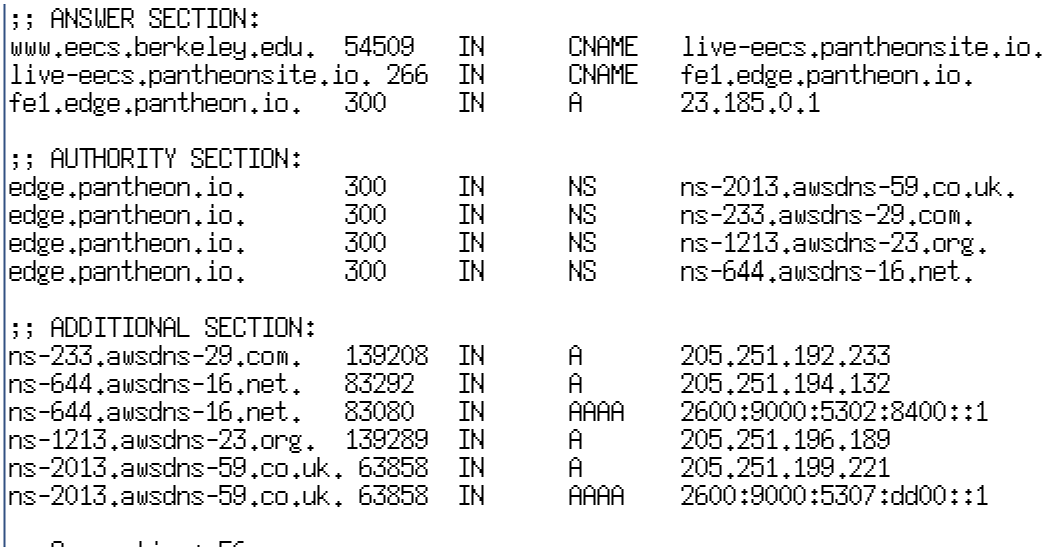
Exercise 3: Digging into DNS (marked, include in the lab report)

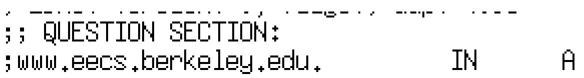
Question 1. What is the IP address of www.eecs.berkeley.edu. What type of DNS query is sent to get this answer?

- The IP address is: 23.185.0.1



```
;; ANSWER SECTION:
www.eecs.berkeley.edu.  54509   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 266  IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   300     IN      A       23.185.0.1

;; 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-233.awsdns-29.com.   139208  IN      A       205.251.192.233
ns-644.awsdns-16.net.   83292   IN      A       205.251.194.132
ns-644.awsdns-16.net.   83080   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  139289  IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 63858  IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 63858  IN      AAAA    2600:9000:5307:dd00::1
```

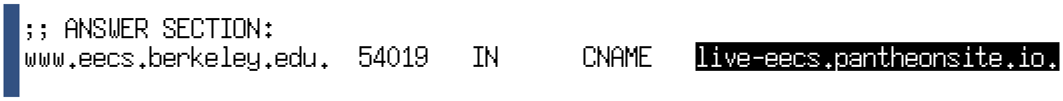
- Query type is ‘A’ -> IPv4 address record. (dig www.eecs.berkeley.edu A)



```
;; QUESTION SECTION:
;www.eecs.berkeley.edu.         IN      A
```

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

- CNAME: live-eecs.pantheonsite.io.



```
;; ANSWER SECTION:
www.eecs.berkeley.edu.  54019   IN      CNAME   live-eecs.pantheonsite.io.
```

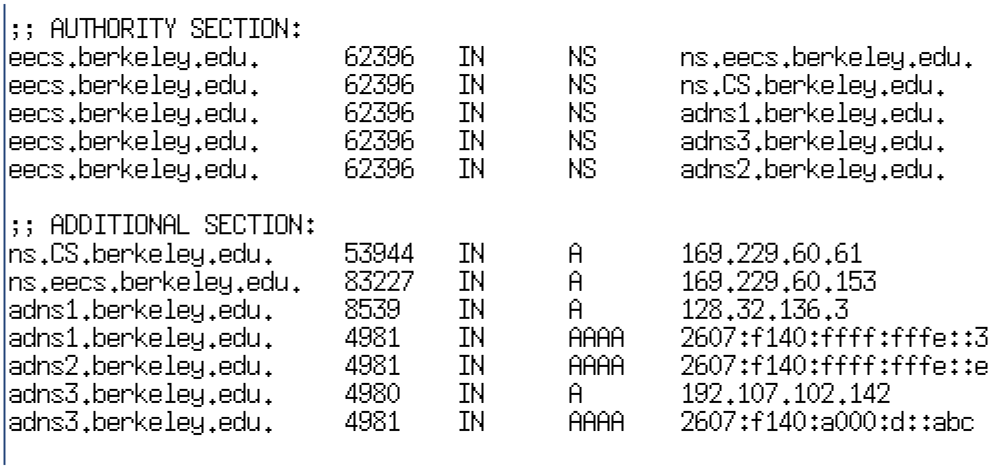
- By command: dig www.eecs.berkeley.edu CNAME

