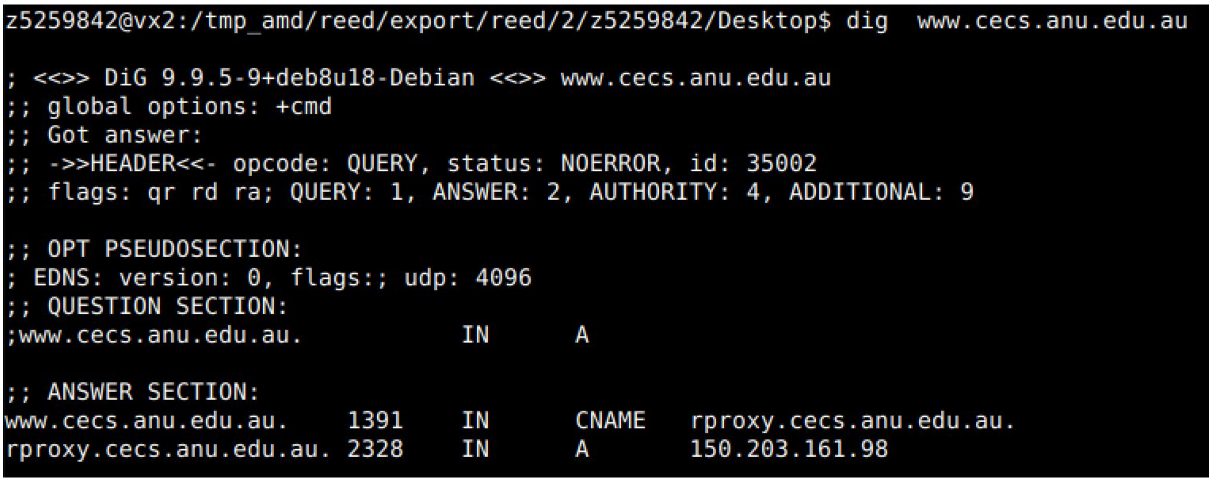
Question 1. What is the IP address of www.cecs.anu.edu.au . What type of DNS query is sent to get this answer?

The IP address of www.cecs.anu.edu.au is 150.203.161.98. The type of DNS query that is sent to get the answer is a Type A query.

