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?

- www.cecs.anu.edu.au is a CNAME record pointing to rproxy.cecs.anu.edu.au. After doing a lookup using dig and an **A query** on rproxy.cecs.anu.edu.au, the following IP address was shown: **150.203.161.98.**

```
$ 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: 45860
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.cecs.anu.edu.au.        IN    A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3083  IN    CNAME rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 3083  IN    A     150.203.161.98

;; Query time: 13 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 30 15:53:08 AEST 2019
;; MSG SIZE  rcvd: 85
```

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

```
$ dig cecs.anu.edu.au CNAME

; <<>> DiG 9.10.6 <<>> cecs.anu.edu.au CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31945
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cecs.anu.edu.au.        IN    CNAME

;; AUTHORITY SECTION:
cecs.anu.edu.au.  1799  IN    SOA   ns1.cecs.anu.edu.au.
hostmaster.cecs.anu.edu.au. 1561697567 10800 3600 604800 86400

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 30 15:54:28 AEST 2019
;; MSG SIZE  rcvd: 95
```

- CNAME for the CECS ANU website is cecs.anu.edu.au, which points to rproxy.cecs.anu.edu.au.
- There are several reasons for using an alias in the form of a CNAME record, including better semantic organisation of site. For example (blog.example.com) might be used to point to a section of the site that's used only for blogging, whereas (www.example.com) might point to the main website.

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

```
;; AUTHORITY SECTION:
cecs.anu.edu.au.  1799  IN    SOA   ns1.cecs.anu.edu.au.
hostmaster.cecs.anu.edu.au. 1561697567 10800 3600 604800 86400

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 30 15:54:28 AEST 2019
;; MSG SIZE  rcvd: 95
```

- The authority section contains the Start of Authority (SOA) record to both `ns1.cecs.anu.edu.au.` & `hostmaster.cecs.anu.edu.au.`
- The additional section for the above query is non-existent.

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

```
$ cat /etc/resolv.conf

#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- I'm using Google's DNS, so the IP address of my local nameserver is `8.8.8.8 and 8.8.4.4.`

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?

```
$ dig NS cecs.anu.edu.au

; <<>> DiG 9.10.6 <<>> NS cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55356
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cecs.anu.edu.au.      IN    NS

;; ANSWER SECTION:
cecs.anu.edu.au.  3599  IN    NS    ns3.cecs.anu.edu.au.
cecs.anu.edu.au.  3599  IN    NS    ns4.cecs.anu.edu.au.
cecs.anu.edu.au.  3599  IN    NS    ns2.cecs.anu.edu.au.
```

```
;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 30 16:12:40 AEST 2019
;; MSG SIZE  rcvd: 98
```

- Nameservers and their respective IP addresses:
  - `ns3.cecs.anu.edu.au -> 150.203.161.50`
  - `ns4.cecs.anu.edu.au -> 150.203.161.38`
  - `ns2.cecs.anu.edu.au -> 150.203.161.36`
- NS query was used to obtain this information.

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?

```
$ dig -x 111.68.101.54

; <<>> DiG 9.10.6 <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59525
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;54.101.68.111.in-addr.arpa. IN    PTR

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 3599 IN      PTR
      webserver.seecs.nust.edu.pk.

;; Query time: 456 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jun 30 16:28:42 AEST 2019
;; MSG SIZE  rcvd: 96
```

- DNS name associated with the given IP address is `webserver.seecs.nust.edu.pk`.
- We get this information by performing a reverse lookup using dig with the -x flag.

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)

```
dig @129.94.242.33 yahoo.com MX

; <<>> 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: 33971
;; 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: 62 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Jun 30 16:47:06 AEST 2019
;; MSG SIZE  rcvd: 38
```

- There's no authoritative answer, as it's not present in the flags section (i.e. `AUTHORITY: 0`).

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

```
$ dig @150.203.161.50 yahoo.com MX

; <<>> DiG 9.10.6 <<>> @150.203.161.50 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 16019
;; 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: 65 msec
;; SERVER: 150.203.161.50#53(150.203.161.50)
;; WHEN: Sun Jun 30 17:01:49 AEST 2019
;; MSG SIZE  rcvd: 38
```

- The output above shows the results of question 7, using the first nameserver obtained in question 5.

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

```
$ dig MX yahoo.com aaonly

; <<>> DiG 9.10.6 <<>> MX yahoo.com aaonly
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49880
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;yahoo.com.            IN    MX

;; ANSWER SECTION:
yahoo.com.       200   IN    MX    1 mta5.am0.yahoodns.net.
yahoo.com.       200   IN    MX    1 mta6.am0.yahoodns.net.
yahoo.com.       200   IN    MX    1 mta7.am0.yahoodns.net.

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jul 01 01:15:37 AEST 2019
;; MSG SIZE  rcvd: 117

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47404
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;aaonly.                        IN      MX

;; AUTHORITY SECTION:
.                       86382 IN     SOA   a.root-servers.net. nstld.verisign-
grs.com. 2019063000 1800 900 604800 86400

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jul 01 01:15:37 AEST 2019
;; MSG SIZE  rcvd: 110
```

- Using the aaonly flag with dig, we're able to set the "aa" flag in the DNS query.

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?

