Exericse 3:

Question 1: dig www.amazon.com.au A in the answer section to get 108.158.18.170

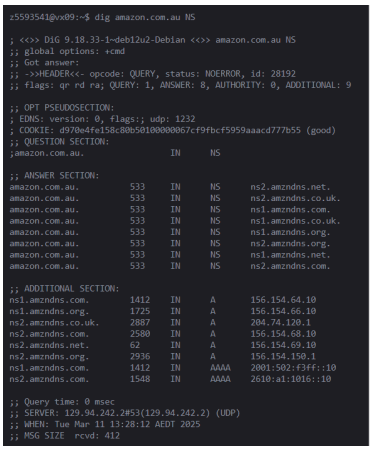
Question 2: tp.04f01a85e-frontier.amazon.com.au. A canonical name is used so users can type www.amazon.com.au or directly amazon.com.au to properly direct the subdomains content

Question 3: EDNS:
Extention Mechanism for DNS is used for expanding the size of UDP packets due to limits in the existing DNS protocol, udp 1232
COOKIE: Cookie is a security feature containing a key 9446c6984643314c0100000067d97b8152f8c1194ded1a77 for example which is sent to a server then sent back to the client. In later queries the client will include to cookies to verify. Good in the response basically means verified.

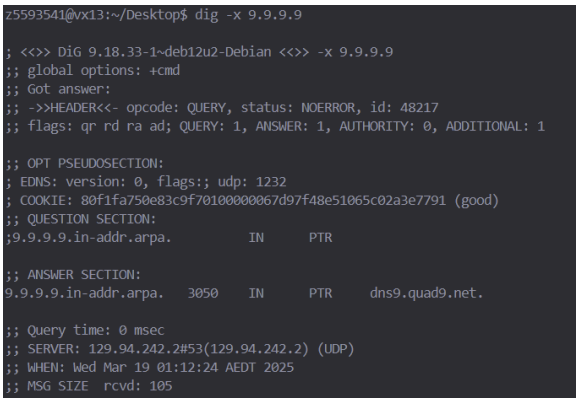
Question 4: The ip address of the local nameserver is 129.94.242.2#53

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

Question 5:

Using dig amazon.com.au NS The dns nameservers are in the answer section in the image. ns2.amzndns.net for example	

Question 6:

You would use dig -x 9.9.9.9: to find the DNS name, The name is dns9.quad9.net.	

Question 7:

I did not get an authoritative answer, There is not flag aa, therefore there was no authoritative answer provided. CSE server does not have authority over yahoo

```
z5593541@vx09:~$ dig yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14884
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 20d8bbeb7f842f1a0100000067cf9e9305a8bc70f37dcef9 (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1001    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1001    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1001    IN      MX      1 mta7.am0.yahoodns.net.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 11 13:23:15 AEDT 2025
;; MSG SIZE  rcvd: 145
```

Question 8:

From one of the nameservers in q5, you get the response REFUSED with a warning. This is because amazon does not host yahoo's records and therefore does not have authority.

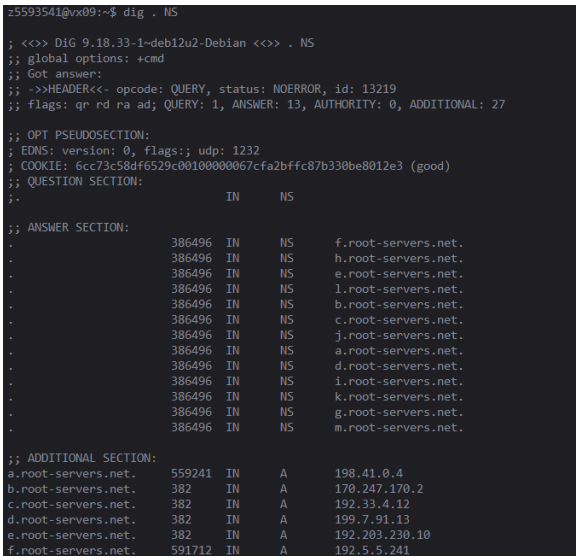
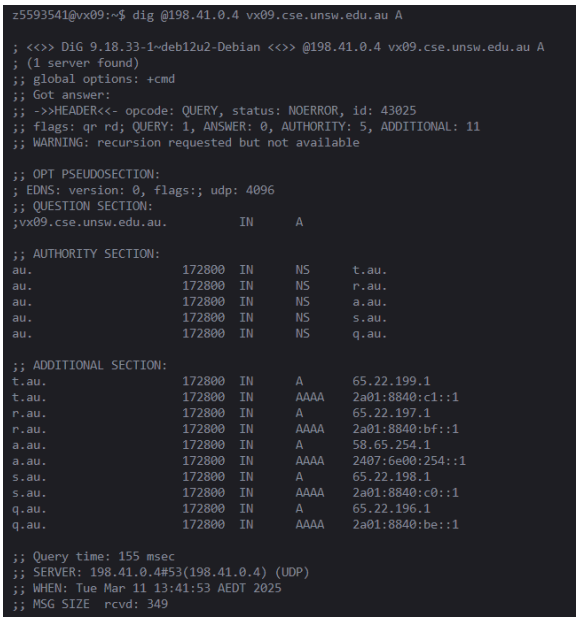
```
z5593541@vx09:~$ dig @156.154.64.10 yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @156.154.64.10 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 36630
;; 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
; EDE: 20 (Not Authoritative)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 0 msec
;; SERVER: 156.154.64.10#53(156.154.64.10) (UDP)
;; WHEN: Tue Mar 11 13:30:44 AEDT 2025
;; MSG SIZE  rcvd: 44
```

