

1. Properly configured DNS MX query

```
jboicken@desktop:~$ dig MX student15.230.com @199.100.16.100

; <<>> DiG 9.16.1-Ubuntu <<>> MX student15.230.com @199.100.16.100
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 5940
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 73302098e00e994b010000005f7c74f51436aa365a1b12e0 (good)
;; QUESTION SECTION:
;student15.230.com.                IN      MX

;; ANSWER SECTION:
student15.230.com.                585931  IN      MX      10 mail.student15.230.com.

;; ADDITIONAL SECTION:
mail.student15.230.com. 66758   IN      A        200.35.23.204

;; Query time: 0 msec
;; SERVER: 199.100.16.100#53(199.100.16.100)
;; WHEN: Tue Oct 06 03:18:12 CDT 2020
;; MSG SIZE rcvd: 111
```

2. netstat -tnl

```
cpre230@mail:~$ netstat -tnl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp6       0      0 :::110                  :::*                     LISTEN
tcp6       0      0 :::143                  :::*                     LISTEN
tcp6       0      0 :::25                   :::*                     LISTEN
tcp6       0      0 :::993                  :::*                     LISTEN
tcp6       0      0 :::995                  :::*                     LISTEN

cpre230@mail:~$ netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:pop3            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:imap2           0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:smtp            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:imaps           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:pop3s           0.0.0.0:*               LISTEN
tcp6       0      0 [::]:pop3               [::]:*                  LISTEN
tcp6       0      0 [::]:imap2              [::]:*                  LISTEN
tcp6       0      0 [::]:smtp                [::]:*                  LISTEN
tcp6       0      0 [::]:imaps               [::]:*                  LISTEN
tcp6       0      0 [::]:pop3s              [::]:*                  LISTEN
```

3. Sending mail from cpre230a --> cpre230b in terminal

```
cpre230@mail:~$ telnet mail.student15.230.com 25
Trying 200.35.23.204...
Connected to mail.student15.230.com.
Escape character is '^]'.
220 mail ESMTP Postfix (Ubuntu)
helo student15.230.com
250 mail
mail from: <cpre230a@student15.230.com>
250 2.1.0 Ok
rcpt to: <cpre230b@student15.230.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Testing 1,2,3...

Will the real Martian please stand up?
.
250 2.0.0 Ok: queued as A121425455
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

4. Read the previously sent message in terminal

```
cpre230@mail:~$ telnet mail.student15.230.com 110
Trying 200.35.23.204...
Connected to mail.student15.230.com.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
USER cpre230b
+OK
PASS cpre230
+OK Logged in.
LIST
+OK 1 messages:
1 515
.
RETR 1
+OK 515 octets
Return-Path: <cpre230a@student15.230.com>
X-Original-To: cpre230b@student15.230.com
Delivered-To: cpre230b@student15.230.com
Received: from student15.230.com (mail.student15.230.com [200.35.23.204])
        by mail (Postfix) with SMTP id A121425455
        for <cpre230b@student15.230.com>; Tue,  6 Oct 2020 01:54:33 +0000 (UTC)
Subject: Testing 1,2,3...
Message-Id: <20201006015515.A121425455@mail>
Date: Tue,  6 Oct 2020 01:54:33 +0000 (UTC)
From: cpre230a@student15.230.com

Will the real Martian please stand up?
.
QUIT
+OK Logging out.
Connection closed by foreign host.
```