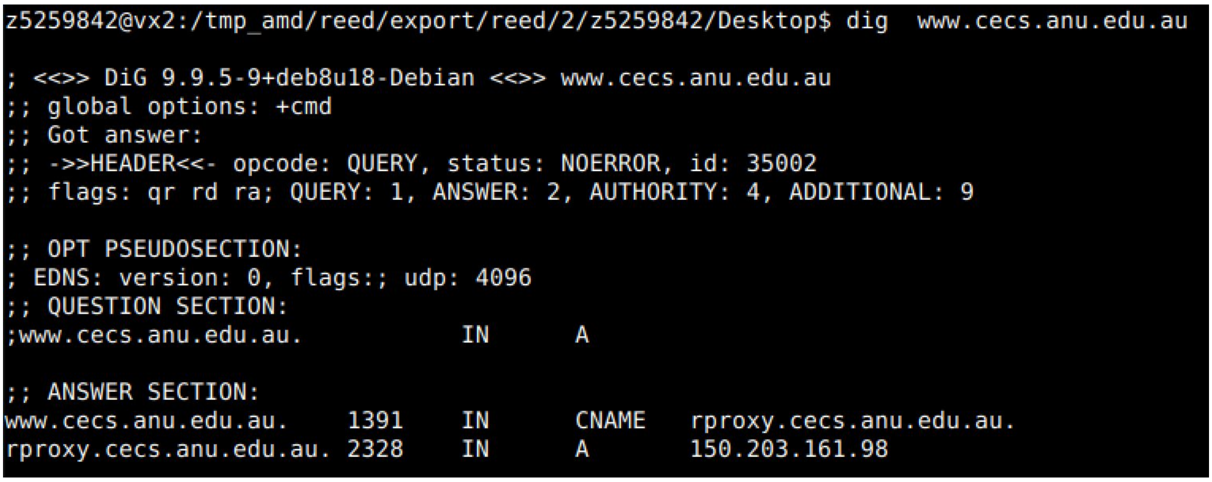


```
z5259842@vx2:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig  www.cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35002
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1391    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 2328    IN      A       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 canonical name can often be difficult to remember. Therefore, an alias is used for this server because it is easier to comprehend and identify instead of the canonical name.

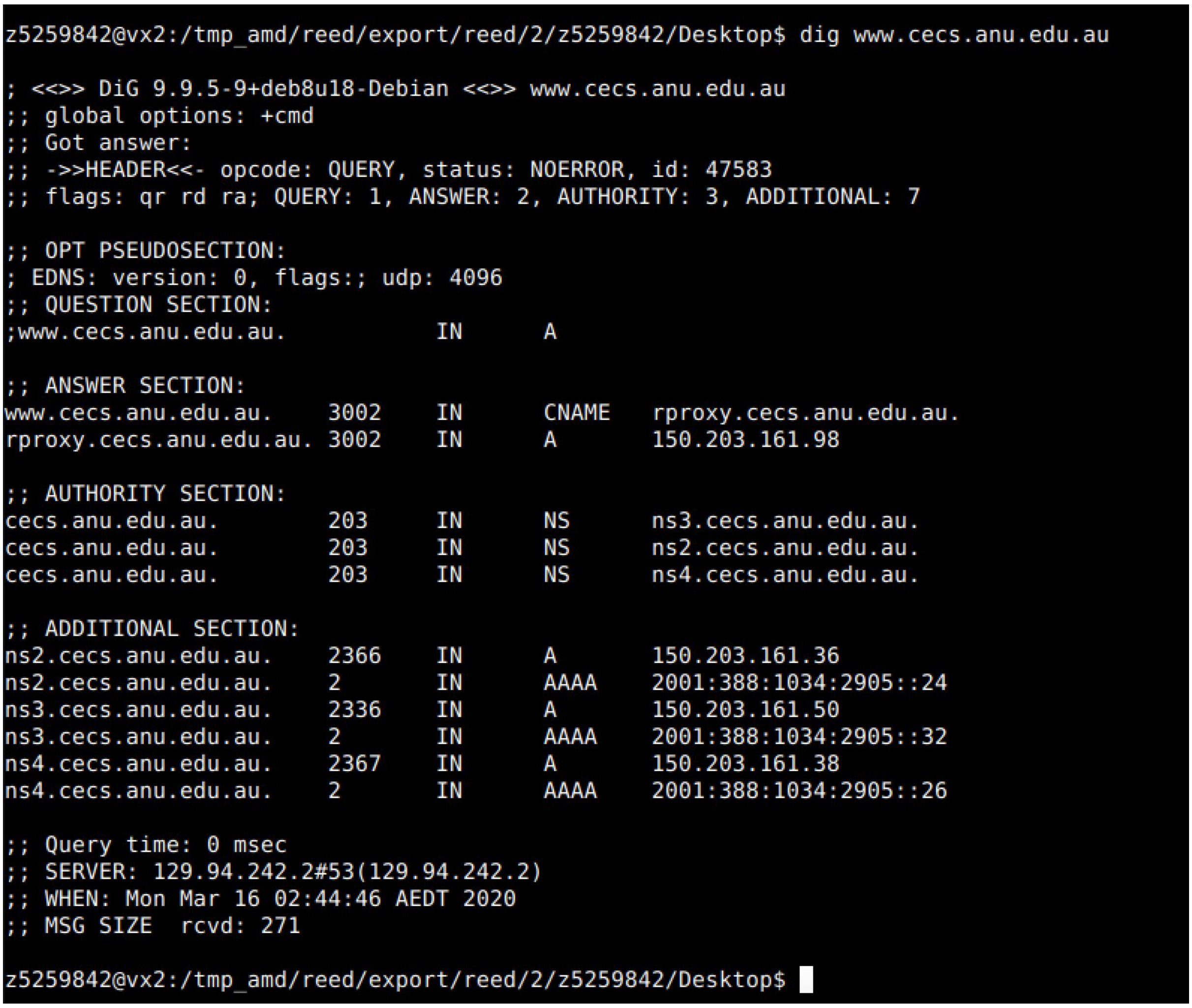


```
