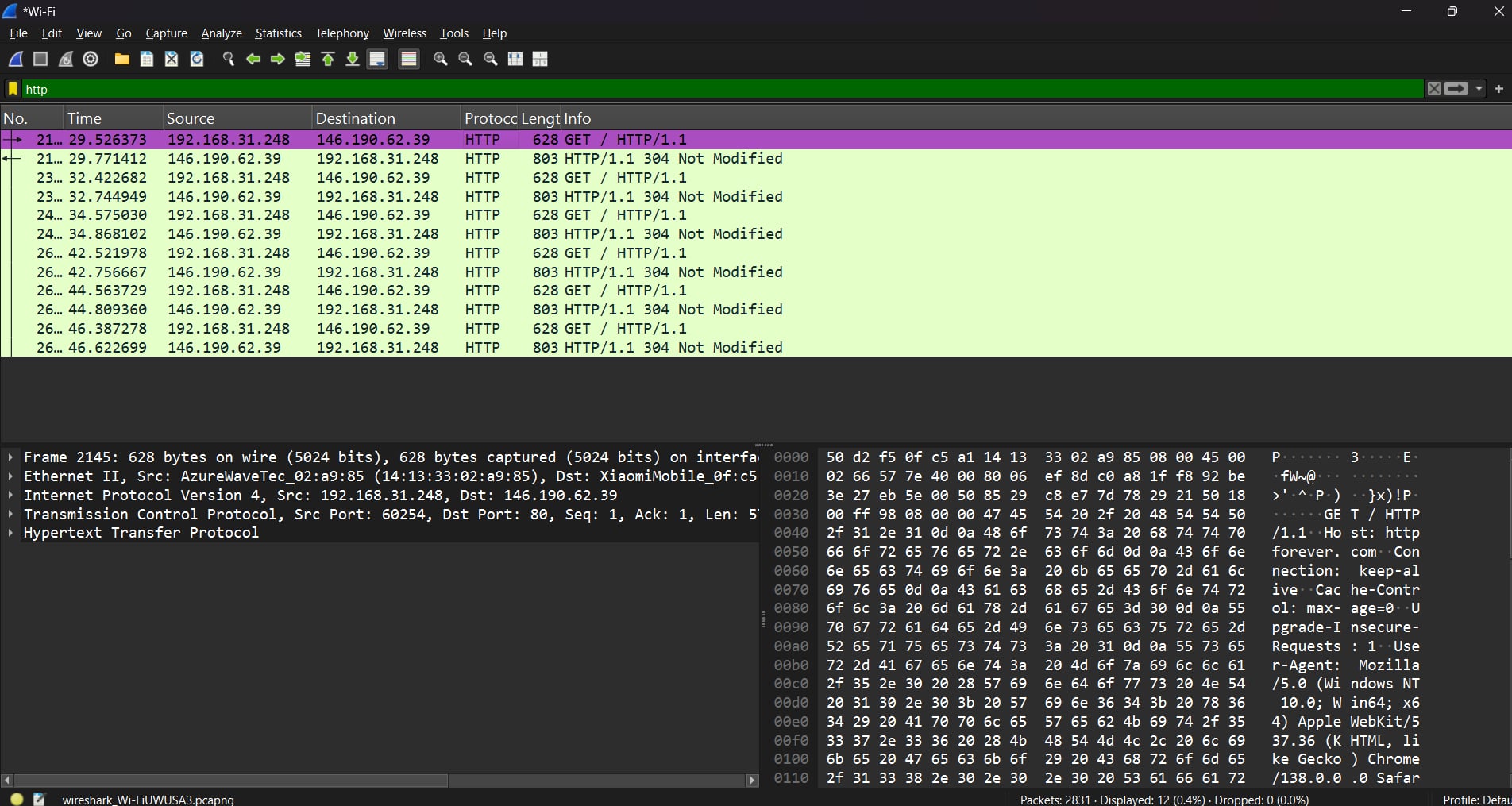
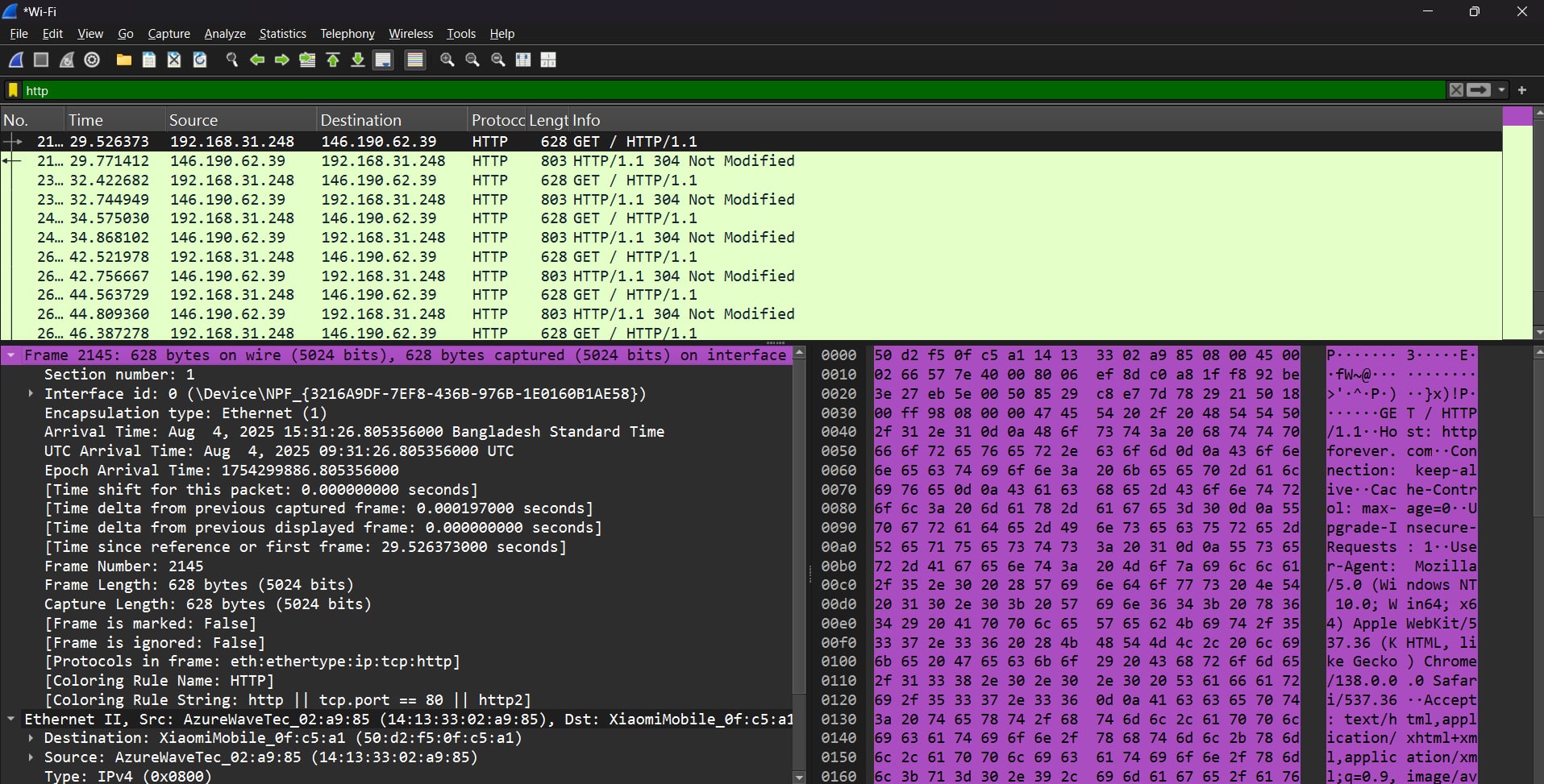
**Wireshark**

