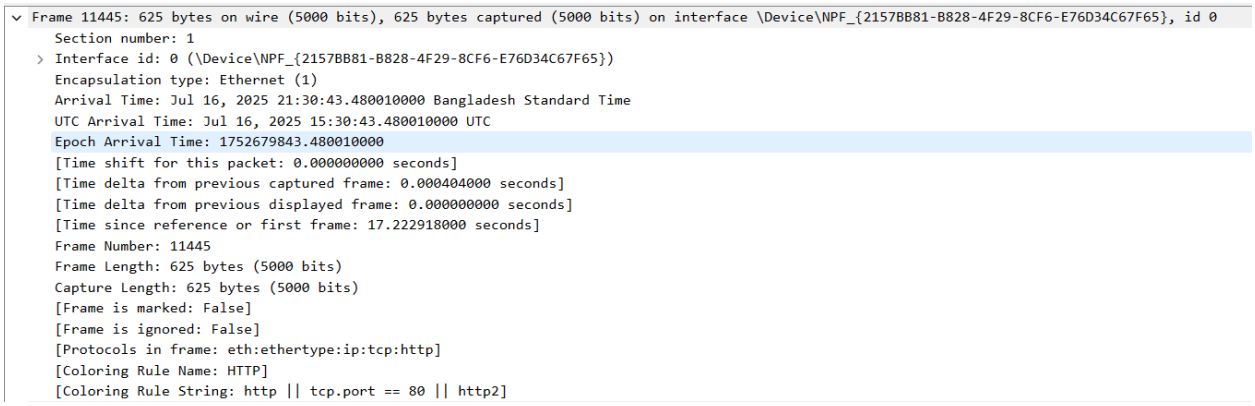
HTTP Request:

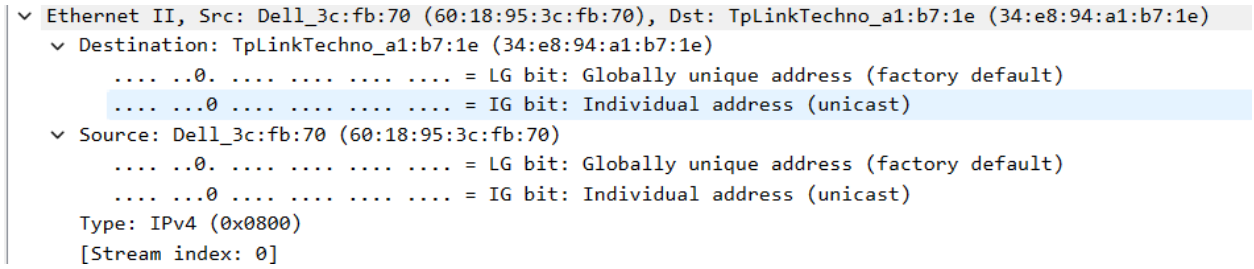
Frame:



The physical layer deals with the transmission of raw bits over a physical medium. This layer isn't explicitly shown in the packet capture, but it underlies the transmission process that Ethernet (Layer 2) depends on. The transmission of bits (represented by Ethernet frames) is what occurs at this layer, although the actual physical medium isn’t captured in the image.

The image shows a packet capture at Layer 2 (Data Link Layer) and Layer 3 (Network Layer), with the details of the frame, including encapsulation type (Ethernet 1), frame length (625 bytes), and the time of arrival. This packet is using the HTTP protocol over TCP (port 80), which is confirmed by the protocol string "eth:ethertype:ip:tcp:http." The source and destination are using Ethernet, which handles the data link layer for proper communication within a local network. The IP layer handles the routing between different networks, and the TCP layer ensures that the data is transferred reliably, while the HTTP application-level protocol facilitates communication between the web browser (client) and web server. The timestamp and additional frame information provide insights into the timing and capture metadata.

