

Capture Packets while sending a email. Dissect the packet sent.

- ⇒ Initially enable telnet on Microsoft features menu.
- ⇒ After that enter following command in command prompt, it makes connections to the smtp server.

```
C:\Users\nabin>telnet gmail-smtp-in.l.google.com 25|
```

- ⇒ Connection has build successfully and receive this message

```
220 mx.google.com ESMTP d9443c01a7336-20084d5c81dsi10021235ad.486 - gsmtpt
```

- ⇒ Now packet has been captured using wireshark

Simple Mail Transfer Protocol

- Response: 220 mx.google.com ESMTP d9443c01a7336-1ff58f42cf6si87975315ad.145 - gsmtpt\r\n
Response code: <domain> Service ready (220)
Response parameter: mx.google.com ESMTP d9443c01a7336-1ff58f42cf6si87975315ad.145 - gsmtpt

This packet is the response from google server showing it is ready. It has respond with the parameter and some encryption.

```
> Frame 158: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF_{F2BC7708-EE66-4425-A13C-41E5C818E7FD}, id 0
> Ethernet II, Src: ChongqingFug_00:d4:c9 (1c:bf:c0:00:d4:c9), Dst: TaicangT&WE1_fa:57:b0 (14:58:08:fa:57:b0)
> Internet Protocol Version 6, Src: 2400:1a00:b1e0:27bc:94e5:a2f8:e8be:3a50, Dst: 2404:6800:4003:c01::1a
> Transmission Control Protocol, Src Port: 55123, Dst Port: 25, Seq: 13, Ack: 76, Len: 2
> [13 Reassembled TCP Segments (14 bytes): #86(1), #89(1), #92(1), #94(1), #96(1), #98(1), #117(1), #131(1), #138(1), #143(1), #145(1), #152(1), #158(2)]
v Simple Mail Transfer Protocol
  v Line-based text data (1 lines)
    hello google\r\n
```

I have sent a message “hello google” to the server and it is captured in the packet.

These all the communication has been done using smtp.