Mr. Phot Koseekrainiramon z5387411

COMP3331 Lab3

Exercise 3: Digging into DNS

```
z5387411@vx11:~$ dig www.stanford.edu

; <<>> DiG 9.16.37-Debian <<>> www.stanford.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36884
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.stanford.edu.              IN      A

;; ANSWER SECTION:
www.stanford.edu.       1800    IN      CNAME   pantheon-systems.map.fastly.net.
pantheon-systems.map.fastly.net. 30 IN  A       151.101.30.133

;; AUTHORITY SECTION:
fastly.net.             1790    IN      NS      ns1.fastly.net.
fastly.net.             1790    IN      NS      ns2.fastly.net.
fastly.net.             1790    IN      NS      ns4.fastly.net.
fastly.net.             1790    IN      NS      ns3.fastly.net.

;; ADDITIONAL SECTION:
ns1.fastly.net.         1329    IN      A       23.235.32.32
ns2.fastly.net.         293     IN      A       104.156.80.32
ns3.fastly.net.         400     IN      A       23.235.36.32
ns4.fastly.net.         1854    IN      A       104.156.84.32

;; Query time: 19 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Jun 18 10:24:48 AEST 2023
;; MSG SIZE  rcvd: 242
```

1. The IP address of www.standford.edu is 151.101.30.133. The type of DNE query being sent is A.

2. The canonical name for the Stanford webserver is pantheon-systems.map.fastly.net. It has an alias name for a client to easily reference to the server.

3. From the picture above, we could see DNS nameservers in the authority section and their IP addresses in the additional section.

4. The IP address of my local nameserver is 239.94.242.2.

```
z5387411@vx08:~$ dig stanford.edu

; <<>> DiG 9.16.37-Debian <<>> stanford.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17534
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;stanford.edu.                  IN      A

;; ANSWER SECTION:
stanford.edu.           1733    IN      A       171.67.215.200

;; AUTHORITY SECTION:
stanford.edu.           31503   IN      NS      argus.stanford.edu.
stanford.edu.           31503   IN      NS      avallone.stanford.edu.
stanford.edu.           31503   IN      NS      ns7.dnsmadeeasy.com.
stanford.edu.           31503   IN      NS      ns6.dnsmadeeasy.com.
stanford.edu.           31503   IN      NS      atalante.stanford.edu.
stanford.edu.           31503   IN      NS      ns5.dnsmadeeasy.com.

;; ADDITIONAL SECTION:
ns5.dnsmadeeasy.com.    78364   IN      A       208.94.148.13
ns5.dnsmadeeasy.com.    1137    IN      AAAA    2600:1800:5::1
ns6.dnsmadeeasy.com.    45790   IN      A       208.80.124.13
ns6.dnsmadeeasy.com.    39247   IN      AAAA    2600:1801:6::1
ns7.dnsmadeeasy.com.    46022   IN      A       208.80.126.13
ns7.dnsmadeeasy.com.    46022   IN      AAAA    2600:1802:7::1
argus.stanford.edu.     591     IN      A       171.64.7.115
argus.stanford.edu.     591     IN      AAAA    2607:f6d0:0:9113::ab40:773
atalante.stanford.edu.  591     IN      A       171.64.7.61
atalante.stanford.edu.  10467   IN      AAAA    2607:f6d0:0:d32::ab40:73d
avallone.stanford.edu.  591     IN      A       204.63.224.53
avallone.stanford.edu.  591     IN      AAAA    2620:6c:40c0:0:204:63:224:53

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Fri Jun 23 12:33:11 AEST 2023
;; MSG SIZE  rcvd: 456
```

5. The DNS nameservers for the standford.edu domain are argus.standford.edu, avallone.standford.edu, ns7.dnsmadeeasy.com, ns6.dnsmadeeasy.com, Atalante.standford.edu, and ns5.dnsmadeeasy.com. Their IP addresses are 171.64.7.115, 204.63.224.53, 208.80.126.13, 208.80.124.13, 171.64.7.61, and 208.61.148.13, . The type of DNS query being sent is NS to get the DNS nameservers and A to get the IP addresses.

```
z5387411@vx12:~$ dig -x 129.25.60.56

; <<>> DiG 9.16.37-Debian <<>> -x 129.25.60.56
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46137
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;56.60.25.129.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
56.60.25.129.in-addr.arpa. 180  IN      PTR     ece.drexel.edu.

;; AUTHORITY SECTION:
25.129.in-addr.arpa.    1565    IN      NS      adns2.drexel.edu.
25.129.in-addr.arpa.    1565    IN      NS      adns1.drexel.edu.

;; ADDITIONAL SECTION:
adns1.drexel.edu.       5090    IN      A       144.118.27.1
adns2.drexel.edu.       5090    IN      A       144.118.27.18

;; Query time: 227 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Jun 19 14:33:05 AEST 2023
;; MSG SIZE  rcvd: 154
```