z5259842@vx2:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig  www.cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35002
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1391    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 2328    IN      A       150.203.161.98
```

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

In the authority section, there are 3 authoritative DNS servers.

The additional section lists the IP addresses of the 3 DNS servers respectively. It contains both the A (IPV4) and AAAA (IPV6) for those servers.

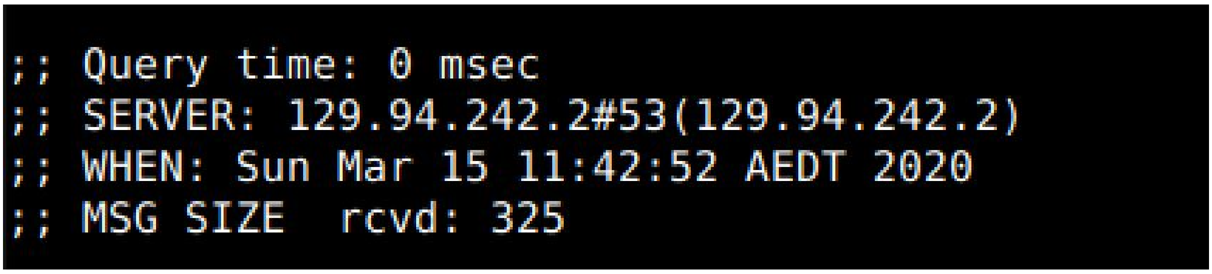


