Exercise 3: Digging into DNS

Question1:

Using the dig command, we can get the IP address of www.eecs.berkeley.edu, which is 23.185.0.1. The query type of this address is type A.

```
;; ANSWER SECTION:
www.eecs.berkeley.edu.  77176   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 9    IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   39      IN      A       23.185.0.1
```

Question2:

From the picture given in question 1. We can find the canonical addresses are live-eecs.pantheonsite.io and fe1.edge.pantheon.io, which is the answer to this question. The reason for using the canonical address is easy for users to remember this address.

Question3:

The AUTHORITY SECTION returns the name lists of servers. All these servers are stored in the DNS record. Furthermore, from the type NS and based on the lecture notes, we can find that these are authoritative DNS servers.

```
;; AUTHORITY SECTION:
edge.pantheon.io.       230     IN      NS      ns-644.awsdns-16.net.
edge.pantheon.io.       230     IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       230     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       230     IN      NS      ns-233.awsdns-29.com.
```

Then, the ADDITIONAL SECTION returns the actual IP address, which you can find as the picture showing below.

```
;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   62236   IN      A       205.251.192.233
ns-233.awsdns-29.com.   164929  IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   57953   IN      A       205.251.194.132
ns-1213.awsdns-23.org.  62670   IN      A       205.251.196.189
ns-2013.awsdns-59.co.uk. 57635  IN      A       205.251.199.221
```

Question4:

The IP address of the local name server is 129.94.242.2.

```
;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Oct 11 19:28:57 AEDT 2020
;; MSG SIZE  rcvd: 369
```

Question5:

From the picture, we can get the names of DNS servers are adns3.berkeley.edu, ns.CS.berkeley.edu, ns.eecs.berkeley.edu, adns1.berkeley.edu, and

adns2.berkeley.edu. The IP address are 192.107.102.142, 169.229.60.61, 169.229.60.153, 128.32.136.3 and 128.32.136.14. Also, from the picture we can get the type query is NS.

```
;; ANSWER SECTION:
eecs.berkeley.edu.      9698    IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      9698    IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      9698    IN      NS      ns.eecs.berkeley.edu.
eecs.berkeley.edu.      9698    IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      9698    IN      NS      adns2.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     58204   IN      A       169.229.60.61
ns.eecs.berkeley.edu.   15743   IN      A       169.229.60.153
adns1.berkeley.edu.     3306    IN      A       128.32.136.3
adns1.berkeley.edu.     3306    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     3306    IN      A       128.32.136.14
adns2.berkeley.edu.     3306    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     3306    IN      A       192.107.102.142
adns3.berkeley.edu.     3306    IN      AAAA    2607:f140:a000:d::abc
```

Question6:

Using the dig command we can get the DNS name of this IP address, 111.68.101.54, which is webserver.seecs.nust.edu.pk. We can also get the DNS query type is PTR from the picture given below.

```
;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 916 IN      PTR     webserver.seecs.nust.edu.pk.
```

Question7:

From the picture, we can get that the response doesn't get an authoritative answer. This is because we cannot find the keyword AA in the flag part.

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @129.94.242.33 yahoo.com -t MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com -t MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54769
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1406    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1406    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1406    IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              53608   IN      NS      ns3.yahoo.com.
yahoo.com.              53608   IN      NS      ns5.yahoo.com.
yahoo.com.              53608   IN      NS      ns2.yahoo.com.
yahoo.com.              53608   IN      NS      ns1.yahoo.com.
yahoo.com.              53608   IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          134948  IN      A       68.180.131.16
ns1.yahoo.com.          63269   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          152375  IN      A       68.142.255.16
ns2.yahoo.com.          75111   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          820     IN      A       27.123.42.42
ns3.yahoo.com.          1314    IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          146810  IN      A       98.138.11.157
ns5.yahoo.com.          11439   IN      A       202.165.97.53
ns5.yahoo.com.          27222   IN      AAAA    2406:2000:ff60::53

;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Oct 11 20:21:26 AEDT 2020
;; MSG SIZE  rcvd: 399
```

Question8:

Based on the result in question 7, I choose ns3.yahoo.com which IP address is 27.123.42.42. We can easily find an AA flag in ns3.tahoo.com, which means this response is an authoritative answer.

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @27.123.42.42  yahoo.com -t MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @27.123.42.42 yahoo.com -t MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6986
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; WARNING: recursion requested but not available
```

Question9:
Based on the result of question7 and question 8, we can find the query type is MX, which is the answer to this question.

