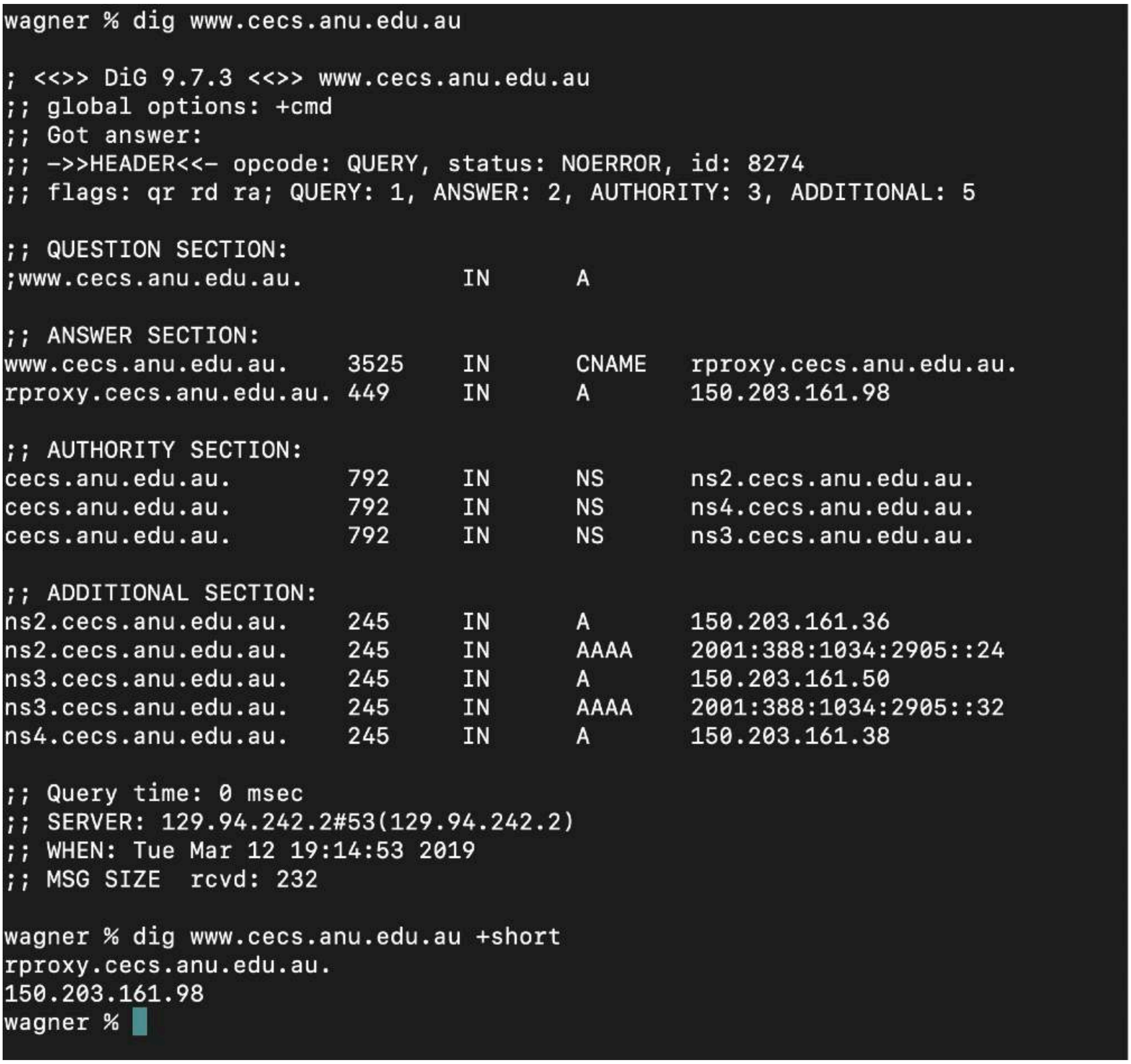
Lab Exercise 4: Exploring TCP

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?

Solution 1 : After running dig **www.cecs.anu.edu.au** I got the result below,



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

; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8274
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3525    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 449     IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        792     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        792     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        792     IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    245     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    245     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    245     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    245     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    245     IN      A       150.203.161.38

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 12 19:14:53 2019
;; MSG SIZE  rcvd: 232

wagner % dig www.cecs.anu.edu.au +short
rproxy.cecs.anu.edu.au.
150.203.161.98
wagner %
```

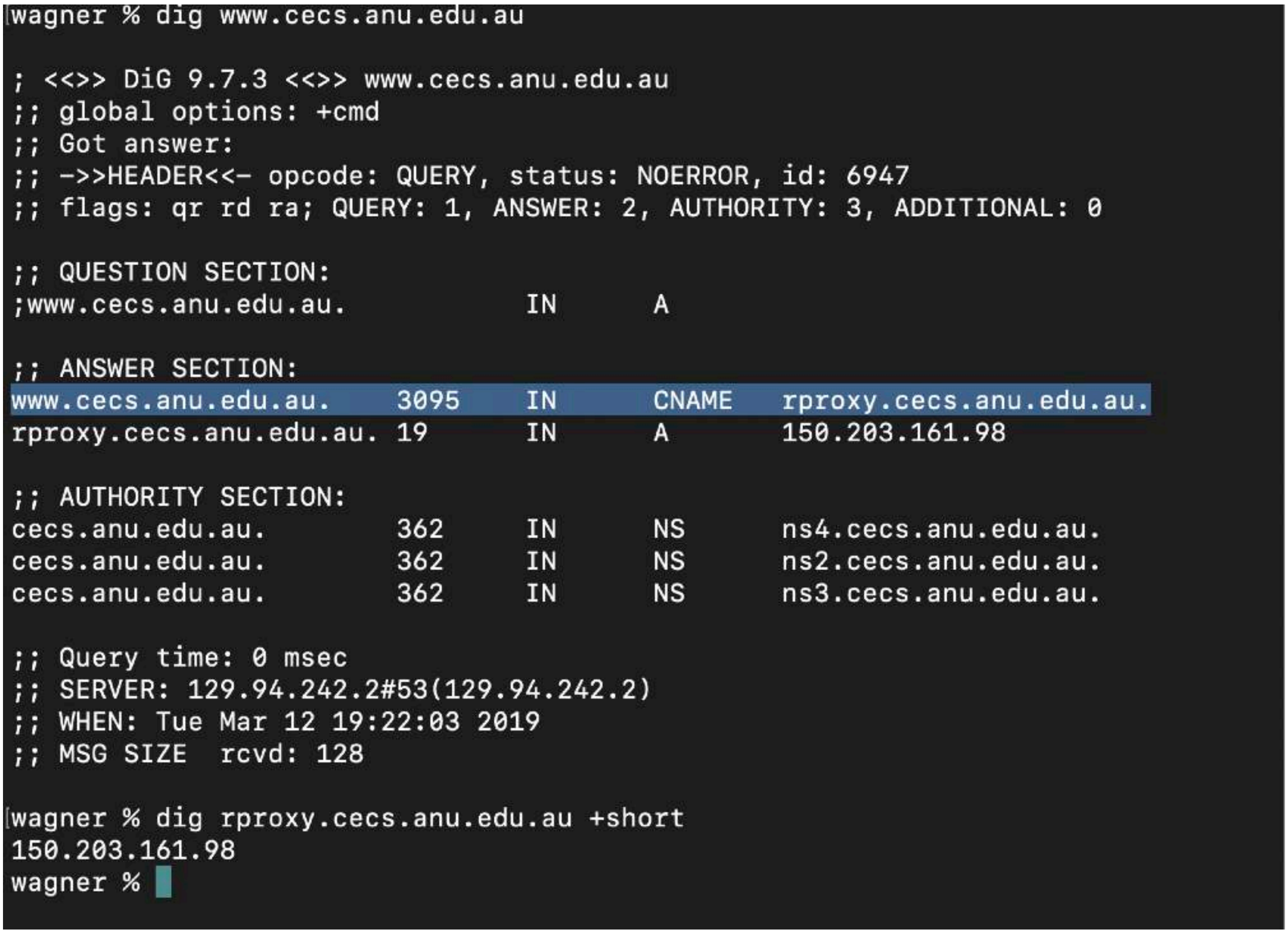
Query : dig www.cecs.anu.edu.au + short

IP : 150.203.161.98

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.

Solution 2 : Canonical name : **rproxy.cecs.anu.edu.au**

IP : 150.203.161.98



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

; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6947
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3095    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 19      IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        362     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        362     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        362     IN      NS      ns3.cecs.anu.edu.au.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 12 19:22:03 2019
;; MSG SIZE  rcvd: 128

wagner % dig rproxy.cecs.anu.edu.au +short
150.203.161.98
wagner %
```