My IP address 🡪 192.168.31.248

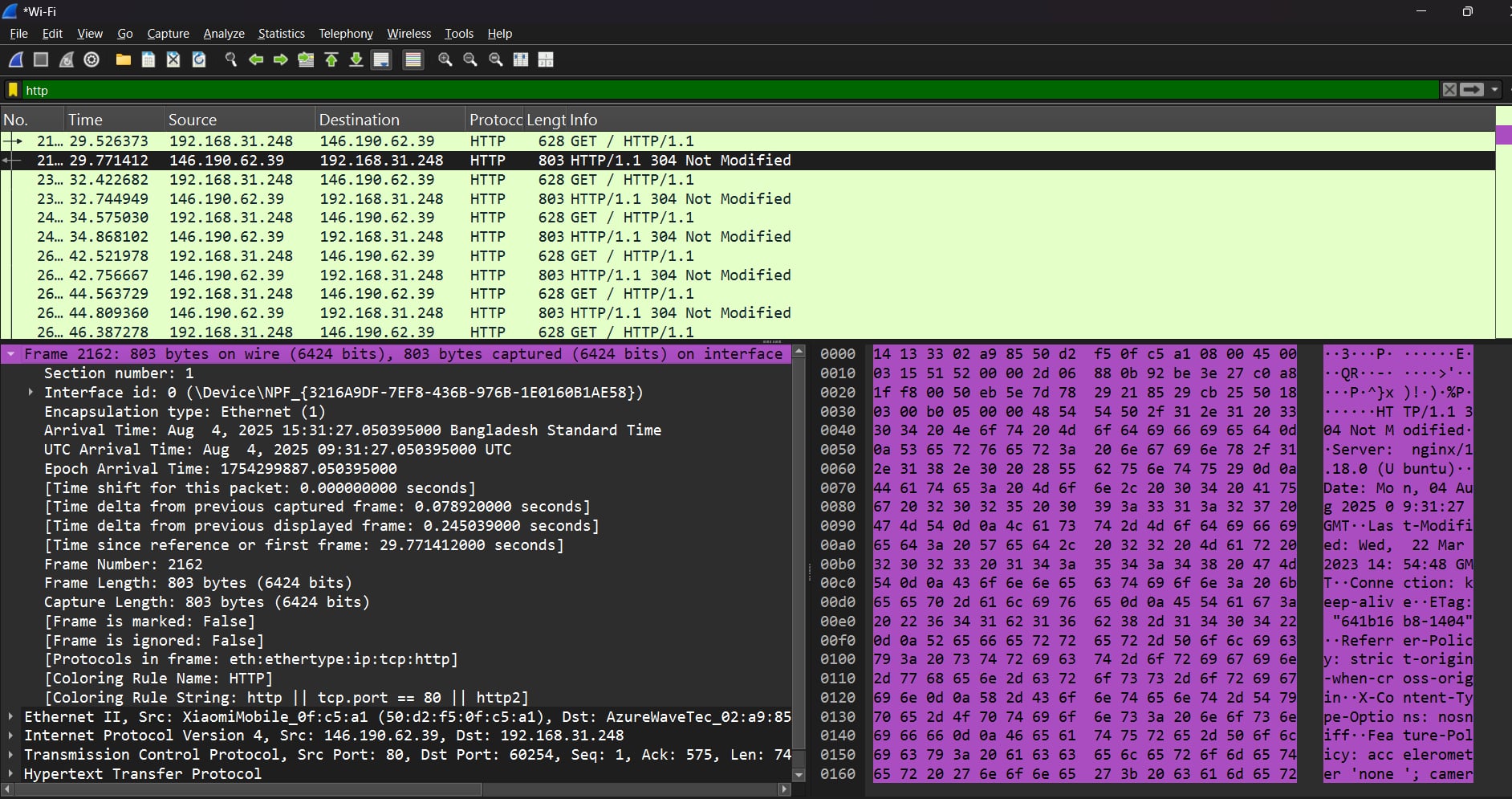
HTTP Forever IP address 🡪 146.190.62.39



**Frame**The request packet is shown below: -

Frame falls under the datalink layer with 628 bytes on both wire and interface captured. The frame indicator is 2145

