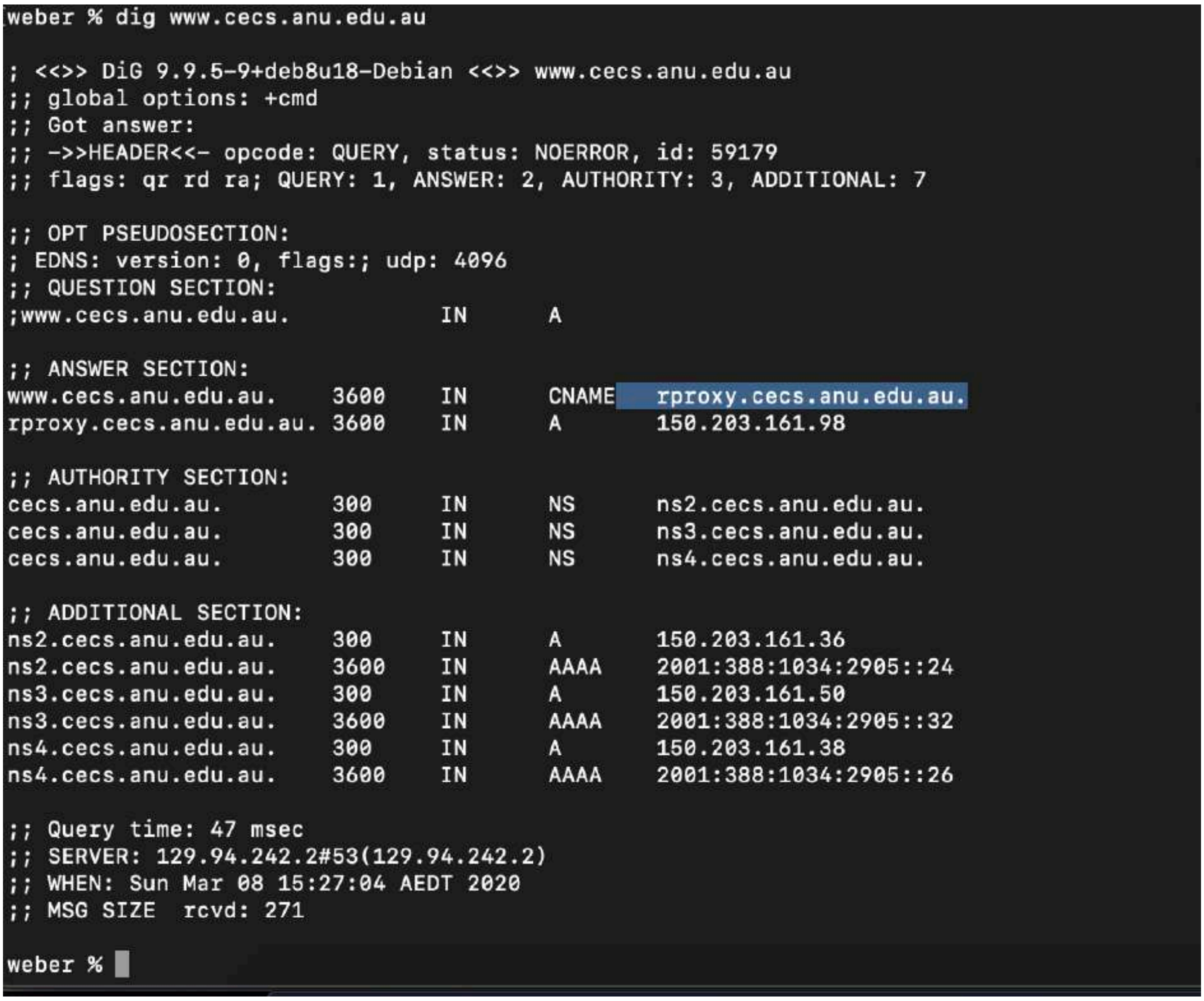
LAB 3

Exercise 3: Digging into DNS (marked, include in the lab report)

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



```
weber % dig www.cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59179
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        300     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        300     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        300     IN      NS      ns4.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    300     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    300     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    300     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    3600    IN      AAAA    2001:388:1034:2905::26

;; Query time: 47 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 08 15:27:04 AEDT 2020
;; MSG SIZE  rcvd: 271

weber %
```

query of type A is sent to get the IP address of www.cecs.anu.edu.au . The IP address is

150.203.161.98

Question 2. What is the canonical name for the CECS ANU web server? Suggest a reason for having an alias for this server.