Having an alias for this server is a better option, as most users are not used in typing the host name. They prefer the suffix “www” in front of the request.

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

Solution 3 : As the record is in the form (Name, Value, Type, TTL) ,
The authority section provides us with three different columns stating the domain name to be **cecs.anu.edu.au**. The type of the DNS query is stated as "NS" and the value is the host-name of an authoritative DNS server which are ns3.cecs.anu.edu.au, ns2.cecs.anu.edu.au and ns4.cecs.anu.edu.au
These host names can be further used to find the IP addresses for hosts in domain.
The additional section contains a Type A record providing the IP address for the host names listed in the authority sections.

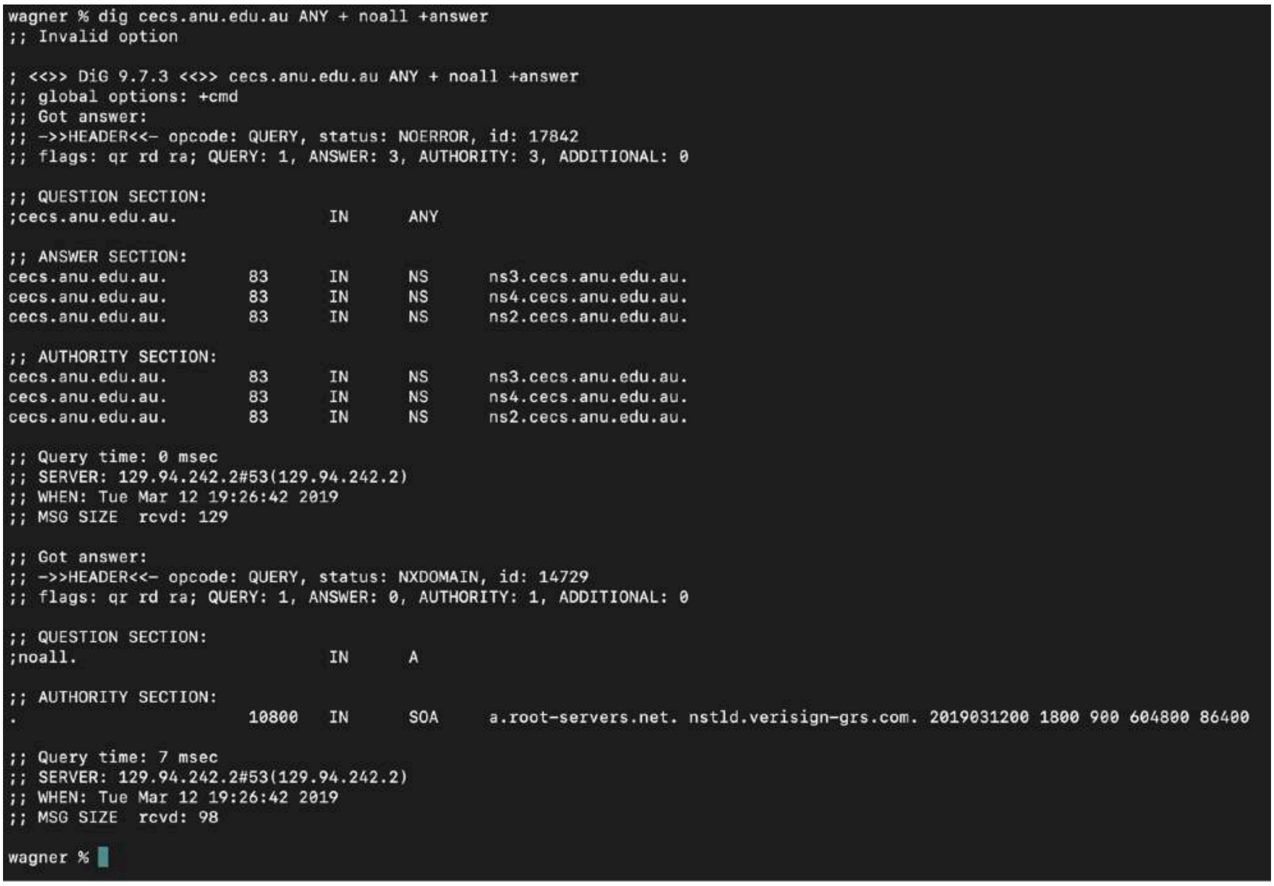
Question 4 : What is the IP address of the local name server for your machine?

Solution 4 : IP : 121.211.192.123

Question 5 : What are the DNS name servers 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?

