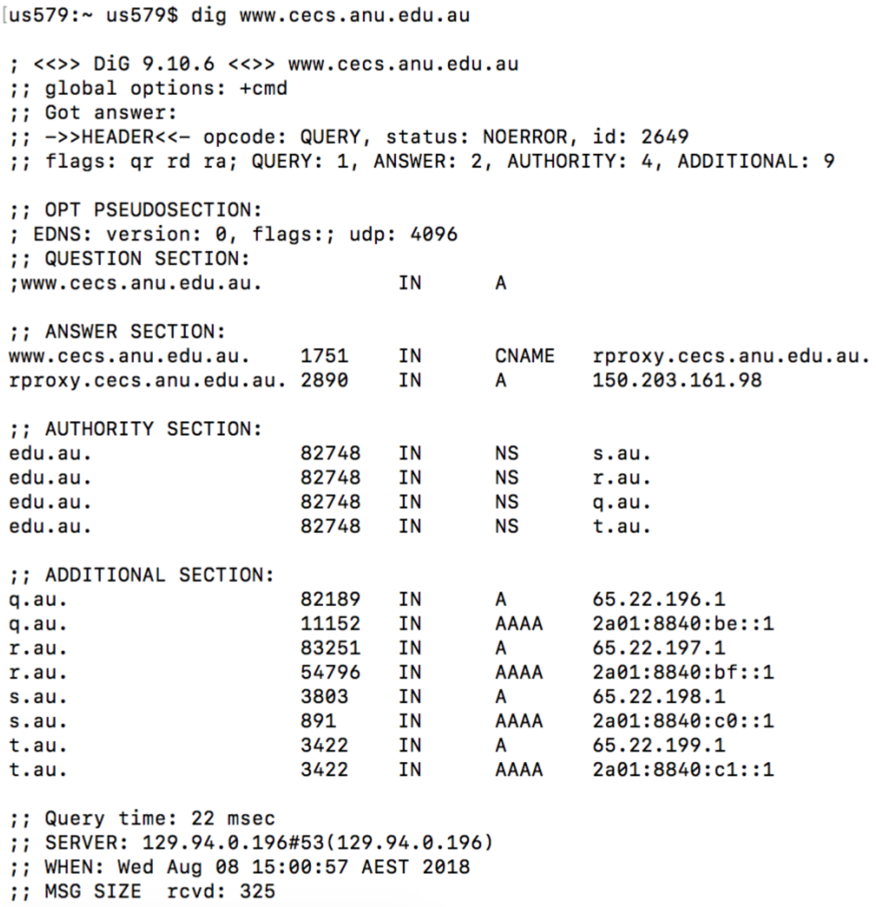
Exercise 3: Digging into DNS

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



```
us579:~ us579$ dig www.cecs.anu.edu.au

; <<>> DiG 9.10.6 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2649
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1751    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 2890    IN      A       150.203.161.98

;; AUTHORITY SECTION:
edu.au.                 82748   IN      NS      s.au.
edu.au.                 82748   IN      NS      r.au.
edu.au.                 82748   IN      NS      q.au.
edu.au.                 82748   IN      NS      t.au.

;; ADDITIONAL SECTION:
q.au.                   82189   IN      A       65.22.196.1
q.au.                   11152   IN      AAAA    2a01:8840:be::1
r.au.                   83251   IN      A       65.22.197.1
r.au.                   54796   IN      AAAA    2a01:8840:bf::1
s.au.                   3803    IN      A       65.22.198.1
s.au.                   891     IN      AAAA    2a01:8840:c0::1
t.au.                   3422    IN      A       65.22.199.1
t.au.                   3422    IN      AAAA    2a01:8840:c1::1

;; Query time: 22 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Wed Aug 08 15:00:57 AEST 2018
;; MSG SIZE  rcvd: 325
```

