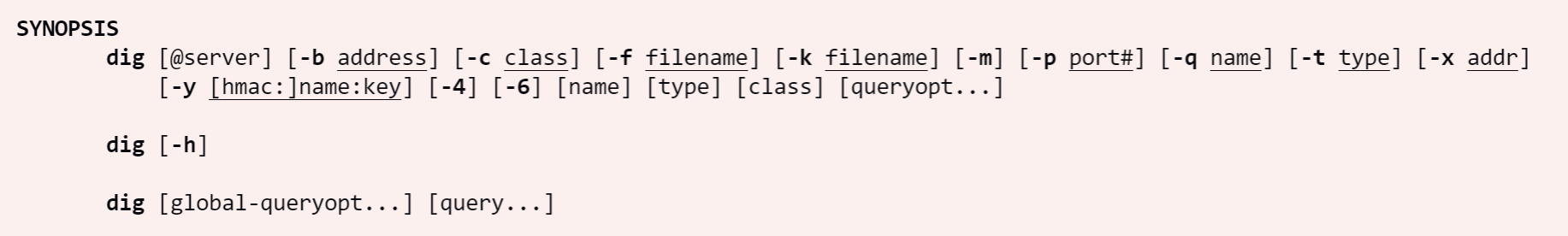
Lab 3

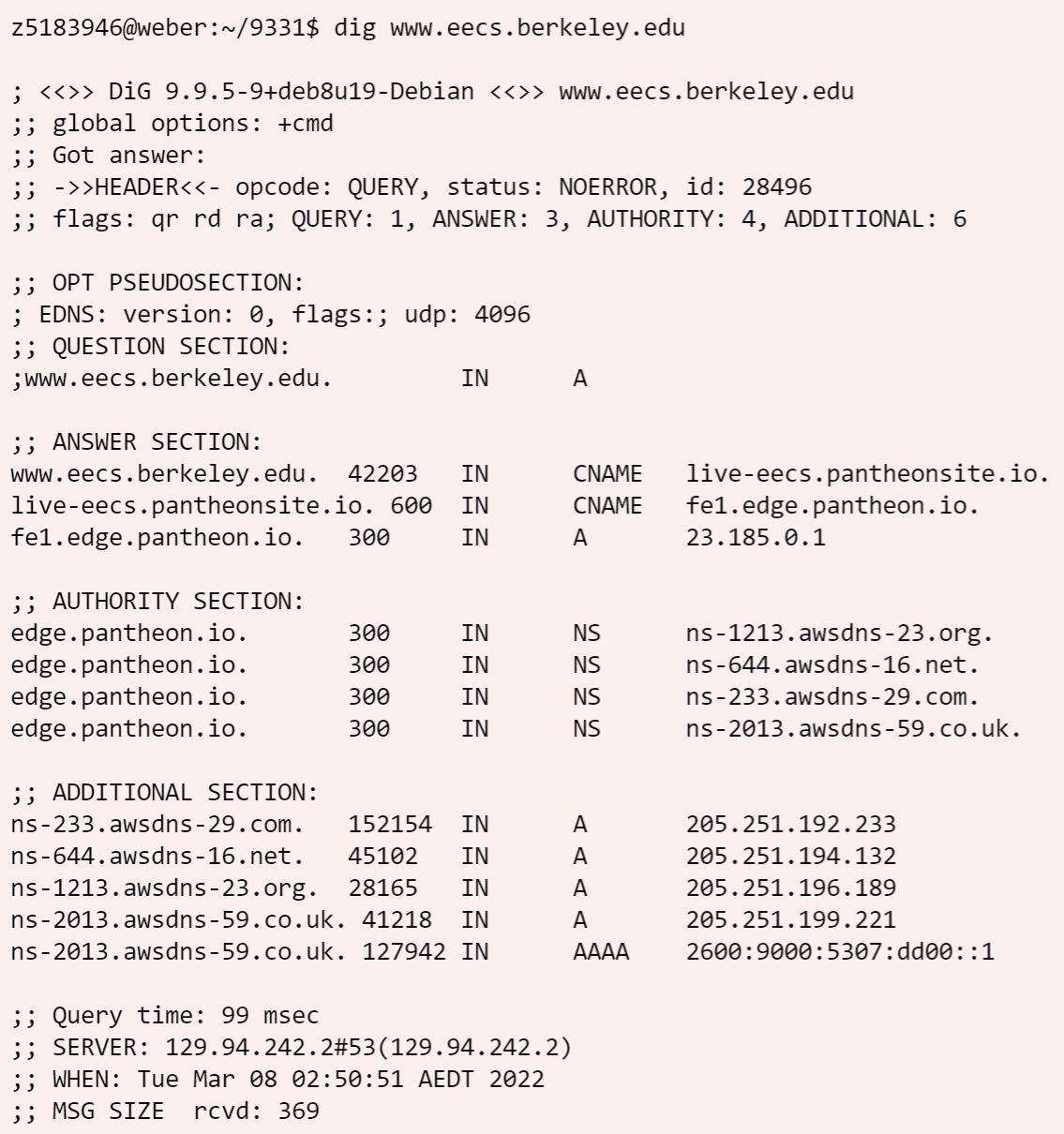
# Exercise 3

man dig returns the usage synopsis of dig.



## 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 image above is the output of **dig www.eecs.berkeley.edu**. The IP address is 23.185.0.1. Type A query is sent to the name server to get this answer.

## Question 2

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

The canonical name for www.eecs.berkeley.edu is live-eecs.pantheonsite.io and the canonical name for live-eecs.pantheonsite.io is fe1.edge.pantheon.io.

One of the reasons for having an alias is to adapt the changing IP. There are two scenarios: The first one is that multiple websites are bound to one server machine. When the IP address changes, the manager only needs to change the record once by changing the type A record of the server machine instead of updating the record of each website separately. The second case is that the website owner may not own the IP, the IP provider may change the address at any time, then they can use alias to bind their website to the provider. By doing this, no change is required when then provider changes the IP address.

