Lab3

LinXing Jia-z5382484

Exercise 3:

Q1:

The IP address of www.princeton.edu is 104.18.5.101. Type A

```
z5382484@vx05:~$ dig www.princeton.edu A

; <<>> DiG 9.18.24-1-Debian <<>> www.princeton.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61348
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f5afeed4d2097cd40100000065e6a04593e615590814ebdb (good)
;; QUESTION SECTION:
;www.princeton.edu.             IN      A

;; ANSWER SECTION:
www.princeton.edu.      1632    IN      CNAME   www.princeton.edu.cdn.cloudflare.net.
www.princeton.edu.cdn.cloudflare.net. 197 IN A  104.18.5.101
www.princeton.edu.cdn.cloudflare.net. 197 IN A  104.18.4.101

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 05 15:32:05 AEDT 2024
;; MSG SIZE  rcvd: 156
```

Q2:

The canonical name for the Princeton webserver is www.princeton.edu.cdn.cloudflare.net. The reason for setting an alias for the server may be to provide a more concise and easy-to-remember access method. The canonical name is relatively long, which is inconvenient for users to remember and input.

Q3:

In the DNS response, HEADER provides basic information about the response, and OPT PSEUDOSECTION provides some additional extended information. HEADER contains opcode: operation code, status: status code, id: unique identifier, used to identify the association between query and response. , flags: flag bit, QUERY: query quantity, etc.,

OPT PSEUDOSECTION contains:

EDNS: Extended DNS, including the EDNS version and other related information.

COOKIE: Cookie used to verify whether the communication between the server and the client is correct.

Q4:

The information about the local nameserver is included at the bottom of the output above, 129.94.242.2. This is the local DNS server for the CSE network.

Q5:

The DNS name server records of the "princeton.edu" domain were queried through the “dig princeton.edu NS”command. Their names and IP addresses are shown in the following table.

Name Servers	IP address
ns6.dnsmadeeasy.com.	208.80.124.13
ns7.dnsmadeeasy.com.	208.80.126.13
a3-67.akam.net.	96.7.49.67
a6-64.akam.net.	23.211.133.64
a7-65.akam.net.	23.61.199.65
a1-158.akam.net.	193.108.91.158
a20-65.akam.net.	95.100.175.65
a24-66.akam.net.	2.16.130.66

```
z5382484@vx21:~$ dig princeton.edu NS

; <<>> DiG 9.18.24-1-Debian <<>> princeton.edu NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63172
;; flags: qr rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 15

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fc8e4a77f1d1203a0100000065f014e421759ec94c535e04 (good)
;; QUESTION SECTION:
;princeton.edu.                 IN      NS

;; ANSWER SECTION:
princeton.edu.          43200   IN      NS      a24-66.akam.net.
princeton.edu.          43200   IN      NS      a1-158.akam.net.
princeton.edu.          43200   IN      NS      a20-65.akam.net.
princeton.edu.          43200   IN      NS      ns5.dnsmadeeasy.com.
princeton.edu.          43200   IN      NS      ns7.dnsmadeeasy.com.
princeton.edu.          43200   IN      NS      ns6.dnsmadeeasy.com.
princeton.edu.          43200   IN      NS      a3-67.akam.net.
princeton.edu.          43200   IN      NS      a7-65.akam.net.
princeton.edu.          43200   IN      NS      a6-64.akam.net.

;; ADDITIONAL SECTION:
ns6.dnsmadeeasy.com.    62749   IN      A       208.80.124.13
ns7.dnsmadeeasy.com.    48901   IN      A       208.80.126.13
a3-67.akam.net.         2724    IN      A       96.7.49.67
a6-64.akam.net.         71274   IN      A       23.211.133.64
a7-65.akam.net.         769     IN      A       23.61.199.65
a1-158.akam.net.        11982   IN      A       193.108.91.158
a20-65.akam.net.        6142    IN      A       95.100.175.65
a24-66.akam.net.        16134   IN      A       2.16.130.66
ns6.dnsmadeeasy.com.    70454   IN      AAAA    2600:1801:6::1
a3-67.akam.net.         626     IN      AAAA    2600:1408:1c::43
a6-64.akam.net.         19231   IN      AAAA    2600:1401:1::40
a7-65.akam.net.         27797   IN      AAAA    2600:1406:32::41
a20-65.akam.net.        18431   IN      AAAA    2a02:26f0:67::41
a24-66.akam.net.        16134   IN      AAAA    2600:1480:9800::42
```

```
;; Query time: 184 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 19:40:04 AEDT 2024
;; MSG SIZE  rcvd: 566
```

