Lab03

COMP3331: Computer Networks and Applications

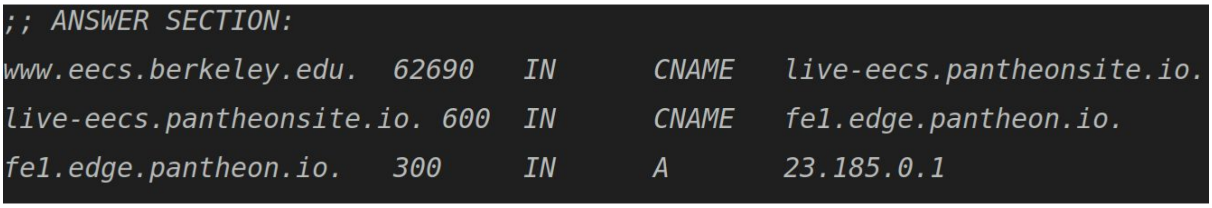
Hoya Lee

Z5226463

11 October 2020

Digging into DNS

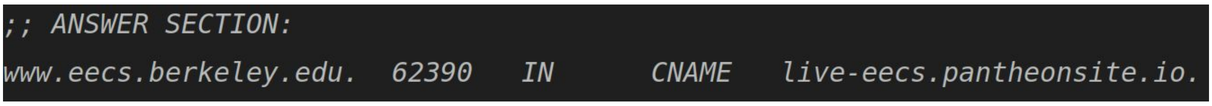
1. What is the IP address of www.eecs.berkeley.edu . What type of DNS query is sent to get this answer?



```
;; ANSWER SECTION:
www.eecs.berkeley.edu.  62690   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
```

The IP Address of www.eecs.berkeley.edu is 23.185.0.1. "*A record*" query was sent to get this answer.

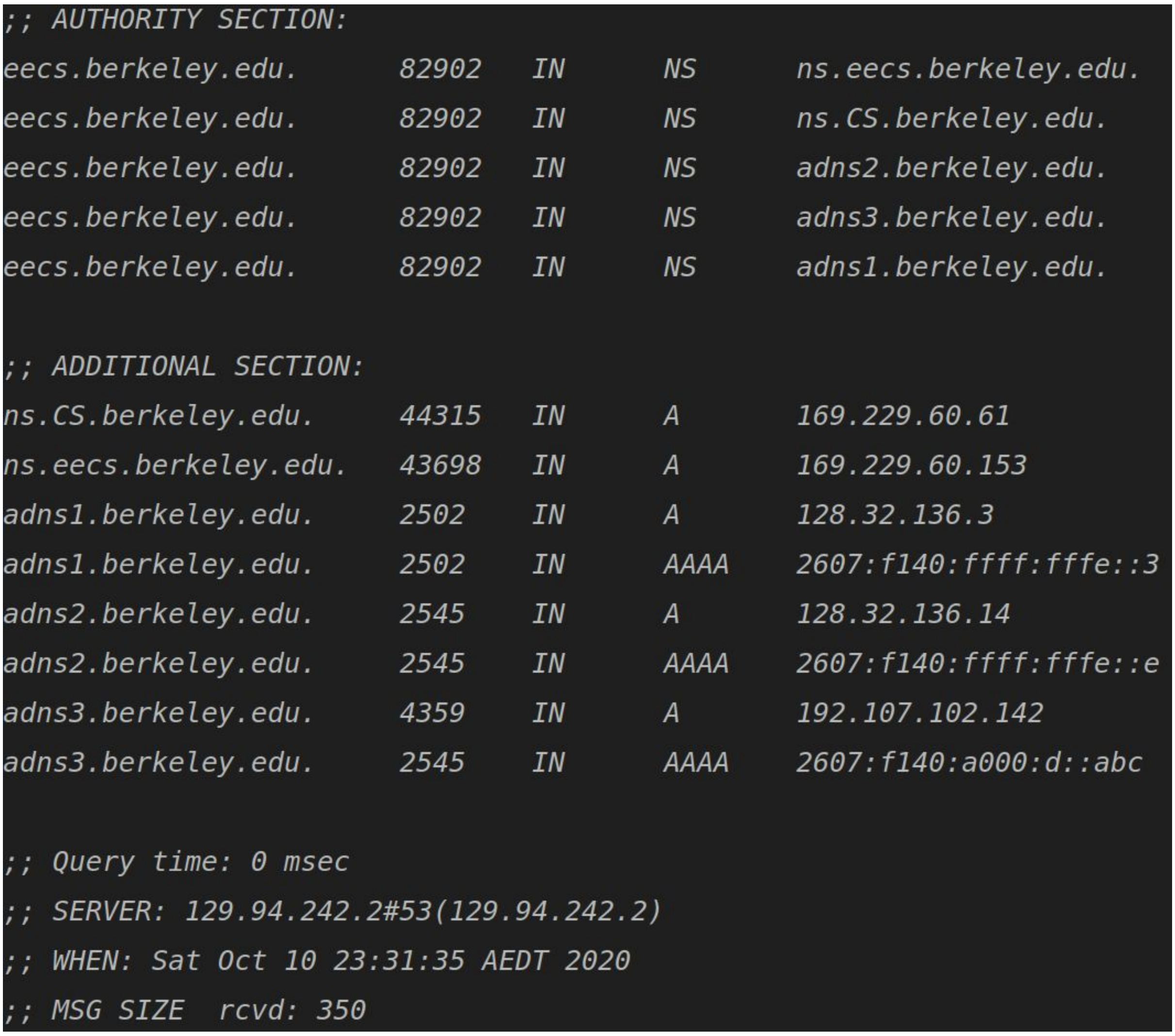
2. What is the canonical name for the eecs.berkeley web server (i.e. www.eecs.berkeley.edu)? Suggest a reason for having an alias for this server.



```
;; ANSWER SECTION:
www.eecs.berkeley.edu.  62390   IN      CNAME   live-eecs.pantheonsite.io.
```