```
z5259842@vx2:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig www.cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47583
;; 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.    3002    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3002    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        203     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        203     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        203     IN      NS      ns4.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    2366    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    2       IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2336    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    2       IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    2367    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    2       IN      AAAA    2001:388:1034:2905::26

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Mar 16 02:44:46 AEDT 2020
;; MSG SIZE  rcvd: 271

z5259842@vx2:/tmp_amd/reed/export/reed/2/z5259842/Desktop$
```

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

This was conducted on TigerVNC.



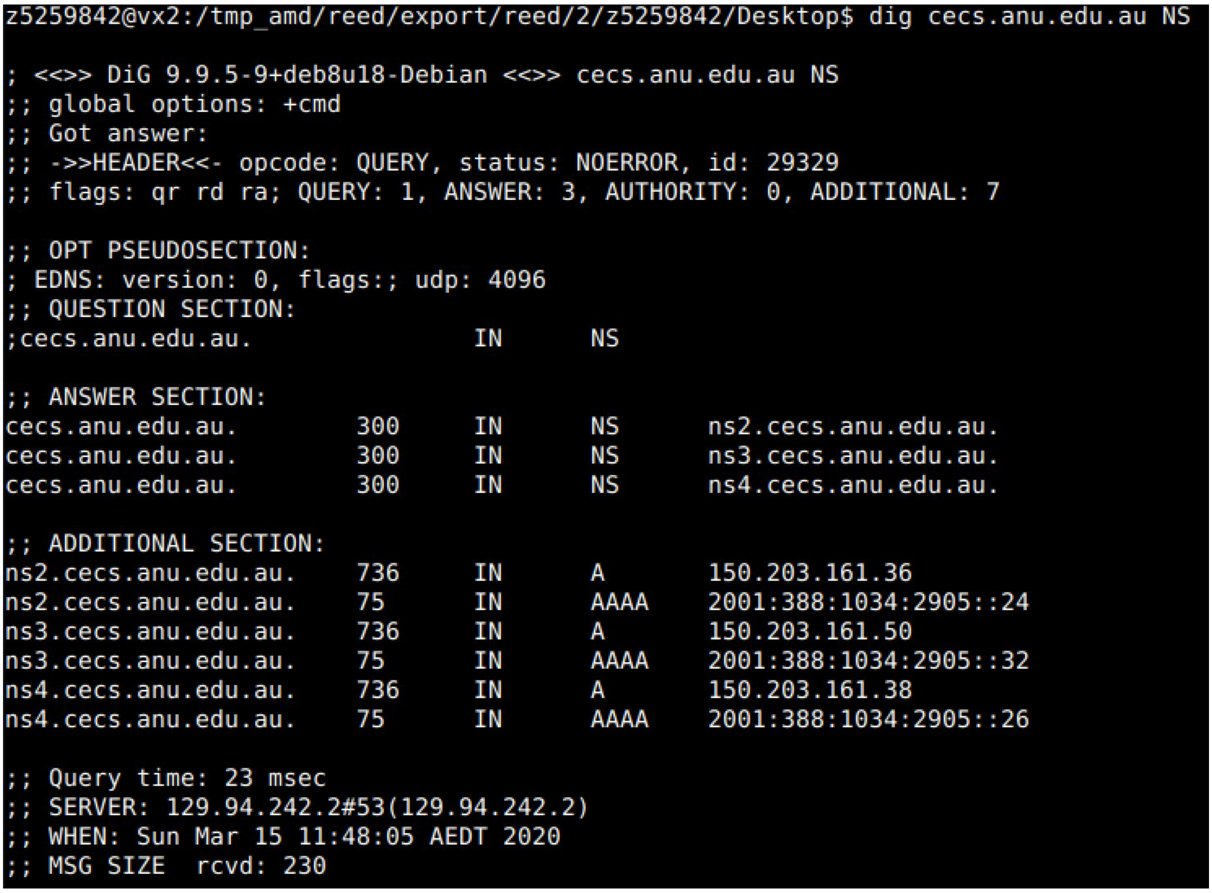
```
;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 15 11:42:52 AEDT 2020
;; MSG SIZE  rcvd: 325
```

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?

The DNS name servers and the respective IP addresses are:

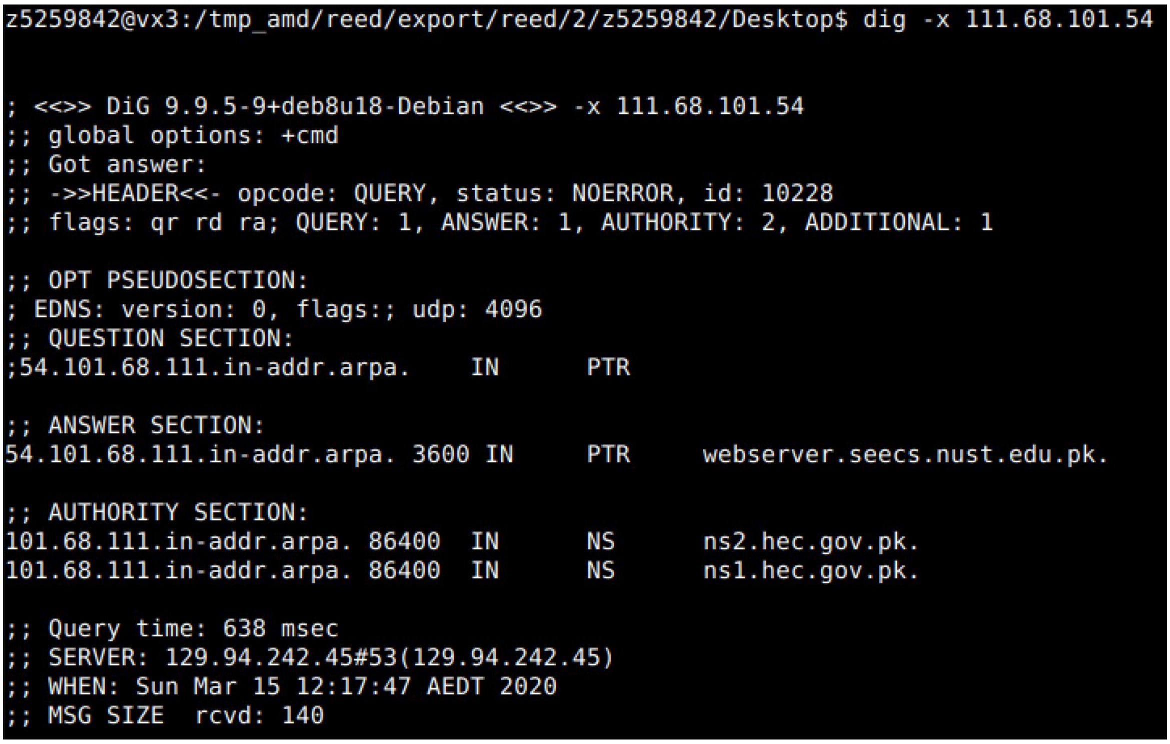
DNS name servers	IPV4	IPV6
ns2.cecs.anu.edu.au.	150.203.161.36	2001:388:1034:2905::24
ns3.cecs.anu.edu.au.	150.203.161.50	2001:388:1034:2905::32
ns4.cecs.anu.edu.au.	150.203.161.38	2001:388:1034:2905::26

The type of DNS query that is sent to obtain this information was a NS query.



