Exercise 3: Digging into DNS

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

- IP Address: 150.203.161.98
- DNS query Type: A

```
[MacPro:~ macpro$ dig www.cecs.anu.edu.au A

; <<>> DiG 9.10.6 <<>> www.cecs.anu.edu.au A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50399
;; 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.        3304    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3304    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        3304    IN      NS      ns2.cecs.anu.edu.au.

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

;; Query time: 48 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Mon Mar 11 21:01:36 AEDT 2019
;; MSG SIZE  rcvd: 271
```

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

- canonical name: rproxy.cecs.anu.edu.au (see picture in Q1)
- IP address: 150.203.161.98 (see picture in Q1)
- reason: Canonical names are usually very long and hard to remember. An alias is more easy to remember.

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, it tells me what DNS servers can provide an authoritative answer to my query. In the output, I can see that there are 3 DNS servers ns2/ns3/ ns4.cecs.au.edu which are responsible for the domain name.
- In the Additional section, it simply lists the IP addresses of DNS servers in the Authority Section. As expected, there are 3 IP addresses corresponding to the 3 DNS servers with authority.

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

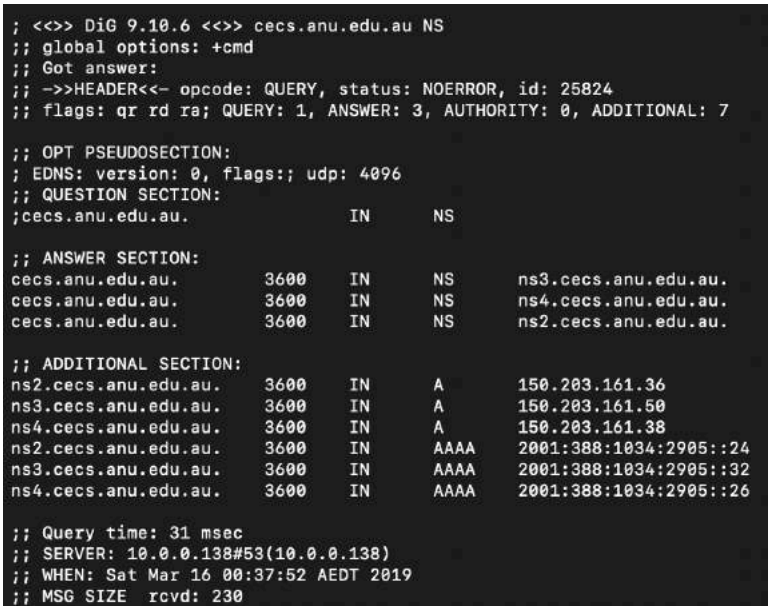
- local nameserver IP address: 10.0.0.138 (see picture in Q1)

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?

- DNS nameservers:

- ns2.cecs.anu.edu.au. IP: 150.203.161.36
- ns3.cecs.anu.edu.au. IP: 150.203.161.50
- ns4.cecs.anu.edu.au. IP: 150.203.161.38

- DNS query type: NS.



```
; <<>> DiG 9.10.6 <<>> cecs.anu.edu.au NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25824
;; 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.        3600    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3600    IN      NS      ns2.cecs.anu.edu.au.

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

;; Query time: 31 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Sat Mar 16 00:37:52 AEDT 2019
;; MSG SIZE  rcvd: 230
```

Question 6. What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?

- DNS Name: www.engineering.unsw.edu.au
- DNS query : dig –x 149.171.158.109

```
; <<>> DiG 9.10.6 <<>> -x 149.171.158.109
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11090
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;109.158.171.149.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
109.158.171.149.in-addr.arpa. 3392 IN   PTR     www.engineering.unsw.edu.au.
109.158.171.149.in-addr.arpa. 3392 IN   PTR     engplws008.ad.unsw.edu.au.
109.158.171.149.in-addr.arpa. 3392 IN   PTR     engplws008.eng.unsw.edu.au.

;; Query time: 4 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Mon Mar 11 21:28:20 AEDT 2019
;; MSG SIZE  rcvd: 166
```

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)

- No, the flags do not contain aa.
- This is because it has authority for only the cse.unsw.edu.au domain and not for the Yahoo domain.

```
; <<>> DiG 9.10.6 <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 6459
;; 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: 12 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Mon Mar 11 22:23:18 AEDT 2019
;; MSG SIZE  rcvd: 38
```

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

- Can not get an authoritative answer, the flags do not contain aa. This has perhaps to do with how the ANU network is configured.

```
; <<>> DiG 9.10.6 <<>> @ns2.cecs.anu.edu.au yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 63953
;; 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: 23 msec
;; SERVER: 150.203.161.36#53(150.203.161.36)
;; WHEN: Mon Mar 11 22:16:53 AEDT 2019
;; 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?

- Type of DNS query: **MX**
- DNS nameservers for yahoo.com: **ns1/ns2/ns3/ns4/ns5.yahoo.com**

```
; <<>> DiG 9.10.6 <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54725
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9
;; 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 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.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.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.          1209600 IN      A       203.84.221.53
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          1209600 IN      A       119.160.253.83
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          86400   IN      AAAA    2406:8600:b8:fe03::1003

;; Query time: 307 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Mon Mar 11 23:22:54 AEDT 2019
;; MSG SIZE  rcvd: 371
```

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).

1. First, find the name server (query type NS) of the "." domain (root domain).

2. Query this nameserver to find the authoritative name server for the "au." domain.

3. Query this second server to find the authoritative nameserver for the "edu.au." domain.

4. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au".

5. Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au.

6. 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. Assuming that current hostname is lyre00.cse.unsw.edu.au. First query for the IP address of the root nameservers as Picture1.
- 2. Next query one of the root nameservers as Picture2.
- 3. Next query one of .au nameservers as Picture3.
- 4. Next query one of edu.au nameservers as Picture4.
- 5. Next query one of unsw.edu.au nameservers as Picture5.
- 6. Next query one of cse.unsw.edu.au nameservers as Picture6.

