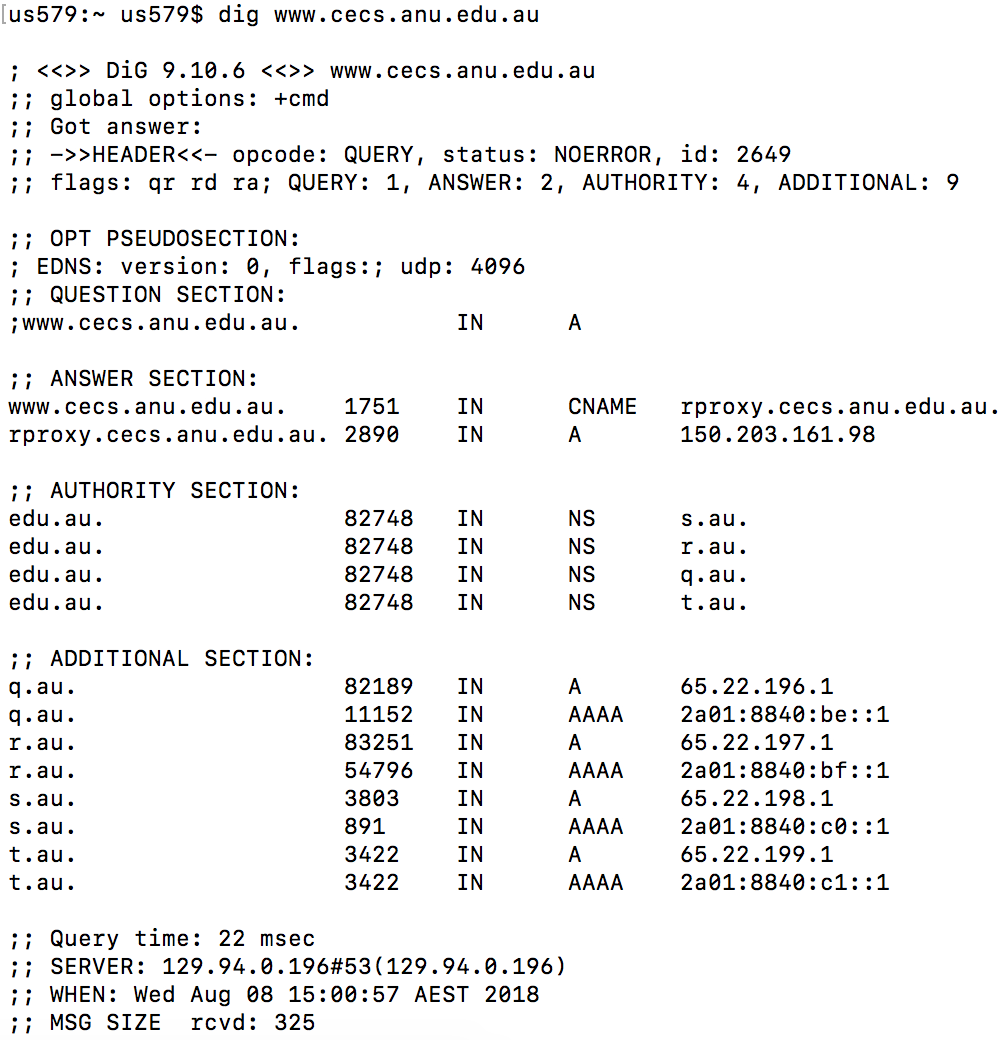
**Exercise 3: Digging into DNS**

Question 1. What is the IP address of [www.cecs.anu.edu.au](http://www.cse.unsw.edu.au/). What type of DNS query is sent to get this answer?