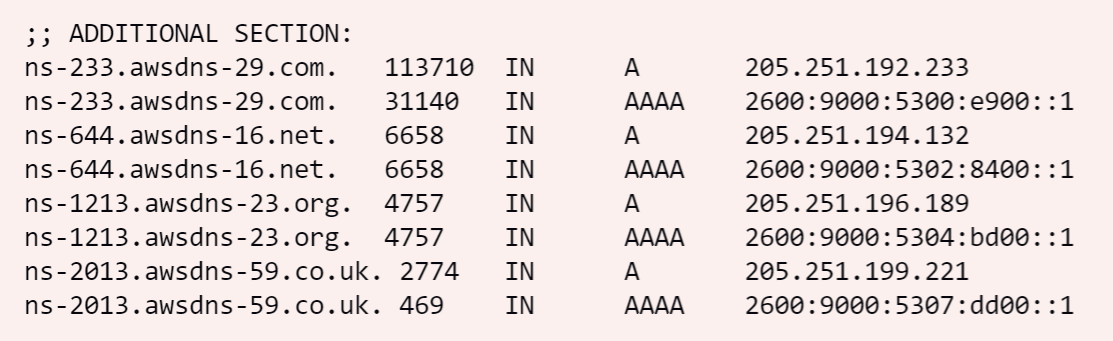
## Question 3

*What can you make of the rest of the response?*

As shown in authority section, there are four servers for answering DNS queries about www.eecs.berkeley.edu which are: ns-644.awsdns-16.net, ns-233.awsdns-29.com, ns-1213.awsdns-23.org, and ns-2013.awsdns-59.co.uk. They are all amazon DNS server.

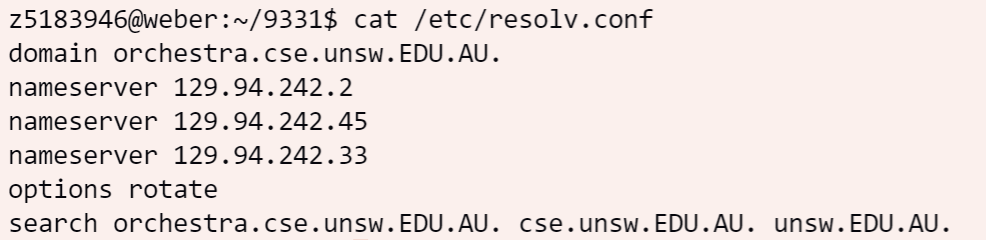
~~As indicated in the additional section ns-2013.awsdns-59.co.uk also supports IPv6.~~

**Update**: According to the result in additional section from another run few days later, it shows that all these four DNS servers support IPv6.



## Question 4

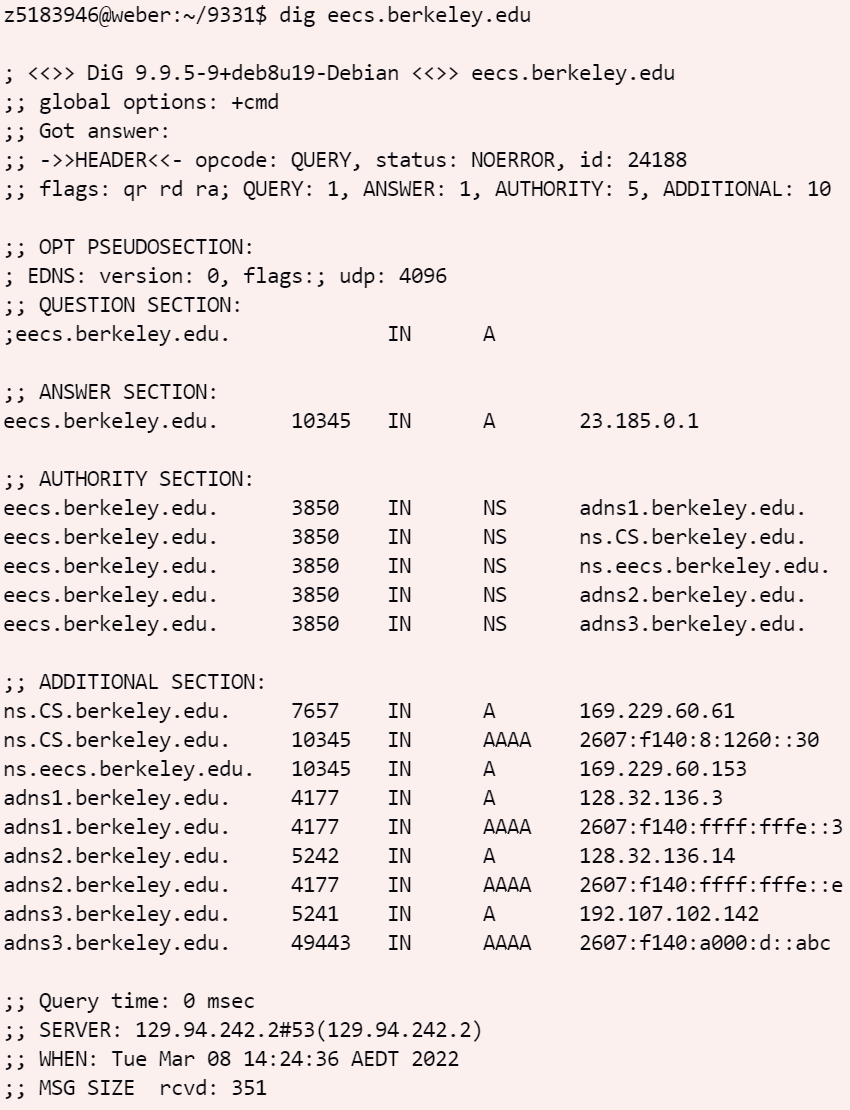
*What is the IP address of the local nameserver for your machine?*



From the result of *cat /etc/resolv.conf,* The IP addresses of the local nameserver for my machine are **129.94.242.2**, **129.94.242.45**, and **129.94.242.33**. The primary local nameserver is **129.94.242.2**.

