Exercise 3: Digging into DNS

```
z5192519@wagner:~$ dig www.eecs.berkeley.edu

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> www.eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7947
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.eecs.berkeley.edu.  16560   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 118  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   52      IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       52      IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       52      IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       52      IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       52      IN      NS      ns-1213.awsdns-23.org.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   57476   IN      A       205.251.192.233
ns-233.awsdns-29.com.   24374   IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   7531    IN      A       205.251.194.132
ns-644.awsdns-16.net.   2026    IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  203     IN      A       205.251.196.189
ns-1213.awsdns-23.org.  203     IN      AAAA    2600:9000:5304:bd00::1
ns-2013.awsdns-59.co.uk. 12769  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 12769  IN      AAAA    2600:9000:5307:dd00::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Oct 11 13:55:54 AEDT 2021
;; MSG SIZE  rcvd: 453
```

Q1:

The IP addresses of www.eecs.berkeley.edu is 23.185.0.1 .

Q2:

The CNAME is live-eecs.pantheonsite.io . The reason to have an alias is because people need to have an easier and memorable way to visit it. And with aliases, we can classify different services which are provided from same IP address.

Q3:

There are 4 authoritative servers in the authority section :

ns-2013.awsdns-59.co.uk, ns-644.awsdns-16.co.uk, ns-233.awsdns-29.co.uk, ns-1213.awsdns-23.co.uk

In the additional section, it records some IP addresses of the previous authoritative servers. (A for IPV4, and AAAA for IPV6)

Q4:

The IP of local nameserver is 129.94.242.2#53.

```
z5192519@wagner:~$ dig eecs.berkeley.edu NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> eecs.berkeley.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38263
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;eecs.berkeley.edu.             IN      NS

;; ANSWER SECTION:
eecs.berkeley.edu.      19581   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      19581   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      19581   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      19581   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      19581   IN      NS      ns.CS.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     27351   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   28122   IN      A       169.229.60.153
adns1.berkeley.edu.     8363    IN      A       128.32.136.3
adns1.berkeley.edu.     4920    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     8363    IN      A       128.32.136.14
adns2.berkeley.edu.     4920    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     4920    IN      A       192.107.102.142
adns3.berkeley.edu.     4920    IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Oct 11 13:59:35 AEDT 2021
;; MSG SIZE  rcvd: 307
```

Q5:

The name servers are adns1.berkeley.edu, adns2.berkeley.edu, adns3.berkeley.edu, ns.CS.berkeley.edu, ns.eecs.berkeley.edu.

The IP addresses are 169.229.60.61, 169.229.60.153, 128.32.136.3, 128.32.136.14, 192.107.102.142 .

```
z5192519@wagner:~$ dig -x 111.68.101.54

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48818
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 2531 IN     PTR     webserver.seecs.nust.edu.pk.
```

Q6:

The DNS name is webserver.seecs.nust.edu.pk . The type of query is PTR.

```
z5192519@wagner:~$ dig @129.94.242.33 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13088
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

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

Q7:

There is no "aa" in flag. This is because the CSE server has no authority for answering queries of yahoo.com domain.

```
z5192519@wagner:~$ dig @ns.CS.berkeley.edu yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns.CS.berkeley.edu yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 40670
;; 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: 166 msec
;; SERVER: 169.229.60.61#53(169.229.60.61)
;; WHEN: Mon Oct 11 14:06:23 AEDT 2021
;; MSG SIZE  rcvd: 38
```

Q8:

The result is that query is refused. As this nameserver is not part of the yahoo mail network, it can not give reply to the DNS query.

```
z5192519@wagner:~$ dig @ns2.yahoo.com yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns2.yahoo.com yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58904
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
;; QUESTION SECTION:
;yahoo.com.                     IN      MX
```

Q9:

Here I obtained an authoritative answer for yahoo mail servers (ns2.yahoo.com). The DNS query type that I sent is MX.

Refer to

```
z5192519@wagner:~$ dig . NS +noall +additional

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> . NS +noall +additional
;; global options: +cmd
a.root-servers.net.     77511   IN      A       198.41.0.4
a.root-servers.net.     283918  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     83502   IN      A       199.9.14.201
b.root-servers.net.     83502   IN      AAAA    2001:500:200::b
```

Refer to

```
z5192519@wagner:~$ dig @199.9.14.201 lyre00.cse.unsw.edu.au NS +noall +additional

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @199.9.14.201 lyre00.cse.unsw.edu.au NS +noall +additional
; (1 server found)
;; global options: +cmd
a.au.                   172800  IN      A       58.65.254.73
a.au.                   172800  IN      AAAA    2407:6e00:254:306::73
c.au.                   172800  IN      A       162.159.24.179
c.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:18b3
d.au.                   172800  IN      A       162.159.25.38
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
m.au.                   172800  IN      A       37.209.192.5
```

Refer to

```
z5192519@wagner:~$ dig @a.au lyre00.cse.unsw.edu.au NS +noall +additional

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @a.au lyre00.cse.unsw.edu.au NS +noall +additional
; (2 servers found)
;; global options: +cmd
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
```

Refer to

```
z5192519@wagner:~$ dig @q.au lyre00.cse.unsw.edu.au NS +noall +additional

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @q.au lyre00.cse.unsw.edu.au NS +noall +additional
; (2 servers found)
;; global options: +cmd
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
```

Refer to

```
z5192519@wagner:~$ dig @ns1.unsw.edu.au lyre00.cse.unsw.edu.au NS +noall +additional

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns1.unsw.edu.au lyre00.cse.unsw.edu.au NS +noall +additional
; (2 servers found)
;; global options: +cmd
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
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.242.2
maestro.orchestra.cse.unsw.edu.au. 300 IN A     129.94.242.33
```

Now inside CSE network

```
z5192519@wagner:~$ dig @129.94.172.11 lyre00.cse.unsw.edu.au A +short
129.94.210.20
z5192519@wagner:~$ dig @129.94.172.11 lyre00.cse.unsw.edu.au AAAA +short
z5192519@wagner:~$
```

Q10:

Following the process as shown, the IP address of lyre00.cse.unsw.edu.au is 129.94.210.20 . And to get this, we have to query 5 DNS nameservers.

Q11:

Yes, it can. A physical machine can have several hostnames and IPs for different services or interfaces.

Exercise 4: A Simple Web Server

(Please check the submitted python file. Testing index.html and png have also been put into the submission)