Q6:

The hostname corresponding to 198.54.223.213 is cput.ac.za, The dig -x command can be used to perform reverse DNS queries and find the corresponding domain name through a given IP address.

```
z5382484@vx12:~$ dig -x 198.54.223.213

; <<>> DiG 9.18.24-1-Debian <<>> -x 198.54.223.213
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47995
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7a400c371a4c99d90100000065efe294d1fa2692232b36f3 (good)
;; QUESTION SECTION:
;213.223.54.198.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
213.223.54.198.in-addr.arpa. 10956 IN   PTR     cput.ac.za.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 16:05:24 AEDT 2024
;; MSG SIZE  rcvd: 108
```

Q7:

We see that the server we queried cannot give us an authoritative answer because “AA” is not included in the flag. This is because it only has permissions on the cse.unsw.edu.au domain, but not on the google domain.

```
z5382484@vx12:~$ dig @129.94.242.2 google.com MX

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.242.2 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53410
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ebdd1bc0b802c90f0100000065efe3aee77bdfbcc1b6a29a (good)
;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             97      IN      MX      10 smtp.google.com.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 16:10:06 AEDT 2024
;; MSG SIZE  rcvd: 88
```

Q8:

Repeated the operation in Q7, but also did not get the authoritative answer.

```
z5382484@vx12:~$ dig @129.94.242.2 princeton.edu MX

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.242.2 princeton.edu MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24221
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: efe6df11b90305570100000065efe450697931d81e7e2862 (good)
;; QUESTION SECTION:
;princeton.edu.                 IN      MX

;; ANSWER SECTION:
princeton.edu.          3600    IN      MX      10 princeton-edu.mail.protection.outlook.com.

;; Query time: 7 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 16:12:48 AEDT 2024
;; MSG SIZE  rcvd: 127
```

Q9:

Use dig to send an MX (Mail Exchange) DNS query. This type of DNS query is specifically used to retrieve mail server information for a domain.

```
z5382484@vx21:~$ dig MX google.com

; <<>> DiG 9.18.24-1-Debian <<>> MX google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53246
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9ff9b3cfde77a1a90100000065f02520f7942b445c241722 (good)
;; QUESTION SECTION:
;google.com.                    IN      MX

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

;; Query time: 8 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 20:49:20 AEDT 2024
;; MSG SIZE  rcvd: 88
```

Q10:

Suppose the IP address we want to query is lyre01.cse.unsw.edu.au, first use NS to query the

name server (root domain) of the "." domain

```
^Cz5382484@vx21:~$ dig . NS

; <<>> DiG 9.18.24-1-Debian <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11677
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d2c5aa5696e9e7650100000065f027b15f3be860bb6dd1b5 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       51797   IN      NS      d.root-servers.net.
.                       51797   IN      NS      a.root-servers.net.
.                       51797   IN      NS      j.root-servers.net.
.                       51797   IN      NS      f.root-servers.net.
.                       51797   IN      NS      g.root-servers.net.
.                       51797   IN      NS      l.root-servers.net.
.                       51797   IN      NS      m.root-servers.net.
.                       51797   IN      NS      c.root-servers.net.
.                       51797   IN      NS      k.root-servers.net.
.                       51797   IN      NS      b.root-servers.net.
.                       51797   IN      NS      e.root-servers.net.
.                       51797   IN      NS      h.root-servers.net.
.                       51797   IN      NS      i.root-servers.net.
```

```
;; ADDITIONAL SECTION:
a.root-servers.net.     138088  IN      A       198.41.0.4
b.root-servers.net.     352256  IN      A       170.247.170.2
c.root-servers.net.     352256  IN      A       192.33.4.12
d.root-servers.net.     352256  IN      A       199.7.91.13
e.root-servers.net.     352256  IN      A       192.203.230.10
f.root-servers.net.     80244   IN      A       192.5.5.241
g.root-servers.net.     348795  IN      A       192.112.36.4
h.root-servers.net.     352256  IN      A       198.97.190.53
i.root-servers.net.     240237  IN      A       192.36.148.17
j.root-servers.net.     352256  IN      A       192.58.128.30
k.root-servers.net.     352256  IN      A       193.0.14.129
l.root-servers.net.     351694  IN      A       199.7.83.42
m.root-servers.net.     352256  IN      A       202.12.27.33
a.root-servers.net.     4418    IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     54673   IN      AAAA    2801:1b8:10::b
c.root-servers.net.     352256  IN      AAAA    2001:500:2::c
d.root-servers.net.     352256  IN      AAAA    2001:500:2d::d
e.root-servers.net.     240327  IN      AAAA    2001:500:a8::e
f.root-servers.net.     352256  IN      AAAA    2001:500:2f::f
g.root-servers.net.     475473  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     352256  IN      AAAA    2001:500:1::53
i.root-servers.net.     240237  IN      AAAA    2001:7fe::53
j.root-servers.net.     352256  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     352256  IN      AAAA    2001:7fd::1
l.root-servers.net.     351694  IN      AAAA    2001:500:9f::42
m.root-servers.net.     352256  IN      AAAA    2001:dc3::35

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2) (UDP)
;; WHEN: Tue Mar 12 21:00:17 AEDT 2024
;; MSG SIZE  rcvd: 851
```