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @27.123.42.42  yahoo.com -t MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @27.123.42.42 yahoo.com -t MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6986
;; 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 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.


z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @129.94.242.33 yahoo.com -t MX

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com -t MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54769
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1406    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1406    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1406    IN      MX      1 mta6.am0.yahoodns.net.
```

Question10:

Using the dig command to check whether the flag is AA. Based on the lecture notes of DNS, we should check each layer to find out the result.

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig . -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> . -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35989
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

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

;; ANSWER SECTION:
.                       51431   IN      NS      c.root-servers.net.
.                       51431   IN      NS      l.root-servers.net.
.                       51431   IN      NS      i.root-servers.net.
.                       51431   IN      NS      d.root-servers.net.
.                       51431   IN      NS      e.root-servers.net.
.                       51431   IN      NS      a.root-servers.net.
.                       51431   IN      NS      m.root-servers.net.
.                       51431   IN      NS      h.root-servers.net.
.                       51431   IN      NS      g.root-servers.net.
.                       51431   IN      NS      j.root-servers.net.
.                       51431   IN      NS      b.root-servers.net.
.                       51431   IN      NS      f.root-servers.net.
.                       51431   IN      NS      k.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     141838  IN      A       198.41.0.4
a.root-servers.net.     246637  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     255752  IN      A       199.9.14.201
b.root-servers.net.     81353   IN      AAAA    2001:500:200::b
c.root-servers.net.     91767   IN      A       192.33.4.12
c.root-servers.net.     91767   IN      AAAA    2001:500:2::c
d.root-servers.net.     91767   IN      A       199.7.91.13
d.root-servers.net.     91767   IN      AAAA    2001:500:2d::d
e.root-servers.net.     346944  IN      A       192.203.230.10
e.root-servers.net.     238223  IN      AAAA    2001:500:a8::e
f.root-servers.net.     309385  IN      A       192.5.5.241
f.root-servers.net.     81353   IN      AAAA    2001:500:2f::f
g.root-servers.net.     174152  IN      A       192.112.36.4
g.root-servers.net.     156243  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     183646  IN      A       198.97.190.53
h.root-servers.net.     589476  IN      AAAA    2001:500:1::53
i.root-servers.net.     157405  IN      A       192.36.148.17
i.root-servers.net.     157405  IN      AAAA    2001:7fe::53
j.root-servers.net.     159271  IN      A       192.58.128.30
j.root-servers.net.     81353   IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     158573  IN      A       193.0.14.129
k.root-servers.net.     328173  IN      AAAA    2001:7fd::1
l.root-servers.net.     221015  IN      A       199.7.83.42
l.root-servers.net.     588243  IN      AAAA    2001:500:9f::42
m.root-servers.net.     213237  IN      A       202.12.27.33
m.root-servers.net.     601632  IN      AAAA    2001:dc3::35

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Oct 11 20:52:44 AEDT 2020
;; MSG SIZE  rcvd: 811
```

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @198.41.0.4 au.  -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @198.41.0.4 au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16843
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 9, ADDITIONAL: 19
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
au.                     172800  IN      NS      m.au.
au.                     172800  IN      NS      d.au.
au.                     172800  IN      NS      q.au.
au.                     172800  IN      NS      t.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      n.au.
au.                     172800  IN      NS      a.au.
au.                     172800  IN      NS      c.au.

