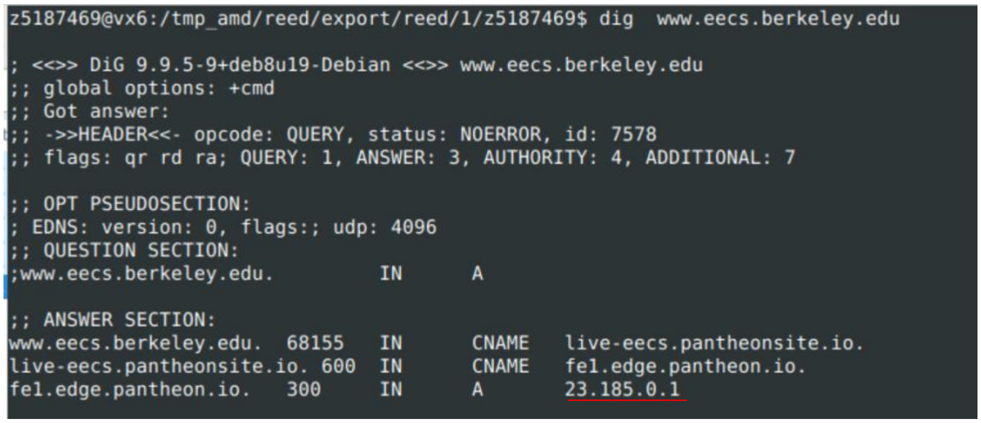
Yiyun Yang
Z5187469

Ex3

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 is 23.185.0.1.
The type of DNS query is recursive query.



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ 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: 7578
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 7