```

Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
Signature Algorithm: sha256WithRSAEncryption
22:8b:0b:ca:3b:65:4b:ed:0e:07:2b:36:88:33:7e:b9:1e:c5:
2b:2c:af:94:26:cc:af:7f:a8:5a:ab:2f:0c:3d:2c:1b:98:88:
7e:f3:c3:80:5e:1d:ae:9d:a9:28:5d:d4:df:cd:67:e1:0e:8a:
c1:a0:c1:8d:82:e6:0f:93:4b:bb:e0:fc:46:38:88:b6:32:cc:
29:80:1d:ad:71:b3:23:5e:1c:81:f7:50:db:e4:d7:9a:60:4f:
55:25:9d:cf:89:30:5a:bf:ab:30:aa:17:bd:49:3e:4b:02:68:
52:1c:75:20:84:c5:05:59:ce:4e:c5:6f:90:5f:a5:d9:6a:b8:
19:6f:a8:09:13:df:08:c0:48:14:6b:1b:a1:3c:71:c3:5e:bc:
4a:5f:c2:7d:cd:6d:99:29:dc:66:0e:82:cb:71:4d:c3:82:40:
0a:24:10:18:f8:64:9a:7b:1c:a1:97:45:bf:49:7d:d7:fe:67:
a7:86:cf:ad:2b:41:a6:bd:88:87:de:82:20:4d:0e:37:6b:ba:
7e:ee:db:1e:52:9d:92:5c:a7:dc:fb:13:3e:38:5a:dd:5e:66:
74:da:25:98:88:45:cb:5e:f4:b5:c1:a6:45:e3:7b:c8:65:61:
64:87:5a:c9:52:83:2d:a7:2f:c0:b8:a5:97:a6:11:c5:c2:7c:
67:c5:4a:d8

```

7. Plaintext IMAP - Wireshark

imap

No.	Time	Source	Destination	Protocol	Length	Info
3370	61.715288290	200.35.23.204	200.35.23.201	IMAP	121	Response: 11 OK Idle completed (81.2
3372	61.715427567	200.35.23.201	200.35.23.204	IMAP	75	Request: 12 noop
3373	61.715555650	200.35.23.204	200.35.23.201	IMAP	110	Response: 12 OK NOOP completed (0.00
3375	61.715612847	200.35.23.201	200.35.23.204	IMAP	92	Request: 13 UID fetch 3: * (FLAGS)
3376	61.715761215	200.35.23.204	200.35.23.201	IMAP	146	Response: 13 OK Fetch completed (0.0
3378	61.715934856	200.35.23.201	200.35.23.204	IMAP	248	Request: 14 UID fetch 3 (UID RFC822.
3379	61.716319938	200.35.23.204	200.35.23.201	IMAP/I...	582	from: cpre230a <cpre230a@student15.2
3381	61.719298117	200.35.23.201	200.35.23.204	IMAP	112	Request: 15 UID fetch 3 (UID RFC822.
3382	61.719588048	200.35.23.204	200.35.23.201	IMAP/I...	954	from: cpre230a <cpre230a@student15.2
3384	61.725407189	200.35.23.201	200.35.23.204	IMAP	178	Request: 16 UID fetch 3 (UID BODY.PE
3385	61.725726181	200.35.23.204	200.35.23.201	IMAP/I...	355	(text/plain)
3387	61.727934110	200.35.23.201	200.35.23.204	IMAP	75	Request: 17 IDLE
3388	61.728107019	200.35.23.204	200.35.23.201	IMAP	76	Response: + idling
3389	61.728107019	200.35.23.204	200.35.23.201	IMAP	82	Response: * OK Still here

Frame 3382: 954 bytes on wire (7632 bits), 954 bytes captured (7632 bits) on interface ens160, id 0

Ethernet II, Src: Intersof_04:0f:04 (00:02:30:04:0f:04), Dst: VMware_86:77:6b (00:50:56:86:77:6b)

Internet Protocol Version 4, Src: 200.35.23.204, Dst: 200.35.23.201

Transmission Control Protocol, Src Port: 143, Dst Port: 58622, Seq: 720, Ack: 270, Len: 888

0090 35 2e 32 33 30 2e 63 6f 6d 3e 0d 0a 58 2d 4f 72 5.230.co m>..X-Or

00a0 69 67 69 6e 61 6c 2d 54 6f 3a 20 63 70 72 65 32 iginal-T o: cpre2

00b0 33 30 62 40 73 74 75 64 65 6e 74 31 35 2e 32 33 30b@stud ent15.23

00c0 30 2e 63 6f 6d 0d 0a 44 65 6c 69 76 65 72 65 64 0.com- D elivered