The canonical name for the CECS ANU web server is rproxy.cecs.anu.edu.au. The IP address of is 150.203.161.98. The reason for having an alias is that it can be easily remembered and identified.

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

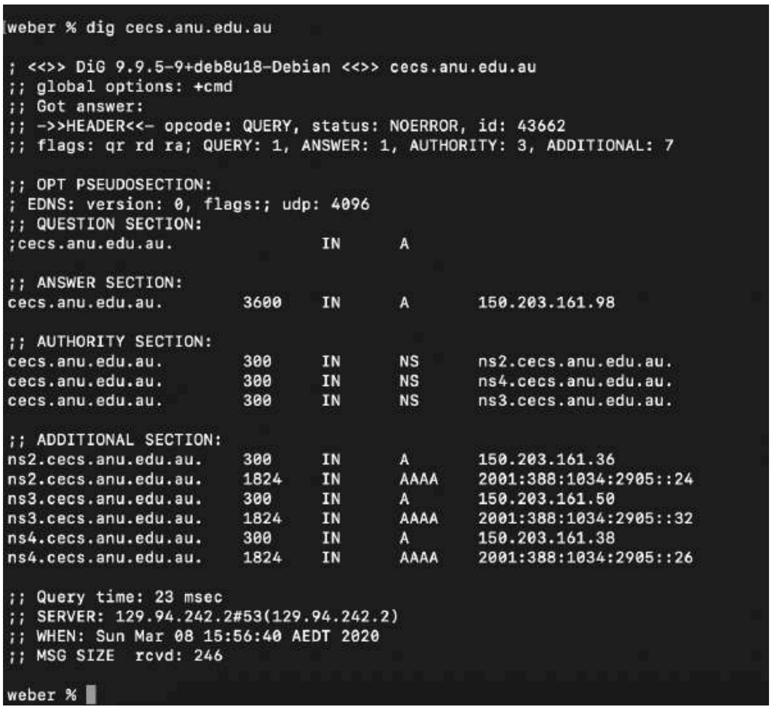
The Authority sections show details of the authoritative server. There are 3 NS records, in which the TTL is 300.

And the Additional sections display IP address of these authoritative server. The type AAAA is the IPv6 address for this domain server.

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

The IP address of the local nameserver is showed at the bottom. That is 129.94.242.2

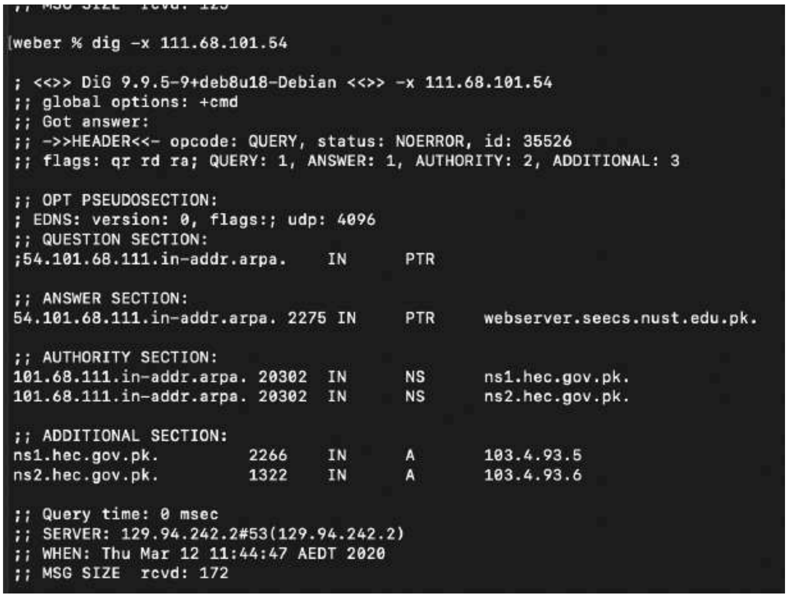
Question 5. What are the DNS nameservers for the "cecs.anu.edu.au" domain (note: the domain name is cecs.anu.edu.au and not www.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?



```
weber % dig cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43662
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 7

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

;; ANSWER SECTION:
cecs.anu.edu.au.        3600    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        300     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        300     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        300     IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    300     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    1824    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    300     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    1824    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    300     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    1824    IN      AAAA    2001:388:1034:2905::26

;; Query time: 23 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 08 15:56:40 AEDT 2020
;; MSG SIZE  rcvd: 246

weber %
```

