

ID: 20301318

## HTTP Request Packet

### Layer-1

```
▼ Frame 5309: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface \Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA})
    Interface name: \Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA}
    Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: May 13, 2025 23:40:49.244169000 Bangladesh Standard Time
    UTC Arrival Time: May 13, 2025 17:40:49.244169000 UTC
    Epoch Arrival Time: 1747158049.244169000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.004056000 seconds]
    [Time delta from previous displayed frame: 219.917655000 seconds]
    [Time since reference or first frame: 270.089598000 seconds]
    Frame Number: 5309
    Frame Length: 483 bytes (3864 bits)
    Capture Length: 483 bytes (3864 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Explanation: Frame is the physical layer header included in the Data Link Layer. This network frame information shows that the frame length is 483 bytes and the frame number is 5309. Moreover, the arrival date and time is also shown here.

### Layer-2

```
▼ Ethernet II, Src: AzureWaveTec_f5:c1:26 (10:68:38:f5:c1:26), Dst: TpLinkTechno_63:80:d5 (74:da:88:63:80:d5)
  ▼ Destination: TpLinkTechno_63:80:d5 (74:da:88:63:80:d5)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: AzureWaveTec_f5:c1:26 (10:68:38:f5:c1:26)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

Explanation: This layer is in the Data Link Layer. It contains the type, the source and the destination MAC addresses for node-to-node data transfer as well as error detection.

## Layer-3

```
▼ Internet Protocol Version 4, Src: 192.168.0.106, Dst: 54.236.92.255
  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: 469
  Identification: 0xdc11 (56337)
  ▼ 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: 128
  Protocol: TCP (6)
  Header Checksum: 0xc813 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.106
  Destination Address: 54.236.92.255
  [Stream index: 59]
```

Explanation: This layer is in the Network Layer that contains the source and destination IP addresses as well as header information for packet routing and addressing. Here the header length is 20 bytes.

## Layer-4

```
▼ Transmission Control Protocol, Src Port: 51375, Dst Port: 80, Seq: 1, Ack: 1, Len: 429
  Source Port: 51375
  Destination Port: 80
  [Stream index: 144]
  [Stream Packet Number: 4]
  ▼ [Conversation completeness: Incomplete, DATA (15)]
    ..0. .... = RST: Absent
    ...0 .... = FIN: Absent
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
    [Completeness Flags: ..DASS]
  [TCP Segment Len: 429]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 206851057
  [Next Sequence Number: 430      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 3526914926
  0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP...]
  Window: 255
  [Calculated window size: 65280]
  [Window size scaling factor: 256]
  Checksum: 0x6992 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  TCP payload (429 bytes)
```

Explanation: This layer is in the Transport Layer. It handles the TCP packets and key components such as source and destination port addresses, sequence number, acknowledgment number, and data segment length. The source port here is 51375 which is dynamically assigned by the client, while the destination port 80 is designated for HTTP traffic on the server. The sequence number or SEQ maintains the correct order of data segments, while the acknowledgment number or ACK allows the receiver to confirm successful data reception. The length or LEN field specifies the size of the transmitted data segment.

## Layer-5

```
▼ Hypertext Transfer Protocol
  ▼ GET / HTTP/1.1\r\n
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
  Host: eu.httpbin.org\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Response in frame: 5355]
  [Full request URI: http://eu.httpbin.org/]
```

Explanation: It is the Application Layer that contains HTTP requests, the GET method (identifies as the request packet). It also contains information regarding headers such as Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept etc. “Connection: keep-alive\r\n” This statement means that the connection is on and that it can send data.