Next query one of the root nameservers as follows:

```
z5382484@vx21:~$ dig @198.41.0.4 lyre01.cse.unsw.edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @198.41.0.4 lyre01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11979
;; 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:
;lyre01.cse.unsw.edu.au.                IN      NS

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

;; ADDITIONAL SECTION:
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

;; Query time: 96 msec
;; SERVER: 198.41.0.4#53(198.41.0.4) (UDP)
;; WHEN: Tue Mar 12 21:06:22 AEDT 2024
;; MSG SIZE  rcvd: 291
```

Use one of the IP addresses to query the name servers for the domain "edu.au.":

```
z5382484@vx21:~$ dig @65.22.196.1 lyre01.cse.unsw.edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @65.22.196.1 lyre01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24657
;; 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:
;lyre01.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
unsw.edu.au.            900     IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            900     IN      NS      ns2.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) (UDP)
;; WHEN: Tue Mar 12 21:09:03 AEDT 2024
;; MSG SIZE  rcvd: 209
```

We can see that the domain name already contains the "unsw.edu.au." field. so query one of them as follows:

```
z5382484@vx21:~$ dig @129.94.0.192 lyre01.cse.unsw.edu.au NS

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.0.192 lyre01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45191
;; 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:
;lyre01.cse.unsw.edu.au.                IN      NS

;; AUTHORITY SECTION:
cse.unsw.edu.au.        300     IN      NS      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        300     IN      NS      maestro.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 300 IN A   129.94.242.2
maestro.orchestra.cse.unsw.edu.au. 300 IN A     129.94.242.33

;; Query time: 4 msec
;; SERVER: 129.94.0.192#53(129.94.0.192) (UDP)
;; WHEN: Tue Mar 12 21:10:50 AEDT 2024
;; MSG SIZE  rcvd: 171
```

We are now referred to the CSE name servers, so we query one of them as follows. (dig A):

```
z5382484@vx21:~$ dig @129.94.172.11 lyre01.cse.unsw.edu.au A

; <<>> DiG 9.18.24-1-Debian <<>> @129.94.172.11 lyre01.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48391
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b410d77ba60c41a00100000065f02bd3f60e979c56c84e30 (good)
;; QUESTION SECTION:
;lyre01.cse.unsw.edu.au.                IN      A

;; ANSWER SECTION:
lyre01.cse.unsw.EDU.AU. 3600    IN      A       129.94.210.21

;; Query time: 0 msec
;; SERVER: 129.94.172.11#53(129.94.172.11) (UDP)
;; WHEN: Tue Mar 12 21:17:55 AEDT 2024
;; MSG SIZE  rcvd: 117
```

The IP address for lyre01.cse.unsw.edu.au is 129.94.210.21. Following the iterative query process