Their IP addresses are 150.203.161.36, 150.203.161.50, 150.203.161.38. The type of query is NS

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?

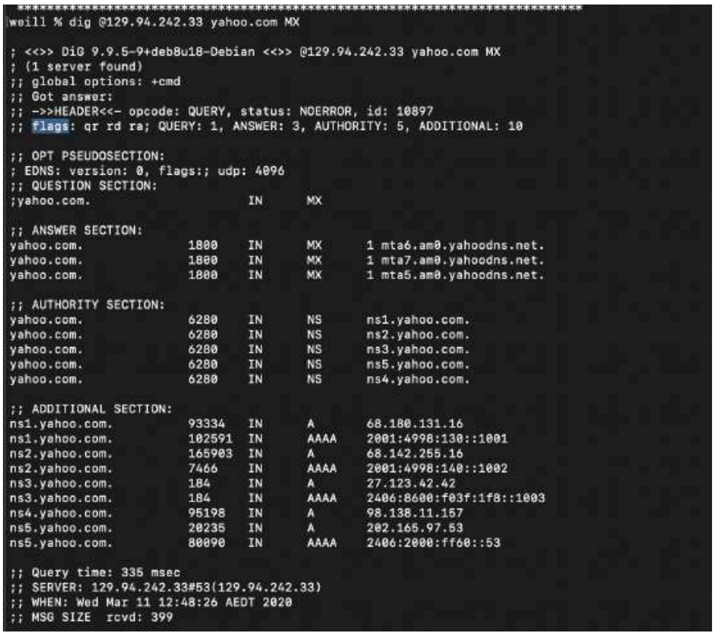


```
;; MSG SIZE  rcvd: 123

weber % dig -x 111.68.101.54

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35526
;; 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. 2275 IN     PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 20302  IN      NS      ns1.hec.gov.pk.
101.68.111.in-addr.arpa. 20302  IN      NS      ns2.hec.gov.pk.

;; ADDITIONAL SECTION:
ns1.hec.gov.pk.         2266    IN      A       103.4.93.5
ns2.hec.gov.pk.         1322    IN      A       103.4.93.6

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Mar 12 11:44:47 AEDT 2020
;; MSG SIZE  rcvd: 172
```

The type of DNS query is PTR. The DNS name associated with 111.68.101.54 is webserver.seecs.nust.edu.pk.

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)

the first step is to query the nameserver for the authoritative hostname of mail server of Yahoo! Mail. the response is shown below.



```
 ***************************************************************************
weill % dig @129.94.242.33 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10897
;; 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.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              6280    IN      NS      ns1.yahoo.com.
yahoo.com.              6280    IN      NS      ns2.yahoo.com.
yahoo.com.              6280    IN      NS      ns3.yahoo.com.
yahoo.com.              6280    IN      NS      ns5.yahoo.com.
yahoo.com.              6280    IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          93334   IN      A       68.180.131.16
ns1.yahoo.com.          102591  IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          165903  IN      A       68.142.255.16
ns2.yahoo.com.          7466    IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          184     IN      A       27.123.42.42
ns3.yahoo.com.          184     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          95198   IN      A       98.138.11.157
ns5.yahoo.com.          20235   IN      A       202.165.97.53
ns5.yahoo.com.          80090   IN      AAAA    2406:2000:ff60::53

;; Query time: 335 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Wed Mar 11 12:48:26 AEDT 2020
;; MSG SIZE  rcvd: 399
```

the flags include:

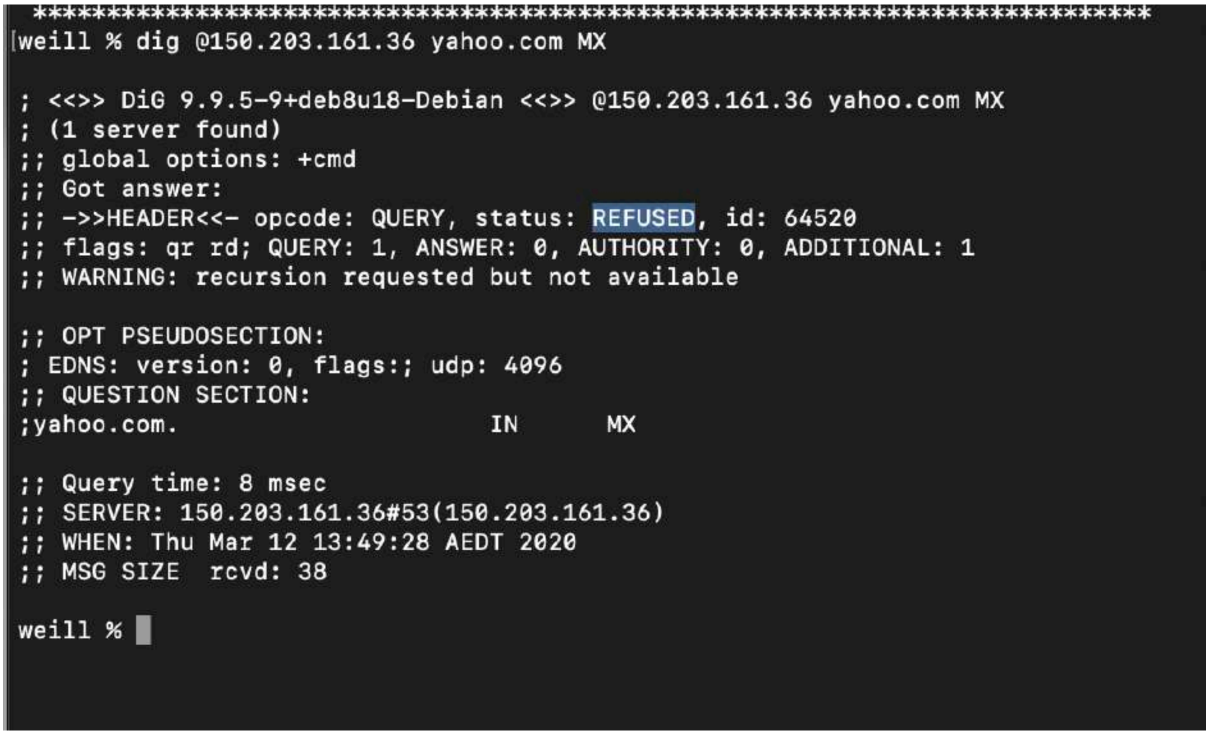
qr – Query?

rd – Recursion Desired

ra -- Recursion Available

and aa (authoritative answer) is not included, so this is not an authoritative answer