```
z5259842@vx2:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig cecs.anu.edu.au NS

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> cecs.anu.edu.au NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29329
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 7

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

;; ANSWER 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.    736     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    75      IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    736     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    75      IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    736     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    75      IN      AAAA    2001:388:1034:2905::26

;; Query time: 23 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 15 11:48:05 AEDT 2020
;; MSG SIZE  rcvd: 230
```

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?



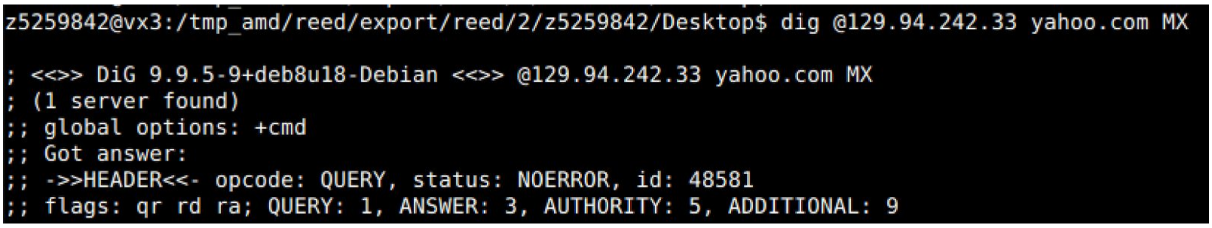
```
z5259842@vx3:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig -x 111.68.101.54


; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10228
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; 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. 3600 IN     PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 86400  IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 86400  IN      NS      ns1.hec.gov.pk.