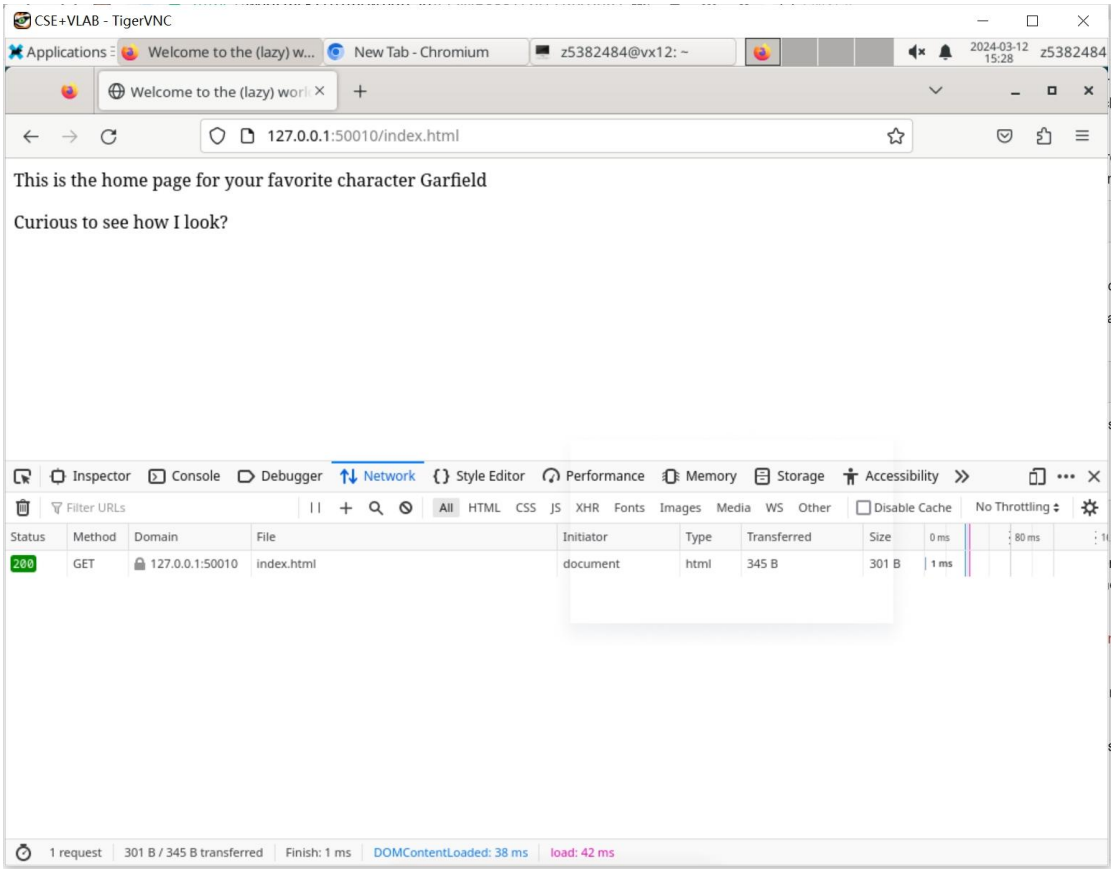
starting from the root domain name server, we must query 5 DNS servers.

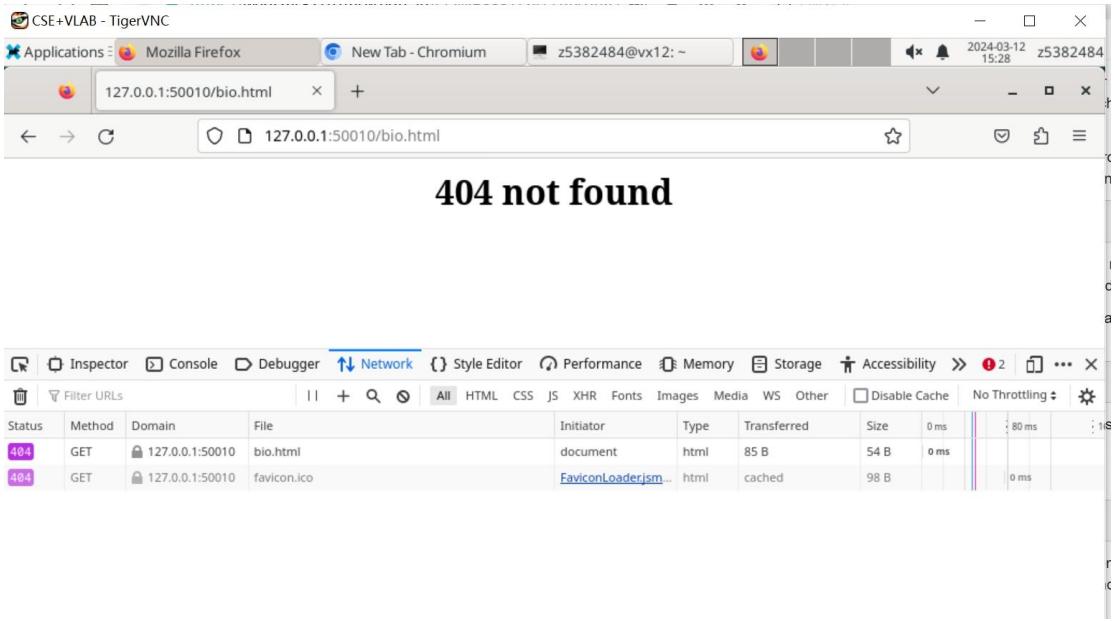
Q11:

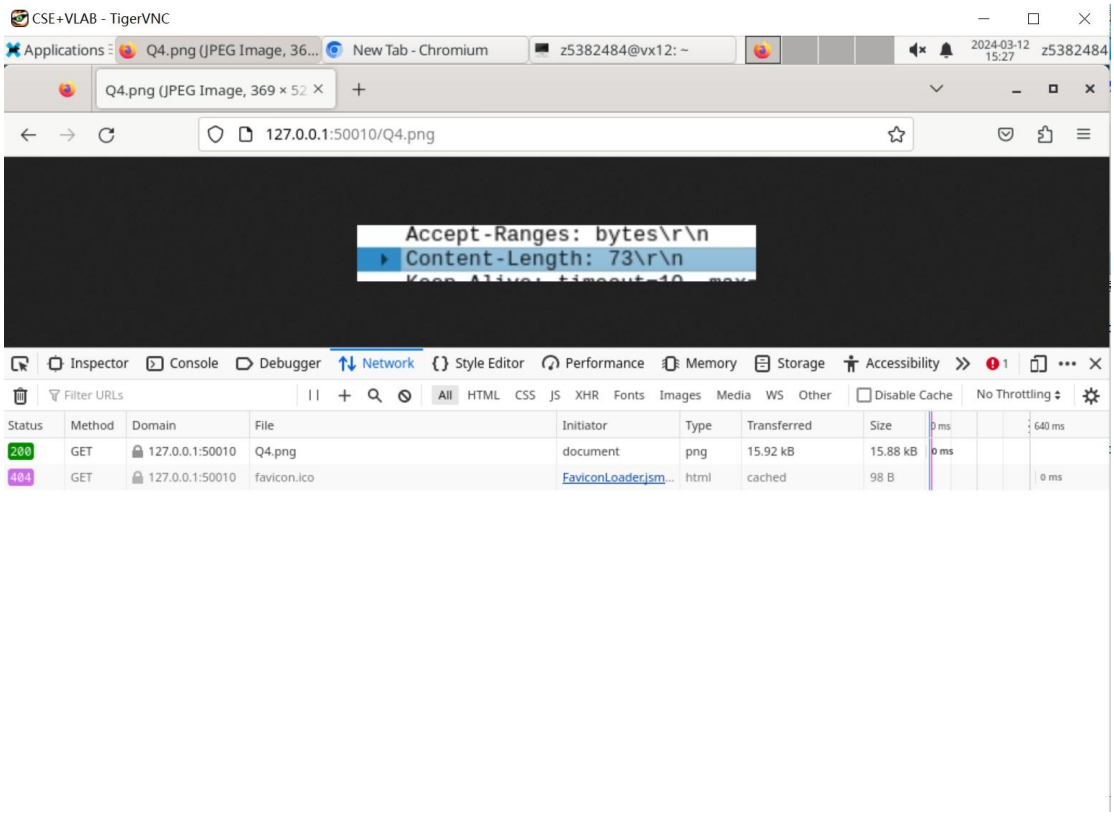
Yes, a physical machine can have multiple names and/or IP addresses associated with it. If a physical machine is connected to multiple networks or subnets, it may be assigned multiple IP addresses, one for each network interface. In addition, a machine may have multiple aliases (also called hostnames) and CNAME records, and these records can be mapped to the same IP address. This allows different names to point to the same physical machine.

Exercise 5:

The running results are as follows:




CSE+VLAB - TigerVNC
Applications
Mozilla Firefox
New Tab - Chromium
z5382484@vx12: ~
2024-03-12 15:28
z5382484
127.0.0.1:50010/bio.html
127.0.0.1:50010/bio.html
404 not found
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Status Method Domain File Initiator Type Transferred Size
404 GET 127.0.0.1:50010 bio.html document html 85 B 54 B
404 GET 127.0.0.1:50010 favicon.ico FaviconLoader.jsm... html cached 98 B


CSE+VLAB - TigerVNC
Applications
Q4.png (JPEG Image, 36...
New Tab - Chromium
z5382484@vx12: ~
2024-03-12 15:27
z5382484
Q4.png (JPEG Image, 369 × 52
127.0.0.1:50010/Q4.png
Accept-Ranges: bytes\r\n
Content-Length: 73\r\n
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Filter URLs
All HTML CSS JS XHR Fonts Images Media WS Other
Disable Cache
No Throttling
Status Method Domain File Initiator Type Transferred Size
200 GET 127.0.0.1:50010 Q4.png document png 15.92 kB 15.88 kB
404 GET 127.0.0.1:50010 favicon.ico FaviconLoader.jsm... html cached 98 B