## Question 5

*What are the DNS nameservers for the “eecs.berkeley.edu.” domain? Find out their IP addresses? What type of DNS query is sent to obtain this information?*



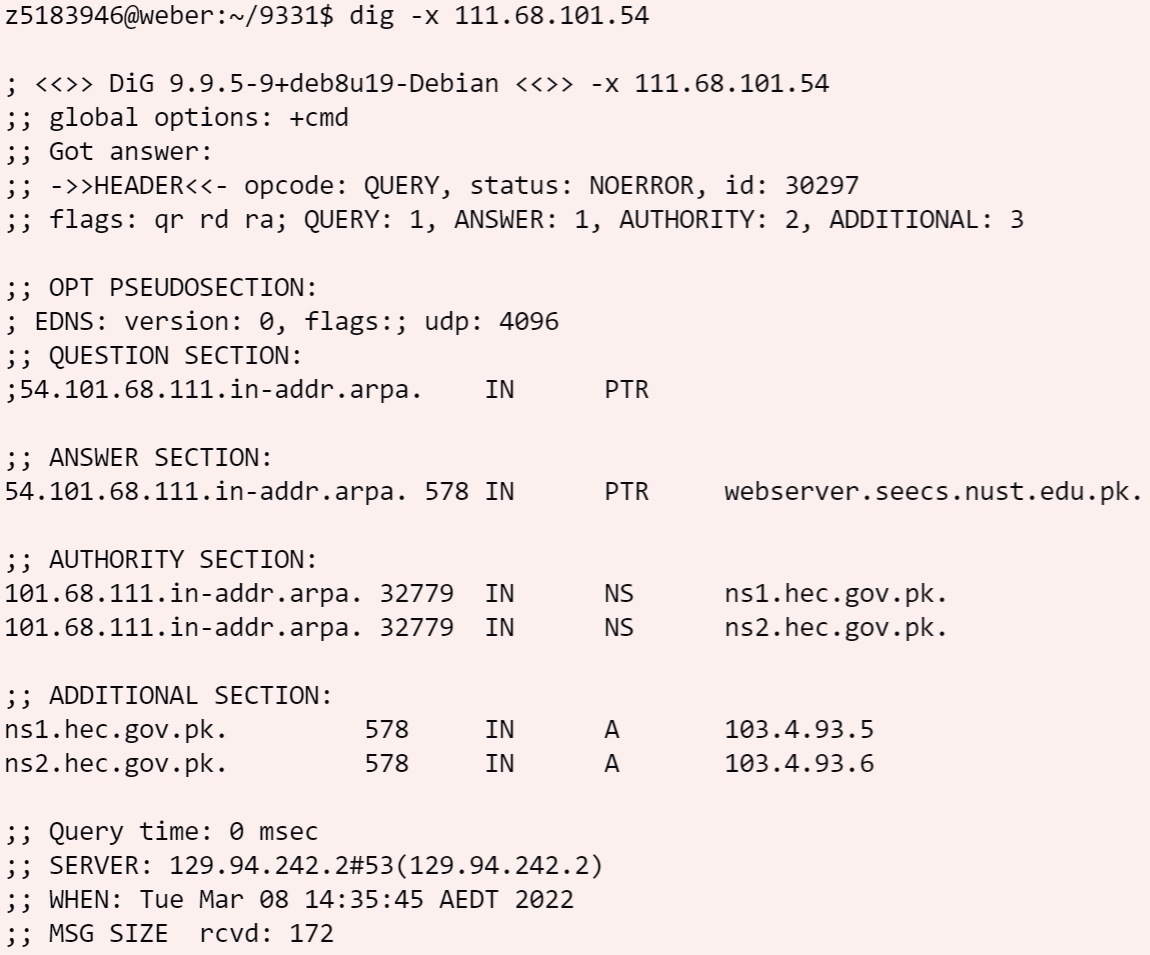
From the output of *dig eecs.berkeley.edu* we can deduce that the nameservers and their IP addresses as follows:

|  |  |  |
| --- | --- | --- |
| Name | IPv4 | IPv6 |
| adns1.berkeley.edu | 128.32.136.3 | 2607:f140:ffff:fffe::3 |
| ns.CS.berkeley.edu | 169.229.60.61 | 2607:f140:8:1260::30 |
| ns.eecs.berkeley.edu | 169.229.60.153 | - |
| adns2.berkeley.edu | 128.32.136.14 | 2607:f140:ffff:fffe::e |
| adns3.berkeley.edu | 192.107.102.142 | 2607:f140:a000:d::abc |

Type **A** query is used to obtain this information.