;; Query time: 638 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Sun Mar 15 12:17:47 AEDT 2020
;; MSG SIZE  rcvd: 140
```

The DNS name associated with 111.68.101.54 is webserver.seecs.nust.edu.pk

The type of DNS query that was sent to obtain this information was a reverse DNS lookup - PTR.

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)

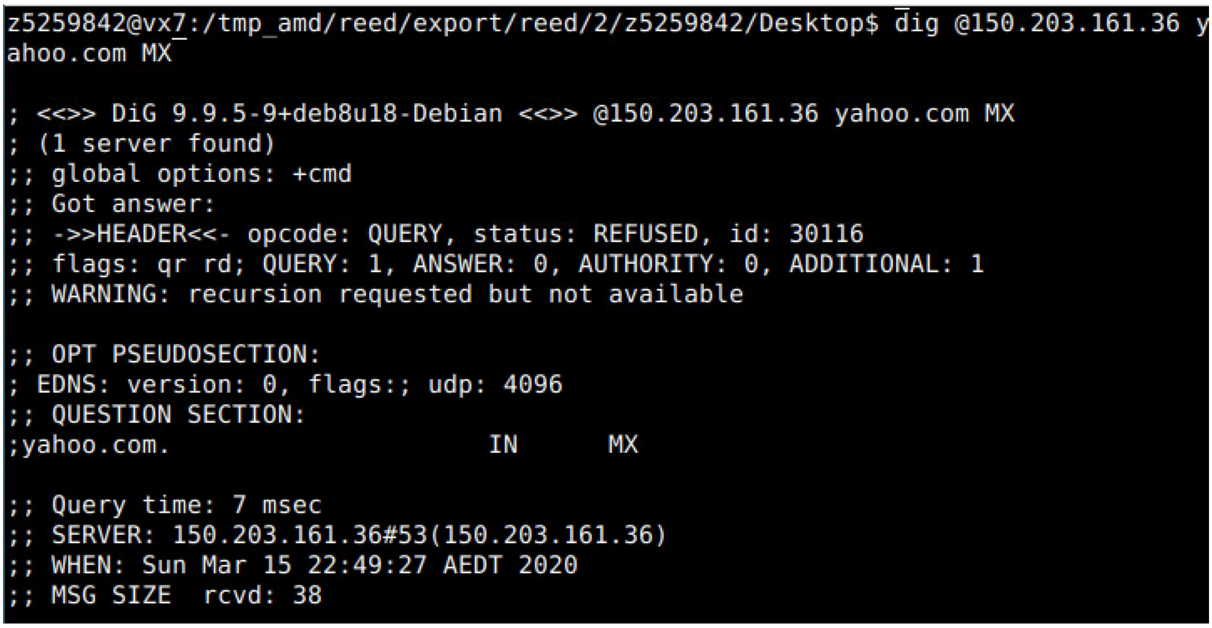
An authoritative answer was not obtained. This can be concluded by examining the flags in the response. The lack of an “aa” (authoritative answer) flag demonstrates that CSE server has no authority over yahoo.com servers.



```
z5259842@vx3:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ 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: 48581
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9
```

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

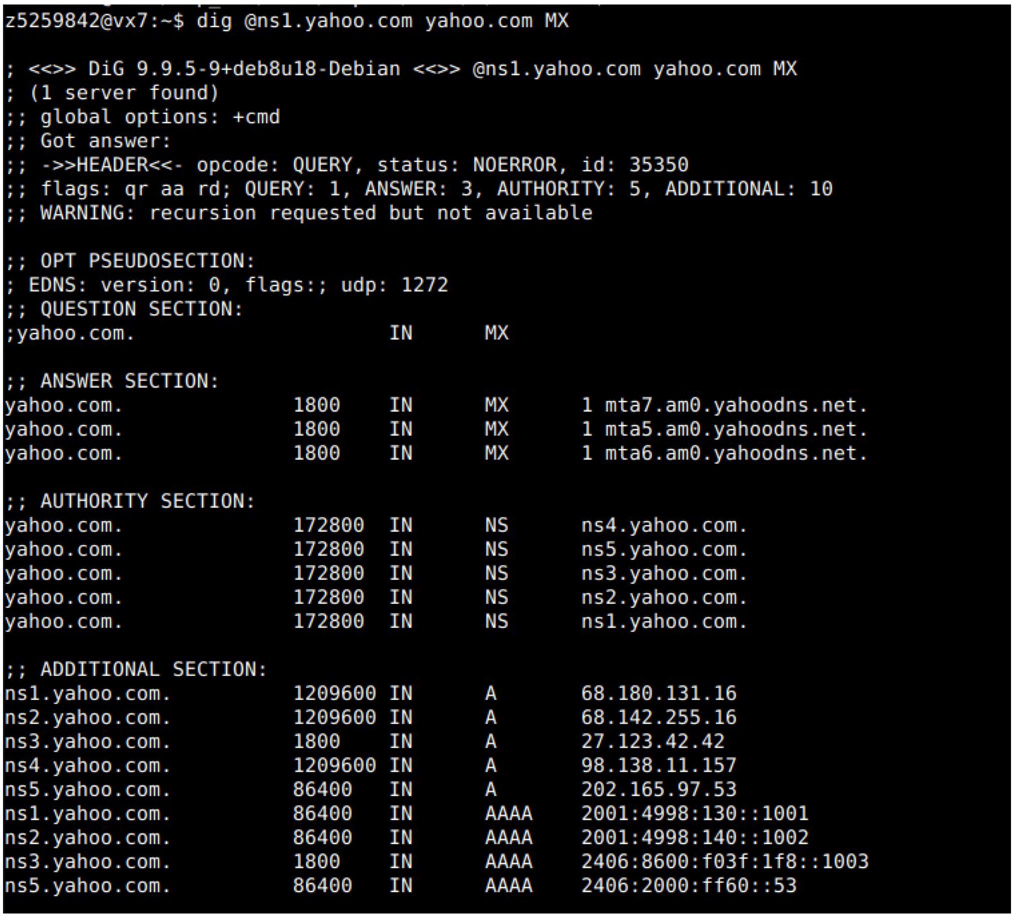
One of the nameservers obtained in Question 5 (150.203.161.36) was used and the result is shown in the header of which the status is “REFUSED”.