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

;; ANSWER SECTION:
www.eecs.berkeley.edu.  68155   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
```

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

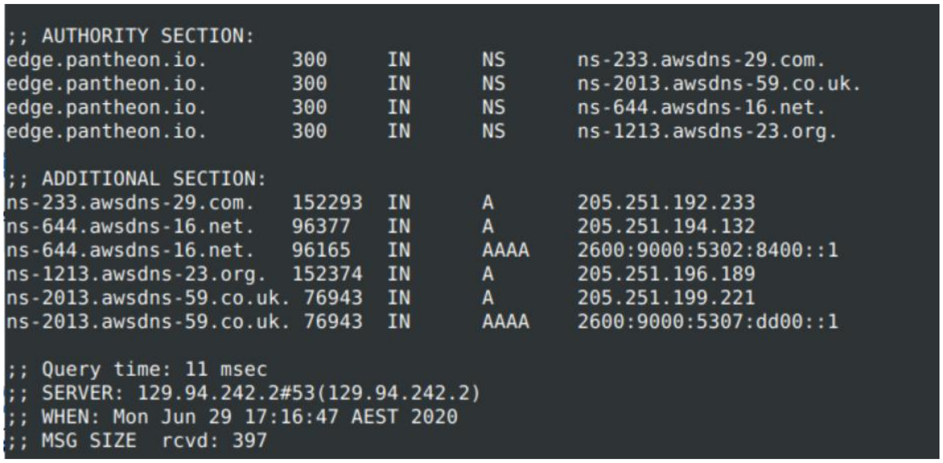
The canonical name for eecs.berkeley is live-eecs.pantheonsite.io.

IP aliasing is associating more than one IP address to a network interface. With this, one node on a network can have multiple connections to a network, each serving a different purpose.

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

We have 4 authoritative name servers for the domain name.

In the additional section, we have A and AAAA, which are IPv4 and IPv6 address.



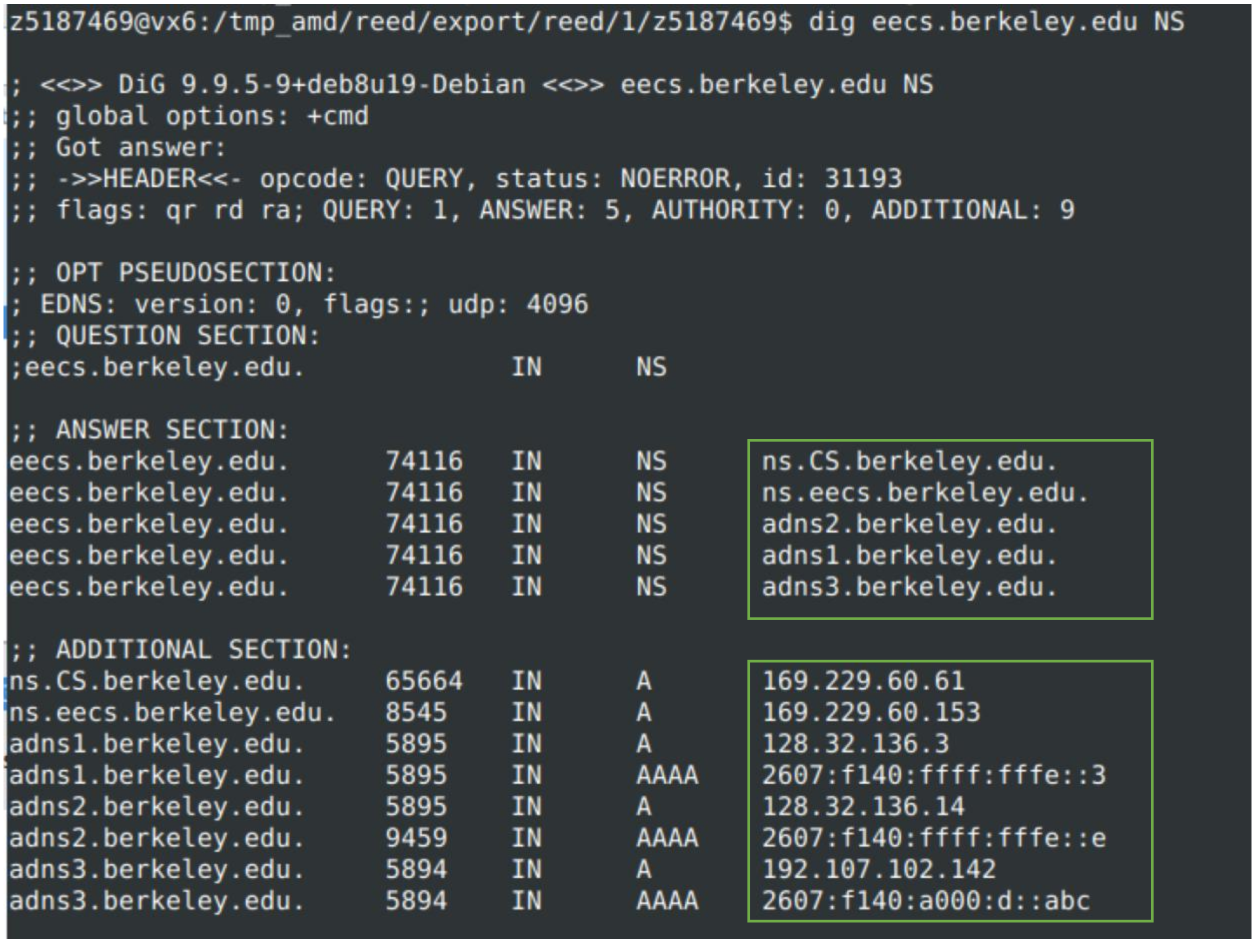
```
;; AUTHORITY SECTION:
edge.pantheon.io.       300     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       300     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       300     IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       300     IN      NS      ns-1213.awsdns-23.org.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   152293  IN      A       205.251.192.233
ns-644.awsdns-16.net.   96377   IN      A       205.251.194.132
ns-644.awsdns-16.net.   96165   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  152374  IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 76943  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 76943  IN      AAAA    2600:9000:5307:dd00::1

;; Query time: 11 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Jun 29 17:16:47 AEST 2020
;; MSG SIZE  rcvd: 397
```

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

The IP address of the local nameserver for my machine is 129.94.242.2.

Question 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?

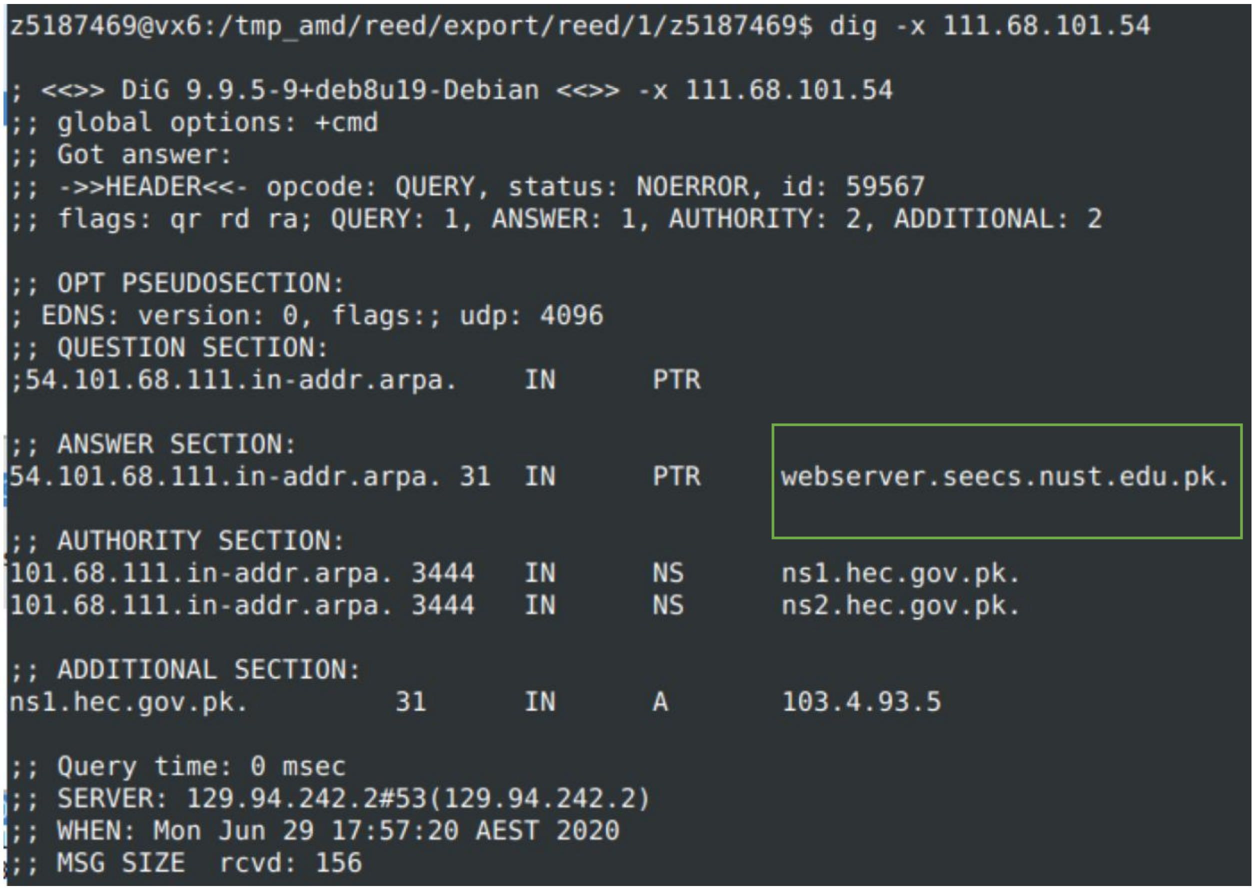
We have 5 DNS nameservers and the first two only have IPv4 address and last three have IPv4 and IPv6 address as highlighted. NS record is sent.



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ dig eecs.berkeley.edu NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> eecs.berkeley.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31193
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 9

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

;; ANSWER SECTION:
eecs.berkeley.edu.      74116   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      74116   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      74116   IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      74116   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      74116   IN      NS      adns3.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     65664   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   8545    IN      A       169.229.60.153
adns1.berkeley.edu.     5895    IN      A       128.32.136.3
adns1.berkeley.edu.     5895    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     5895    IN      A       128.32.136.14
adns2.berkeley.edu.     9459    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     5894    IN      A       192.107.102.142
adns3.berkeley.edu.     5894    IN      AAAA    2607:f140:a000:d::abc
```

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?