## Question 6

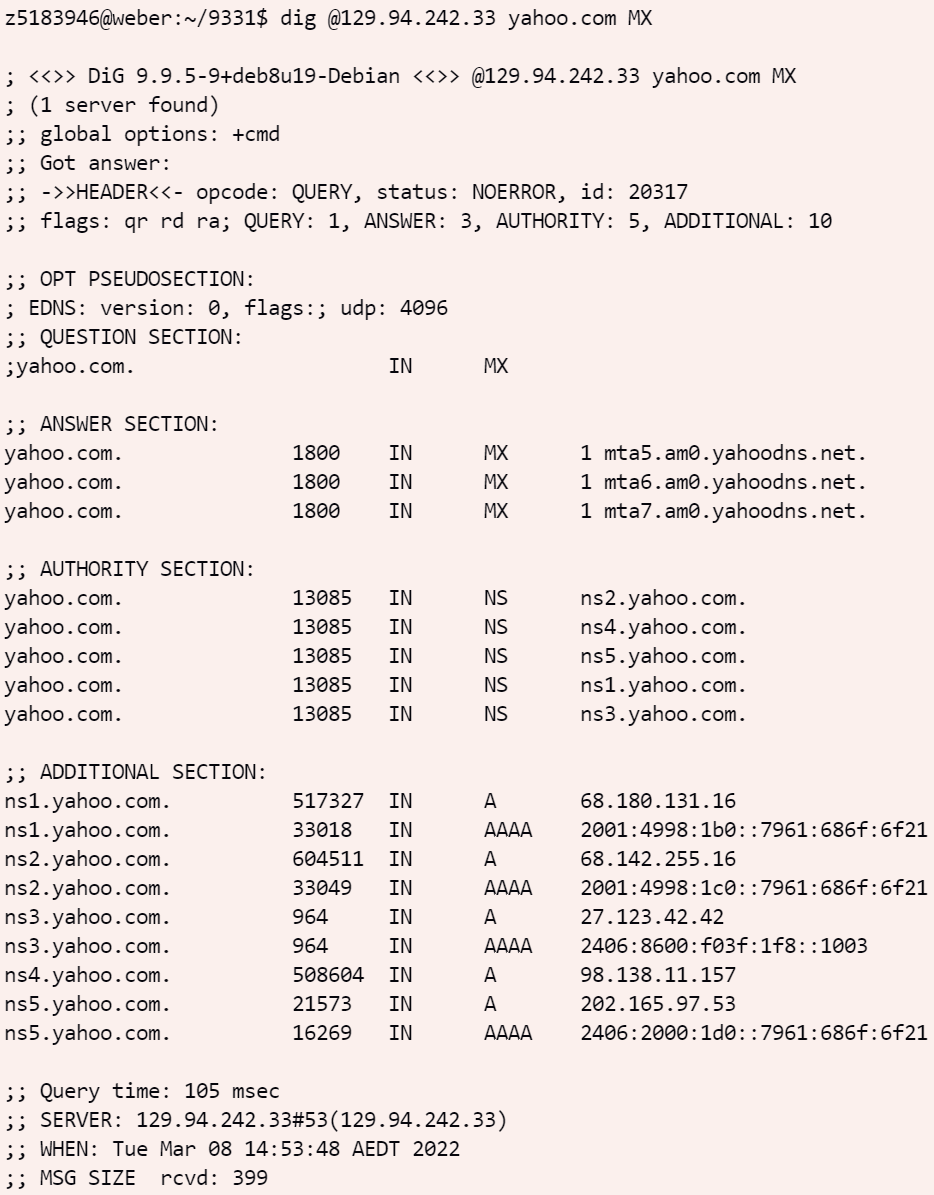
*What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?*



According to answer section in the output from *dig -x 111.68.101.54,* the DNS name associated with 111.68.101.54 is **webserver.seecs.nust.edu.pk**. **PTR** query is sent to obtain this information.

## Question 7

*Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail. Did you get an authoritative answer? Why?*

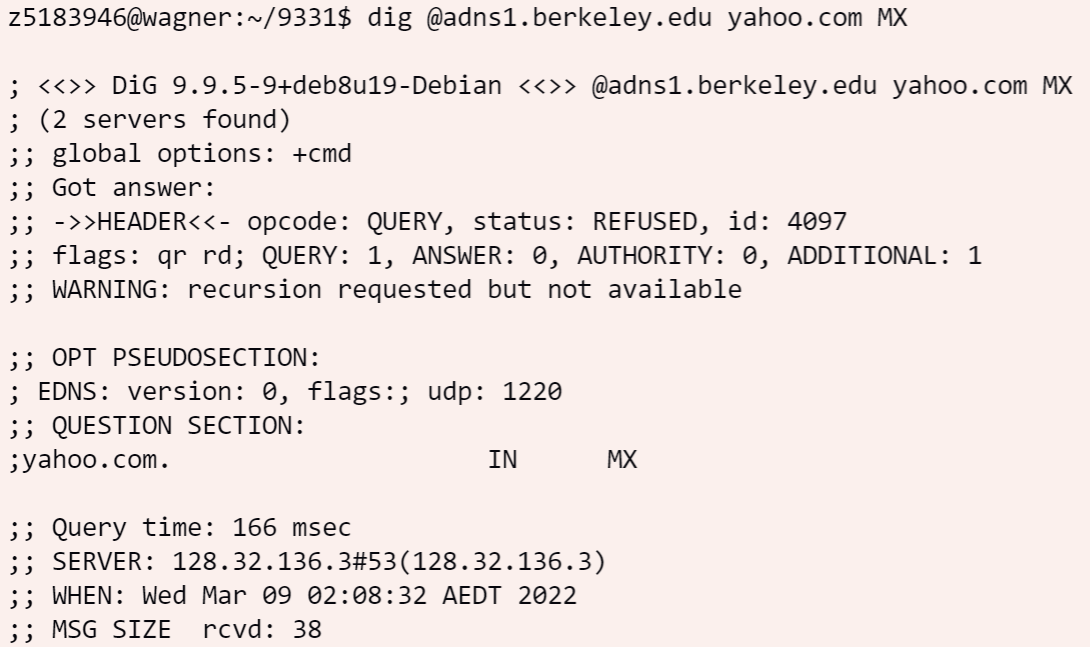


After running *dig @129.94.242.33 yahoo.com MX*, we can see that the answer is **not authoritative** because **aa** (Authoritative Answer) is not included in flags field.

## Question 8

*Repeat the above but use one of the nameservers obtained in Question 5. What is the result?*

