E2

Question 1: What transport layer protocol is being used by the DNS messages?

A: The protocol is UDP

Question 2: What are the source and destination port for the DNS query message and the corresponding response?

A: DNS query message:

Source port: 3742

destination port: 53

DNS response message:

source port: 53

destination port: 3742

```
Source Port: 3742
Destination Port: 53
```

```
Source Port: 53
Destination Port: 3742
```

Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?

A: IP address: 128.238.38.160

```
Source Address: 128.238.38.160
```

Yes, it is same.

```
Destination Address: 128.238.38.160
```

Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?

A: One question, no answer

The question is a standard query for the DNS record type A (IPv4 address) and class IN (Internet)

```
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
> www.mit.edu: type A, class IN
```

Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?

A: In “Answers”: IP address associated with the hostname www.mit.edu is 18.7.22.83

```
Answers
> www.mit.edu: type A, class IN, addr 18.7.22.83
```

In “Authority”: the RRs indicate that authoritative name servers for the "mit.edu" domain are ns BITSY.mit.edu, ns STRAWB.mit.edu, and ns W20NS.mit.edu.

```
Authoritative nameservers
> mit.edu: type NS, class IN, ns BITSY.mit.edu
> mit.edu: type NS, class IN, ns STRAWB.mit.edu
> mit.edu: type NS, class IN, ns W20NS.mit.edu
```

In “Additional Information”: We may assume that the authoritative name servers for the "mit.edu" domain are dispersed across a number of IP addresses

```
Additional records
> BITSY.mit.edu: type A, class IN, addr 18.72.0.3
> STRAWB.mit.edu: type A, class IN, addr 18.71.0.151
> W20NS.mit.edu: type A, class IN, addr 18.70.0.160
```

E3:

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

A:

```
z5340468@vx03:~$ dig A www.stanford.edu

; <<>> DiG 9.16.37-Debian <<>> A www.stanford.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47825
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

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

;; ANSWER SECTION:
www.stanford.edu.       1345    IN      CNAME   pantheon-systems.map.fastly.net.
pantheon-systems.map.fastly.net. 30 IN  A       151.101.30.133

;; AUTHORITY SECTION:
fastly.net.             1579    IN      NS      ns3.fastly.net.
fastly.net.             1579    IN      NS      ns1.fastly.net.
fastly.net.             1579    IN      NS      ns4.fastly.net.
fastly.net.             1579    IN      NS      ns2.fastly.net.

;; ADDITIONAL SECTION:
ns1.fastly.net.         561     IN      A       23.235.32.32
ns2.fastly.net.         3364    IN      A       104.156.80.32
ns3.fastly.net.         1327    IN      A       23.235.36.32
ns4.fastly.net.         1971    IN      A       104.156.84.32

;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sat Mar 11 01:21:31 AEDT 2023
;; MSG SIZE  rcvd: 242
```

IP address is 151.101.30.133, it is A record query. The A record maps a domain name to an IPv4 address.

Question 2. What is the canonical name for the Stanford webserver (i.e., www.stanford.edu)? Suggest a reason for having an alias for this serve

A: pantheon-systems.map.fastly.net.

So, if we use an alias, we don't need to update every client that uses the server's IP address when changing the IP address.

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

A:

Authority section: The authoritative nameservers for the fastly.net domain are shown in the response's Authority section. If the domain's nameservers are not already cached, this information will help recursive nameservers discover them.

Additional section: The IP addresses of the nameservers provided in the Authority section are included in the Additional portion of the answer. This information is supplied to assist resolvers in contacting the authoritative nameservers in order to retrieve the necessary DNS records.

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

A: It is 172.31.192.1

Question 5. What are the DNS nameservers for the "stanford.edu.” domain (note: the domain name is stanford.edu and not www.stanford.edu . This is an example of what is referred to as the apex/naked domain)? Find their IP addresses. What type of DNS query is sent to obtain this information?

