CS 176A: Homework 2

Bharat Kathi

Part 1:

1. Note: to answer these questions, it may be helpful for you to first read through the Wireshark lab.

(a) What is a whois database?

A whois database is a publicly accessible collection of records containing domain registration information.

(b) Use a whois database on the Internet to lookup ucsb.edu. Who is in charge of the UCSB network? What are the names of the UCSB name servers? When did UCSB obtain its original DNS entry? Which whois database did you use to find this information?

I used http://whois.educause.edu.

The nameservers are:

- NS2.UCSB.EDU
- BRU-NS2.BROWN.EDU
- NS1.UCSB.EDU

The registrant is the ETS Network & Communications Services department at the University of California, Santa Barbara. The administrative contact is Kevin Schmidt. UCSB obtained the original entry on 27-Apr-1987.

(c) Use nslookup to find a Web server that has multiple IP addresses (do not use an example from class). List the name of that web server and the addresses it maps to.

Name: storkecentr.al

Addresses: 104.21.69.135, 172.67.208.246

(d) Does the UCSB web server have multiple IP addresses?

No.

(e) On a machine in CSIL, type the command “ip addr show”. What IP address does your machine have? (Hint: it is the address that starts with 128.111). Include the name of the machine you are on so we can check your answer (i.e. csil-01.cs.ucsb.edu)

csilvm-10.cs.ucsb.edu
128.111.30.210

2. Install and compile the Python programs TCPClient and UDPClient on one host and TCPServer and UDPServer on another host (the code is available in section 2.7 of the textbook).

(a) Suppose you run TCPClient before running TCPServer. What happens? Why?

The client will try to establish a connection with the server, which fails since the server is not running at this point, returning a connection refused error.

(b) Suppose you run UDPClient before you run UDPServer. What happens? Why?

Since UDP is connectionless, there will be no error returned. However the initial data that was sent by the client never reaches the server since it was not listening at the time. Once the server is online, it starts receiving data from the client.

(c) What happens if you use different port numbers for the client and server sides?

If we use different ports, then the TCP client will fail to connect to the server. The UDP client will still send packets but they won’t be received by the server.

3. Suppose that in UDPClient.py, after we create the socket, we add the line:
clientSocket.bind((”, 5432))
Will it become necessary to change UDPServer.py? What are the port numbers for the sockets in UDPClient and UDPServer? What were they before making this change?

No, since the server port is still the same. The client binding only changes the source port of the UDP packets.

Part 2.1:

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

They are sent over UDP.

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

Destination port for the query message is 53. The source port for the response message is also 53.

3. To what IP address is the DNS query message sent? This is the IP address of a local DNS server.

The IP address is 128.111.1.1.

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

It’s a query for an A record.

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

Yes, it appears to query the static.ietf.org domain name for images.

Part 2.2:

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

The destination port for the query message is 53. The source port for the response message is also 53.

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

The query message is sent to 128.111.1.2.

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

The response message contains 3 answers. The type A records return an ip address and type CNAME records return the CNAME alias. All records return the name, type, class, and a ttl (time to live).

Part 2.3:

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 nameservers?

The response message provided 8 nameservers:

- asia1.akam.net
- eur5.akam.net
- ns1-37.akam.net
- asia2.akam.net
- use2.akam.net
- use5.akam.net

- usw2.akam.net
- ns1-173.akam.net

It does not also return the IP addresses of the nameservers.