Lab03

Exercise 3: Digging into the DNS

1. The IP address of www.eecs.berkeley.edu is 23.185.0.1. The type of DNS query is Type A.

```
; <<>> DiG 9.16.27-Debian <<>> www.eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3706
;; 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.  39239   IN      CNAME   live-eecs.pantheonsite.io
live-eecs.pantheonsite.io. 148  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   300     IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       300     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       300     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       300     IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       300     IN      NS      ns-1213.awsdns-23.org.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   11228   IN      A       205.251.192.233
ns-233.awsdns-29.com.   82261   IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   30809   IN      A       205.251.194.132
ns-644.awsdns-16.net.   30809   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  18590   IN      A       205.251.196.189
ns-1213.awsdns-23.org.  4823    IN      AAAA    2600:9000:5304:bd00::1
ns-2013.awsdns-59.co.uk. 15050  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 15050  IN      AAAA    2600:9000:5307:dd00::1
```

2. The canonical names for the eecs.berkeley webserver is live-eecs.pantheonsite.io and fe1.edge.pantheon.io. A reason for having an alias for the webserver would be the alias name being easier for a client to use and remember if they frequently visit the site.
3. From the rest of the response, the authority section tells us that there are 4 nameserver records that are authoritative which are edge.pantheon.io. The additional section gives us the IP addresses of the nameservers in the authority section.
4. The IP address of the local nameserver for my machine is 129.94.242.45.

```
;; Query time: 8 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Tue Jun 28 09:25:17 AEST 2022
;; MSG SIZE  rcvd: 453
```

5. The DNS nameservers for eecs.berkely.edu are:

```
;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     64667   IN      A       169.229.60.61
ns.CS.berkeley.edu.     76696   IN      AAAA    2607:f140:8:1260::30
ns.eecs.berkeley.edu.   41720   IN      A       169.229.60.153
ns.eecs.berkeley.edu.   21541   IN      AAAA    2607:f140:8:2160::30
adns1.berkeley.edu.     687     IN      A       128.32.136.3
adns1.berkeley.edu.     5513    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     5512    IN      A       128.32.136.14
adns2.berkeley.edu.     5512    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     6224    IN      A       192.107.102.142
adns3.berkeley.edu.     3417    IN      AAAA    2607:f140:a000:d::abc
```

The first IP's of the nameservers are IP addresses while the second IP's of the same nameservers are the IPV6 addresses.

6. The DNS name associated with 111.68.101.54 is webserver.seecs.nust.edu.pk. The type of DNS query is PTR.

```
; <<>> DiG 9.16.27-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52825
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; 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. 2951 IN     PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 44558  IN      NS      ns1.hec.gov.pk.
101.68.111.in-addr.arpa. 44558  IN      NS      ns2.hec.gov.pk.

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Tue Jun 28 09:24:08 AEST 2022
;; MSG SIZE  rcvd: 140
```

7. No, I did not receive an authoritative answer. This is because there are no AA (Authoritative Answer) flags which suggests that CSE servers has no authority over the yahoo mail servers.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47975
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10
```

8. The result was a query status "REFUSED."

```
z5361001@corelli:~$ dig @adns1.berkeley.edu yahoo.com

; <<>> DiG 9.16.27-Debian <<>> @adns1.berkeley.edu yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 34162
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 756ac4889b8e13d7f9964bf862ba381891e7693393502b6c (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; Query time: 164 msec
;; SERVER: 128.32.136.3#53(128.32.136.3)
;; WHEN: Tue Jun 28 09:07:04 AEST 2022
;; MSG SIZE  rcvd: 66
```

9. The nameserver I used was ns1.yahoo.com and the DNS query was type A. Also, the server contains the AA flag, meaning it will return an authoritative answer.

```
z5361001@corelli:~$ dig @ns1.yahoo.com yahoo.com

; <<>> DiG 9.16.27-Debian <<>> @ns1.yahoo.com yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13072
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
; COOKIE: a7c0cb4b2e1da1603fd4229662ba37ea86527a5cbca79764 (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              1800    IN      A       74.6.231.20
yahoo.com.              1800    IN      A       74.6.143.26
yahoo.com.              1800    IN      A       98.137.11.163
yahoo.com.              1800    IN      A       98.137.11.164
yahoo.com.              1800    IN      A       74.6.143.25
yahoo.com.              1800    IN      A       74.6.231.21

;; Query time: 140 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Tue Jun 28 09:06:18 AEST 2022
;; MSG SIZE  rcvd: 162
```

10. I had to query 4 requests.
11. Yes. One physical machine can have several IP addresses/names associated with it.

Exercise 4: A Simple Web Server