The canonical name (CNAME) of the web server is live-eecs.pantheonsite.io. The reason for having an alias for the server is because they want all queries to flow through a proxy system, instead of mapping straight to the resource being requested. Moreover, it is also easier for people to remember the alias (*www*) as it is more readable and more widely used.

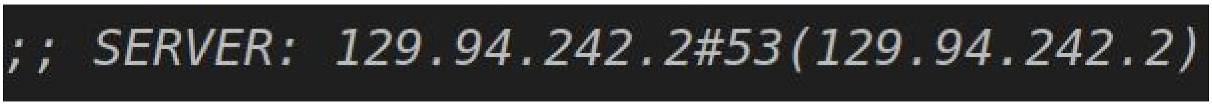
3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?



```
;; AUTHORITY SECTION:
eecs.berkeley.edu.      82902   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      82902   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      82902   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      82902   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      82902   IN      NS      adns1.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     44315   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   43698   IN      A       169.229.60.153
adns1.berkeley.edu.     2502    IN      A       128.32.136.3
adns1.berkeley.edu.     2502    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     2545    IN      A       128.32.136.14
adns2.berkeley.edu.     2545    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     4359    IN      A       192.107.102.142
adns3.berkeley.edu.     2545    IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sat Oct 10 23:31:35 AEDT 2020
;; MSG SIZE  rcvd: 350
```

From the Authority section, it can be inferred that the domain has five DNS servers. The Authority section encompasses the details of the name servers. The additional section provides the IP addresses, specifically IPv4 (*A records*) and IPv6(*AAAA records)* for the name servers. The section below the additional section shows the details about the query: the time it took, the server it is from (*CSE Machine)* when the query was made, and the message size.