IP Address: 150.203.161.98

It’s a type A Standard Query

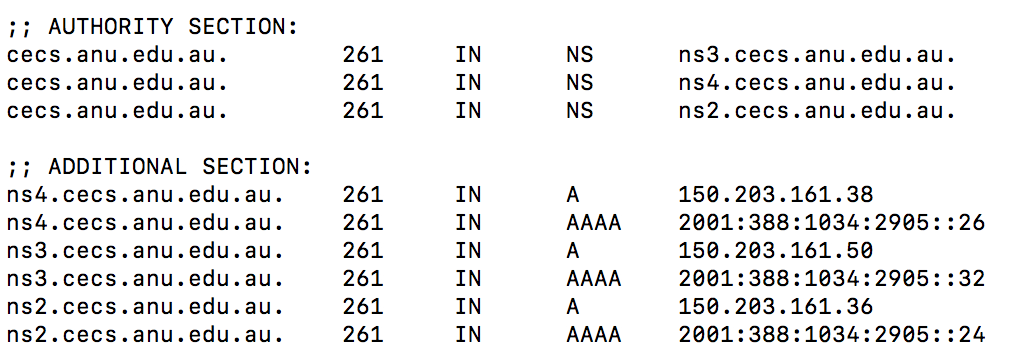
Question 2. What is the canonical name for the CECS ANU web server? What is its IP address? Suggest a reason for having an alias for this server.

Canonical Name: rproxy.cecs.anu.edu.au

IP Address: 150.203.161.98

It is easy for client accessing the web

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



In the authority section, it tells us what DNS servers can provide an authoritative answer to my Quary.

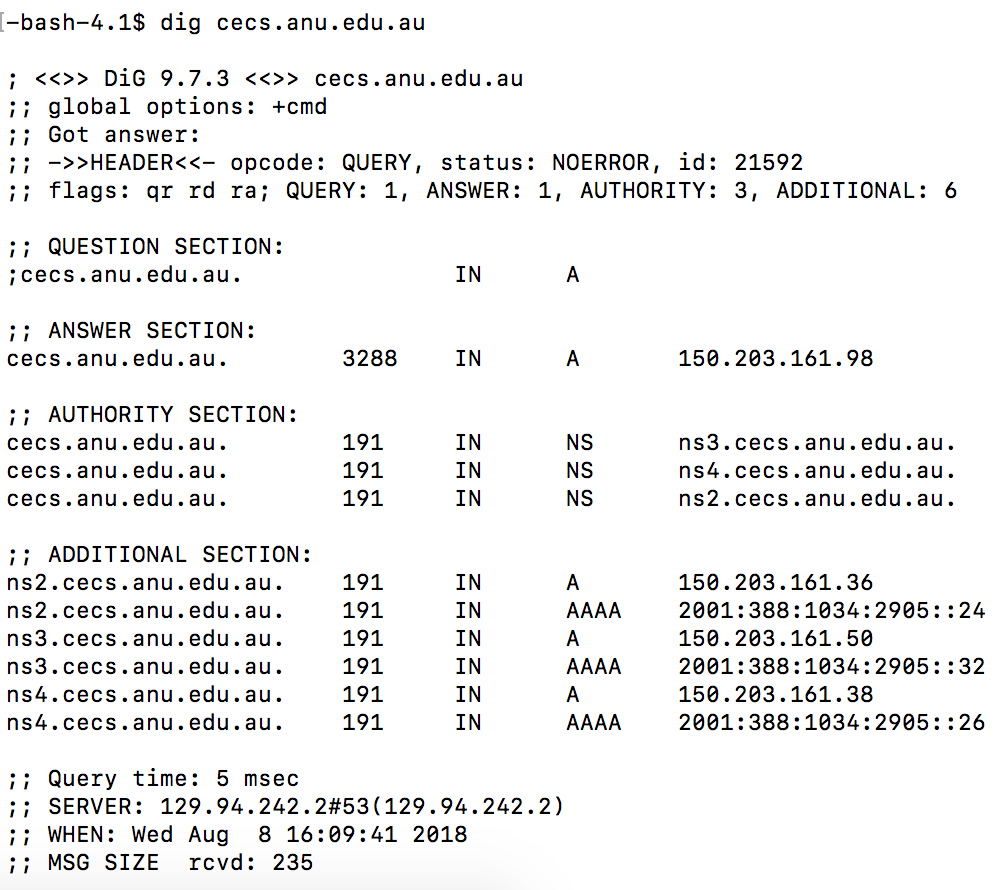
In the additional section ,it is simply shows the IP address of DNS servers in the authority section.

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

;; SERVER: 129.94.242.2#53(129.94.242.2)

The local IP address is 129.94.242.2

Question 5. What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and not [www.cecs.anu.edu.au](http://www.cse.unsw.edu.au/))? Find out their IP addresses? What type of DNS query is sent to obtain this information?



