PART A

1i)

```
root@kali: /
File  Edit  View  Search  Terminal  Help
root@kali:/# dig www.anuflora.com

; <<>> DiG 9.10.6-Debian <<>> www.anuflora.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55044
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;www.anuflora.com.              IN      A

;; ANSWER SECTION:
www.anuflora.com.       5       IN      CNAME   anuflora.com.
anuflora.com.           5       IN      A       103.243.175.98

;; Query time: 17 msec
;; SERVER: 192.168.25.2#53(192.168.25.2)
;; WHEN: Sun Sep 16 03:21:18 EDT 2018
;; MSG SIZE  rcvd: 75

root@kali:/#
```

The IP address of the authoritative name server is 103.243.175.98.

The server is not hosted inside NUS because, when a domain name is resolved, the local DNS server queries the root DNS server. The root DNS server will query the TLDs. The TLD will find the respective DNS server, which will in turn delegate part of its authority to other servers. However, the TLD for www.anuflora.com is different from TLD of www.nus.edu.sg. Furthermore, the sub-domain nus is missing from www.anuflora.com. Therefore, the DNS server for www.anuflora.com is not hosted in NUS server.

ii) The host name of the mail servers for comp.nus.edu.sg is **84-102.comp.nus.edu.sg** and **84-101.comp.nus.edu.sg**. This result was obtained from the command: **dig –t MX comp.nus.edu.sg**. However to resolve the IP addresses of these hosts, I ran **dig 84-101.comp.nus.edu.sg** and **dig 84-102.comp.nus.edu.sg** to get the IP addresses **137.132.84.101** and **137.132.84.102.**

2)

```
root@kali:~# openssl s_client -connect smtp.gmail.com:465 -crlf
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = smtp.gmail.com
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google LLC/CN=smtp.gmail.com
   i:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
 1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
   i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
---
Server certificate
-----BEGIN CERTIFICATE-----
```

```
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 00 68 2d ab 93 bf 02 8a-00 07 51 41 01 53 26 2a   .h-.......QA.S&*
    0010 - f5 d3 90 7b 59 5e df 4d-01 2a 50 09 76 ca ae 77   ...{Y^.M.*P.v..w
    0020 - 6f f3 1b 31 f4 86 97 b6-2b 70 b8 5e c9 77 84 44   o..1....+p.^.w.D
    0030 - e2 59 83 a4 2d 76 45 ca-9b 91 ba d8 2f 29 a7 c1   .Y..-vE...../)..
    0040 - 09 ba 14 38 ac 1c 75 00-15 31 90 c7 83 4d eb c6   ...8..u..1...M..
    0050 - 46 20 ba e8 ee f2 6c 3f-fe cf 0d fc 0d 09 85 58   F ....l?.......X
    0060 - d8 1a a6 9a 1b a5 fc ae-30 d5 d5 ad cb 48 41 f1   ........0....HA.
    0070 - 0e 44 01 3c 95 82 a4 29-51 d7 8d e7 86 9c 06 6c   .D.<...)Q......l
    0080 - ee 67 b4 0d 92 b1 d8 59-ce 3c 09 54 0f d9 51 00   .g.....Y.<.T..Q.
    0090 - 49 67 9a 4c b9 52 b3 8a-60 d9 aa 2e 12 63 94 2b   Ig.L.R..`....c.+
    00a0 - 8d cf 3b 52 72 6a d2 a7-cf 8c 51 c6 6f f1 b6 3b   ..;Rrj....Q.o..;
    00b0 - c4 62 c0 0a 47 d5 d5 22-7e 59 a5 a9 c5 14 1a f3   .b..G.."~Y......
    00c0 - d2 4c fa 6e eb fc 60 4a-ad 90 af 14 56 da 8c cf   .L.n..`J....V...
    00d0 - be 2f 68 d8 75 d9 c8 5f-0d 50                     ./h.u.._.P

    Start Time: 1537164579
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: yes
---
220 smtp.gmail.com ESMTP f67-v6sm38342096pfe.75 - gsmtp
ehlo gmail.com
250-smtp.gmail.com at your service, [137.132.228.43]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
```

```
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
AUTH LOGIN cm[redacted]==
334 UGFzc3dvcmQ6
U[redacted]h
235 2.7.0 Accepted
MAIL FROM:rdheeraj1994@gmail.com
555 5.5.2 Syntax error. f67-v6sm38342096pfe.75 - gsmtp
mail from: rdheeraj1994@gmail.com
555 5.5.2 Syntax error. f67-v6sm38342096pfe.75 - gsmtp
rcpt to: dheerajasum@gmail.com
503 5.5.1 MAIL first. f67-v6sm38342096pfe.75 - gsmtp
mail from: <rdheeraj1994@gmail.com>
250 2.1.0 OK f67-v6sm38342096pfe.75 - gsmtp
rcpt to: <rdheeraj1994@gmail.com>
250 2.1.5 OK f67-v6sm38342096pfe.75 - gsmtp
DATA
354 Go ahead f67-v6sm38342096pfe.75 - gsmtp
FROM:rdheeraj1994@gmail.com
TO:rdheeraj1994@gmail.com
Subject:CS3103 Test Email
DOT.
My first email with openssl! for CS3103
.
250 2.0.0 OK 1537164995 f67-v6sm38342096pfe.75 - gsmtp
QUIT
DONE
```