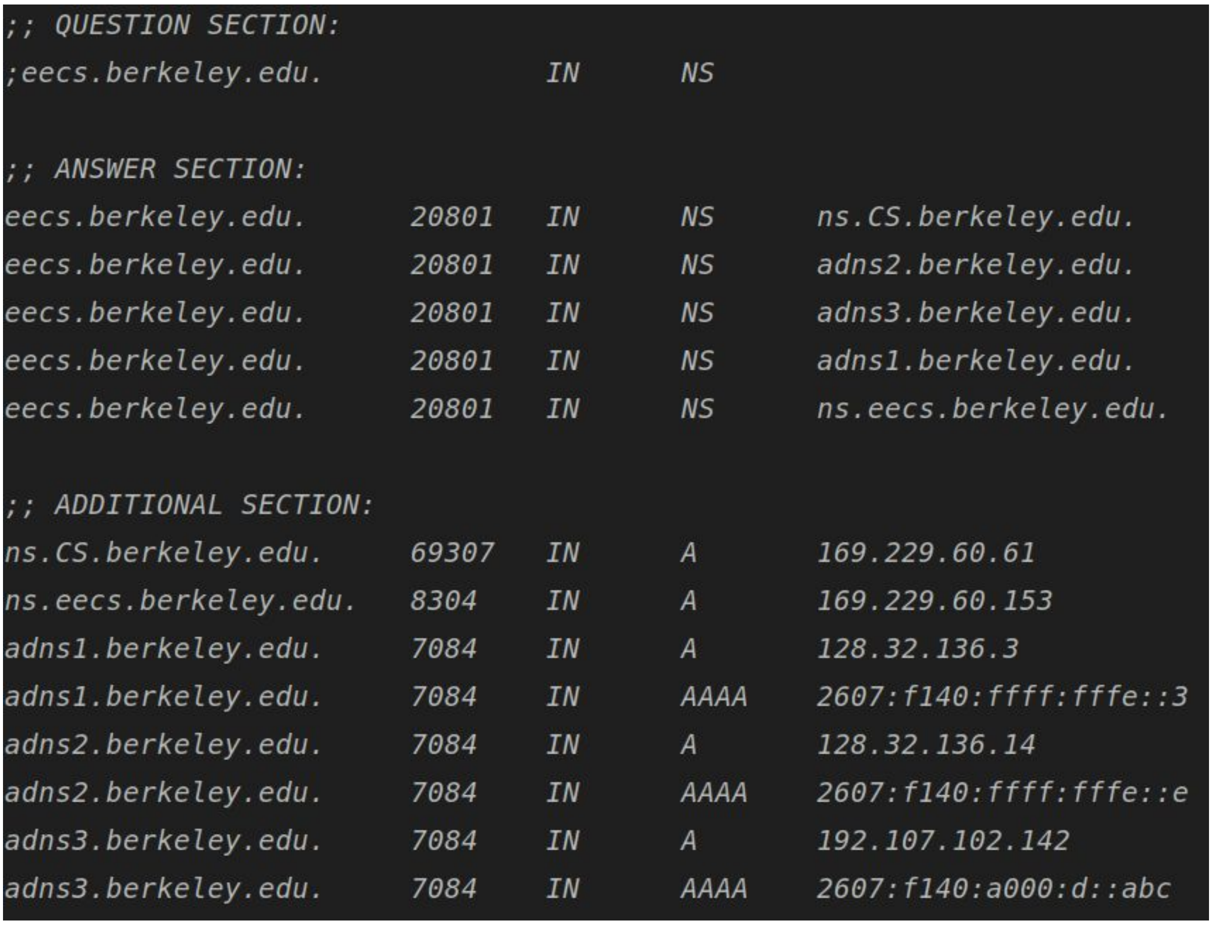
4. What is the IP address of the local nameserver for your machine?



```
;; SERVER: 129.94.242.2#53(129.94.242.2)
```

The IP address of my local nameserver is 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?