IP Address: 150.203.161.98

It's a type A Standard Query

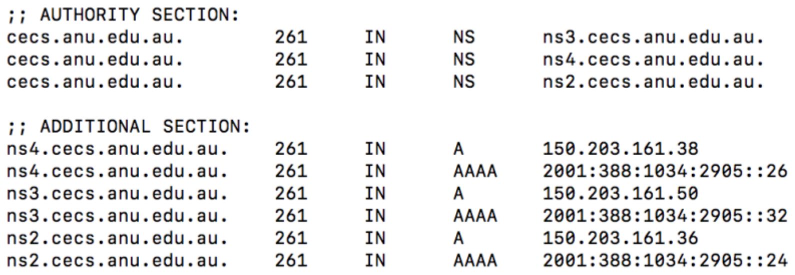
Question 2. What is the canonical name for the CECS ANU web server? What is its IP address? Suggest a reason for having an alias for this server.

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)?



```
;; AUTHORITY SECTION:
cecs.anu.edu.au.        261     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        261     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        261     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns4.cecs.anu.edu.au.    261     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    261     IN      AAAA    2001:388:1034:2905::26
ns3.cecs.anu.edu.au.    261     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    261     IN      AAAA    2001:388:1034:2905::32
ns2.cecs.anu.edu.au.    261     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    261     IN      AAAA    2001:388:1034:2905::24
```

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

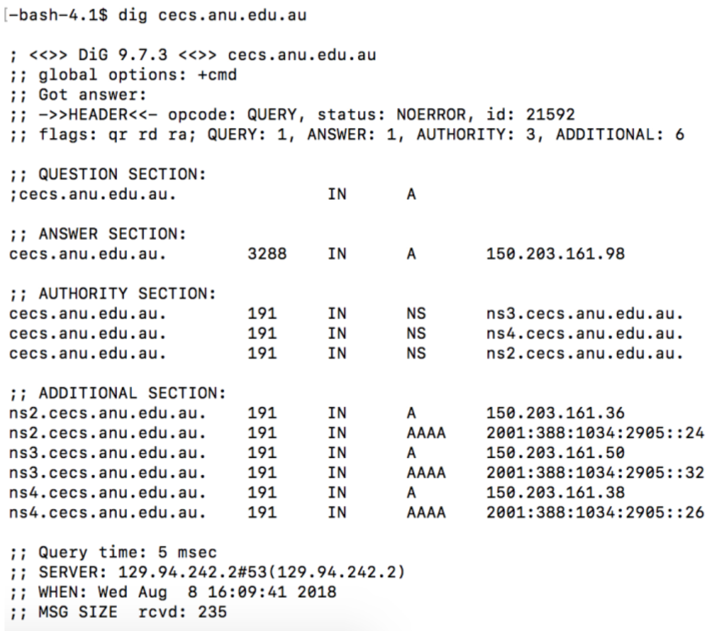
In the additional section ,it is simply shows the IP address of DNS servers in the authority section.

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)? Find out their IP addresses? What type of DNS query is sent to obtain this information?



```
-bash-4.1$ dig cecs.anu.edu.au

; <<>> DiG 9.7.3 <<>> cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21592
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;cecs.anu.edu.au.               IN      A

;; ANSWER SECTION:
cecs.anu.edu.au.        3288    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        191     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        191     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        191     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    191     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    191     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    191     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    191     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    191     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    191     IN      AAAA    2001:388:1034:2905::26

;; Query time: 5 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Aug  8 16:09:41 2018
;; MSG SIZE  rcvd: 235
```

There are:

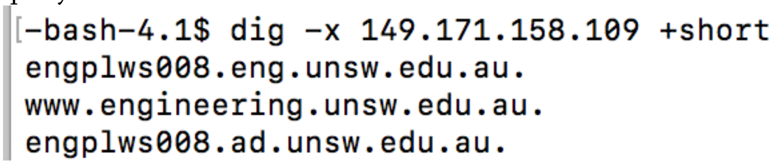
ns2.cecs.anu.edu.au.   IP = 150.203.161.36

