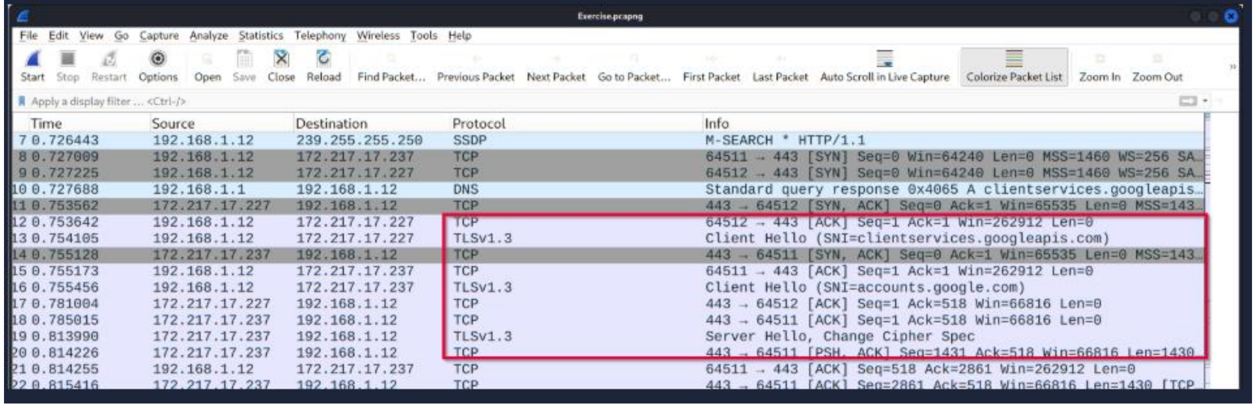
WIRESHARK

Encrypted Protocol Analysis: Decrypting HTTPS Write Up

- Sometime, malicious activity is also done in HTTPS (Hypertext Transfer Protocol Secure)
- HTTPS encrypts the data while it is being transferred to the network.
- Without having the encryption and decryption pairs, it will be difficult to read what is being transferred.

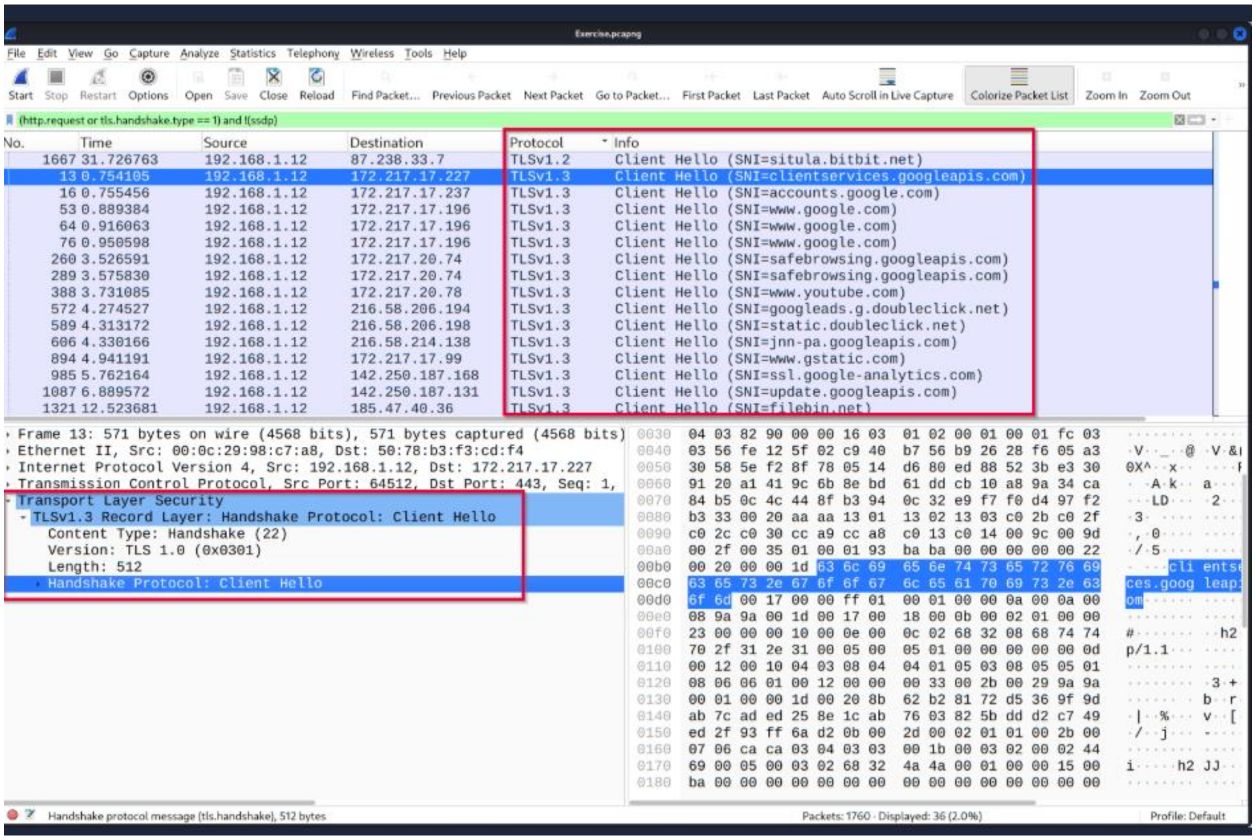
Notes	Wireshark Filter
"HTTPS Parameters" for grabbing the low-hanging fruits:	
• **Request:** Listing all requests	• `http.request`
• **TLS:** Global TLS search	• `tls`
• TLS Client Request	• `tls.handshake.type == 1`
• TLS Server response	• `tls.handshake.type == 2`
• Local Simple Service Discovery Protocol (SSDP)	• `ssdp`
Note: SSDP is a network protocol that provides advertisement and discovery of network services.	


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out
Apply a display filter ... <Ctrl-/>

```
   Time      Source          Destination      Protocol  Info
 7 0.726443  192.168.1.12    239.255.255.250  SSDP      M-SEARCH * HTTP/1.1
 8 0.727009  192.168.1.12    172.217.17.237   TCP       64511 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA…
 9 0.727225  192.168.1.12    172.217.17.227   TCP       64512 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA…
10 0.727688  192.168.1.1     192.168.1.12     DNS       Standard query response 0x4065 A clientservices.googleapis…
11 0.753562  172.217.17.227  192.168.1.12     TCP       443 → 64512 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=143…
12 0.753642  192.168.1.12    172.217.17.227   TCP       64512 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
13 0.754105  192.168.1.12    172.217.17.227   TLSv1.3   Client Hello (SNI=clientservices.googleapis.com)
14 0.755128  172.217.17.237  192.168.1.12     TCP       443 → 64511 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=143…
15 0.755173  192.168.1.12    172.217.17.237   TCP       64511 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
16 0.755456  192.168.1.12    172.217.17.237   TLSv1.3   Client Hello (SNI=accounts.google.com)
17 0.781004  172.217.17.227  192.168.1.12     TCP       443 → 64512 [ACK] Seq=1 Ack=518 Win=66816 Len=0
18 0.785015  172.217.17.237  192.168.1.12     TCP       443 → 64511 [ACK] Seq=1 Ack=518 Win=66816 Len=0
19 0.813990  172.217.17.237  192.168.1.12     TLSv1.3   Server Hello, Change Cipher Spec
20 0.814226  172.217.17.237  192.168.1.12     TCP       443 → 64511 [PSH, ACK] Seq=1431 Ack=518 Win=66816 Len=1430…
21 0.814255  192.168.1.12    172.217.17.237   TCP       64511 → 443 [ACK] Seq=518 Ack=2861 Win=262912 Len=0
22 0.815416  172.217.17.237  192.168.1.12     TCP       443 → 64511 [ACK] Seq=2861 Ack=518 Win=66816 Len=1430 [TCP…
```

- Like a TCP three-way-handshake, a TLS also has handshakes between the client and the server.

- Client Hello: (http.request or tls.handshake.type ==1) and !(ssdp) <--- this is to filter the start of the conversation between the client and the server for both unencrypted (http) and encrypted web traffic (https) and ignores the ssdp (Simple Service Discovery Protocol) that is used by devices such as smart tv's, printers, routers , etc.
- Server Hello: (http.request or tls.handshake.type ==2) and !(ssdp) <--- this is to filter out responses from the server during an unencrypted or an encrypted connection. This allows us to see the communication of a connection by capturing the client's intent for http or the server response for the TLS.


