Lab 3 Answers

Exercise 3

```
weill % 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: 54077
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 6

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

;; ANSWER SECTION:
www.eecs.berkeley.edu.  5801    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.       136     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       136     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       136     IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       136     IN      NS      ns-1213.awsdns-23.org.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   78219   IN      A       205.251.192.233
ns-233.awsdns-29.com.   7523    IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   73936   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  78653   IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 73618  IN      A       205.251.199.221

;; Query time: 24 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Oct 11 15:02:34 AEDT 2020
;; MSG SIZE  rcvd: 369
```

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

   23.185.0.1, query type A was used.

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

live-eecs.pantheonsite.io. The alias could be used for providing a separate hostname for specific network services, such as email or FTP, and pointing that hostname to the root domain.

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

   Authority sections lists servers which have the authority to answer DNS queries about the target domain. It looks like a few are listed for different countries (e.g. ns-2013.awsdns-59.co.uk and ns-644.awsdns-16.net) to redirect DNS queries to the root server. Based on the address names it looks like they're hosted on AWS. The additional section lists TTL values for cached data on the server we received data from. Based on the answers in the additional section, ns-233.awsdns-29.com appears to be the closest DNS server with a TTL of 7523.

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

   129.94.242.2

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.      24617   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      24617   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      24617   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      24617   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      24617   IN      NS      adns2.berkeley.edu.
```

The above screenshot shows the DNS servers for eecs.berkeley.edu.

```
;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     73123   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   12120   IN      A       169.229.60.153
adns1.berkeley.edu.     99      IN      A       128.32.136.3
adns1.berkeley.edu.     99      IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     99      IN      A       128.32.136.14
adns2.berkeley.edu.     99      IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     99      IN      A       192.107.102.142
adns3.berkeley.edu.     99      IN      AAAA    2607:f140:a000:d::abc
```

The above screenshot shows the corresponding IP addresses (rightmost column) for each DNS nameserver (leftmost column) listed in the first screenshot.

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?

```
weill % 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: 47255
;; 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. 76  IN      PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 5807   IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 5807   IN      NS      ns1.hec.gov.pk.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Oct 11 15:45:52 AEDT 2020
;; MSG SIZE  rcvd: 140
```

As shown in the reverse lookup query in the above screenshot, the DNS name is webserver.seecs.nust.edu.pk. A PTR type query is sent to obtain this information.

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)

```
weill % dig @129.94.242.33 yahoo.com

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55451
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10

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

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

;; AUTHORITY SECTION:
yahoo.com.              69885   IN      NS      ns4.yahoo.com.
yahoo.com.              69885   IN      NS      ns1.yahoo.com.
yahoo.com.              69885   IN      NS      ns2.yahoo.com.
yahoo.com.              69885   IN      NS      ns3.yahoo.com.
yahoo.com.              69885   IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          151225  IN      A       68.180.131.16
ns1.yahoo.com.          79546   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          168652  IN      A       68.142.255.16
ns2.yahoo.com.          1250    IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1646    IN      A       27.123.42.42
ns3.yahoo.com.          1332    IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          163087  IN      A       98.138.11.157
ns5.yahoo.com.          27716   IN      A       202.165.97.53
ns5.yahoo.com.          43499   IN      AAAA    2406:2000:ff60::53

;; Query time: 100 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Oct 11 15:50:09 AEDT 2020
;; MSG SIZE  rcvd: 416
```

It was not an authoritative answer, the flags section in the output does not include aa (authoritative answer)

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

```
weill % dig @128.32.136.3 yahoo.com

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @128.32.136.3 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 40488
;; 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      A

;; Query time: 166 msec
;; SERVER: 128.32.136.3#53(128.32.136.3)
;; WHEN: Sun Oct 11 16:03:36 AEDT 2020
;; MSG SIZE  rcvd: 38
```

Also not an authoritative answer.

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

```
weill % dig @68.180.131.16 yahoo.com

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @68.180.131.16 yahoo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44992
;; flags: qr aa rd; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available

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

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

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          86400   IN      A       202.165.97.53
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::1003
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:ff60::53

;; Query time: 145 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Sun Oct 11 16:15:31 AEDT 2020
;; MSG SIZE  rcvd: 416
```

DNS query type A was used.

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?
    5
11. Can one physical machine have several names and/or IP addresses associated with it?
    Yes