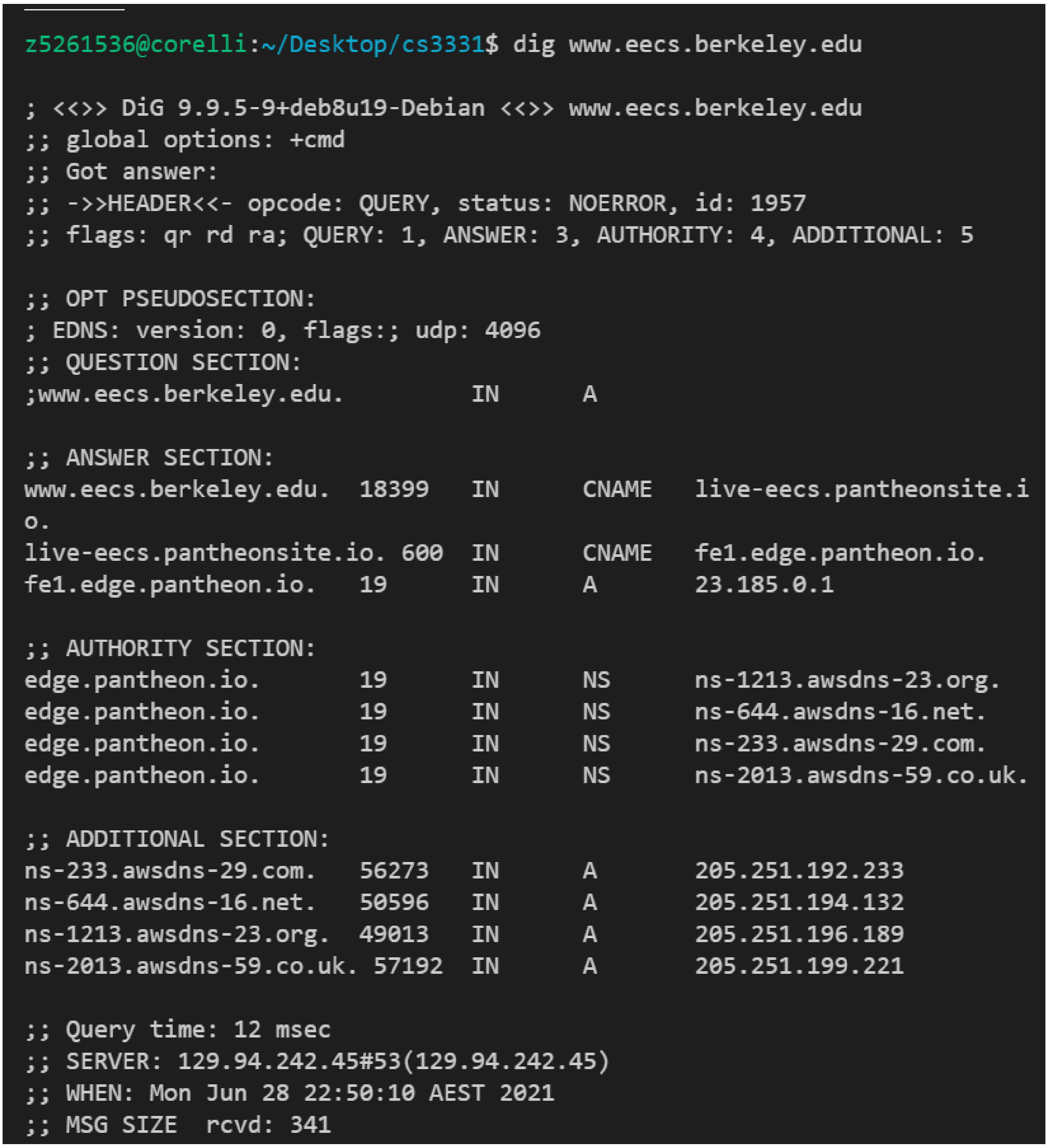
Lab Exercise 3: DNS & Socket Programming

Exercise 3: Digging into DNS

Question 1. What is the IP address of www.eecs.berkeley.edu. What type of DNS query is sent to get this answer?

The IP address of the website is 23.185.0.01

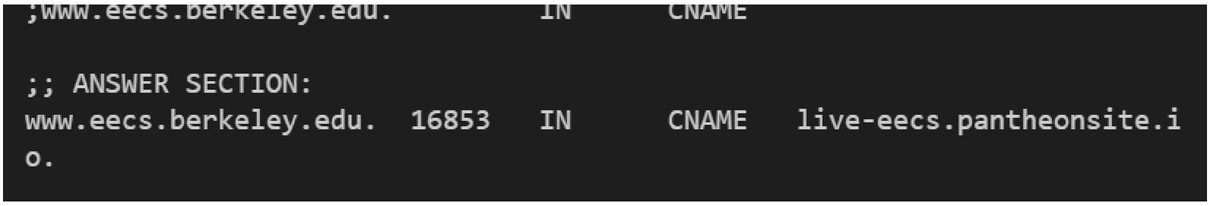
The type of DNS query sent to get this answer is A record type.



```
z5261536@corelli:~/Desktop/cs3331$ dig www.eecs.berkeley.edu

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> www.eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1957
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.eecs.berkeley.edu.         IN      A

;; ANSWER SECTION:
www.eecs.berkeley.edu.  18399   IN      CNAME   live-eecs.pantheonsite.i
o.
live-eecs.pantheonsite.io. 600  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   19      IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       19      IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       19      IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       19      IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       19      IN      NS      ns-2013.awsdns-59.co.uk.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   56273   IN      A       205.251.192.233
ns-644.awsdns-16.net.   50596   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  49013   IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 57192  IN      A       205.251.199.221

;; Query time: 12 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 28 22:50:10 AEST 2021
;; MSG SIZE  rcvd: 341
```

Question 2. What is the canonical name for the eecs.berkeley webserver (i.e. www.eecs.berkeley.edu)? Suggest a reason for having an alias for this server.

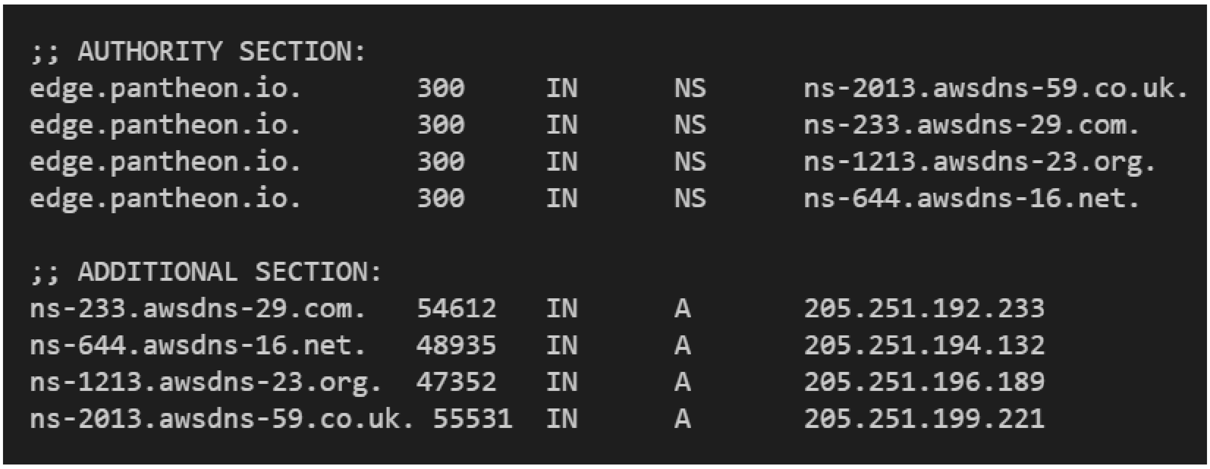
Canonical name for the webserver is live-eecs.pantheonsite.io.



```
;www.eecs.berkeley.edu.         IN      CNAME

;; ANSWER SECTION:
www.eecs.berkeley.edu.  16853   IN      CNAME   live-eecs.pantheonsite.i
o.
```

