Exercise 3

```
z5542052@cello15:~$ dig www.hi.is

; <<>> DiG 9.18.24-1-Debian <<>> www.hi.is
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12426
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: dc014e0e31a0e041010000006673cc6534d9a1aa9452d484 (good)
;; QUESTION SECTION:
;www.hi.is.                     IN      A

;; ANSWER SECTION:
www.hi.is.              63      IN      CNAME   web-lb.rhi.hi.is.
web-lb.rhi.hi.is.       84098   IN      A       130.208.165.186

;; Query time: 0 msec
;; SERVER: 129.94.208.2#53(129.94.208.2) (UDP)
;; WHEN: Thu Jun 20 16:29:57 AEST 2024
;; MSG SIZE  rcvd: 112
```

Question 1. What is the IP address of **www.hi.is** ? What type of DNS query is sent to get this answer?

In the ANSWER SECTION, The IP address of www.hi.is is 130.208.165.186.

We can find the type of DNS query under QUESTION SECTION, which is type A DNS

Question 2. What is the canonical name for the webserver (i.e., www.hi.is)? Suggest a reason for having an alias for this server.

In the ANSWER SECTION, the canonical name for www.hi.is is web-lb.rhi.hi.is.

Reason: Aliases are easy for human to recall compared to the IP address, additionally it can also maintain when the IP address of a server change.

Question 3. What can you make of the rest of the response/what is it used for (i.e., the details available in the DNS response (cookies and other fields))?

flags: Give us summary of the response.

Cookies: Record the cookie the sent by the server.

The section at the bottom gave us brief information from the query sender, query time, sender IP address, time of query sent and the message size.

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

129.94.208.2

Question 5. What are the DNS nameservers for the " **hi.is** " domain (note: the domain name is **hi.is** and not www.hi.is . This is an example of what is referred to as the apex/naked domain)? Find their IP addresses. Which DNS query type is used to obtain this information?

```
z5542052@cello15:~$ dig hi.is NS

; <<>> DiG 9.18.24-1-Debian <<>> hi.is NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47964
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 975b0cf10e8542be010000006673d61499c18d13eb2d4a69 (good)
;; QUESTION SECTION:
;hi.is.                         IN      NS

;; ANSWER SECTION:
hi.is.                  5974    IN      NS      dvalinn.rhnet.is.
hi.is.                  5974    IN      NS      borg.rhi.hi.is.
hi.is.                  5974    IN      NS      info.rhi.hi.is.

;; ADDITIONAL SECTION:
borg.rhi.hi.is.         17471   IN      A       130.208.165.54
info.rhi.hi.is.         64073   IN      A       130.208.143.33

;; Query time: 0 msec
;; SERVER: 129.94.208.2#53(129.94.208.2) (UDP)
;; WHEN: Thu Jun 20 17:11:16 AEST 2024
;; MSG SIZE  rcvd: 171
```

```
z5542052@cello15:~$ dig dvalinn.rhnet.is

; <<>> DiG 9.18.24-1-Debian <<>> dvalinn.rhnet.is
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59480
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9cf1df88d47be57a010000006673d743d3552d8d62ea1b96 (good)
;; QUESTION SECTION:
;dvalinn.rhnet.is.              IN      A

;; ANSWER SECTION:
dvalinn.rhnet.is.       10917   IN      A       130.208.16.21

;; Query time: 0 msec
;; SERVER: 129.94.208.2#53(129.94.208.2) (UDP)
;; WHEN: Thu Jun 20 17:16:19 AEST 2024
;; MSG SIZE  rcvd: 89
```

NS DNS query type is used to obtain the nameserver and A DNS query type is used to obtain the IP address. The nameservers are: dvalinn.rhnet.is(130.208.16.21) , borg.rhi.hi.is(130.208.165.54) and info.rhi.hi.is(130.208.143.33).