The response packet is shown below: -

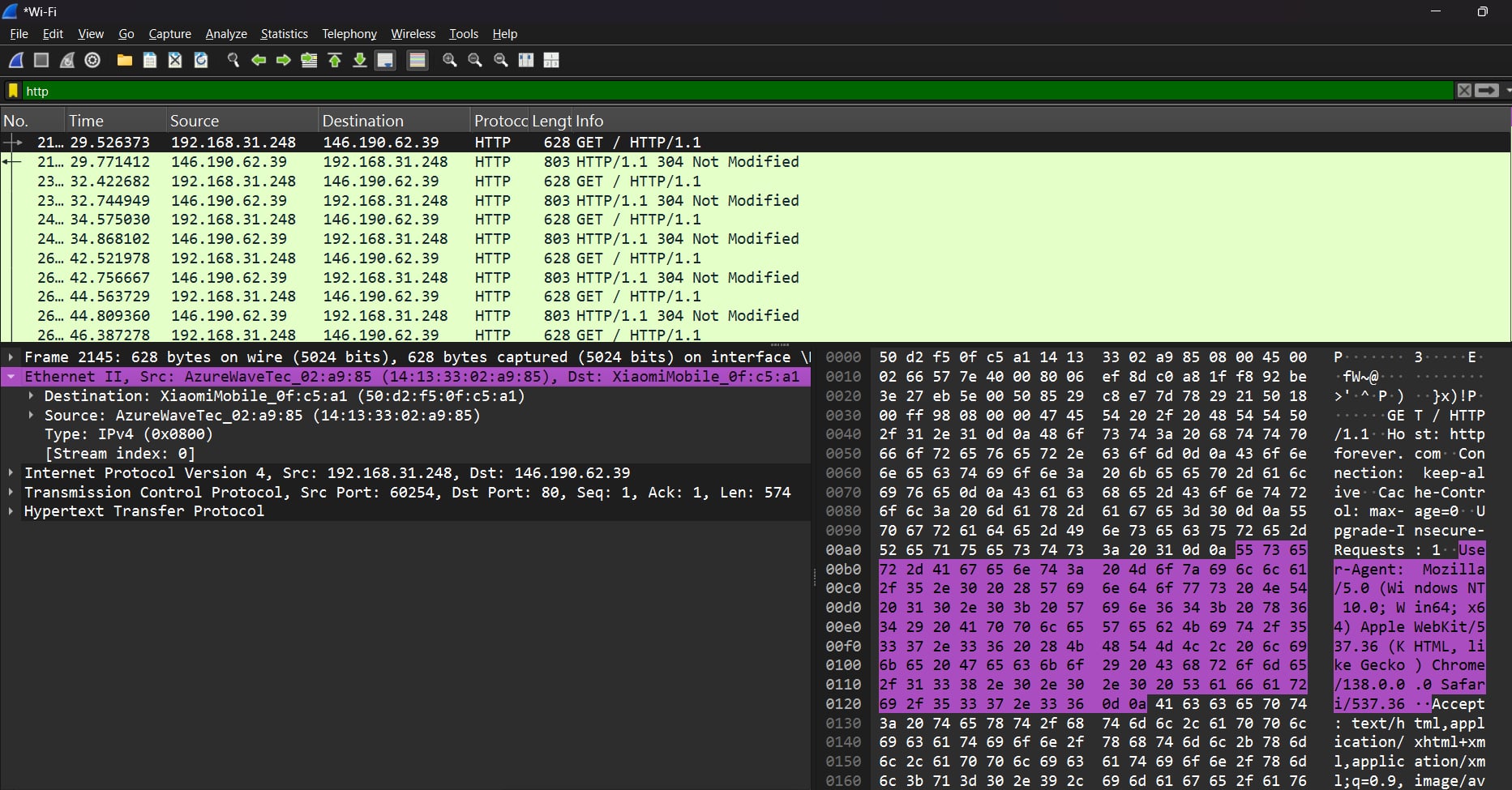


Similarly Frame 2162 captures 803 bytes on both wire and interface on the response packet during this transmission.