```
z5259842@vx7:/tmp_amd/reed/export/reed/2/z5259842/Desktop$ dig @150.203.161.36 y
ahoo.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: 30116
;; 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: 7 msec
;; SERVER: 150.203.161.36#53(150.203.161.36)
;; WHEN: Sun Mar 15 22:49:27 AEDT 2020
;; 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?

The DNS query type used to obtain this information was MX. In the flags there is an “aa” flag, indicating that it is the authoritative answer.

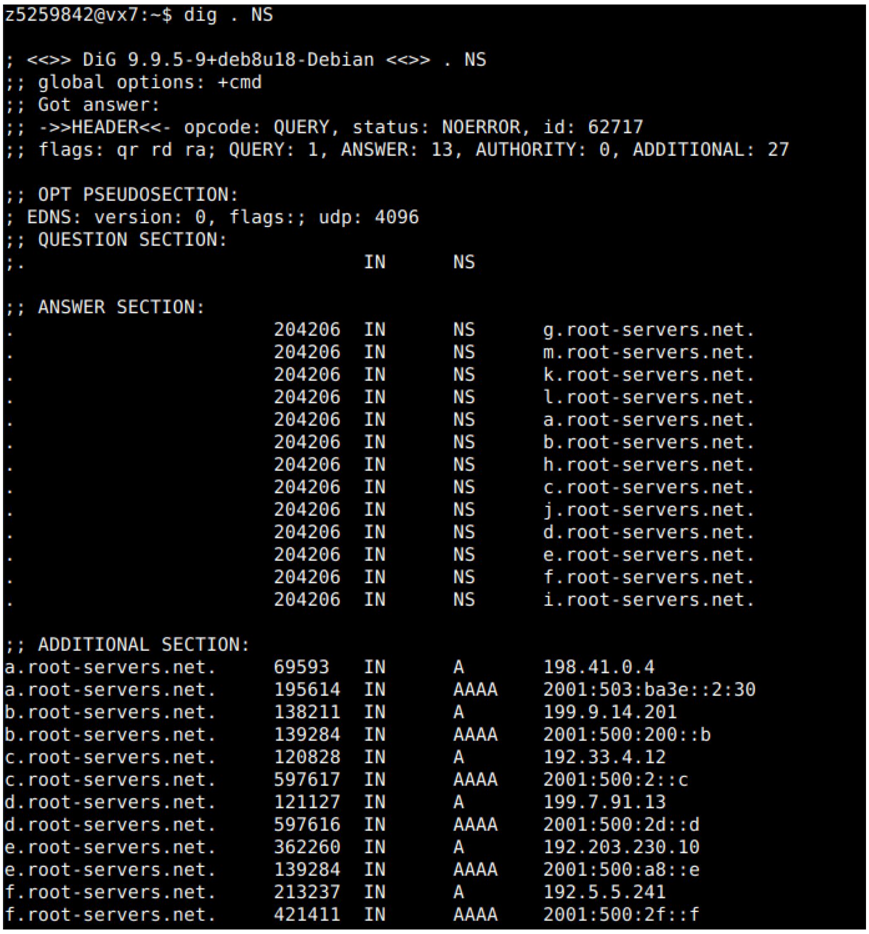


```
z5259842@vx7:~$ dig @ns1.yahoo.com yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35350
;; 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 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.

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

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?

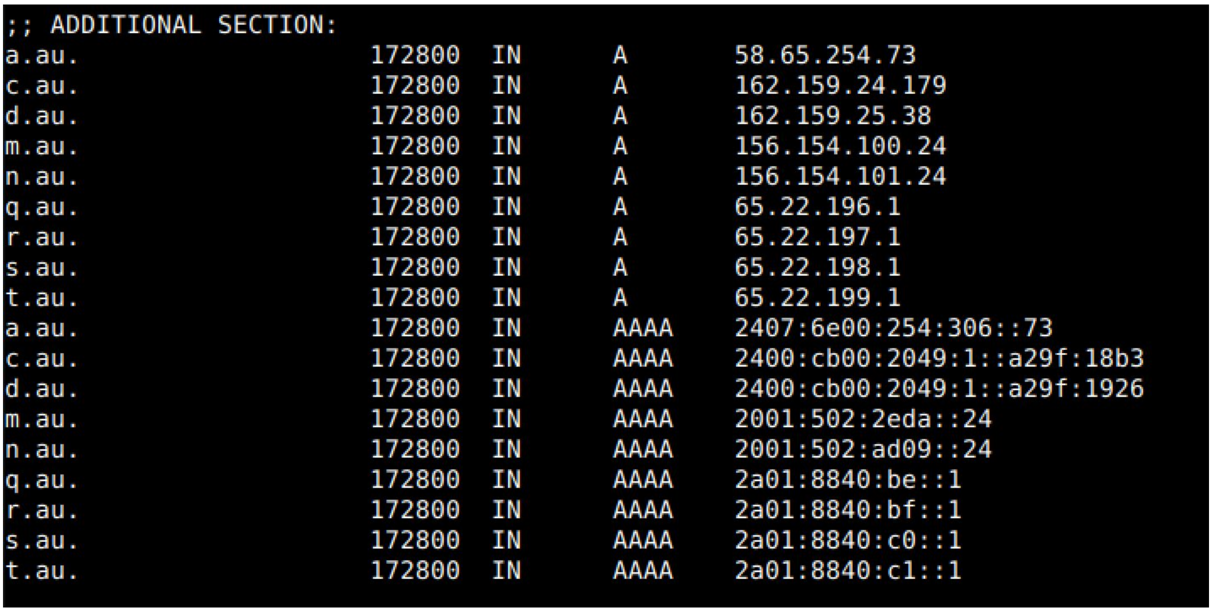
6 DNS servers are queried to get the authoritative answer.. The IP address of the host is 129.94.210.20.

dig . NS



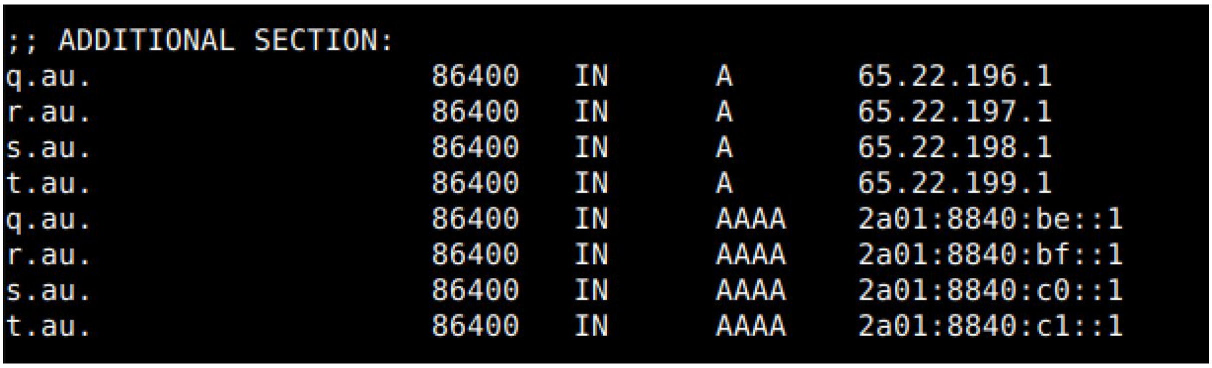
```
z5259842@vx7:~$ dig . NS