Question 6. What is the DNS name associated with the IP address 18.67.93.67 ? Which DNS query type is used to obtain this information?

```
z5542052@cello15:~$ dig -x 18.67.93.67

; <<>> DiG 9.18.24-1-Debian <<>> -x 18.67.93.67
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33692
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a0bb13c4b0d96b17010000006673cd8678d615777bdf379e (good)
;; QUESTION SECTION:
;67.93.67.18.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
67.93.67.18.in-addr.arpa. 52141 IN      PTR     server-18-67-93-67.syd62.r.cloudfron
t.net.

;; Query time: 0 msec
;; SERVER: 129.94.208.2#53(129.94.208.2) (UDP)
;; WHEN: Thu Jun 20 16:34:46 AEST 2024
;; MSG SIZE  rcvd: 136
```

DNS query type PTR is used to track the DNS name of a specific IP address. The DNS name is server-18-67-93-67.syd62.r.cloudfront.net

Question 7. Run, dig and query the CSE nameserver (129.94.242.2) for the mail servers for outlook.com (again, the domain name is outlook.com, not www.outlook.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 message to determine the answer)

```
z5542052@cello15:~$ dig @129.94.242.2 outlook.com

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.242.2 outlook.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18987
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ba73eceb25e7b864010000006673cdb97552c4e7d8f09d25 (good)
;; QUESTION SECTION:
;outlook.com.                   IN      A

;; ANSWER SECTION:
outlook.com.            300     IN      A       52.96.229.242
outlook.com.            300     IN      A       52.96.223.2
outlook.com.            300     IN      A       52.96.222.194
outlook.com.            300     IN      A       52.96.91.34
outlook.com.            300     IN      A       52.96.228.130
outlook.com.            300     IN      A       52.96.111.82
outlook.com.            300     IN      A       52.96.214.50
outlook.com.            300     IN      A       52.96.222.226
outlook.com.            300     IN      A       52.96.172.98

;; Query time: 16 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Thu Jun 20 16:35:37 AEST 2024
;; MSG SIZE  rcvd: 212
```

No, I didn't get an authoritative answer, since the flags doesn't contain aa.

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

```
z5542052@cello15:~$ dig @borg.rhi.hi.is outlook.com

; <<>> DiG 9.18.24-1-Debian <<>> @borg.rhi.hi.is outlook.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 63854
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d160e546879165ec010000006673dc8958174390cca9e9bb (good)
;; QUESTION SECTION:
;outlook.com.                   IN      A

;; Query time: 348 msec
;; SERVER: 130.208.165.54#53(borg.rhi.hi.is) (UDP)
;; WHEN: Thu Jun 20 17:38:49 AEST 2024
;; MSG SIZE  rcvd: 68
```

Didn't get a response with borg.rhi.hi.is to outlook.com. The status is REFUSED.