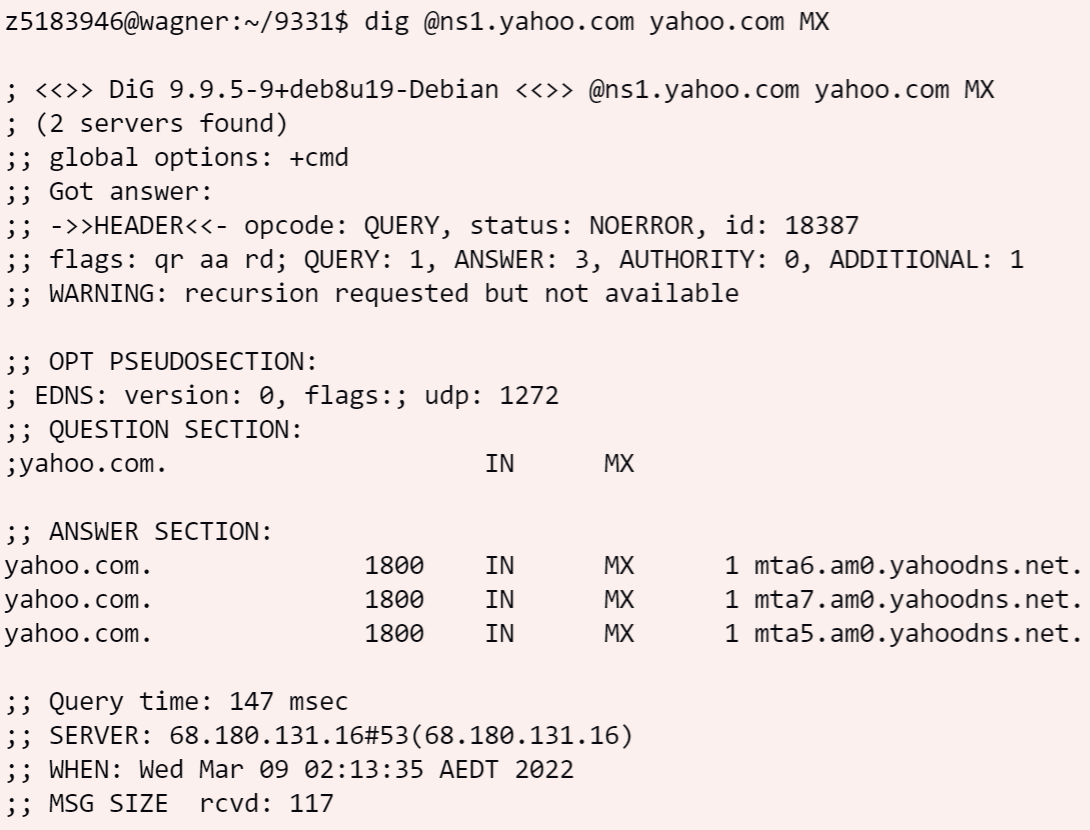
For this question, I picked 128.32.136.3 (adns1.berkeley.edu) as the nameserver, and the answer from command *dig @169.229.60.61 yahoo.com MX* shows that the query is refused in the status field. The reason might be that CSE machine doesn’t have permission to access that nameserver of Berkeley.



## Question 9

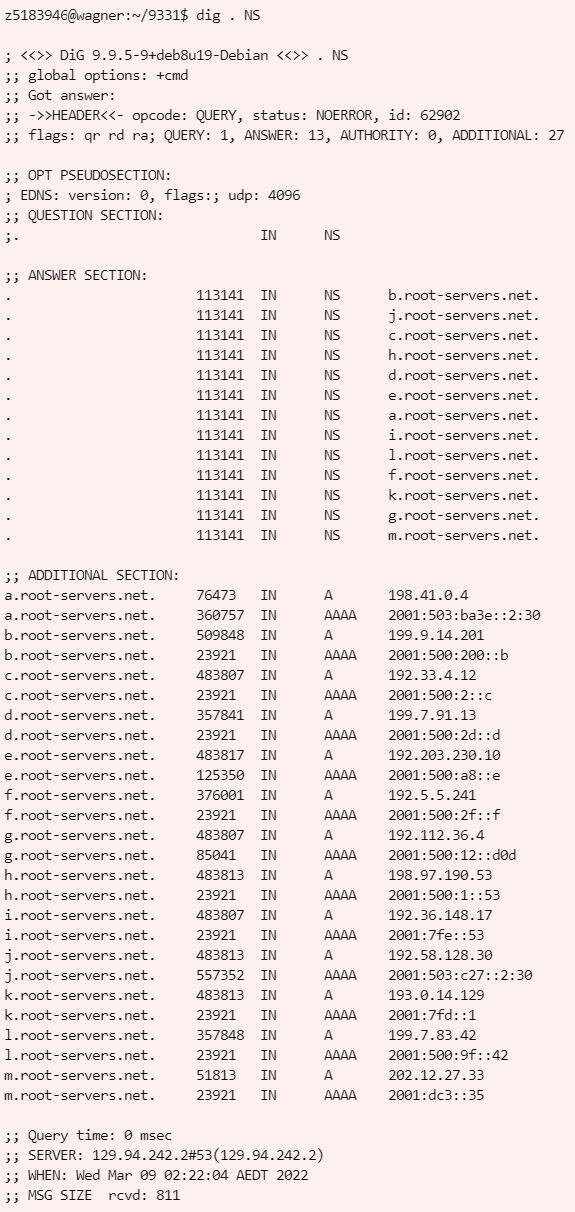
*Obtain the authoritative answer for the mail servers for Yahoo! Mail. What type of DNS query is sent to obtain this information?*

Use the authoritative server of yahoo provides the authoritative answer. It is achieved by sending the **MX** query: *dig @ns1.yahoo.com yahoo.com MX.*

