Computer Networks Lab (CS302)

Report Submission: CN Assignment Lab-2

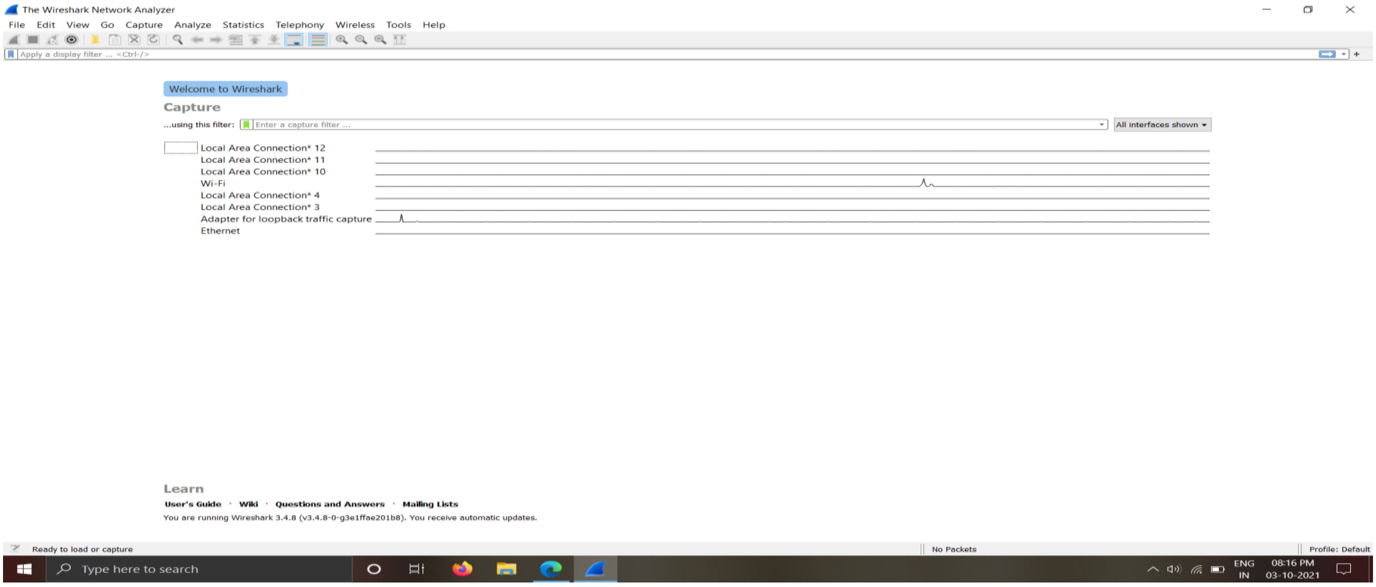
Group Members

1.Mahadev M Hatti	**191CS133**
2.Darshan A V	**191CS219**

Question-5: Capture HTTP packets by visiting a HTTP Website, analyse the packets and significance of its various fields. Do the same for HTTPS packets and compare both

Capture HTTP packets by visiting a HTTP Website:

1.In the below fig. selects the Wi-Fi option from the Interface list options.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Type here to search
ENG IN
08:16 PM 03-10-2021

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

Local Area Connection* 12
Local Area Connection* 11
Local Area Connection* 10
Wi-Fi
Local Area Connection* 4
Local Area Connection* 3
Adapter for loopback traffic capture
Ethernet

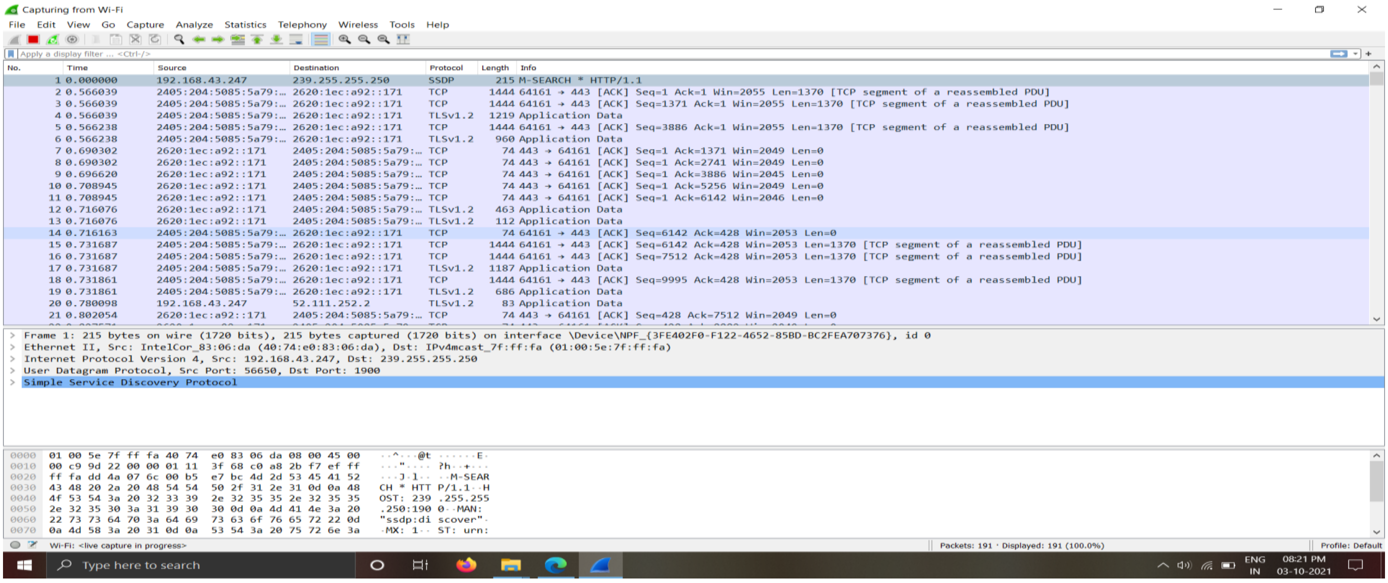
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.8 (v3.4.8-0-g3e1ffae201b8). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

2.In the new window you can see all the current traffic on the network. (Clear cache – Before capturing the traffic, you need to clear your browser’s cache.)