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

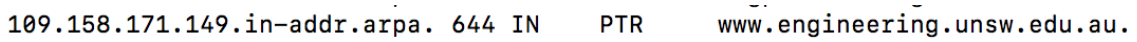
ns4.cecs.anu.edu.au.   IP = 150.203.161.38

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?



```
[-bash-4.1$ dig -x 149.171.158.109 +short
engplws008.eng.unsw.edu.au.
www.engineering.unsw.edu.au.
engplws008.ad.unsw.edu.au.
```

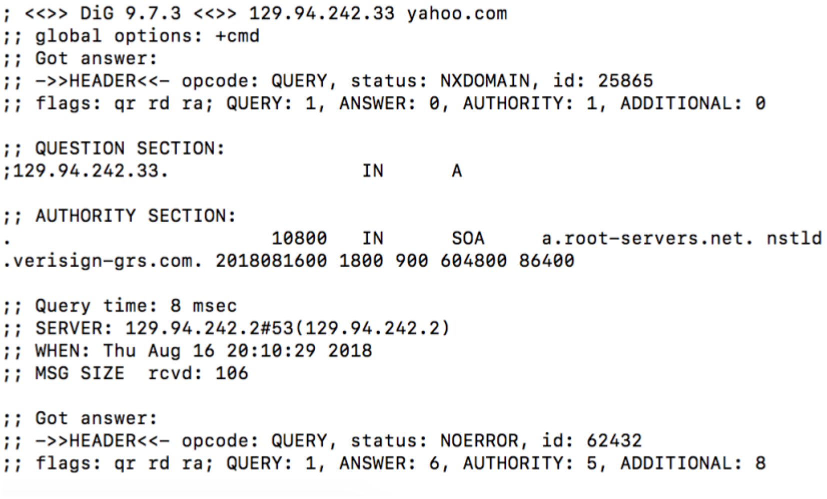


```
109.158.171.149.in-addr.arpa. 644 IN    PTR     www.engineering.unsw.edu.au.
```

DNS Name: 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). 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)

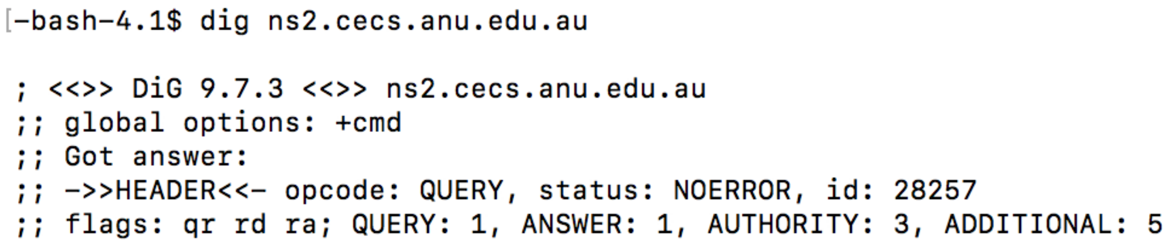


```
; <<>> DiG 9.7.3 <<>> 129.94.242.33 yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 25865
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;129.94.242.33.                 IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld
.verisign-grs.com. 2018081600 1800 900 604800 86400

;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Thu Aug 16 20:10:29 2018
;; MSG SIZE  rcvd: 106

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62432
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8
```

No there is NOT an authoritative answer.