A:

```
z5340468@vx04:~$ dig NS stanford.edu

; <<>> DiG 9.16.37-Debian <<>> NS stanford.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41949
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 13

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

;; ANSWER SECTION:
stanford.edu.           8055    IN      NS      ns7.dnsmadeeasy.com.
stanford.edu.           8055    IN      NS      atalante.stanford.edu.
stanford.edu.           8055    IN      NS      ns5.dnsmadeeasy.com.
stanford.edu.           8055    IN      NS      ns6.dnsmadeeasy.com.
stanford.edu.           8055    IN      NS      avallone.stanford.edu.
stanford.edu.           8055    IN      NS      argus.stanford.edu.

;; ADDITIONAL SECTION:
ns5.dnsmadeeasy.com.    76328   IN      A       208.94.148.13
ns5.dnsmadeeasy.com.    62735   IN      AAAA    2600:1800:5::1
ns6.dnsmadeeasy.com.    59671   IN      A       208.80.124.13
ns6.dnsmadeeasy.com.    59671   IN      AAAA    2600:1801:6::1
ns7.dnsmadeeasy.com.    77250   IN      A       208.80.126.13
ns7.dnsmadeeasy.com.    12894   IN      AAAA    2600:1802:7::1
argus.stanford.edu.     314     IN      A       171.64.7.115
argus.stanford.edu.     314     IN      AAAA    2607:f6d0:0:9113::ab40:773
atalante.stanford.edu.  314     IN      A       171.64.7.61
atalante.stanford.edu.  314     IN      AAAA    2607:f6d0:0:d32::ab40:73d
avallone.stanford.edu.  314     IN      A       204.63.224.53
avallone.stanford.edu.  314     IN      AAAA    2620:6c:40c0:0:204:63:224:53

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sat Mar 11 02:38:41 AEDT 2023
;; MSG SIZE  rcvd: 440
```

There are 6 nameservers:
ns7.dnsmadeeasy.com 208.80.126.13,
atalante.stanford.edu 171.64.7.61,
ns5.dnsmadeeasy.com 208.94.148.13,
ns6.dnsmadeeasy.com 208.80.124.13,
avallone.stanford.edu 204.63.224.53,
argus.stanford.edu 171.64.7.115.
NS query, asks the authoritative DNS server for the domain to provide the list

servers that are responsible for the domain.

Question 6. What is the DNS name associated with the IP address 129.25.60.56 ? What type of DNS query is sent to obtain this information?

A:

```
z5340468@vx08:~$ nslookup 129.25.60.56
56.60.25.129.in-addr.arpa       name = ece.drexel.edu.

Authoritative answers can be found from:
25.129.in-addr.arpa     nameserver = adns2.drexel.edu.
25.129.in-addr.arpa     nameserver = adns1.drexel.edu.
adns1.drexel.edu        internet address = 144.118.27.1
adns2.drexel.edu        internet address = 144.118.27.18
```

Name is ece.drexel.edu. The type of DNS query sent to obtain this information was a PTR (pointer) query.

Question 7. Run, dig and query the CSE nameserver (129.94.242.33) for the mail servers for google.com (again, the domain name is google.com, not www.google.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 message to determine the answer)
A:

```
z5340468@vx08:~$ dig @129.94.242.33 google.com MX

; <<>> DiG 9.16.37-Debian <<>> @129.94.242.33 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64040
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 18

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

;; ANSWER SECTION:
google.com.             300     IN      MX      10 smtp.google.com.

;; AUTHORITY SECTION:
google.com.             114440  IN      NS      ns3.google.com.
google.com.             114440  IN      NS      ns4.google.com.
google.com.             114440  IN      NS      ns1.google.com.
google.com.             114440  IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        300     IN      A       172.253.118.27
smtp.google.com.        300     IN      A       64.233.170.26
smtp.google.com.        300     IN      A       74.125.130.27
smtp.google.com.        300     IN      A       74.125.200.26
smtp.google.com.        300     IN      A       74.125.200.27
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c00::1a
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c00::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c05::1b
smtp.google.com.        300     IN      AAAA    2404:6800:4003:c1a::1b
ns1.google.com.         118559  IN      A       216.239.32.10
ns1.google.com.         118548  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         19858   IN      A       216.239.34.10
ns2.google.com.         18728   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         118644  IN      A       216.239.36.10
ns3.google.com.         118604  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         191328  IN      A       216.239.38.10
ns4.google.com.         115535  IN      AAAA    2001:4860:4802:38::a

;; Query time: 104 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Mar 12 02:19:11 AEDT 2023
;; MSG SIZE  rcvd: 500
```