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Type here to search
ENG IN
08:21 PM 03-10-2021

```
No.  Time       Source                 Destination            Protocol  Length Info
   1 0.000000   192.168.43.247         239.255.255.250        SSDP       215 M-SEARCH * HTTP/1.1
   2 0.566039   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=1 Ack=1 Win=2055 Len=1370 [TCP segment of a reassembled PDU]
   3 0.566039   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=1371 Ack=1 Win=2055 Len=1370 [TCP segment of a reassembled PDU]
   4 0.566039   2405:204:5085:5a79:…   2620:1ec:a92::171      TLSv1.2   1219 Application Data
   5 0.566238   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=3886 Ack=1 Win=2055 Len=1370 [TCP segment of a reassembled PDU]
   6 0.566238   2405:204:5085:5a79:…   2620:1ec:a92::171      TLSv1.2    960 Application Data
   7 0.690302   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=1 Ack=1371 Win=2049 Len=0
   8 0.690302   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=1 Ack=2741 Win=2049 Len=0
   9 0.696620   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=1 Ack=3886 Win=2045 Len=0
  10 0.708945   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=1 Ack=5256 Win=2049 Len=0
  11 0.708945   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=1 Ack=6142 Win=2046 Len=0
  12 0.716076   2620:1ec:a92::171      2405:204:5085:5a79:…   TLSv1.2    463 Application Data
  13 0.716076   2620:1ec:a92::171      2405:204:5085:5a79:…   TLSv1.2    112 Application Data
  14 0.716163   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP         74 64161 → 443 [ACK] Seq=6142 Ack=428 Win=2053 Len=0
  15 0.731687   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=6142 Ack=428 Win=2053 Len=1370 [TCP segment of a reassembled PDU]
  16 0.731687   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=7512 Ack=428 Win=2053 Len=1370 [TCP segment of a reassembled PDU]
  17 0.731687   2405:204:5085:5a79:…   2620:1ec:a92::171      TLSv1.2   1187 Application Data
  18 0.731861   2405:204:5085:5a79:…   2620:1ec:a92::171      TCP       1444 64161 → 443 [ACK] Seq=9995 Ack=428 Win=2053 Len=1370 [TCP segment of a reassembled PDU]
  19 0.731861   2405:204:5085:5a79:…   2620:1ec:a92::171      TLSv1.2    686 Application Data
  20 0.780098   192.168.43.247         52.111.252.2           TLSv1.2     83 Application Data
  21 0.802054   2620:1ec:a92::171      2405:204:5085:5a79:…   TCP         74 443 → 64161 [ACK] Seq=428 Ack=7512 Win=2049 Len=0
```

```
> Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: IntelCor_83:06:da (40:74:e0:83:06:da), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.43.247, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 56650, Dst Port: 1900
> Simple Service Discovery Protocol
```

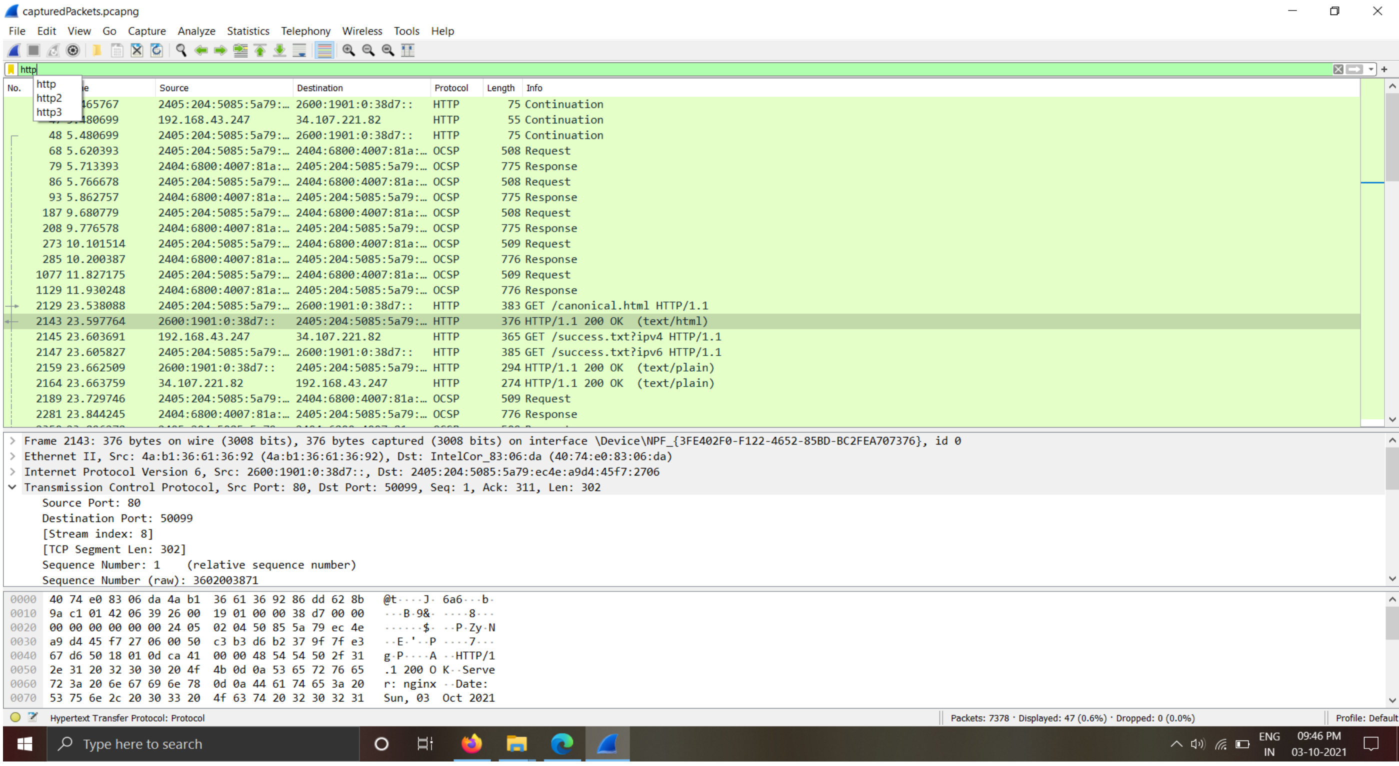
```
0000  01 00 5e 7f ff fa 40 74  e0 83 06 da 08 00 45 00   ··^···@t ······E·
0010  00 c9 9d 22 00 00 01 11  3f 68 c0 a8 2b f7 ef ff   ···"···· ?h··+···
0020  ff fa dd 4a 07 6c 00 b5  e7 bc 4d 2d 53 45 41 52   ···J·l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
```

Wi-Fi: <live capture in progress> | Packets: 191 · Displayed: 191 (100.0%) | Profile: Default

3.Use filter section to filter out Specific Packets related to http protocol.

From this Pane you can observe:

- No. – The number of a captured packet.
- Time – This shows you when the packet was captured with regards to when you started capturing.
- Source – This is the origin of a captured packet in the form of an address.
- Destination – The destination address of a captured packet.
- Protocol – The type of a captured packet.
- Length – This shows you the length of a captured packet. This is expressed in bytes.



