

HTTP Request Packet (GET /) – Observed in Wireshark

```
▼ Frame 1408503: Packet, 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E})
    Interface name: \Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 6, 2025 00:29:26.458534000 Bangladesh Standard Time
    UTC Arrival Time: Nov 5, 2025 18:29:26.458534000 UTC
    Epoch Arrival Time: 1762367366.458534000
    [Time shift for this packet: 0.00000000 seconds]
    [Time delta from previous captured frame: 522.000 microseconds]
    [Time delta from previous displayed frame: 14.885000 milliseconds]
    [Time since reference or first frame: 10 minutes, 26.000573000 seconds]
    Frame Number: 1408503
    Frame Length: 518 bytes (4144 bits)
    Capture Length: 518 bytes (4144 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    Character encoding: ASCII (0)
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
▼ Ethernet II, Src: ASUSTekCOMPU_43:4c:8b (7c:10:c9:43:4c:8b), Dst: TPLink_67:f7:08 (3c:64:cf:67:f7:08)
  ▼ Destination: TPLink_67:f7:08 (3c:64:cf:67:f7:08)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: ASUSTekCOMPU_43:4c:8b (7c:10:c9:43:4c:8b)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

```
▼ Transmission Control Protocol, Src Port: 51578, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
  Source Port: 51578
  Destination Port: 80
  [Stream index: 538]
  [Stream Packet Number: 4]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 464]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2768854702
  [Next Sequence Number: 465 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 670114477
  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: 0x93dd [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  [Client Contiguous Streams: 1]
  [Server Contiguous Streams: 1]
  TCP payload (464 bytes)
```

```

▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: httpforever.com\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/141.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Referer: https://www.google.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Response in frame: 1408045]
  [Full request URI: http://httpforever.com/]

▼ Internet Protocol Version 4, Src: 192.168.0.101, Dst: 146.190.62.39
  0100 .... = Version: 4
  ... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 504
  Identification: 0xdcdc (56540)
  ▶ 010. .... = Flags: 0x2, Don't fragment
  ... 0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.101
  Destination Address: 146.190.62.39
  [Stream index: 168]

```

Frame Layer (Physical)

- Packet number: 1408503
- Size: 518 bytes
- Arrival time: shows when the packet reached my computer
- This layer just tells Wireshark about the physical capture, nothing about the actual data.

Ethernet II (Data Link)

- Source MAC: my computer (7c:10:c9:43:4c:8b)
- Destination MAC: router (3c:64:cf:67:f7:08)
- Type: IPv4 → tells that the next layer is IP
- This is how my computer communicates on the local network.

IP Layer (Network)

- Source IP: 192.168.0.101 → my computer
- Destination IP: 146.190.62.39 → server
- TTL: 128 → how many hops the packet can take
- Protocol: TCP → the next layer is TCP
- This layer is responsible for sending the packet to the right computer over the internet.

TCP Layer (Transport)

- Source port: 51578 → random client port
- Destination port: 80 → standard HTTP port
- Sequence number & acknowledgment number → keep track of packet order
- Flags: PSH, ACK → PSH means send data immediately, ACK confirms previous data
- Window size: 65280 → flow control
- TCP ensures reliable delivery of the HTTP data.

HTTP Layer (Application)

- GET / HTTP/1.1 → requesting the home page
- Host: httpforever.com → target server
- Connection: keep-alive → keep TCP connection open
- User-Agent → tells server which browser I am using
- Accept → types of content my browser can handle
- Other headers: referer, encoding, language
- This layer contains the actual web request I am sending

HTTP Response Packet — Observed in Wireshark

```
▼ Frame 1412281: Packet, 1331 bytes on wire (10648 bits), 1331 bytes captured (10648 bits) on interface \Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E}, id 0
  Section number: 1
  ▾ Interface id: 0 (\Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E})
    Interface name: \Device\NPF_{83604A78-22EC-43B4-BB2F-050FD635436E}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 6, 2025 00:29:27.765521000 Bangladesh Standard Time
    UTC Arrival Time: Nov 5, 2025 18:29:27.765521000 UTC
    Epoch Arrival Time: 1762367367.765521000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 333.000 microseconds]
    [Time delta from previous displayed frame: 2.254000 milliseconds]
    [Time since reference or first frame: 10 minutes, 27.307560000 seconds]
    Frame Number: 1412281
    Frame Length: 1331 bytes (10648 bits)
    Capture Length: 1331 bytes (10648 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http+xml]
    Character encoding: ASCII (8)
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]

