Gmail Packet Analysis

Introduction

This report presents a detail analysis of network packets captured during the process of sending an email via Gmail's web interface. The experiment was conducted using Wireshark focusing on the details of the captured packets without applying specific filters but by searching for mail.google.com.

Overview of Captured Packet

311 7.504468 192.168.1.183 142.250.182.5 TLSv1.3 886 Client Hello (SNI=mail.google.com)

Fig: Packet

```
0010
                 13
             e0
97
9929
                                    21 9b 73
a3 a0 24
                 b9 00 00 2e
                                3Ь
                                               63
                                                   4d
0030
          03
9949
0050
          39 85
                                               dØ 5b
0070
             fa
                 9d 07
                                       47 Ød cØ 3c
26 91 Ø5 9b
0080
          98
0090
                 93
                                               66
00a0
                                                   50
             9a b7
b4 db
                                               22
b3
eebe
                 db 60
                                        08 87
                                                   84
00c0
                                            12
                                                   d1
00d0
                                               a8
00e0
                                           8b 0c
             20
                 89
                                               1d
0100
                     bd
                                           21 ae
                 1b 7b
                                     8b 2d 8a
0110
              Ød
                                               1d 27
0120
             8b b9 54
                                               38 28
                                        04 19
0130
                 c8 6d
9149
             19
                                               30 6b
          d5
0150
          e0
                 f6 83
                                               48
                                                   1d
                                                      32 00 1d
0160
          20
                 8d
                                           dd
                                               5d
0170
              89
0190
          69
                                        00 7a 7a 00
34 c7 14 e2
          02 01
                 01
                     00 0b 00
                                                      01
01a0
01b0
                 01 9e
             c3
                 83 f1
             58
01c0
             4b
01d0
                 21
01e0
                 6a
                     c8
                                        34 67 47
                                               46
0200
0210
      5d e0 ac 09 da
                                     10
                                           be
                                                      bd 35
0220
          2a 10 74 53 da
                                     5d
          d0
```

Figure 2: Frame

Overview of Captured Packet

> Frame Number: 311

Bytes on Wire: 886 (7088 bits)Capture Interface: en0, id 0

> Ethernet Source: 5e:ba:2e:5e:ed:3c

➤ Destination: TaicangT&WEl 00:84:20(ac:37:28:00:84:20)

> Source IP: 192.168.1.183

> Destination IP: 142.250.182.5

➤ Protocol: TCP

➤ Source Port: 57363

➤ Destination Port: 443 (HTTPS)

Detailed IPV4 Header Analysis

The IPV4 header captured contains the below information:

Field	Value	Description
Version	4	IPv4
Header Length	20 bytes (5)	Standard IPv4 header length
Differentiated Services Field	0x00	DSCP: CS0, ECN: Not-ECT
Total Length	872	Total IP packet length
Identification	0x6cd4 (27860)	Packet identifier
Flags	0x2	Don't fragment flag set
Fragment Offset	0	No fragmentation
Time to Live	128	Maximum hop count
Protocol	TCP (6)	Transport layer protocol
Header Checksum	0x835c	Validation disabled
Source Address	192.168.1.183	Sender's IP address
Destination Address	142.250.182.5	Recipient's IP address (Google
server)		

TCP Header Information

Field	Value
Source Port	57363
Destination Port	443
Sequence Number	1413
Acknowledgment Number	1
Flags	PSH, ACK
window Size	66304
Urgent Pointer	0

TLS Handshake Analysis

The packet capture reveals the initiation of a TLS handshake:

➤ Client Hello: SNI (Server Name Indication): mail.google.com

> TLS Version: TLS 1.3

➤ Cipher Suites: [List of supported cipher suites]

> Server Hello: Selected Cipher Suite: [Specific cipher suite]

> TLS Version: TLS 1.3

Conclusion

In conclusion, this report provided a detailed analysis of captured packet while sending an email via Gmail's web interface. It highlighted the use of HTTPS for secure communication, the details of IPv4 and TCP header with explanation of their header field.