http

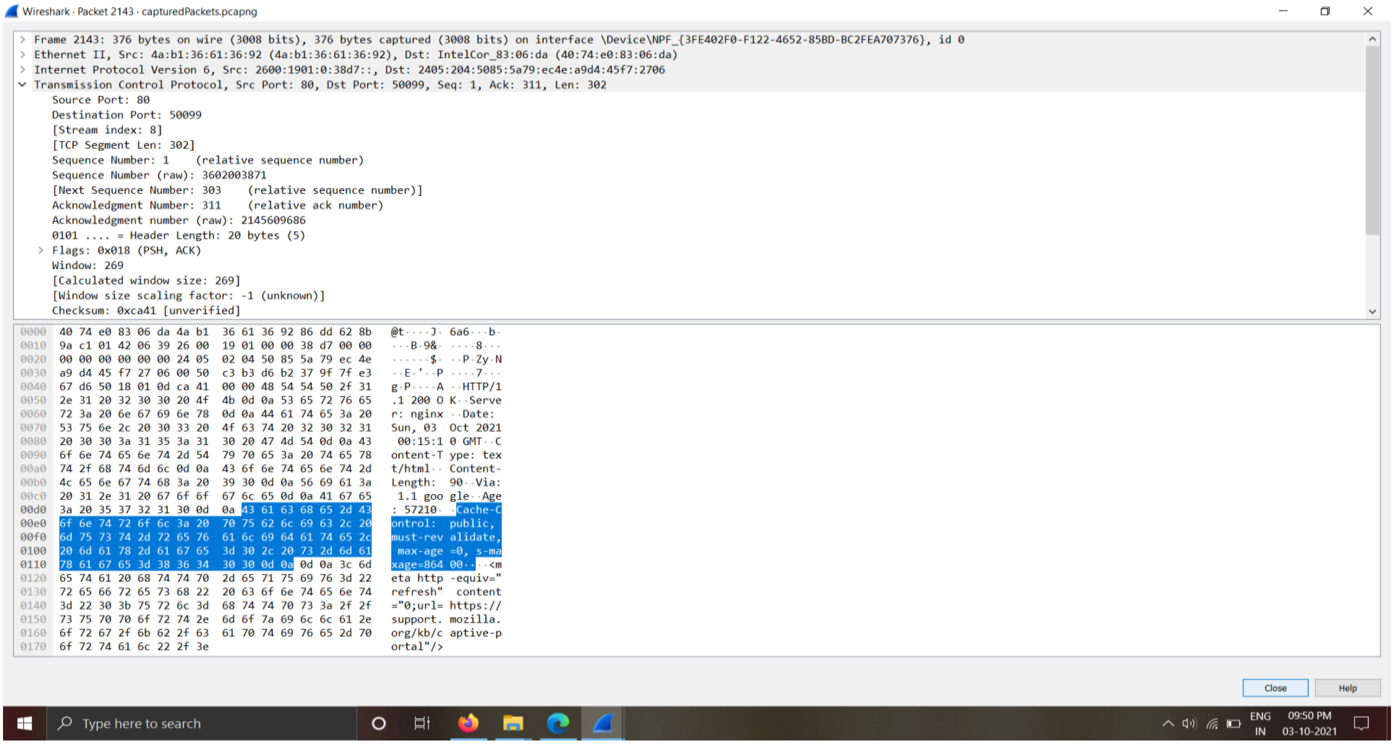
```
No.  Time       Source                 Destination            Protocol Length Info
         465767 2405:204:5085:5a79:… 2600:1901:0:38d7::     HTTP       75 Continuation
         480699 192.168.43.247         34.107.221.82          HTTP       55 Continuation
   48 5.480699  2405:204:5085:5a79:… 2600:1901:0:38d7::     HTTP       75 Continuation
   68 5.620393  2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      508 Request
   79 5.713393  2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      775 Response
   86 5.766678  2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      508 Request
   93 5.862757  2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      775 Response
  187 9.680779  2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      508 Request
  208 9.776578  2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      775 Response
  273 10.101514 2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      509 Request
  285 10.200387 2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      776 Response
 1077 11.827175 2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      509 Request
 1129 11.930248 2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      776 Response
 2129 23.538088 2405:204:5085:5a79:… 2600:1901:0:38d7::     HTTP      383 GET /canonical.html HTTP/1.1
 2143 23.597764 2600:1901:0:38d7::     2405:204:5085:5a79:… HTTP      376 HTTP/1.1 200 OK  (text/html)
 2145 23.603691 192.168.43.247         34.107.221.82          HTTP      365 GET /success.txt?ipv4 HTTP/1.1
 2147 23.605827 2405:204:5085:5a79:… 2600:1901:0:38d7::     HTTP      385 GET /success.txt?ipv6 HTTP/1.1
 2159 23.662509 2600:1901:0:38d7::     2405:204:5085:5a79:… HTTP      294 HTTP/1.1 200 OK  (text/plain)
 2164 23.663759 34.107.221.82          192.168.43.247         HTTP      274 HTTP/1.1 200 OK  (text/plain)
 2189 23.729746 2405:204:5085:5a79:… 2404:6800:4007:81a:… OCSP      509 Request
 2281 23.844245 2404:6800:4007:81a:… 2405:204:5085:5a79:… OCSP      776 Response
```

```
> Frame 2143: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2600:1901:0:38d7::, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
v Transmission Control Protocol, Src Port: 80, Dst Port: 50099, Seq: 1, Ack: 311, Len: 302
    Source Port: 80
    Destination Port: 50099
    [Stream index: 8]
    [TCP Segment Len: 302]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3602003871
```

```
0000  40 74 e0 83 06 da 4a b1  36 61 36 92 86 dd 62 8b   @t····J· 6a6···b·
0010  9a c1 01 42 06 39 26 00  19 01 00 00 38 d7 00 00   ···B·9&· ····8···
0020  00 00 00 00 00 00 24 05  02 04 50 85 5a 79 ec 4e   ······$· ··P·Zy·N
0030  a9 d4 45 f7 27 06 00 50  c3 b3 d6 b2 37 9f 7f e3   ··E·'··P ····7···
0040  67 d6 50 18 01 0d ca 41  00 00 48 54 54 50 2f 31   g·P····A ··HTTP/1
0050  2e 31 20 32 30 30 20 4f  4b 0d 0a 53 65 72 76 65   .1 200 O K··Serve
0060  72 3a 20 6e 67 69 6e 78  0d 0a 44 61 74 65 3a 20   r: nginx ··Date: 
0070  53 75 6e 2c 20 30 33 20  4f 63 74 20 32 30 32 31   Sun, 03  Oct 2021
```

Hypertext Transfer Protocol: Protocol | Packets: 7378 · Displayed: 47 (0.6%) · Dropped: 0 (0.0%) | Profile: Default