;; ADDITIONAL SECTION:
m.au.                   172800  IN      A       156.154.100.24
m.au.                   172800  IN      AAAA    2001:502:2eda::24
d.au.                   172800  IN      A       162.159.25.38
d.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:1926
q.au.                   172800  IN      A       65.22.196.1
q.au.                   172800  IN      AAAA    2a01:8840:be::1
t.au.                   172800  IN      A       65.22.199.1
t.au.                   172800  IN      AAAA    2a01:8840:c1::1
s.au.                   172800  IN      A       65.22.198.1
s.au.                   172800  IN      AAAA    2a01:8840:c0::1
r.au.                   172800  IN      A       65.22.197.1
r.au.                   172800  IN      AAAA    2a01:8840:bf::1
n.au.                   172800  IN      A       156.154.101.24
n.au.                   172800  IN      AAAA    2001:502:ad09::24
a.au.                   172800  IN      A       58.65.254.73
a.au.                   172800  IN      AAAA    2407:6e00:254:306::73
c.au.                   172800  IN      A       162.159.24.179
c.au.                   172800  IN      AAAA    2400:cb00:2049:1::a29f:18b3

;; Query time: 119 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sun Oct 11 20:55:03 AEDT 2020
;; MSG SIZE  rcvd: 571
```

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @58.65.254.73 edu.au. -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @58.65.254.73 edu.au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22919
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
edu.au.                 86400   IN      NS      r.au.
edu.au.                 86400   IN      NS      t.au.
edu.au.                 86400   IN      NS      s.au.
edu.au.                 86400   IN      NS      q.au.

;; ADDITIONAL SECTION:
q.au.                   86400   IN      A       65.22.196.1
r.au.                   86400   IN      A       65.22.197.1
s.au.                   86400   IN      A       65.22.198.1
t.au.                   86400   IN      A       65.22.199.1
q.au.                   86400   IN      AAAA    2a01:8840:be::1
r.au.                   86400   IN      AAAA    2a01:8840:bf::1
s.au.                   86400   IN      AAAA    2a01:8840:c0::1
t.au.                   86400   IN      AAAA    2a01:8840:c1::1

;; Query time: 158 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Sun Oct 11 20:56:56 AEDT 2020
;; MSG SIZE  rcvd: 275
```

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @65.22.196.1 unsw.edu.au. -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @65.22.196.1 unsw.edu.au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22435
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

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

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        900     IN      A       129.94.0.192
ns2.unsw.edu.au.        900     IN      A       129.94.0.193
ns3.unsw.edu.au.        900     IN      A       192.155.82.178
ns1.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        900     IN      AAAA    2001:388:c:35::2

;; Query time: 24 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Sun Oct 11 20:58:08 AEDT 2020
;; MSG SIZE  rcvd: 198

z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @129.94.0.192 cse.unsw.edu.au. -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.0.192 cse.unsw.edu.au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43222
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cse.unsw.edu.au.               IN      NS

;; AUTHORITY SECTION:
cse.unsw.edu.au.        10800   IN      NS      maestro.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        10800   IN      NS      beethoven.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.2
maestro.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.242.33

;; Query time: 3 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Sun Oct 11 20:59:23 AEDT 2020
;; MSG SIZE  rcvd: 164
```

```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @129.94.172.11 lyre00.cse.unsw.edu.au. -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.172.11 lyre00.cse.unsw.edu.au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38009
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lyre00.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
cse.unsw.edu.au.        900     IN      SOA     maestro.orchestra.cse.unsw.edu.au. hostmaster.cse.unsw.edu.au. 2020100101 2000 300 1209600 900

;; Query time: 0 msec
;; SERVER: 129.94.172.11#53(129.94.172.11)
;; WHEN: Sun Oct 11 21:01:03 AEDT 2020
;; MSG SIZE  rcvd: 116
```

Finally, we can find the AA flag in the flag part, which means this response is an authoritative answer.

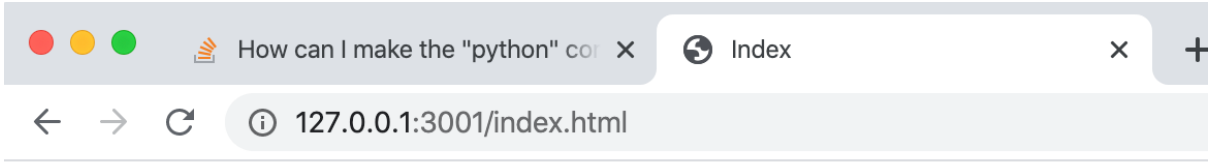
```
z5241868@vx6:/tmp_amd/kamen/export/kamen/5/z5241868$ dig @129.94.172.11 lyre00.cse.unsw.edu.au. -t ns

; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.172.11 lyre00.cse.unsw.edu.au. -t ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38009
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

Question11:
Yes, of course. Consider we can find multiple physical networks in our machine. We can also find one IP address for each network. For example, if our smartphone turns on a personal hotspot, we will have 2 networks with our phone. Each network will have its own IP address.

