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?

```
grieg % 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: 47179
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    2518    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1183    IN      A       150.203.161.98

;; AUTHORITY SECTION:
edu.au.                 15186   IN      NS      s.au.
edu.au.                 15186   IN      NS      t.au.
edu.au.                 15186   IN      NS      r.au.
edu.au.                 15186   IN      NS      q.au.

;; ADDITIONAL SECTION:
q.au.                   10710   IN      A       65.22.196.1
q.au.                   2426    IN      AAAA    2a01:8840:be::1
r.au.                   11768   IN      A       65.22.197.1
r.au.                   11447   IN      AAAA    2a01:8840:bf::1
s.au.                   18769   IN      A       65.22.198.1
t.au.                   18344   IN      A       65.22.199.1
t.au.                   235     IN      AAAA    2a01:8840:c1::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug  9 10:52:16 2018
;; MSG SIZE  rcvd: 286
```

The IP address is : 150.203.161.98

Type of DNS query: A

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.

The canonical name: rproxy.cecs.anu.edu.au

The IP address is: 150.203.161.98

Having an alias can be used to provide multiple network addresses on a single physical interface. It can prove convenient when running multiple services. If the IP address ever changes, one only has to record the change in one place within the network.

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

An authoritative stores all DNS names in the domain that it has authority for.

Additional section is the authoritative servers that may be used.

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

IP: 129.94.242.2 (In Server Section)

Question 5. What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and notwww.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

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

; <<>> DiG 9.7.3 <<>> cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63740
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

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

;; ANSWER SECTION:
cecs.anu.edu.au.        3465    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        441     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        441     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        441     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    441     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    441     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    441     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    441     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    441     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    441     IN      AAAA    2001:388:1034:2905::26

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug  9 10:56:52 2018
;; MSG SIZE  rcvd: 235
```

They are:

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

The type of DNS query is NS.

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?

```
grieg % dig 149.171.158.109

; <<>> DiG 9.7.3 <<>> 149.171.158.109
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6801
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;149.171.158.109.               IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2018080801 1800 900 604800

;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug  9 11:02:38 2018
;; MSG SIZE  rcvd: 108
```

DNS name : a.root-servers.net nstld.verisign-grs.com

Type: SOA

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)

```
grieg % 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: 36183
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              894     IN      A       98.138.219.232
yahoo.com.              894     IN      A       72.30.35.9
yahoo.com.              894     IN      A       72.30.35.10
yahoo.com.              894     IN      A       98.137.246.7
yahoo.com.              894     IN      A       98.137.246.8
yahoo.com.              894     IN      A       98.138.219.231

;; AUTHORITY SECTION:
yahoo.com.              14893   IN      NS      ns1.yahoo.com.
yahoo.com.              14893   IN      NS      ns4.yahoo.com.
yahoo.com.              14893   IN      NS      ns3.yahoo.com.
yahoo.com.              14893   IN      NS      ns5.yahoo.com.
yahoo.com.              14893   IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          409392  IN      A       68.180.131.16
ns1.yahoo.com.          5005    IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86223   IN      A       68.142.255.16
ns2.yahoo.com.          18906   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          176555  IN      A       203.84.221.53
ns3.yahoo.com.          92150   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          93031   IN      A       98.138.11.157
ns5.yahoo.com.          79095   IN      A       119.160.253.83

;; Query time: 7 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Thu Aug  9 11:04:23 2018
;; MSG SIZE  rcvd: 377
```

No, it is not an authoritative answer, because there is not an “aa” flags which means “authoritative answer” in Flags.

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

```
grieg % dig 150.203.161.36 ns3.cecs.anu.edu.au

; <<>> DiG 9.7.3 <<>> 150.203.161.36 ns3.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23529
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;150.203.161.36.                        IN      A

;; AUTHORITY SECTION:
.                       5694    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20180
81600 1800 900 604800 86400

;; Query time: 5 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug 16 23:57:53 2018
;; MSG SIZE  rcvd: 107

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62466
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;ns3.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
ns3.cecs.anu.edu.au.    3073    IN      A       150.203.161.50

;; AUTHORITY SECTION:
cecs.anu.edu.au.        150     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        150     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        150     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    1924    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    64      IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    64      IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    1924    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    124     IN      AAAA    2001:388:1034:2905::26

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug 16 23:57:53 2018
;; MSG SIZE  rcvd: 219
```

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

```
grieg % dig yahoo.com

; <<>> DiG 9.7.3 <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15487
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              1800    IN      A       98.137.246.7
yahoo.com.              1800    IN      A       98.137.246.8
yahoo.com.              1800    IN      A       98.138.219.231
yahoo.com.              1800    IN      A       98.138.219.232
yahoo.com.              1800    IN      A       72.30.35.9
yahoo.com.              1800    IN      A       72.30.35.10