**Ethernet**

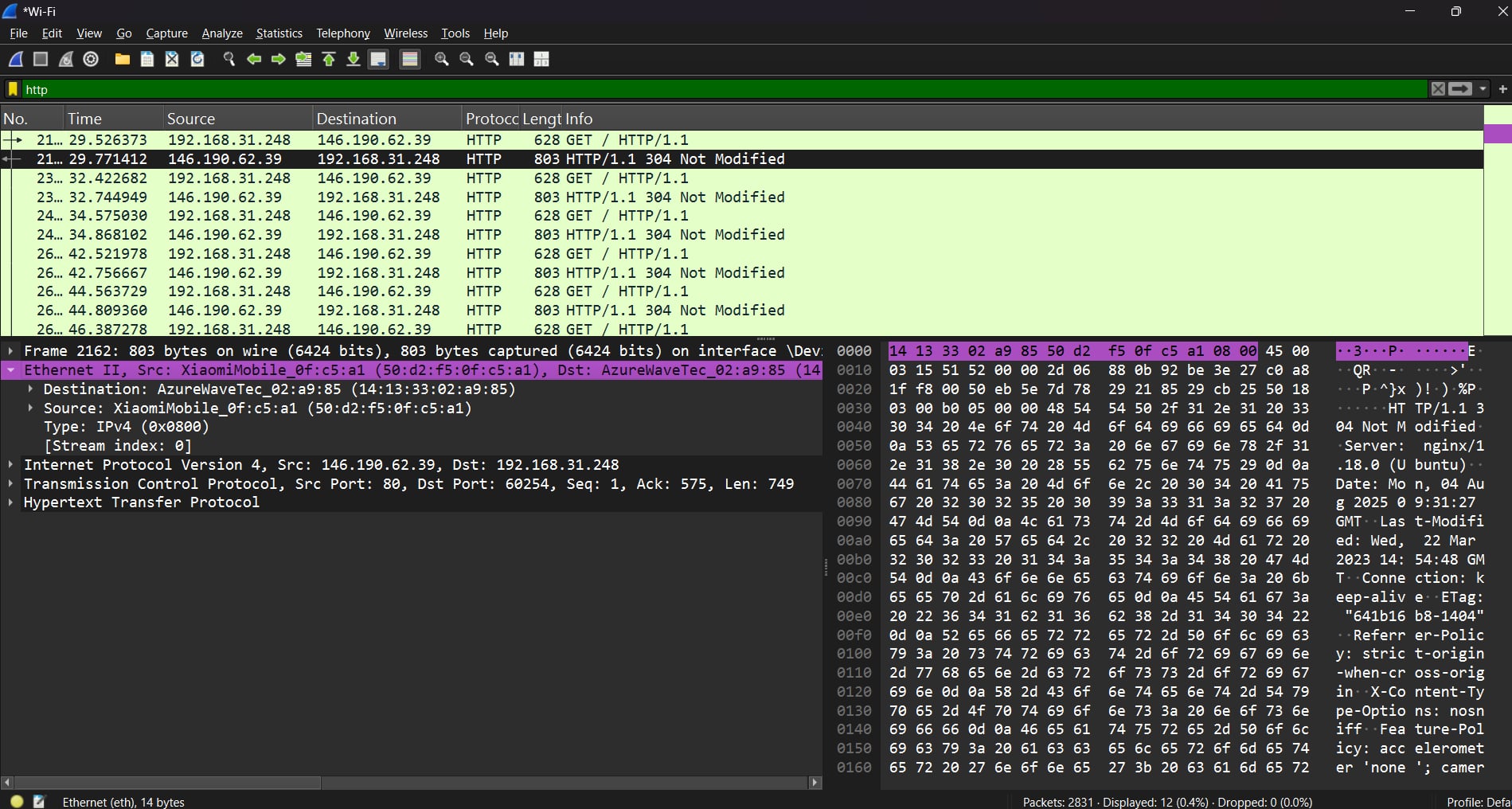
It falls under the data link layer

The request packet is shown below:



Ethernet2 falls under the datalink layer. The **source** indicates the device's MAC address that will send the frame: AzureWaveTec\_02:a9:85 (14:13:33:02:a9:85). The **destination** is the device that will receive the frame: XiaomiMobile\_0f:c5:a1 (50:d2:f5:0f:c5:a1). Both addresses are shown in hexadecimal format, with a human-readable name for the vendor prefix. This frame is a response originating from IP 192.168.31.248 to 146.190.62.39.

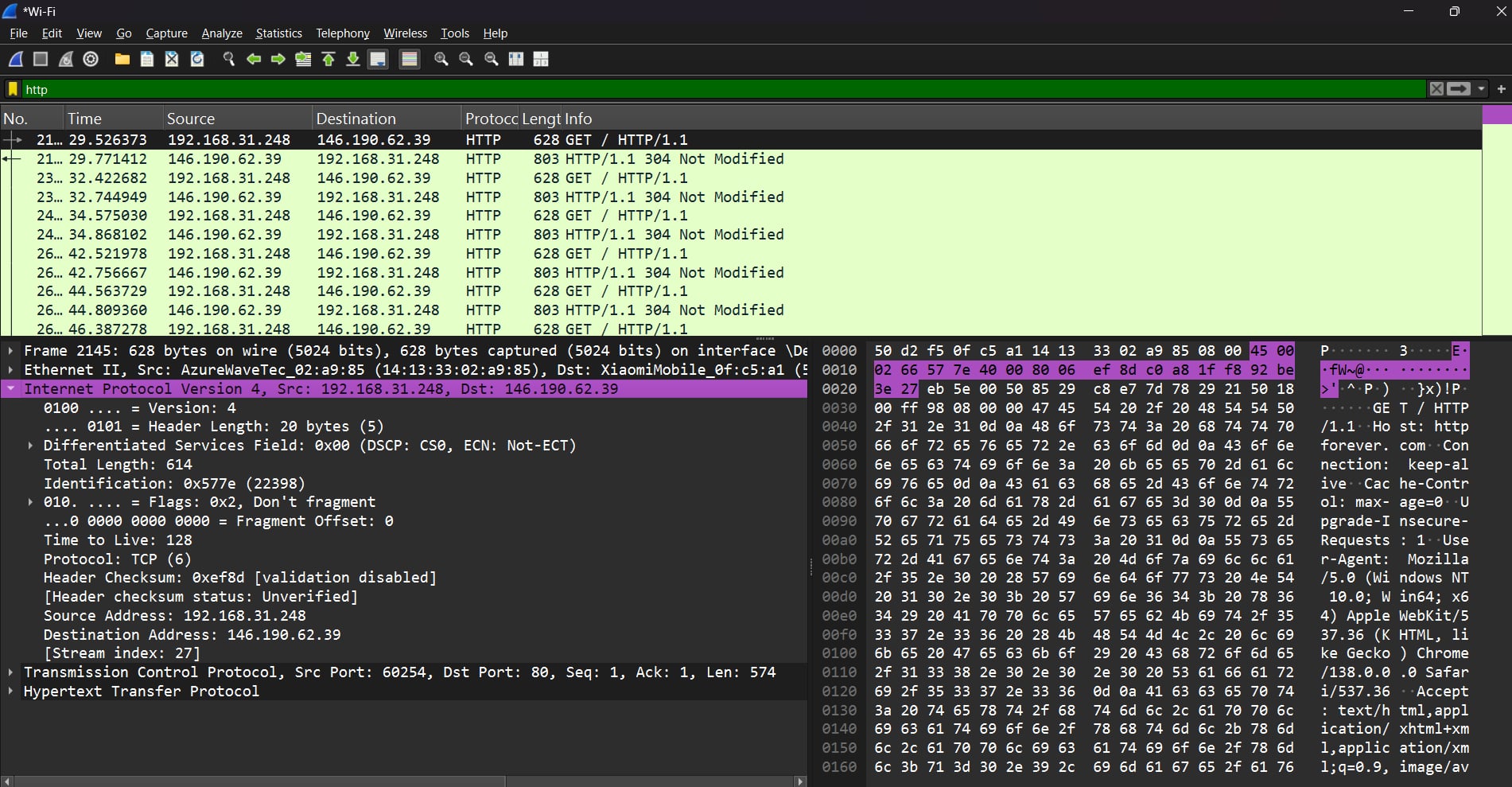
The response packet is shown below:



The source indicates the device's MAC address that will send the frame: XiaomiMobile\_0f:c5:a1 (50:d2:f5:0f:c5:a1). The destination is the device that will receive the frame: AzureWaveTec\_02:a9:85 (14:13:33:02:a9:85). Both addresses are shown in hexadecimal format, with a human-readable name for the vendor prefix. This frame is a request originating from IP 146.190.62.39 to 192.168.31.248.

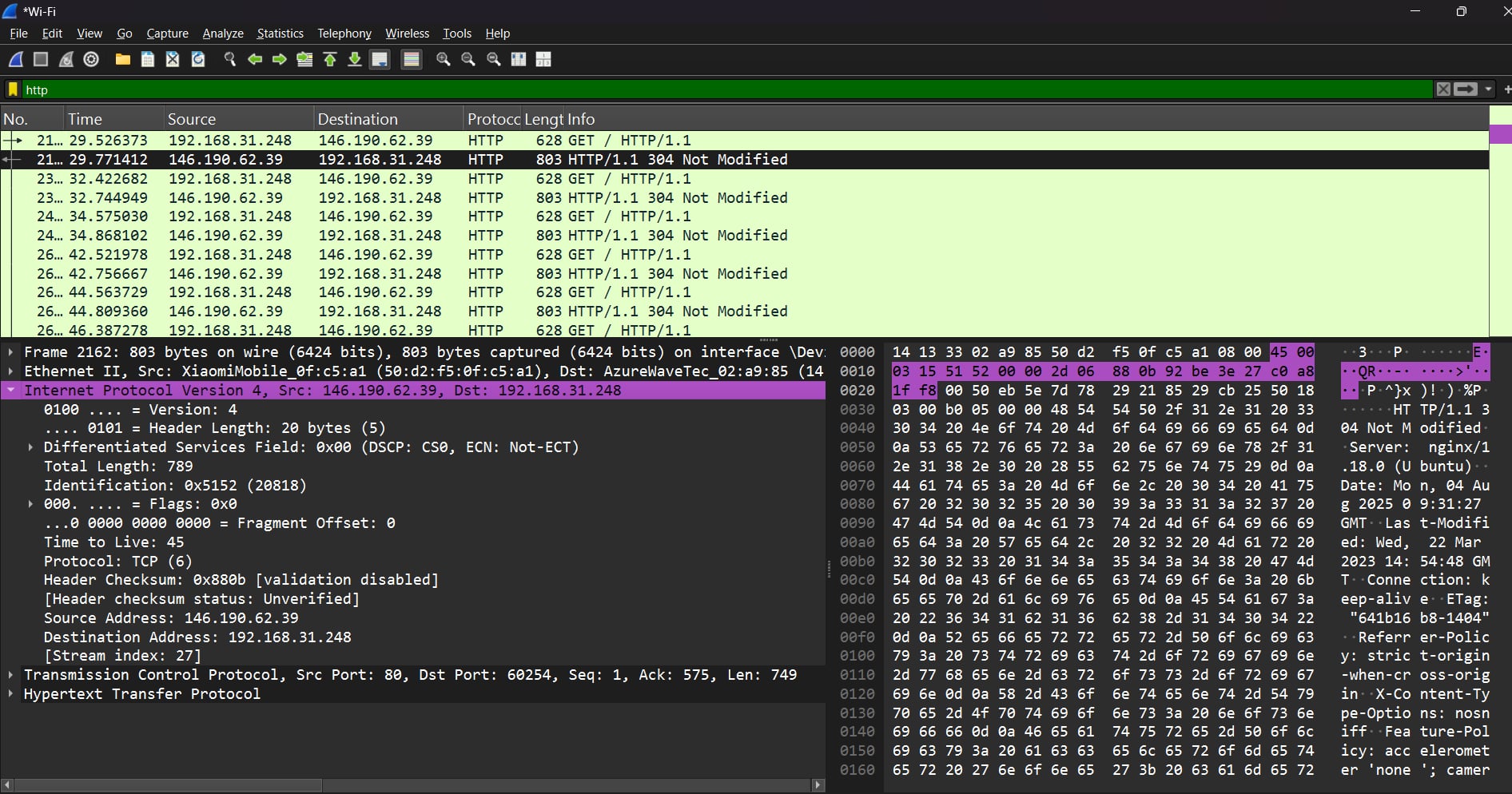
**Internet Protocol Version 4:**

The request packet is shown below:



It is an **IPv4** packet, which operates at the **network layer**. The packet has a **Header Length** of 20 bytes (5 \* 32-bit words) and a **Total Length** of 614 bytes. The **source IP address** is 192.168.31.248, and the **destination IP address** is 146.190.62.39. The **Time to Live (TTL)** is set to 128. The **Protocol** is TCP (indicated by the number 6), and the **Don't Fragment** flag is set, which means this packet must not be fragmented. The **identification number** for this packet is 0x577e (or 22398).