Solution 5 : To get the information about the DNS servers ,

Query : dig cecs.anu.edu.au ANY + noall +answer



```
wagner % dig cecs.anu.edu.au ANY + noall +answer
;; Invalid option

; <<>> DiG 9.7.3 <<>> cecs.anu.edu.au ANY + noall +answer
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17842
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;cecs.anu.edu.au.               IN      ANY

;; ANSWER SECTION:
cecs.anu.edu.au.        83      IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        83      IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        83      IN      NS      ns2.cecs.anu.edu.au.

;; AUTHORITY SECTION:
cecs.anu.edu.au.        83      IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        83      IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        83      IN      NS      ns2.cecs.anu.edu.au.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 12 19:26:42 2019
;; MSG SIZE  rcvd: 129

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14729
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;noall.                         IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2019031200 1800 900 604800 86400

;; Query time: 7 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 12 19:26:42 2019
;; MSG SIZE  rcvd: 98

wagner %
```

For IP addresses,
Query : dig name_of_host +short

DNS server names	IP
ns2.cecs.anu.edu.au.	150.203.161.36
ns3.cecs.anu.edu.au.	150.203.161.50
ns4.cecs.anu.edu.au.	150.203.161.38

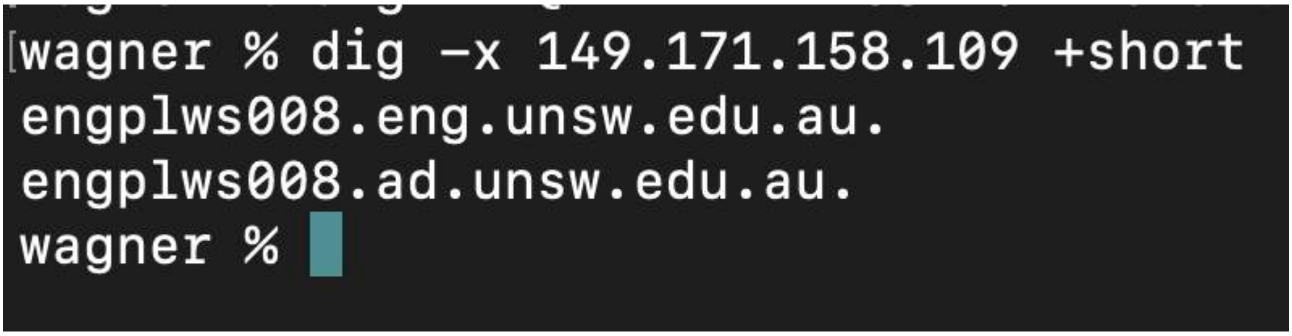
Question 6 : What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?

Solution 6 : The following output was observed,

Name : www.engineering.unsw.edu.au

Query : dig -x 149.171.158.109 +short

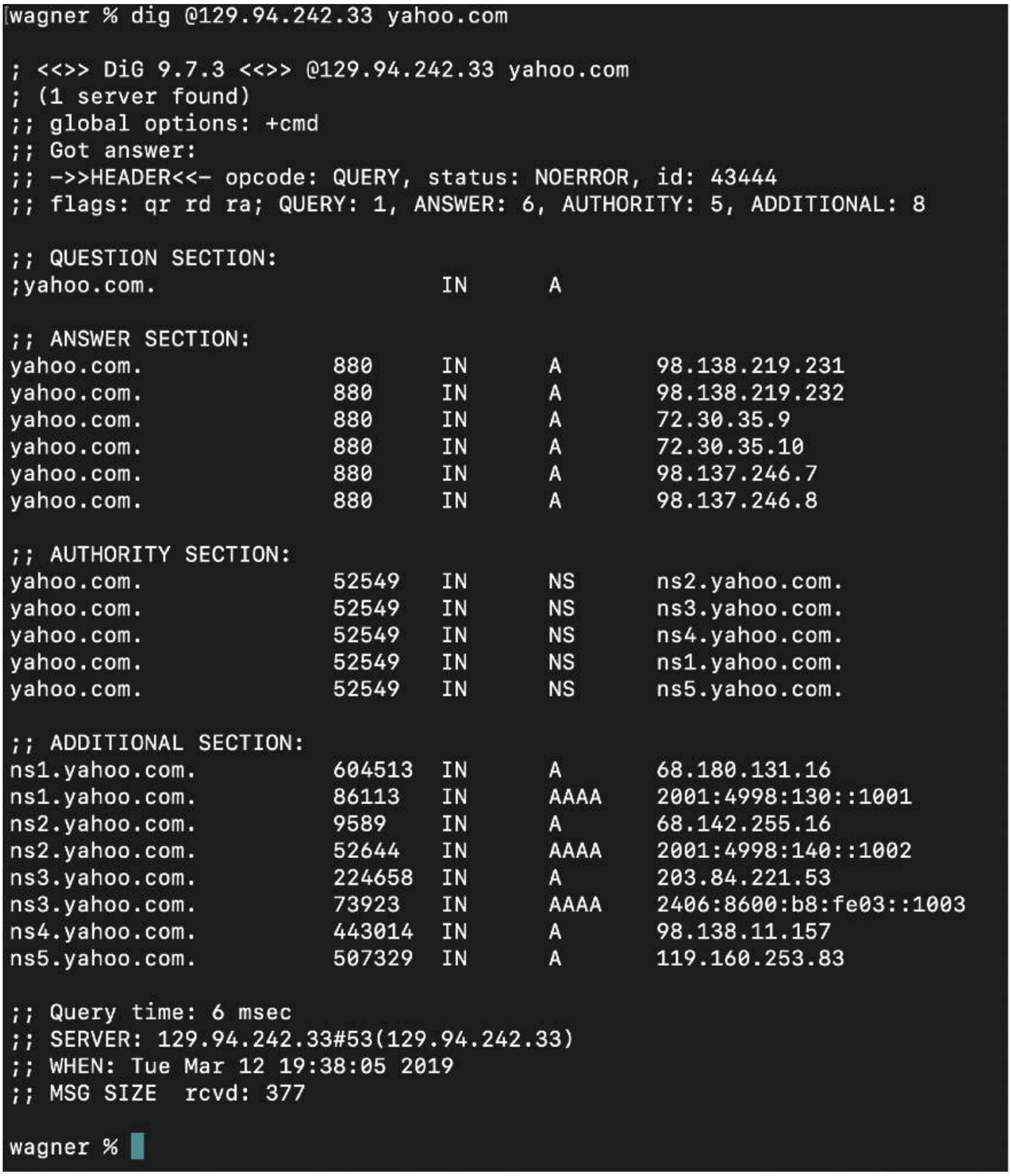
The same IP address also corresponds to engplws008.ad.unsw.edu.au.



```
[wagner % dig -x 149.171.158.109 +short
 engplws008.eng.unsw.edu.au.
 engplws008.ad.unsw.edu.au.
 wagner % 
```

Question 7 : Run dig and query the CSE name server (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?