The list of commands used has been highlighted in red. The password and other sensitive data have been censored ☺.

3)

```
root@kali:~# openssl s_client -connect pop.gmail.com:995 -crlf -ign_eof
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = pop.gmail.com
verify return:1
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google LLC/CN=pop.gmail.com
   i:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
 1 s:/C=US/O=Google Trust Services/CN=Google Internet Authority G3
   i:/OU=GlobalSign Root CA - R2/O=GlobalSign/CN=GlobalSign
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEgDCCA2igAwIBAgIIL3uwCWr78EYwDQYJKoZIhvcNAQELBQAwVDELMAkGA1UE
```

```
---
+OK Gpop ready for requests from 137.132.228.43 65-v6mb72133609ott
USER [redacted]
+OK send PASS
PASS [redacted]
+OK Welcome.
list
+OK 2 messages (40223 bytes)
1 39658
2 565

RETR 2
+OK message follows
Return-Path: <[redacted]@gmail.com>
Received: from gmail.com ([137.132.228.43])
        by smtp.gmail.com with ESMTPSA id f67-v6sm38342096pfe.75.2018.09.16.23.14.12
        for <[redacted]@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-CHACHA20-POLY1305 bits=256/256);
        Sun, 16 Sep 2018 23:16:34 -0700 (PDT)
Message-ID: <5b9f46c2.1c69fb81.e3124.b491@mx.google.com>
Date: Sun, 16 Sep 2018 23:16:34 -0700 (PDT)
FROM:[redacted]@gmail.com
TO:[redacted]@gmail.com
Subject:CS3103 Test Email

DOT.
My first email with openssl! for CS3103

QUIT
+OK Farewell.
read:errno=0
```

The above screenshots show the interaction between the gmail pop server and myself.

4)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# telnet 192.168.25.138 21
Trying 192.168.25.138...
Connected to 192.168.25.138.
Escape character is '^]'.
220 (vsFTPd 3.0.3)
USER seed
331 Please specify the password.
PASS Venkat1972
230 Login successful.
PWD
257 "/home/seed" is the current directory
PASV
227 Entering Passive Mode (192,168,25,138,49,156).
EPSV
229 Entering Extended Passive Mode (|||32558|)
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# telnet 192.168.25.138 32558
Trying 192.168.25.138...
Connected to 192.168.25.138.
Escape character is '^]'.
drwxrwxr-x    2 1000     1000         4096 Jan 14  2018 Customization
drwxr-xr-x    6 1000     1000         4096 Sep 12 14:17 Desktop
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Documents
drwxr-xr-x    2 1000     1000         4096 May 09 14:15 Downloads
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Music
drwxr-xr-x    3 1000     1000         4096 Jan 14  2018 Pictures
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Public
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Templates
drwxr-xr-x    2 1000     1000         4096 Jul 25  2017 Videos
drwxrwxr-x    4 1000     1000         4096 May 01 00:35 android
drwxrwxr-x    2 1000     1000         4096 Jan 14  2018 bin
-rw-r--r--    1 1000     1000         8980 Jul 25  2017 examples.desktop
drwxrwxr-x    3 1000     1000         4096 May 09 00:33 lib
drwxrwxr-x    4 1000     1000         4096 May 09 00:35 source
-rw-rw-r--    1 1000     1000           10 Sep 17 14:31 test.txt
Connection closed by foreign host.
root@kali:~#
```

Above is the screenshot that lists the commands used to execute FTP protocol using telnet. The above command was achieved by running two VMs; one Kali Linux and one Ubuntu with the Ubuntu being the server and Kali being the client. After entering the correct credentials (username and password), the client opens 2 random unprivileged ports (port number greater than 1023) locally. The first port it opened establishes a TCP connection to the server at port 21 on server side. Now, the client is connected to the server.

Subsequently, the server issues the PASV command during which the server issues opens a random unprivileged port and sends the port number to the client. The client initiates a connection to the port number specified by the

server. Therefore, in total 2 TCP connections are needed to carry out directory listing and/or file transfer.

PART B

* Please Refer to the code submitted for part b.