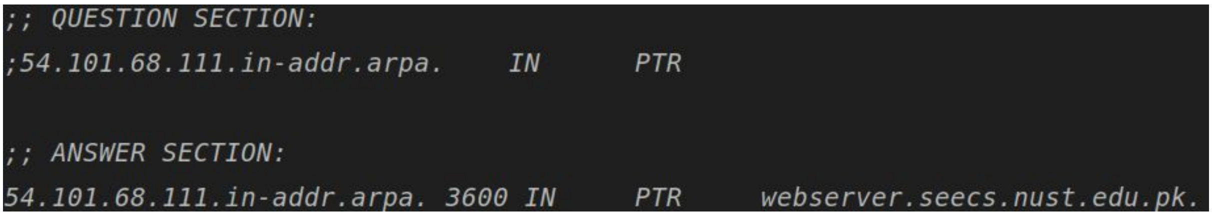
```
;; QUESTION SECTION:
;eecs.berkeley.edu.             IN      NS

;; ANSWER SECTION:
eecs.berkeley.edu.      20801   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      20801   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      20801   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      20801   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      20801   IN      NS      ns.eecs.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     69307   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   8304    IN      A       169.229.60.153
adns1.berkeley.edu.     7084    IN      A       128.32.136.3
adns1.berkeley.edu.     7084    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     7084    IN      A       128.32.136.14
adns2.berkeley.edu.     7084    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     7084    IN      A       192.107.102.142
adns3.berkeley.edu.     7084    IN      AAAA    2607:f140:a000:d::abc
```

There are five DNS nameservers for eecs.berkeley.edu. These nameservers are:

- ns.CS.berkeley.edu. With IPv4 169.229.60.61
- adns2.berkeley.edu. With IPv4 128.32.136.14 and IPv6 2607:f140:ffff:fffe::e
- adns3.berkeley.edu. With IPv4 192.107.102.142 and I2607:f140:a000:d::abc
- adns1.berkeley.edu. With IPv4 128.32.136.3 and IPv6 2607:f140:ffff:fffe::3
- ns.eecs.berkeley.edu. With IPv4 169.229.60.153

The type of query sent to retrieve the information above is an *NS* (nameserver) record query.

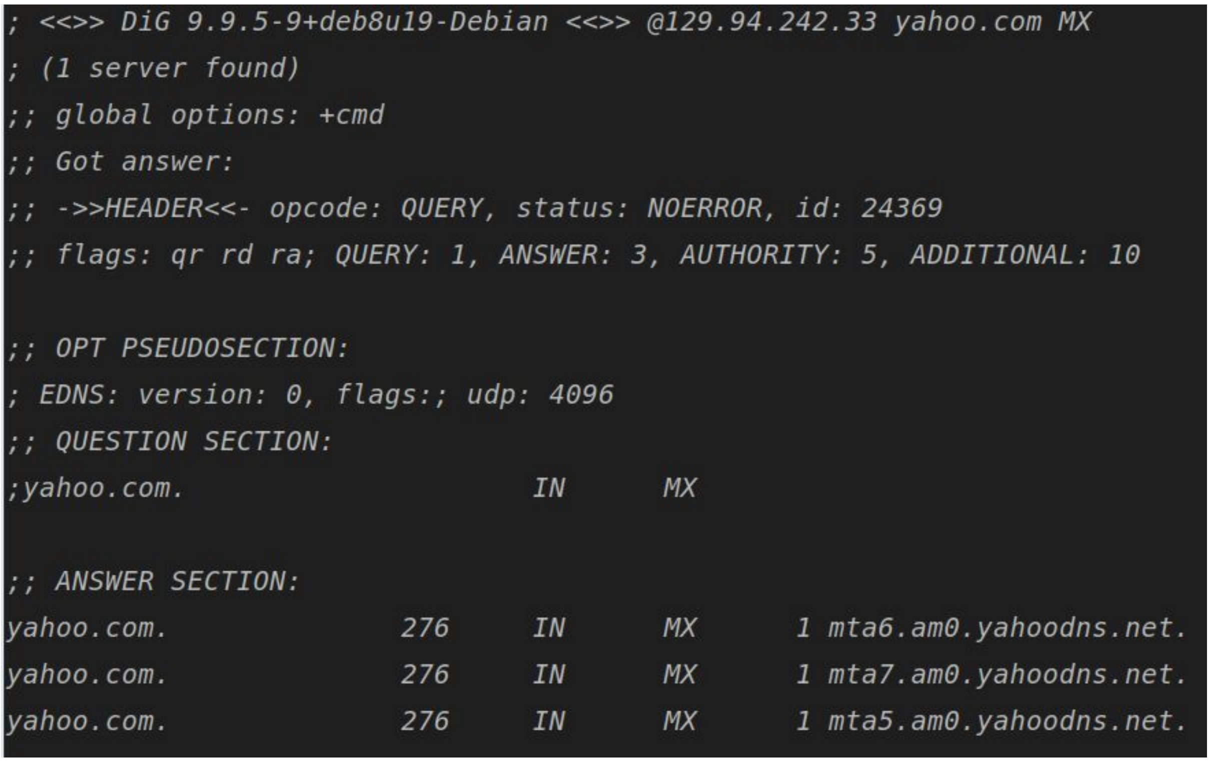
6. What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?



```
;; QUESTION SECTION:
;54.101.68.111.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 3600 IN     PTR     webserver.seecs.nust.edu.pk.
```