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out

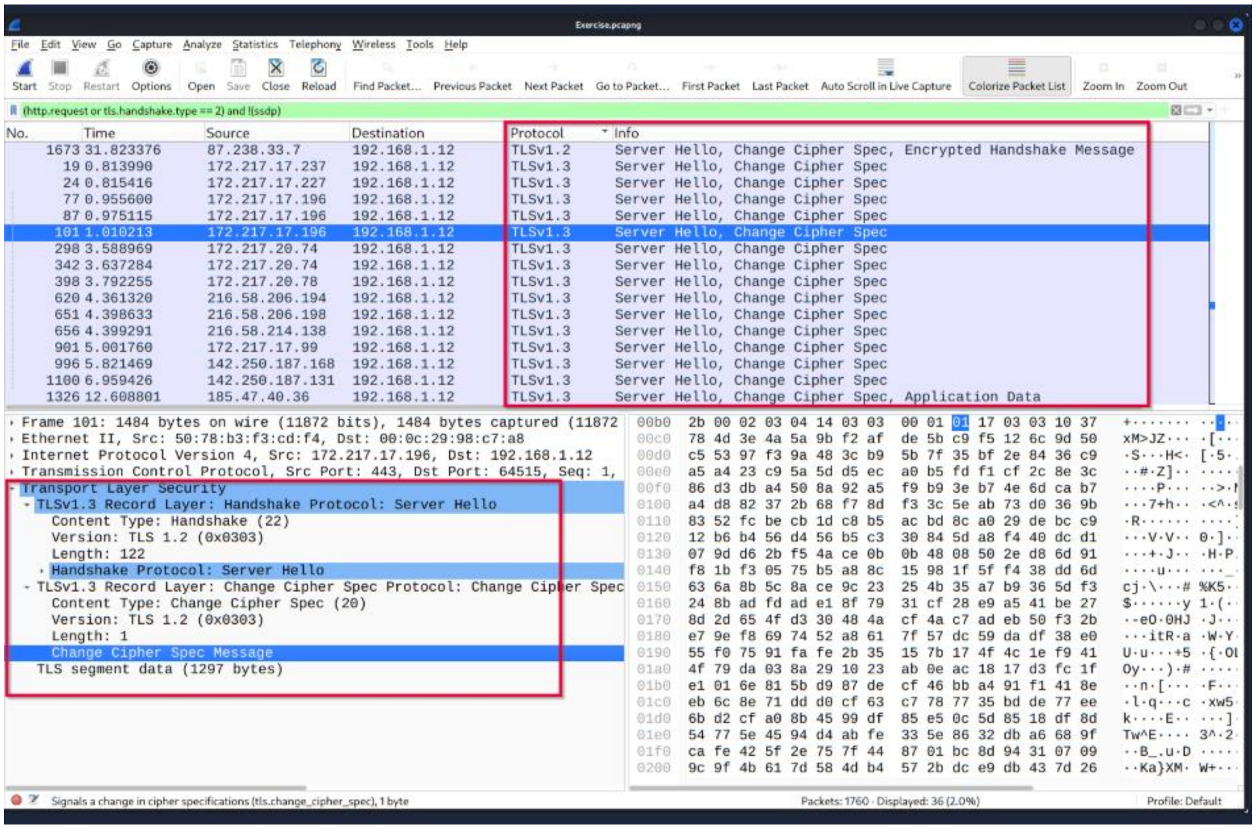
(http.request or tls.handshake.type == 1) and !(ssdp)

```
No.   Time       Source        Destination      Protocol  Info
 1667 31.726763  192.168.1.12  87.238.33.7      TLSv1.2   Client Hello (SNI=situla.bitbit.net)
   13 0.754105   192.168.1.12  172.217.17.227   TLSv1.3   Client Hello (SNI=clientservices.googleapis.com)
   16 0.755456   192.168.1.12  172.217.17.237   TLSv1.3   Client Hello (SNI=accounts.google.com)
   53 0.889384   192.168.1.12  172.217.17.196   TLSv1.3   Client Hello (SNI=www.google.com)
   64 0.916063   192.168.1.12  172.217.17.196   TLSv1.3   Client Hello (SNI=www.google.com)
   76 0.950598   192.168.1.12  172.217.17.196   TLSv1.3   Client Hello (SNI=www.google.com)
  260 3.526591   192.168.1.12  172.217.20.74    TLSv1.3   Client Hello (SNI=safebrowsing.googleapis.com)
  289 3.575830   192.168.1.12  172.217.20.74    TLSv1.3   Client Hello (SNI=safebrowsing.googleapis.com)
  388 3.731085   192.168.1.12  172.217.20.78    TLSv1.3   Client Hello (SNI=www.youtube.com)
  572 4.274527   192.168.1.12  216.58.206.194   TLSv1.3   Client Hello (SNI=googleads.g.doubleclick.net)
  589 4.313172   192.168.1.12  216.58.206.198   TLSv1.3   Client Hello (SNI=static.doubleclick.net)
  606 4.330166   192.168.1.12  216.58.214.138   TLSv1.3   Client Hello (SNI=jnn-pa.googleapis.com)
  894 4.941191   192.168.1.12  172.217.17.99    TLSv1.3   Client Hello (SNI=www.gstatic.com)
  985 5.762164   192.168.1.12  142.250.187.168  TLSv1.3   Client Hello (SNI=ssl.google-analytics.com)
 1087 6.889572   192.168.1.12  142.250.187.131  TLSv1.3   Client Hello (SNI=update.googleapis.com)
 1321 12.523681  192.168.1.12  185.47.40.36     TLSv1.3   Client Hello (SNI=filebin.net)
```

```
› Frame 13: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
› Ethernet II, Src: 00:0c:29:98:c7:a8, Dst: 50:78:b3:f3:cd:f4
› Internet Protocol Version 4, Src: 192.168.1.12, Dst: 172.217.17.227
› Transmission Control Protocol, Src Port: 64512, Dst Port: 443, Seq: 1,
⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    › Handshake Protocol: Client Hello
```

```
0030  04 03 82 90 00 00 16 03  01 02 00 01 00 01 fc 03
0040  03 56 fe 12 5f 02 c9 40  b7 56 b9 26 28 f6 05 a3   ·V·_·@ ·V·&(
0050  30 58 5e f2 8f 78 05 14  d6 80 ed 88 52 3b e3 30   0X^··x··
0060  91 20 a1 41 9c 6b 8e bd  61 dd cb 10 a8 9a 34 ca   ··A·k·· a
0070  84 b5 0c 4c 44 8f b3 94  0c 32 e9 f7 f0 d4 97 f2   ···LD··· ·2
0080  b3 33 00 20 aa aa 13 01  13 02 13 03 c0 2b c0 2f   ·3
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0
00a0  00 2f 00 35 01 00 01 93  ba ba 00 00 00 00 00 22   ·/·5
00b0  00 20 00 00 1d 63 6c 69  65 6e 74 73 65 72 76 69   ·····cli entse
00c0  63 65 73 2e 67 6f 6f 67  6c 65 61 70 69 73 2e 63   ces.goog leap
00d0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 0a 00   om
00e0  08 9a 9a 00 1d 00 17 00  18 00 0b 00 02 01 00 00
00f0  23 00 00 00 10 00 0e 00  0c 02 68 32 08 68 74 74   #········ ·h2
0100  70 2f 31 2e 31 00 05 00  05 01 00 00 00 00 00 0d   p/1.1
0110  00 12 00 10 04 03 08 04  04 01 05 03 08 05 05 01
0120  08 06 06 01 00 12 00 00  00 33 00 2b 00 29 9a 9a   ·3·+
0130  00 01 00 00 1d 00 20 8b  62 b2 81 72 d5 36 9f 9d   b··r
0140  ab 7c ad ed 25 8e 1c ab  76 03 82 5b dd d2 c7 49   ·|·%··· v··[
0150  ed 2f 93 ff 6a d2 0b 00  2d 00 02 01 01 00 2b 00   ·/··j··· -
0160  07 06 ca ca 03 04 03 03  00 1b 00 03 02 00 02 44
0170  69 00 05 00 03 02 68 32  4a 4a 00 01 00 00 15 00   i····h2 JJ
0180  ba 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Handshake protocol message (tls.handshake), 512 bytes   Packets: 1760 · Displayed: 36 (2.0%)   Profile: Default


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet… Previous Packet Next Packet Go to Packet… First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out

```
(http.request or tls.handshake.type == 2) and !(ssdp)

No.   Time       Source           Destination   Protocol  Info
 1673 31.823376  87.238.33.7      192.168.1.12  TLSv1.2   Server Hello, Change Cipher Spec, Encrypted Handshake Message
   19 0.813990   172.217.17.237   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
   24 0.815416   172.217.17.227   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
   77 0.955600   172.217.17.196   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
   87 0.975115   172.217.17.196   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  101 1.010213   172.217.17.196   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  298 3.588969   172.217.20.74    192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  342 3.637284   172.217.20.74    192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  398 3.792255   172.217.20.78    192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  620 4.361320   216.58.206.194   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  651 4.398633   216.58.206.198   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  656 4.399291   216.58.214.138   192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  901 5.001760   172.217.17.99    192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
  996 5.821469   142.250.187.168  192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
 1100 6.959426   142.250.187.131  192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec
 1326 12.608801  185.47.40.36     192.168.1.12  TLSv1.3   Server Hello, Change Cipher Spec, Application Data
```