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

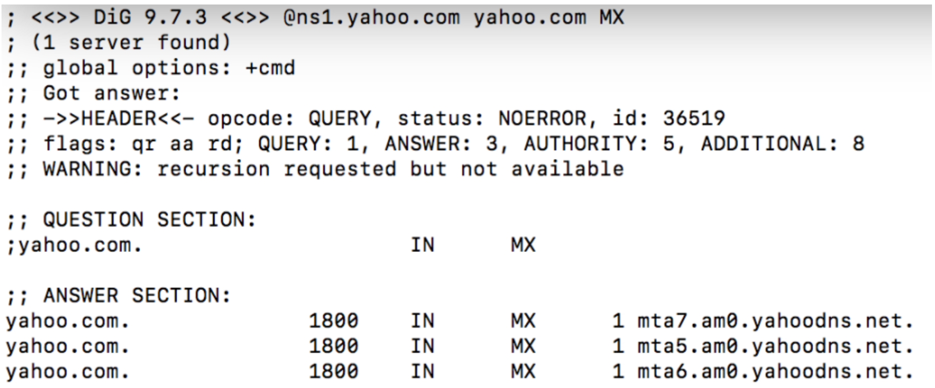
Question 8. Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?



```
[-bash-4.1$ dig ns2.cecs.anu.edu.au

 ; <<>> DiG 9.7.3 <<>> ns2.cecs.anu.edu.au
 ;; global options: +cmd
 ;; Got answer:
 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28257
 ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 5
```

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?



```
; <<>> DiG 9.7.3 <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36519
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; 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.
```

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?

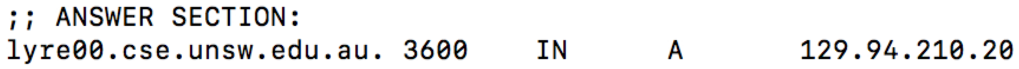
QUERY 1: dig @198.41.0.4 lyre00.cse.unsw.edu.au   au.   NS

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



```
;; ANSWER SECTION:
lyre00.cse.unsw.edu.au. 3600    IN      A       129.94.210.20
```

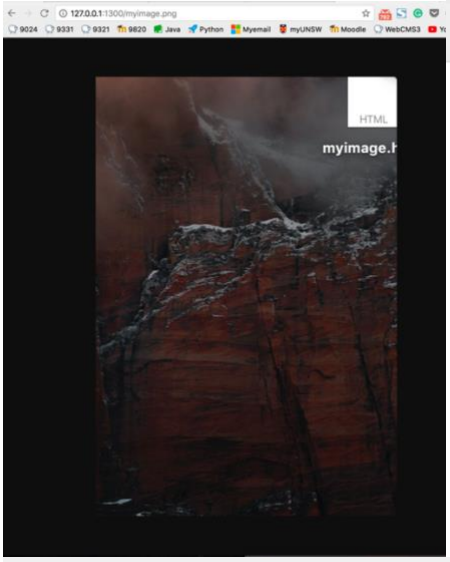
The IP of my mechine is 129.94.210.20

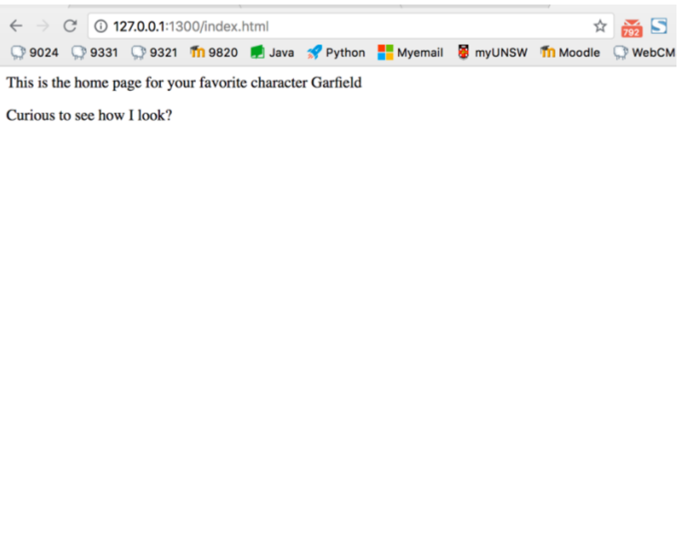
Question 11. Can one physical machine have several names and/or IP addresses associated with it?