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

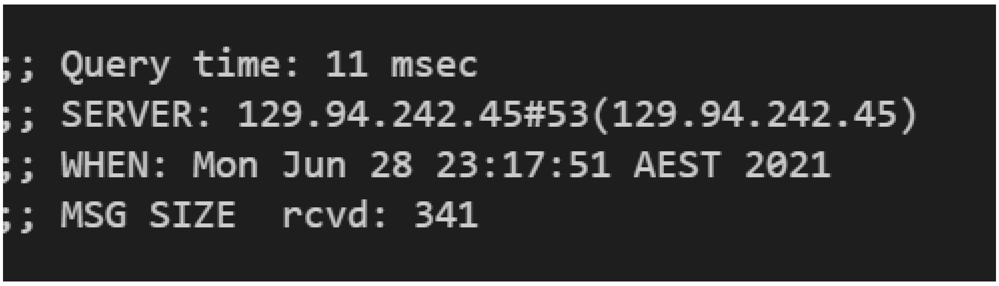
The Authority section indicates the servers **like ns-2013.awsdns-59.co.uk. , ns-233.awsdns-29.com.** that are the ultimate authority of answering DNS queries about that domain **edge.pantheon.io**. And the Additional section displays all these authoritative servers like **ns-233.awsdns-29.com.** with their IP addresses.



```
;; AUTHORITY SECTION:
edge.pantheon.io.       300     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       300     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       300     IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       300     IN      NS      ns-644.awsdns-16.net.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   54612   IN      A       205.251.192.233
ns-644.awsdns-16.net.   48935   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  47352   IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 55531  IN      A       205.251.199.221
```

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

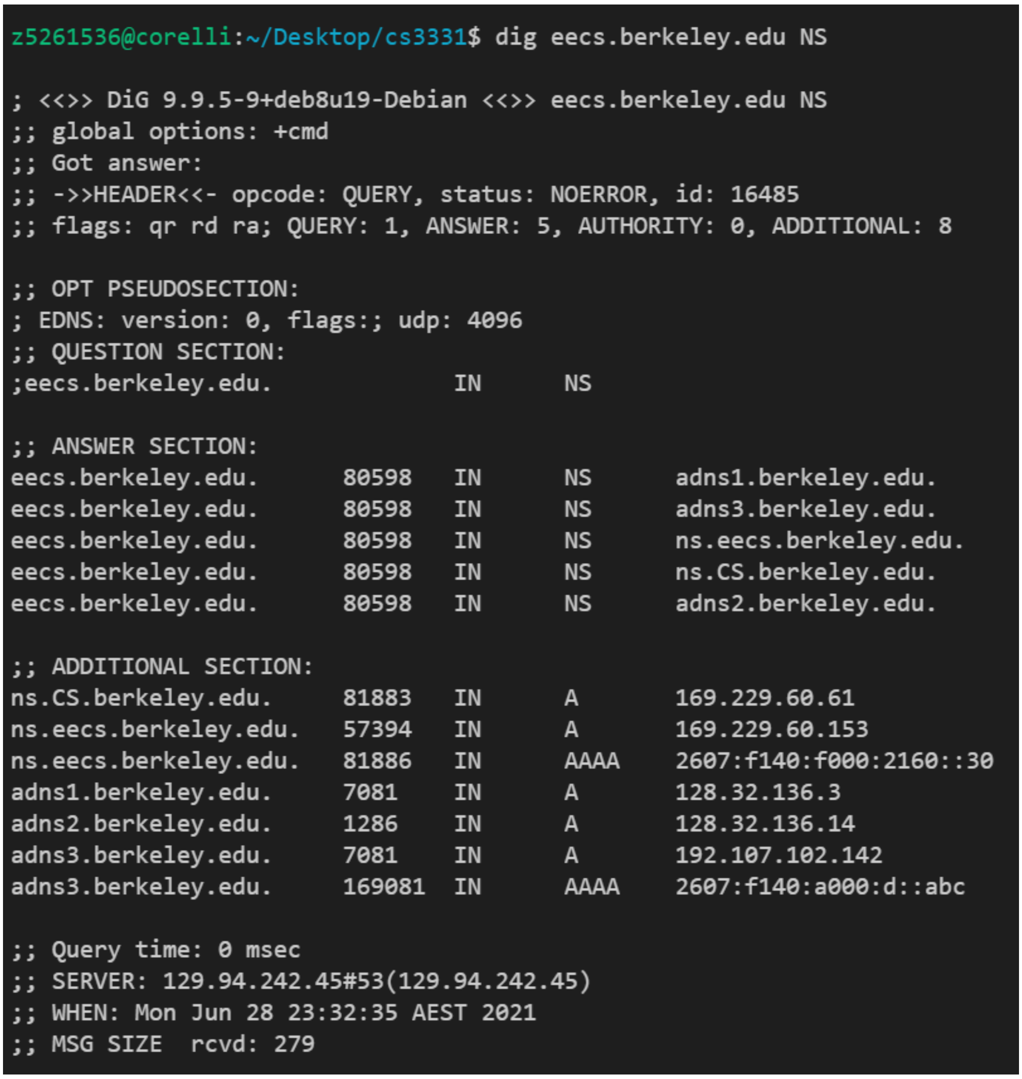
129.94.242.45



```
;; Query time: 11 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 28 23:17:51 AEST 2021
;; MSG SIZE  rcvd: 341
```

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?