# HTTP Response Packet

## Layer-1

```
▼ Frame 5355: 1007 bytes on wire (8056 bits), 1007 bytes captured (8056 bits) on interface \Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA})
    Interface name: \Device\NPF_{6A46FAD0-17C0-4617-9868-33B4EB9FFCCA}
    Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: May 13, 2025 23:40:53.886644000 Bangladesh Standard Time
    UTC Arrival Time: May 13, 2025 17:40:53.886644000 UTC
    Epoch Arrival Time: 1747158053.886644000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 4.642475000 seconds]
    [Time since reference or first frame: 274.732073000 seconds]
    Frame Number: 5355
    Frame Length: 1007 bytes (8056 bits)
    Capture Length: 1007 bytes (8056 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Explanation: Frame is the physical layer header included in the Data Link Layer. This network frame information shows that the frame length is 1007 bytes and the frame number is 5355. Moreover, the arrival date and time is also shown here.

## Layer-2

```
▼ Ethernet II, Src: TpLinkTechno_63:80:d5 (74:da:88:63:80:d5), Dst: AzureWaveTec_f5:c1:26 (10:68:38:f5:c1:26)
  ▼ Destination: AzureWaveTec_f5:c1:26 (10:68:38:f5:c1:26)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: TpLinkTechno_63:80:d5 (74:da:88:63:80:d5)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

Explanation: This layer is in the Data Link Layer. It contains the type, the source and the destination MAC addresses for node-to-node data transfer as well as error detection.

## Layer-3

```
▼ Internet Protocol Version 4, Src: 54.236.92.255, Dst: 192.168.0.106
  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: 993
  Identification: 0x5e25 (24101)
  ▼ 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: 240
  Protocol: TCP (6)
  Header Checksum: 0xd3f3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 54.236.92.255
  Destination Address: 192.168.0.106
  [Stream index: 59]
```

Explanation: This layer is in the Network Layer that contains the source and destination IP addresses as well as header information for packet routing and addressing. Here the header length is 20 bytes.

## Layer-4

```
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 51375, Seq: 8880, Ack: 430, Len: 953
  Source Port: 80
  Destination Port: 51375
  [Stream index: 144]
  [Stream Packet Number: 15]
  ▶ [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 953]
  Sequence Number: 8880 (relative sequence number)
  Sequence Number (raw): 3526923805
  [Next Sequence Number: 9833 (relative sequence number)]
  Acknowledgment Number: 430 (relative ack number)
  Acknowledgment number (raw): 206851486
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
  Window: 110
  [Calculated window size: 28160]
  [Window size scaling factor: 256]
  Checksum: 0x2d2b [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  TCP payload (953 bytes)
  TCP segment data (953 bytes)
  ▶ [8 Reassembled TCP Segments (9832 bytes): #5346(239), #5347(1440), #5348(1440), #5350(1440), #5352(1440), #5353(1440), #5354(1440), #5355(953)]
```

Explanation: This layer is in the Transport Layer. It handles the TCP packets and key components such as source and destination port addresses, sequence number, acknowledgment number, and data segment length. The source port here is 80 which is used by the server to send HTTP responses, while the destination port 51375 is the client's dynamic port number to receive the HTTP response. Port 80 serves as the default port for HTTP communication. The sequence number or SEQ maintains the correct order of

data segments, while the acknowledgment number or ACK allows the receiver to confirm successful data reception. The length or LEN field specifies the size of the transmitted data segment.

## Layer-5

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Tue, 13 May 2025 17:40:53 GMT\r\n
    Content-Type: text/html; charset=utf-8\r\n
    ▶ Content-Length: 9593\r\n
    Connection: keep-alive\r\n
    Server: gunicorn/19.9.0\r\n
    Access-Control-Allow-Origin: *\r\n
    Access-Control-Allow-Credentials: true\r\n
    \r\n
    [Request in frame: 5309]
    [Time since request: 4.642475000 seconds]
    [Request URI: /]
    [Full request URI: http://eu.httpbin.org/]
    File Data: 9593 bytes
```

Explanation: This is the Application Layer that contains the HTTP version (1.1) and Status code 200 (OK). It also contains HTTP response headers along with the date, content length, last modification date, server name etc.