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

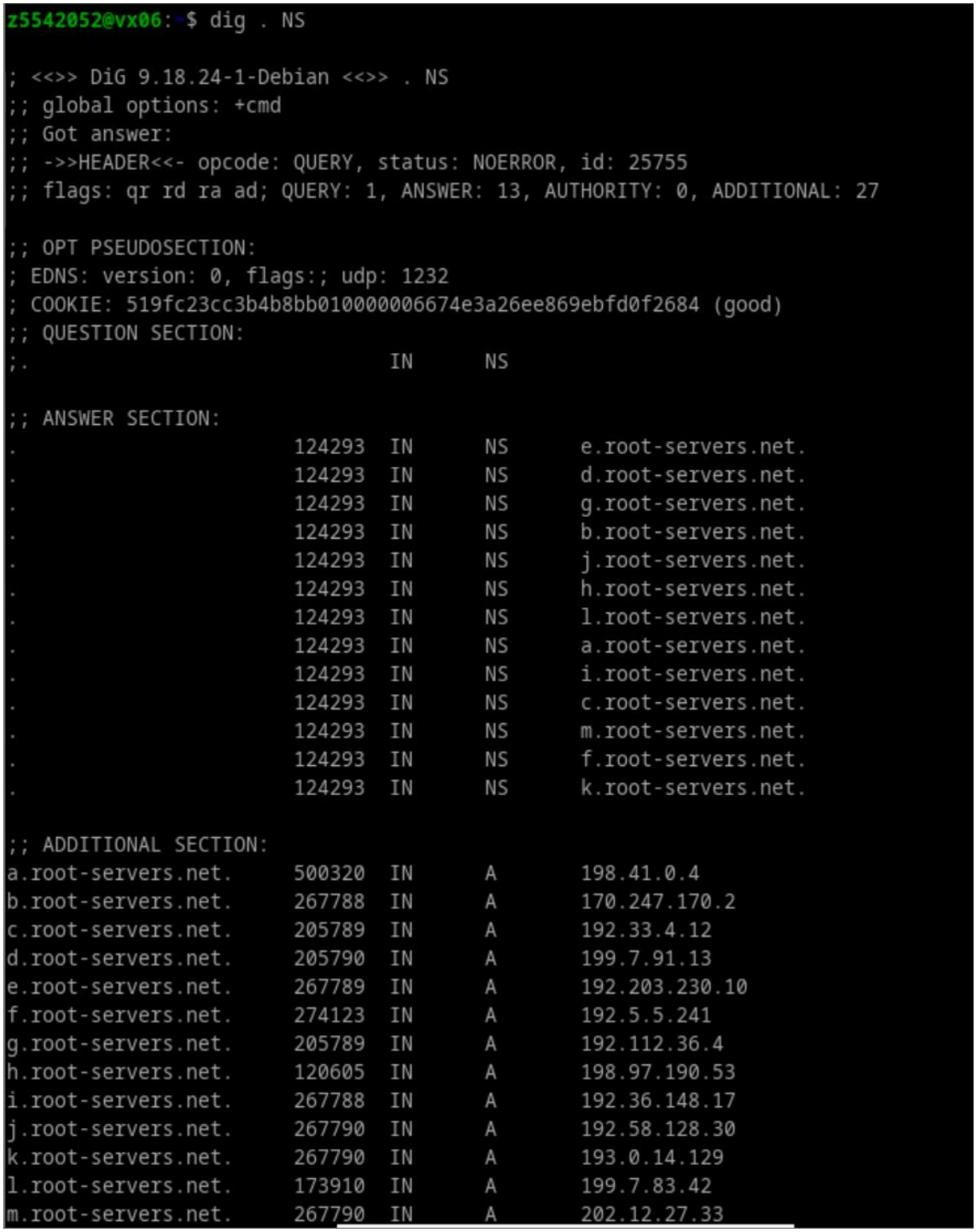
```
z5542052@cello15:~$ dig outlook.com NS

; <<>> DiG 9.18.24-1-Debian <<>> outlook.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54095
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 67b3b0f8bace61bb010000006673deb3ad0d0d2a414bb3b8 (good)
;; QUESTION SECTION:
;outlook.com.                   IN      NS

;; ANSWER SECTION:
outlook.com.            162     IN      NS      nse13.o365filtering.com.
outlook.com.            162     IN      NS      nse21.o365filtering.com.
outlook.com.            162     IN      NS      nse24.o365filtering.com.
outlook.com.            162     IN      NS      ns2-38.azure-dns.net.
outlook.com.            162     IN      NS      nse12.o365filtering.com.
outlook.com.            162     IN      NS      ns3-38.azure-dns.org.
outlook.com.            162     IN      NS      ns4-38.azure-dns.info.
outlook.com.            162     IN      NS      ns1-38.azure-dns.com.

;; Query time: 4 msec
;; SERVER: 129.94.208.2#53(129.94.208.2) (UDP)
;; WHEN: Thu Jun 20 17:48:03 AEST 2024
;; MSG SIZE  rcvd: 302
```

