Ashlyn Goh 1002840 Cl02

50.005 – Lab 7

DNS basics

Question 1: Using dig, find the IP address for `thyme.lcs.mit.edu`. What is the IP address?
IP address is 18.26.0.122.

Question 2: The dig answer for the previous question includes a record of type `CNAME`. What does `CNAME` mean?
A Canonical Name or CNAME record is a type of DNS record that maps an alias name to a true or canonical domain name. These records are typically used to map a subdomain such as www or mail to the domain hosting that subdomain's content.

Question 3: What is the expiration time for the `CNAME` record?
It expires in 1605s.

Question 4: Run the following commands to find out what your computer receives when it looks up *'ai'* and *'ai.'* in the `mit.edu` domain. What are the two resulting IP addresses?
From '*ai*': none
From '*ai.*': 209.59.119.34

Question 5: Why are the results for both queries different? Look up the manual for `dig` to find out what the `+domain` parameter does. Based on the output of the two commands, what is the difference between the DNS searches being performed for *'ai'* and *'ai.'*?
The +domain parameter sets the search list to contain the single domain. We get different outputs from the two commands because the dot in the domain name indicates an absolute path. For 'ai', the domain is resolved to be 'mit.edu.ai' which is unavailable. For 'ai.', DNS looks for 'ai' alone which is resolved to the IP address of 209.59.119.34.

Understanding hierarchy

Question 6: Use `dig` to query one of the DNS root servers for the IP address of `lirone.csail.mit.edu` without using recursion. What is the command that you use to do this?

```
dig @a.root-servers.net lirone.csail.mit.edu +norecurs
```

Question 7: Go through the DNS hierarchy from the root until you have found the IP address of `lirone.csail.mit.edu`. You should disable recursion and follow the referrals manually. Which commands did you use, and what address did you find?

```
dig @a.root-servers.net lirone.csail.mit.edu +norecurs
dig @a.edu-servers.net lirone.csail.mit.edu +norecurs
dig @usw2.akam.net lirone.csail.mit.edu +norecurs
dig @auth-ns0.csail.mit.edu lirone.csail.mit.edu +norecurs
```

The IP address is 128.52.129.186 which brings us to the lirone.csail.mit.edu page.

Understanding caching

Question 8: Without using recursion, query your default DNS server for information about `www.dmoz.org` and answer the following questions.

- **What is the command that you used?**
- **Did your default server have the answer in its cache? How did you know?**
- **How long did the query take?**

***Note:* If the information was cached, find another host name that was not cached and complete all the questions in this section using that host.**

Command: `dig www.dmoz.org +norecurs`

My default server did not have the answer in its cache because there was no answer section that gave me the IP address of www.dmoz.org.

The query took 282ms.

Question 9: Query your default DNS server for information about the host in the previous question, using the recursion option this time. How long did the query take?

It took 88ms.

Question 10: Query your default DNS server for information about the same host without using recursion. How long did the query take? Has the cache served its purpose? Explain why.

It took 12ms.

The cache has served its purpose because it remembered the previous answer and significantly decreased the amount of time it took to get the IP address of the host.

Part 2: Tracing DNS using Wireshark

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

They are sent over UDP.

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

Destination port is port 53. The source port is 57763.

Question 3: What is the IP address to which the DNS query message was sent? Use ifconfig to determine the IP address of your local DNS server. Are these two addresses the same?

192.168.2.11. They are not the same.

Question 4: Examine the second DNS query message. What type of DNS query is it? Does the query message contains any answers?
The second DNS query message is a recursive DNS query of type A and class IN.
It does not contain any answers.

Question 5: Examine the second DNS response message. How many answers are provided? What does each of these answers contain?
2 answers were provided. One answer is a CNAME record pointing to updatekeepalive.glb.mcafee.com. The other answer is an A record with address of 161.69.12.13.

Question 6: Locate a TCP SYN packet sent by your host subsequent to the above DNS response. This packet opens a TCP connection between your host and the web server. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
The destination IP address of the TCP SYN packet is to 161.69.12.13 which coincides with the IP address of updatekeepalive.glb.mcafree.com (from above).