Exercise 3: Digging into DNS (marked, include in the lab report, 5 Marks)

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

```
E   pantheon-systems.map.f
    151.101.30.133
```

The IP address of www.stanford.edu is 151.101.30.133. This can be found in the second line of the answer section, after IN A. The type of DNS query sent to get this answer is type A, as shown by the A in the same line.

```
z5359932@vx08:~$ dig www.stanford.edu

; <<>> DiG 9.16.44-Debian <<>> www.stanford.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40115
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b46bcb71c560a14901000000651cb122508b35a29228f87e (good)
;; QUESTION SECTION:
;www.stanford.edu.              IN      A

;; ANSWER SECTION:
www.stanford.edu.       1390    IN      CNAME   pantheon-systems.map.fastly.net.
pantheon-systems.map.fastly.net. 30 IN  A       151.101.30.133

;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Oct 04 11:26:10 AEDT 2023
;; MSG SIZE  rcvd: 134
```

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

The canonical name for the Standford webserver is pantheon-systems.map.fastly.net. This is indicated in the first line of the answer section, which shows that the CNAME of www.stanford.edu is pantheon-systems.map.fastly.net. A reason for having an alias for this server is that this alias is used for the cloud network, to access the server on the cloud. Through the alias, you can have more than one domain name for the same website. This allows the website to have distributed traffic.

Question 3. What can you make of the rest of the response/what it is used for (i.e. the details available in the DNS response (cookie and other fields))?

To provide security in the DNS system, there are cookies. This is shown in the screenshot below. A DNS cookie is a security mechanism which protects against DNS poisoning and known as an OPT record. This means that it does not hold any DNS data – rather it carries information about the interactive exchange of questions and answers for a particular transaction. These DNS cookies provide a layer of protection against off-path attacks. There are two types of DNS cookies: client cookies and server cookies. The client cookie holds information about the server IP address, the client IP address, and an encoded message which is more than 64 bit long that is private to the client. On the other hand, server cookies

carry information about the client IP address, the client cookie, and an encoded message that is at least 64 bits that is changed periodically.

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b46bcb71c560a14901000000651cb122508b35a29228f87e (good)
```

In addition to this, we can also see the time to live function (TTL) of the DNS in the response. This is the number next to www.stanford.edu. In the answer section. The TTL signifies the duration a packet remains valid in a network before a router discards it. It also dictates the period a DNS resolver should retain a query in its cache before seeking a new query. Consequently, a higher TTL results in quicker responses for relatively static resources.

```
1390
```

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

The IP address of the local nameserver for the machine is 129.94.242.2, as shown in the screenshot below.

```
;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Oct 04 11:26:10 AEDT 2023
```

Question 5. What are the DNS nameservers for the "stanford.edu.” domain (note: the domain name is stanford.edu and notwww.stanford.edu . This is an example of what is referred to as the apex/naked domain)? Find their IP addresses. Which DNS query type is used to obtain this information?

```
z5359932@vx08:~$ dig stanford.edu NS

; <<>> DiG 9.16.44-Debian <<>> stanford.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46970
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6db16fdf01bf6f5501000000651cb3c91f2a39cc96ec7755 (good)
;; QUESTION SECTION:
;stanford.edu.                  IN      NS

;; ANSWER SECTION:
stanford.edu.           40200   IN      NS      argus.stanford.edu.
stanford.edu.           40200   IN      NS      ns7.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      ns5.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      ns6.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      avallone.stanford.edu.
stanford.edu.           40200   IN      NS      atalante.stanford.edu.

;; ADDITIONAL SECTION:
ns5.dnsmadeeasy.com.    20777   IN      A       208.94.148.13
ns6.dnsmadeeasy.com.    75362   IN      A       208.80.124.13
ns7.dnsmadeeasy.com.    16317   IN      A       208.80.126.13
ns5.dnsmadeeasy.com.    23212   IN      AAAA    2600:1800:5::1
ns7.dnsmadeeasy.com.    16788   IN      AAAA    2600:1802:7::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Oct 04 11:37:29 AEDT 2023
;; MSG SIZE  rcvd: 308
```

As shown below, the DNS nameservers for the “stanford.edu” domain is argus.standford.edu., ns7.dnsmadeeasy.com., ns5.dnsmadeeasy.com., ns6.dnsmadeeasy.com., avallone.stanford.edu., atalante.stanford.edu.. This can be seen in the answer section, after all the ‘NS’, which shows that it is a type NS query.