```
› Frame 101: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872
› Ethernet II, Src: 50:78:b3:f3:cd:f4, Dst: 00:0c:29:98:c7:a8
› Internet Protocol Version 4, Src: 172.217.17.196, Dst: 192.168.1.12
› Transmission Control Protocol, Src Port: 443, Dst Port: 64515, Seq: 1,
˅ Transport Layer Security
  ˅ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    › Handshake Protocol: Server Hello
  ˅ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  TLS segment data (1297 bytes)
```

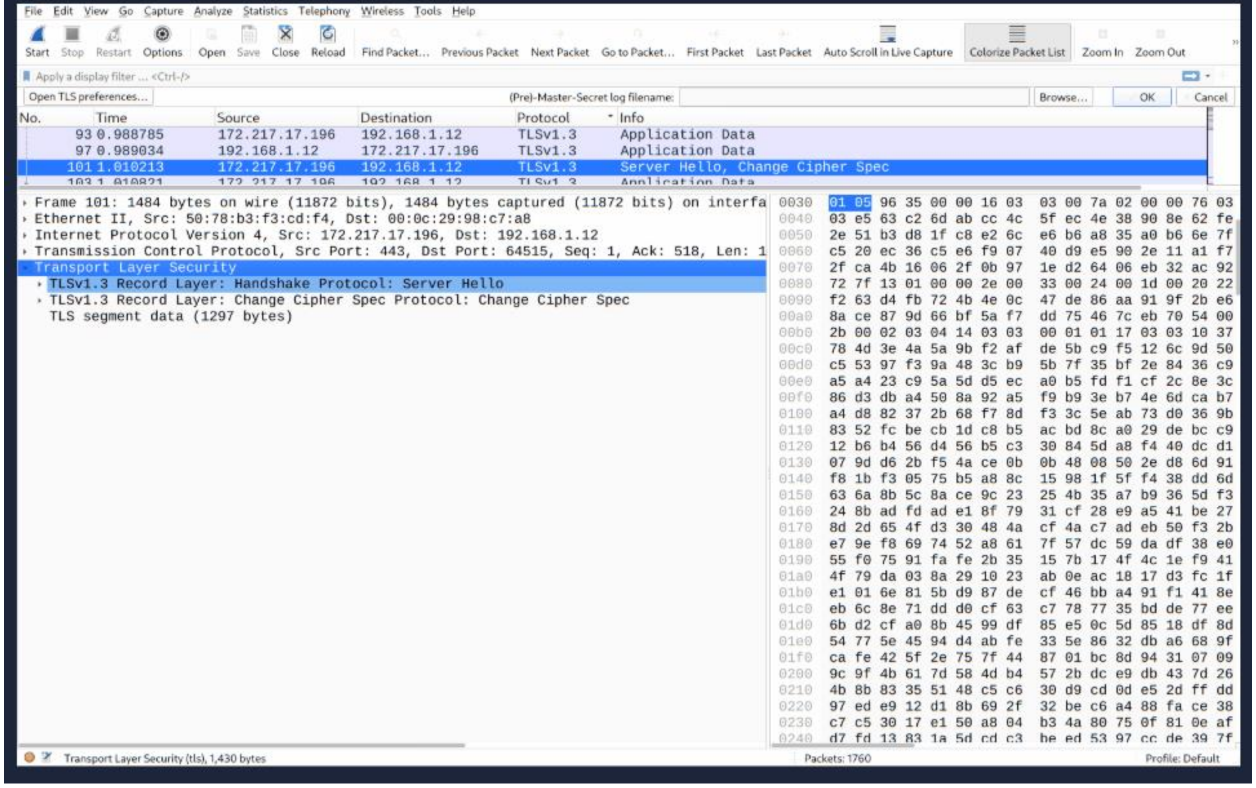
```
00b0  2b 00 02 03 04 14 03 03  00 01 01 17 03 03 10 37   +·······  ·····
00c0  78 4d 3e 4a 5a 9b f2 af  de 5b c9 f5 12 6c 9d 50   xM>JZ···  ·[···
00d0  c5 53 97 f3 9a 48 3c b9  5b 7f 35 bf 2e 84 36 c9   ·S···H<·  [·5·
00e0  a5 a4 23 c9 5a 5d d5 ec  a0 b5 fd f1 cf 2c 8e 3c   ··#·Z]··  ····
00f0  86 d3 db a4 50 8a 92 a5  f9 b9 3e b7 4e 6d ca b7   ····P···  ··>·
0100  a4 d8 82 37 2b 68 f7 8d  f3 3c 5e ab 73 d0 36 9b   ···7+h··  ·<^·
0110  83 52 fc be cb 1d c8 b5  ac bd 8c a0 29 de bc c9   ·R······  ····
0120  12 b6 b4 56 d4 56 b5 c3  30 84 5d a8 f4 40 dc d1   ···V·V··  0·]·
0130  07 9d d6 2b f5 4a ce 0b  0b 48 08 50 2e d8 6d 91   ···+·J··  ·H·P
0140  f8 1b f3 05 75 b5 a8 8c  15 98 1f 5f f4 38 dd 6d   ····u···  ···_
0150  63 6a 8b 5c 8a ce 9c 23  25 4b 35 a7 b9 36 5d f3   cj·\···#  %K5·
0160  24 8b ad fd ad e1 8f 79  31 cf 28 e9 a5 41 be 27   $······y  1·(·
0170  8d 2d 65 4f d3 30 48 4a  cf 4a c7 ad eb 50 f3 2b   ·-eO·0HJ  ·J··
0180  e7 9e f8 69 74 52 a8 61  7f 57 dc 59 da df 38 e0   ···itR·a  ·W·Y
0190  55 f0 75 91 fa fe 2b 35  15 7b 17 4f 4c 1e f9 41   U·u···+5  ·{·OL
01a0  4f 79 da 03 8a 29 10 23  ab 0e ac 18 17 d3 fc 1f   Oy···)·#  ····
01b0  e1 01 6e 81 5b d9 87 de  cf 46 bb a4 91 f1 41 8e   ··n·[···  ·F··
01c0  eb 6c 8e 71 dd d0 cf 63  c7 78 77 35 bd de 77 ee   ·l·q···c  ·xw5
01d0  6b d2 cf a0 8b 45 99 df  85 e5 0c 5d 85 18 df 8d   k····E··  ···]
01e0  54 77 5e 45 94 d4 ab fe  33 5e 86 32 db a6 68 9f   Tw^E····  3^·2
01f0  ca fe 42 5f 2e 75 7f 44  87 01 bc 8d 94 31 07 09   ··B_.u·D  ····
0200  9c 9f 4b 61 7d 58 4d b4  57 2b dc e9 db 43 7d 26   ··Ka}XM·  W+··
```

Signals a change in cipher specifications (tls.change_cipher_spec), 1 byte   Packets: 1760 · Displayed: 36 (2.0%)   Profile: Default

Encrypted Key Log Files

- It is a text file that has unique key pairs to decrypt the encrypted traffic session.
- These key pairs are automatically created when a connection is established with an SSL/TLS-enabled webpage.

Adding key log files with the "right-click" menu:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet… Previous Packet Next Packet Go to Packet… First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out
Apply a display filter … <Ctrl-/>
Open TLS preferences…
Browse…
OK
Cancel

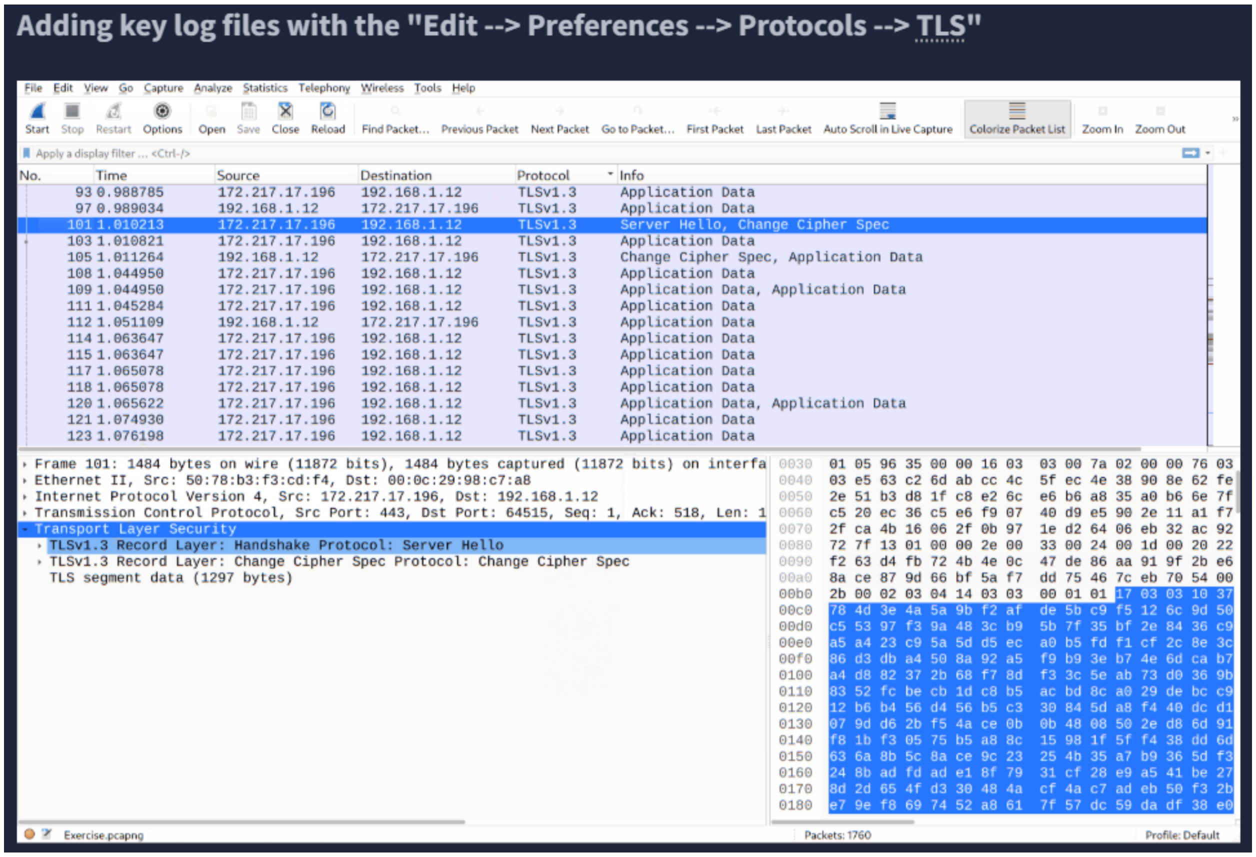
(Pre)-Master-Secret log filename:

```
No.   Time        Source          Destination     Protocol  Info
   93 0.988785    172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   97 0.989034    192.168.1.12    172.217.17.196  TLSv1.3   Application Data
  101 1.010213    172.217.17.196  192.168.1.12    TLSv1.3   Server Hello, Change Cipher Spec
  103 1.010821    172.217.17.196  192.168.1.12    TLSv1.3   Application Data
```

```
› Frame 101: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interfa
› Ethernet II, Src: 50:78:b3:f3:cd:f4, Dst: 00:0c:29:98:c7:a8
› Internet Protocol Version 4, Src: 172.217.17.196, Dst: 192.168.1.12
› Transmission Control Protocol, Src Port: 443, Dst Port: 64515, Seq: 1, Ack: 518, Len: 1
⌄ Transport Layer Security
  › TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  › TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    TLS segment data (1297 bytes)
```

```
0030  01 05 96 35 00 00 16 03  03 00 7a 02 00 00 76 03
0040  03 e5 63 c2 6d ab cc 4c  5f ec 4e 38 90 8e 62 fe
0050  2e 51 b3 d8 1f c8 e2 6c  e6 b6 a8 35 a0 b6 6e 7f
0060  c5 20 ec 36 c5 e6 f9 07  40 d9 e5 90 2e 11 a1 f7
0070  2f ca 4b 16 06 2f 0b 97  1e d2 64 06 eb 32 ac 92
0080  72 7f 13 01 00 00 2e 00  33 00 24 00 1d 00 20 22
0090  f2 63 d4 fb 72 4b 4e 0c  47 de 86 aa 91 9f 2b e6
00a0  8a ce 87 9d 66 bf 5a f7  dd 75 46 7c eb 70 54 00
00b0  2b 00 02 03 04 14 03 03  00 01 01 17 03 03 10 37
00c0  78 4d 3e 4a 5a 9b f2 af  de 5b c9 f5 12 6c 9d 50
00d0  c5 53 97 f3 9a 48 3c b9  5b 7f 35 bf 2e 84 36 c9
00e0  a5 a4 23 c9 5a 5d d5 ec  a0 b5 fd f1 cf 2c 8e 3c
00f0  86 d3 db a4 50 8a 92 a5  f9 b9 3e b7 4e 6d ca b7
0100  a4 d8 82 37 2b 68 f7 8d  f3 3c 5e ab 73 d0 36 9b
0110  83 52 fc be cb 1d c8 b5  ac bd 8c a0 29 de bc c9
0120  12 b6 b4 56 d4 56 b5 c3  30 84 5d a8 f4 40 dc d1
0130  07 9d d6 2b f5 4a ce 0b  0b 48 08 50 2e d8 6d 91
0140  f8 1b f3 05 75 b5 a8 8c  15 98 1f 5f f4 38 dd 6d
0150  63 6a 8b 5c 8a ce 9c 23  25 4b 35 a7 b9 36 5d f3
0160  24 8b ad fd ad e1 8f 79  31 cf 28 e9 a5 41 be 27
0170  8d 2d 65 4f d3 30 48 4a  cf 4a c7 ad eb 50 f3 2b
0180  e7 9e f8 69 74 52 a8 61  7f 57 dc 59 da df 38 e0
0190  55 f0 75 91 fa fe 2b 35  15 7b 17 4f 4c 1e f9 41
01a0  4f 79 da 03 8a 29 10 23  ab 0e ac 18 17 d3 fc 1f
01b0  e1 01 6e 81 5b d9 87 de  cf 46 bb a4 91 f1 41 8e
01c0  eb 6c 8e 71 dd d0 cf 63  c7 78 77 35 bd de 77 ee
01d0  6b d2 cf a0 8b 45 99 df  85 e5 0c 5d 85 18 df 8d
01e0  54 77 5e 45 94 d4 ab fe  33 5e 86 32 db a6 68 9f
01f0  ca fe 42 5f 2e 75 7f 44  87 01 bc 8d 94 31 07 09
0200  9c 9f 4b 61 7d 58 4d b4  57 2b dc e9 db 43 7d 26
0210  4b 8b 83 35 51 48 c5 c6  30 d9 cd 0d e5 2d ff dd
0220  97 ed e9 12 d1 8b 69 2f  32 be c6 a4 88 fa ce 38
0230  c7 c5 30 17 e1 50 a8 04  b3 4a 80 75 0f 81 0e af
0240  d7 fd 13 83 1a 5d cd c3  be ed 53 97 cc de 39 7f
```

Transport Layer Security (tls), 1,430 bytes   Packets: 1760   Profile: Default



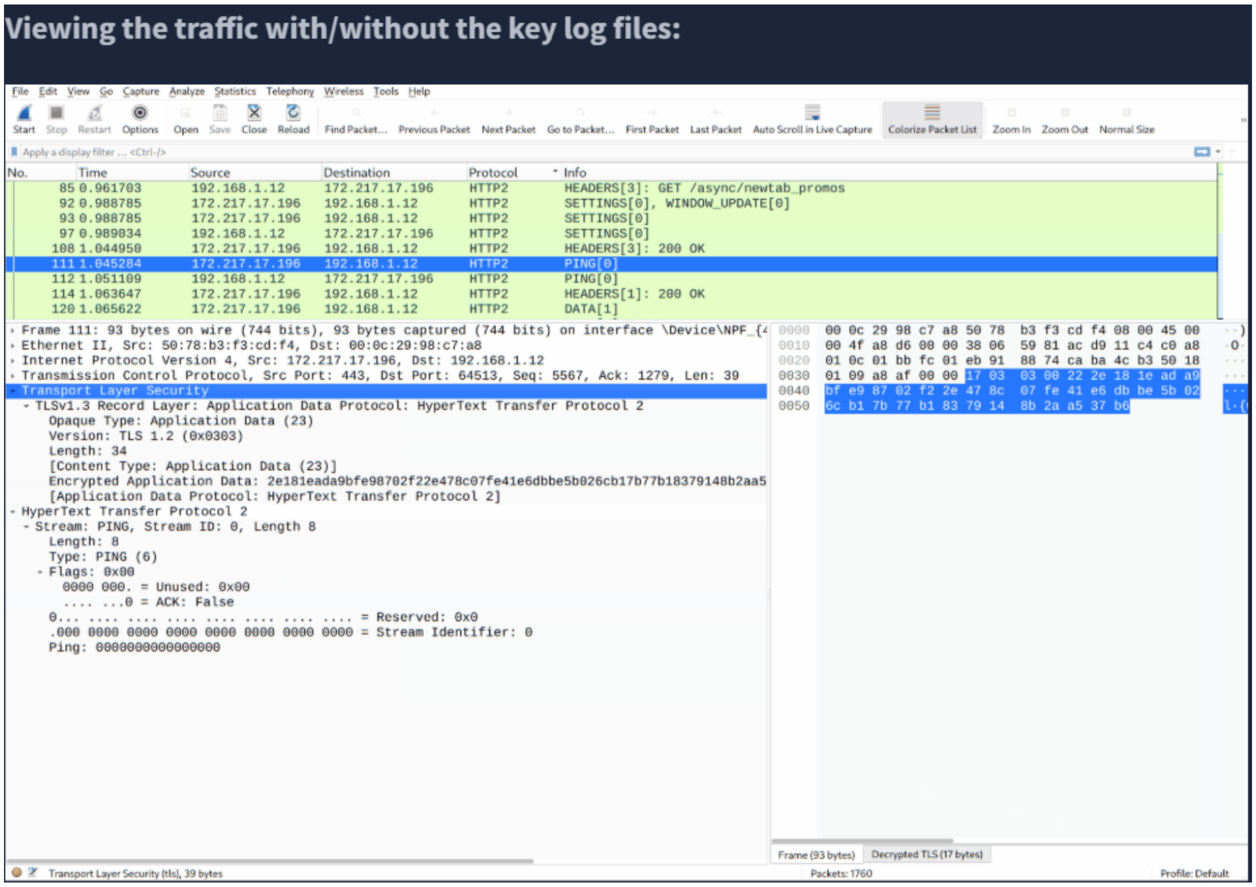
Adding key log files with the "Edit --> Preferences --> Protocols --> TLS"

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet… Previous Packet Next Packet Go to Packet… First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out
Apply a display filter … <Ctrl-/>

```
No.      Time       Source          Destination     Protocol  Info
    93 0.988785   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
    97 0.989034   192.168.1.12    172.217.17.196  TLSv1.3   Application Data
   101 1.010213   172.217.17.196  192.168.1.12    TLSv1.3   Server Hello, Change Cipher Spec
   103 1.010821   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   105 1.011264   192.168.1.12    172.217.17.196  TLSv1.3   Change Cipher Spec, Application Data
   108 1.044950   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   109 1.044950   172.217.17.196  192.168.1.12    TLSv1.3   Application Data, Application Data
   111 1.045284   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   112 1.051109   192.168.1.12    172.217.17.196  TLSv1.3   Application Data
   114 1.063647   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   115 1.063647   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   117 1.065078   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   118 1.065078   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   120 1.065622   172.217.17.196  192.168.1.12    TLSv1.3   Application Data, Application Data
   121 1.074930   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
   123 1.076198   172.217.17.196  192.168.1.12    TLSv1.3   Application Data
```

```
› Frame 101: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interfa
› Ethernet II, Src: 50:78:b3:f3:cd:f4, Dst: 00:0c:29:98:c7:a8
› Internet Protocol Version 4, Src: 172.217.17.196, Dst: 192.168.1.12
› Transmission Control Protocol, Src Port: 443, Dst Port: 64515, Seq: 1, Ack: 518, Len: 1
⌄ Transport Layer Security
  › TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  › TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    TLS segment data (1297 bytes)
```