Yes, a physical machine can have multiple names and IP addresses

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

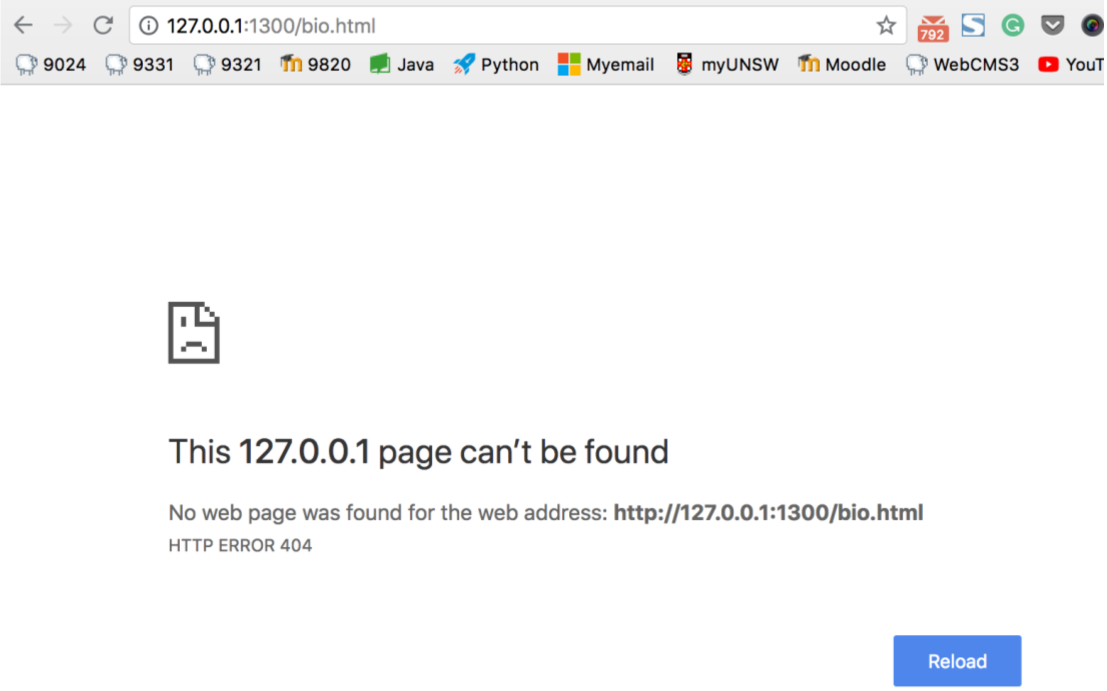
(*) Exercise 4: A Simple Web Server


127.0.0.1:1300/myimage.png
9024 9331 9321 9820 Java Python Myemail myUNSW Moodle WebCMS3
HTML
myimage.h


127.0.0.1:1300/index.html
9024 9331 9321 9820 Java Python Myemail myUNSW Moodle WebCM

This is the home page for your favorite character Garfield

Curious to see how I look?