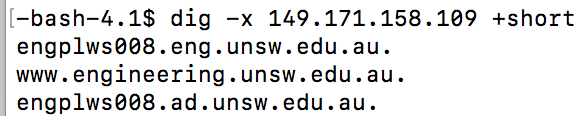
There are:

ns2.cecs.anu.edu.au. IP = 150.203.161.36

ns3.cecs.anu.edu.au. IP = 150.203.161.50

ns4.cecs.anu.edu.au. IP = 150.203.161.38

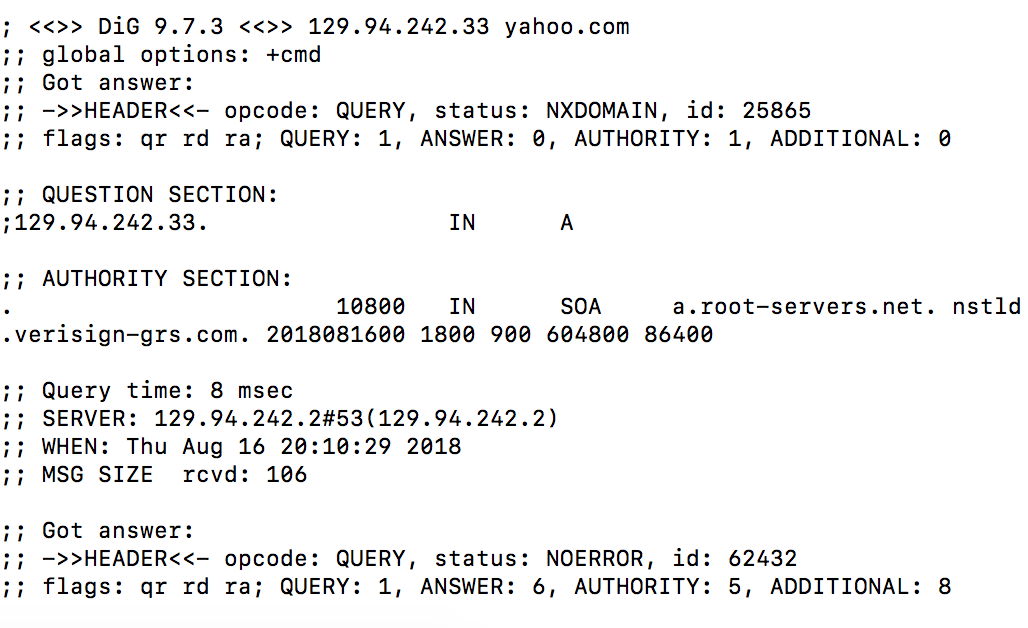
It’s a type NS Standard Query

Question 6. What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?



DNS Name: [www.engineering.unsw.edu.au](http://www.engineering.unsw.edu.au)

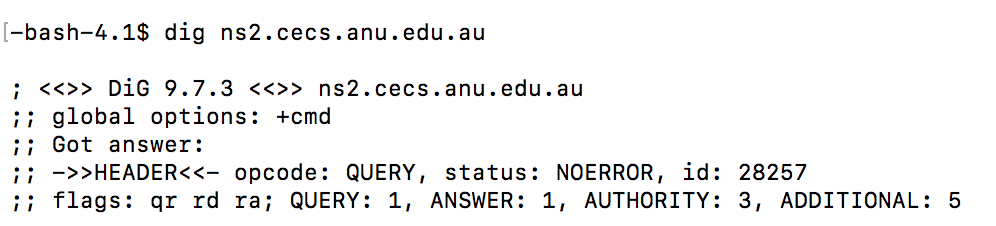
It’s a type PTR Standard Query

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](http://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 NOT an authoritative answer.

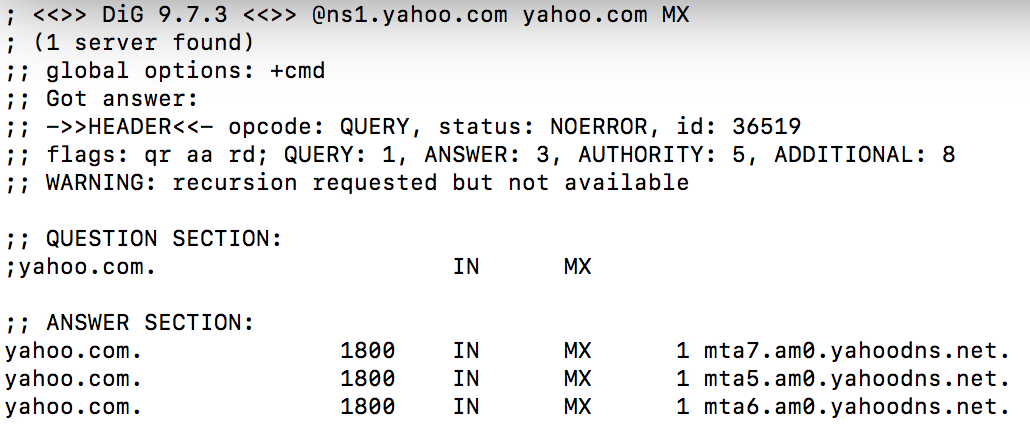
In the flags line of the DNS response message, there is no “AA” or Authoritative Answer flag.