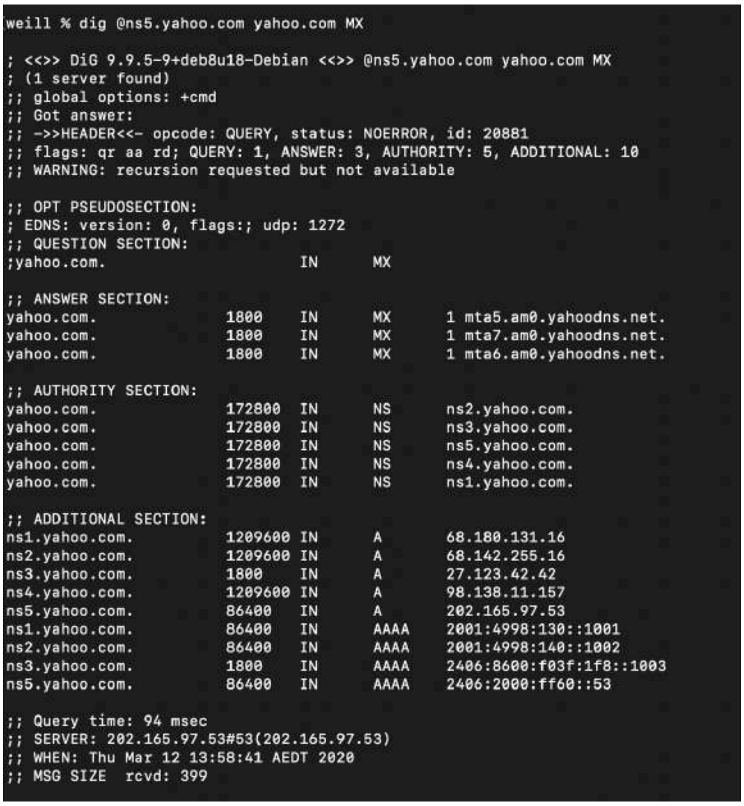
Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?



```
 ****************************************************************************
weill % dig @150.203.161.36 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @150.203.161.36 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 64520
;; 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: 8 msec
;; SERVER: 150.203.161.36#53(150.203.161.36)
;; WHEN: Thu Mar 12 13:49:28 AEDT 2020
;; MSG SIZE  rcvd: 38

weill % ▌
```

The query is refused

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

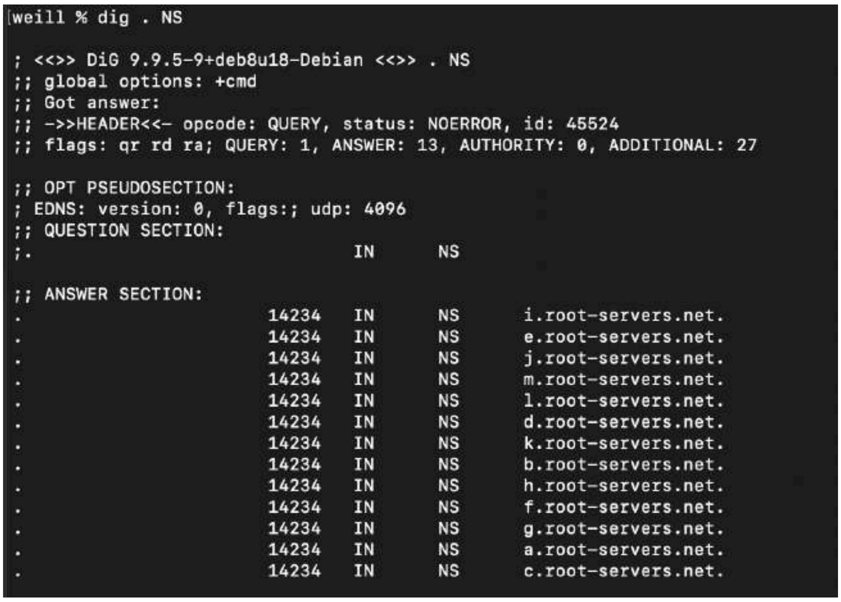


```
weill % dig @ns5.yahoo.com yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @ns5.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20881
;; 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      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.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
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          86400   IN      A       202.165.97.53
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::1003
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:ff60::53

;; Query time: 94 msec
;; SERVER: 202.165.97.53#53(202.165.97.53)
;; WHEN: Thu Mar 12 13:58:41 AEDT 2020
;; MSG SIZE  rcvd: 399
```

there are 3 mail servers: mta5.am0.yahoodns.net, mta7.am0.yahoodns.net and mta6.am0.yahoodns.net. The type of query is MX