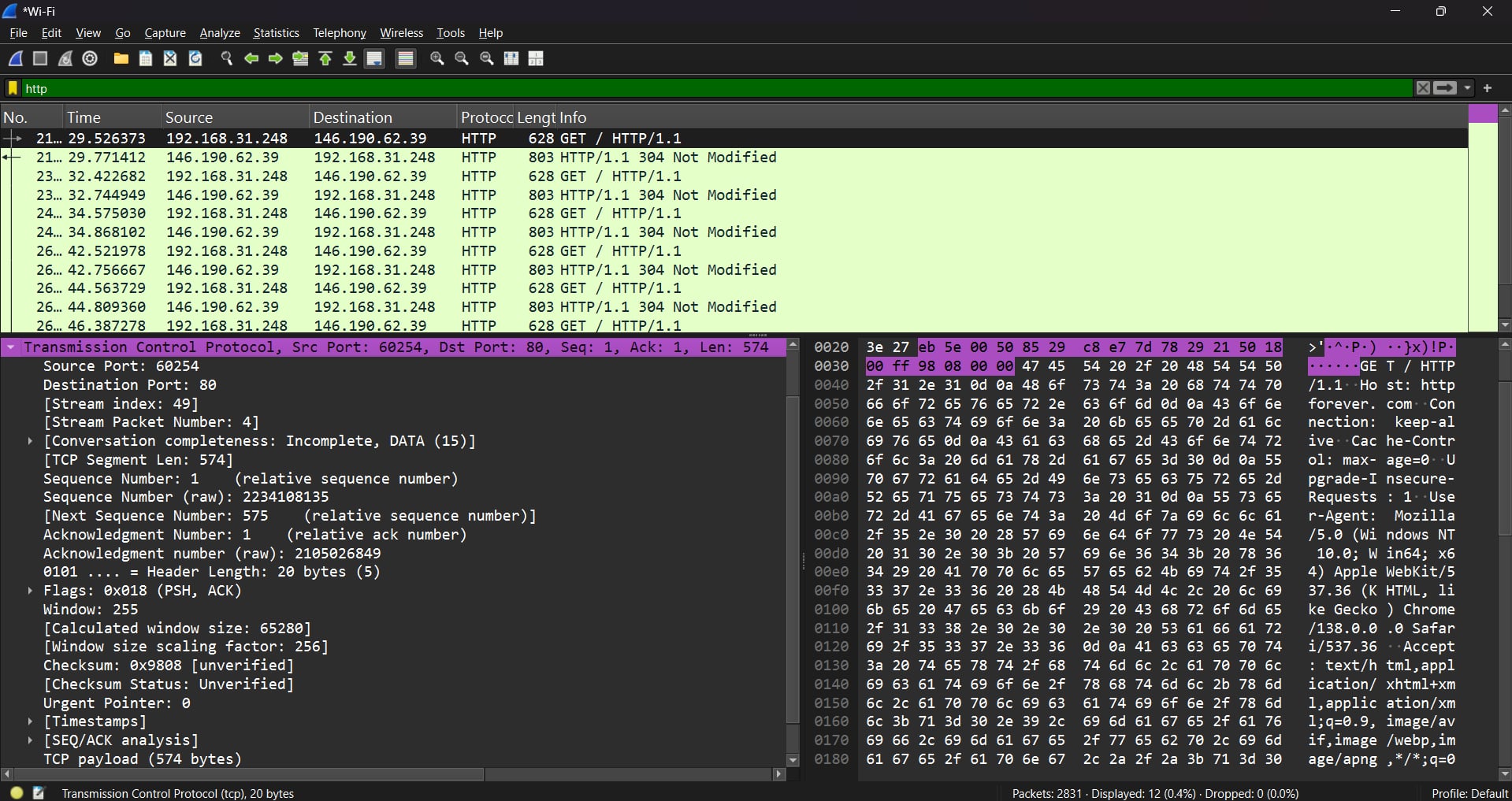
The response packet is shown below:



It is an **IPv4** packet, which operates at the **network layer**. The packet has a **Header Length** of 20 bytes (5 \* 32-bit words) and a **Total Length** of 789 bytes. The **source IP address** is 146.190.62.39, and the **destination IP address** is 192.168.31.248. The **Time to Live (TTL)** is set to 45. The **Protocol** is TCP (indicated by the number 6), and the **Flags** are all set to 0, which means this packet **can be fragmented** if necessary. The **identification number** for this packet is 0x5152 (or 20818).