Exercise 4: result WebServer.py

Local Test:

1. index.html

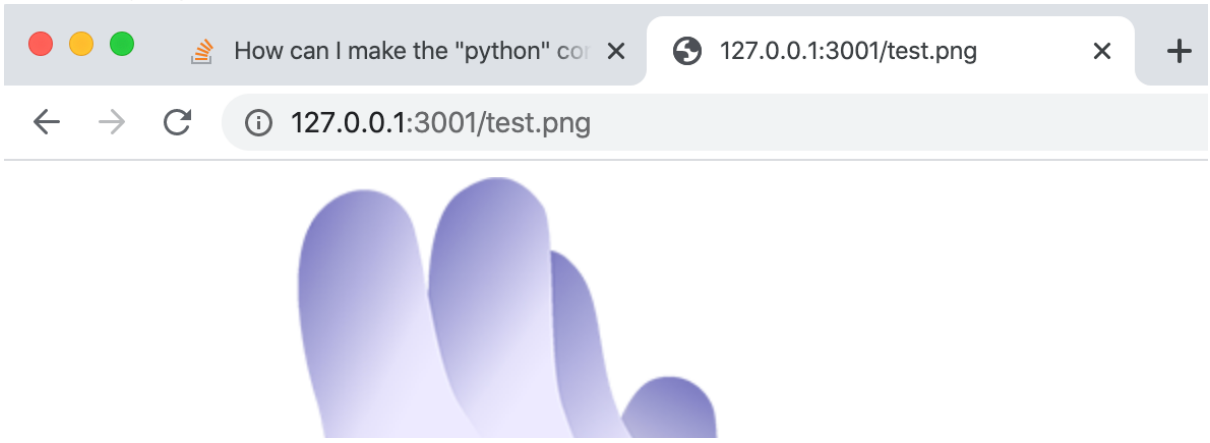


Test Page for Roy's COMP9331 Lab4

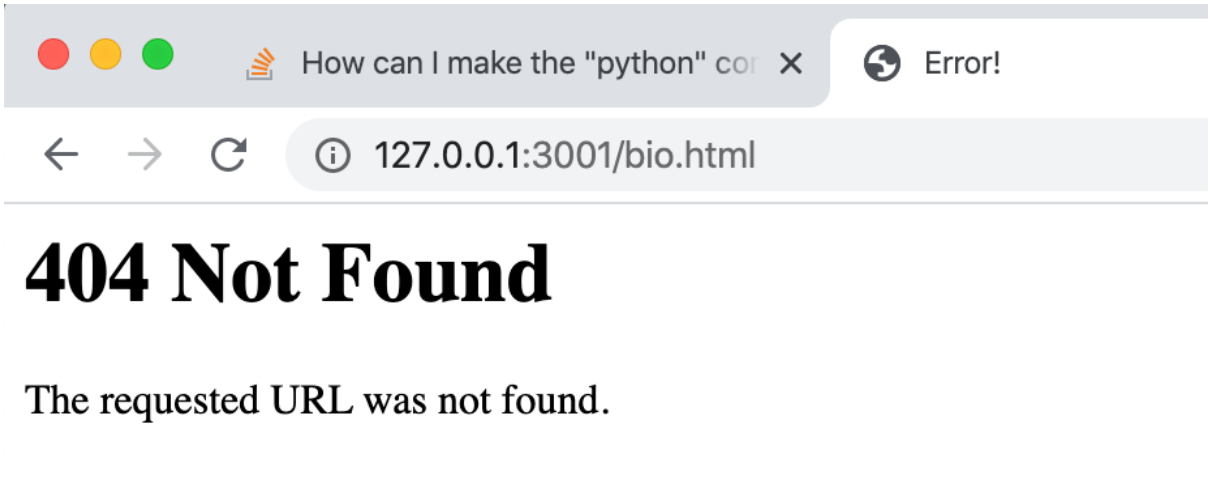
Getting Data successful from WebServer!