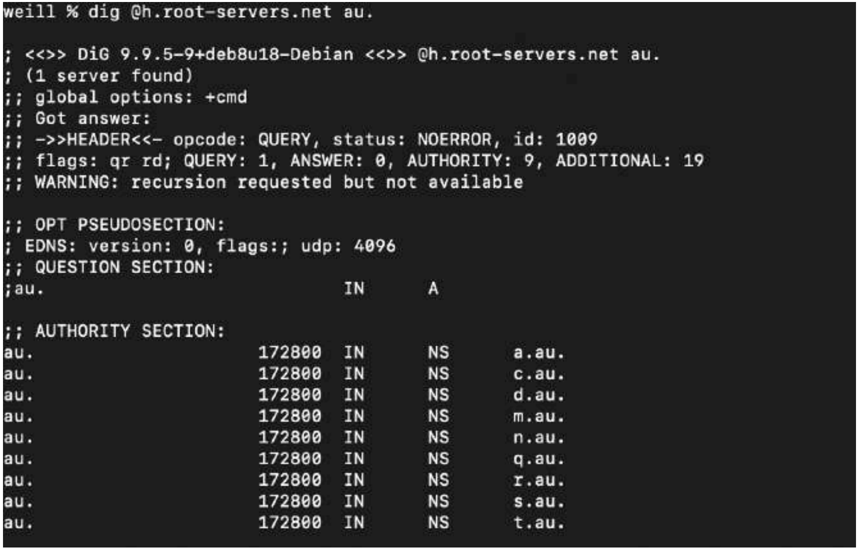
Question 10. In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. 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?

(1) find the name server of "." domain



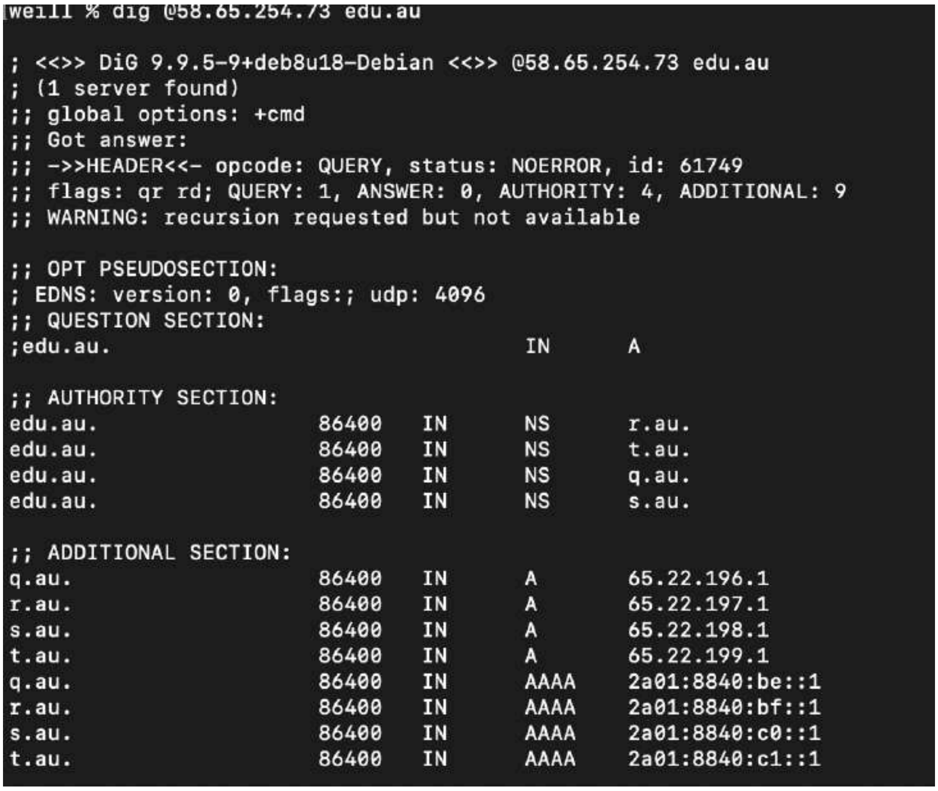
```
[weill % dig . NS

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45524
;; 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:
.                       14234   IN      NS      i.root-servers.net.
.                       14234   IN      NS      e.root-servers.net.
.                       14234   IN      NS      j.root-servers.net.
.                       14234   IN      NS      m.root-servers.net.
.                       14234   IN      NS      l.root-servers.net.
.                       14234   IN      NS      d.root-servers.net.
.                       14234   IN      NS      k.root-servers.net.
.                       14234   IN      NS      b.root-servers.net.
.                       14234   IN      NS      h.root-servers.net.
.                       14234   IN      NS      f.root-servers.net.
.                       14234   IN      NS      g.root-servers.net.
.                       14234   IN      NS      a.root-servers.net.
.                       14234   IN      NS      c.root-servers.net.
```