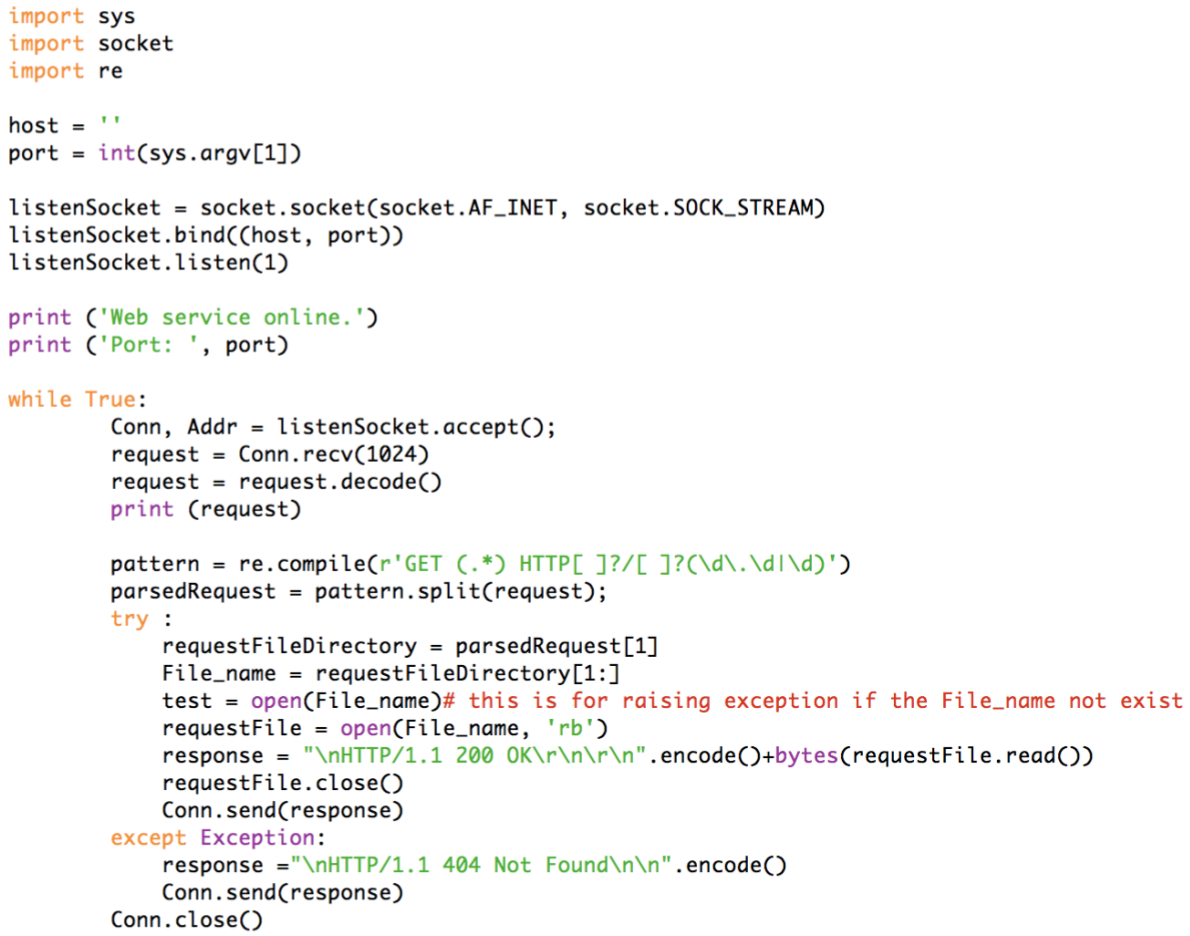

127.0.0.1:1300/bio.html
792
9024 9331 9321 9820 Java Python Myemail myUNSW Moodle WebCMS3 YouT

This 127.0.0.1 page can’t be found

No web page was found for the web address: **http://127.0.0.1:1300/bio.html**

HTTP ERROR 404

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



```python
import sys
import socket
import re

host = ''
port = int(sys.argv[1])

listenSocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listenSocket.bind((host, port))
listenSocket.listen(1)

print ('Web service online.')
print ('Port: ', port)

while True:
        Conn, Addr = listenSocket.accept();
        request = Conn.recv(1024)
        request = request.decode()
        print (request)

        pattern = re.compile(r'GET (.*) HTTP[ ]?/[ ]?(\d\.\d|\d)')
        parsedRequest = pattern.split(request);
        try :
            requestFileDirectory = parsedRequest[1]
            File_name = requestFileDirectory[1:]
            test = open(File_name)# this is for raising exception if the File_name not exist
            requestFile = open(File_name, 'rb')
            response = "\nHTTP/1.1 200 OK\r\n\r\n".encode()+bytes(requestFile.read())
            requestFile.close()
            Conn.send(response)
        except Exception:
            response ="\nHTTP/1.1 404 Not Found\n\n".encode()
            Conn.send(response)
        Conn.close()
```