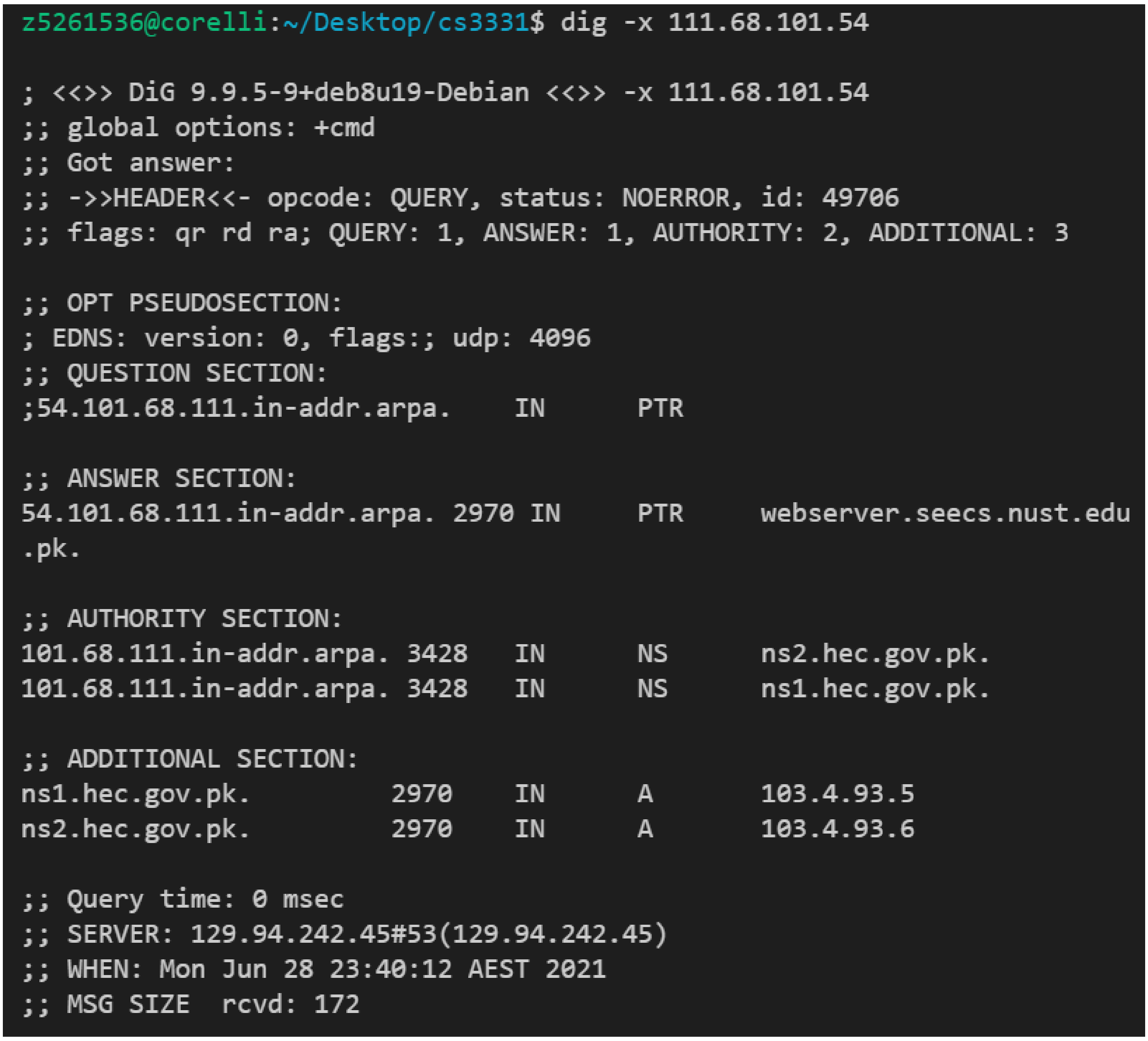
DNS nameserver			Type	IP addresses
ns.CS.berkeley.edu.	81883	IN	A	169.229.60.61
ns.eecs.berkeley.edu.	57394	IN	A	169.229.60.153
ns.eecs.berkeley.edu.	81886	IN	AAAA	2607:f140:f000:2160::30
adns1.berkeley.edu.	7081	IN	A	128.32.136.3
adns2.berkeley.edu.	1286	IN	A	128.32.136.14
adns3.berkeley.edu.	7081	IN	A	192.107.102.142
adns3.berkeley.edu.	169081	IN	AAAA	2607:f140:a000:d::abc



```
z5261536@corelli:~/Desktop/cs3331$ dig eecs.berkeley.edu NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> eecs.berkeley.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16485
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;eecs.berkeley.edu.             IN      NS

;; ANSWER SECTION:
eecs.berkeley.edu.      80598   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      80598   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      80598   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      80598   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      80598   IN      NS      adns2.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     81883   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   57394   IN      A       169.229.60.153
ns.eecs.berkeley.edu.   81886   IN      AAAA    2607:f140:f000:2160::30
adns1.berkeley.edu.     7081    IN      A       128.32.136.3
adns2.berkeley.edu.     1286    IN      A       128.32.136.14
adns3.berkeley.edu.     7081    IN      A       192.107.102.142
adns3.berkeley.edu.     169081  IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 28 23:32:35 AEST 2021
;; MSG SIZE  rcvd: 279
```

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?

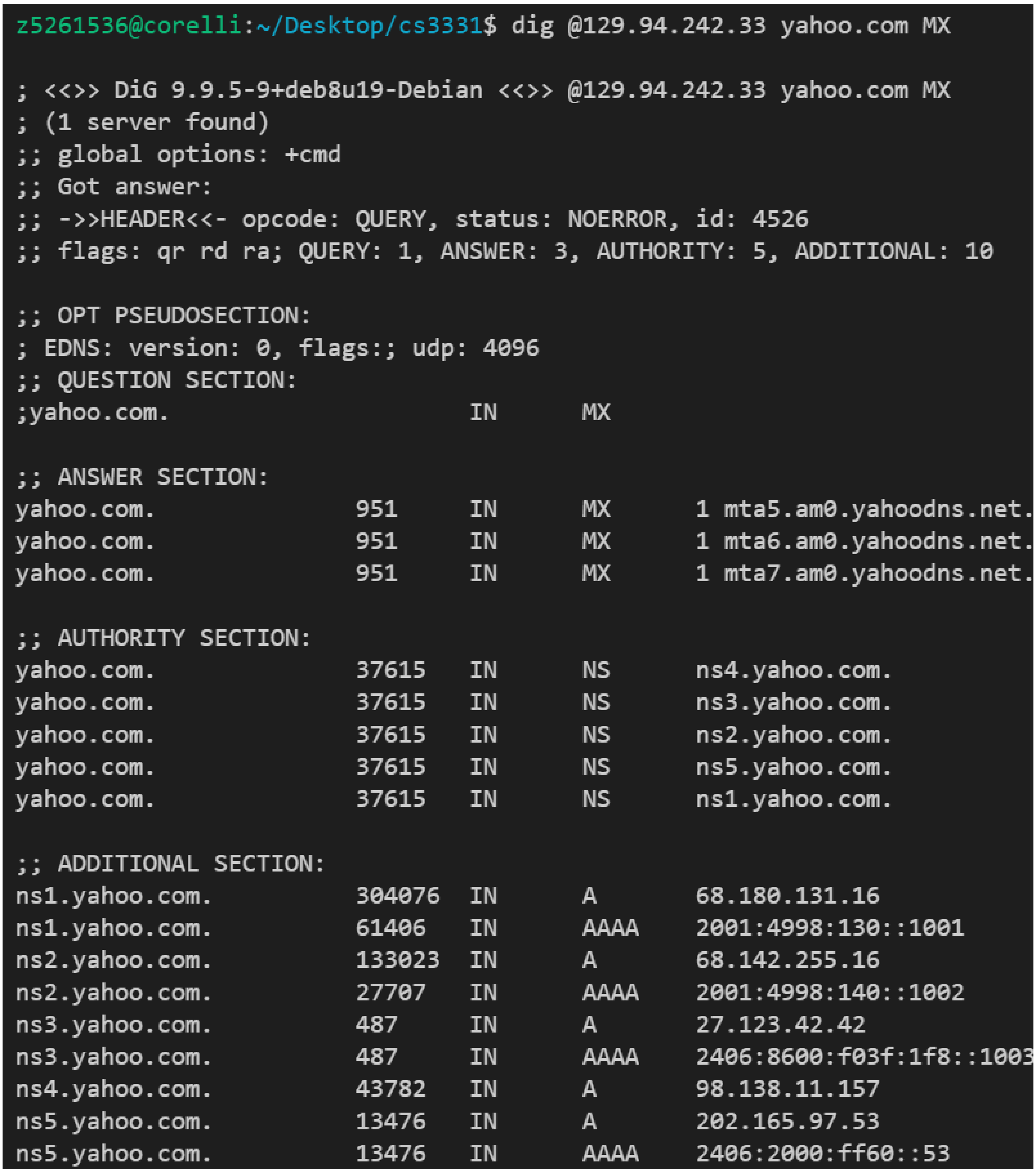
DNS name: webserver.seecs.nust.edu.pk. Type of DNS query: PTR



```
z5261536@corelli:~/Desktop/cs3331$ dig -x 111.68.101.54

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49706
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;54.101.68.111.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 2970 IN     PTR     webserver.seecs.nust.edu
.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 3428   IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 3428   IN      NS      ns1.hec.gov.pk.

;; ADDITIONAL SECTION:
ns1.hec.gov.pk.         2970    IN      A       103.4.93.5
ns2.hec.gov.pk.         2970    IN      A       103.4.93.6

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 28 23:40:12 AEST 2021
;; MSG SIZE  rcvd: 172
```