Reason

- We can have multiple sub-domains as CNAME that all point to the same A record. E.g mail.google.com, maps.google.com all point to google.com.
- And if we want to change the IP address of A record then any CNAME record pointing to it will also be changed.

di

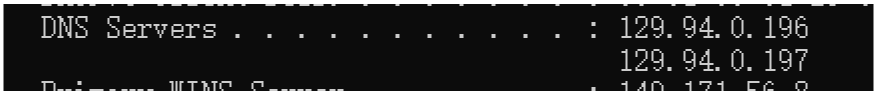
Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?



```
;; AUTHORITY SECTION:
eecs.berkeley.edu.      62396   IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      62396   IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      62396   IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      62396   IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      62396   IN      NS      adns2.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     53944   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   83227   IN      A       169.229.60.153
adns1.berkeley.edu.     8539    IN      A       128.32.136.3
adns1.berkeley.edu.     4981    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     4981    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     4980    IN      A       192.107.102.142
adns3.berkeley.edu.     4981    IN      AAAA    2607:f140:a000:d::abc
```

- In authority section, it tells me what DNS servers can provide me a authority answer for my DNS query
  - In my output, there are 5 name servers
- The additional section typically includes the IP addresses of the DNS servers listed in the authority section

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



```
   DNS Servers . . . . . . . . . . . : 129.94.0.196
                                       129.94.0.197
```

- Found this in windows10 by ipconfig/all

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?

- DNS server: (check with screenshot in question 3)
  - ns.eecs.berkeley.edu. IP = 169.229.60.153
  - adns1.berkeley.edu. IP = 128.32.136.3
  - ns.CS.berkeley.edu. IP = 169.229.60.61
  - adns3.berkeley.edu. IP = 192.107.102.142
  - adns2.berkeley.edu. IP = 128.32.136.14
- dig eecs.berkeley.edu NS
- query type :NS - Name server record type

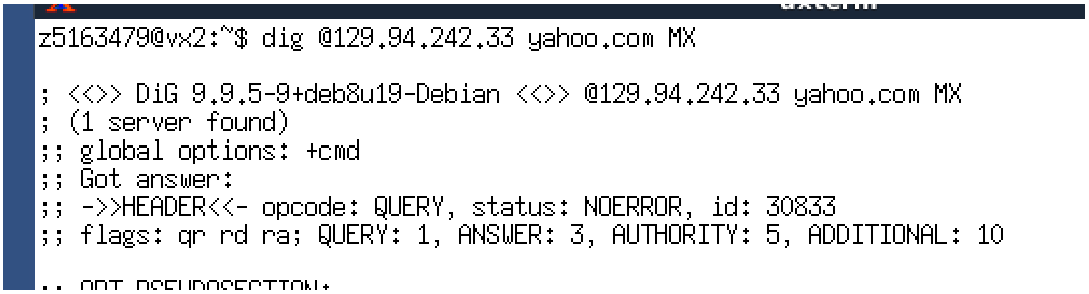
di

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?

- webserver.seecs.nust.edu.pk.
- dig -x 111.68.101.54 +short

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)

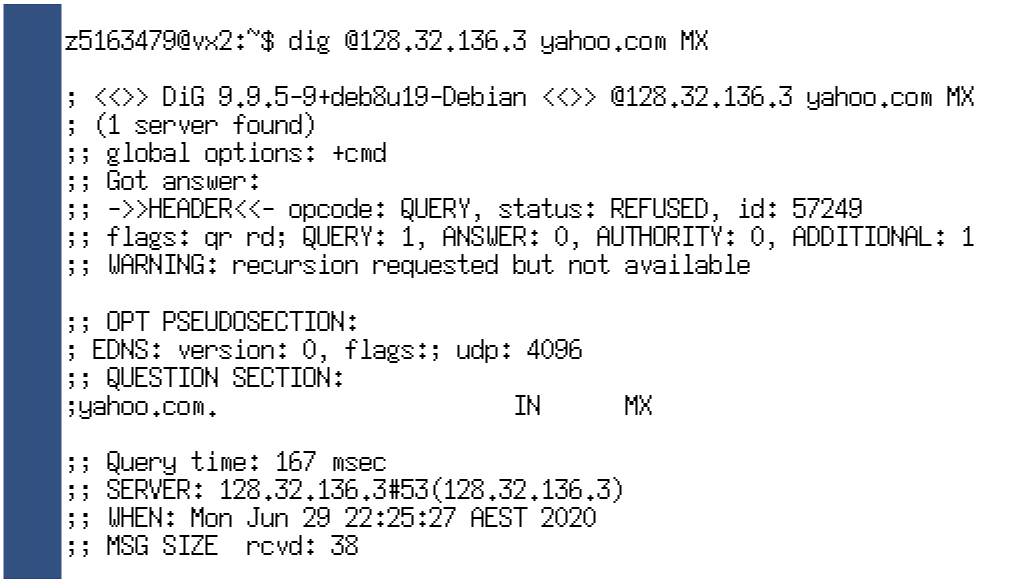
- even the response contains authority section, but there is no authoritative answer
- since the flags in response message that doesn't have '**AA**'



```
z5163479@vx2:~$ 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: 30833
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
```