Solution 7 : Query : dig @129.94.242.33 yahoo.com



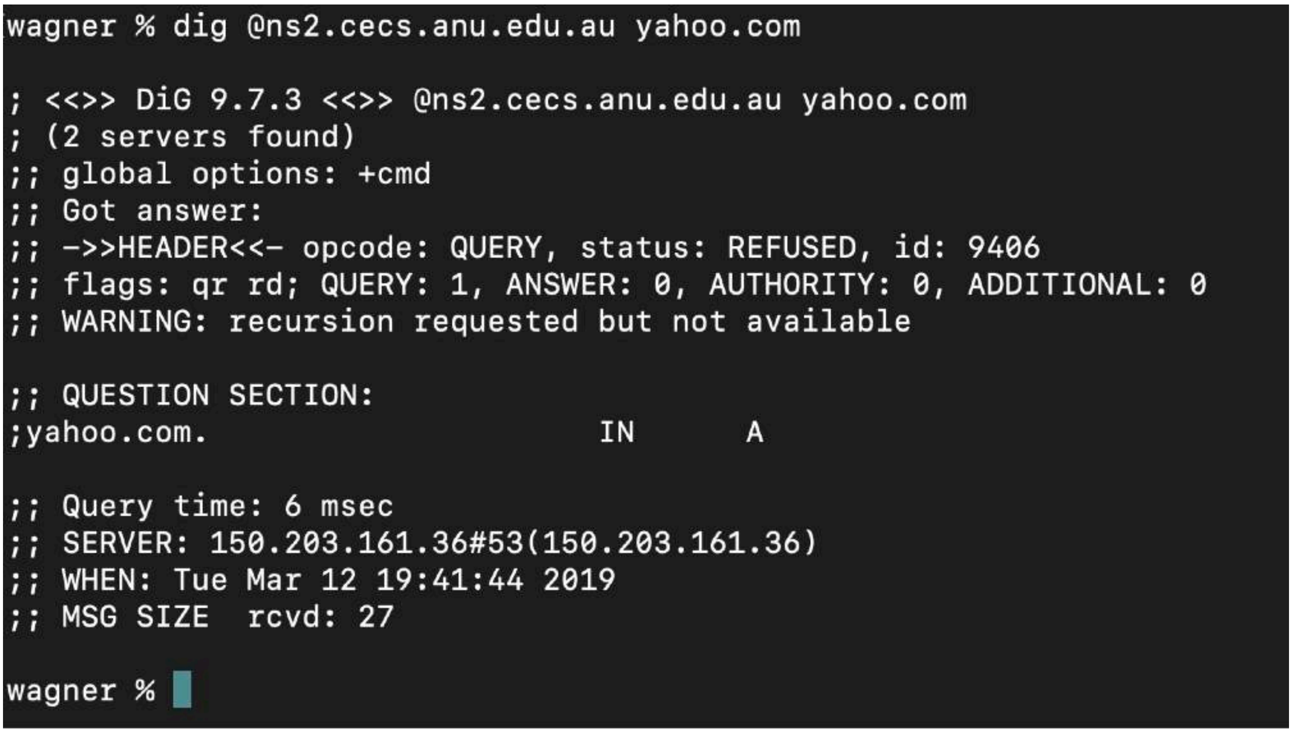
```
[wagner % dig @129.94.242.33 yahoo.com

; <<>> DiG 9.7.3 <<>> @129.94.242.33 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43444
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              880     IN      A       98.138.219.231
yahoo.com.              880     IN      A       98.138.219.232
yahoo.com.              880     IN      A       72.30.35.9
yahoo.com.              880     IN      A       72.30.35.10
yahoo.com.              880     IN      A       98.137.246.7
yahoo.com.              880     IN      A       98.137.246.8

;; AUTHORITY SECTION:
yahoo.com.              52549   IN      NS      ns2.yahoo.com.
yahoo.com.              52549   IN      NS      ns3.yahoo.com.
yahoo.com.              52549   IN      NS      ns4.yahoo.com.
yahoo.com.              52549   IN      NS      ns1.yahoo.com.
yahoo.com.              52549   IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          604513  IN      A       68.180.131.16
ns1.yahoo.com.          86113   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          9589    IN      A       68.142.255.16
ns2.yahoo.com.          52644   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          224658  IN      A       203.84.221.53
ns3.yahoo.com.          73923   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          443014  IN      A       98.138.11.157
ns5.yahoo.com.          507329  IN      A       119.160.253.83

;; Query time: 6 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Mar 12 19:38:05 2019
;; MSG SIZE  rcvd: 377

wagner %
```

No, there is not an authoritative answer because there is no “AA” flag in the authoritative section.This is because it just has authority for cse.unsw.edu.au domain and not yahoo.com.

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

Solution 8 :

The Query “dig @ns2.cecs.anu.edu.au yahoo.com" gives the WARNING : recursion requested but not available.The reason could be that the DNS server is not replying to the query.



```
wagner % dig @ns2.cecs.anu.edu.au yahoo.com

; <<>> DiG 9.7.3 <<>> @ns2.cecs.anu.edu.au yahoo.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 9406
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; Query time: 6 msec
;; SERVER: 150.203.161.36#53(150.203.161.36)
;; WHEN: Tue Mar 12 19:41:44 2019
;; MSG SIZE  rcvd: 27

wagner %
```

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

Solution 9 : Query : dig yahoo.com gives us,

```
yahoo.com.      47619   IN   NS  ns5.yahoo.com.
yahoo.com.      47619   IN   NS  ns4.yahoo.com.
yahoo.com.      47619   IN   NS  ns1.yahoo.com.
yahoo.com.      47619   IN   NS  ns3.yahoo.com.
yahoo.com.      47619   IN   NS  ns2.yahoo.com.
```

To obtain the authoritative answer for any one (ns1.yahoo.com.) server
Query : dig @ns1.yahoo.com. yahoo.com MX.