In authoritative section, there are four authoritative nameservers for the google.com domain: ns1.google.com, ns2.google.com, ns3.google.com, and ns4.google.com.The CSE nameserver is not authoritative for the google.com domain because there is a ‘ra’ response in flag. ‘ra’ flag means the server

supports recursive queries and ‘rd’ flag means the query was made with the recursive option.

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

A:

```
z5340468@vx08:~$ dig @208.94.148.13 google.com MX

; <<>> DiG 9.16.37-Debian <<>> @208.94.148.13 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 21485
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      MX

;; Query time: 4 msec
;; SERVER: 208.94.148.13#53(208.94.148.13)
;; WHEN: Sun Mar 12 02:32:16 AEDT 2023
;; MSG SIZE  rcvd: 39
```

There is a ‘REFUSED’ status, which means that the DNS server received the query but refused to give an answer. According to the ‘WARNING’, the DNS server does not support received queries, so it just provides answers for the domains for which it is authoritative.

Question 9. Obtain the authoritative answer for the mail servers for google.com. What type of DNS query is sent to obtain this information?
A:

```
z5340468@vx08:~$ dig google.com MX

; <<>> DiG 9.16.37-Debian <<>> google.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30420
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 18

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

;; ANSWER SECTION:
google.com.             177     IN      MX      10 smtp.google.com.

;; AUTHORITY SECTION:
google.com.             113322  IN      NS      ns3.google.com.
google.com.             113322  IN      NS      ns1.google.com.
google.com.             113322  IN      NS      ns4.google.com.
google.com.             113322  IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
smtp.google.com.        177     IN      A       74.125.24.27
smtp.google.com.        177     IN      A       74.125.68.26
smtp.google.com.        177     IN      A       74.125.130.27
smtp.google.com.        177     IN      A       74.125.200.27
smtp.google.com.        177     IN      A       74.125.24.26
smtp.google.com.        177     IN      AAAA    2404:6800:4003:c01::1b
smtp.google.com.        177     IN      AAAA    2404:6800:4003:c02::1b
smtp.google.com.        177     IN      AAAA    2404:6800:4003:c03::1a
smtp.google.com.        177     IN      AAAA    2404:6800:4003:c00::1a
ns1.google.com.         117430  IN      A       216.239.32.10
ns1.google.com.         117430  IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         18740   IN      A       216.239.34.10
ns2.google.com.         18740   IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         117486  IN      A       216.239.36.10
ns3.google.com.         117486  IN      AAAA    2001:4860:4802:36::a
ns4.google.com.         190210  IN      A       216.239.38.10
ns4.google.com.         114417  IN      AAAA    2001:4860:4802:38::a

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 12 02:37:49 AEDT 2023
;; MSG SIZE  rcvd: 500
```

It should be MX 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). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.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?