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). 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)

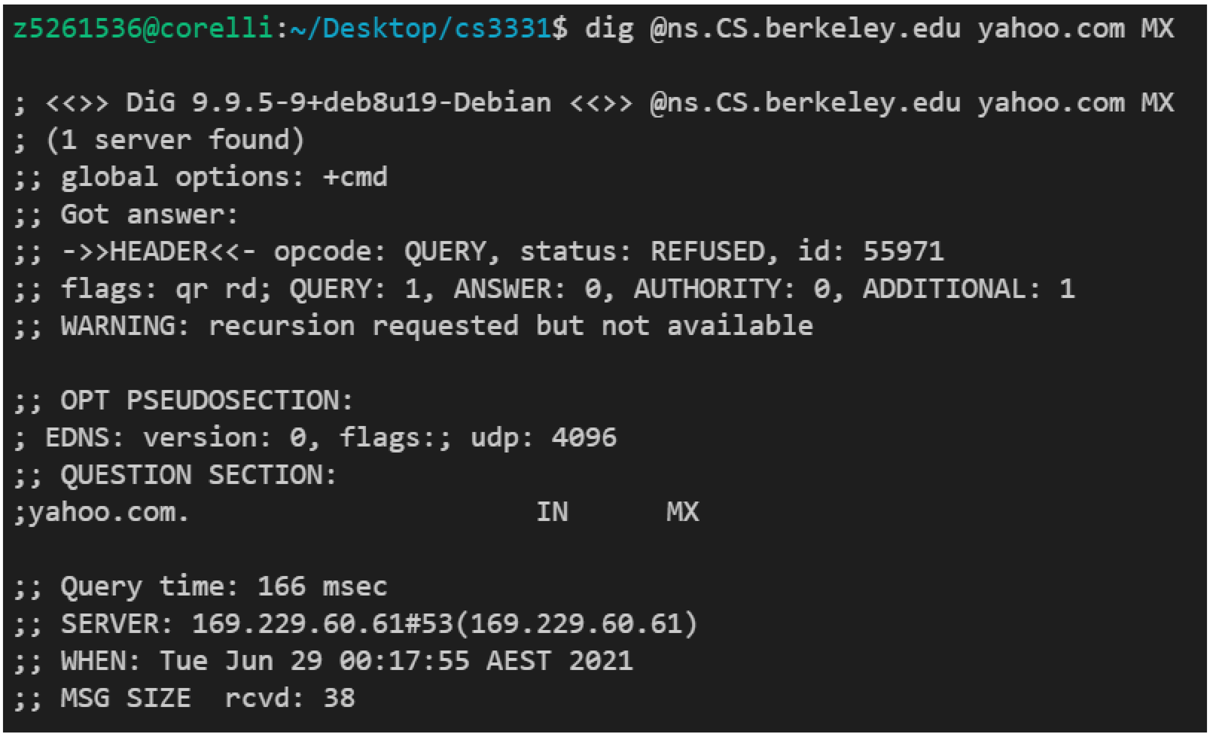
From the flags in the response, we get qr, rd, ra which stand for query, recursion desired and recursion available. However, they don't have a flag called aa – authoritative answer, so I didn't get an authoritative answer.



```
z5261536@corelli:~/Desktop/cs3331$ dig @129.94.242.33 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4526
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              951     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              951     IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              951     IN      MX      1 mta7.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              37615   IN      NS      ns4.yahoo.com.
yahoo.com.              37615   IN      NS      ns3.yahoo.com.
yahoo.com.              37615   IN      NS      ns2.yahoo.com.
yahoo.com.              37615   IN      NS      ns5.yahoo.com.
yahoo.com.              37615   IN      NS      ns1.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          304076  IN      A       68.180.131.16
ns1.yahoo.com.          61406   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          133023  IN      A       68.142.255.16
ns2.yahoo.com.          27707   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          487     IN      A       27.123.42.42
ns3.yahoo.com.          487     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          43782   IN      A       98.138.11.157
ns5.yahoo.com.          13476   IN      A       202.165.97.53
ns5.yahoo.com.          13476   IN      AAAA    2406:2000:ff60::53
```

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

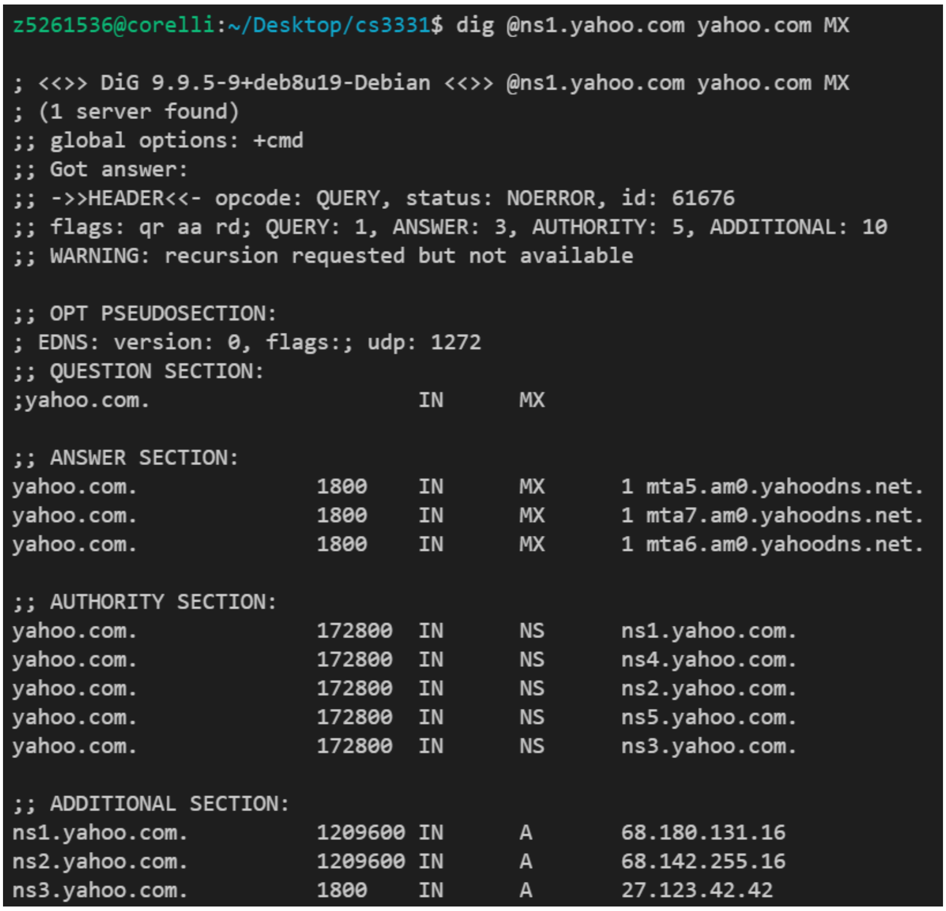
Assume we use the name server **ns.CS.berkeley.edu** obtained in Q5, and the result is below, I didn’t get an answer.



```
z5261536@corelli:~/Desktop/cs3331$ dig @ns.CS.berkeley.edu yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns.CS.berkeley.edu yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 55971
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 166 msec
;; SERVER: 169.229.60.61#53(169.229.60.61)
;; WHEN: Tue Jun 29 00:17:55 AEST 2021
;; MSG SIZE  rcvd: 38
```

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 MX type of DNS query is sent to obtain this information.