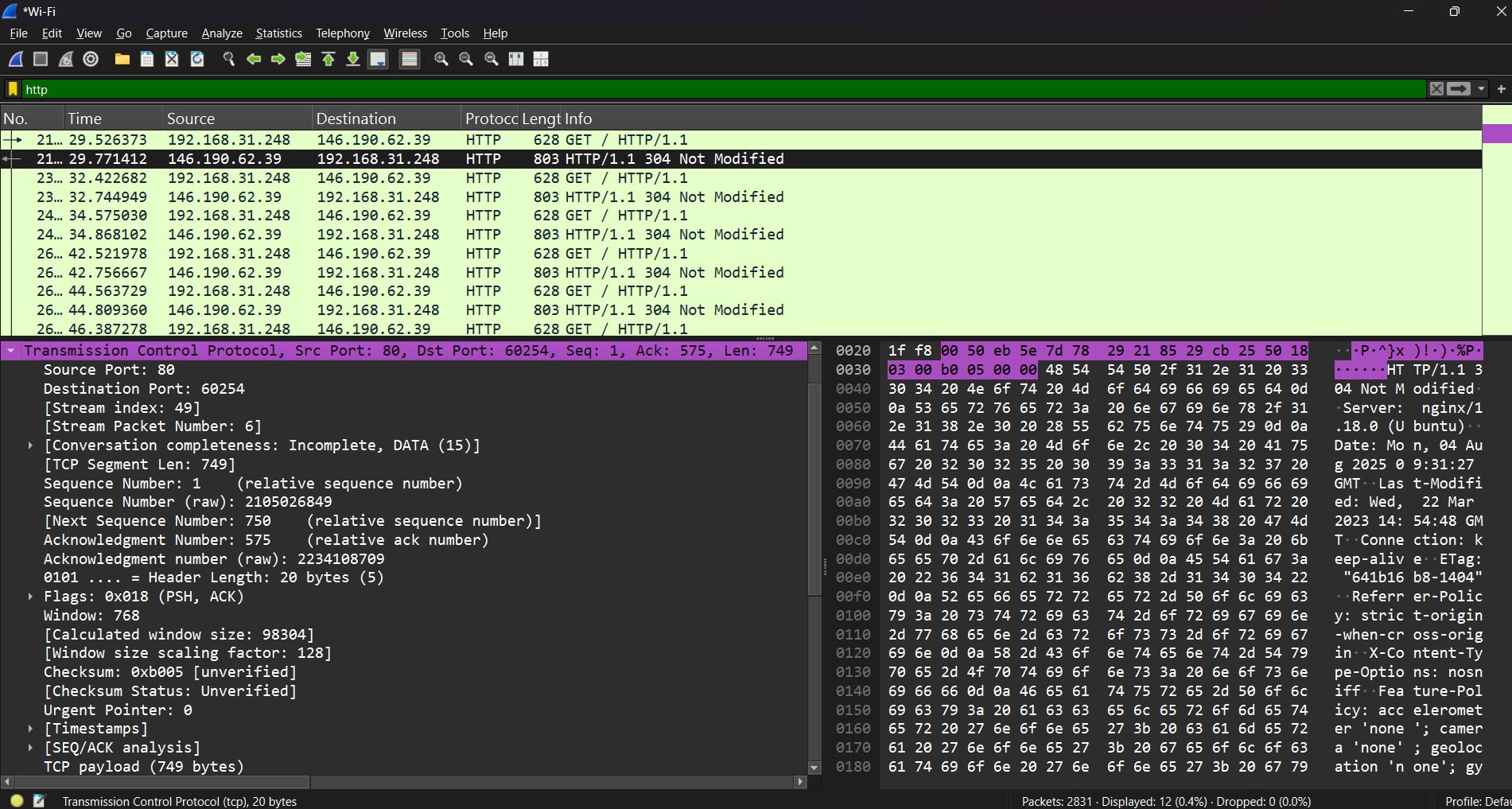
**Transmission Control Protocol:**

The request packet is shown below:



Here, **Source port is 60254**. This indicates the sending device started the conversation. **Destination port is 80**. This indicates the data is meant for a web server, making this conversation likely part of an online Browse session. The **Sequence number is 1** (relative) with a raw number of 2234108135. It also has an **Acknowledgement number of 1** (relative), with a raw number of 2105026849. The **Next sequence number is 575**, which means the segment contains 574 bytes of data.

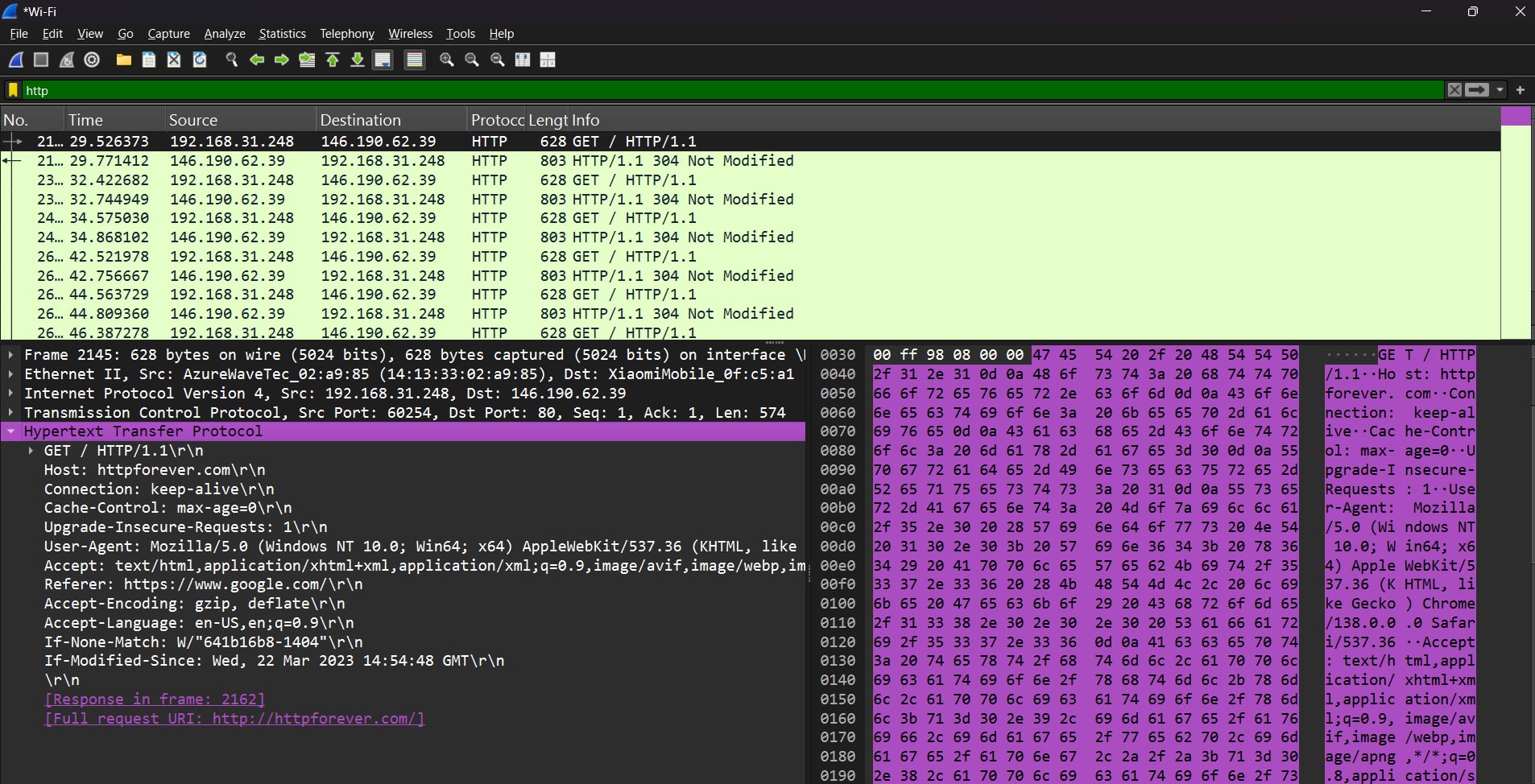
The response packet is shown below:



Here, Source port is 80. This indicates the web server is sending the data. Destination port is 60254. This indicates the packet is a response to the client. The Sequence number is 1 (relative) with a raw number of 2105026849. The Acknowledgement number is 575 (relative), with a raw number of 2234108709. This confirms that the recipient has received the first packet and is now expecting the next segment to start at sequence number 575. The Next sequence number is 750, which means the segment contains 749 bytes of data.