A:

```
z5340468@vx08:~$ dig NS .

; <<>> DiG 9.16.37-Debian <<>> NS .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58278
;; 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:
.                       465827  IN      NS      b.root-servers.net.
.                       465827  IN      NS      j.root-servers.net.
.                       465827  IN      NS      a.root-servers.net.
.                       465827  IN      NS      d.root-servers.net.
.                       465827  IN      NS      e.root-servers.net.
.                       465827  IN      NS      c.root-servers.net.
.                       465827  IN      NS      m.root-servers.net.
.                       465827  IN      NS      i.root-servers.net.
.                       465827  IN      NS      g.root-servers.net.
.                       465827  IN      NS      h.root-servers.net.
.                       465827  IN      NS      l.root-servers.net.
.                       465827  IN      NS      k.root-servers.net.
.                       465827  IN      NS      f.root-servers.net.
```

```
z5340468@vx08:~$ dig NS au. @b.root-servers.net.

; <<>> DiG 9.16.37-Debian <<>> NS au. @b.root-servers.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8774
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;au.                            IN      NS

;; AUTHORITY SECTION:
au.                     172800  IN      NS      c.au.
au.                     172800  IN      NS      d.au.
au.                     172800  IN      NS      q.au.
au.                     172800  IN      NS      r.au.
au.                     172800  IN      NS      s.au.
au.                     172800  IN      NS      t.au.
```

```
z5340468@vx08:~$ dig NS edu.au. @c.au.

; <<>> DiG 9.16.37-Debian <<>> NS edu.au. @c.au.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14406
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;edu.au.                                IN      NS

;; AUTHORITY SECTION:
edu.au.                 900     IN      NS      t.au.
edu.au.                 900     IN      NS      r.au.
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      q.au.
```

```
z5340468@vx08:~$ dig NS edu.au. @t.au.

; <<>> DiG 9.16.37-Debian <<>> NS edu.au. @t.au.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62683
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;edu.au.                                IN      NS

;; ANSWER SECTION:
edu.au.                 900     IN      NS      q.au.
edu.au.                 900     IN      NS      r.au.
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      t.au.
```

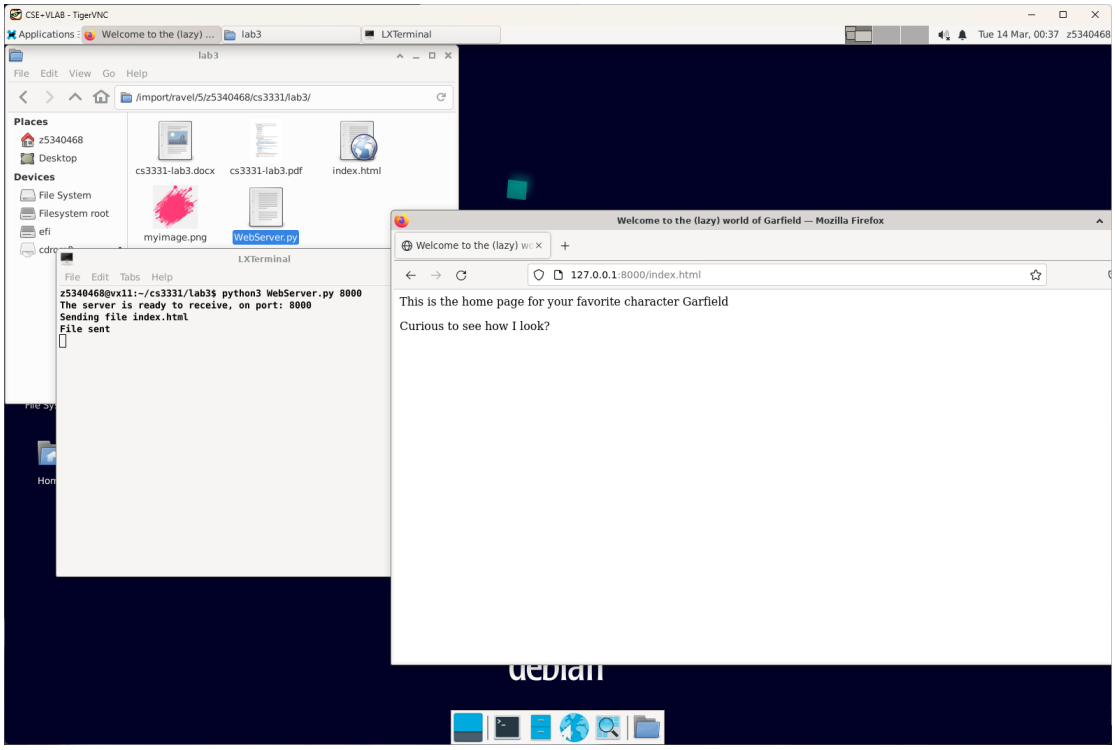
```
z5340468@vx08:~$ dig NS unsw.edu.au. @q.au.

; <<>> DiG 9.16.37-Debian <<>> NS unsw.edu.au. @q.au.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46816
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;unsw.edu.au.                   IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.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: 12 msec
;; SERVER: 65.22.196.1#53(65.22.196.1)
;; WHEN: Sun Mar 12 02:46:25 AEDT 2023
;; MSG SIZE  rcvd: 198
```

