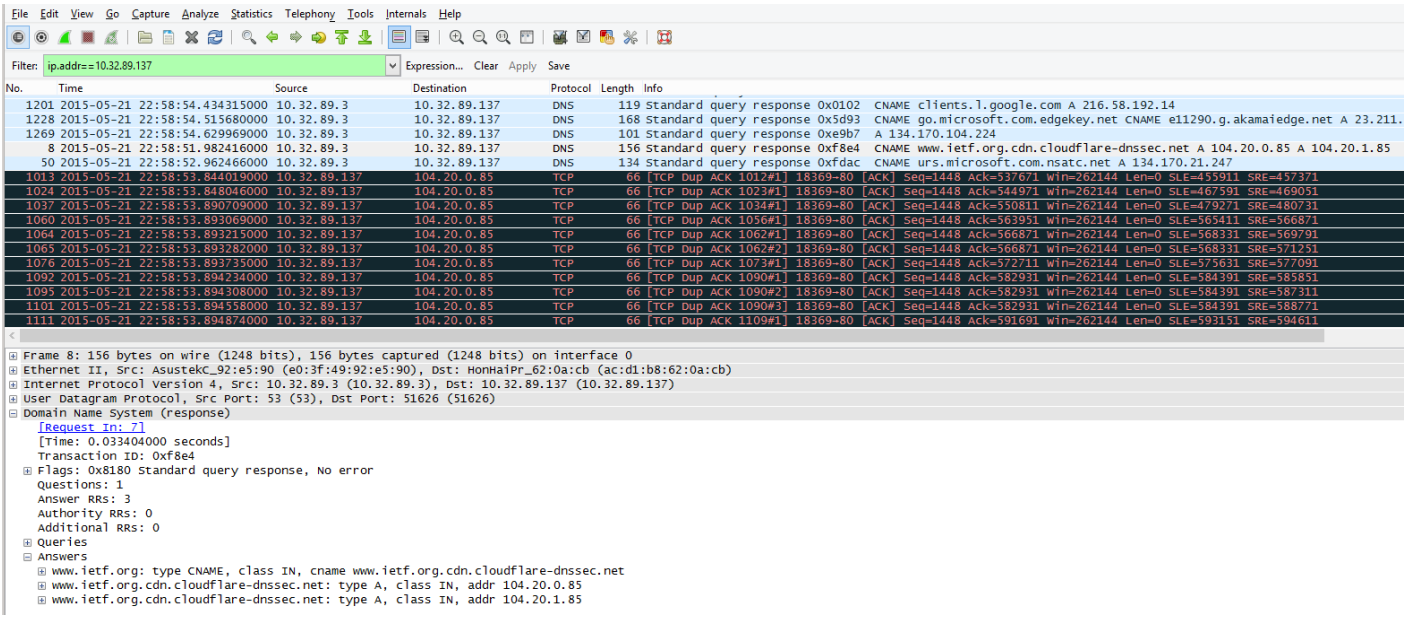
```
C:\Users\Larsen>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Adonis
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : dynadock Ethernet
   Physical Address. . . . . . . . . : 00-50-B6-65-2D-12
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Killer e2200 Gigabit Ethernet Controller
<NDIS 6.30>
   Physical Address. . . . . . . . . : 34-E6-D7-43-C3-82
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : AE-D1-B8-62-0A-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Killer Wireless-n/a/ac 1525 Wireless Netw
ork Adapter
   Physical Address. . . . . . . . . : AC-D1-B8-62-0A-CB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::89fb:e5b:647c:f4ef%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.32.89.137(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, May 19, 2015 9:38:09 PM
   Lease Expires . . . . . . . . . . : Friday, May 22, 2015 11:58:25 AM
   Default Gateway . . . . . . . . . : 10.32.89.3
   DHCP Server . . . . . . . . . . . : 10.32.89.3
   DHCPv6 IAID . . . . . . . . . . . : 95211960
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1C-86-8C-F1-34-E6-D7-43-C3-82

   DNS Servers . . . . . . . . . . . : 10.32.89.3
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : AC-D1-B8-62-0A-CC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

- In the ipconfig that I did it showed that my local DNS server was 10.32.89.3, so yes they are the same.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
   - It's a type A Standard Query and it doesn't contain any answers

-

8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
    - There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address.
    -
9. 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?
    - Yes it does. The first SYN packet was sent to 104.20.0.85 which corresponds to the first IP address provided in the DNS response message.
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    - No
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    - The destination port of the DNS query is 53 and the source port of the DNS response is 53.
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - The DNS query message is sent to IP 10.32.89.3. This is the same IP address of my local DNS server.
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
    - The query is of type A and it doesn’t contain any answers.
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
    - The response DNS message contains only 3 answers containing the name of the host, the type of address, the class, the IP address
15. Provide a screenshot.



16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - It was sent to 10.32.89.3 which again is my default DNS server.
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    - It's a type NS DNS query that doesn't contain any answers.
18. 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 http://www.mit.edu and http://www.mit.edu.edgekey.netThe response message does not contain any nameservers. If it did they would be under additional records right under answers, but there is nothing below answers..
19. Provide a screenshot.
    -
20. 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?
    -
21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    -
22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
    -
23. Provide a screenshot.
    -