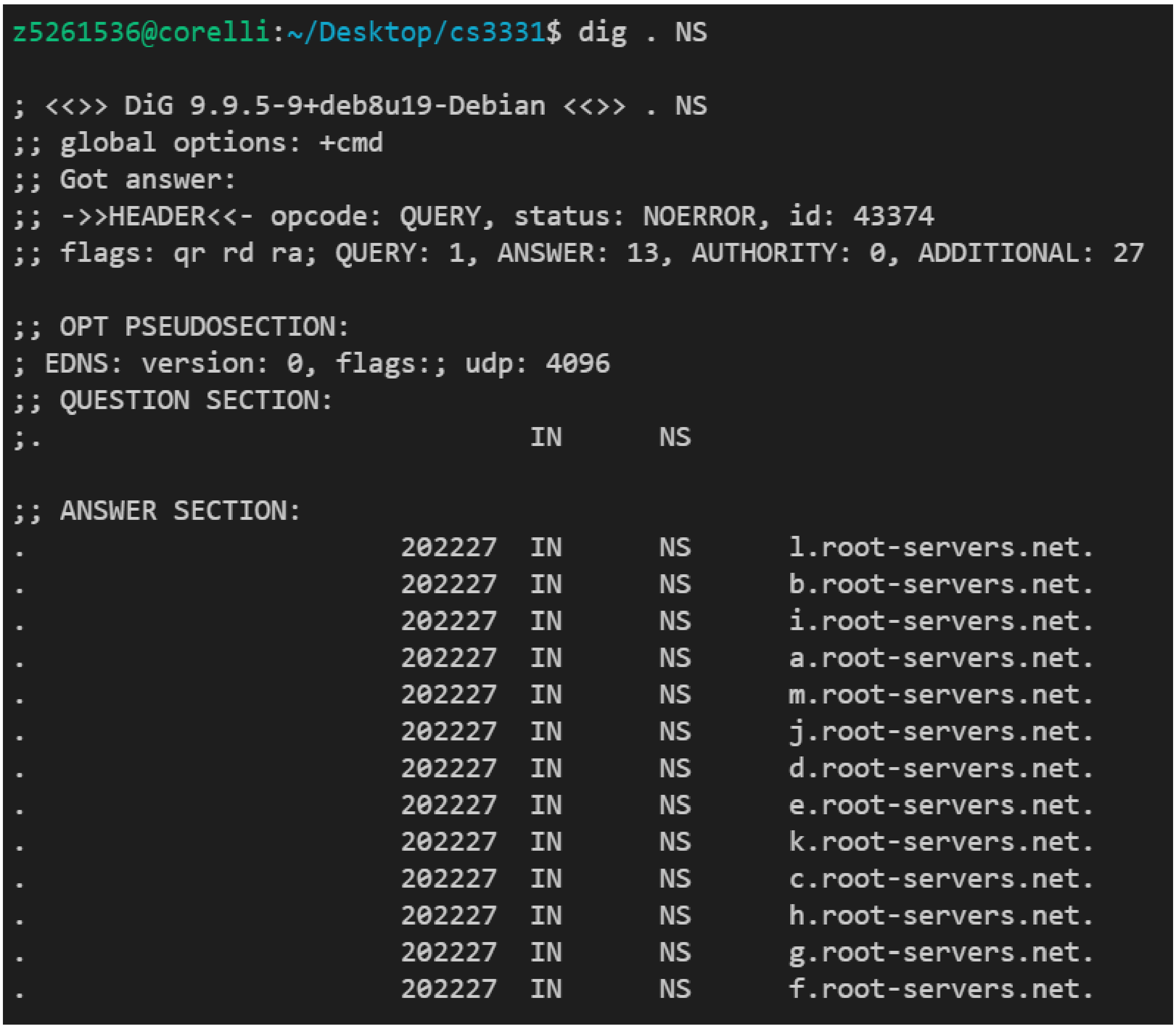


```
z5261536@corelli:~/Desktop/cs3331$ dig @ns1.yahoo.com yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61676
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
```

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). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.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?

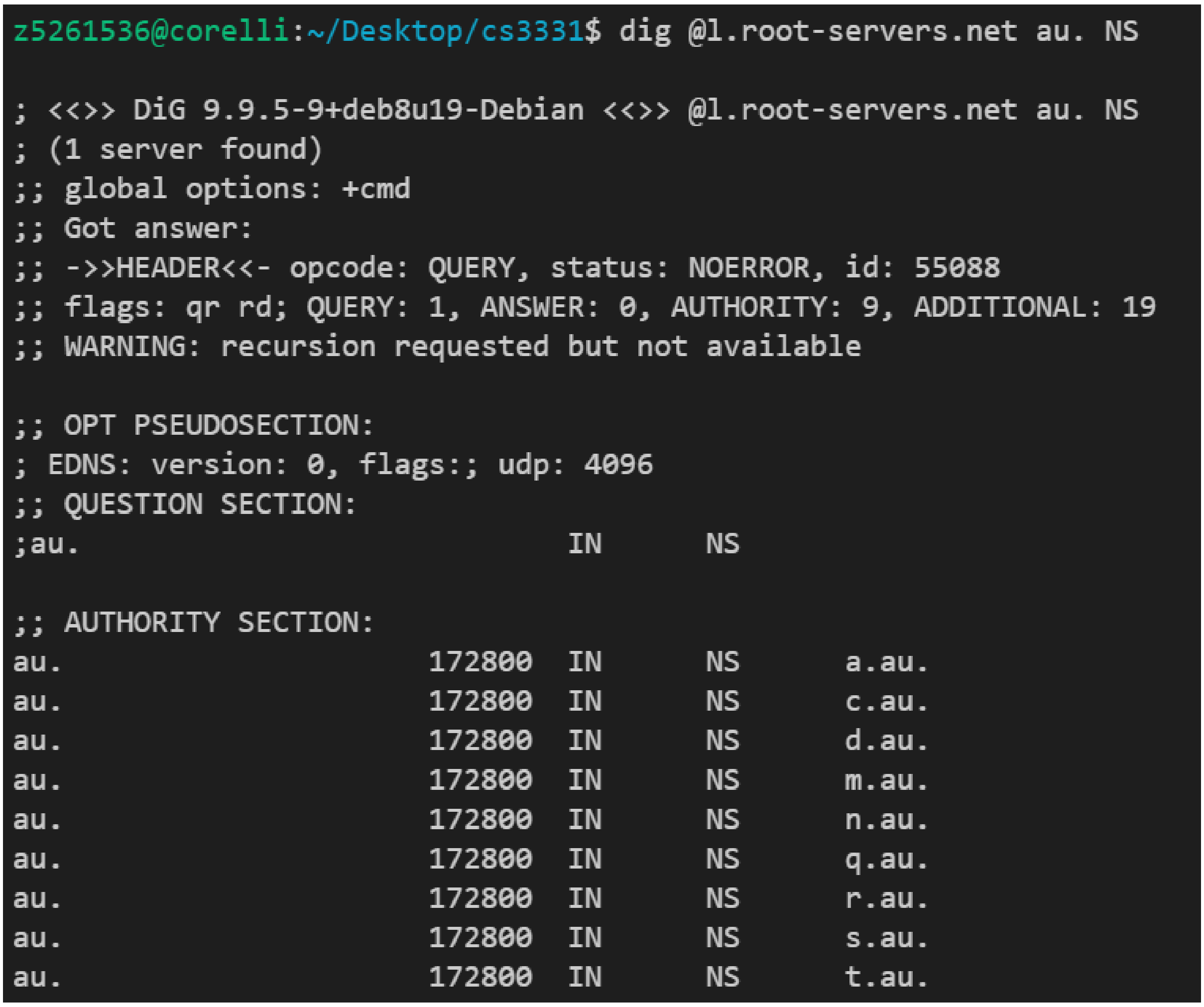
The IP address of lyre00.cse.unsw.edu.au is: 129.94.210.20, I queried on 6 DNS servers to get the answer, below is the process.