(2) find the authoritative name server for the "au." domain



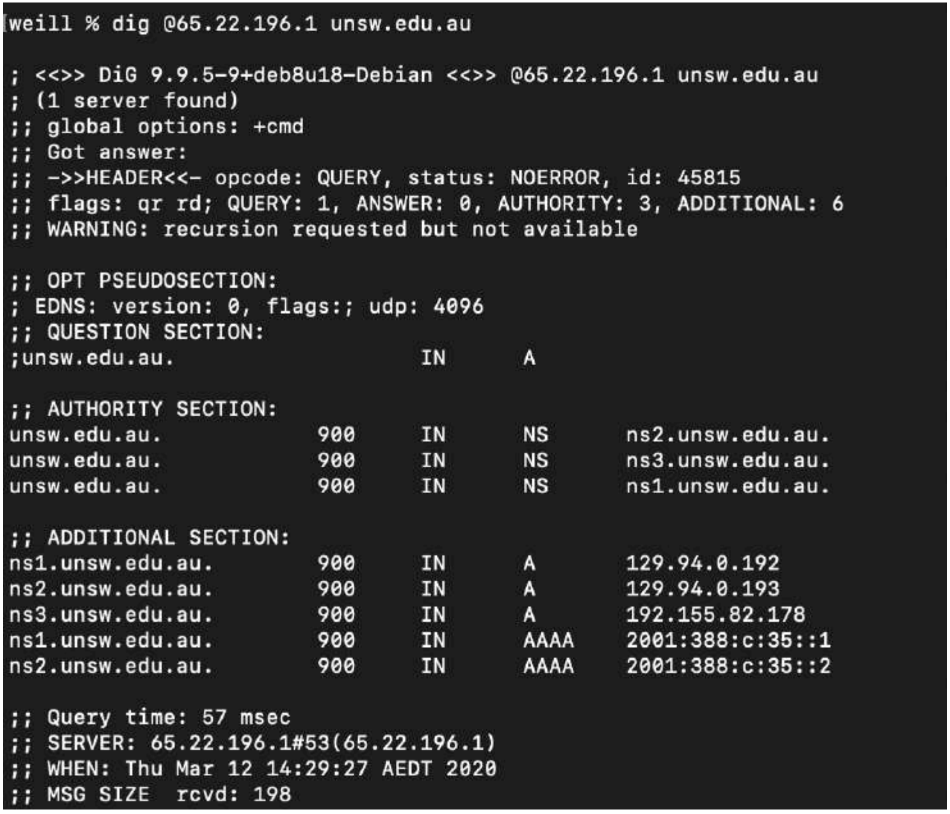
```
weill % dig @h.root-servers.net au.

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @h.root-servers.net au.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1009
;; 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      A

;; 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) find the authoritative name server for the "edu.au." domain



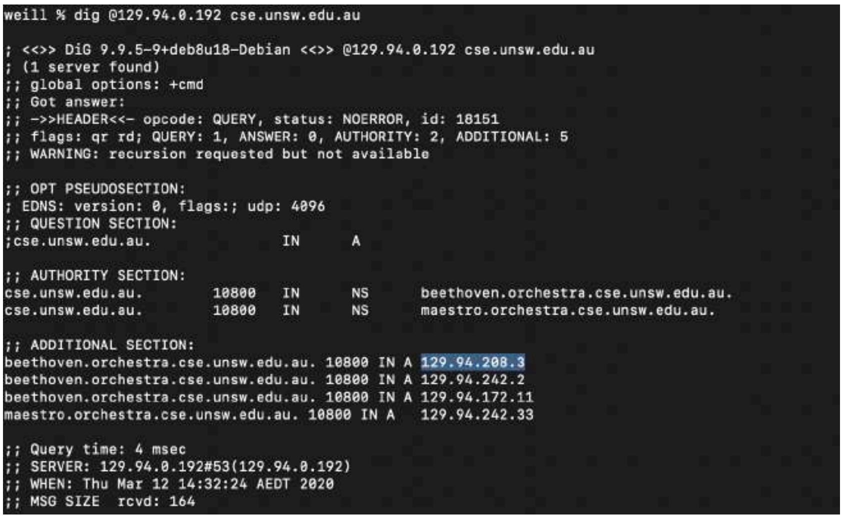
```
weill % dig @58.65.254.73 edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @58.65.254.73 edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61749
;; 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      A

;; 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.

