lab03.md

Lab03

Digging into DNS

1. What is the IP address of www.eecs.berkeley.edu . What type of DNS query is sent to get this answer?

```
z5206205@vx3:~$ 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: 7807
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 8

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

;; ANSWER SECTION:
www.eecs.berkeley.edu.  69783   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 600  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   300     IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       124     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       124     IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       124     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       124     IN      NS      ns-644.awsdns-16.net.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   154482  IN      A       205.251.192.233
ns-644.awsdns-16.net.   99689   IN      A       205.251.194.132
ns-644.awsdns-16.net.   98566   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  97941   IN      A       205.251.196.189
ns-1213.awsdns-23.org.  97941   IN      AAAA    2600:9000:5304:bd00::1
ns-2013.awsdns-59.co.uk. 98561  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 92195  IN      AAAA    2600:9000:5307:dd00::1

;; Query time: 16 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 29 16:40:18 AEST 2020
;; MSG SIZE  rcvd: 425
```

IP Address: 23.185.0.1

DNS Query: Recursion Query

2. What is the canonical name for the eecs.berkeley web server? Suggest a reason for having an alias for this server.

Canonical name:

- live-eecs.pantheonsite.io
- fe1.edge.pantheon.io

A reason for having alias' for this server is to have multiple backup addresses.

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

Authority section contains 4 DNS servers. Additional section contains A(IPV4) and AAAA(IPV6) types.

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

129.94.242.45

5. What are the DNS nameservers for the " www.eecs.berkeley.edu ." domain (note: the domain name is eecs.berkeley.edu and not www.eecs.berkeley.edu)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

```
dig eecs.berkeley.edu
```

```
z5206205@vx3:~$ dig eecs.berkeley.edu

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> eecs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17701
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 9

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

;; ANSWER SECTION:
eecs.berkeley.edu.      21356   IN      A       23.185.0.1

;; AUTHORITY SECTION:
eecs.berkeley.edu.      74237   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      74237   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      74237   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      74237   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      74237   IN      NS      adns3.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     65785   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   8658    IN      A       169.229.60.153
adns1.berkeley.edu.     9574    IN      A       128.32.136.3
adns1.berkeley.edu.     6016    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     9574    IN      A       128.32.136.14
adns2.berkeley.edu.     6016    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     6015    IN      A       192.107.102.142
adns3.berkeley.edu.     6015    IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 29 17:45:41 AEST 2020
;; MSG SIZE  rcvd: 323
```

- adns1.berkeley.edu
  - 128.32.136.3
- ns.eecs.berkeley.edu
  - 169.229.60.153
- adns2.berkeley.edu
  - 128.32.136.3
- ns.CS.berkeley.edu
  - 169.229.60.61
- adns3.berkeley.edu
  - 192.107.102.142

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?

```
z5206205@vx3:~$ 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: 19974
;; 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. 3479 IN     PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 5224   IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 5224   IN      NS      ns1.hec.gov.pk.

;; ADDITIONAL SECTION:
ns1.hec.gov.pk.         1811    IN      A       103.4.93.5
ns2.hec.gov.pk.         1811    IN      A       103.4.93.6

;; Query time: 0 msec
;; SERVER: 129.94.242.45#53(129.94.242.45)
;; WHEN: Mon Jun 29 17:27:40 AEST 2020
;; MSG SIZE  rcvd: 172
```

OR

```
z5206205@vx3:~$ dig -x 111.68.101.54 +short
webserver.seecs.nust.edu.pk.
```

- webserver.seecs.nust.edu.pk

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 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: 32803
;; 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

;; ANSWER SECTION:
yahoo.com.              56      IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              56      IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              56      IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              85729   IN      NS      ns4.yahoo.com.
yahoo.com.              85729   IN      NS      ns2.yahoo.com.
yahoo.com.              85729   IN      NS      ns3.yahoo.com.
yahoo.com.              85729   IN      NS      ns1.yahoo.com.
yahoo.com.              85729   IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          236114  IN      A       68.180.131.16
ns1.yahoo.com.          9229    IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          154133  IN      A       68.142.255.16
ns2.yahoo.com.          66792   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          216     IN      A       27.123.42.42
ns3.yahoo.com.          216     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          63831   IN      A       98.138.11.157
ns5.yahoo.com.          60354   IN      A       202.165.97.53
ns5.yahoo.com.          86188   IN      AAAA    2406:2000:ff60::53

;; Query time: 1 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Mon Jun 29 17:39:51 AEST 2020
;; MSG SIZE  rcvd: 399
```

Because the flags do not contain an "aa" flag, there's no authoritative answer.

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

```
z5206205@vx3:~$ dig @192.107.102.142 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @192.107.102.142 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 6811
;; 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: 167 msec
;; SERVER: 192.107.102.142#53(192.107.102.142)
;; WHEN: Mon Jun 29 17:50:16 AEST 2020
;; MSG SIZE  rcvd: 38
```

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

```
z5206205@vx3:~$ dig yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20371
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9

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

;; ANSWER SECTION:
yahoo.com.              1216    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1216    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1216    IN      MX      1 mta6.am0.yahoodns.net.
```

Query: MX

- mta5.am0.yahoodns.net
- mta6.am0.yahoodns.net
- mta7.am0.yahoodns.net

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 //Get a.root-servers.net ip address
dig @198.41.0.4 au. -t NS //use this ip to get get a.au ip
dig @58.65.254.73 edu.au -t NS //use this ip to get q.edu.au ip
dig @65.22.196.1 unsw.edu.au. -t NS //use this ip to get ns1.unsw.edu.au ip
dig @129.94.0.192 cse.unsw.edu.au. -t NS //use this ip to get beethoven.orchestra.cse.unsw.edu.au ip
dig @129.94.208.3 cse.unsw.edu.au. -t A //use this ip to find host name
```

```
z5206205@vx3:~$ dig @129.94.208.3 cse.unsw.edu.au. -t A

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.208.3 cse.unsw.edu.au. -t A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48803
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
cse.unsw.edu.au.        3600    IN      A       129.94.242.53
cse.unsw.edu.au.        3600    IN      A       129.94.242.19
cse.unsw.edu.au.        3600    IN      A       129.94.242.49

;; 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: 129.94.208.3#53(129.94.208.3)
;; WHEN: Mon Jun 29 18:27:54 AEST 2020
;; MSG SIZE  rcvd: 180
```

IP: 129.94.242.53

Obtained by querying 6 DNS servers.

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

Yes, because an IP address is allowed to have multiple alias'.