1. Find the name server the "." Domain, one of them would be **l.root-servers.net.**



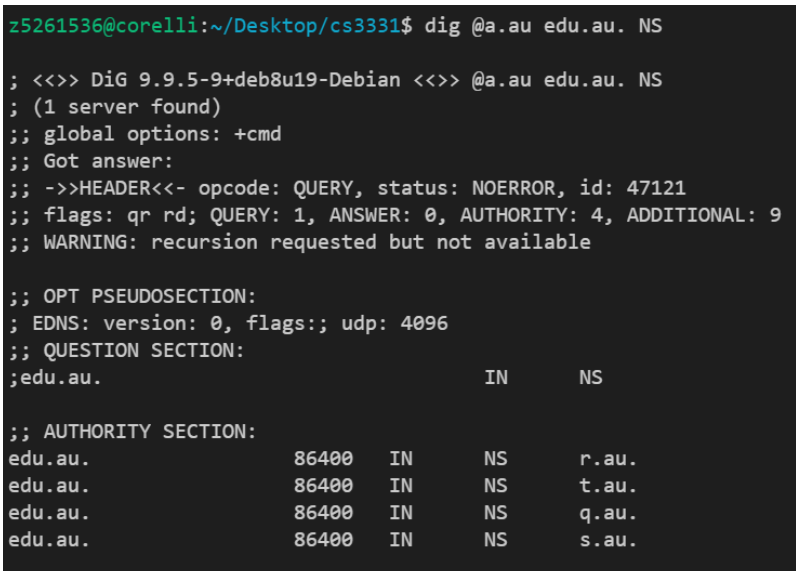
```
z5261536@corelli:~/Desktop/cs3331$ dig . NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43374
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       202227  IN      NS      l.root-servers.net.
.                       202227  IN      NS      b.root-servers.net.
.                       202227  IN      NS      i.root-servers.net.
.                       202227  IN      NS      a.root-servers.net.
.                       202227  IN      NS      m.root-servers.net.
.                       202227  IN      NS      j.root-servers.net.
.                       202227  IN      NS      d.root-servers.net.
.                       202227  IN      NS      e.root-servers.net.
.                       202227  IN      NS      k.root-servers.net.
.                       202227  IN      NS      c.root-servers.net.
.                       202227  IN      NS      h.root-servers.net.
.                       202227  IN      NS      g.root-servers.net.
.                       202227  IN      NS      f.root-servers.net.
```

2. query this nameserver l.root-servers.net. to find the authoritative name server for the "au." Domain: dig @l.root-servers.net au. NS, one of the server would be a.au.



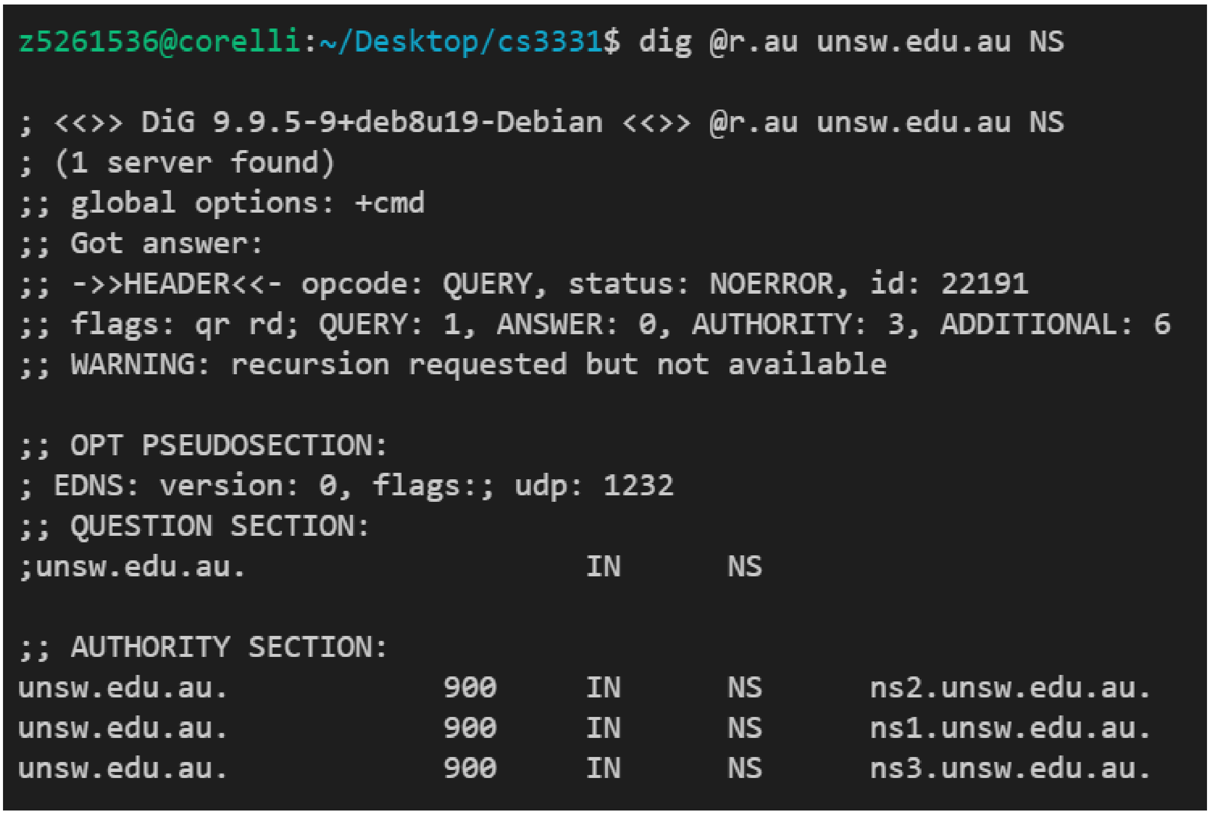
```
z5261536@corelli:~/Desktop/cs3331$ dig @l.root-servers.net au. NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @l.root-servers.net au. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55088
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 19
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;au.                            IN      NS

;; AUTHORITY SECTION:
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      c.au.
au.                     172800  IN      NS      d.au.
au.                     172800  IN      NS      m.au.
au.                     172800  IN      NS      n.au.
au.                     172800  IN      NS      q.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      t.au.
```