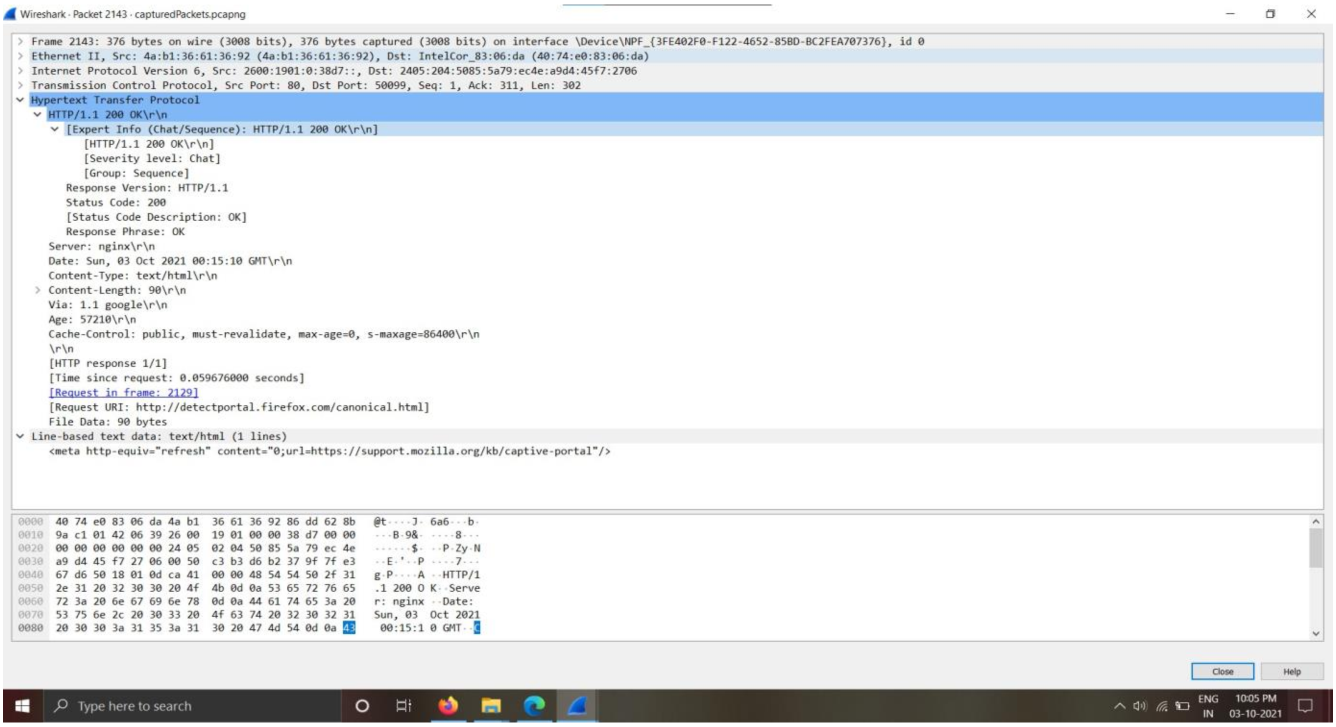
4. Choose the packet you want to read. Double-click on it.



```
> Frame 2143: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2600:1901:0:38d7::, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
v Transmission Control Protocol, Src Port: 80, Dst Port: 50099, Seq: 1, Ack: 311, Len: 302
     Source Port: 80
     Destination Port: 50099
     [Stream index: 8]
     [TCP Segment Len: 302]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 3602003871
     [Next Sequence Number: 303    (relative sequence number)]
     Acknowledgment Number: 311    (relative ack number)
     Acknowledgment number (raw): 2145609686
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x018 (PSH, ACK)
     Window: 269
     [Calculated window size: 269]
     [Window size scaling factor: -1 (unknown)]
     Checksum: 0xca41 [unverified]
```

```
0000  40 74 e0 83 06 da 4a b1  36 61 36 92 86 dd 62 8b   @t····J· 6a6···b·
0010  9a c1 01 42 06 39 26 00  19 01 00 00 38 d7 00 00   ···B·9&· ····8···
0020  00 00 00 00 00 00 24 05  02 04 50 85 5a 79 ec 4e   ······$· ··P·Zy·N
0030  a9 d4 45 f7 27 06 00 50  c3 b3 d6 b2 37 9f 7f e3   ··E·'··P ····7···
0040  67 d6 50 18 01 0d ca 41  00 00 48 54 54 50 2f 31   g·P····A ··HTTP/1
0050  2e 31 20 32 30 30 20 4f  4b 0d 0a 53 65 72 76 65   .1 200 O K··Serve
0060  72 3a 20 6e 67 69 6e 78  0d 0a 44 61 74 65 3a 20   r: nginx ··Date: 
0070  53 75 6e 2c 20 30 33 20  4f 63 74 20 32 30 32 31   Sun, 03  Oct 2021
0080  20 30 30 3a 31 35 3a 31  30 20 47 4d 54 0d 0a 43    00:15:1 0 GMT··C
0090  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
00a0  74 2f 68 74 6d 6c 0d 0a  43 6f 6e 74 65 6e 74 2d   t/html·· Content-
00b0  4c 65 6e 67 74 68 3a 20  39 30 0d 0a 56 69 61 3a   Length:  90··Via:
00c0  20 31 2e 31 20 67 6f 6f  67 6c 65 0d 0a 41 67 65    1.1 goo gle··Age
00d0  3a 20 35 37 32 31 30 0d  0a 43 61 63 68 65 2d 43   : 57210· ·Cache-C
00e0  6f 6e 74 72 6f 6c 3a 20  70 75 62 6c 69 63 2c 20   ontrol:  public, 
00f0  6d 75 73 74 2d 72 65 76  61 6c 69 64 61 74 65 2c   must-rev alidate,
0100  20 6d 61 78 2d 61 67 65  3d 30 2c 20 73 2d 6d 61    max-age =0, s-ma
0110  78 61 67 65 3d 38 36 34  30 30 0d 0a 0d 0a 3c 6d   xage=864 00····<m
0120  65 74 61 20 68 74 74 70  2d 65 71 75 69 76 3d 22   eta http -equiv="
0130  72 65 66 72 65 73 68 22  20 63 6f 6e 74 65 6e 74   refresh"  content
0140  3d 22 30 3b 75 72 6c 3d  68 74 74 70 73 3a 2f 2f   ="0;url= https://
0150  73 75 70 70 6f 72 74 2e  6d 6f 7a 69 6c 6c 61 2e   support. mozilla.
0160  6f 72 67 2f 6b 62 2f 63  61 70 74 69 76 65 2d 70   org/kb/c aptive-p
0170  6f 72 74 61 6c 22 2f 3e                            ortal"/>
```