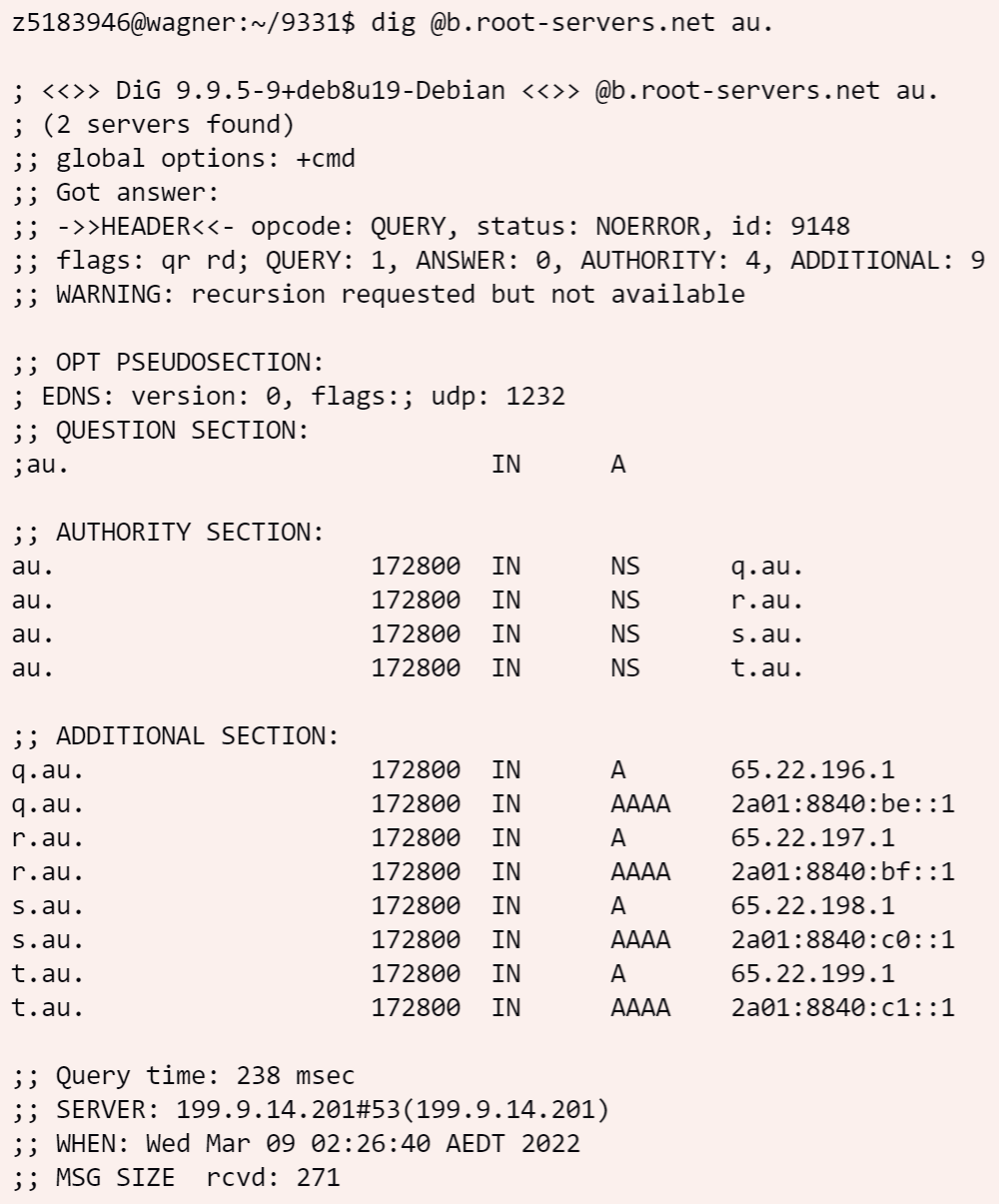


## Question 10

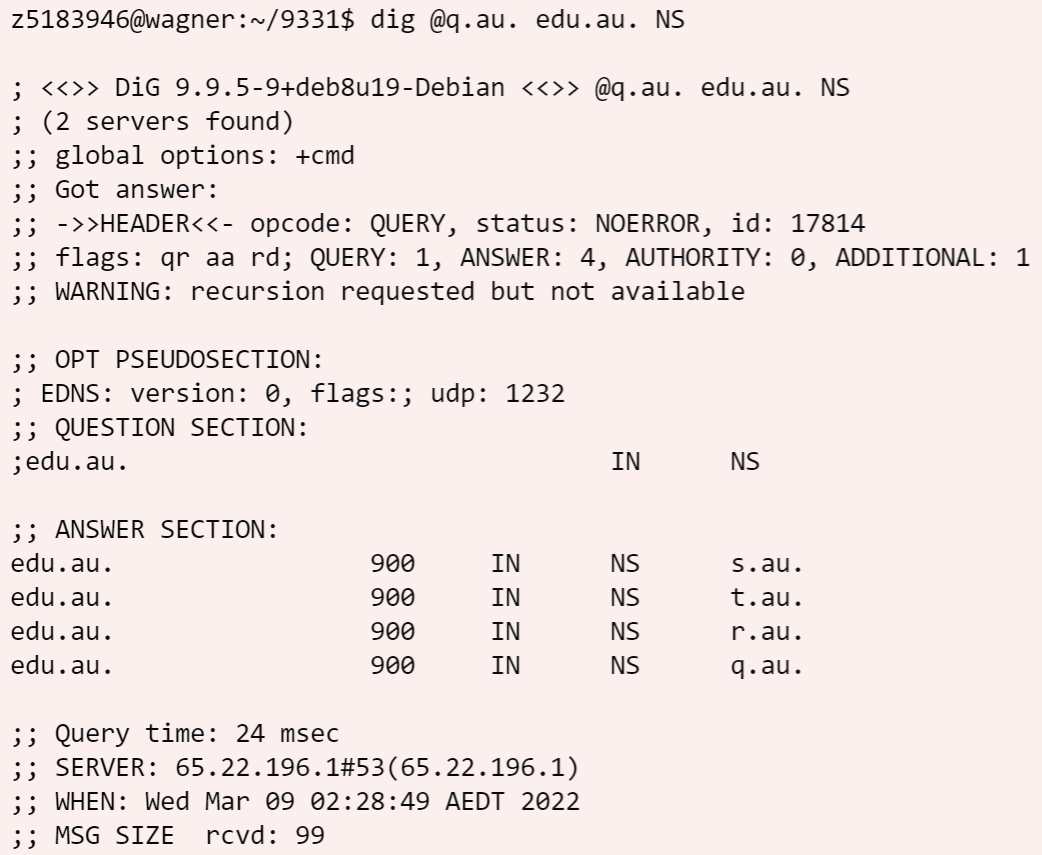
To find the IP address of *lyre00.cse.unsw.edu.au* iteratively, we need to find the root nameserver first. The root nameserver can be found by running *dig . NS*:



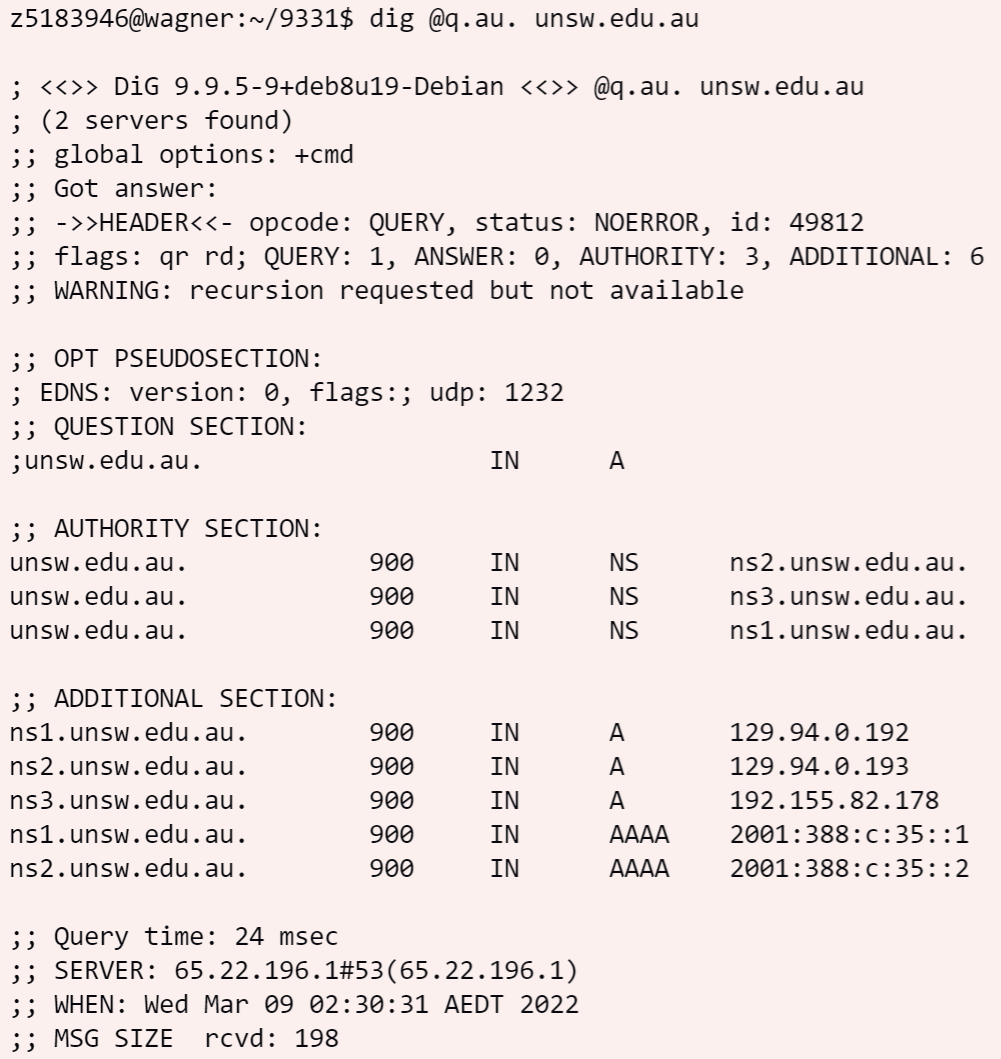
Then, query the root server(b.root-servers.net) to get the authoritative name server for the "au." Domain by running *dig @b.root-servers.net au.*:



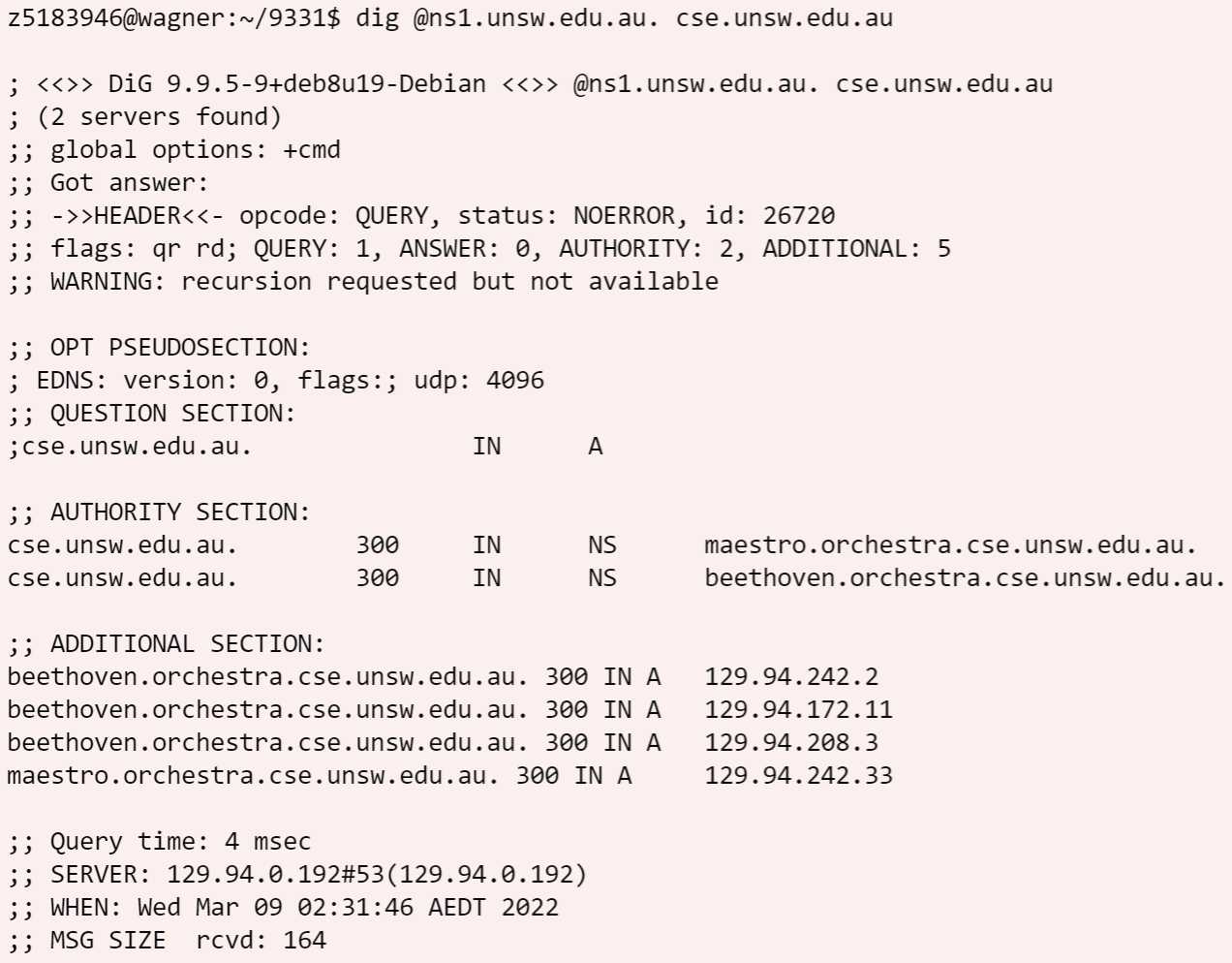
Query this second server(q.au.) to find the authoritative nameserver for the "edu.au." domain, from the result we can see that q.au. is still responsible for “edu.au” domain.