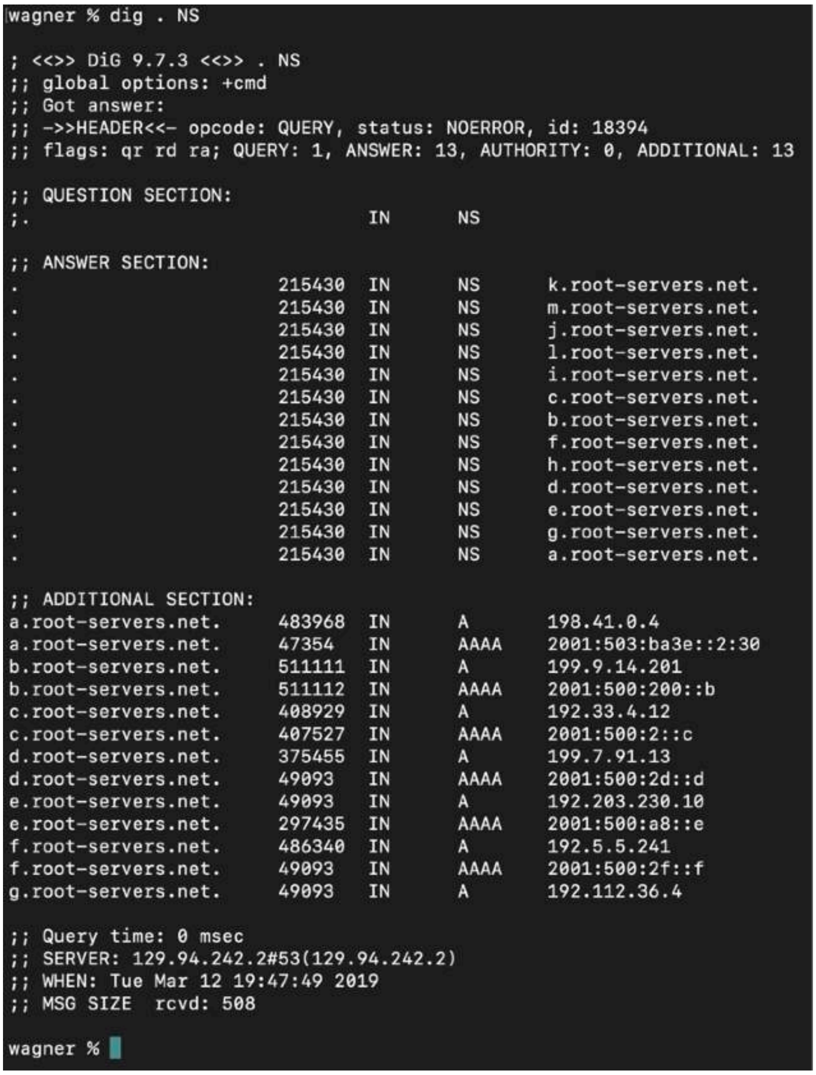
The output is something like,

```
yahoo.com.      1800    IN   MX 1 mta5.am0.yahoodns.net.
yahoo.com.      1800    IN   MX 1 mta6.am0.yahoodns.net.
yahoo.com.      1800    IN   MX 1 mta7.am0.yahoodns.net.
```

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 name server to find the authoritative name server for the "au." domain. Query this second server to find the authoritative name server for the "edu.au." domain. Now query this name server to find the authoritative name server for "unsw.edu.au". Next query the name server of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the name server for 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?

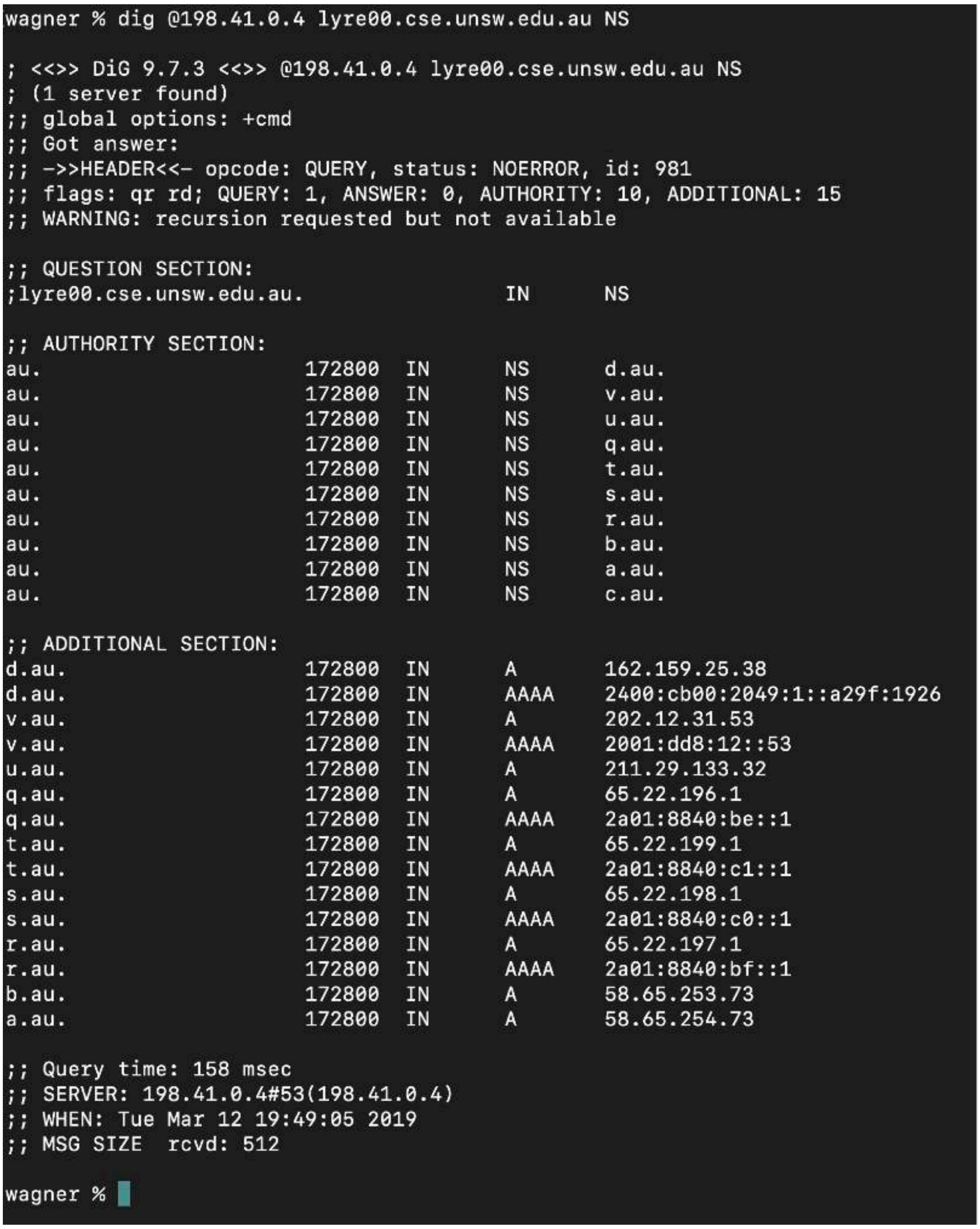
Solution 10 :

