*Name: Kwa Li Ying*
*Student ID: 1003833*
*Class: CI03*

# CSE Lab 6 Report

## PART 1: Exploring DNS using dig

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

The 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?

`CNAME` means canonical name. It means that `thyme.lcs.mit.edu` is an alias of another (canonical) hostname called `mercury.lcs.mit.edu`.

**Question 3:** What is the expiration time for the `CNAME` record?

The expiration time is 600 seconds.

**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?

- `dig +domain=mit.edu ai`
- `dig +domain=mit.edu ai.`

For 'ai', the query does not return any IP address in the answer section.

For 'ai.', the resulting IP address is 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=somename` sets the search list to contain the single domain `somename`, as if specified in a domain directive in `/etc/resolv.conf`, and enable search list processing as if the `+search` option were given. This means that it will only search for results under the given domain name, which is `mit.edu`.

For 'ai' the command looks for the word hostname starting with ai within the `mit.edu` domain. Thus the query finds results for the hostname `ai.mit.edu`.

For 'ai.', however, the command is interpreted as 'ai.' is the absolute hostname to query for, thus disregarding the `+domain` option in the command.

**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?

*Name: Kwa Li Ying*
*Student ID: 1003833*
*Class: CI03*

```
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?

Commands:

- `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`

IP Address:

- 128.52.129.186

**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.

The command I used is `dig www.dmoz.org +norecurs`.

My default server did not have the answer in its cache. It did not return an answer section.

The query took 5ms.

**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?

The query took 214ms.

**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.

The query took 6ms. The cache has served its purpose as an answer section is returned this time.

*Name: Kwa Li Ying*
*Student ID: 1003833*
*Class: CI03*

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?

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

**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?

The DNS query message was sent to 192.168.2.11. The IP address of my local DNS server is 192.168.1.1. They are not the same.

**Question 4:** Examine the second DNS query message. What type of DNS query is it? Does the query message contain any answers?

It is a standard query. The query message 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?

There are 2 answers provided. The first answer (CNAME) provides the canonical name updatekeepalive.glb.mcafee.com to the alias hostname updatekeepalive.mcafee.com, and the second answer (authoritative) contains the IP address 161.69.12.13 for the hostname updatekeepalive.glb.mcafee.com.

**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?

Yes, the destination IP address (161.69.12.13) corresponds to the IP address provided in the DNS response message.