```
; <<>> DiG 9.10.6 <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62326
;; 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:
.                       186547  IN      NS      a.root-servers.net.
.                       186547  IN      NS      b.root-servers.net.
.                       186547  IN      NS      c.root-servers.net.
.                       186547  IN      NS      d.root-servers.net.
.                       186547  IN      NS      e.root-servers.net.
.                       186547  IN      NS      f.root-servers.net.
.                       186547  IN      NS      g.root-servers.net.
.                       186547  IN      NS      h.root-servers.net.
.                       186547  IN      NS      i.root-servers.net.
.                       186547  IN      NS      j.root-servers.net.
.                       186547  IN      NS      k.root-servers.net.
.                       186547  IN      NS      l.root-servers.net.
.                       186547  IN      NS      m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3599288 IN      A       198.41.0.4
b.root-servers.net.     3599288 IN      A       199.9.14.201
c.root-servers.net.     3599288 IN      A       192.33.4.12
d.root-servers.net.     3599288 IN      A       199.7.91.13
e.root-servers.net.     3599288 IN      A       192.203.230.10
f.root-servers.net.     3599288 IN      A       192.5.5.241
g.root-servers.net.     3599288 IN      A       192.112.36.4
h.root-servers.net.     3599288 IN      A       198.97.190.53
i.root-servers.net.     3599288 IN      A       192.36.148.17
j.root-servers.net.     3599288 IN      A       192.58.128.30
k.root-servers.net.     3599288 IN      A       193.0.14.129
l.root-servers.net.     3599288 IN      A       199.7.83.42
m.root-servers.net.     3599288 IN      A       202.12.27.33
a.root-servers.net.     3599288 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3599994 IN      AAAA    2001:500:200::b
c.root-servers.net.     3599288 IN      AAAA    2001:500:2::c
d.root-servers.net.     3599288 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3599288 IN      AAAA    2001:500:a8::e
f.root-servers.net.     3599288 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3599288 IN      AAAA    2001:500:12::d0d
h.root-servers.net.     3599288 IN      AAAA    2001:500:1::53
i.root-servers.net.     3599288 IN      AAAA    2001:7fe::53
j.root-servers.net.     3599288 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3599288 IN      AAAA    2001:7fd::1
l.root-servers.net.     3599288 IN      AAAA    2001:500:9f::42
m.root-servers.net.     3599288 IN      AAAA    2001:dc3::35

;; Query time: 14 msec
;; SERVER: 10.0.0.138#53(10.0.0.138)
;; WHEN: Mon Mar 11 22:27:55 AEDT 2019
;; MSG SIZE  rcvd: 811
```

```
; <<>> DiG 9.10.6 <<>> @198.41.0.4 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24784
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 20
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      b.au.
au.                     172800  IN      NS      c.au.
au.                     172800  IN      NS      d.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.
au.                     172800  IN      NS      u.au.
au.                     172800  IN      NS      v.au.

;; ADDITIONAL SECTION:
a.au.                   172800  IN      A       58.65.254.73
b.au.                   172800  IN      A       58.65.253.73
c.au.                   172800  IN      A       162.159.24.179
d.au.                   172800  IN      A       162.159.25.38
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
u.au.                   172800  IN      A       211.29.133.32
v.au.                   172800  IN      A       202.12.31.53
a.au.                   172800  IN      AAAA    2407:6e00:254:306::73
b.au.                   172800  IN      AAAA    2407:6e00:253:306::73
c.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
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
v.au.                   172800  IN      AAAA    2001:dd8:12::53

;; Query time: 263 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Mon Mar 11 22:31:26 AEDT 2019
;; MSG SIZE  rcvd: 623
```

```
; <<>> DiG 9.10.6 <<>> @58.65.254.73 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30211
;; 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:
;lyre00.cse.unsw.edu.au.                IN      NS

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

;; Query time: 22 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Mon Mar 11 22:34:16 AEDT 2019
;; MSG SIZE  rcvd: 291
```

```
; <<>> DiG 9.10.6 <<>> @65.22.196.1 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30506
;; 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:
;lyre00.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.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: 22 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Mon Mar 11 22:37:10 AEDT 2019
;; MSG SIZE  rcvd: 209
```

```
; <<>> DiG 9.10.6 <<>> @129.94.0.192 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9292
;; 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:
;lyre00.cse.unsw.edu.au.                IN      NS

;; 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: 11 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Mon Mar 11 22:38:42 AEDT 2019
;; MSG SIZE  rcvd: 171
```

```
; <<>> DiG 9.10.6 <<>> @129.94.242.33 lyre00.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60902
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; 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.unsw.edu.au.
cse.unsw.edu.au.        3600    IN      NS      beethoven.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  129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 3600 IN A  129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 3600 IN A  129.94.242.2

;; Query time: 14 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Mon Mar 11 22:42:35 AEDT 2019
;; MSG SIZE  rcvd: 187
```

The IP address for lyre00.cse.unsw.edu.au is 129.94.210.20.

Following the iterative query process starting at the root nameserver, we had to query 5 DNS servers:

1: a.root-servers.net, 2: a.au, 3: q.au, 4 : unsw.edu.au, 5: maestro.orchestra.cse.unsw.edu.au

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

- Yes, a machine may have several network interfaces. Moreover, a network interface can have several IP addresses associated with it at any given time. An IP address may have been associated with several hostnames (additional hostnames are known as "aliases").