```
0030  01 05 96 35 00 00 16 03  03 00 7a 02 00 00 76 03
0040  03 e5 63 c2 6d ab cc 4c  5f ec 4e 38 90 8e 62 fe
0050  2e 51 b3 d8 1f c8 e2 6c  e6 b6 a8 35 a0 b6 6e 7f
0060  c5 20 ec 36 c5 e6 f9 07  40 d9 e5 90 2e 11 a1 f7
0070  2f ca 4b 16 06 2f 0b 97  1e d2 64 06 eb 32 ac 92
0080  72 7f 13 01 00 00 2e 00  33 00 24 00 1d 00 20 22
0090  f2 63 d4 fb 72 4b 4e 0c  47 de 86 aa 91 9f 2b e6
00a0  8a ce 87 9d 66 bf 5a f7  dd 75 46 7c eb 70 54 00
00b0  2b 00 02 03 04 14 03 03  00 01 01 17 03 03 10 37
00c0  78 4d 3e 4a 5a 9b f2 af  de 5b c9 f5 12 6c 9d 50
00d0  c5 53 97 f3 9a 48 3c b9  5b 7f 35 bf 2e 84 36 c9
00e0  a5 a4 23 c9 5a 5d d5 ec  a0 b5 fd f1 cf 2c 8e 3c
00f0  86 d3 db a4 50 8a 92 a5  f9 b9 3e b7 4e 6d ca b7
0100  a4 d8 82 37 2b 68 f7 8d  f3 3c 5e ab 73 d0 36 9b
0110  83 52 fc be cb 1d c8 b5  ac bd 8c a0 29 de bc c9
0120  12 b6 b4 56 d4 56 b5 c3  30 84 5d a8 f4 40 dc d1
0130  07 9d d6 2b f5 4a ce 0b  0b 48 08 50 2e d8 6d 91
0140  f8 1b f3 05 75 b5 a8 8c  15 98 1f 5f f4 38 dd 6d
0150  63 6a 8b 5c 8a ce 9c 23  25 4b 35 a7 b9 36 5d f3
0160  24 8b ad fd ad e1 8f 79  31 cf 28 e9 a5 41 be 27
0170  8d 2d 65 4f d3 30 48 4a  cf 4a c7 ad eb 50 f3 2b
0180  e7 9e f8 69 74 52 a8 61  7f 57 dc 59 da df 38 e0
```



Viewing the traffic with/without the key log files:

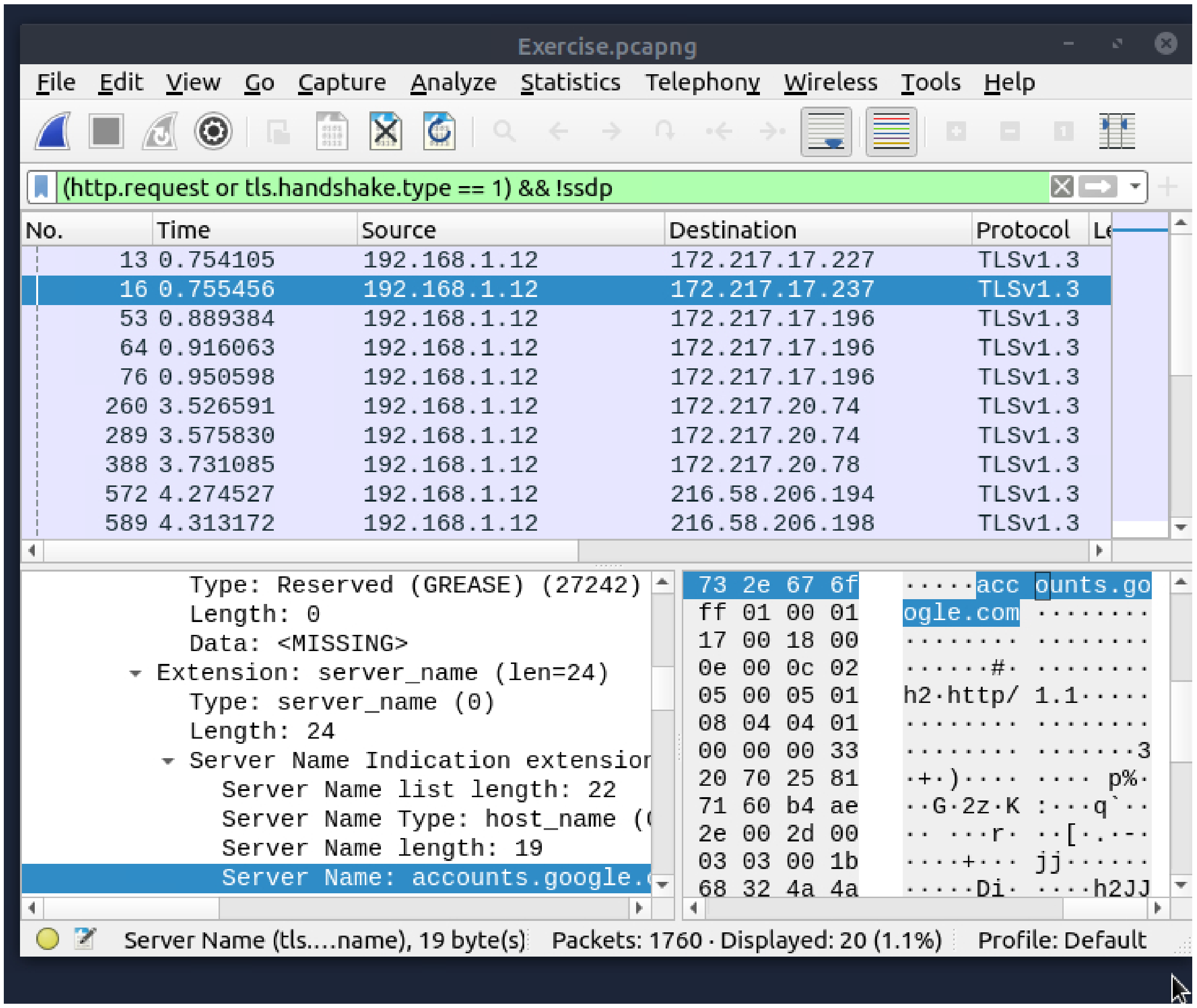
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture Colorize Packet List Zoom In Zoom Out Normal Size
Apply a display filter ... <Ctrl-/>
Frame (93 bytes) Decrypted TLS (17 bytes)
Transport Layer Security (tls), 39 bytes
Packets: 1760
Profile: Default

```
No.    Time      Source          Destination     Protocol   Info
   85 0.961703   192.168.1.12    172.217.17.196  HTTP2      HEADERS[3]: GET /async/newtab_promos
   92 0.988785   172.217.17.196  192.168.1.12    HTTP2      SETTINGS[0], WINDOW_UPDATE[0]
   93 0.988785   172.217.17.196  192.168.1.12    HTTP2      SETTINGS[0]
   97 0.989034   192.168.1.12    172.217.17.196  HTTP2      SETTINGS[0]
  108 1.044950   172.217.17.196  192.168.1.12    HTTP2      HEADERS[3]: 200 OK
  111 1.045284   172.217.17.196  192.168.1.12    HTTP2      PING[0]
  112 1.051109   192.168.1.12    172.217.17.196  HTTP2      PING[0]
  114 1.063647   172.217.17.196  192.168.1.12    HTTP2      HEADERS[1]: 200 OK
  120 1.065622   172.217.17.196  192.168.1.12    HTTP2      DATA[1]
```

```
› Frame 111: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{4
› Ethernet II, Src: 50:78:b3:f3:cd:f4, Dst: 00:0c:29:98:c7:a8
› Internet Protocol Version 4, Src: 172.217.17.196, Dst: 192.168.1.12
› Transmission Control Protocol, Src Port: 443, Dst Port: 64513, Seq: 5567, Ack: 1279, Len: 39
˅ Transport Layer Security
  ˅ TLSv1.3 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 34
      [Content Type: Application Data (23)]
      Encrypted Application Data: 2e181eada9bfe98702f22e478c07fe41e6dbbe5b026cb17b77b18379148b2aa5
      [Application Data Protocol: HyperText Transfer Protocol 2]
˅ HyperText Transfer Protocol 2
  ˅ Stream: PING, Stream ID: 0, Length 8
      Length: 8
      Type: PING (6)
    ˅ Flags: 0x00
        0000 000. = Unused: 0x00
        .... ...0 = ACK: False
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0000 0000 = Stream Identifier: 0
      Ping: 0000000000000000
```

```
0000  00 0c 29 98 c7 a8 50 78  b3 f3 cd f4 08 00 45 00   ··)
0010  00 4f a8 d6 00 00 38 06  59 81 ac d9 11 c4 c0 a8   ·O·
0020  01 0c 01 bb fc 01 eb 91  88 74 ca ba 4c b3 50 18   ···
0030  01 09 a8 af 00 00 17 03  03 00 22 2e 18 1e ad a9   ···
0040  bf e9 87 02 f2 2e 47 8c  07 fe 41 e6 db be 5b 02   ···
0050  6c b1 7b 77 b1 83 79 14  8b 2a a5 37 b6            l·{
```

1. **What is the frame number of the "Client Hello" message sent to "account.google.com"?**
   - We will input the filter associating with the client sending a request during a TLS handshake
   - (http.request or tls.handshake.type ==1) && !ssdp <--- filtering the start of a web connection and isolating additional traffic.


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(http.request or tls.handshake.type == 1) && !ssdp
```

```
No.   Time      Source         Destination     Protocol
   13 0.754105  192.168.1.12   172.217.17.227  TLSv1.3
   16 0.755456  192.168.1.12   172.217.17.237  TLSv1.3
   53 0.889384  192.168.1.12   172.217.17.196  TLSv1.3
   64 0.916063  192.168.1.12   172.217.17.196  TLSv1.3
   76 0.950598  192.168.1.12   172.217.17.196  TLSv1.3
  260 3.526591  192.168.1.12   172.217.20.74   TLSv1.3
  289 3.575830  192.168.1.12   172.217.20.74   TLSv1.3
  388 3.731085  192.168.1.12   172.217.20.78   TLSv1.3
  572 4.274527  192.168.1.12   216.58.206.194  TLSv1.3
  589 4.313172  192.168.1.12   216.58.206.198  TLSv1.3
```