```
;; ANSWER SECTION:
stanford.edu.           40200   IN      NS      argus.stanford.edu.
stanford.edu.           40200   IN      NS      ns7.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      ns5.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      ns6.dnsmadeeasy.com.
stanford.edu.           40200   IN      NS      avallone.stanford.edu.
stanford.edu.           40200   IN      NS      atalante.stanford.edu.
```

We can find the IP addresses of these nameservers in the additional section of the response, as shown in the screenshot below.

```
ns5.dnsmadeeasy.com.    20777   IN      A       208.94.148.13
ns6.dnsmadeeasy.com.    75362   IN      A       208.80.124.13
ns7.dnsmadeeasy.com.    16317   IN      A       208.80.126.13
```

The DNS query type used to obtain this information is a type A query, as shown above.

Question 6. What is the DNS name associated with the IP address 129.25.60.56 ? Which DNS query type is used to obtain this information?

```
z5359932@vx08:~$ dig -x 129.25.60.56

; <<>> DiG 9.16.44-Debian <<>> -x 129.25.60.56
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21940
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 91ec7daa08ffaa7501000000651cb5587bcecd709d22bfff (good)
;; QUESTION SECTION:
;56.60.25.129.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
56.60.25.129.in-addr.arpa. 95   IN      PTR     ece.drexel.edu.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Oct 04 11:44:08 AEDT 2023
;; MSG SIZE  rcvd: 110
```

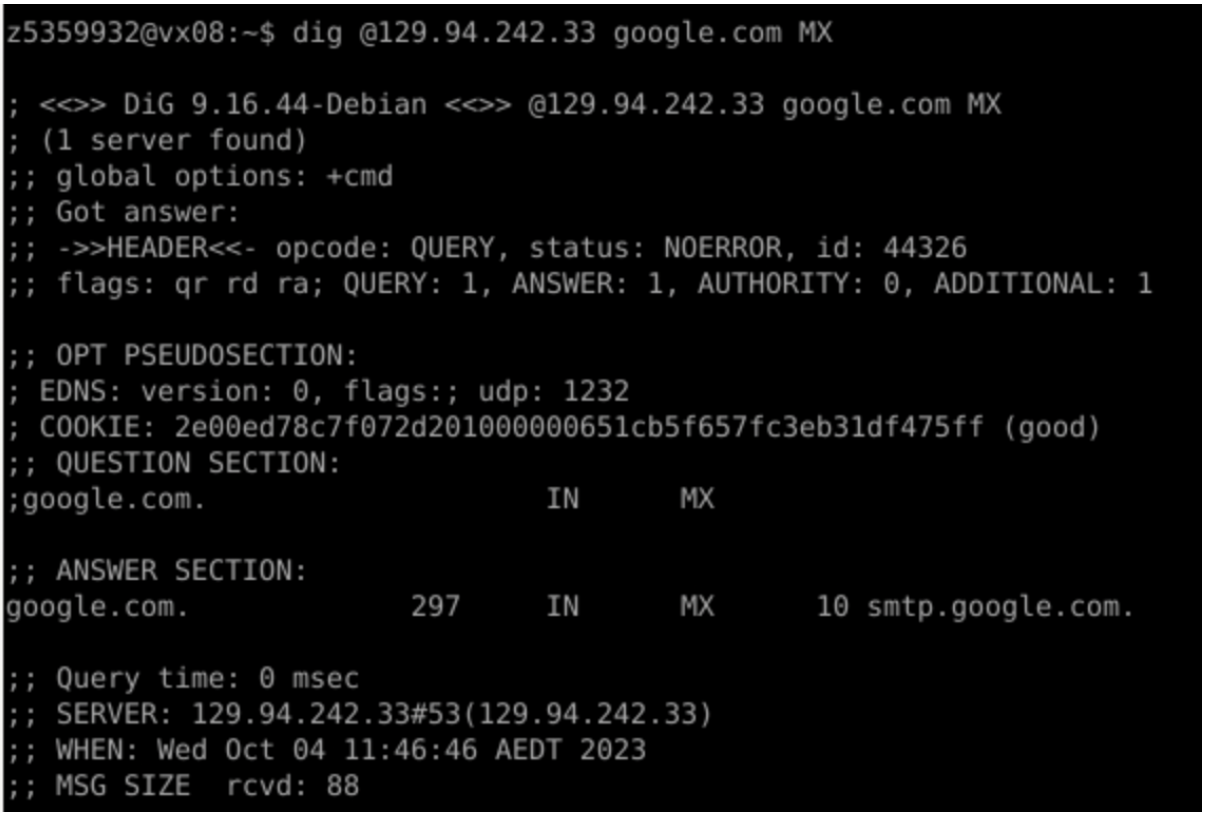
The DNS name associated with the IP address 129.25.60.56 is ece.drexel.edu., as shown in the answer section. This was obtained by the DNS query type PTR, also known as a pointer record. This type gives information about the domain name lined to the IP address. This is the opposite of the type A query, which specifies the IP address once given the domain name. Additionally, we can see that the IP address has been reversed in the answer section. This is because of how PTR records are stored under the IP address.