Query 1 : dig . NS



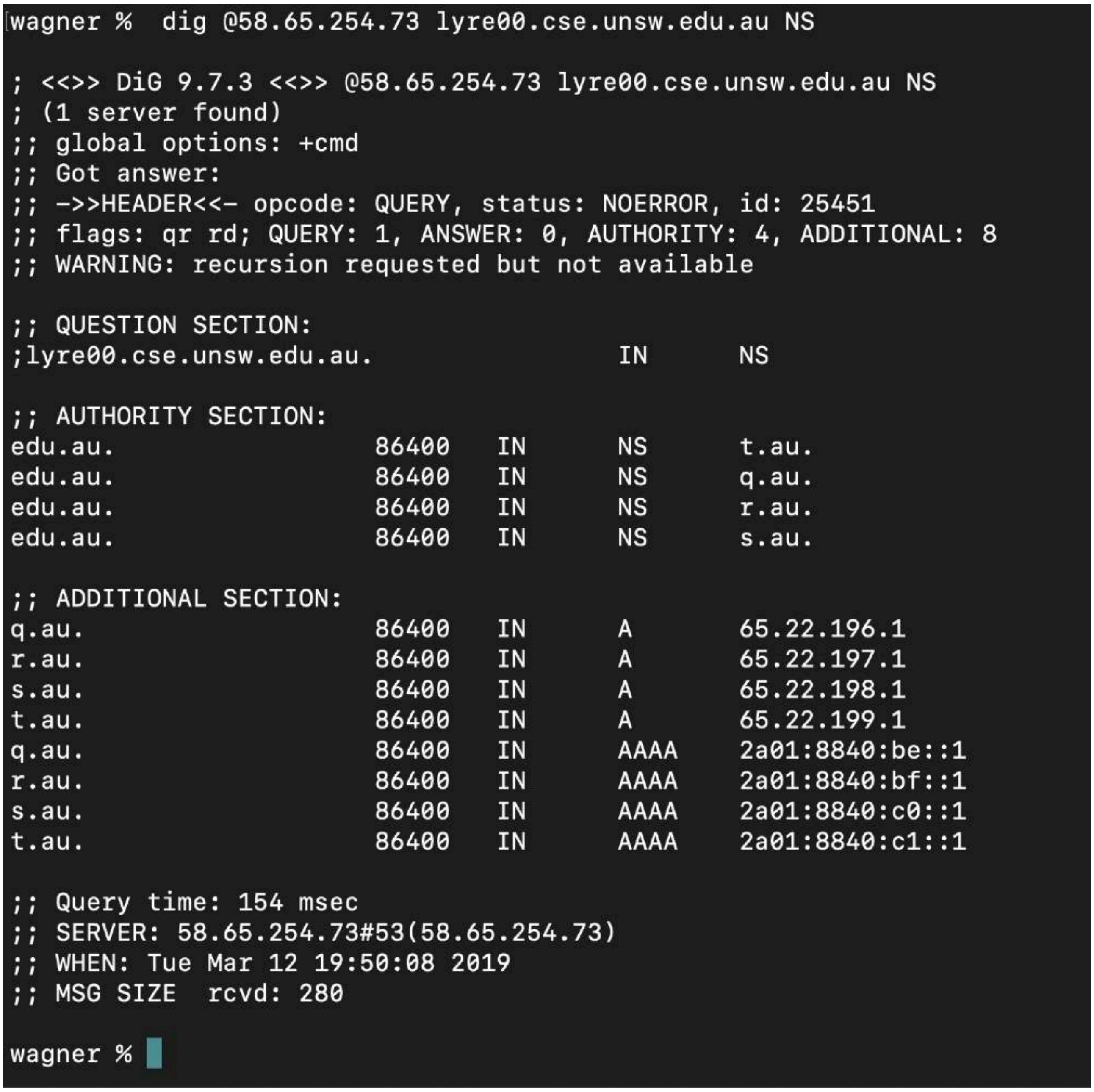
```
wagner % dig . NS

; <<>> DiG 9.7.3 <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18394
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       215430  IN      NS      k.root-servers.net.
.                       215430  IN      NS      m.root-servers.net.
.                       215430  IN      NS      j.root-servers.net.
.                       215430  IN      NS      l.root-servers.net.
.                       215430  IN      NS      i.root-servers.net.
.                       215430  IN      NS      c.root-servers.net.
.                       215430  IN      NS      b.root-servers.net.
.                       215430  IN      NS      f.root-servers.net.
.                       215430  IN      NS      h.root-servers.net.
.                       215430  IN      NS      d.root-servers.net.
.                       215430  IN      NS      e.root-servers.net.
.                       215430  IN      NS      g.root-servers.net.
.                       215430  IN      NS      a.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     483968  IN      A       198.41.0.4
a.root-servers.net.     47354   IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     511111  IN      A       199.9.14.201
b.root-servers.net.     511112  IN      AAAA    2001:500:200::b
c.root-servers.net.     408929  IN      A       192.33.4.12
c.root-servers.net.     407527  IN      AAAA    2001:500:2::c
d.root-servers.net.     375455  IN      A       199.7.91.13
d.root-servers.net.     49093   IN      AAAA    2001:500:2d::d
e.root-servers.net.     49093   IN      A       192.203.230.10
e.root-servers.net.     297435  IN      AAAA    2001:500:a8::e
f.root-servers.net.     486340  IN      A       192.5.5.241
f.root-servers.net.     49093   IN      AAAA    2001:500:2f::f
g.root-servers.net.     49093   IN      A       192.112.36.4

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 12 19:47:49 2019
;; MSG SIZE  rcvd: 508

wagner %
```