;; AUTHORITY SECTION:
yahoo.com.              15799   IN      NS      ns5.yahoo.com.
yahoo.com.              15799   IN      NS      ns2.yahoo.com.
yahoo.com.              15799   IN      NS      ns3.yahoo.com.
yahoo.com.              15799   IN      NS      ns1.yahoo.com.
yahoo.com.              15799   IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          429541  IN      A       68.180.131.16
ns1.yahoo.com.          5911    IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          87129   IN      A       68.142.255.16
ns2.yahoo.com.          15845   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          438332  IN      A       203.84.221.53
ns3.yahoo.com.          13664   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          168605  IN      A       98.138.11.157
ns5.yahoo.com.          101981  IN      A       119.160.253.83

;; Query time: 159 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug  9 10:49:17 2018
;; MSG SIZE  rcvd: 377
```

```
grieg % 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: 36183
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              894     IN      A       98.138.219.232
yahoo.com.              894     IN      A       72.30.35.9
yahoo.com.              894     IN      A       72.30.35.10
yahoo.com.              894     IN      A       98.137.246.7
yahoo.com.              894     IN      A       98.137.246.8
yahoo.com.              894     IN      A       98.138.219.231

;; AUTHORITY SECTION:
yahoo.com.              14893   IN      NS      ns1.yahoo.com.
yahoo.com.              14893   IN      NS      ns4.yahoo.com.
yahoo.com.              14893   IN      NS      ns3.yahoo.com.
yahoo.com.              14893   IN      NS      ns5.yahoo.com.
yahoo.com.              14893   IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          409392  IN      A       68.180.131.16
ns1.yahoo.com.          5005    IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86223   IN      A       68.142.255.16
ns2.yahoo.com.          18906   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          176555  IN      A       203.84.221.53
ns3.yahoo.com.          92150   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          93031   IN      A       98.138.11.157
ns5.yahoo.com.          79095   IN      A       119.160.253.83

;; Query time: 7 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Thu Aug  9 11:04:23 2018
;; MSG SIZE  rcvd: 377
```

Type: NS

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.

```
grieg % dig . ns

; <<>> DiG 9.7.3 <<>> . ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1756
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 12

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       107828  IN      NS      i.root-servers.net.
.                       107828  IN      NS      b.root-servers.net.
.                       107828  IN      NS      h.root-servers.net.
.                       107828  IN      NS      f.root-servers.net.
.                       107828  IN      NS      j.root-servers.net.
.                       107828  IN      NS      m.root-servers.net.
.                       107828  IN      NS      g.root-servers.net.
.                       107828  IN      NS      k.root-servers.net.
.                       107828  IN      NS      l.root-servers.net.
.                       107828  IN      NS      e.root-servers.net.
.                       107828  IN      NS      c.root-servers.net.
.                       107828  IN      NS      d.root-servers.net.
.                       107828  IN      NS      a.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     99141   IN      A       198.41.0.4
a.root-servers.net.     58260   IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     6964    IN      A       199.9.14.201
c.root-servers.net.     113503  IN      A       192.33.4.12
c.root-servers.net.     86598   IN      AAAA    2001:500:2::c
d.root-servers.net.     213756  IN      A       199.7.91.13
d.root-servers.net.     86598   IN      AAAA    2001:500:2d::d
e.root-servers.net.     265749  IN      AAAA    2001:500:a8::e
g.root-servers.net.     265749  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     131830  IN      A       198.97.190.53
h.root-servers.net.     86598   IN      AAAA    2001:500:1::53
i.root-servers.net.     457647  IN      A       192.36.148.17

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug  9 11:37:25 2018
;; MSG SIZE  rcvd: 492
```

2.

```
grieg % dig @198.41.0.4 au. ns

; <<>> DiG 9.7.3 <<>> @198.41.0.4 au. ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35773
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 16
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;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

;; Query time: 211 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Thu Aug  9 11:42:26 2018
;; MSG SIZE  rcvd: 508
```

3.

```
grieg % dig @58.65.254.73 edu.au. ns

; <<>> DiG 9.7.3 <<>> @58.65.254.73 edu.au. ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13353
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; 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      s.au.
edu.au.                 86400   IN      NS      q.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: 17 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Thu Aug  9 11:43:48 2018
;; MSG SIZE  rcvd: 264
```

4.

```
grieg % dig @65.22.196.1 unsw.edu.au. ns

; <<>> DiG 9.7.3 <<>> @65.22.196.1 unsw.edu.au. ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55546
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns1.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: 14 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Thu Aug  9 11:45:59 2018
;; MSG SIZE  rcvd: 187
```

5.

```
grieg % dig @129.94.0.192 cse.unsw.edu.au. ns

; <<>> DiG 9.7.3 <<>> @129.94.0.192 cse.unsw.edu.au. ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41835
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 4
;; WARNING: recursion requested but not available

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

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

;; ADDITIONAL SECTION:
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
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.2
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 Aug  9 11:47:49 2018
;; MSG SIZE  rcvd: 153
```

My machine ip address is 124.94.242.2

So there are 5 DNS servers to query to get authoritative answer.

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

Yes, a machine may have several network interfaces and a network interface can have several IP address associated with it at any given time. So an IP address may have associated with several names ("aliases"). To obtain the canonical name for the machine, use dig with query type=cname.