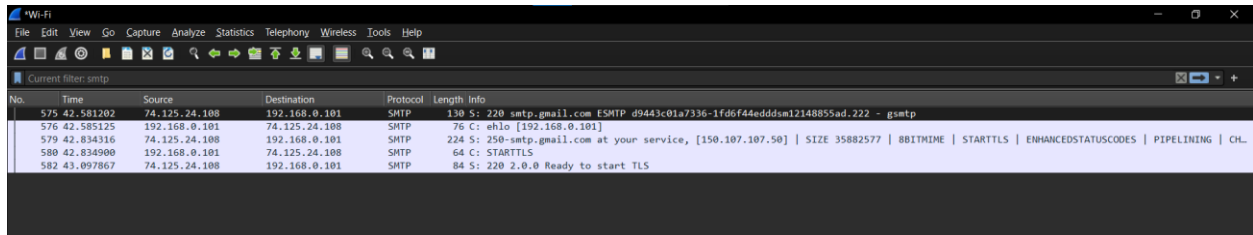


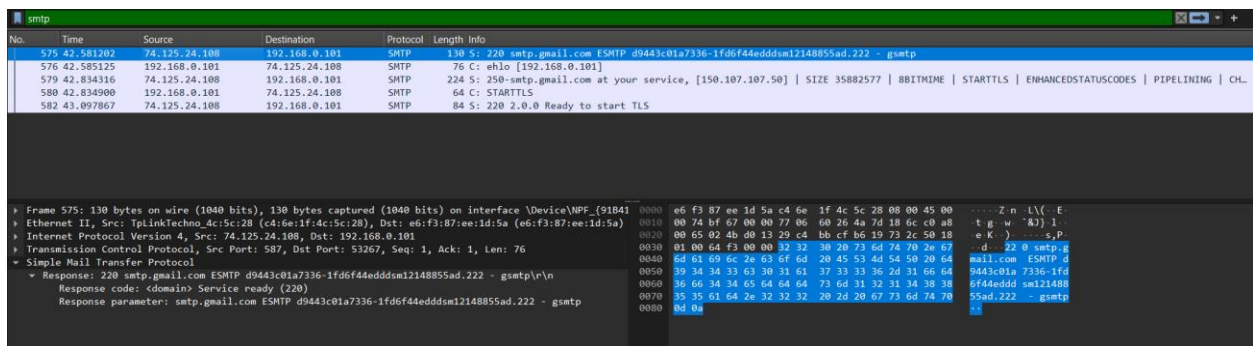
This experiment was done on Wireshark to capture a packet while sending an email.

Before any SMTP communication happens, a TCP connection is established between the client and the server. The SMTP server, upon accepting the TCP connection, sends a greeting message to the client.



No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130	S: 220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76	C: ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224	S: 250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CHL
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64	C: STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84	S: 220 2.0.0 Ready to start TLS

The packets were filtered using smtp filter and following packets were visible.



No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130	S: 220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76	C: ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224	S: 250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CHL
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64	C: STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84	S: 220 2.0.0 Ready to start TLS

Frame 575: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface \Device\NPF_{91841...}	0000	e6 f3 87 ee 1d 5a c4 6e 1f 4c 5c 28 08 00 45 00	-----Z n \X(E-
↳ Ethernet II, Src: TplinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28), Dst: e6:f3:87:ee:1d:5a (e6:f3:87:ee:1d:5a)	0010	00 74 bf 67 00 00 77 06 60 26 4a 7d 18 6c c0 a8	t g w '8j) 1 -
↳ Internet Protocol Version 4, Src: 74.125.24.108, Dst: 192.168.0.101	0020	00 65 02 4b 00 15 29 c4 bb cf b6 19 73 2c 5b 18	e K) c p-
↳ Transmission Control Protocol, Src Port: 587, Dst Port: 53267, Seq: 1, Ack: 1, Len: 76	0030	01 00 64 f3 00 00 32 32 30 20 73 6d 74 79 29 67	- d . 22 0 smtp g
↳ Simple Mail Transfer Protocol	0040	6d 61 69 6c 2e 63 6f 6d 20 45 53 4d 54 50 20 64	mail.com ESMTP d
↳ Response: 220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt\r\n	0050	39 34 34 33 63 30 31 61 37 33 33 36 2d 31 66 64	9443c01a 7336-1fd
Response code: <domain> Service ready (220)	0060	36 66 34 34 65 64 64 64 73 6d 31 32 31 34 39 38	644eddd sm121488
Response parameter: smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt	0070	35 35 61 64 2e 32 32 32 20 2d 20 67 73 6d 74 79	55ad.222 - gsmt
	0080	8d 0a	8d

This packet is part of an SMTP communication. The source is an IP address associated with Gmail's SMTP server (74.125.24.108) communicating with a device on a local network (192.168.0.101). The packet is a server response indicating that the SMTP server (smtp.gmail.com) is ready to accept a connection. The server sends a response code 220, which signifies that the service is ready.