5. Here are some additional information from the captured http packet:

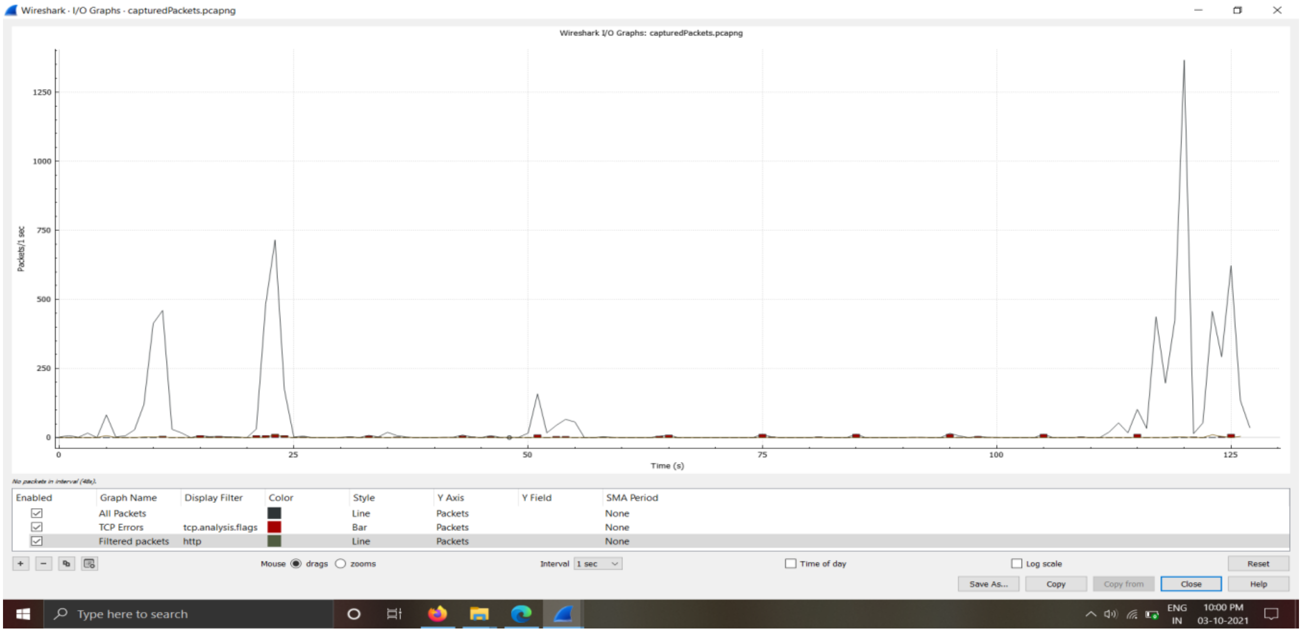


```
> Frame 2143: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2600:1901:0:38d7::, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
> Transmission Control Protocol, Src Port: 80, Dst Port: 50099, Seq: 1, Ack: 311, Len: 302
v Hypertext Transfer Protocol
   v HTTP/1.1 200 OK\r\n
      v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
           [HTTP/1.1 200 OK\r\n]
           [Severity level: Chat]
           [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
     Server: nginx\r\n
     Date: Sun, 03 Oct 2021 00:15:10 GMT\r\n
     Content-Type: text/html\r\n
   > Content-Length: 90\r\n
     Via: 1.1 google\r\n
     Age: 57210\r\n
     Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400\r\n
     \r\n
     [HTTP response 1/1]
     [Time since request: 0.059676000 seconds]
     [Request in frame: 2129]
     [Request URI: http://detectportal.firefox.com/canonical.html]
     File Data: 90 bytes
v Line-based text data: text/html (1 lines)
     <meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal"/>
```

```
0000  40 74 e0 83 06 da 4a b1  36 61 36 92 86 dd 62 8b   @t····J· 6a6···b·
0010  9a c1 01 42 06 39 26 00  19 01 00 00 38 d7 00 00   ···B·9&· ····8···
0020  00 00 00 00 00 00 24 05  02 04 50 85 5a 79 ec 4e   ······$· ··P·Zy·N
0030  a9 d4 45 f7 27 06 00 50  c3 b3 d6 b2 37 9f 7f e3   ··E·'··P ····7···
0040  67 d6 50 18 01 0d ca 41  00 00 48 54 54 50 2f 31   g·P····A ··HTTP/1
0050  2e 31 20 32 30 30 20 4f  4b 0d 0a 53 65 72 76 65   .1 200 O K··Serve
0060  72 3a 20 6e 67 69 6e 78  0d 0a 44 61 74 65 3a 20   r: nginx ··Date: 
0070  53 75 6e 2c 20 30 33 20  4f 63 74 20 32 30 32 31   Sun, 03  Oct 2021
0080  20 30 30 3a 31 35 3a 31  30 20 47 4d 54 0d 0a 43    00:15:1 0 GMT··C
```

I/O GRAPHS:

It shows the graph for the network traffic.



Wireshark · I/O Graphs · capturedPackets.pcapng
Wireshark I/O Graphs: capturedPackets.pcapng
Packets/1 sec
1250
1000
750
500
250
0
25
50
75
100
125
Time (s)
No packets in interval (48s).
Type here to search
ENG
IN
10:00 PM
03-10-2021

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None
☑	Filtered packets	http	🟩	Line	Packets		None

Mouse ● drags ○ zooms

Interval 1 sec

□ Time of day

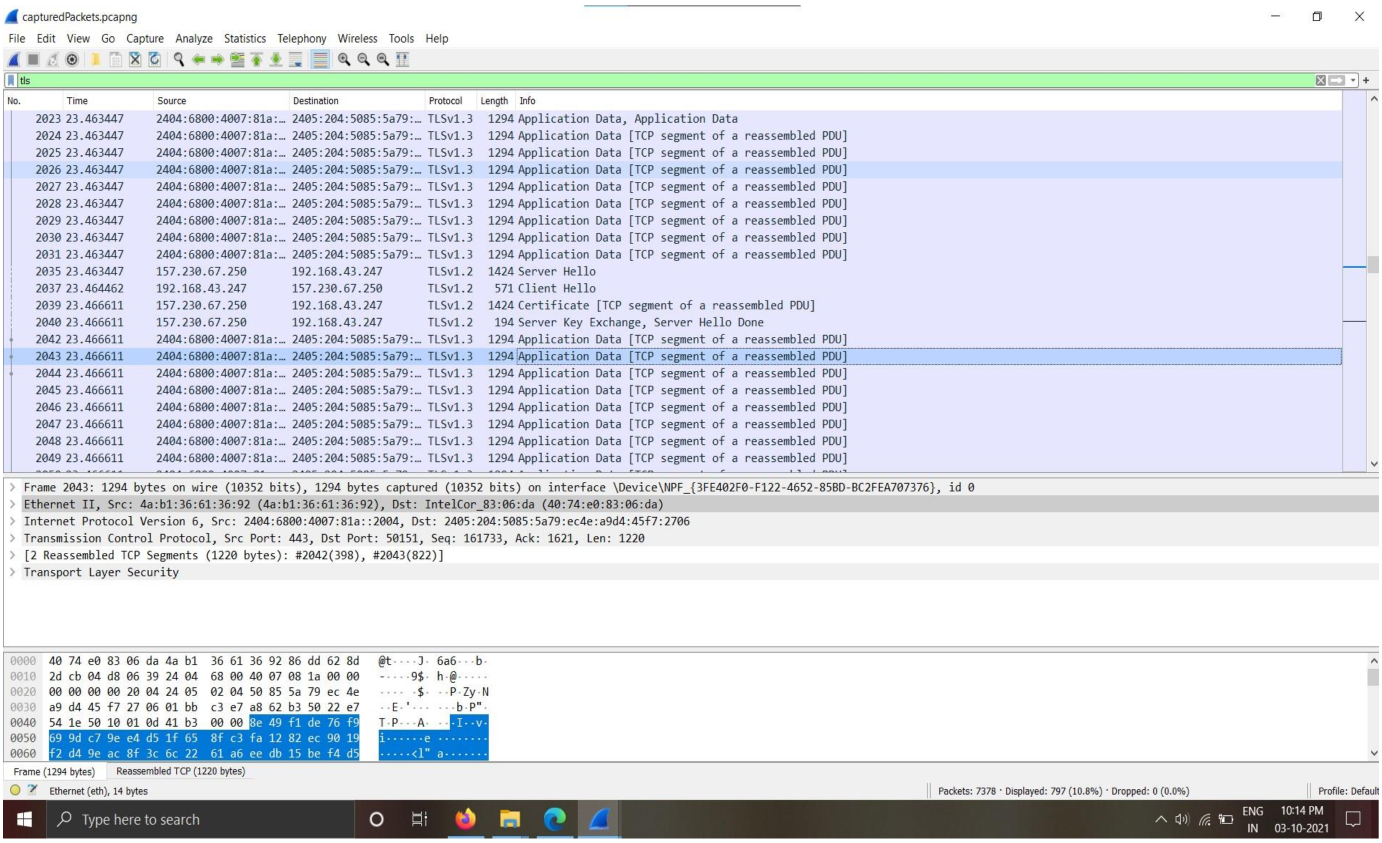
□ Log scale

Capture HTTPS packets:

1.. Use filter section to filter out Specific Packets related to https protocol. (HTTPS means HTTP over TLS).