Then I pick nse13.o365filtering.com as the nameserver

```
z5542052@cello15:~$ dig @nse13.o365filtering.com outlook.com MX

; <<>> DiG 9.18.24-1-Debian <<>> @nse13.o365filtering.com outlook.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22208
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 8, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;outlook.com.                   IN      MX

;; ANSWER SECTION:
outlook.com.            300     IN      MX      5 outlook-com.olc.protection.outlook
.com.

;; AUTHORITY SECTION:
outlook.com.            300     IN      NS      nse12.o365filtering.com.
outlook.com.            300     IN      NS      nse21.o365filtering.com.
outlook.com.            300     IN      NS      nse24.o365filtering.com.
outlook.com.            300     IN      NS      nse13.o365filtering.com.
outlook.com.            300     IN      NS      ns1-38.azure-dns.com.
outlook.com.            300     IN      NS      ns2-38.azure-dns.net.
outlook.com.            300     IN      NS      ns3-38.azure-dns.org.
outlook.com.            300     IN      NS      ns4-38.azure-dns.info.

;; Query time: 296 msec
;; SERVER: 104.47.2.8#53(nse13.o365filtering.com) (UDP)
;; WHEN: Thu Jun 20 17:48:35 AEST 2024
;; MSG SIZE  rcvd: 311
```

We use type MX DNS query to obtain this information.

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). If you are using VLAB then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, flute00.cse.unsw.edu.au or flute01.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 your host's IP address. How many DNS servers do you have to query for an authoritative answer?



```
z5542052@vx06:~$ dig . NS

; <<>> DiG 9.18.24-1-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25755
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 519fc23cc3b4b8bb010000006674e3a26ee869ebfd0f2684 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       124293  IN      NS      e.root-servers.net.
.                       124293  IN      NS      d.root-servers.net.
.                       124293  IN      NS      g.root-servers.net.
.                       124293  IN      NS      b.root-servers.net.
.                       124293  IN      NS      j.root-servers.net.
.                       124293  IN      NS      h.root-servers.net.
.                       124293  IN      NS      l.root-servers.net.
.                       124293  IN      NS      a.root-servers.net.
.                       124293  IN      NS      i.root-servers.net.
.                       124293  IN      NS      c.root-servers.net.
.                       124293  IN      NS      m.root-servers.net.
.                       124293  IN      NS      f.root-servers.net.
.                       124293  IN      NS      k.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     500320  IN      A       198.41.0.4
b.root-servers.net.     267788  IN      A       170.247.170.2
c.root-servers.net.     205789  IN      A       192.33.4.12
d.root-servers.net.     205790  IN      A       199.7.91.13
e.root-servers.net.     267789  IN      A       192.203.230.10
f.root-servers.net.     274123  IN      A       192.5.5.241
g.root-servers.net.     205789  IN      A       192.112.36.4
h.root-servers.net.     120605  IN      A       198.97.190.53
i.root-servers.net.     267788  IN      A       192.36.148.17
j.root-servers.net.     267790  IN      A       192.58.128.30
k.root-servers.net.     267790  IN      A       193.0.14.129
l.root-servers.net.     173910  IN      A       199.7.83.42
m.root-servers.net.     267790  IN      A       202.12.27.33
```