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

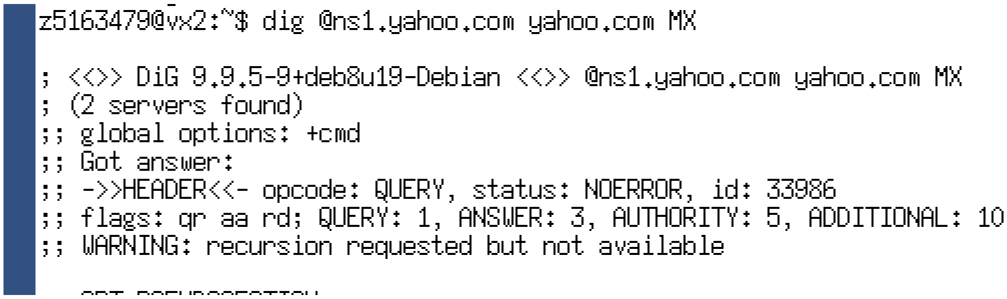
- Still not have an authoritative answer



```
z5163479@vx2:~$ dig @128.32.136.3 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @128.32.136.3 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 57249
;; 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: Mon Jun 29 22:25:27 AEST 2020
;; MSG SIZE  rcvd: 38
```

di

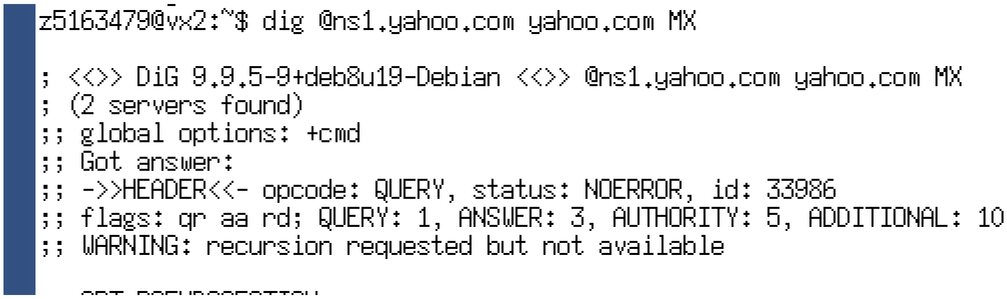
- For get an authoritative answer, I will use a yahoo authoritative name server, which is ns1.yahoo.com
- The result I got is:



```
z5163479@vx2:~$ dig @ns1.yahoo.com yahoo.com MX

; <<>> 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: 33986
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available
```

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

- ‘dig @ns1.yahoo.com yahoo.com MX’
- Query the domain with yahoo’s authoritative name server + Mail exchange record type

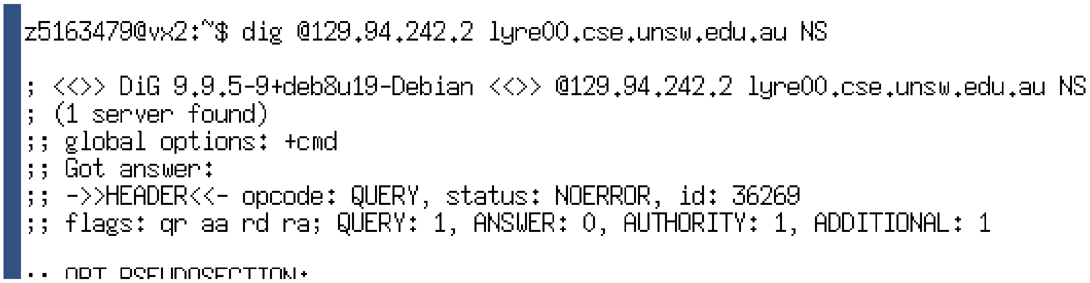


```
z5163479@vx2:~$ dig @ns1.yahoo.com yahoo.com MX

; <<>> 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: 33986
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available
```

di

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?

- I used 6 queries
- Which are
  - ‘dig . NS’ -> found 198.41.0.4
  - ‘dig @198.41.0.4 au. NS’ -> found 58.65.254.73
  - ‘dig @58.65.254.73 edu.au NS’ -> found 65.22.196.1
  - ‘dig @65.22.196.1 unsw.edu.au NS’ -> found 129.94.0.192
  - ‘dig @129.94.242.2 lyre00.cse.unsw.edu.au NS’ -> found a authoritative answer



```
z5163479@vx2:~$ dig @129.94.242.2 lyre00.cse.unsw.edu.au NS

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.2 lyre00.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36269
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

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

- Yes, a physical machine can have multiple names and IP addresses associated with it

di

di