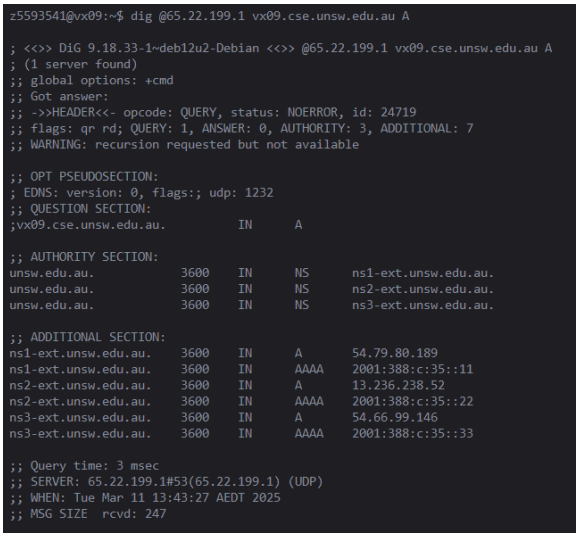
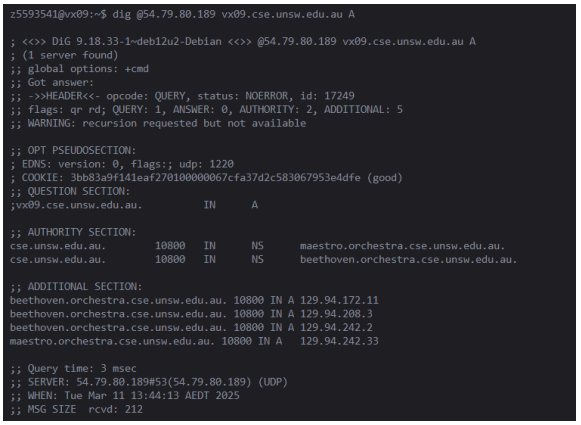
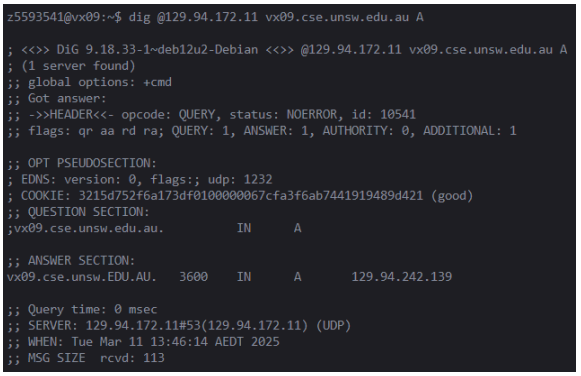
Question 9:

You would use the dns query dig @68.180.131.16 yahoo.com MX to obtain Yahoo's authoritative nameservers. Returning mta6.am0.yahoodns.net and 2 more etc.

```
z5593541@vx09:~$ dig @68.180.131.16 yahoo.com MX

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> @68.180.131.16 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23139
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
; COOKIE: a21629d8f5957d9b19fc32f267cfa0d567192c663860eb1b (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.

;; Query time: 155 msec
;; SERVER: 68.180.131.16#53(68.180.131.16) (UDP)
;; WHEN: Tue Mar 11 13:32:53 AEDT 2025
;; MSG SIZE  rcvd: 145
```

Question 10:

dig . NS to get 198.41.0.4	
dig @198.41.0.4 vx09.cse.unsw.edu.au A to get the address records to find 65.22.199.1	

dig @65.22.199.1 vx09.cse.unsw.edu.au A to find 54.79.80.189	
dig @54.79.80.189 vx09.cse.unsw.edu.au A to find 129.94.172.11	
dig @129.94.172.11 vx09.cse.unsw.edu.au A to get 129.94.242.139. The flag aa stand for authoritative address therefore we found the authoritative nameserver. Therefore 5 dns servers were queried to find the authoritative answer.	

Question 11: One physical machine can have several names and/or IP addresses associated with it, for example multiple aliases or CNAMEs that all point to one server. A machine could also have Ip aliases one for internal or external or ipv4 and ipv6