From this Pane you can observe:

- No. – The number of a captured packet.
- Time – This shows you when the packet was captured with regards to when you started capturing.
- Source – This is the origin of a captured packet in the form of an address.
- Destination – The destination address of a captured packet.
- Protocol – The type of a captured packet.
- Length – This shows you the length of a captured packet. This is expressed in bytes.

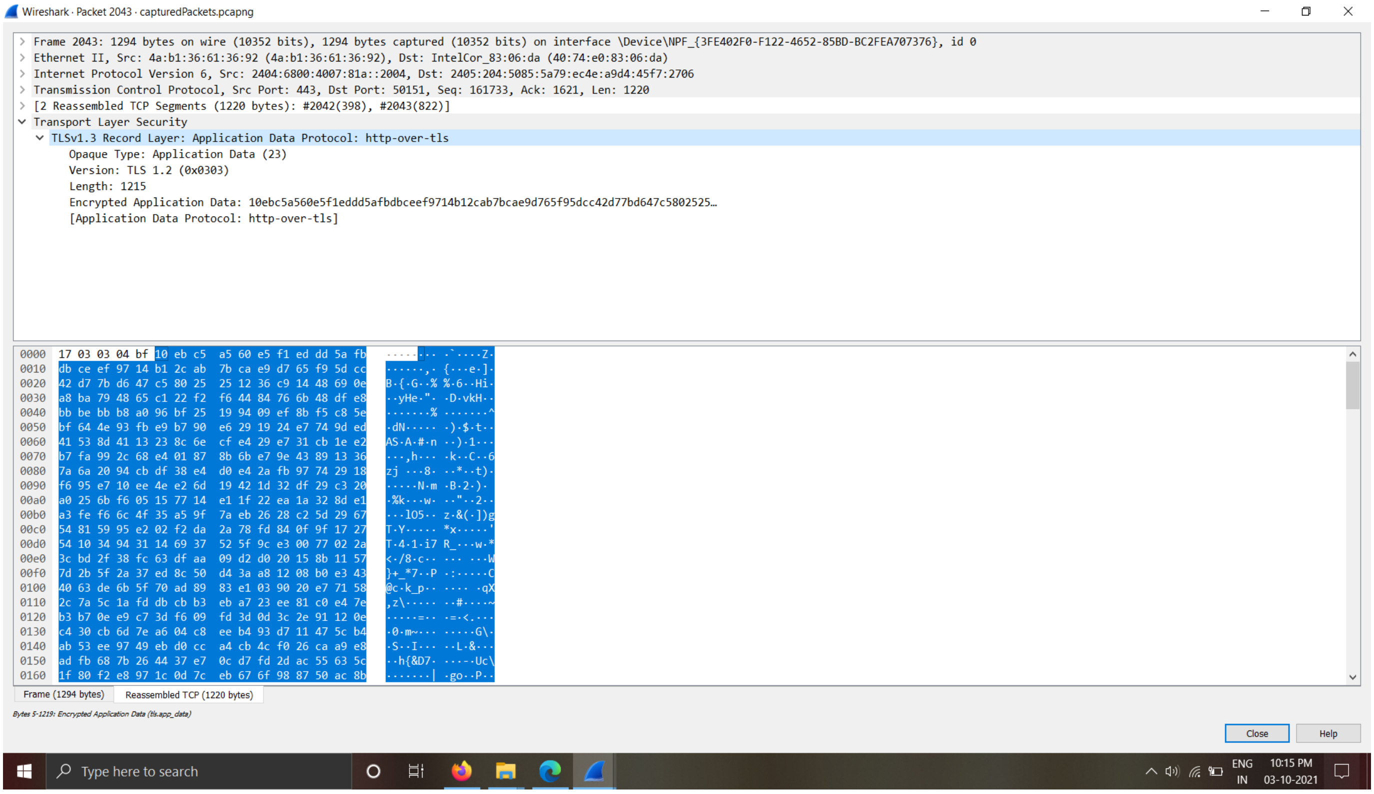

capturedPackets.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls

```
No.  Time      Source               Destination          Protocol Length Info
2023 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data, Application Data
2024 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2025 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2026 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2027 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2028 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2029 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2030 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2031 23.463447 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2035 23.463447 157.230.67.250       192.168.43.247       TLSv1.2  1424 Server Hello
2037 23.464462 192.168.43.247       157.230.67.250       TLSv1.2   571 Client Hello
2039 23.466611 157.230.67.250       192.168.43.247       TLSv1.2  1424 Certificate [TCP segment of a reassembled PDU]
2040 23.466611 157.230.67.250       192.168.43.247       TLSv1.2   194 Server Key Exchange, Server Hello Done
2042 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2043 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2044 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2045 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2046 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2047 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2048 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
2049 23.466611 2404:6800:4007:81a:… 2405:204:5085:5a79:… TLSv1.3  1294 Application Data [TCP segment of a reassembled PDU]
```

```
> Frame 2043: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2404:6800:4007:81a::2004, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
> Transmission Control Protocol, Src Port: 443, Dst Port: 50151, Seq: 161733, Ack: 1621, Len: 1220
> [2 Reassembled TCP Segments (1220 bytes): #2042(398), #2043(822)]
> Transport Layer Security
```

```
0000  40 74 e0 83 06 da 4a b1  36 61 36 92 86 dd 62 8d   @t····J· 6a6···b·
0010  2d cb 04 d8 06 39 24 04  68 00 40 07 08 1a 00 00   -····9$· h·@·····
0020  00 00 00 00 20 04 24 05  02 04 50 85 5a 79 ec 4e   ···· ·$· ··P·Zy·N
0030  a9 d4 45 f7 27 06 01 bb  c3 e7 a8 62 b3 50 22 e7   ··E·'··· ···b·P"·
0040  54 1e 50 10 01 0d 41 b3  00 00 8e 49 f1 de 76 f9   T·P···A· ···I··v·
0050  69 9d c7 9e e4 d5 1f 65  8f c3 fa 12 82 ec 90 19   i······e ········
0060  f2 d4 9e ac 8f 3c 6c 22  61 a6 ee db 15 be f4 d5   ·····<l" a·······
```