```
;56.60.25.129.in-a
```

Question 7. Run, dig and query the CSE nameserver (129.94.242.33) for the mail servers for google.com (again, the domain name is google.com, not www.google.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 message to determine the answer)

```
smtp.google.com.
```

The mail server is smtp.google.com., which is shown in the answer section after MX, which stands for the mail exchange record.



We did not get an authoritative answer, because we don't have the flags 'aa'. The reason for this is because the CSE server is not google and does not have the same authority as google. Since we asked the CSE server, which is not the source of mail server, it is not authoritative.

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

As shown in the screenshot below, the status of the request is REFUSED. Additionally, we can see in the warning message that recursion was requested but not available. This is a security feature, where Stanford would not perform recursive query since we are not within the Stanford network. Therefore, we cannot get any information from the requests that we make to the nameservers obtained in Question 5.

```
z5359932@vx08:~$ dig @208.94.148.13 google.com MX

; <<>> DiG 9.16.44-Debian <<>> @208.94.148.13 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 44658
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      MX

;; Query time: 4 msec
;; SERVER: 208.94.148.13#53(208.94.148.13)
;; WHEN: Wed Oct 04 11:53:52 AEDT 2023
;; MSG SIZE  rcvd: 39
```

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

In order to find the authoritative answer for the mail servers for google.com, we must first search for the name servers of google.com.

```
z5359932@vx08:~$ dig google.com NS

; <<>> DiG 9.16.44-Debian <<>> google.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65472
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2e3473c9f6da2be501000000651cb8d2d4d9ff3781de0746 (good)
;; QUESTION SECTION:
;google.com.                    IN      NS

;; ANSWER SECTION:
google.com.             79899   IN      NS      ns4.google.com.
google.com.             79899   IN      NS      ns3.google.com.
google.com.             79899   IN      NS      ns1.google.com.
google.com.             79899   IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         257970  IN      A       216.239.32.10
ns2.google.com.         157950  IN      A       216.239.34.10
ns3.google.com.         256679  IN      A       216.239.36.10

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Oct 04 11:58:58 AEDT 2023
;; MSG SIZE  rcvd: 187
```

From this, we can see that there are 4 nameservers of google.com. We will send out a query to one of the name servers, asking about the mail servers of google.com.

```
z5359932@vx08:~$ dig @ns1.google.com google.com MX

; <<>> DiG 9.16.44-Debian <<>> @ns1.google.com google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59756
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 10
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        300     IN      A       142.251.175.27
smtp.google.com.        300     IN      A       74.125.24.26
smtp.google.com.        300     IN      A       74.125.24.27
smtp.google.com.        300     IN      A       142.250.4.27
smtp.google.com.        300     IN      A       142.251.10.27
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c1c::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c03::1a
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c03::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c06::1b

;; Query time: 92 msec
;; SERVER: 216.239.32.10#53(216.239.32.10)
;; WHEN: Wed Oct 04 11:59:29 AEDT 2023
;; MSG SIZE  rcvd: 252
```

Now, in the flag section, we can see an ‘aa’, which signifies that this is an authoritative answer. In the answer section, we can see the same mail server of smtp.google.com, which was DNS queried by the type MX.

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, flute00.cse.unsw.edu.au or flute01.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?