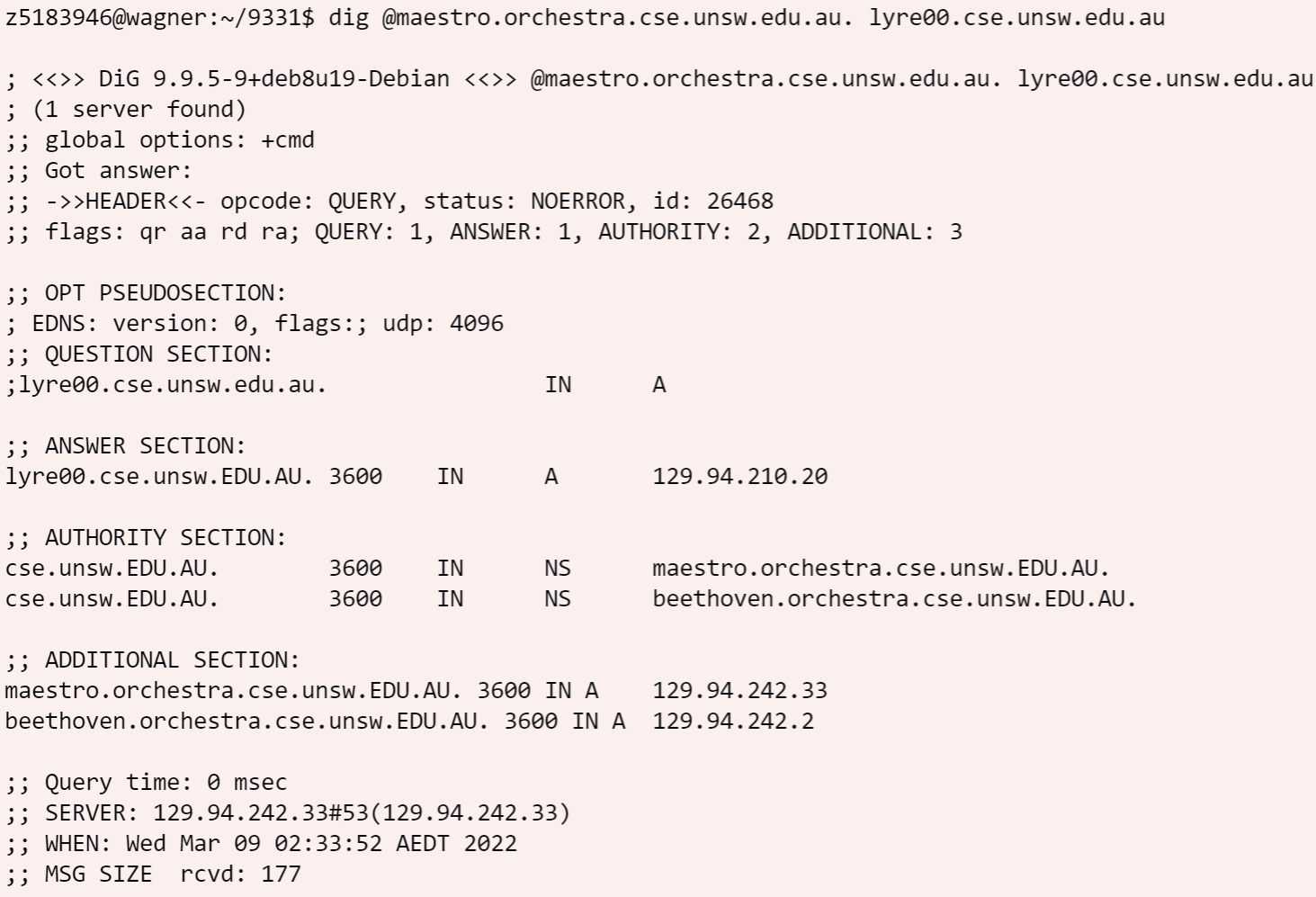
Then query q.au. for ”unsw.edu.au”:



Then query *ns1.unsw.edu.au* for authoritative server for cse.unsw.edu.au:



Finally, query *maestro.orchestra.cse.unsw.edu.au.* for the IP address for *lyre00.cse.unsw.edu.au*:



Then we get the desired IP address: **129.94.210.20**.

To get the authoritative answer, there are **4** name servers used, that are:

*b.root-servers.net au.*

*q.au.*

*ns1.unsw.edu.au.*

*maestro.orchestra.cse.unsw.edu.au.*

With *q.au.* queried twice, for au. and edu.au respectively.

## Question 11

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

One physical machine can have multiple names associated with it. The machine manager just needs to set several type A records all having IP address of this machine as value but with different names. They can also use CNAME to create alias easily for one machine.

It can also have several IP addresses associated with. Because each network interface can be assigned with a IP address and a machine may have multiple interface installed.