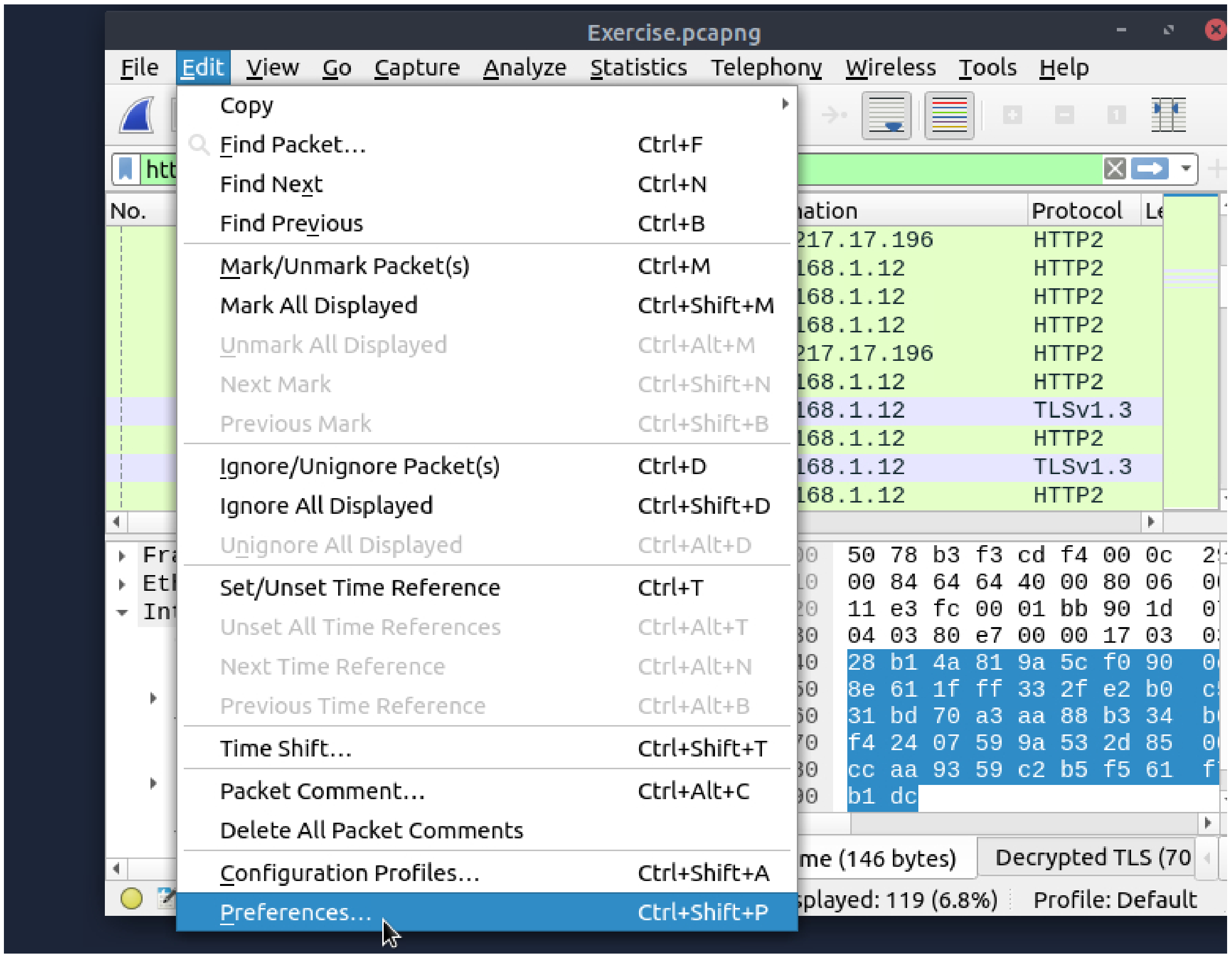
```
        Type: Reserved (GREASE) (27242)
        Length: 0
        Data: <MISSING>
    Extension: server_name (len=24)
        Type: server_name (0)
        Length: 24
        Server Name Indication extension
            Server Name list length: 22
            Server Name Type: host_name (
            Server Name length: 19
            Server Name: accounts.google.
```

```
73 2e 67 6f   ·····acc ounts.go
ff 01 00 01   ogle.com ········
17 00 18 00   ········ ········
0e 00 0c 02   ······#· ········
05 00 05 01   h2·http/ 1.1·····
08 04 04 01   ········ ········
00 00 00 33   ········ ·······3
20 70 25 81   ·+·)···· ····  p%·
71 60 b4 ae   ··G·2z·K :···q`··
2e 00 2d 00   ··  ···r· ··[·.-·
03 03 00 1b   ····+··· jj······
68 32 4a 4a   ·····Di· ····h2JJ
```

Server Name (tls....name), 19 byte(s) Packets: 1760 · Displayed: 20 (1.1%) Profile: Default

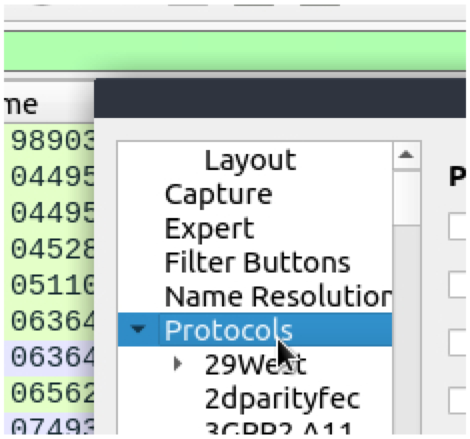
Answer: 16

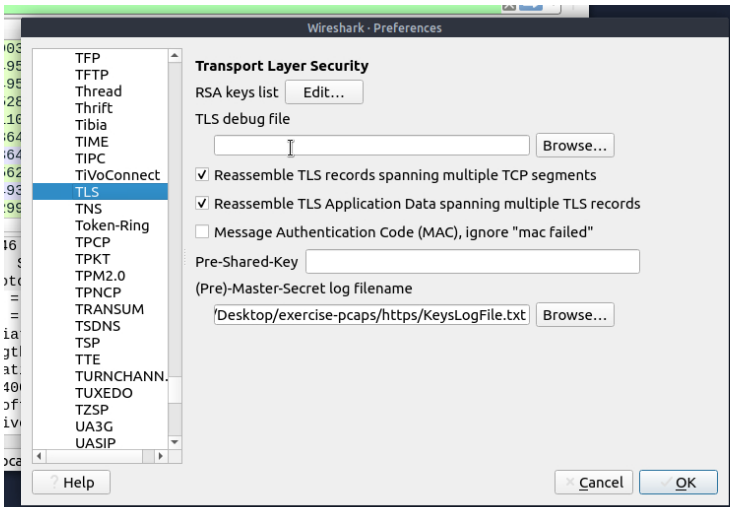
2. **Decrypt the Traffic with the "KeysLogFile.txt" file. What is the number of HTTP2 packets?**
   - First, we need to add the KeyLogFile.txt


Exercise.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Copy
Find Packet… Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles… Ctrl+Shift+A
Preferences… Ctrl+Shift+P
No.
ation
Protocol
me (146 bytes)
Decrypted TLS (70
splayed: 119 (6.8%)
Profile: Default

```
217.17.196   HTTP2
168.1.12     HTTP2
168.1.12     HTTP2
168.1.12     HTTP2
217.17.196   HTTP2
168.1.12     HTTP2
168.1.12     TLSv1.3
168.1.12     HTTP2
168.1.12     TLSv1.3
168.1.12     HTTP2
```

```
50 78 b3 f3 cd f4 00 0c
00 84 64 64 40 00 80 06
11 e3 fc 00 01 bb 90 1d
04 03 80 e7 00 00 17 03
28 b1 4a 81 9a 5c f0 90
8e 61 1f ff 33 2f e2 b0
31 bd 70 a3 aa 88 b3 34
f4 24 07 59 9a 53 2d 85
cc aa 93 59 c2 b5 f5 61
b1 dc
```





Transport Layer Security

RSA keys list Edit...

TLS debug file Browse...