```
;; ADDITIONAL SECTION:
a.root-servers.net.     71132   IN      A       198.41.0.4
```

```
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61519
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

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

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

;; ADDITIONAL SECTION:
d.au.                   172800  IN      A       162.159.25.38
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
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
c.au.                   172800  IN      A       162.159.24.179
c.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:18b3

;; Query time: 96 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Wed Oct 04 12:05:05 AEDT 2023
;; MSG SIZE  rcvd: 391
```

```
z5359932@vx08:~$ dig @d.au edu.au. NS

; <<>> DiG 9.16.44-Debian <<>> @d.au edu.au. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45342
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;edu.au.                                IN      NS

;; AUTHORITY SECTION:
edu.au.                 900     IN      NS      r.au.
edu.au.                 900     IN      NS      t.au.
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      q.au.

;; ADDITIONAL SECTION:
q.au.                   900     IN      A       65.22.196.1
r.au.                   900     IN      A       65.22.197.1
s.au.                   900     IN      A       65.22.198.1
t.au.                   900     IN      A       65.22.199.1
q.au.                   900     IN      AAAA    2a01:8840:be::1
r.au.                   900     IN      AAAA    2a01:8840:bf::1
s.au.                   900     IN      AAAA    2a01:8840:c0::1
t.au.                   900     IN      AAAA    2a01:8840:c1::1

;; Query time: 8 msec
;; SERVER: 162.159.25.38#53(162.159.25.38)
;; WHEN: Wed Oct 04 12:14:19 AEDT 2023
;; MSG SIZE  rcvd: 275
```

```
z5359932@vx08:~$ dig @t.au unsw.edu.au. NS

; <<>> DiG 9.16.44-Debian <<>> @t.au unsw.edu.au. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41641
;; 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:
;unsw.edu.au.                   IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        900     IN      A       129.94.0.192
ns1.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        900     IN      A       129.94.0.193
ns2.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::2
ns3.unsw.edu.au.        900     IN      A       192.155.82.178

;; Query time: 8 msec
;; SERVER: 65.22.199.1#53(65.22.199.1)
;; WHEN: Wed Oct 04 12:14:50 AEDT 2023
;; MSG SIZE  rcvd: 198
```

```
z5359932@vx08:~$ dig @ns1.unsw.edu.au cse.unsw.edu.au. NS

; <<>> DiG 9.16.44-Debian <<>> @ns1.unsw.edu.au cse.unsw.edu.au. NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36150
;; 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:
;cse.unsw.edu.au.               IN      NS

;; AUTHORITY SECTION:
cse.unsw.edu.au.        300     IN      NS      maestro.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        300     IN      NS      beethoven.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: 4 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Wed Oct 04 12:15:48 AEDT 2023
;; MSG SIZE  rcvd: 164
```

```
z5359932@vx10:~$ dig @129.94.242.2 lyre00.cse.unsw.edu.au A

; <<>> DiG 9.16.44-Debian <<>> @129.94.242.2 lyre00.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46949
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d5a58b990bdbadd8010000006523265 76a3f98ab6dec399b (good)
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      A

;; ANSWER SECTION:
lyre00.cse.unsw.EDU.AU. 3600    IN      A       129.94.210.20

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Oct 09 08:59:51 AEDT 2023
;; MSG SIZE  rcvd: 117
```

As shown above, the IP address of the host is 129.94.210.20. In order to get an authoritative answer, we performed 5 queries. This can be seen in the flag section, with only the last screenshot having the ‘aa’ tag.

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

One physical machine can have several names and/or IP addresses associated with it. As shown above, there can be multiple aliases, which can be useful to identify different functions and roles that the physical machine may perform. Additionally, there may be multiple names for external and internal use. Furthermore, in the event of a network failure, redirecting traffic to a different IP address will ensure that the machine runs its service smoothly for clients.