No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130 S:	220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmtp
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76 C:	ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224 S:	250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CHUNKING
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64 C:	STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84 S:	220 2.0.0 Ready to start TLS

Frame 576: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF... Ethernet II, Src: e6:f3:87:ee:1d:5a (e6:f3:87:ee:1d:5a), Dst: TpLinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28) Internet Protocol Version 4, Src: 192.168.0.101, Dst: 74.125.24.108 Transmission Control Protocol, Src Port: 53267, Dst Port: 587, Seq: 1, Ack: 77, Len: 22 Simple Mail Transfer Protocol Command Line: ehlo [192.168.0.101]\r\n Command: ehlo Request parameter: [192.168.0.101]	0000 c4 6e 1f 4c 5c 28 e6 f3 87 ee 1d 5a 08 00 45 00 n \(\[...Z E. 0010 00 3e c7 6a 40 00 80 06 00 00 c0 a8 00 65 4a 7d > 30[...e7] 0020 18 6c d0 13 02 4b b6 19 73 2c 29 c4 bc 1b 50 18 1- C e,) P 0030 02 00 24 27 00 00 05 68 6c 6f 20 5b 31 39 32 2a - \$' 00 1c [192 0040 31 36 38 2e 30 2e 31 30 31 5d 0d 0a 168.0.10 1]-
---	---

This packet is part of an SMTP communication sequence, where the device with IP address 192.168.0.101 on a local network sends an ehlo command to the Gmail SMTP server (74.125.24.108) to initiate communication and request the server's capabilities. The ehlo command is used in SMTP to acknowledge the mail server and establish an extended SMTP session.

No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130 S:	220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmtp
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76 C:	ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224 S:	250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CH...
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64 C:	STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84 S:	220 2.0.0 Ready to start TLS

Frame 579: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF... Ethernet II, Src: TpLinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28), Dst: e6:f3:87:ee:1d:5a (e6:f3:87:ee:1d:5a) Internet Protocol Version 4, Src: 74.125.24.108, Dst: 192.168.0.101 Transmission Control Protocol, Src Port: 587, Dst Port: 53267, Seq: 77, Ack: 23, Len: 170 Simple Mail Transfer Protocol Response: 250-smtp.gmail.com at your service, [150.107.107.50]\r\n Response code: Requested mail action okay, completed (250) Response parameter: smtp.gmail.com at your service, [150.107.107.50] Response parameter: SIZE 35882577 Response parameter: 8BITMIME Response parameter: STARTTLS Response parameter: ENHANCEDSTATUSCODES Response parameter: PIPELINING Response parameter: CHUNKING Response parameter: SMTPUTF8	0000 e6 f3 87 ee 1d 5a c4 6e 1f 4c 5c 28 08 00 45 00Z n \(\[E. 0010 00 d2 bf 69 00 00 77 06 5f c6 4a 7d 18 6c c0 a8 ...i w _]) 1- 0020 00 65 02 4b d0 13 29 c4 bc 1b b6 19 73 42 50 18 e K) - aBP 0030 01 00 2e fd 00 00 32 35 30 2d 73 6f 74 70 2e 6f 25 0-smtp.g 0040 6d 61 69 6c 2e 63 6f 6d 20 61 74 20 79 6f 75 72 mail.com at your 0050 20 73 65 72 76 69 63 65 2c 20 5b 31 35 30 2e 31 service, [150.1 0060 30 37 2e 31 30 37 2e 35 30 5d 0d 0a 32 35 30 2d 07.107.5 0]-250- 0070 53 49 5a 45 20 33 35 38 38 32 35 37 0d 0a 32 SIZE 358 82577--2 0080 35 30 2d 38 42 49 54 4d 49 4d 45 0d 0a 32 35 30 50-8BITM IME-250 0090 2d 53 54 41 52 54 54 4c 53 0d 0a 32 35 30 2d 45 -STARTTL S--250-E 00a0 4e 48 41 4e 43 45 44 53 54 41 5a 55 53 43 4f 44 ENHANCED STATUSCOD 00b0 45 53 0d 0a 32 35 30 2d 50 49 50 45 4c 49 4a 49 ES--250- PIPELINI 00c0 4e 47 0d 0a 32 35 30 2d 43 48 55 4e 4b 49 4a 47 HG--250- CHUNKING 00d0 0d 0a 32 35 30 20 53 4d 54 50 55 54 46 38 0d 0a --250 SM TPUTF8-
--	---