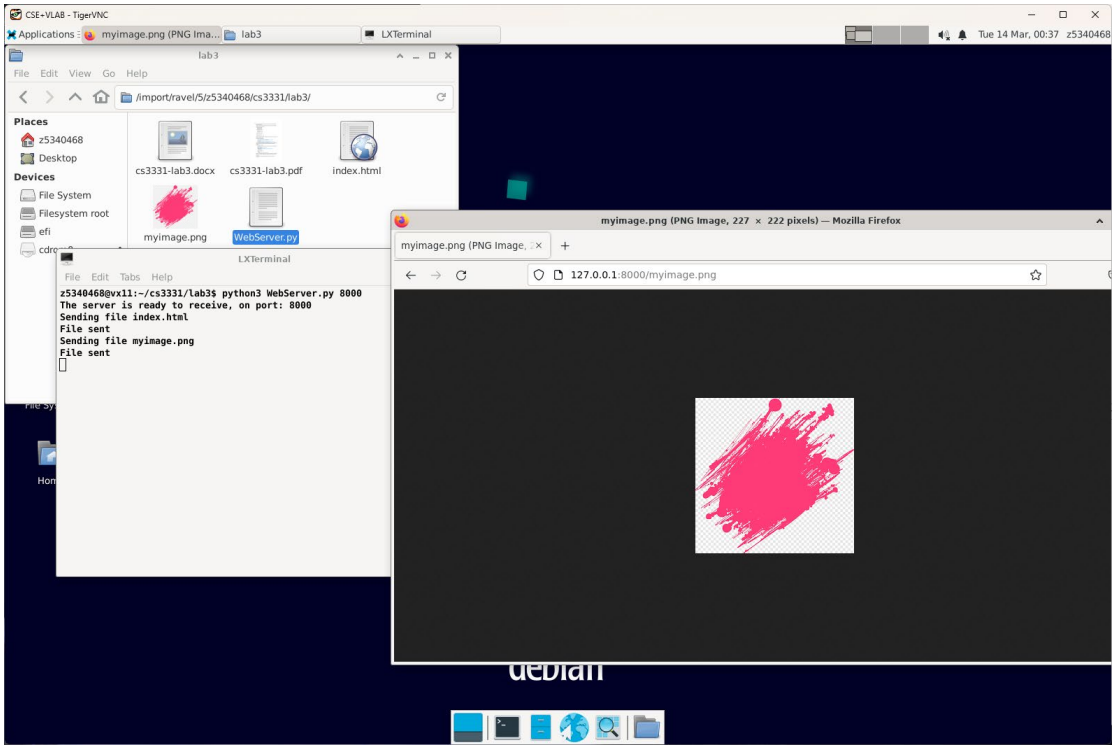
There are 5 steps.