3. Query this second server **a.au** to find the authoritative nameserver for the "edu.au." domain: dig @a.au edu.au. NS



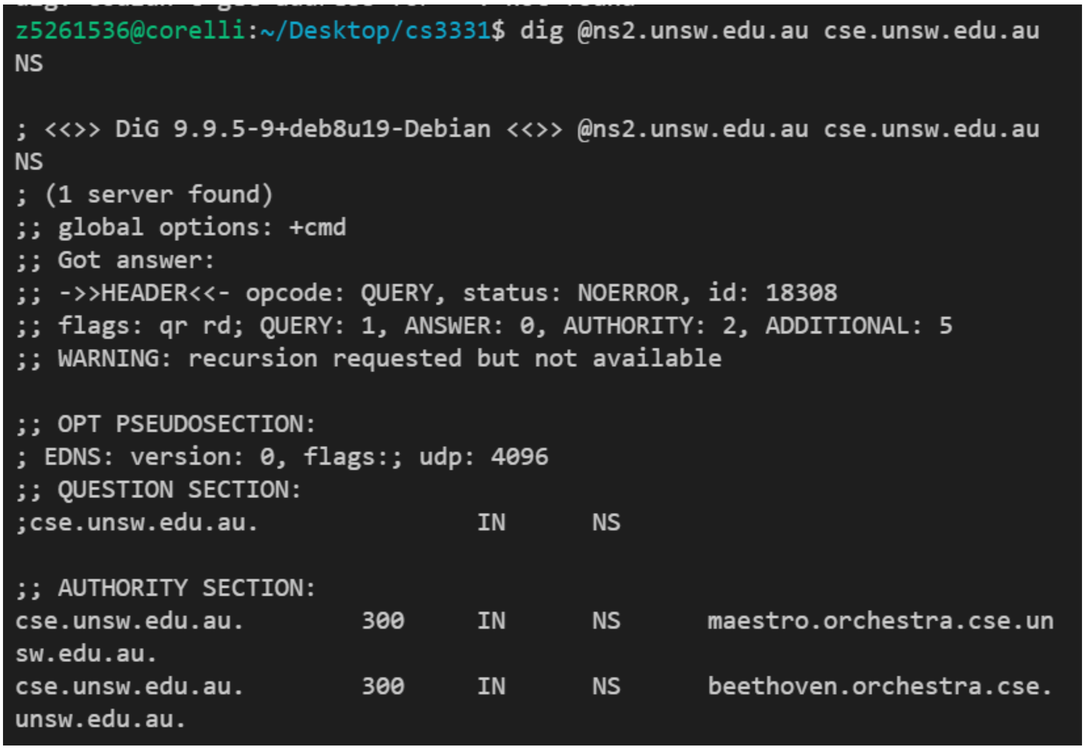
```
z5261536@corelli:~/Desktop/cs3331$ dig @a.au edu.au. NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @a.au edu.au. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47121
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;edu.au.                        IN      NS

;; AUTHORITY SECTION:
edu.au.                 86400   IN      NS      r.au.
edu.au.                 86400   IN      NS      t.au.
edu.au.                 86400   IN      NS      q.au.
edu.au.                 86400   IN      NS      s.au.
```

4. Now query the nameserver **r.au** to find the authoritative nameserver for "unsw.edu.au": dig @r.au unsw.edu.au NS



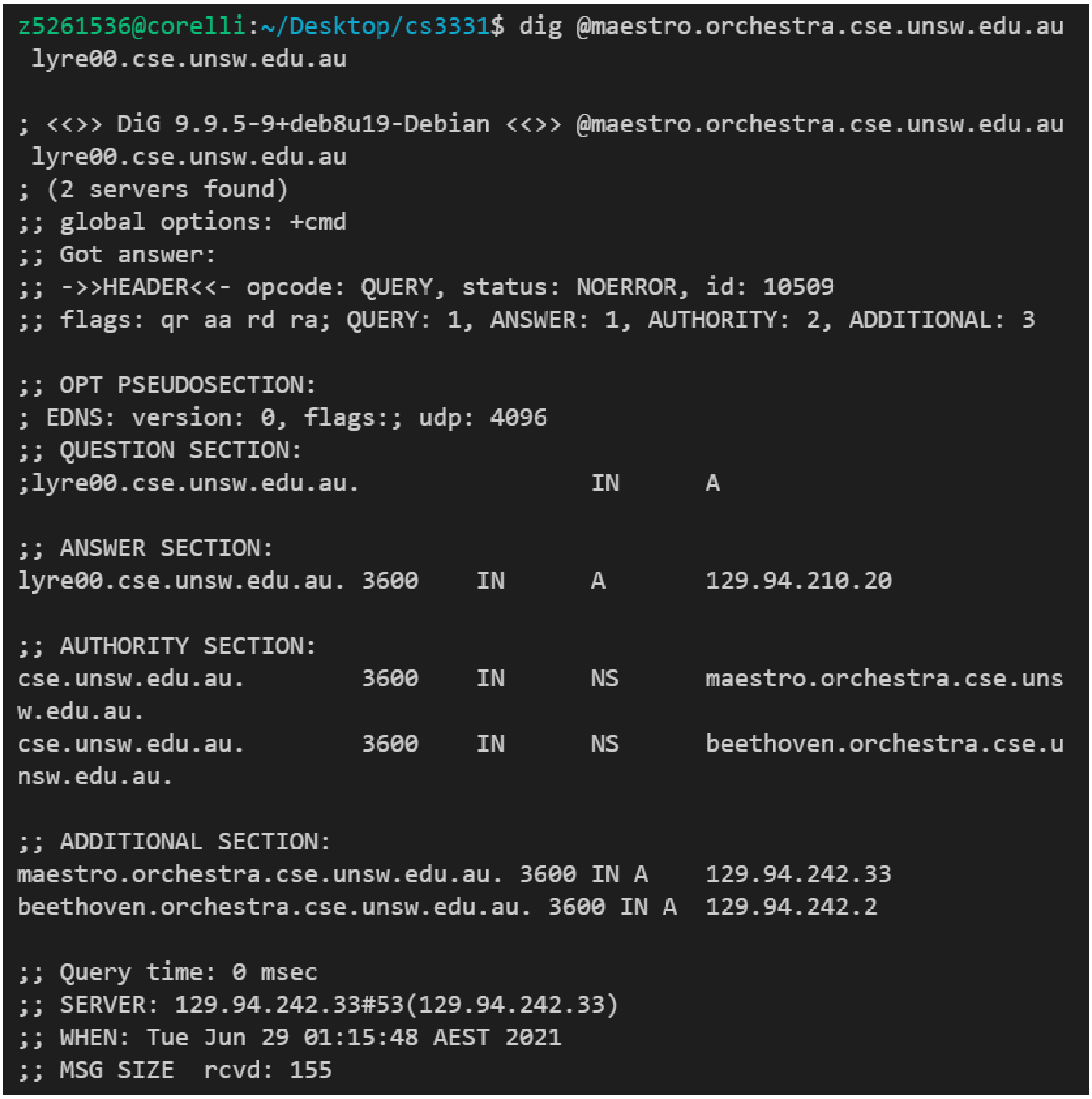
```
z5261536@corelli:~/Desktop/cs3331$ dig @r.au unsw.edu.au NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @r.au unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22191
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;unsw.edu.au.                   IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
```

