Exercise 3: Digging into DNS

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

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

```
Alex@lab3$ dig www.eecs.berkeley.edu. +short
live-eecs.pantheonsite.io.
fe1.edge.pantheon.io.
23.185.0.1
```

The DNS query type is of type A.

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

The Canonical name for www.eecs.berkeley.edu is live-eecs.pantheonsite.io.

```
Alex@lab3$ dig www.eecs.berkeley.edu. cname +short
live-eecs.pantheonsite.io.
```

Reason for having an alias for this server: A CNAME record can prove convenient when running multiple services (like an FTP server (port 21/22) and a web server (port 80/443), each running different ports) from a single IP address. Then, if the IP address ever changes, one only has to record the change in one place within the network.

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

The Authority section is the name servers that return the ultimate authoritative response (i.e. This hostname has this IP or CNAME). The additional section provides more information about the Name servers that returned the authoritative response and the dig query itself.

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

;; ADDITIONAL SECTION:
ns-644.awsdns-16.net.   64863   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  47926   IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 60979  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 147703 IN      AAAA    2600:9000:5307:dd00::1
```

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

The IP address of the local nameserver is (Assuming only IPv4 and I am on vlab):

```
Alex@lab3$ grep nameserver /etc/resolv.conf
nameserver 129.94.242.2
nameserver 129.94.242.45
nameserver 129.94.242.33
```

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

```
;; AUTHORITY SECTION:
eecs.berkeley.edu.     84755   IN     NS     adns2.berkeley.edu.
eecs.berkeley.edu.     84755   IN     NS     adns1.berkeley.edu.
eecs.berkeley.edu.     84755   IN     NS     ns.CS.berkeley.edu.
eecs.berkeley.edu.     84755   IN     NS     ns.eecs.berkeley.edu.
eecs.berkeley.edu.     84755   IN     NS     adns3.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     263     IN     A       169.229.60.61
ns.CS.berkeley.edu.     263     IN     AAAA    2607:f140:8:1260::30
ns.eecs.berkeley.edu.   2951    IN     A       169.229.60.153
ns.eecs.berkeley.edu.   263     IN     AAAA    2607:f140:8:2160::30
adns1.berkeley.edu.     9155    IN     A       128.32.136.3
adns1.berkeley.edu.     8660    IN     AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     8660    IN     A       128.32.136.14
adns2.berkeley.edu.     8660    IN     AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     9155    IN     A       192.107.102.142
adns3.berkeley.edu.     4645    IN     AAAA    2607:f140:a000:d::abc
```

DNS query type is of NS

Question 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?

```
Alex@lab3$ dig -x 111.68.101.54
;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 3600 IN     PTR     webserver.seecs.nust.edu.pk.
```

The type of DNS query is reverse lookup

Question 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)

```
Alex@lab3$ dig @129.94.242.2 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.2 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7298
;; 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.              1060    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1060    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1060    IN      MX      1 mta5.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              7046    IN      NS      ns4.yahoo.com.
yahoo.com.              7046    IN      NS      ns1.yahoo.com.
yahoo.com.              7046    IN      NS      ns3.yahoo.com.
yahoo.com.              7046    IN      NS      ns5.yahoo.com.
yahoo.com.              7046    IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          511288  IN      A       68.180.131.16
ns1.yahoo.com.          26979   IN      AAAA    2001:4998:1b0::7961:686f:6f21
ns2.yahoo.com.          250989  IN      A       68.142.255.16
ns2.yahoo.com.          27010   IN      AAAA    2001:4998:1c0::7961:686f:6f21
ns3.yahoo.com.          909     IN      A       27.123.42.42
ns3.yahoo.com.          909     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          502565  IN      A       98.138.11.157
ns5.yahoo.com.          8099    IN      A       202.165.97.53
ns5.yahoo.com.          15534   IN      AAAA    2406:2000:1d0::7961:686f:6f21

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 08 16:34:27 AEDT 2022
;; MSG SIZE  rcvd: 399
```

we did not get an authoritative, it did not come from an authoritative server. We did not get an “aa” flag in the response.

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

```
Alex@lab3$ dig @adns2.berkeley.edu. yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @adns2.berkeley.edu. yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 65178
;; 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
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 167 msec
;; SERVER: 128.32.136.14#53(128.32.136.14)
;; WHEN: Tue Mar 08 16:38:37 AEDT 2022
;; MSG SIZE  rcvd: 38
```

No response from the Nameserver

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

```
Alex@lab3$ dig @ns1.yahoo.com yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39707
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.

;; Query time: 142 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Tue Mar 08 16:43:04 AEDT 2022
;; MSG SIZE  rcvd: 117
```

DNS query is of type MX and is recursive

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, drum00.cse.unsw.edu.au or drum01.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?

I am using VLAB. The IP of lyre00.cse.unsw.edu.au is: 129.94.210.21

```
Alex@lab3$ dig lyre01.cse.unsw.edu.au. +short
129.94.210.21

Alex@lab3$ dig . NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13432
;; 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:
.                       126072  IN      NS      m.root-servers.net.
.                       126072  IN      NS      d.root-servers.net.
.                       126072  IN      NS      b.root-servers.net.
.                       126072  IN      NS      g.root-servers.net.
.                       126072  IN      NS      k.root-servers.net.
.                       126072  IN      NS      a.root-servers.net.
.                       126072  IN      NS      c.root-servers.net.
.                       126072  IN      NS      i.root-servers.net.
.                       126072  IN      NS      e.root-servers.net.
.                       126072  IN      NS      j.root-servers.net.
.                       126072  IN      NS      h.root-servers.net.
.                       126072  IN      NS      f.root-servers.net.
.                       126072  IN      NS      l.root-servers.net.
```

```
Alex@lab3$ dig @a.root-servers.net lyre01.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @a.root-servers.net lyre01.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20195
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lyre01.cse.unsw.edu.au.            IN      A

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

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

;; Query time: 141 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Mar 08 22:46:49 AEDT 2022
;; MSG SIZE  rcvd: 291
```

```
Alex@lab3$ dig @q.au. lyre01.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @q.au. lyre01.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4019
;; 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:
```

```
;lyre01.cse.unsw.edu.au.            IN      A

;; AUTHORITY SECTION:
unsw.edu.au.        900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.        900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.        900     IN      NS      ns2.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: 24 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Tue Mar 08 22:47:32 AEDT 2022
;; MSG SIZE  rcvd: 209


Alex@lab3$ dig @ns3.unsw.edu.au. lyre01.cse.unsw.edu.au

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns3.unsw.edu.au. lyre01.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5140
;; 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:
;lyre01.cse.unsw.edu.au.            IN      A

;; 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: 159 msec
;; SERVER: 192.155.82.178#53(192.155.82.178)
;; WHEN: Tue Mar 08 22:47:47 AEDT 2022
;; MSG SIZE  rcvd: 171


Alex@lab3$ dig @beethoven.orchestra.cse.unsw.edu.au. lyre01.cse.unsw.edu.au
```

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @beethoven.orchestra.cse.unsw.edu.au.
lyre01.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20660
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lyre01.cse.unsw.edu.au.            IN      A

;; ANSWER SECTION:
lyre01.cse.unsw.EDU.AU. 3600    IN      A       129.94.210.21

;; 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: Tue Mar 08 22:48:25 AEDT 2022
;; MSG SIZE  rcvd: 177
```

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

Yes.