00d0 2d 54 6f 3a 20 63 70 72 65 32 33 30 62 40 73 74 -To: cpr e230b@st

00e0 75 64 65 6e 74 31 35 2e 32 33 30 2e 63 6f 6d 0d ugent15. 230.com-

00f0 0a 52 65 63 65 69 76 65 64 3a 20 66 72 6f 6d 20 -Receive d: from

Internet Message Access Protocol: Protocol

Packets: 42518 · Displayed: 105 (

8. Plaintext SMTP - Wireshark

smtp						
No.	Time	Source	Destination	Protocol	Length	Info
42	20.091869030	200.35.23.204	200.35.23.201	SMTP	82	S: 250 2.1.5 Ok
44	20.091975450	200.35.23.201	200.35.23.204	SMTP	74	C: DATA
46	20.092132721	200.35.23.204	200.35.23.201	SMTP	105	S: 354 End data with <CR><LF>.<CR><LF>
48	20.093100257	200.35.23.201	200.35.23.204	SMTP	501	C: DATA fragment, 433 bytes
49	20.093163017	200.35.23.201	200.35.23.204	SMTP/I...	71	from: cpre230b <cpre230b@student15.230.com>
51	20.095661578	200.35.23.204	200.35.23.201	SMTP	104	S: 250 2.0.0 Ok: queued as D983F20F59
53	20.110559374	200.35.23.201	200.35.23.204	SMTP	74	C: QUIT
54	20.110741401	200.35.23.204	200.35.23.201	SMTP	83	S: 221 2.0.0 Bye

▶ Frame 48: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface any, id 0
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 4, Src: 200.35.23.201, Dst: 200.35.23.204
 ▶ Transmission Control Protocol, Src Port: 37078, Dst Port: 25, Seq: 130, Ack: 254, Len: 433
 ▶ Simple Mail Transfer Protocol
 ↳ Line-based text data (14 lines)
 To: cpre230a@student15.230.com\r\n
 From: cpre230b <cpre230b@student15.230.com>\r\n
 Subject: how\r\n

0000 64 65 6e 74 31 35 2e 32 33 30 2e 63 6f 6d 3e 0d dent15.2 30.com>
 0090 0a 53 75 62 6a 65 63 74 3a 20 68 6f 77 0d 0a 4d .Subject : how
 00a0 65 73 73 61 67 65 2d 49 44 3a 20 3c 39 39 33 38 message-I D: <9938
 00b0 38 37 36 37 2d 30 32 61 62 2d 62 39 38 33 2d 31 8767-02a b-b983-1
 00c0 36 34 33 2d 36 32 33 63 33 62 61 32 65 64 37 32 643-623c 3ba2ed72
 00d0 40 73 74 75 64 65 6e 74 31 35 2e 32 33 30 2e 63 @student 15.230.c
 00e0 6f 6d 3e 0d 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 om> .Dat e: Mon,

9. Screenshot of test messages in Thunderbird

Inbox - cpre230b@student15.2

Get Messages Write Chat Address Book Tag

- ✉ cpre230a@....230.com
 - Inbox
 - Sent
 - Trash
- ✉ cpre230b@....230.com
 - Inbox
 - Sent
 - Trash
- Local Folders
 - Trash
 - Outbox

☆ | ☆ | ☆ | ☆ | ☆
 ☆ Subject
 ☆ Testing 1,2,3...
 ☆ Testing This Wireshark
 ☆ Testing for Wireshark

From Me <cpre230a@student15.230.com>
 Subject **Testing This Wireshark**
 To Me <cpre230b@student15.230.com>
 Will the real slim shady please stand up?

Inbox - cpre230a@student15.230.com

Get Messages Write Chat Address Book Tag Quick

- ✉ cpre230a@....230.com
 - Inbox
 - Sent
 - Trash
- ✉ cpre230b@....230.com
 - Inbox
 - Sent
 - Trash
- Local Folders
 - Trash
 - Outbox

☆ | ☆ | ☆ | ☆ | ☆
 ☆ Subject
 ☆ Testing b
 ☆ Testing this again
 ☆ Mess
 ☆ how

From Me <cpre230b@student15.230.com>
 Subject **Testing this again**
 To Me <cpre230a@student15.230.com>