✓ Reassemble TLS records spanning multiple TCP segments

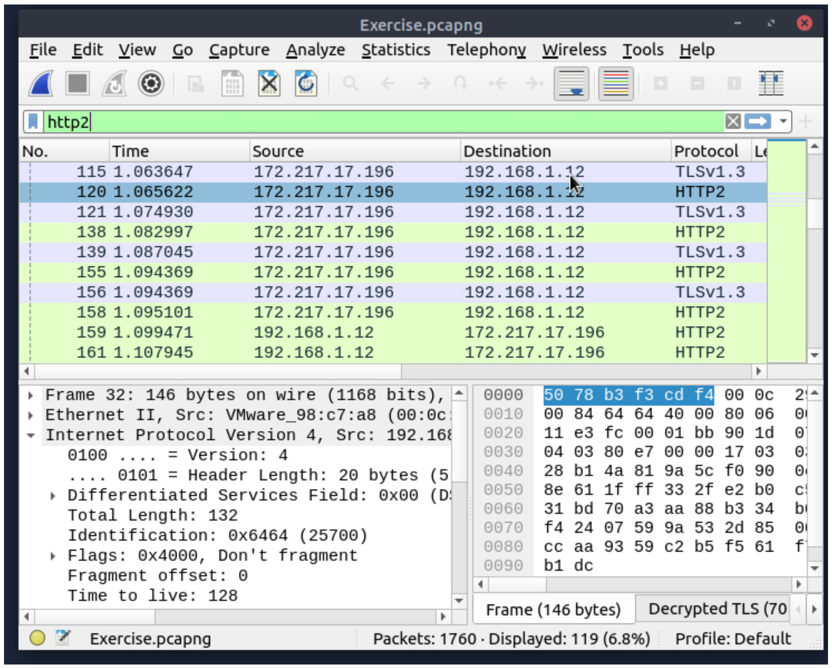
✓ Reassemble TLS Application Data spanning multiple TLS records

Message Authentication Code (MAC), ignore "mac failed"

Pre-Shared-Key

(Pre)-Master-Secret log filename

'Desktop/exercise-pcaps/https/KeysLogFile.txt Browse...


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame (146 bytes)
Decrypted TLS (70

http2

```
No.  Time      Source         Destination    Protocol
 115 1.063647  172.217.17.196 192.168.1.12   TLSv1.3
 120 1.065622  172.217.17.196 192.168.1.12   HTTP2
 121 1.074930  172.217.17.196 192.168.1.12   TLSv1.3
 138 1.082997  172.217.17.196 192.168.1.12   HTTP2
 139 1.087045  172.217.17.196 192.168.1.12   TLSv1.3
 155 1.094369  172.217.17.196 192.168.1.12   HTTP2
 156 1.094369  172.217.17.196 192.168.1.12   TLSv1.3
 158 1.095101  172.217.17.196 192.168.1.12   HTTP2
 159 1.099471  192.168.1.12   172.217.17.196 HTTP2
 161 1.107945  192.168.1.12   172.217.17.196 HTTP2
```

```
› Frame 32: 146 bytes on wire (1168 bits),
› Ethernet II, Src: VMware_98:c7:a8 (00:0c
⌄ Internet Protocol Version 4, Src: 192.168
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5
  › Differentiated Services Field: 0x00 (D
    Total Length: 132
    Identification: 0x6464 (25700)
  › Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 128
```

```
0000  50 78 b3 f3 cd f4 00 0c
0010  00 84 64 64 40 00 80 06
0020  11 e3 fc 00 01 bb 90 1d
0030  04 03 80 e7 00 00 17 03
0040  28 b1 4a 81 9a 5c f0 90
0050  8e 61 1f ff 33 2f e2 b0
0060  31 bd 70 a3 aa 88 b3 34
0070  f4 24 07 59 9a 53 2d 85
0080  cc aa 93 59 c2 b5 f5 61
0090  b1 dc
```

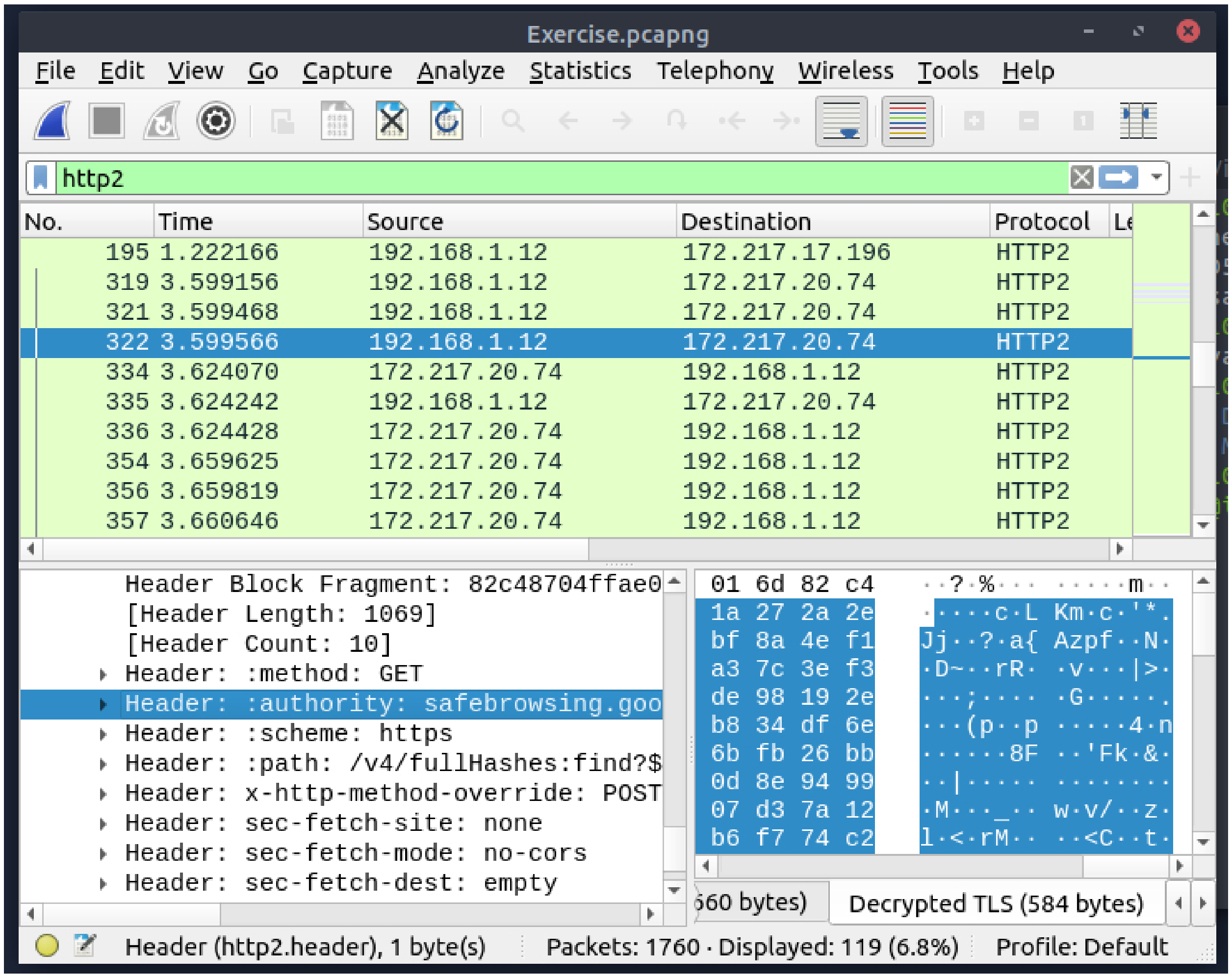
Exercise.pcapng Packets: 1760 · Displayed: 119 (6.8%) Profile: Default

Answer: 115

- There is a total of 119 packets, but notice there are 4 TLSv1.3 packets. We need to deduct the 4 from the 119 displayed packets.

3. **Go to Frame 322. What is the authority header of the HTTP2 packet? (Defanged the address)**

- On the same http2 traffic go to frame 322 – > Hypertext Transfer Protocol 2 -> Stream Headers -> Headers