The Gmail SMTP server (74.125.24.108) is responding to the ehlo command sent by the device with IP address 192.168.0.101. The server responds with a 250 response code, indicating that the requested mail action is okay and completed.

Following are the response parameters:

SIZE 35882577: The maximum message size the server is willing to accept.

8BITMIME: Indicates support for 8-bit MIME encoding.

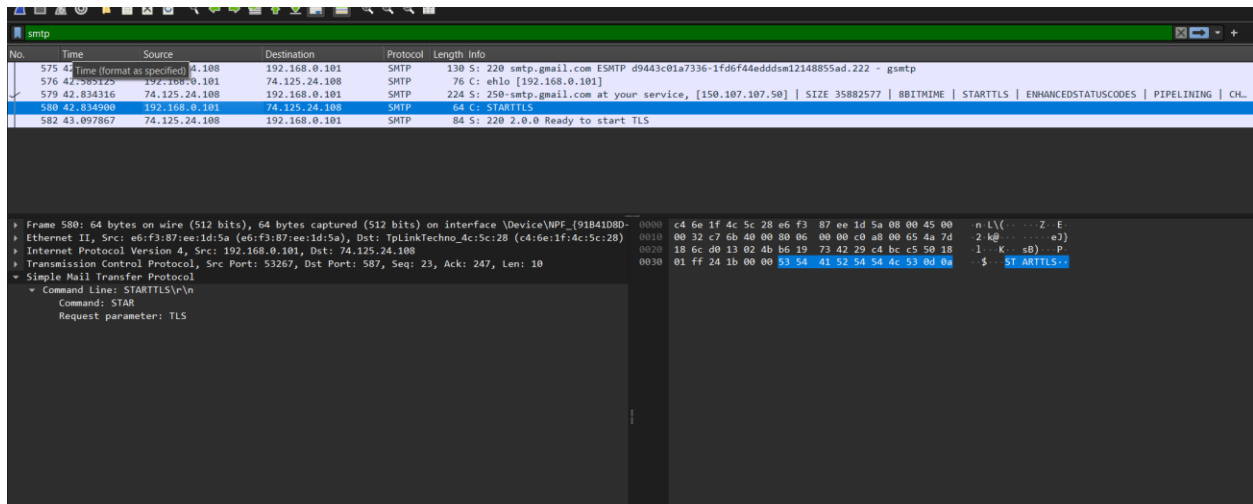
STARTTLS: Indicates support for upgrading to a secure connection using TLS.

ENHANCEDSTATUSCODES: Indicates support for enhanced status codes.

PIPELINING: Indicates support for command pipelining, allowing multiple commands to be sent without waiting for individual responses.

CHUNKING: Indicates support for the BDAT command, which allows the message to be sent in chunks.

SMTPUTF8: Indicates support for the SMTPUTF8 extension, allowing UTF-8 encoding in email addresses and headers.



The image shows a Wireshark packet capture of an SMTP session. The packet list on the left shows five packets. Packet 580, at time 42.834900, is an SMTP packet from 192.168.0.101 to 74.125.24.108, containing the command '64 C: STARTTLS'. The packet details pane on the right shows the 'Simple Mail Transfer Protocol' section expanded, displaying the command line 'STARTTLS\r\n' and the request parameter 'TLS'. The packet bytes pane on the right shows the raw data, with the ASCII column displaying 'S T A R T T L S'.