The DNS name associated with the given IP address was webserver.seecs.nust.edu.pk. The type of DNS query sent for the reverse lookup is a *PTR* record query.

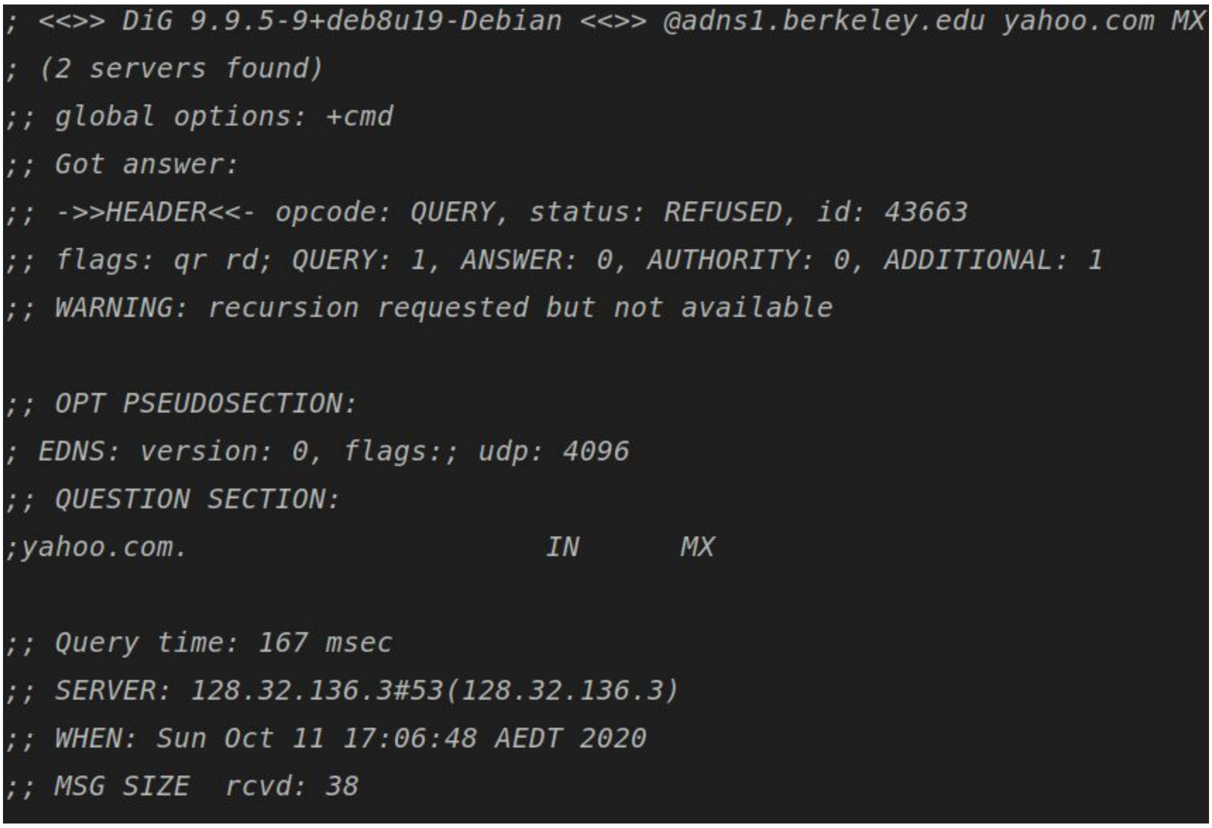
7. Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not www.yahoo.com). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does 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: 24369
;; 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.              