I pick a.root-servers.net(198.41.0.4)

```
z5542052@vx06:~$ dig @198.41.0.4 lyre00.cse.unsw.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @198.41.0.4 lyre00.cse.unsw.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16763
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lyre00.cse.unsw.au.            IN      NS

;; AUTHORITY SECTION:
au.                     172800  IN      NS      t.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      q.au.

;; ADDITIONAL SECTION:
t.au.                   172800  IN      A       65.22.199.1
t.au.                   172800  IN      AAAA    2a01:8840:c1::1
r.au.                   172800  IN      A       65.22.197.1
r.au.                   172800  IN      AAAA    2a01:8840:bf::1
a.au.                   172800  IN      A       58.65.254.1
a.au.                   172800  IN      AAAA    2407:6e00:254::1
s.au.                   172800  IN      A       65.22.198.1
s.au.                   172800  IN      AAAA    2a01:8840:c0::1
q.au.                   172800  IN      A       65.22.196.1
q.au.                   172800  IN      AAAA    2a01:8840:be::1

;; Query time: 92 msec
;; SERVER: 198.41.0.4#53(198.41.0.4) (UDP)
;; WHEN: Fri Jun 21 13:17:26 AEST 2024
;; MSG SIZE  rcvd: 347
```

We are now referred to .au nameserver Then I pick a.au(58.65.254.1).

```
z5542052@vx06:~$ dig @65.22.199.1 edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @65.22.199.1 edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23575
;; flags: qr aa rd; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;edu.au.                                IN      NS

;; ANSWER SECTION:
edu.au.                 3600    IN      NS      a.au.
edu.au.                 3600    IN      NS      q.au.
edu.au.                 3600    IN      NS      r.au.
edu.au.                 3600    IN      NS      s.au.
edu.au.                 3600    IN      NS      t.au.

;; Query time: 0 msec
;; SERVER: 65.22.199.1#53(65.22.199.1) (UDP)
;; WHEN: Fri Jun 21 13:25:12 AEST 2024
;; MSG SIZE  rcvd: 115
```

Then we are referred to edu.au, the IP didn’t change, we still use t.au to do next step

n

```
z5542052@vx06:~$ dig @t.au lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @t.au lyre00.cse.unsw.edu.au NS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29043
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            3600    IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            3600    IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            3600    IN      NS      ns3.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        3600    IN      A       129.94.0.192
ns1.unsw.edu.au.        3600    IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        3600    IN      A       129.94.0.193
ns2.unsw.edu.au.        3600    IN      AAAA    2001:388:c:35::2
ns3.unsw.edu.au.        3600    IN      A       192.155.82.178

;; Query time: 4 msec
;; SERVER: 65.22.199.1#53(t.au) (UDP)
;; WHEN: Fri Jun 21 13:26:43 AEST 2024
;; MSG SIZE  rcvd: 209
```

Now we are referred to unsw.edu.au. nameserver. I choose ns1.unsw.edu.au(129.94.9.192)

```
z5542052@vx06:~$ dig @ns1.unsw.edu.au lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @ns1.unsw.edu.au lyre00.cse.unsw.edu.au NS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44908
;; 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.        300     IN      NS      maestro.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        300     IN      NS      beethoven.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.242.2
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.172.11
maestro.orchestra.cse.unsw.edu.au. 300 IN A     129.94.242.33

;; Query time: 4 msec
;; SERVER: 129.94.0.192#53(ns1.unsw.edu.au) (UDP)
;; WHEN: Fri Jun 21 13:28:52 AEST 2024
;; MSG SIZE  rcvd: 171
```

Now we are referred to the CSE nameserver, we now send type A DNS query.

```
z5542052@vx06:~$ dig @129.94.208.3 lyre00.cse.unsw.edu.au A

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.208.3 lyre00.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29288
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c65b1f01771c3d7c010000006674f4e33f3d7c14a3f96004 (good)
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      A

;; ANSWER SECTION:
lyre00.cse.unsw.EDU.AU. 3600    IN      A       129.94.210.20

;; Query time: 0 msec
;; SERVER: 129.94.208.3#53(129.94.208.3) (UDP)
;; WHEN: Fri Jun 21 13:34:59 AEST 2024
;; MSG SIZE  rcvd: 117
```

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

We query 5 DNS servers for an authoritative answer.

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

Yes, it can have multiple names and IP addresses associated with it since it can have multiple network interfaces.

Exercise 4:

To achieve persistent, I set timeout to each connection, when connection is closed, it have to build connection again.