 Will the real slim Martian please beam me up?

10. Encrypted SMTP - Wireshark

tcp.port == 587						
No.	Time	Source	Destination	Protocol	Length	Info
87	3.913297548	37.56.23.100	64.39.3.204	SMTP	76	C: STARTTLS
88	3.913317439	64.39.3.204	37.56.23.100	TCP	66	587 → 47952 [ACK] Seq=189 Ack=33
89	3.913340191	64.39.3.204	37.56.23.100	SMTP	96	S: 220 2.0.0 Ready to start TLS
90	3.913694261	37.56.23.100	64.39.3.204	TCP	66	47952 → 587 [ACK] Seq=33 Ack=219
91	3.915250714	37.56.23.100	64.39.3.204	TLSv1.3	345	Client Hello
92	3.915268968	64.39.3.204	37.56.23.100	TCP	66	587 → 47952 [ACK] Seq=219 Ack=312
93	3.916810297	64.39.3.204	37.56.23.100	TLSv1.3	1571	Server Hello, Change Cipher Spec,
94	3.917199040	37.56.23.100	64.39.3.204	TCP	66	47952 → 587 [ACK] Seq=312 Ack=166

▶ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
 ▶ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 ▶ TLSv1.3 Record Layer: Application Data Protocol: smtp
 Opaque Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 23
 Encrypted Application Data: 5e66d266ded88eb77940337fefbf0ceb75e5c7c171b80a
 ▶ TLSv1.3 Record Layer: Application Data Protocol: smtp
 ▶ TLSv1.3 Record Layer: Application Data Protocol: smtp
 ▶ TLSv1.3 Record Layer: Application Data Protocol: smtp

0030 01 fc 80 ed 00 00 01 01 08 0a 29 e3 ef 1a fe d8
 0040 4b 02 16 03 03 00 7a 02 00 00 76 03 03 b4 f1 6c K.....z...v...l
 0050 23 6f a5 6b 80 12 10 4b 85 c2 f8 ef dc 3f 29 8c #o.k...K.....?)
 0060 a1 27 67 8e d0 d1 22 d7 64 ec d4 ca 20 20 8c 39 .'g...". d... .9

The scaled window size (if scaling has been used) (tcp.window size), 2 bytes Packets: 162224 · Displayed: 953 (0.6%) Profile: Default

11. Encrypted IMAP - Wireshark

tcp.port == 993						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.319719532	64.5.53.201	64.5.53.204	TLSv1.2	94	Application Data
7	0.320172694	64.5.53.204	64.5.53.201	TLSv1.2	145	Application Data
8	0.320216134	64.5.53.201	64.5.53.204	TCP	66	57692 → 993 [ACK] Seq=29 Ack=80
9	0.320403702	64.5.53.201	64.5.53.204	TLSv1.2	99	Application Data
10	0.320687146	64.5.53.204	64.5.53.201	TLSv1.2	134	Application Data
11	0.320710470	64.5.53.201	64.5.53.204	TCP	66	57692 → 993 [ACK] Seq=62 Ack=148
12	0.323903336	64.5.53.201	64.5.53.204	TLSv1.2	99	Application Data
13	0.324276692	64.5.53.204	64.5.53.201	TLSv1.2	98	Application Data

▶ Frame 7: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface ens160, id 0
 ▶ Ethernet II, Src: Intersof_04:07:04 (00:02:30:04:07:04), Dst: VMware_86:46:31 (00:50:56:86:46:31)
 ▶ Internet Protocol Version 4, Src: 64.5.53.204, Dst: 64.5.53.201
 ▶ Transmission Control Protocol, Src Port: 993, Dst Port: 57692, Seq: 1, Ack: 29, Len: 79
 ▶ Transport Layer Security
 ▶ TLSv1.2 Record Layer: Application Data Protocol: imap
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 74
 Encrypted Application Data: 903f5d016de99f334cb0d83ae2f8c0dc6fbec542cbbdd5e7...