5. Next query the nameserver of unsw.edu.au – **ns2.unsw.edu.au** to find the authoritative name server of cse.unsw.edu.au. : dig @ ns2.unsw.edu.au cse.unsw.edu.au NS



```
z5261536@corelli:~/Desktop/cs3331$ dig @ns2.unsw.edu.au cse.unsw.edu.au
NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns2.unsw.edu.au cse.unsw.edu.au
NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18308
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cse.unsw.edu.au.               IN      NS

;; AUTHORITY SECTION:
cse.unsw.edu.au.        300     IN      NS      maestro.orchestra.cse.un
sw.edu.au.
cse.unsw.edu.au.        300     IN      NS      beethoven.orchestra.cse.
unsw.edu.au.
```

6. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host: dig @maestro.orchestra.cse.unsw.edu.au lyre00.cse.unsw.edu.au



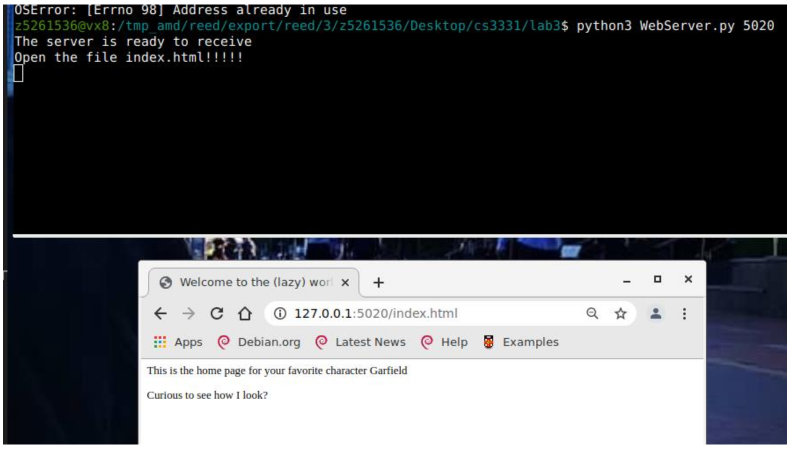
```
z5261536@corelli:~/Desktop/cs3331$ dig @maestro.orchestra.cse.unsw.edu.au
 lyre00.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @maestro.orchestra.cse.unsw.edu.au
 lyre00.cse.unsw.edu.au
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10509
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      A

;; ANSWER SECTION:
lyre00.cse.unsw.edu.au. 3600    IN      A       129.94.210.20

;; AUTHORITY SECTION:
cse.unsw.edu.au.        3600    IN      NS      maestro.orchestra.cse.uns
w.edu.au.
cse.unsw.edu.au.        3600    IN      NS      beethoven.orchestra.cse.u
nsw.edu.au.

;; ADDITIONAL SECTION:
maestro.orchestra.cse.unsw.edu.au. 3600 IN A    129.94.242.33
beethoven.orchestra.cse.unsw.edu.au. 3600 IN A  129.94.242.2

;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Jun 29 01:15:48 AEST 2021
;; MSG SIZE  rcvd: 155
```

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 associate with it.

Exercise 4: A Simple Web Server

```
http://127.0.0.1:port/index.html
```

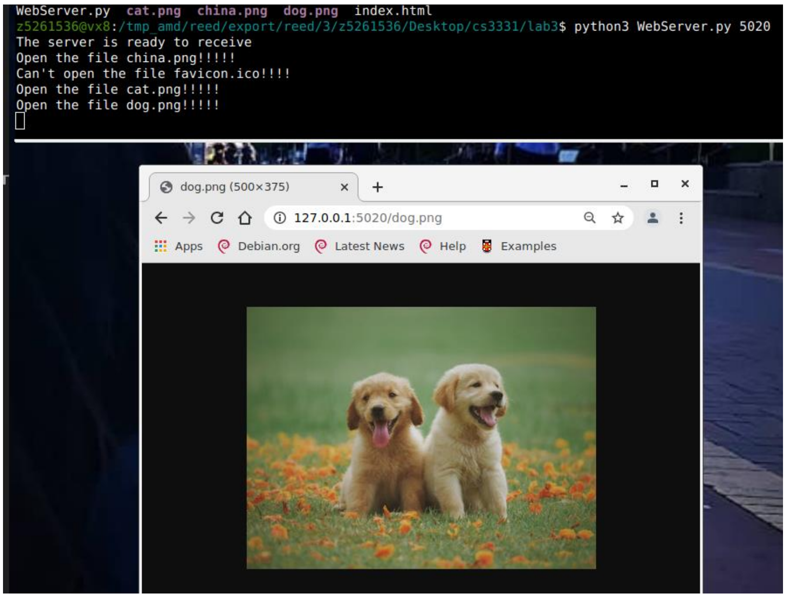


```
OSError: [Errno 98] Address already in use
z5261536@vx8:/tmp_amd/reed/export/reed/3/z5261536/Desktop/cs3331/lab3$ python3 WebServer.py 5020
The server is ready to receive
Open the file index.html!!!!!
```

This is the home page for your favorite character Garfield

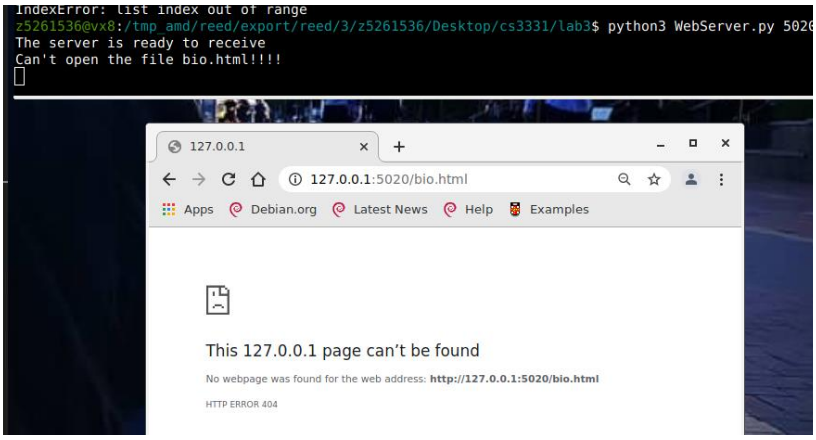
Curious to see how I look?

```
http://127.0.0.1:port/myimage.png
```



```
WebServer.py  cat.png  china.png  dog.png  index.html
z5261536@vx8:/tmp_amd/reed/export/reed/3/z5261536/Desktop/cs3331/lab3$ python3 WebServer.py 5020
The server is ready to receive
Open the file china.png!!!!!
Can't open the file favicon.ico!!!!
Open the file cat.png!!!!!
Open the file dog.png!!!!!
```

```
http://127.0.0.1:port/bio.html
```



```
IndexError: list index out of range
z5261536@vx8:/tmp_amd/reed/export/reed/3/z5261536/Desktop/cs3331/lab3$ python3 WebServer.py 502
The server is ready to receive
Can't open the file bio.html!!!!
```

This 127.0.0.1 page can’t be found

No webpage was found for the web address: **http://127.0.0.1:5020/bio.html**

HTTP ERROR 404