Toh Yong Cheng

1000039

# Internet Domain Name System

Question 1

18.26.0.122

Question 2

Canonical Name

Question 3

1352 seconds

Question 4

128.52.32.80

No IP Address received (209.59.119.34 from Javier's computer)

Question 5

The results are different because the first search searches for results that has 'ai' which corresponds to 'mit.edu'. However, the second search

only searches for 'ai.' which has no relation to 'mit.edu'.

Placing a '.' causes the search to search absolutely, which results in the results as shown.

Question 6

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

Question 7

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

;; ANSWER SECTION:

lirone.csail.mit.edu. 1800 IN CNAME lirone.lcs.mit.edu.

lirone.lcs.mit.edu. 1800 IN A 18.26.1.36

Question 8

dig @192.168.2.11 [www.dmoz.org](http://www.dmoz.org) +norecurs

Yes, there is caching. The query time was only 6ms.

Question 9

It took 261ms.

Question 10

It took only 2ms. Yes it has served its purpose.

# Wireshark Labs

Question 1

They are SNMP, DNS, TCP and HTTP.

Question 2

0.024143s

Question 3

128.119.245.12

192.168.1.102

Question 4

It is a GET request. HTTP/1.1.

The requesting browser uses Netscape 7.01 on a Windows NT 5.1 Operating System. It uses en-US, rv:1.0.2

Question 5

The next request is a HTTP GET for the /favicon.ico. The request was unsuccessful (404 Not found).

# Tracing DNS with Wireshark

Question 1

It is sent over UDP.

Question 2:

Destination Port: Domain (53)

Response Source Port: Domain (53)

Question 3:

The message is sent to 192.168.2.11

No if is diferent from the IP address of my local DNS server (from hostel) but yes for school.

Question 4:

It is a standard query with type A (host address). There is no answers.

Question 5:

There is 1 answer. It contains:

www.ietf.org: type A, class IN, addr 4.31.198.44

Name: www.ietf.org

Type: A (Host address)

Class: IN (0x0001)

Time to live: 21 minutes, 21 seconds

Data length: 4

Addr: 4.31.198.44 (4.31.198.44)

Question 6:

The destination is 4.31.198.44 which is the same as the answer in the DNS response message.

Question 7:

No it does not.

# nslookup with Wireshark

Question 1:

Destination Port: Domain (53)

Response Source Port: Domain (53)

Question 2:

192.168.2.11

No it is not (hostel) but yes for school.

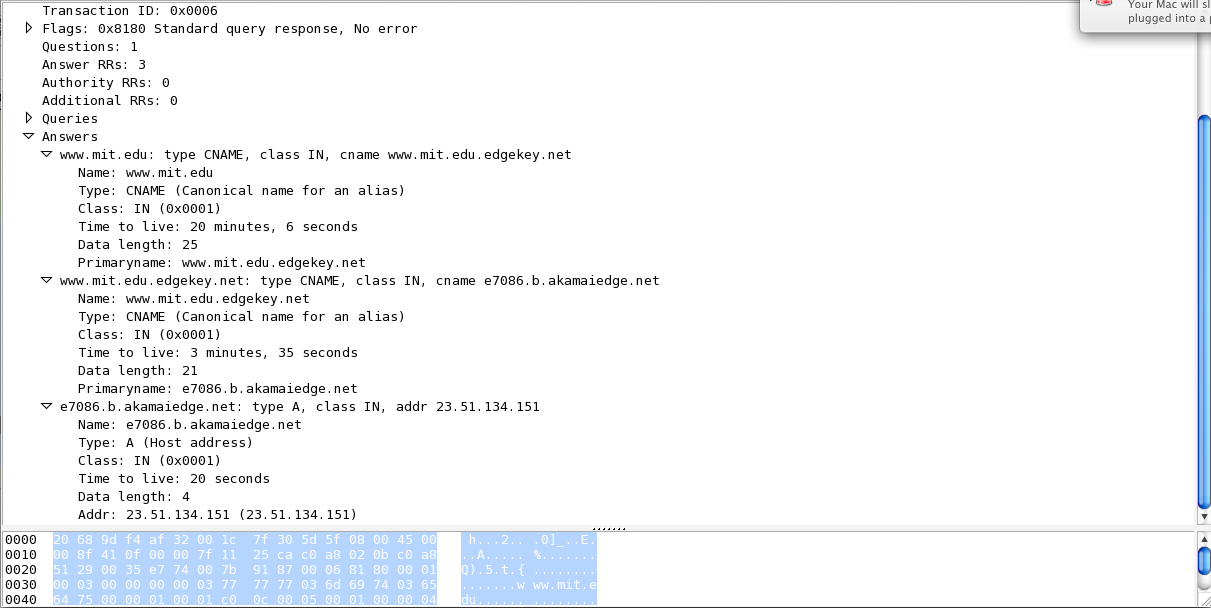
Question 3:

It is a Type A standard query. The query does not have any answers.

Question 4:

There are 3 answers. It contains information about the name, type, class, time to live, data length and domain name of the answer responses.

Question 5:



# nslookup with WireShark

Question 1:

192.168.2.11

No it is not (hostel) but yes (school).

Question 2:

It is a type NS standard query. The query does not have any answers.

Question 3:

It provides the following name servers:

* use2.akam.net
* usw2.akam.net
* use5.akam.net
* asia2.akam.net
* asia1.akam.net
* eur5.akam.net
* ns1-37.akam.net
* ns1-173.akam.net

Yes it provides IP addresses of 2 MIT name servers:

* use2.akam.net – 23.62.62.195
* eur5.akam.net – 23.74.25.64