2. Choose the packet you want to read. Double-click on it.

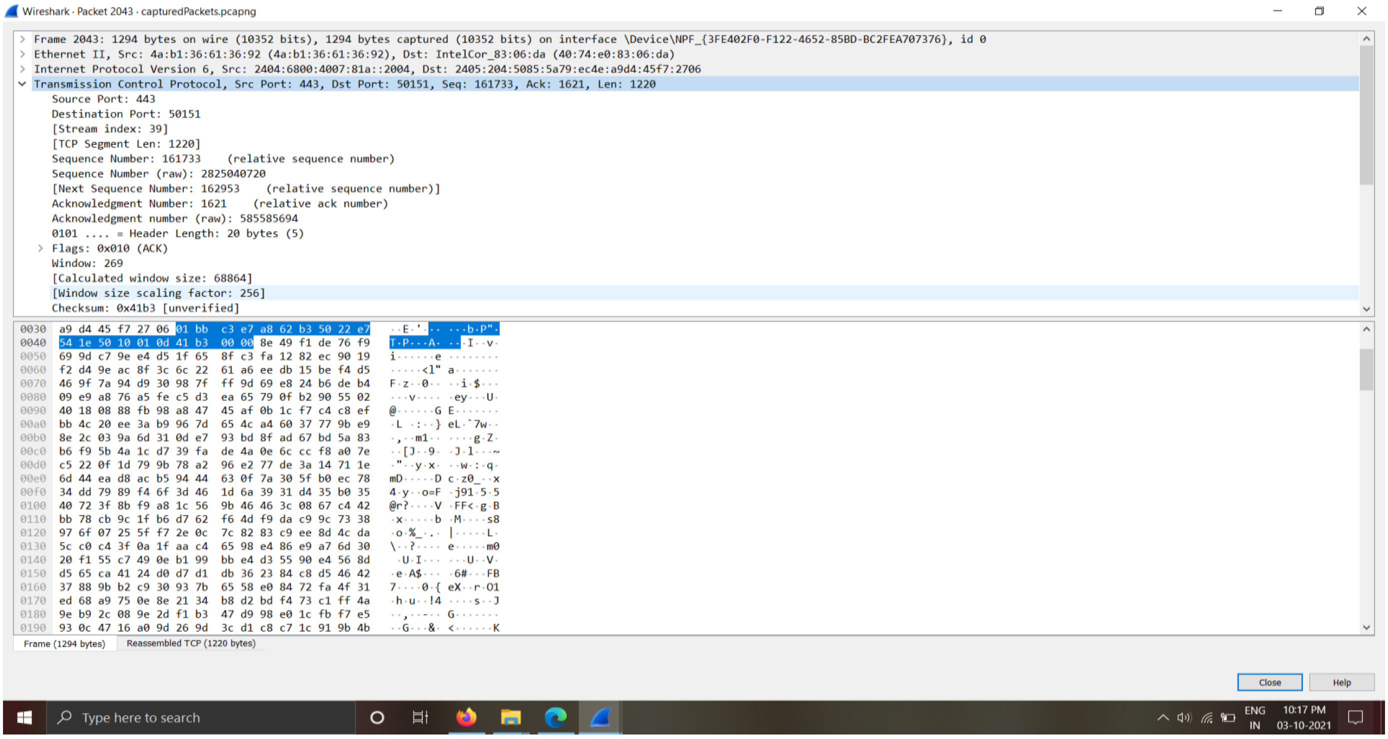


```
> Frame 2043: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2404:6800:4007:81a::2004, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
> Transmission Control Protocol, Src Port: 443, Dst Port: 50151, Seq: 161733, Ack: 1621, Len: 1220
> [2 Reassembled TCP Segments (1220 bytes): #2042(398), #2043(822)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
        Opaque Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 1215
        Encrypted Application Data: 10ebc5a560e5f1eddd5afbdbceef9714b12cab7bcae9d765f95dcc42d77bd647c5802525…
        [Application Data Protocol: http-over-tls]
```

```
0000  17 03 03 04 bf 10 eb c5  a5 60 e5 f1 ed dd 5a fb   ········ ·`····Z·
0010  db ce ef 97 14 b1 2c ab  7b ca e9 d7 65 f9 5d cc   ······,· {···e·]·
0020  42 d7 7b d6 47 c5 80 25  25 12 36 c9 14 48 69 0e   B·{·G··% %·6··Hi·
0030  a8 ba 79 48 65 c1 22 f2  f6 44 84 76 6b 48 df e8   ··yHe·"· ·D·vkH··
0040  bb be bb b8 a0 96 bf 25  19 94 09 ef 8b f5 c8 5e   ·······% ·······^
0050  bf 64 4e 93 fb e9 b7 90  e6 29 19 24 e7 74 9d ed   ·dN····· ·)·$·t··
0060  41 53 8d 41 13 23 8c 6e  cf e4 29 e7 31 cb 1e e2   AS·A·#·n ··)·1···
0070  b7 fa 99 2c 68 e4 01 87  8b 6b e7 9e 43 89 13 36   ···,h··· ·k··C··6
0080  7a 6a 20 94 cb df 38 e4  d0 e4 2a fb 97 74 29 18   zj ···8· ··*··t)·
0090  f6 95 e7 10 ee 4e e2 6d  19 42 1d 32 df 29 c3 20   ·····N·m ·B·2·)·
00a0  a0 25 6b f6 05 15 77 14  e1 1f 22 ea 1a 32 8d e1   ·%k···w· ··"··2··
00b0  a3 fe f6 6c 4f 35 a5 9f  7a eb 26 28 c2 5d 29 67   ···lO5·· z·&(·])g
00c0  54 81 59 95 e2 02 f2 da  2a 78 fd 84 0f 9f 17 27   T·Y····· *x·····'
00d0  54 10 34 94 31 14 69 37  52 5f 9c e3 00 77 02 2a   T·4·1·i7 R_···w·*
00e0  3c bd 2f 38 fc 63 df aa  09 d2 d0 20 15 8b 11 57   <·/8·c·· ··· ···W
00f0  7d 2b 5f 2a 37 ed 8c 50  d4 3a a8 12 08 b0 e3 43   }+_*7··P ·:·····C
0100  40 63 de 6b 5f 70 ad 89  83 e1 03 90 20 e7 71 58   @c·k_p·· ···· ·qX
0110  2c 7a 5c 1a fd db cb b3  eb a7 23 ee 81 c0 e4 7e   ,z\····· ··#····~
0120  b3 b7 0e e9 c7 3d f6 09  fd 3d 0d 3c 2e 91 12 0e   ·····=·· ·=·<.···
0130  c4 30 cb 6d 7e a6 04 c8  ee b4 93 d7 11 47 5c b4   ·0·m~··· ·····G\·
0140  ab 53 ee 97 49 eb d0 cc  a4 cb 4c f0 26 ca a9 e8   ·S··I··· ··L·&···
0150  ad fb 68 7b 26 44 37 e7  0c d7 fd 2d ac 55 63 5c   ··h{&D7· ···-·Uc\
0160  1f 80 f2 e8 97 1c 0d 7c  eb 67 6f 98 87 50 ac 8b   ·······| ·go··P··
```

Bytes 5-1219: Encrypted Application Data (tls.app_data)