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 NOT an authoritative answer,as flags still not contain an’AA’.

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



I queried yahoo’s Authoritative Name Server with the domain name with MX(Mail exchange) type.

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?

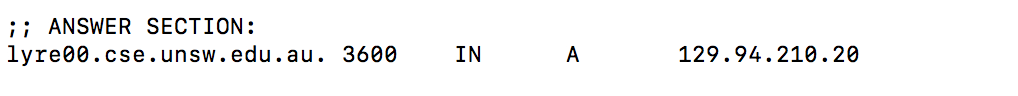
QUERY 1: dig @198.41.0.4 lyre00.cse.unsw.edu.au au. NS

QUERY 2: dig @58.65.254.73 lyre00.cse.unsw.edu.au edu.au. NS

QUERY 3: dig @65.22.199.1 lyre00.cse.unsw.edu.au unsw.edu.au. NS

QUERY 4: dig @129.94.0.192 lyre00.cse.unsw.edu.au cse.unsw.edu.au. NS

QUERY 5: dig @129.94.172.11 lyre00.cse.unsw.edu.au A



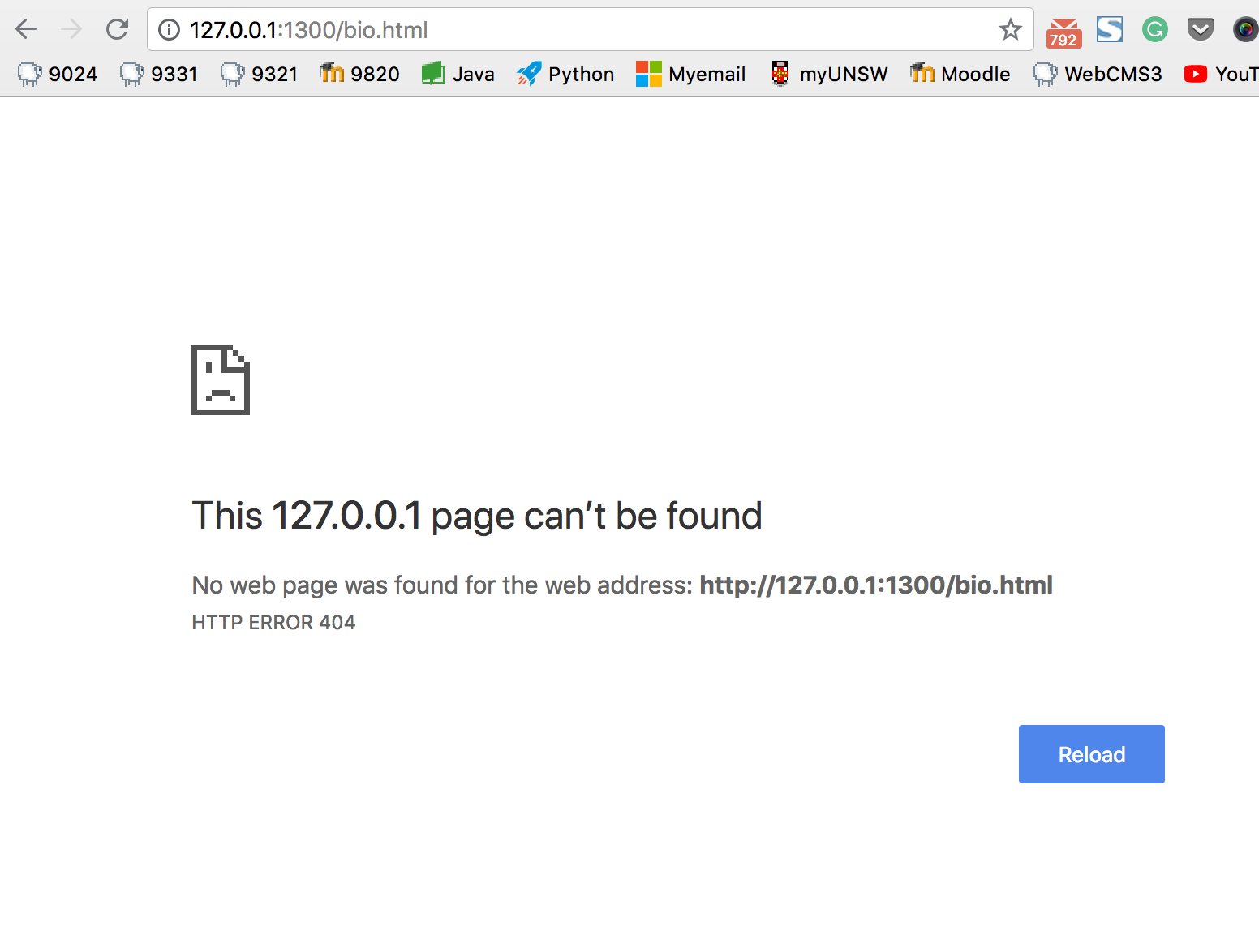
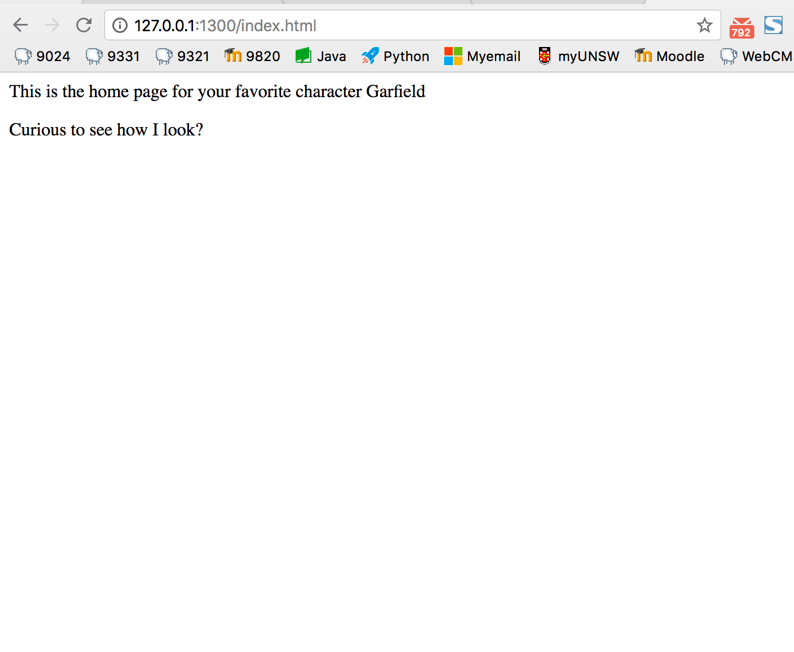
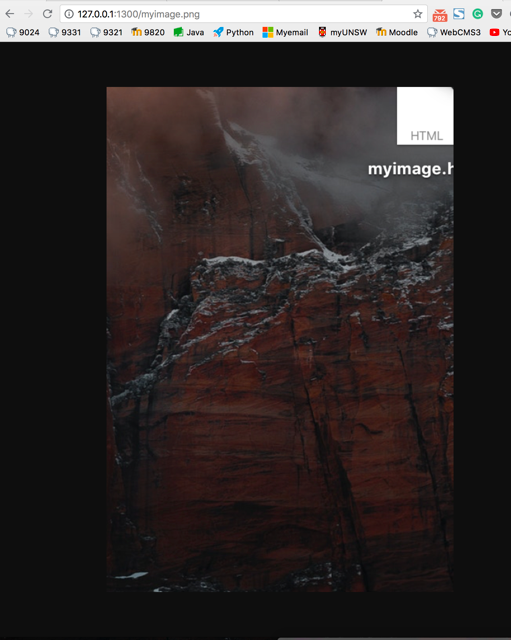
The IP of my mechine is 129.94.210.20

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

An IP address may associated with several names that known as “aliases”.

**(\*) Exercise 4: A Simple Web Server**



For this exercise, I use python and the code is below: