1. IP address of thyme.lcs.mit.edu: 18.26.0.122
2. CName is a type or resource record in the Domain Name System (DNS) used to specify that a domain name is an alias for another domain (the canonical domain). They are bindings which redirect one domain name to another
3. 397

4)‘ai’ 128.52.32.80/Auth-ns0.csail.mit.edu bug-domain.csail.mit.edu

‘ai.’ 209.59.119.34

Q5: +domain=somename: Set the search list to contain the single domain somename, so in here would be mit.edu, asif specified in a domain directive in /etc/resolve.cnf, and enable search list processing as if the search option were given. By nslookup, we can tell that at the above IP address, the name contains the string ‘offshore.ai.”

The results are different because a trailing dot in the domain name signals an absolute path. Therefore, DNS looks for ‘’ai’’ alone when there is a trailing dot. When there is no trailing dot, the dig command looked for ‘ai’ within the mit.edu domain

Understanding Hierarchy

Q6 To look for lirone.csail.mit.edu from the root servers without recursion, I used the command dig @a.root-servers.net lirone.csil.mit.edu +norecurs.

Q7 I used the following list of commands:

* [dig@a.root-servers.net](mailto:dig@a.root-servers.net) lirone.csail.mit.edu +norecurs
* [dig@a.edu-servers.net](mailto:dig@a.edu-servers.net) lirone.csail.mit.edu +norecurs
* dig@use5.akam.net lirone.csail.mit.edu +norecurs
* dig@auth-ns3.csail.mit.edu lirone.csail.mit.edu +norecurs

After this series of commands, I discovered that lirone.csail.mit.edu has an ip address of 18.220.24.14 and that it is actually a synonym for lirone.lcs.mit.edu

Understanding Caching

I used the command **dig www.dmoz.org +norecurs**. This sends a DNS request to the default server 127.0.0.1. However, the default server did have the answer in its cache because it provided me the ip address of www.dmoz.org in the answer section of the results. The query took 5 milliseconds. I looked for a domain name ``www.thetimes.com'' and discovered it was not in the default server's cache. I know this because when I ran **dig www.thetimes.com +norecurs**, I was sent to the .com DNS servers, which means I had to go to the root servers and start a hierarchical query.

I ran {dig www.thetimes.com} and it returned in 3240 milliseconds.

I ran {dig www.thetimes.com} and it returned in 3 milliseconds. The cache has served its purpose because it significantly decreased the amount of time it took to get the ip address of [www.thetimes.com](http://www.thetimes.com).

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

They are sent over UDP

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

The destination port for the DNS query is 57763 and the source port of the DNS response is 53

1. 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?

It’s sent to 192.168.2.11 which is the IP address of one of my local DNS servers.

1. 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.

1. 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, data length and the IP address

1. 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 first SYN packet was sent to 65.246.255.51 which corresponds to the first IP address provided in the DNS response message.