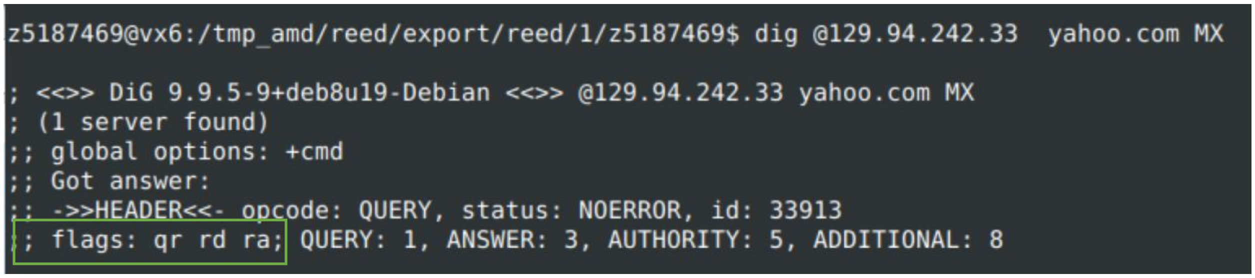
It is DNS Reverse Look-up Using dig -x.



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ 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: 59567
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; 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. 31  IN      PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 3444   IN      NS      ns1.hec.gov.pk.
101.68.111.in-addr.arpa. 3444   IN      NS      ns2.hec.gov.pk.

;; ADDITIONAL SECTION:
ns1.hec.gov.pk.         31      IN      A       103.4.93.5

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Jun 29 17:57:20 AEST 2020
;; MSG SIZE  rcvd: 156
```

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)

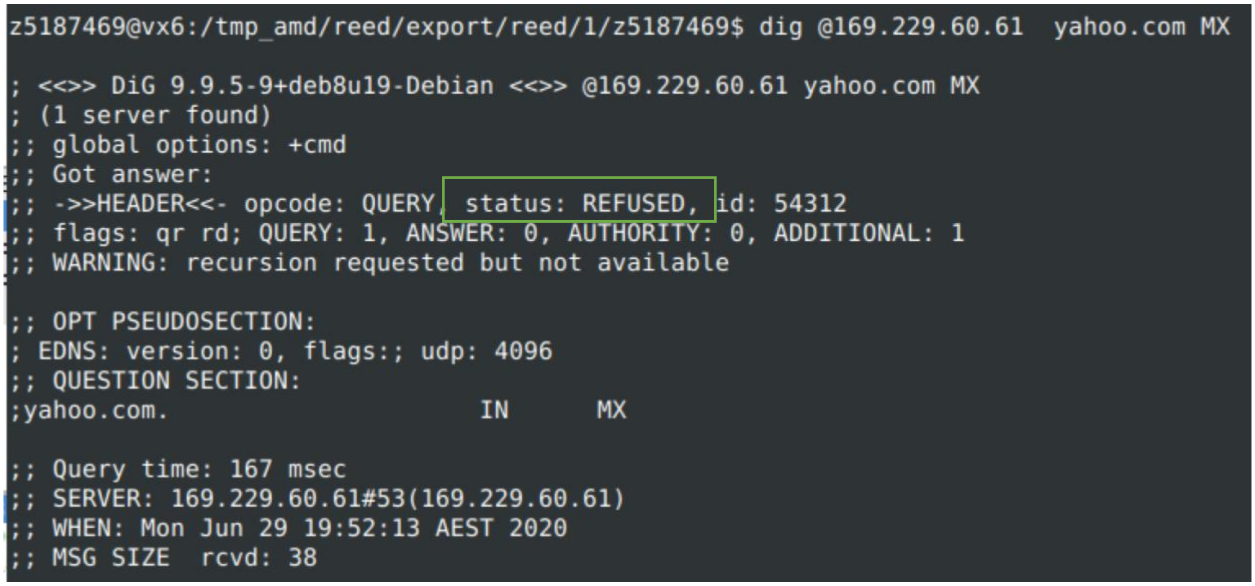
No, there is no aa flag for authoritative answer.



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ dig @129.94.242.33  yahoo.com MX

; <<>> 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: 33913
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8
```