;; ADDITIONAL SECTION:
q.au.                   86400   IN      A       65.22.196.1
r.au.                   86400   IN      A       65.22.197.1
s.au.                   86400   IN      A       65.22.198.1
t.au.                   86400   IN      A       65.22.199.1
q.au.                   86400   IN      AAAA    2a01:8840:be::1
r.au.                   86400   IN      AAAA    2a01:8840:bf::1
s.au.                   86400   IN      AAAA    2a01:8840:c0::1
t.au.                   86400   IN      AAAA    2a01:8840:c1::1
```

(4) find the authoritative name server for the “unsw.edu.au.” domain



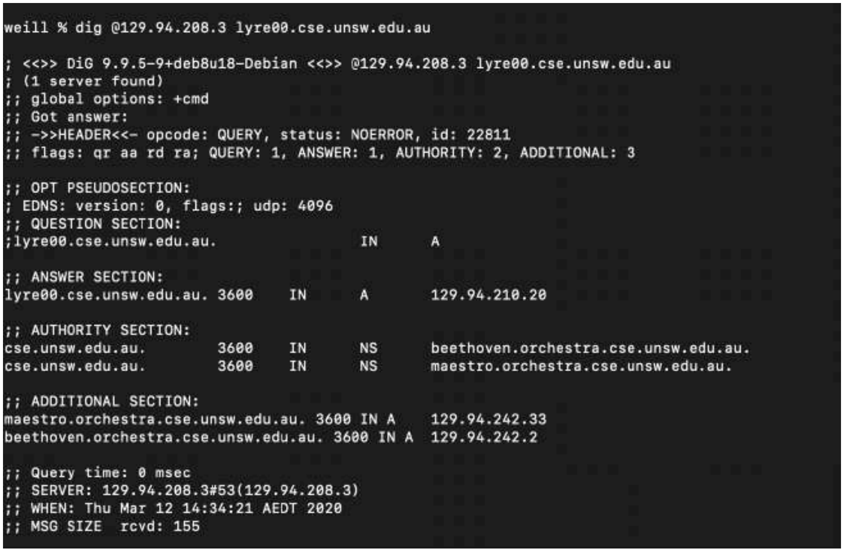
```
weill % dig @65.22.196.1 unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @65.22.196.1 unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45815
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

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

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

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        900     IN      A       129.94.0.192
ns2.unsw.edu.au.        900     IN      A       129.94.0.193
ns3.unsw.edu.au.        900     IN      A       192.155.82.178
ns1.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::2

;; Query time: 57 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Thu Mar 12 14:29:27 AEDT 2020
;; MSG SIZE  rcvd: 198
```

(5) find the authoritative name server for the “cse.unsw.edu.au.” domain



```
weill % dig @129.94.0.192 cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @129.94.0.192 cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18151
;; 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      A

;; AUTHORITY SECTION:
cse.unsw.edu.au.        10800   IN      NS      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        10800   IN      NS      maestro.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.2
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.172.11
maestro.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.242.33

;; Query time: 4 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Thu Mar 12 14:32:24 AEDT 2020
;; MSG SIZE  rcvd: 164
```

(5) find the authoritative name server for the “**lyre00.cse.unsw.edu.au**” domain



```
weill % dig @129.94.208.3 lyre00.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @129.94.208.3 lyre00.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22811
;; 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      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        3600    IN      NS      maestro.orchestra.cse.unsw.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: 129.94.208.3#53(129.94.208.3)
;; WHEN: Thu Mar 12 14:34:21 AEDT 2020
;; MSG SIZE  rcvd: 155
```

the IP address of my machine is 129.94.242.20. I query 6 servers to get the answer

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

yes, a machine may have multiple names as well as IP addresses associated. Actually, this is also a common fact. For example, a machine may be both connected to Internet by Wifi and Lan. Then it may has 2 IP addresses. Also, for a server, it’s essential to have multiple IP addresses, especially when there is need implement server virtualization.

.