276     IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              276     IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              276     IN      MX      1 mta5.am0.yahoodns.net.
```

No, an authoritative answer was not obtained as there was no *aa* flag in the response. The reason behind this is because CSE nameserver was queried and not a DNS server which has authority over those records (e.g. Yahoo DNS servers)

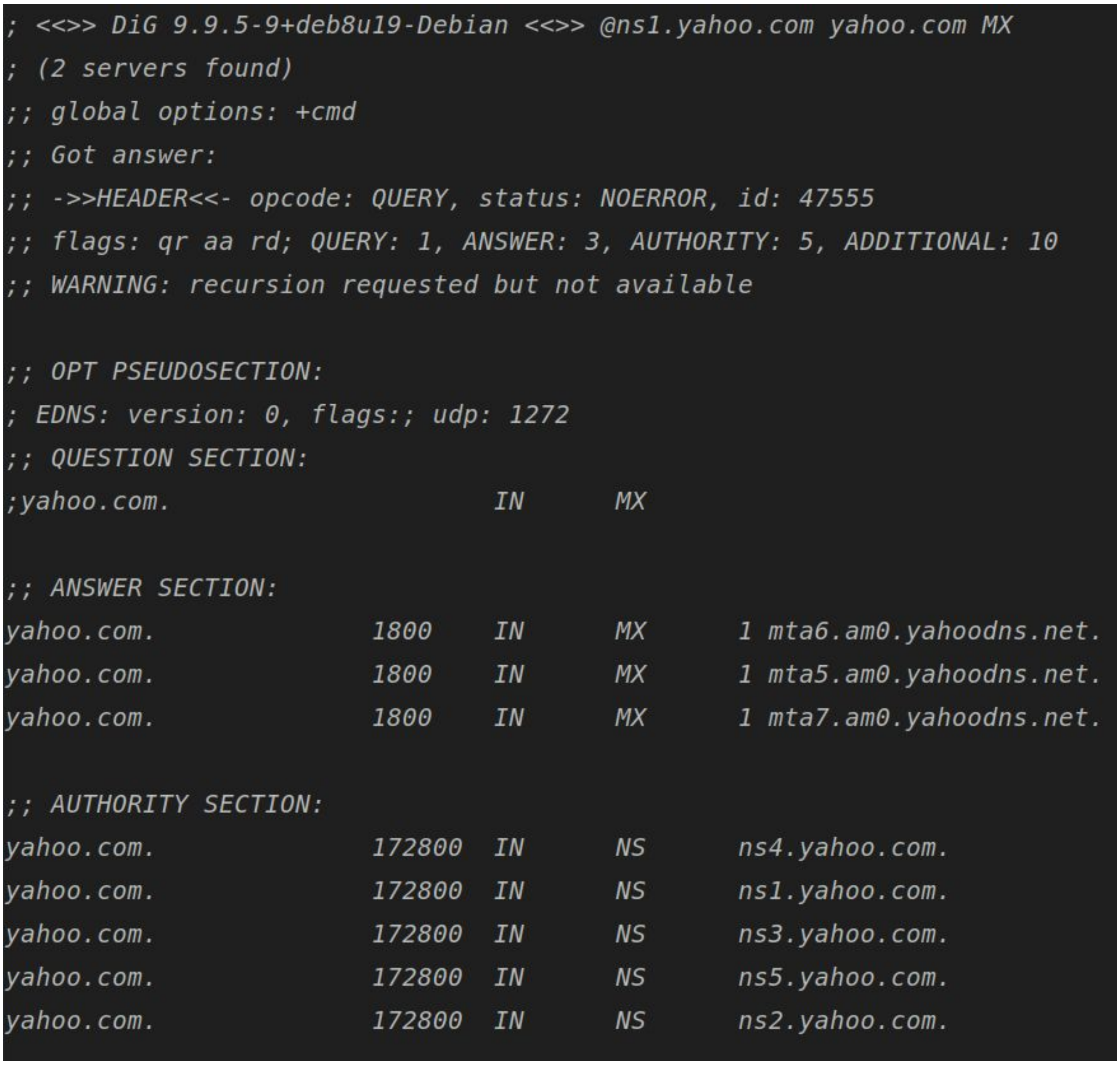
8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?