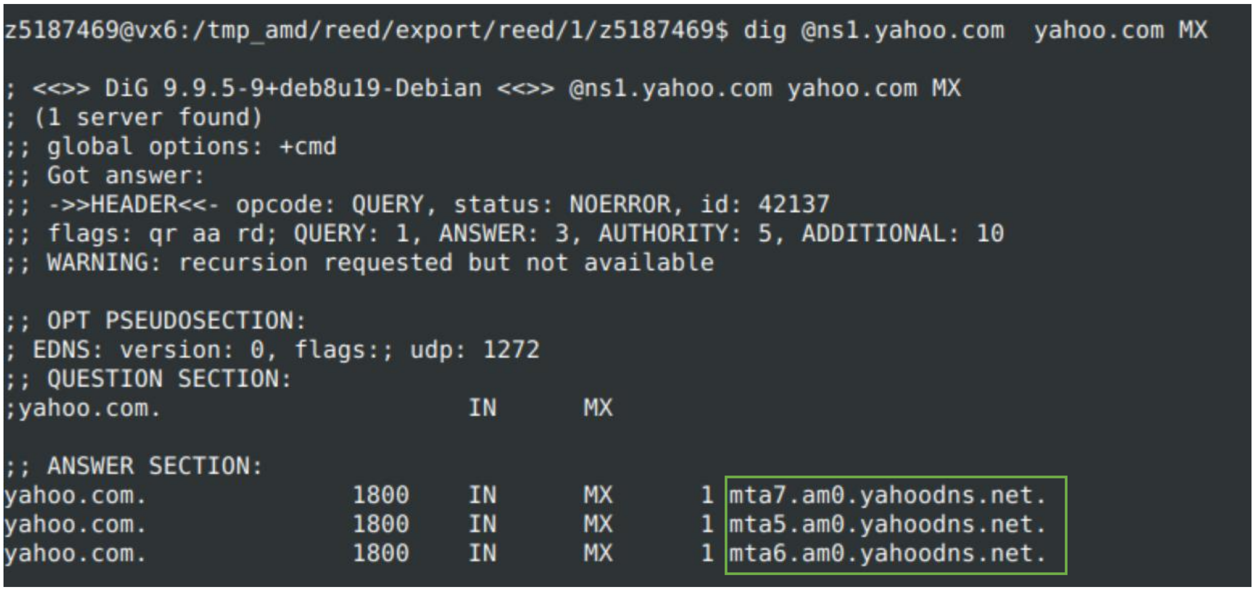
Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?

There is no response as the status is refused. This may be because eecs.berkeley prohibit users performing DNS queries outside its network.



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ dig @169.229.60.61  yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @169.229.60.61 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 54312
;; 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: 169.229.60.61#53(169.229.60.61)
;; WHEN: Mon Jun 29 19:52:13 AEST 2020
;; MSG SIZE  rcvd: 38
```

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



```
z5187469@vx6:/tmp_amd/reed/export/reed/1/z5187469$ 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: 42137
;; 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 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
```

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). 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?

Total 5 requests:

dig NS → a.root-servers.net

dig @198.41.0.4 lyre00.cse.unsw.edu.au → a.au

dig @58.65.254.73 lyre00.cse.unsw.edu.au → q.au

dig @65.22.196.1 lyre00.cse.unsw.edu.au → ns1.unsw.edu.au.

dig @129.94.0.192 lyre00.cse.unsw.edu.au → beethoven.orchestra.cse.unsw.edu.au.

dig @129.94.208.3 lyre00.cse.unsw.edu.au → 129.94.210.20

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

Yes, one physical machine can have several names and IP addresses associated with it.