Have a nice day!

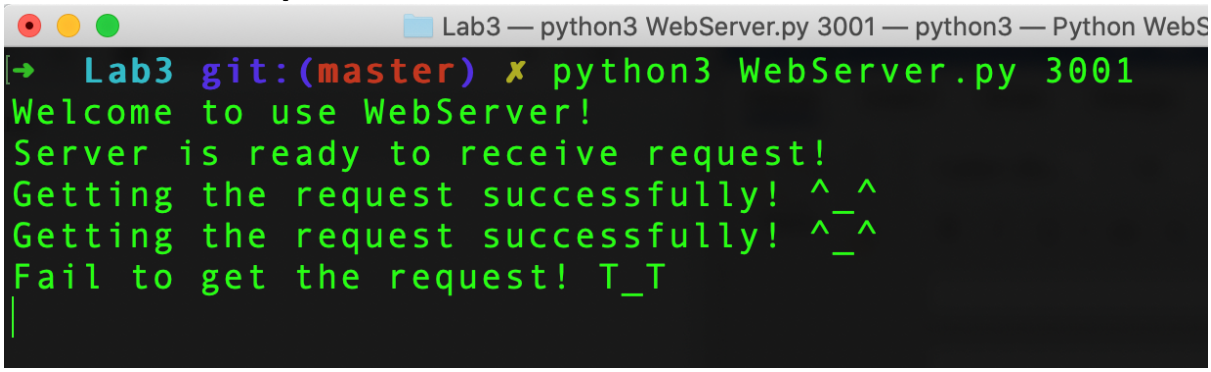
2. test.png



3. bio.html

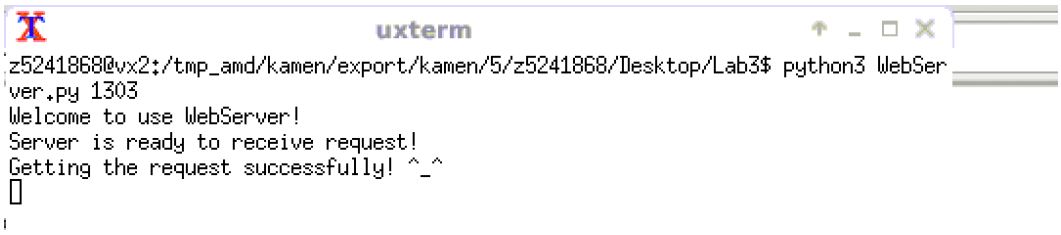


4. Terminal Output



Vlab Test:

Index.html



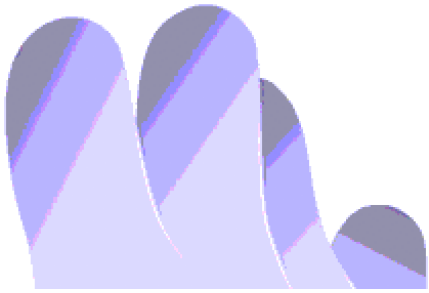
Test.png

```
uxterm
z5241868@vx2:/tmp_amd/kamen/export/kamen/5/z5241868/Desktop/Lab3$ python3 WebSer
ver.py 1303
Welcome to use WebServer!
Server is ready to receive request!
Getting the request successfully! ^_^
Getting the request successfully! ^_^
```

127.0.0.1:1303/test.png

127.0.0.1:1303/test.png

Apps Debian.org Latest News Help



Bio.html

```
uxterm
z5241868@vx2:/tmp_amd/kamen/export/kamen/5/z5241868/Desktop/Lab3$ python3 WebSer
ver.py 1303
Welcome to use WebServer!
Server is ready to receive request!
Getting the request successfully! ^_^
Getting the request successfully! ^_^
Fail to get the request! T_T
```

Error!

127.0.0.1:1303/bio.html

Apps Debian.org Latest News Help

404 Not Found

The requested URL was not found.