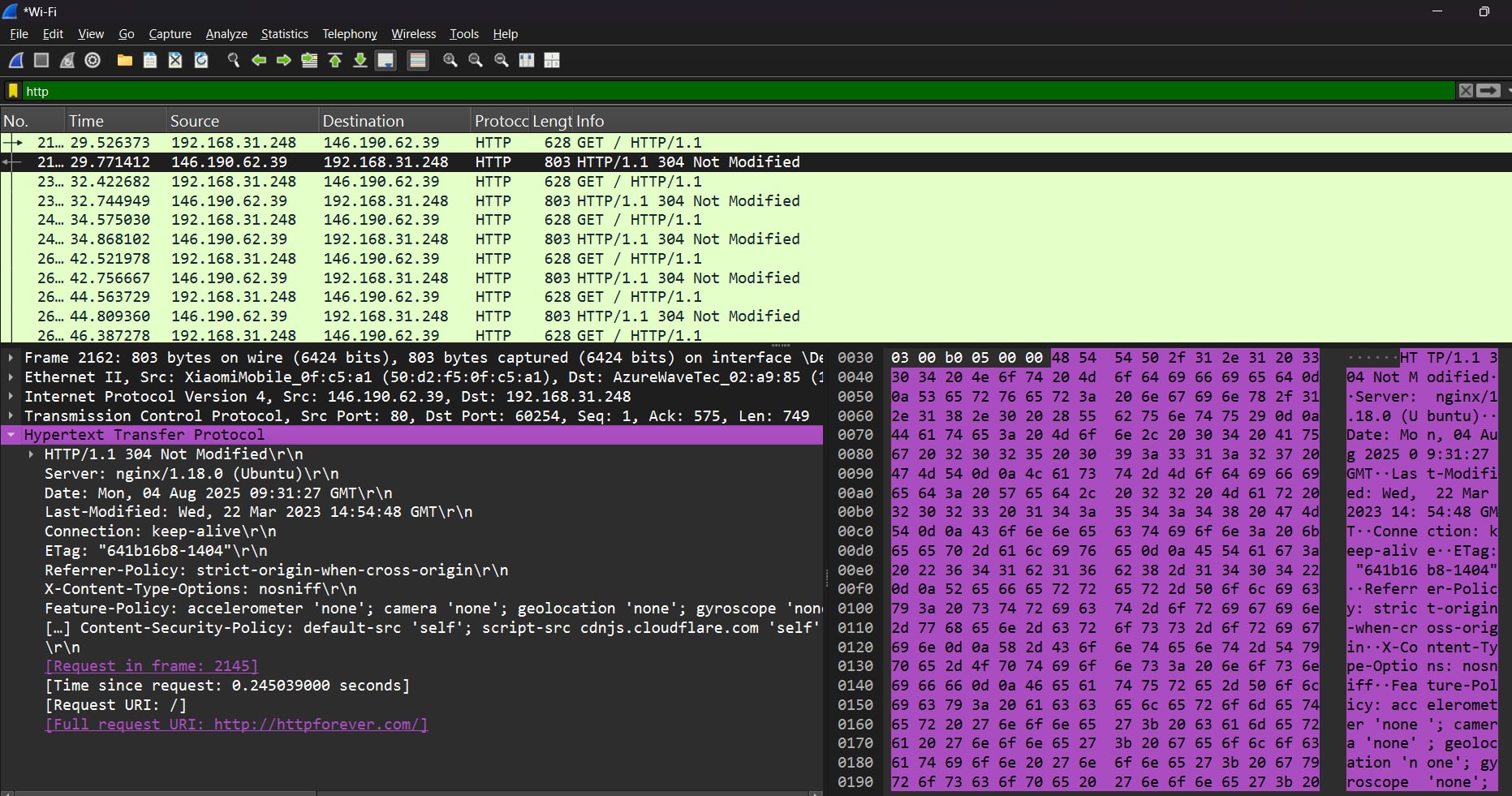
**Hypertext transfer protocol:**

The request packet is shown below:



Here, the browser is fetching information using the **"GET" method**. The requested host is **"httpforever.com"** as displayed in the "Host" line. The **"Connection"** header asks for the connection to remain open for future exchanges. The **"Cache-Control"** header, set to max-age=0, tells the browser to always check with the server for a fresh copy of the page. The **"User-Agent"** header indicates the operating system is Windows 10 and the browser is Chrome. The browser also sends an **"If-None-Match"** header with a tag "641b16b8-1404", which is an identifier for a specific version of the requested resource. The **"If-Modified-Since"** header indicates the last time the resource was modified, allowing the server to check if a newer version is available.

The response packet is shown below:

****

Here, the server has sent a response with the status code "HTTP/1.1 304 Not Modified". This means the resource requested by the browser has not changed since the last time it was fetched, so the server did not send the entire content again. The "Server" header indicates the web server software is nginx running on Ubuntu. The "Date" and "Last-Modified" headers provide timestamps for the server's response and the last time the resource was changed. The "ETag" header contains the identifier "641b16b8-1404", which matches the If-None-Match header from the browser's request, confirming the resource has not been modified. The "Connection" header is set to keep-alive, which means the server is also willing to keep the connection open for subsequent requests.