```
$ dig . NS

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8812
;; 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:
.                 17657 IN     NS    g.root-servers.net.
.                 17657 IN     NS    l.root-servers.net.
.                 17657 IN     NS    c.root-servers.net.
.                 17657 IN     NS    j.root-servers.net.
.                 17657 IN     NS    b.root-servers.net.
.                 17657 IN     NS    h.root-servers.net.
.                 17657 IN     NS    e.root-servers.net.
.                 17657 IN     NS    d.root-servers.net.
.                 17657 IN     NS    f.root-servers.net.
.                 17657 IN     NS    i.root-servers.net.
.                 17657 IN     NS    m.root-servers.net.
.                 17657 IN     NS    k.root-servers.net.
.                 17657 IN     NS    a.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.    82763 IN    A     198.41.0.4
a.root-servers.net.    227511      IN    AAAA  2001:503:ba3e::2:30
b.root-servers.net.    398906      IN    A     199.9.14.201
b.root-servers.net.    346452      IN    AAAA  2001:500:200::b
c.root-servers.net.    230042      IN    A     192.33.4.12
c.root-servers.net.    506671      IN    AAAA  2001:500:2::c
d.root-servers.net.    309016      IN    A     199.7.91.13
d.root-servers.net.    346452      IN    AAAA  2001:500:2d::d
e.root-servers.net.    64358 IN    A     192.203.230.10
e.root-servers.net.    590754      IN    AAAA  2001:500:a8::e
f.root-servers.net.    227569      IN    A     192.5.5.241
f.root-servers.net.    346452      IN    AAAA  2001:500:2f::f
```

```
g.root-servers.net.    398906      IN    A     192.112.36.4
g.root-servers.net.    394454      IN    AAAA  2001:500:12::d0d
h.root-servers.net.    122128      IN    A     198.97.190.53
h.root-servers.net.    319724      IN    AAAA  2001:500:1::53
i.root-servers.net.    484914      IN    A     192.36.148.17
i.root-servers.net.    346453      IN    AAAA  2001:7fe::53
j.root-servers.net.    297561      IN    A     192.58.128.30
j.root-servers.net.    346452      IN    AAAA  2001:503:c27::2:30
k.root-servers.net.    389452      IN    A     193.0.14.129
k.root-servers.net.    506671      IN    AAAA  2001:7fd::1
l.root-servers.net.    234286      IN    A     199.7.83.42
l.root-servers.net.    346452      IN    AAAA  2001:500:9f::42
m.root-servers.net.    309188      IN    A     202.12.27.33
m.root-servers.net.    346452      IN    AAAA  2001:dc3::35

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jul 01 01:46:09 AEST 2019
;; MSG SIZE  rcvd: 811

$ dig @198.41.0.4 williams.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> @198.41.0.4
williams.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46332
;; 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:
;williams.cse.unsw.edu.au.   IN    A

;; 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: 166 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Mon Jul 01 01:46:46 AEST 2019
;; MSG SIZE  rcvd: 625
```

```
$ dig @58.65.254.73 williams.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> @58.65.254.73
williams.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16379
;; 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:
;williams.cse.unsw.edu.au.   IN    A

;; AUTHORITY SECTION:
edu.au.                7200  IN    NS    r.au.
edu.au.                7200  IN    NS    t.au.
edu.au.                7200  IN    NS    q.au.
edu.au.                7200  IN    NS    s.au.

;; ADDITIONAL SECTION:
q.au.            7200  IN    A     65.22.196.1
r.au.            7200  IN    A     65.22.197.1
s.au.            7200  IN    A     65.22.198.1
t.au.            7200  IN    A     65.22.199.1
q.au.            7200  IN    AAAA  2a01:8840:be::1
r.au.            7200  IN    AAAA  2a01:8840:bf::1
s.au.            7200  IN    AAAA  2a01:8840:c0::1
t.au.            7200  IN    AAAA  2a01:8840:c1::1

;; Query time: 153 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Mon Jul 01 01:46:56 AEST 2019
;; MSG SIZE  rcvd: 293

$ dig @65.22.196.1 williams.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> @65.22.196.1
williams.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49736
;; 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:
;williams.cse.unsw.edu.au.   IN    A

;; AUTHORITY SECTION:
unsw.edu.au.           900   IN    NS    ns2.unsw.edu.au.
unsw.edu.au.           900   IN    NS    ns1.unsw.edu.au.
unsw.edu.au.           900   IN    NS    ns3.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: Mon Jul 01 01:47:08 AEST 2019
;; MSG SIZE  rcvd: 211

$ dig @129.94.0.192 williams.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> @129.94.0.192
williams.cse.unsw.edu.au
```

```
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23467
;; 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:
;williams.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      129.94.242.2
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: 4 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Mon Jul 01 01:47:18 AEST 2019
;; MSG SIZE  rcvd: 173

$ dig @129.94.242.2 williams.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u17-Debian <<>> @129.94.242.2
williams.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33917
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
williams.cse.unsw.edu.au. 3600     IN    A     129.94.242.20

;; 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: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Jul 01 01:47:27 AEST 2019
;; MSG SIZE  rcvd: 157
```

- IP Address: `129.94.242.20`, found after running the 6 queries as shown above.

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

- One physical machine **CAN** have multiple names and IP addresses. For example, if I have two network cards, connected to my PCI slot, I can have two IP addresses on that computer.