```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @adns1.berkeley.edu yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 43663
;; 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: 128.32.136.3#53(128.32.136.3)
;; WHEN: Sun Oct 11 17:06:48 AEDT 2020
;; MSG SIZE  rcvd: 38
```

When the question above was repeated with all five nameservers obtained from question 5, the result was not obtained. This can be seen from the fact that the *status* is set to *REFUSED.* This is a result of the way in which the DNS is configured -- it is not allowing requests such as this. Also, this is because my machine (CSE machine) is not part of berkeley, and hence service is not provided for the CSE machine.

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



```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @ns1.yahoo.com yahoo.com MX
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47555
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; 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 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.

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

The authoritative answer for the yahoo mail server was obtained by using one of the Yahoo DNS servers. From the response above, it can be seen that the response is authoritative as the flag is set as *aa*. It provides the MX records for the yahoo domain. The type of the DNS query sent to obtain this information is an *MX* record query.

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?

   a. Contact root nameserver

      Command: dig . NS

      Answer: a.root-servers.net

   b. Contact AU nameserver

      Command: dig @a.root-servers.net weber.orchestra.cse.unsw.EDU.AU

      Answer: m.au

   c. Contact edu.au nameserver

      Command: dig @m.au weber.orchestra.cse.unsw.EDU.AU

      Answer: q.au

   d. Contact unsw.edu.au nameserver

      Command: dig @q.au weber.orchestra.cse.unsw.EDU.AU

      Answer: ns1.unsw.edu.au

   e. Contact cse.unsw.edu.au nameserver

      Command: dig @ns1.unsw.edu.au weber.orchestra.cse.unsw.EDU.AU

      Answer: beethoven.orchestra.cse.unsw.edu.au

   f. Authoritative answer from the cse.unsw.edu.au nameserver

      Command: dig @beethoven.orchestra.cse.unsw.edu.au weber.orchestra.cse.unsw.EDU.AU

      Answer: 129.94.242.49

A total of 5 DNS servers (root, au, edu.au, unsw.edu.au, cse.unsw.edu.au) to get an authoritative answer.

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

One physical machine can have multiple names and IP addresses associated with it. Multiple IP addresses can be used across different network interface cards or on the same network interface card. It is essential when implementing server virtualization. Each virtual server running on the same hardware will need its own IP address to function. A physical machine can also have multiple names if you add multiple A records where the names map to the same IP address.