No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130	S: 220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76	C: ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224	S: 250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CHL
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64	C: STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84	S: 220 2.0.0 Ready to start TLS

Frame 580: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{91B41D80-...} (c4:6e:1f:4c:5c:28) on interface \Device\NPF_{91B41D80-...} (c4:6e:1f:4c:5c:28)

Ethernet II, Src: TpLinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28), Dst: TpLinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28)

Internet Protocol Version 4, Src: 192.168.0.101, Dst: 74.125.24.108

Transmission Control Protocol, Src Port: 53267, Dst Port: 587, Seq: 23, Ack: 247, Len: 10

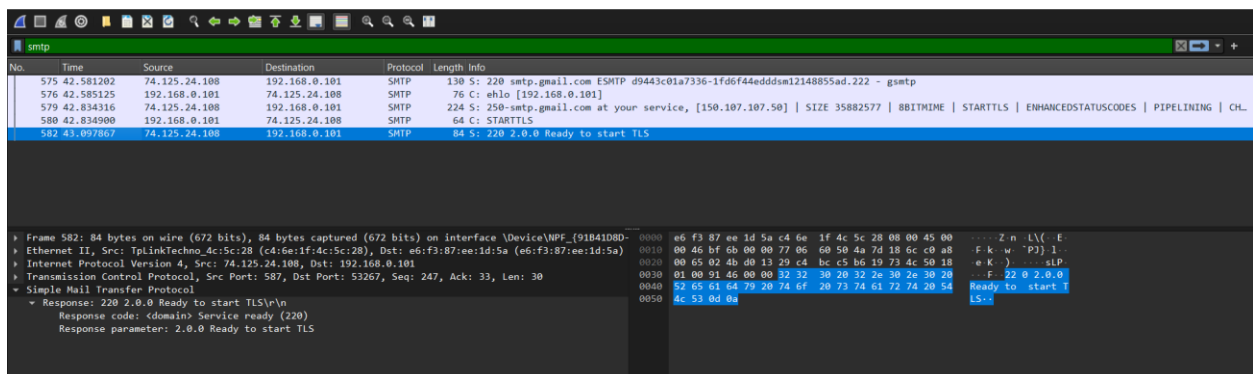
Simple Mail Transfer Protocol

Command Line: STARTTLS\r\n

Command: START

Request parameter: TLS

The device with IP address 192.168.0.101 on a local network sends a STARTTLS command to the Gmail SMTP server (74.125.24.108). The STARTTLS command is used to initiate a secure connection by upgrading the current plain text connection to an encrypted one using TLS.



The image shows a Wireshark packet capture of an SMTP session. The packet list on the left shows five packets. Packet 582, at time 43.097867, is an SMTP packet from 74.125.24.108 to 192.168.0.101, containing the response '84 S: 220 2.0.0 Ready to start TLS'. The packet details pane on the right shows the 'Simple Mail Transfer Protocol' section expanded, displaying the response code '220' and the response parameter '2.0.0 Ready to start TLS'. The packet bytes pane on the right shows the raw data, with the ASCII column displaying '2 2 0 2 . 0 . 0 R e a d y t o s t a r t T L S'.

No.	Time	Source	Destination	Protocol	Length	Info
575	42.581202	74.125.24.108	192.168.0.101	SMTP	130	S: 220 smtp.gmail.com ESMTP d9443c01a7336-1fd6f44edddsm12148855ad.222 - gsmt
576	42.585125	192.168.0.101	74.125.24.108	SMTP	76	C: ehlo [192.168.0.101]
579	42.834316	74.125.24.108	192.168.0.101	SMTP	224	S: 250-smtp.gmail.com at your service, [150.107.107.50] SIZE 35882577 8BITMIME STARTTLS ENHANCEDSTATUSCODES PIPELINING CHL
580	42.834900	192.168.0.101	74.125.24.108	SMTP	64	C: STARTTLS
582	43.097867	74.125.24.108	192.168.0.101	SMTP	84	S: 220 2.0.0 Ready to start TLS

Frame 582: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{91B41D80-...} (c4:6e:1f:4c:5c:28) on interface \Device\NPF_{91B41D80-...} (c4:6e:1f:4c:5c:28)

Ethernet II, Src: TpLinkTechno_4c:5c:28 (c4:6e:1f:4c:5c:28), Dst: e6:f3:87:ee:1d:5a (e6:f3:87:ee:1d:5a)

Internet Protocol Version 4, Src: 74.125.24.108, Dst: 192.168.0.101

Transmission Control Protocol, Src Port: 587, Dst Port: 53267, Seq: 247, Ack: 33, Len: 30

Simple Mail Transfer Protocol

Response: 220 2.0.0 Ready to start TLS\r\n

Response code: (domain) Service ready (220)

Response parameter: 2.0.0 Ready to start TLS

The Gmail SMTP server (74.125.24.108) responds to the STARTTLS command sent by the device with IP address 192.168.0.101. The server responds with a 220 response code, indicating that it is ready to start TLS encryption.