2. Capture the packet while sending and email.

➤ The Simple Mail Transfer Protocol (SMTP) is an application used by mail servers to send, receive, and relay outgoing email between senders and receivers. Enabling Telnet in Windows feature on and off is useful for capturing packets while sending an email because Telnet allows you to manually communicate with an email server using the Simple Mail Transfer Protocol (SMTP). This can be helpful for debugging and understanding the email sending process at a low level. • Telnet: Telnet is a network protocol used to provide a command-line interface for communication with remote devices or servers. • SMTP: SMTP is the protocol used to send emails across the Internet. By using Telnet, you can manually connect to an SMTP server and send commands directly to it. • Example: Using Telnet, you can type SMTP commands like HELO, MAIL FROM, RCPT TO, and DATA to manually send an email. This helps in understanding how email servers respond to different commands.

In Windows :

- **1st step** :- Search Turn on/off windows feature open it and find TELNET client and turn it on.

- **2nd step**: Open CMD and type (telnet smtp.gmail.com 587)

The command telnet smtp.gmail.com 587 is used to manually connect to Gmail's SMTP server using Telnet on port 587. Here's a breakdown of what each part of the command does: • telnet: This is the command to start the Telnet client, which allows you to communicate with remote servers using the Telnet protocol. • smtp.gmail.com: This is the address of Gmail's SMTP server, which is used to send emails. • 587: This is the port number for the SMTP server. Port 587 is commonly used for sending emails securely using the STARTTLS command to upgrade to an encrypted connection.

```
220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f318478sm19765055ad.154 - gsmtp
helo
501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection.
501 5.5.4  https://support.google.com/mail/?p=helo d9443c01a7336-1fd6f318478sm19765055ad.154 - gsmtp

Connection to host lost.

C:\Users\Ckdnw>_
```

This is the picture of cmd after building connection with google server using smtp……..

```
► Frame 83: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface \Device\NPF_{03381486-83EC-4EC6-BAD6-13BD82938993}, id 0
► Ethernet II, Src: 9e:c6:b8:de:19:3a (9e:c6:b8:de:19:3a), Dst: ChongqingFug_b0:26:45 (1c:bf:c0:b0:26:45)
► Internet Protocol Version 4, Src: 74.125.130.108, Dst: 192.168.119.182
► Transmission Control Protocol, Src Port: 587, Dst Port: 49850, Seq: 77, Ack: 7, Len: 171
▼ Simple Mail Transfer Protocol
   ▼ Response: 501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection.\r\n
      Response code: Syntax error in parameters or arguments (501)
      Response parameter: 5.5.4 Empty HELO/EHLO argument not allowed, closing connection.
      Response parameter: 5.5.4  https://support.google.com/mail/?p=helo d9443c01a7336-1fd6f318478sm19765055ad.154 - gsmtp
```

```
0000  1c bf c0 b0 26 45 9e c6  b8 de 19 3a 08 00 45 60   ····&E·· ···:··E`
0010  00 d3 12 8a 00 00 78 06  29 f3 4a 7d 82 6c c0 a8   ······x· )·J}·l··
0020  77 b6 02 4b c2 ba 3b 8a  cc 58 cb a9 89 a2 50 18   w··K··;· ·X···P·
0030  01 00 12 f3 00 00 35 30  31 2d 35 2e 35 2e 34 20   ······50 1-5.5.4
0040  45 6d 70 74 79 20 48 45  4c 4f 2f 45 48 4c 4f 20   Empty HE LO/EHLO
0050  61 72 67 75 6d 65 6e 74  20 6e 6f 74 20 61 6c 6c   argument  not all
0060  6f 77 65 64 2c 20 63 6c  6f 73 69 6e 67 20 63 6f   owed, cl osing co
0070  6e 6e 65 63 74 69 6f 6e  2e 0d 0a 35 30 31 20 35   nnection .··501 5
0080  2e 35 2e 34 20 20 68 74  74 70 73 3a 2f 2f 73 75   .5.4  ht tps://su
0090  70 70 6f 72 74 2e 67 6f  6f 67 6c 65 2e 63 6f 6d   pport.go ogle.com
00a0  2f 6d 61 69 6c 2f 3f 70  3d 68 65 6c 6f 20 64 39   /mail/?p =helo d9
00b0  34 34 33 63 30 31 61 37  33 33 36 2d 31 66 64 36   443c01a7 336-1fd6
00c0  66 33 31 38 34 37 38 73  6d 31 39 37 36 35 30 35   f318478s m1976505
00d0  35 61 64 2e 31 35 34 20  2d 20 67 73 6d 74 70 0d   5ad.154  - gsmtp·
00e0  0a                                                 ·
```

Capturing smtp….

```
220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f318478sm19765055ad.154 - gsmtp
helo
501-5.5.4 Empty HELO/EHLO argument not allowed, closing connection.
501 5.5.4  https://support.google.com/mail/?p=helo d9443c01a7336-1fd6f318478sm19765055ad.154 - gsmtp
```

Follow request of smtp… as cmd in wireshark.