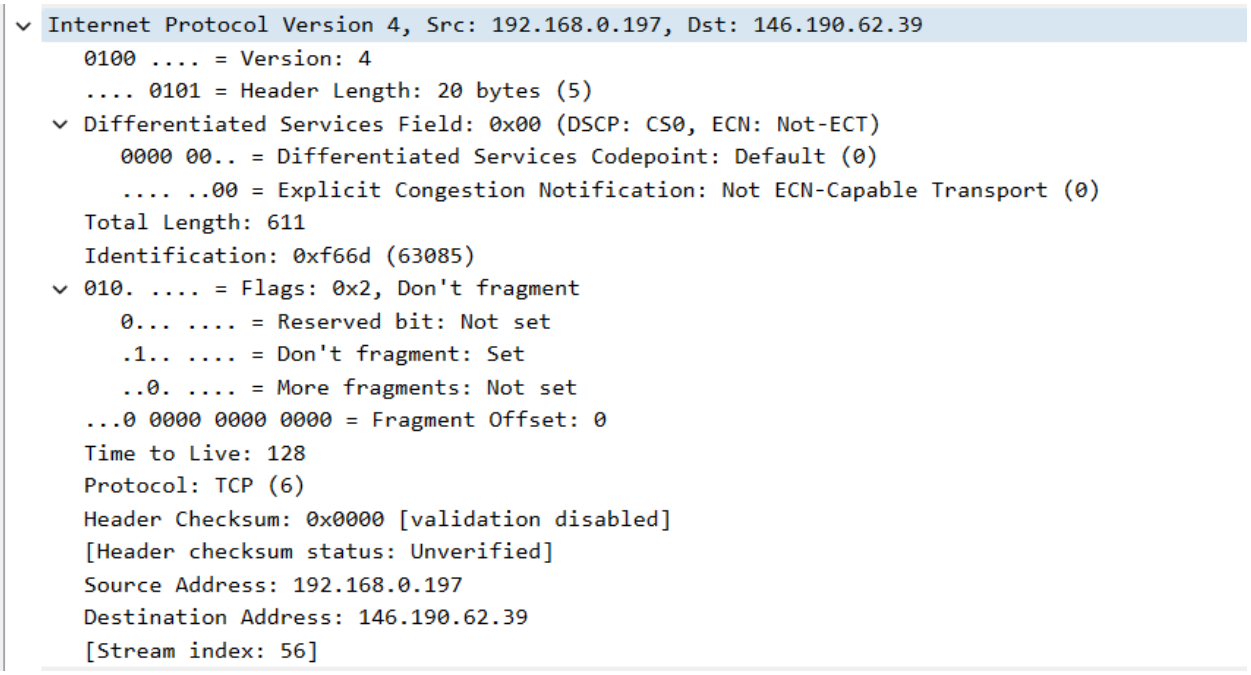
Ethernet:



This image shows the Ethernet II frame. It is a part of the Data Link Layer. The source and destination MAC addresses are displayed here. The Data Link layer manages the data transfer across the physical link by managing the frames structure, addressing (with MAC addresses),

error detection (through CRC), and access to the transmission medium. In this frame, we can see that the source and destination are both identified using their MAC addresses, making this is an Operation of Layer.

IPV4:



This image shows the IP packet. It is a part of Network Layer. The source IP address is 192.168.0.197 which is the IP of my desktop as it is HTTP request and destination IP address is 146.190.62.39 which is the IP of the website I pinged. The Network Layer is responsible for routing packets between different networks, and the IP header includes vital information like source and destination IP addresses, fragmentation details and routing information.

TCP:

```
Source Port: 50818
Destination Port: 80
[Stream index: 63]
[Stream Packet Number: 4]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 571]
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 1889553293
[Next Sequence Number: 572    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 2224898575
0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
Window: 517
[Calculated window size: 132352]
[Window size scaling factor: 256]
Checksum: 0x94a8 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
v [SEQ/ACK analysis]
   [iRTT: 0.241498000 seconds]
   [Bytes in flight: 571]
   [Bytes sent since last PSH flag: 571]
TCP payload (571 bytes)
```

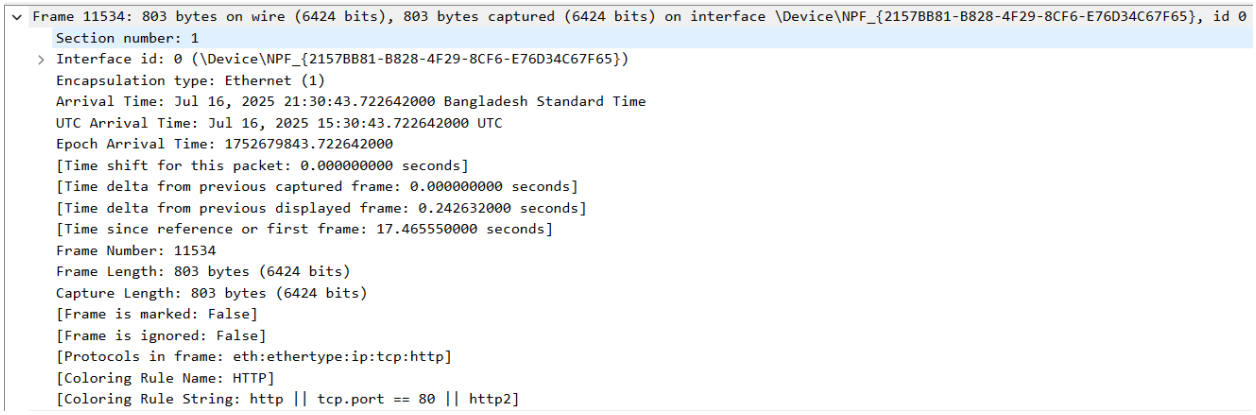
This shows the TCP segment which is a part of Transport Layer. It shows information like source port and destination port, sequence and acknowledgement numbers, flags, window size and the TCP Payload. Here, Source Port is 50818 which randomly generated for our device and Destination port is 80 which is well-known port for Web browsing. Here TCP segment length is 571, payload is 571 bytes, checksum is 0x94a8 ,header length 20 bytes and two bits are true which is acknowledgement and push bits.Window size is 132352 , sequence and acknowledgement both have value 1.