6. ^ The name associated with the IP address is ece.drexel.edu. The type of DNS query being sent is PTR.

```
z5387411@vx08:~$ dig @129.94.242.33 google.com MX

; <<>> DiG 9.16.37-Debian <<>> @129.94.242.33 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30294
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 18

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

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; AUTHORITY SECTION:
google.com.             16134   IN      NS      ns3.google.com.
google.com.             16134   IN      NS      ns4.google.com.
google.com.             16134   IN      NS      ns1.google.com.
google.com.             16134   IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        300     IN      A       172.253.118.27
smtp.google.com.        300     IN      A       74.125.24.27
smtp.google.com.        300     IN      A       74.125.68.26
smtp.google.com.        300     IN      A       142.251.175.26
smtp.google.com.        300     IN      A       172.253.118.26
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c02::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c05::1a
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c05::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c1c::1b
ns1.google.com.         163631  IN      A       216.239.32.10
ns1.google.com.         163618  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         63806   IN      A       216.239.34.10
ns2.google.com.         63806   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         163713  IN      A       216.239.36.10
ns3.google.com.         163681  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         160604  IN      A       216.239.38.10
ns4.google.com.         160604  IN      AAAA    2001:4860:4802:38::a
```

7. ^ No (no aa flags). The answer is not from the server with authority (might be from a cache).

```
z5387411@vx08:~$ dig @171.64.7.115 google.com MX

; <<>> DiG 9.16.37-Debian <<>> @171.64.7.115 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 24027
;; 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: 57b378774a8661970100000064950711897fb8112113153f (good)
;; QUESTION SECTION:
;google.com.                    IN      MX

;; Query time: 164 msec
;; SERVER: 171.64.7.115#53(171.64.7.115)
;; WHEN: Fri Jun 23 12:44:33 AEST 2023
;; MSG SIZE  rcvd: 67
```

8. ^ Not getting an authoritative answer (no aa flags). It is because the answer is not from the server that has authority.

1)

```
z5387411@vx08:~$ dig @129.94.242.33 google.com SOA

; <<>> DiG 9.16.37-Debian <<>> @129.94.242.33 google.com SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43983
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
google.com.             60      IN      SOA     ns1.google.com. dns-admin.google.com. 542507634 900 900 1800 60

;; AUTHORITY SECTION:
google.com.             15894   IN      NS      ns3.google.com.
google.com.             15894   IN      NS      ns1.google.com.
google.com.             15894   IN      NS      ns2.google.com.
google.com.             15894   IN      NS      ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         163391  IN      A       216.239.32.10
ns1.google.com.         163378  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         63566   IN      A       216.239.34.10
ns2.google.com.         63566   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         163473  IN      A       216.239.36.10
ns3.google.com.         163441  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         160364  IN      A       216.239.38.10
ns4.google.com.         160364  IN      AAAA    2001:4860:4802:38::a

;; Query time: 104 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Fri Jun 23 12:52:28 AEST 2023
;; MSG SIZE  rcvd: 333
```

2)

```
z5387411@vx08:~$ dig @216.239.32.10 google.com MX

; <<>> DiG 9.16.37-Debian <<>> @216.239.32.10 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32524
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 10
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        300     IN      A       172.217.194.27
smtp.google.com.        300     IN      A       172.217.194.26
smtp.google.com.        300     IN      A       142.250.4.26
smtp.google.com.        300     IN      A       142.250.4.27
smtp.google.com.        300     IN      A       74.125.200.27
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c04::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c04::1a
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c06::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c06::1a

;; Query time: 96 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Fri Jun 23 12:53:49 AEST 2023
;; MSG SIZE  rcvd: 252
```

9. ^ By sending SOA type of DNS query to get the authoritative nameserver and use its IP address (from an A-type) as a query with MX type for the mail servers for google.com.

