Yiyun Yang

Z5187469

Ex3

**Question 1. What is the IP address of [www.eecs.berkeley.edu](https://eecs.berkeley.edu/). What type of DNS query is sent to get this answer?**

The IP address is 23.185.0.1.   
The type of DNS query is recursive query.

A screen shot of a smart phone

Description automatically generated

**Question 2. What is the canonical name for the eecs.berkeley web server? Suggest a reason for having an alias for this server.**

The canonical name for eecs.berkeley is live-eecs.pantheonsite.io.

IP aliasing is associating more than one IP address to a network interface. With this, one node on a network can have multiple connections to a network, each serving a different purpose.

**Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?**

We have 4 authoritative name servers for the domain name.

In the additional section, we have A and AAAA, which are IPv4 and IPv6 address.

A screen shot of a computer

Description automatically generated

**Question 4. What is the IP address of the local nameserver for your machine?**

The IP address of the local nameserver for my machine is 129.94.242.2.

**Question 5. What are the DNS nameservers for the “ [www.eecs.berkeley.edu](https://eecs.berkeley.edu/).” domain (note: the domain name is [eecs.berkeley.edu](https://eecs.berkeley.edu/)and not [www.eecs.berkeley.edu](https://eecs.berkeley.edu/))? Find out their IP addresses? What type of DNS query is sent to obtain this information?**

We have 5 DNS nameservers and the first two only have IPv4 address and last three have IPv4 and IPv6 address as highlighted. NS record is sent.

A screenshot of text

Description automatically generated

**Question 6. What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?**

It is DNS Reverse Look-up Using dig -x.

**Screen of a cell phone

Description automatically generated**

**Question 7. Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not [www.yahoo.com](http://www.yahoo.com/)). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)**

No, there is no aa flag for authoritative answer.

**A screenshot of a cell phone

Description automatically generated**

**Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?**

There is no response as the status is refused. This may be because eecs.berkeley prohibit users performing DNS queries outside its network.

**A screenshot of a cell phone

Description automatically generated**

**Question 9. Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?**

**A screen shot of a computer

Description automatically generated**

**Question 10. In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?**

Total 5 requests:

dig NS 🡪 a.root-servers.net

dig @198.41.0.4 lyre00.cse.unsw.edu.au 🡪 a.au

dig @58.65.254.73 lyre00.cse.unsw.edu.au 🡪 q.au

dig @65.22.196.1 lyre00.cse.unsw.edu.au 🡪 ns1.unsw.edu.au.

dig @129.94.0.192 lyre00.cse.unsw.edu.au 🡪 beethoven.orchestra.cse.unsw.edu.au.

dig @129.94.208.3 lyre00.cse.unsw.edu.au 🡪 129.94.210.20

**Question 11. Can one physical machine have several names and/or IP addresses associated with it?**

Yes, one physical machine can have several names and IP addresses associated with it.