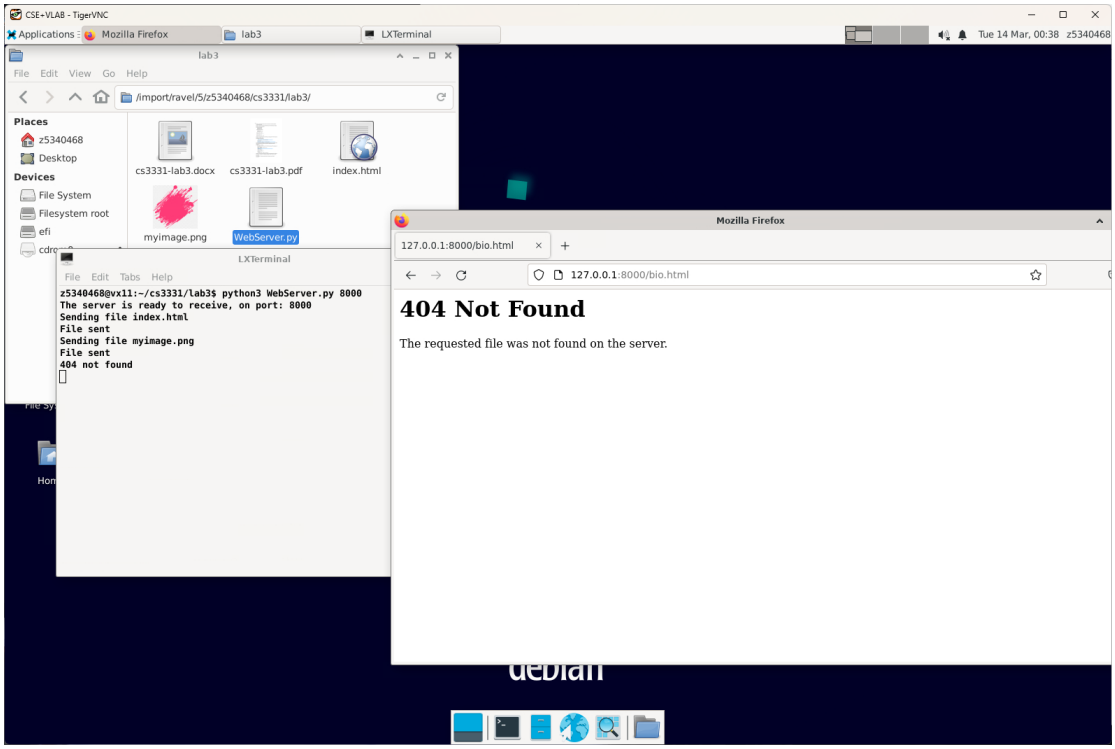
Question 11. Can one physical machine have several names and/or IP addresses associated with it?

A: Yes it is, for load balancing or fault-tolerant.

E4:


CSE+VLAB - TigerVNC
Welcome to the (lazy) world of Garfield — Mozilla Firefox
127.0.0.1:8000/index.html
This is the home page for your favorite character Garfield
Curious to see how I look?
z5340468@vx11:~/cs3331/lab3$ python3 WebServer.py 8000
The server is ready to receive, on port: 8000
Sending file index.html
File sent


CSE+VLAB - TigerVNC
myimage.png (PNG Image, 227 × 222 pixels) — Mozilla Firefox
127.0.0.1:8000/myimage.png
z5340468@vx11:~/cs3331/lab3$ python3 WebServer.py 8000
The server is ready to receive, on port: 8000
Sending file index.html
File sent
Sending file myimage.png
File sent


CSE+VLAB - TigerVNC
Applications
Mozilla Firefox
lab3
LXTerminal
Tue 14 Mar, 00:38 z5340468
lab3
File Edit View Go Help
/import/ravel/5/z5340468/cs3331/lab3/
Places
z5340468
Desktop
Devices
File System
Filesystem root
efi
cs3331-lab3.docx
cs3331-lab3.pdf
index.html
myimage.png
WebServer.py
LXTerminal
File Edit Tabs Help
z5340468@vx11:~/cs3331/lab3$ python3 WebServer.py 8000
The server is ready to receive, on port: 8000
Sending file index.html
File sent
Sending file myimage.png
File sent
404 not found
Mozilla Firefox
127.0.0.1:8000/bio.html
127.0.0.1:8000/bio.html
404 Not Found
The requested file was not found on the server.
debian