HTTP:

This image shows an HTTP request, which operates at the Application layer. The HTTP method is GET here which shows it is a HTTP request. It also shows other headers like URL(/) , Host, User-Agent, Accept and Connection. The Application manages communication between user application and network services, with HTTP being the protocol used for web-based interactions.

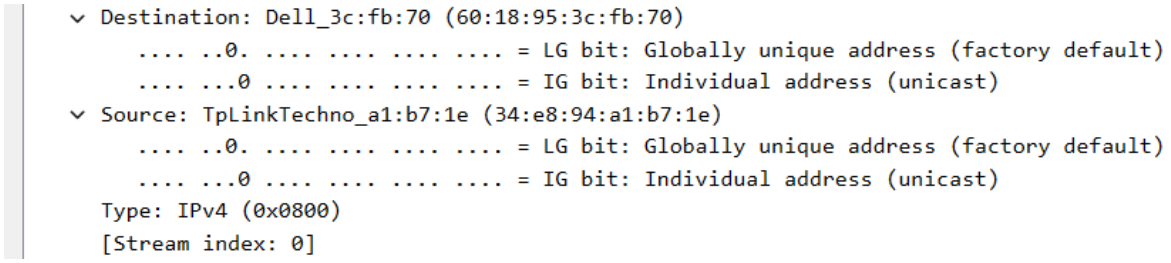
HTTP Response:

Frame:



This image shows details of the frame. Here , the frame length is 803 bytes and the captured frame length is also 803 bytes. It used HTTP and TCP protocols in application and Network layer. It also shows the timestamp of the response.

Ethernet:



This image shows the Ethernet II frame. The Data Link Layer handles the MAC addressing (source and destination), ensuring that data is transferred reliably across the local network. Here, the source MAC address (TpLinkTechno_a1:b7:1e) and destination MAC address (Dell_3c:fb:70) are shown, which helps ensure that the data reaches the correct physical device.

IPV4:

```
Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.197
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 789
    Identification: 0x1c8a (7306)
  010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 43
    Protocol: TCP (6)
    Header Checksum: 0x9e06 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 146.190.62.39
    Destination Address: 192.168.0.197
    [Stream index: 56]
```

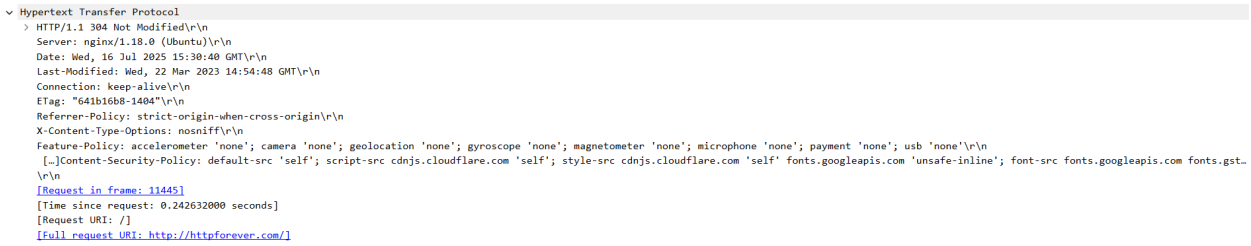
Again this image shows the IP addresses of destination and source devices. This time the addresses are reversed as it is a response packet. The source this time is 146.190.62.39 which is the IP address of the website and the destination IP address is 192.168.0.197 which is the IP address of my PC.

TCP:

```
Transmission Control Protocol, Src Port: 80, Dst Port: 50818, Seq: 1, Ack: 572, Len: 749
    Source Port: 80
    Destination Port: 50818
    [Stream index: 63]
    [Stream Packet Number: 6]
  [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 749]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2224898575
    [Next Sequence Number: 750    (relative sequence number)]
    Acknowledgment Number: 572    (relative ack number)
    Acknowledgment number (raw): 1889553864
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
    Window: 501
    [Calculated window size: 64128]
    [Window size scaling factor: 128]
    Checksum: 0x61fa [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
      [iRTT: 0.241498000 seconds]
      [Bytes in flight: 749]
      [Bytes sent since last PSH flag: 749]
    TCP payload (749 bytes)
```

This image shows the TCP information, here the port numbers are also reversed as it is a response packet now the source port is 80 which is the web port and the destination port is 50818 which is the port number my pc has been assigned. We can see now the sequence number is 1 and acknowledgement number is 571 that means data till 570 has been received. Here also the PSH and ACK flags are on.

HTTP:



This image shows that it is a HTTP response packet. It includes a response code which is 304 NOT MODIFIED. It means the requested resource has not been changed since last time it was accessed.