1)

```
z5387411@vx08:~$ dig . NS

; <<>> DiG 9.16.37-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9266
;; 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:
.                       13481   IN      NS      a.root-servers.net.
.                       13481   IN      NS      b.root-servers.net.
.                       13481   IN      NS      g.root-servers.net.
.                       13481   IN      NS      i.root-servers.net.
.                       13481   IN      NS      j.root-servers.net.
.                       13481   IN      NS      f.root-servers.net.
.                       13481   IN      NS      c.root-servers.net.
.                       13481   IN      NS      k.root-servers.net.
.                       13481   IN      NS      d.root-servers.net.
.                       13481   IN      NS      h.root-servers.net.
.                       13481   IN      NS      m.root-servers.net.
.                       13481   IN      NS      l.root-servers.net.
.                       13481   IN      NS      e.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     337899  IN      A       198.41.0.4
a.root-servers.net.     148824  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     217512  IN      A       199.9.14.201
b.root-servers.net.     32632   IN      AAAA    2001:500:200::b
c.root-servers.net.     267041  IN      A       192.33.4.12
c.root-servers.net.     32632   IN      AAAA    2001:500:2::c
d.root-servers.net.     217003  IN      A       199.7.91.13
d.root-servers.net.     32632   IN      AAAA    2001:500:2d::d
e.root-servers.net.     273927  IN      A       192.203.230.10
e.root-servers.net.     32632   IN      AAAA    2001:500:a8::e
f.root-servers.net.     2860    IN      A       192.5.5.241
f.root-servers.net.     32632   IN      AAAA    2001:500:2f::f
```

2)

```
z5387411@vx08:~$ dig @198.41.0.4 au. SOA

; <<>> DiG 9.16.37-Debian <<>> @198.41.0.4 au. SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25193
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;au.                            IN      SOA

;; AUTHORITY SECTION:
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.

;; ADDITIONAL SECTION:
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
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

;; Query time: 140 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Fri Jun 23 13:25:35 AEST 2023
;; MSG SIZE  rcvd: 391
```

3)

```
z5387411@vx08:~$ dig @162.159.24.179 edu.au. SOA

; <<>> DiG 9.16.37-Debian <<>> @162.159.24.179 edu.au. SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22222
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
edu.au.                 900     IN      NS      q.au.
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      t.au.
edu.au.                 900     IN      NS      r.au.

;; ADDITIONAL SECTION:
q.au.                   900     IN      A       65.22.196.1
r.au.                   900     IN      A       65.22.197.1
s.au.                   900     IN      A       65.22.198.1
t.au.                   900     IN      A       65.22.199.1
q.au.                   900     IN      AAAA    2a01:8840:be::1
r.au.                   900     IN      AAAA    2a01:8840:bf::1
s.au.                   900     IN      AAAA    2a01:8840:c0::1
t.au.                   900     IN      AAAA    2a01:8840:c1::1

;; Query time: 4 msec
;; SERVER: 162.159.24.179#53(162.159.24.179)
;; WHEN: Fri Jun 23 13:26:53 AEST 2023
;; MSG SIZE  rcvd: 275
```

4)

```
z5387411@vx08:~$ dig @65.22.196.1 unsw.edu.au. SOA

; <<>> DiG 9.16.37-Debian <<>> @65.22.196.1 unsw.edu.au. SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64293
;; 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:
;unsw.edu.au.                   IN      SOA

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.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: 8 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Fri Jun 23 13:27:52 AEST 2023
;; MSG SIZE  rcvd: 198
```

5)

```
z5387411@vx08:~$ dig @192.155.82.178 cse.unsw.edu.au. SOA

; <<>> DiG 9.16.37-Debian <<>> @192.155.82.178 cse.unsw.edu.au. SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1931
;; 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:
;cse.unsw.edu.au.               IN      SOA

;; AUTHORITY SECTION:
cse.unsw.edu.au.        300     IN      NS      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        300     IN      NS      maestro.orchestra.cse.unsw.edu.au.

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

;; Query time: 160 msec
;; SERVER: 192.155.82.178#53(192.155.82.178)
;; WHEN: Fri Jun 23 13:29:28 AEST 2023
;; MSG SIZE  rcvd: 164
```

6)

```
z5387411@vx08:~$ dig @129.94.242.2 lyre00.cse.unsw.edu.au. A

; <<>> DiG 9.16.37-Debian <<>> @129.94.242.2 lyre00.cse.unsw.edu.au. A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21085
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; 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      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: Fri Jun 23 13:31:01 AEST 2023
;; MSG SIZE  rcvd: 177
```

10. ^ 6 DNS queries were sent to find the IP address of lyre00.cse.unsw.edu.au (129.94.210.20).

11. Yes. One example is when a device connects to many networks which are varied in IP addresses.

Exercise 4: A Simple Web Server