Query 2 : dig @198.41.0.4 lyre00.cse.unsw.edu.au NS



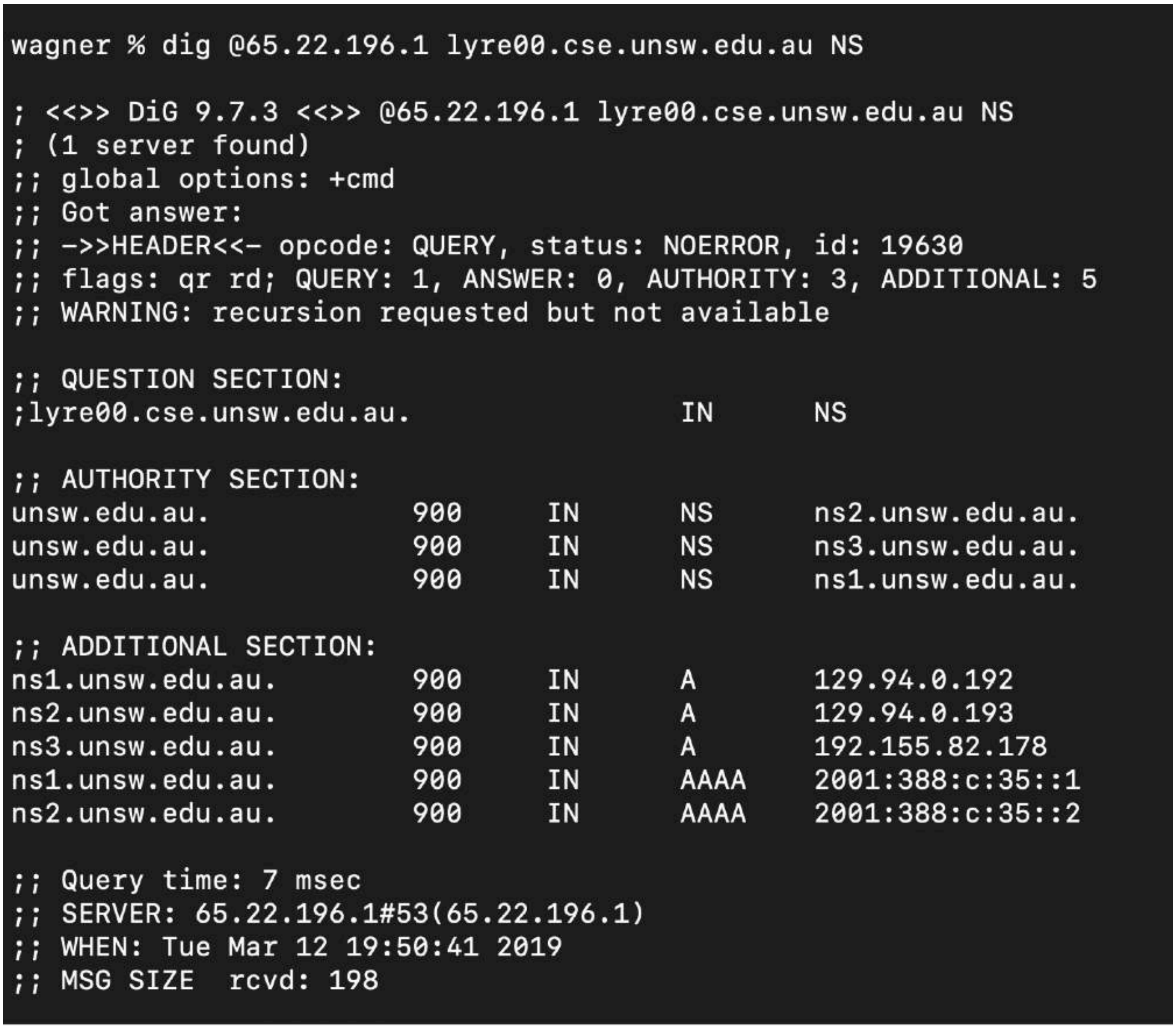
```
wagner % dig @198.41.0.4 lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @198.41.0.4 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 981
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
au.                     172800  IN      NS      d.au.
au.                     172800  IN      NS      v.au.
au.                     172800  IN      NS      u.au.
au.                     172800  IN      NS      q.au.
au.                     172800  IN      NS      t.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      b.au.
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      c.au.

;; ADDITIONAL SECTION:
d.au.                   172800  IN      A       162.159.25.38
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
v.au.                   172800  IN      A       202.12.31.53
v.au.                   172800  IN      AAAA    2001:dd8:12::53
u.au.                   172800  IN      A       211.29.133.32
q.au.                   172800  IN      A       65.22.196.1
q.au.                   172800  IN      AAAA    2a01:8840:be::1
t.au.                   172800  IN      A       65.22.199.1
t.au.                   172800  IN      AAAA    2a01:8840:c1::1
s.au.                   172800  IN      A       65.22.198.1
s.au.                   172800  IN      AAAA    2a01:8840:c0::1
r.au.                   172800  IN      A       65.22.197.1
r.au.                   172800  IN      AAAA    2a01:8840:bf::1
b.au.                   172800  IN      A       58.65.253.73
a.au.                   172800  IN      A       58.65.254.73

;; Query time: 158 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Mar 12 19:49:05 2019
;; MSG SIZE  rcvd: 512

wagner %
```

Query 3 : dig @ 58.65.254.73 lyre00.cse.unsw.edu.au NS



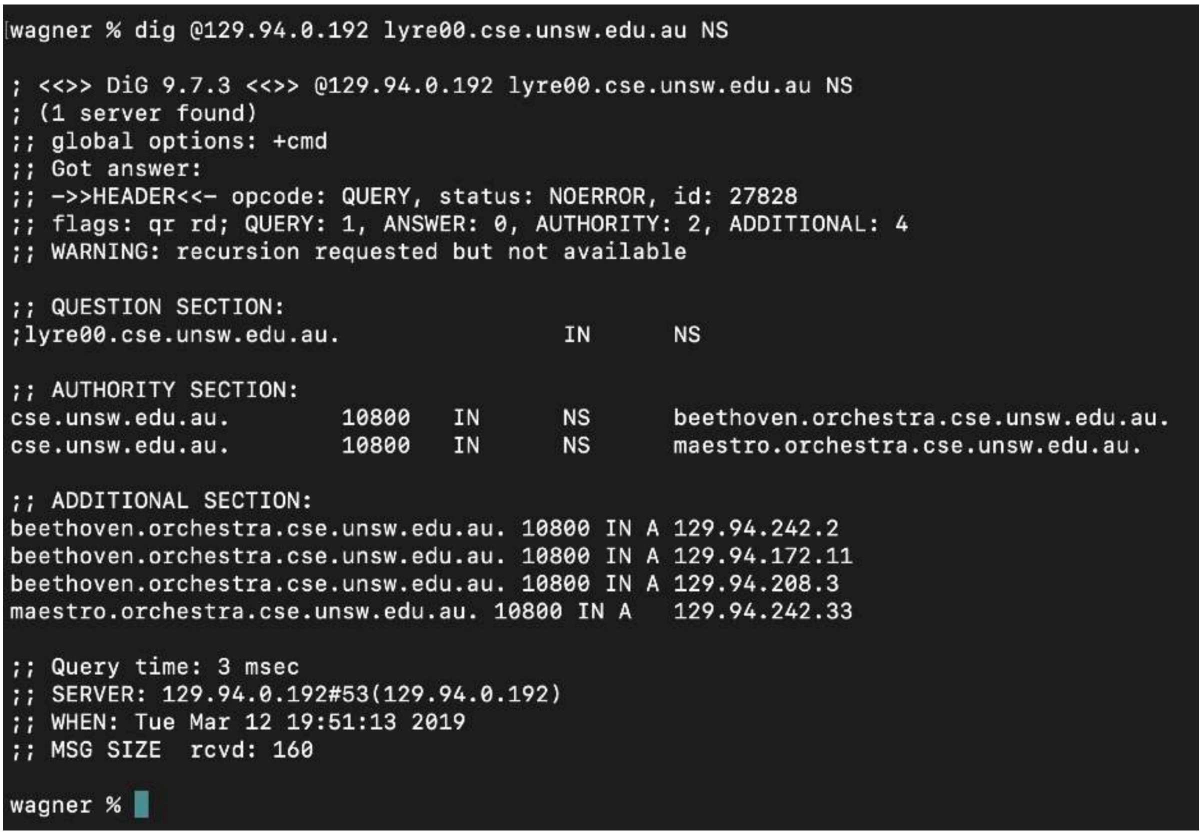
```
wagner %  dig @58.65.254.73 lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @58.65.254.73 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25451
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

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

;; Query time: 154 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Tue Mar 12 19:50:08 2019
;; MSG SIZE  rcvd: 280

wagner %
```