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62717
;; 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:
.                       204206  IN      NS      g.root-servers.net.
.                       204206  IN      NS      m.root-servers.net.
.                       204206  IN      NS      k.root-servers.net.
.                       204206  IN      NS      l.root-servers.net.
.                       204206  IN      NS      a.root-servers.net.
.                       204206  IN      NS      b.root-servers.net.
.                       204206  IN      NS      h.root-servers.net.
.                       204206  IN      NS      c.root-servers.net.
.                       204206  IN      NS      j.root-servers.net.
.                       204206  IN      NS      d.root-servers.net.
.                       204206  IN      NS      e.root-servers.net.
.                       204206  IN      NS      f.root-servers.net.
.                       204206  IN      NS      i.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     69593   IN      A       198.41.0.4
a.root-servers.net.     195614  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     138211  IN      A       199.9.14.201
b.root-servers.net.     139284  IN      AAAA    2001:500:200::b
c.root-servers.net.     120828  IN      A       192.33.4.12
c.root-servers.net.     597617  IN      AAAA    2001:500:2::c
d.root-servers.net.     121127  IN      A       199.7.91.13
d.root-servers.net.     597616  IN      AAAA    2001:500:2d::d
e.root-servers.net.     362260  IN      A       192.203.230.10
e.root-servers.net.     139284  IN      AAAA    2001:500:a8::e
f.root-servers.net.     213237  IN      A       192.5.5.241
f.root-servers.net.     421411  IN      AAAA    2001:500:2f::f
```

dig @a.root-servers.net. au. NS



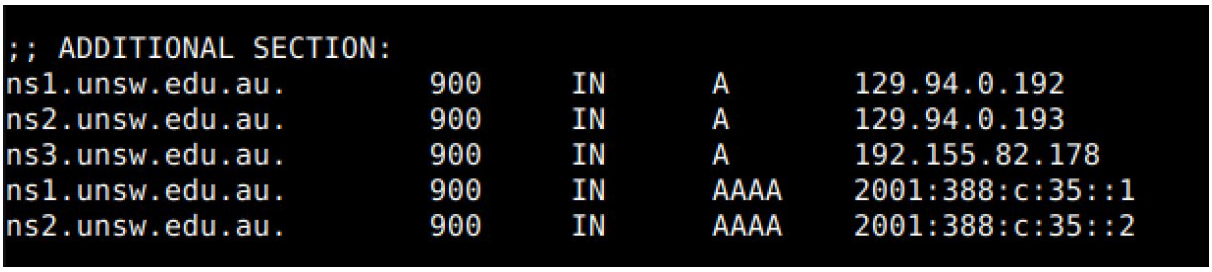
```
;; ADDITIONAL SECTION:
a.au.                   172800  IN      A       58.65.254.73
c.au.                   172800  IN      A       162.159.24.179
d.au.                   172800  IN      A       162.159.25.38
m.au.                   172800  IN      A       156.154.100.24
n.au.                   172800  IN      A       156.154.101.24
q.au.                   172800  IN      A       65.22.196.1
r.au.                   172800  IN      A       65.22.197.1
s.au.                   172800  IN      A       65.22.198.1
t.au.                   172800  IN      A       65.22.199.1
a.au.                   172800  IN      AAAA    2407:6e00:254:306::73
c.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
m.au.                   172800  IN      AAAA    2001:502:2eda::24
n.au.                   172800  IN      AAAA    2001:502:ad09::24
q.au.                   172800  IN      AAAA    2a01:8840:be::1
r.au.                   172800  IN      AAAA    2a01:8840:bf::1
s.au.                   172800  IN      AAAA    2a01:8840:c0::1
t.au.                   172800  IN      AAAA    2a01:8840:c1::1
```

dig @a.au. edu.au. NS



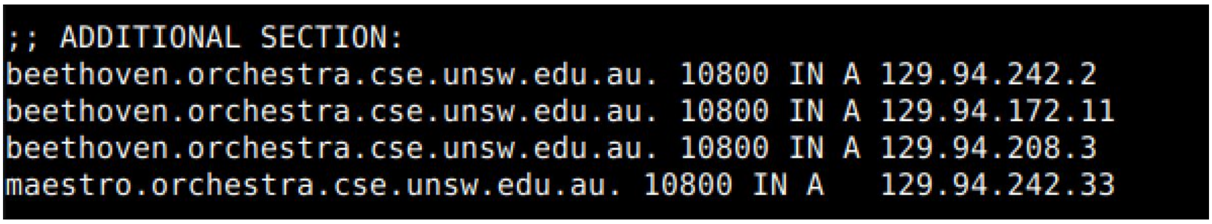
```
;; ADDITIONAL SECTION:
q.au.                   86400   IN      A       65.22.196.1
r.au.                   86400   IN      A       65.22.197.1
s.au.                   86400   IN      A       65.22.198.1
t.au.                   86400   IN      A       65.22.199.1
q.au.                   86400   IN      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
```

dig @q.au. unsw.edu.au NS



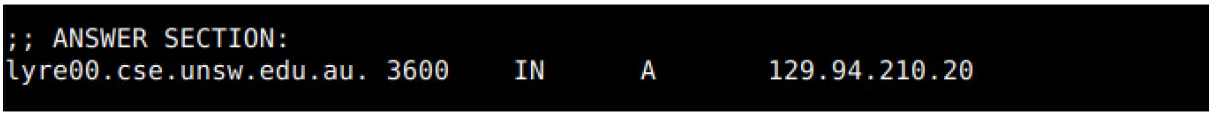
```
;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        900     IN      A       129.94.0.192
ns2.unsw.edu.au.        900     IN      A       129.94.0.193
ns3.unsw.edu.au.        900     IN      A       192.155.82.178
ns1.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.       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

dig @ns1.unsw.edu.au cse.unsw.edu.au NS



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

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



```
;; ANSWER SECTION:
lyre00.cse.unsw.edu.au. 3600    IN      A       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.
A machine can have several IP addresses, and these IP addresses have multiple aliases for one canonical name.