3. Here are some additional information from the captured http packet:



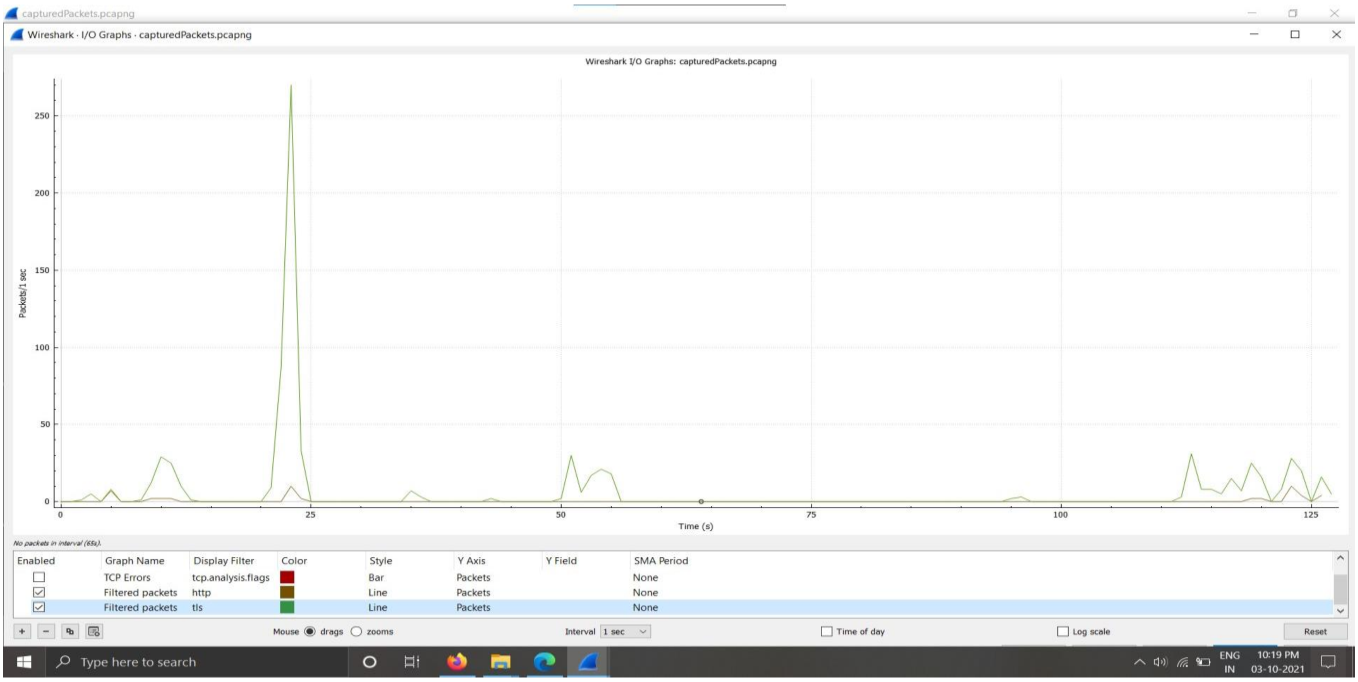
Wireshark · Packet 2043 · capturedPackets.pcapng

```
> Frame 2043: 1294 bytes on wire (10352 bits), 1294 bytes captured (10352 bits) on interface \Device\NPF_{3FE402F0-F122-4652-85BD-BC2FEA707376}, id 0
> Ethernet II, Src: 4a:b1:36:61:36:92 (4a:b1:36:61:36:92), Dst: IntelCor_83:06:da (40:74:e0:83:06:da)
> Internet Protocol Version 6, Src: 2404:6800:4007:81a::2004, Dst: 2405:204:5085:5a79:ec4e:a9d4:45f7:2706
v Transmission Control Protocol, Src Port: 443, Dst Port: 50151, Seq: 161733, Ack: 1621, Len: 1220
    Source Port: 443
    Destination Port: 50151
    [Stream index: 39]
    [TCP Segment Len: 1220]
    Sequence Number: 161733    (relative sequence number)
    Sequence Number (raw): 2825040720
    [Next Sequence Number: 162953    (relative sequence number)]
    Acknowledgment Number: 1621    (relative ack number)
    Acknowledgment number (raw): 585585694
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 269
    [Calculated window size: 68864]
    [Window size scaling factor: 256]
    Checksum: 0x41b3 [unverified]
```

```
0030  a9 d4 45 f7 27 06 01 bb  c3 e7 a8 62 b3 50 22 e7   ··E·'··· ···b·P"·
0040  54 1e 50 10 01 0d 41 b3  00 00 8e 49 f1 de 76 f9   T·P···A· ···I··v·
0050  69 9d c7 9e e4 d5 1f 65  8f c3 fa 12 82 ec 90 19   i······e ········
0060  f2 d4 9e ac 8f 3c 6c 22  61 a6 ee db 15 be f4 d5   ·····<l" a·······
0070  46 9f 7a 94 d9 30 98 7f  ff 9d 69 e8 24 b6 de b4   F·z··0·· ··i·$···
0080  09 e9 a8 76 a5 fe c5 d3  ea 65 79 0f b2 90 55 02   ···v···· ·ey···U·
0090  40 18 08 88 fb 98 a8 47  45 af 0b 1c f7 c4 c8 ef   @······G E·······
00a0  bb 4c 20 ee 3a b9 96 7d  65 4c a4 60 37 77 9b e9   ·L ·:··} eL·`7w··
00b0  8e 2c 03 9a 6d 31 0d e7  93 bd 8f ad 67 bd 5a 83   ·,··m1·· ····g·Z·
00c0  b6 f9 5b 4a 1c d7 39 fa  de 4a 0e 6c cc f8 a0 7e   ··[J··9· ·J·l···~
00d0  c5 22 0f 1d 79 9b 78 a2  96 e2 77 de 3a 14 71 1e   ·"··y·x· ··w·:·q·
00e0  6d 44 ea d8 ac b5 94 44  63 0f 7a 30 5f b0 ec 78   mD·····D c·z0_··x
00f0  34 dd 79 89 f4 6f 3d 46  1d 6a 39 31 d4 35 b0 35   4·y··o=F ·j91·5·5
0100  40 72 3f 8b f9 a8 1c 56  9b 46 46 3c 08 67 c4 42   @r?····V ·FF<·g·B
0110  bb 78 cb 9c 1f b6 d7 62  f6 4d f9 da c9 9c 73 38   ·x·····b ·M····s8
0120  97 6f 07 25 5f f7 2e 0c  7c 82 83 c9 ee 8d 4c da   ·o·%_·.· |·····L·
0130  5c c0 c4 3f 0a 1f aa c4  65 98 e4 86 e9 a7 6d 30   \··?···· e·····m0
0140  20 f1 55 c7 49 0e b1 99  bb e4 d3 55 90 e4 56 8d    ·U·I··· ···U··V·
0150  d5 65 ca 41 24 d0 d7 d1  db 36 23 84 c8 d5 46 42   ·e·A$··· ·6#···FB
0160  37 88 9b b2 c9 30 93 7b  65 58 e0 84 72 fa 4f 31   7····0·{ eX··r·O1
0170  ed 68 a9 75 0e 8e 21 34  b8 d2 bd f4 73 c1 ff 4a   ·h·u··!4 ····s··J
0180  9e b9 2c 08 9e 2d f1 b3  47 d9 98 e0 1c fb f7 e5   ··,··-·· G·······
0190  93 0c 47 16 a0 9d 26 9d  3c d1 c8 c7 1c 91 9b 4b   ··G···&· <······K
```

I/O GRAPHS:

It shows the graph for the network traffic.



Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
□	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None
☑	Filtered packets	http	🟫	Line	Packets		None
☑	Filtered packets	tls	🟩	Line	Packets		None