Query 4 : dig @65.22.196.1 lyre00.cse.unsw.edu.au NS



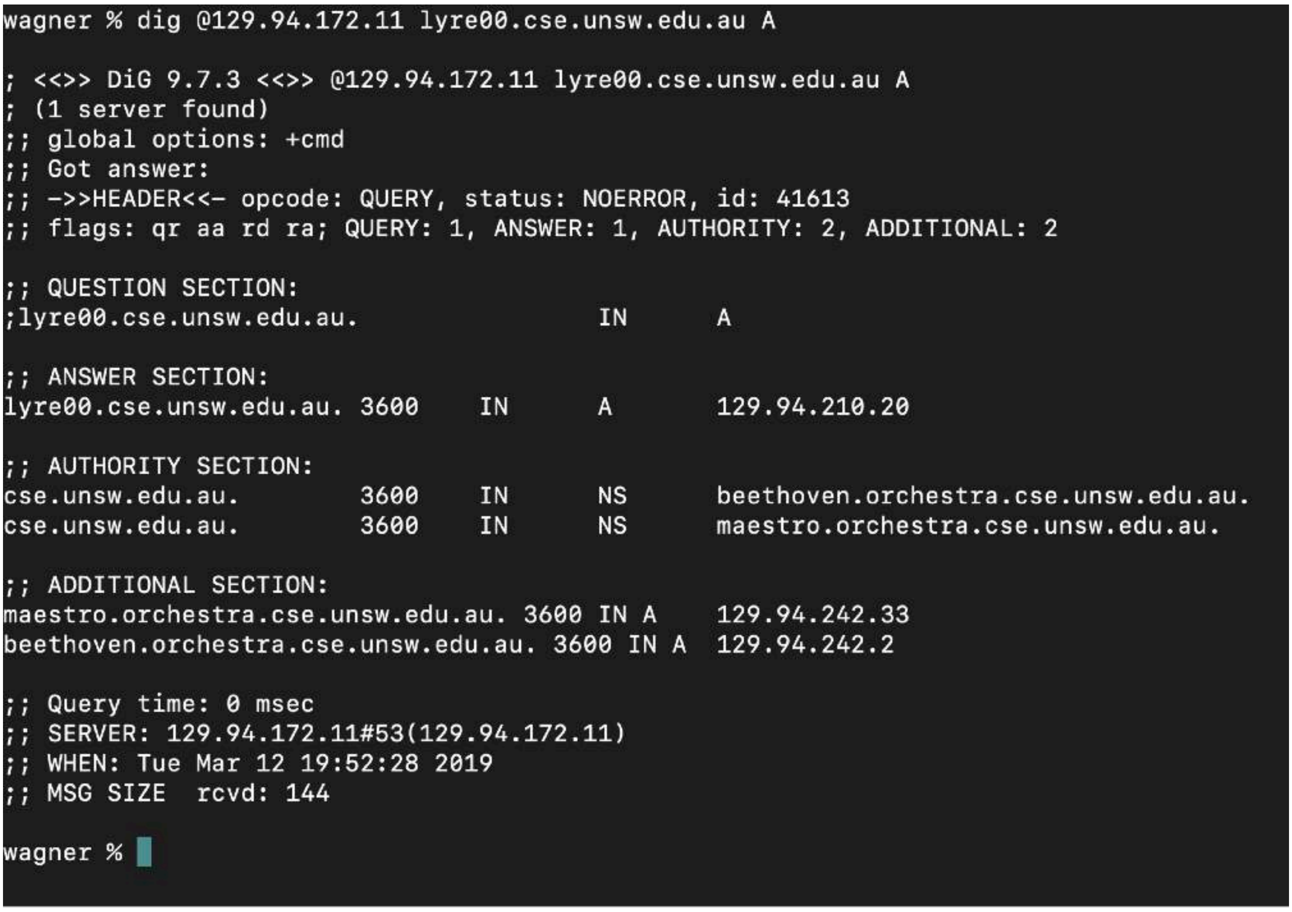
```
wagner % dig @65.22.196.1 lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @65.22.196.1 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19630
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

;; 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: 7 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Tue Mar 12 19:50:41 2019
;; MSG SIZE  rcvd: 198
```

Query 5: dig @129.94.0.192 lyre00.cse.unsw.edu.au NS



```
[wagner % dig @129.94.0.192 lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @129.94.0.192 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27828
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; 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 129.94.242.2
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

;; Query time: 3 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Tue Mar 12 19:51:13 2019
;; MSG SIZE  rcvd: 160

wagner %
```

Query 6 : dig @129.94.172.11 lyre00.cse.unsw.edu.au A



```
wagner % dig @129.94.172.11 lyre00.cse.unsw.edu.au A

; <<>> DiG 9.7.3 <<>> @129.94.172.11 lyre00.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41613
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; 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: 129.94.172.11#53(129.94.172.11)
;; WHEN: Tue Mar 12 19:52:28 2019
;; MSG SIZE  rcvd: 144

wagner %
```

We are now being referred to lyre00.cse.unsw.edu.au and the IP address is 129.94.210.20 and we had to 5 DNS servers to get the authoritative answer.

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

Solution 11 : Yes, one physical machine can have several names and/or IP addresses associated with it.