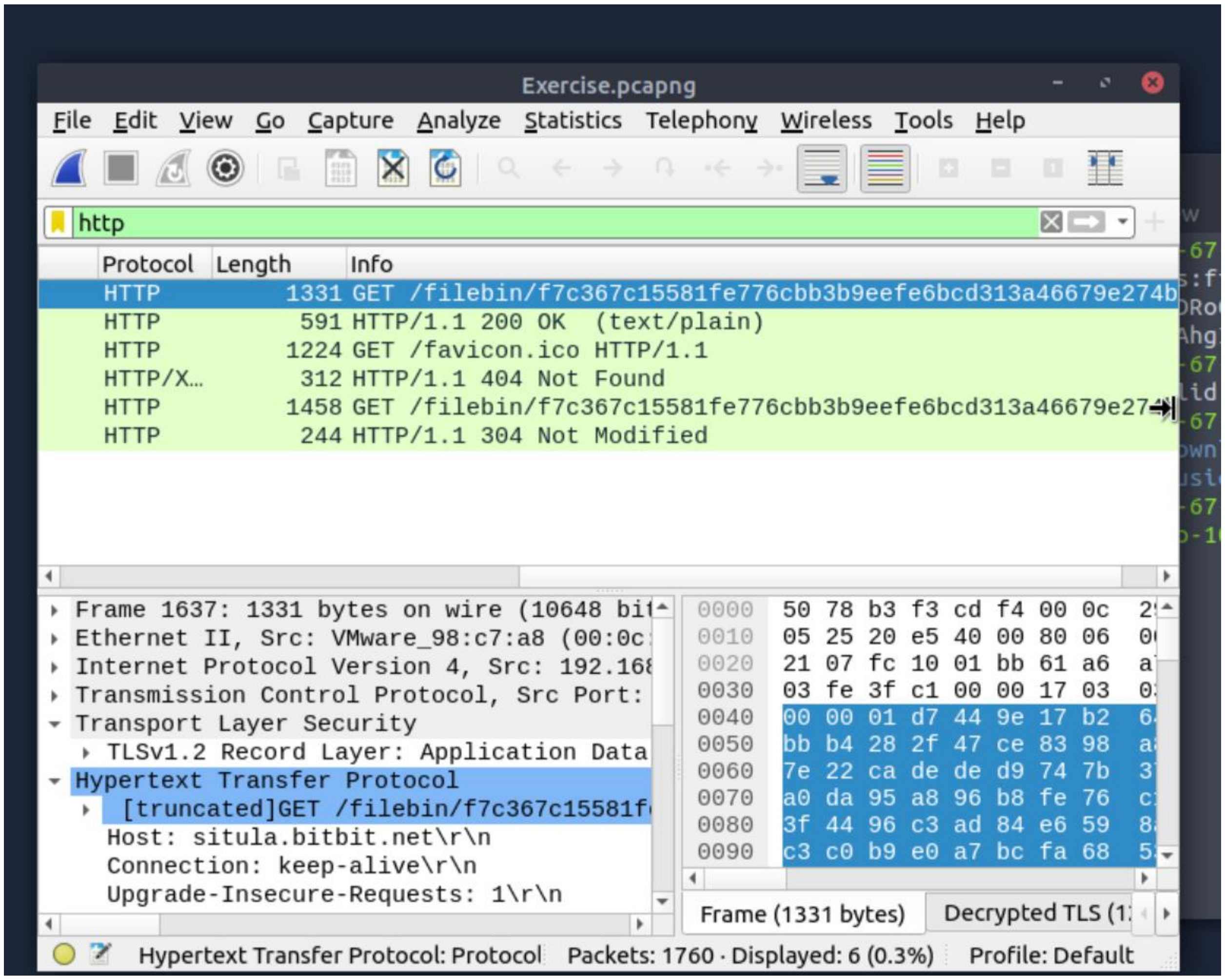


```
http2

No.   Time      Source         Destination     Protocol
  195 1.222166  192.168.1.12   172.217.17.196  HTTP2
  319 3.599156  192.168.1.12   172.217.20.74   HTTP2
  321 3.599468  192.168.1.12   172.217.20.74   HTTP2
  322 3.599566  192.168.1.12   172.217.20.74   HTTP2
  334 3.624070  172.217.20.74  192.168.1.12    HTTP2
  335 3.624242  192.168.1.12   172.217.20.74   HTTP2
  336 3.624428  172.217.20.74  192.168.1.12    HTTP2
  354 3.659625  172.217.20.74  192.168.1.12    HTTP2
  356 3.659819  172.217.20.74  192.168.1.12    HTTP2
  357 3.660646  172.217.20.74  192.168.1.12    HTTP2

      Header Block Fragment: 82c48704ffae0
      [Header Length: 1069]
      [Header Count: 10]
    ▸ Header: :method: GET
    ▸ Header: :authority: safebrowsing.goo
    ▸ Header: :scheme: https
    ▸ Header: :path: /v4/fullHashes:find?$
    ▸ Header: x-http-method-override: POST
    ▸ Header: sec-fetch-site: none
    ▸ Header: sec-fetch-mode: no-cors
    ▸ Header: sec-fetch-dest: empty

01 6d 82 c4   ··?·%···  ·····m··
1a 27 2a 2e   ·····c·L  Km·c·'*.
bf 8a 4e f1   Jj··?·a{  Azpf··N·
a3 7c 3e f3   ·D~··rR·  ·v···|>·
de 98 19 2e   ···;····  ·G·····.
b8 34 df 6e   ···(p··p  ·····4·n
6b fb 26 bb   ······8F  ··'Fk·&·
0d 8e 94 99   ··|·····  ········
07 d3 7a 12   ·M···_··  w·v/··z·
b6 f7 74 c2   l·<·rM··  ··<C··t·

560 bytes)   Decrypted TLS (584 bytes)

Header (http2.header), 1 byte(s)   Packets: 1760 · Displayed: 119 (6.8%)   Profile: Default
```

Answer: safebrowsing[.]google[.]com

4. Investigate the decrypted packets and find the flag. What is the flag?

- To find the flag, I filtered to http, since the file should be a readable file. I found a few results


Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

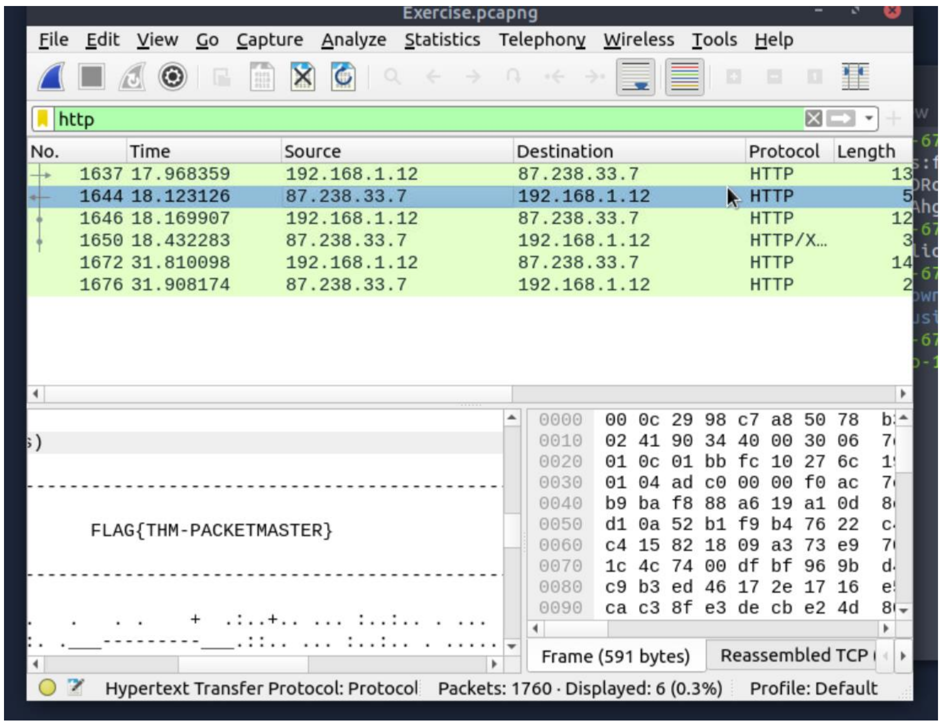
```
http

Protocol  Length  Info
HTTP        1331  GET /filebin/f7c367c15581fe776cbb3b9eefe6bcd313a46679e274b
HTTP         591  HTTP/1.1 200 OK  (text/plain)
HTTP        1224  GET /favicon.ico HTTP/1.1
HTTP/X…      312  HTTP/1.1 404 Not Found
HTTP        1458  GET /filebin/f7c367c15581fe776cbb3b9eefe6bcd313a46679e27
HTTP         244  HTTP/1.1 304 Not Modified
```

```
▸ Frame 1637: 1331 bytes on wire (10648 bit
▸ Ethernet II, Src: VMware_98:c7:a8 (00:0c
▸ Internet Protocol Version 4, Src: 192.16
▸ Transmission Control Protocol, Src Port:
▾ Transport Layer Security
   ▸ TLSv1.2 Record Layer: Application Data
▾ Hypertext Transfer Protocol
   ▸ [truncated]GET /filebin/f7c367c15581f
     Host: situla.bitbit.net\r\n
     Connection: keep-alive\r\n
     Upgrade-Insecure-Requests: 1\r\n
```

```
0000  50 78 b3 f3 cd f4 00 0c  2
0010  05 25 20 e5 40 00 80 06  0
0020  21 07 fc 10 01 bb 61 a6  a
0030  03 fe 3f c1 00 00 17 03  0
0040  00 00 01 d7 44 9e 17 b2  6
0050  bb b4 28 2f 47 ce 83 98  a
0060  7e 22 ca de de d9 74 7b  3
0070  a0 da 95 a8 96 b8 fe 76  c
0080  3f 44 96 c3 ad 84 e6 59  8
0090  c3 c0 b9 e0 a7 bc fa 68  5
```

```
Hypertext Transfer Protocol: Protocol   Packets: 1760 · Displayed: 6 (0.3%)   Profile: Default
```

- Here there is a text/plain file from packet 1644



Exercise.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.   Time       Source        Destination   Protocol  Length
 1637 17.968359  192.168.1.12  87.238.33.7   HTTP      13
 1644 18.123126  87.238.33.7   192.168.1.12  HTTP      5
 1646 18.169907  192.168.1.12  87.238.33.7   HTTP      12
 1650 18.432283  87.238.33.7   192.168.1.12  HTTP/X…   3
 1672 31.810098  192.168.1.12  87.238.33.7   HTTP      14
 1676 31.908174  87.238.33.7   192.168.1.12  HTTP      2
```

```
s)
------------------------------------------------

      FLAG{THM-PACKETMASTER}

------------------------------------------------
.   .   . .   +  .:..+.. ... :..:.. . ...
:. .___---------___.::.. ... :..:.. . .....
```

```
0000  00 0c 29 98 c7 a8 50 78  b
0010  02 41 90 34 40 00 30 06  7
0020  01 0c 01 bb fc 10 27 6c  1
0030  01 04 ad c0 00 00 f0 ac  7
0040  b9 ba f8 88 a6 19 a1 0d  8
0050  d1 0a 52 b1 f9 b4 76 22  c
0060  c4 15 82 18 09 a3 73 e9  7
0070  1c 4c 74 00 df bf 96 9b  d
0080  c9 b3 ed 46 17 2e 17 16  e
0090  ca c3 8f e3 de cb e2 4d  8
```

Hypertext Transfer Protocol: Protocol Packets: 1760 · Displayed: 6 (0.3%) Profile: Default

Answer: FLAG{THM-PACKETMASTER}