▼ Ethernet II, Src: TPLink_67:f7:08 (3c:64:cf:67:f7:08), Dst: ASUSTekCOMPU_43:4c:8b (7c:10:c9:43:4c:8b)
  ▾ Destination: ASUSTekCOMPU_43:4c:8b (7c:10:c9:43:4c:8b)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: TPLink_67:f7:08 (3c:64:cf:67:f7:08)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]

  ▾ Internet Protocol Version 4, Src: 146.190.62.39, Dst: 192.168.0.101
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1317
    Identification: 0x9d11 (40209)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 48
    Protocol: TCP (6)
    Header Checksum: 0x16cf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 146.190.62.39
    Destination Address: 192.168.0.101
    [Stream index: 168]
```

```

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 56036, Seq: 1, Ack: 417, Len: 1277
  Source Port: 80
  Destination Port: 56036
  [Stream index: 539]
  [Stream Packet Number: 6]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 1277]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1794358368
  [Next Sequence Number: 1278 (relative sequence number)]
  Acknowledgment Number: 417 (relative ack number)
  Acknowledgment number (raw): 2676273008
  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: 501
  [Calculated window size: 64128]
  [Window size scaling factor: 128]
  Checksum: 0xd35a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ [Timestamps]
  ▶ [SEQ/ACK analysis]
  [Client Contiguous Streams: 1]
  [Server Contiguous Streams: 1]
  TCP payload (1277 bytes)

▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
  Server: nginx/1.18.0 (Ubuntu)\r\n
  Date: Wed, 05 Nov 2025 18:29:27 GMT\r\n
  Content-Type: image/svg+xml\r\n
  Content-Length: 451\r\n
  Last-Modified: Wed, 16 Nov 2022 20:59:46 GMT\r\n
  Connection: keep-alive\r\n
  ETag: "63754f42-1c3"\r\n
  Referrer-Policy: strict-origin-when-cross-origin\r\n
  X-Content-Type-Options: nosniff\r\n
  Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'
  [...] Content-Security-Policy: default-src 'self'; script-src cdnjs.cloudflare.com 'self' 'report-sha256'; style-src cdnjs.cloudflare.com 'self' fonts.googleapis.com 'self';
  Accept-Ranges: bytes\r\n
  \r\n
  [Request in frame: 1411563]
  [Time since request: 223.635000 milliseconds]
  [Request URI: /css/images/header-major-on-light.svg]
  [Full request URI: http://httpforever.com/css/images/header-major-on-light.svg]
  File Data: 451 bytes

```

Frame Layer (Physical)

- Packet number: 1412281
- Size: 1331 bytes
- Arrival time: shows when the response reached my computer
- This layer just gives basic info about the captured packet.

Ethernet II (Data Link)

- Source MAC: 3c:64:cf:67:f7:08 → server/router
- Destination MAC: 7c:10:c9:43:4c:8b → my computer
- Type: IPv4 → next layer is IP
- Shows how the server communicates with my computer over the local network.

IP Layer (Network)

- Source IP: 146.190.62.39 → server
- Destination IP: 192.168.0.101 → my computer
- TTL: 48 → number of hops allowed
- Protocol: TCP → transport layer protocol
- Total Length: 1317 bytes → size of IP packet including TCP and HTTP data

- Responsible for routing the packet from the server to my computer.

TCP Layer (Transport)

- Source Port: 80 → standard HTTP port on server
- Destination Port: 56036 → client port on my computer
- Sequence Number: 1 → position of first byte in this segment
- Acknowledgment Number: 417 → confirms receipt of previous request bytes
- Flags: PSH, ACK → PSH pushes the data to the application immediately, ACK confirms request was received
- Window size: 64128 → flow control
- Ensures reliable delivery of the HTTP response.

HTTP Layer (Application)

- Status Line: HTTP/1.1 200 OK → server successfully processed my GET request
- Server: nginx/1.18.0 → web server software
- Date: Wed, 05 Nov 2025 18:29:27 GMT → server timestamp
- Content-Type: image/svg+xml → type of data sent
- Content-Length: 451 → size of the payload
- Connection: keep-alive → TCP connection stays open for future requests
- ETag, Referrer-Policy, X-Content-Type-Options, Feature-Policy → additional security and caching info
- This layer contains the actual web content sent from the server to my browser.