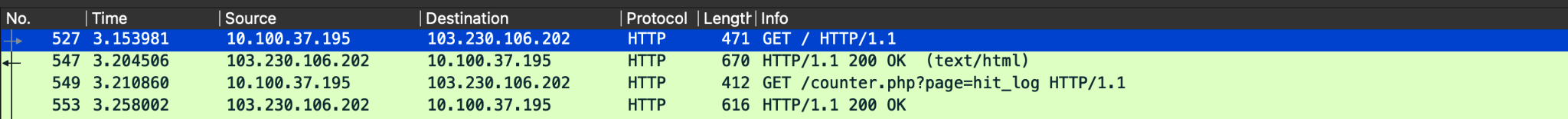
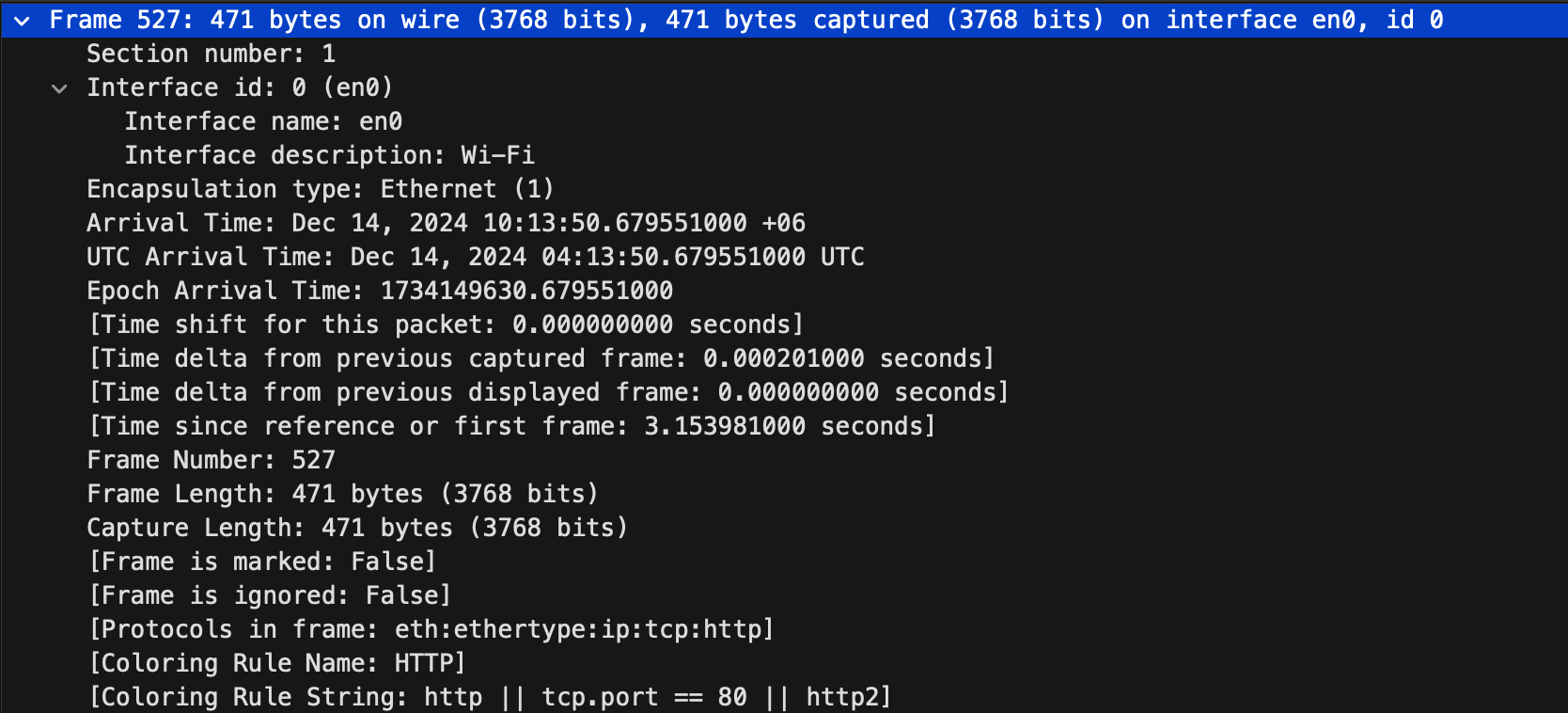
**Answer to the Question no 02(Wireshark):**

The layers of the captured networks using wireshark are explained below:

**HTTP Request header packet:**

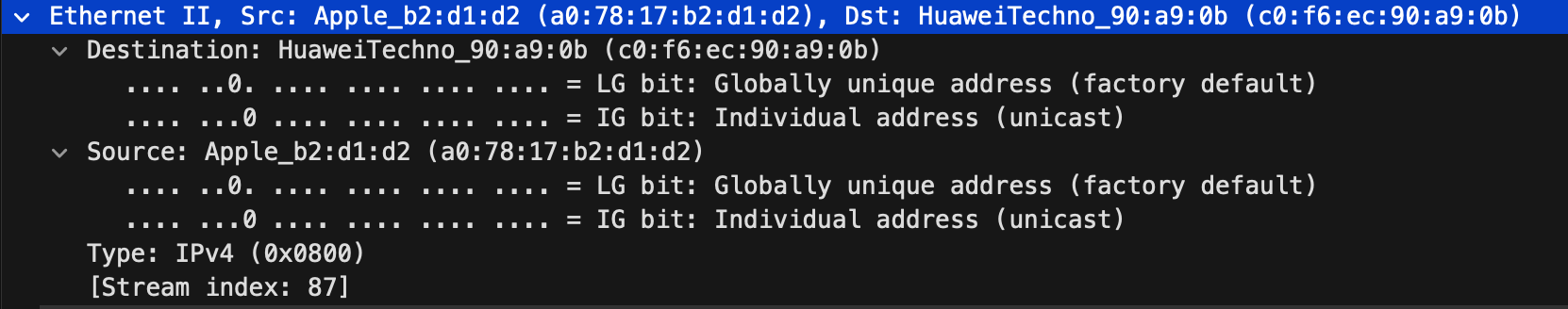
****

**(i) Frame 527/Physical Layer:**



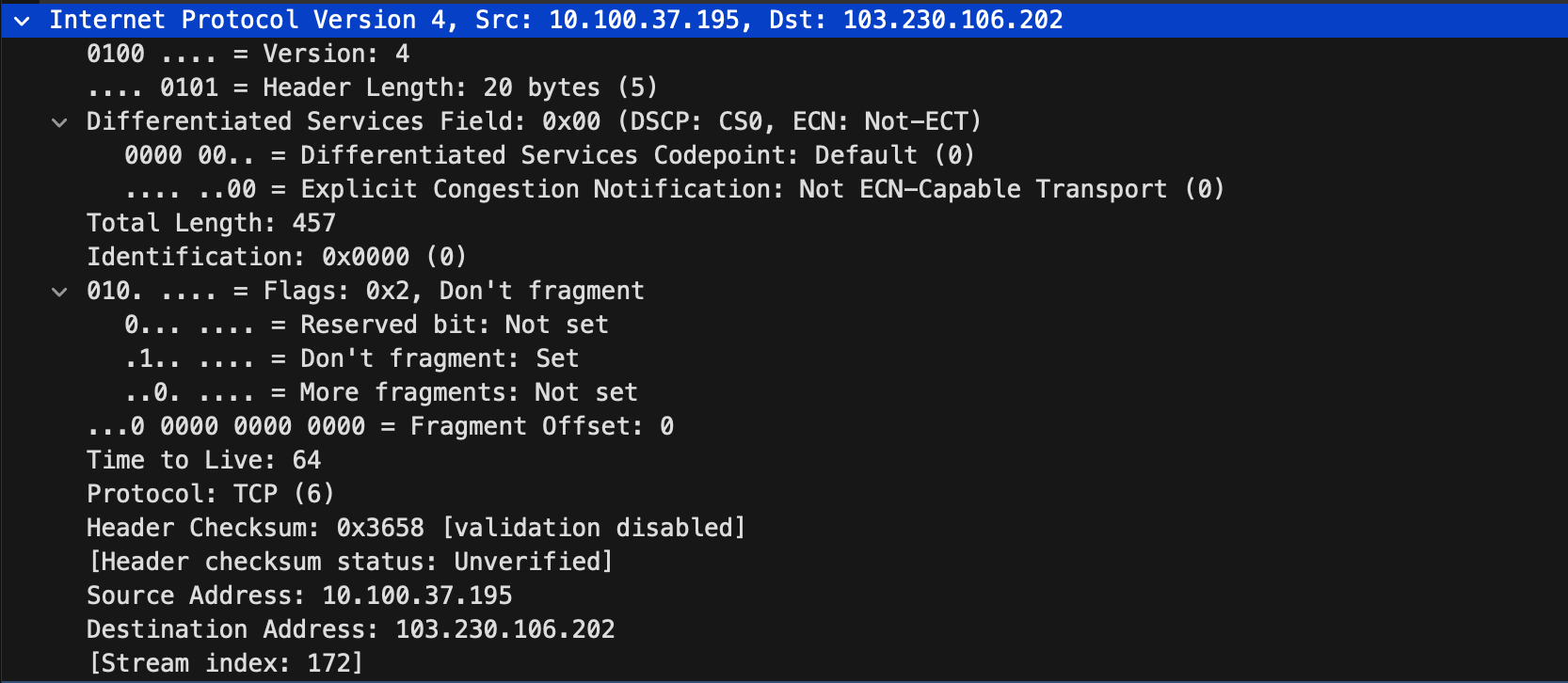
This layer uses the protocol of the **Physical Layer.** This Ethernet frame is part of an HTTP communication observed on interface en0, which indicates Wi-Fi interface. The arrival time is **December 14, 2024, 10:13:50.679551000 UTC+6** (local time), with no time shift or delay from the previous frame.

**(ii) Ethernet II/Datalink Layer:**



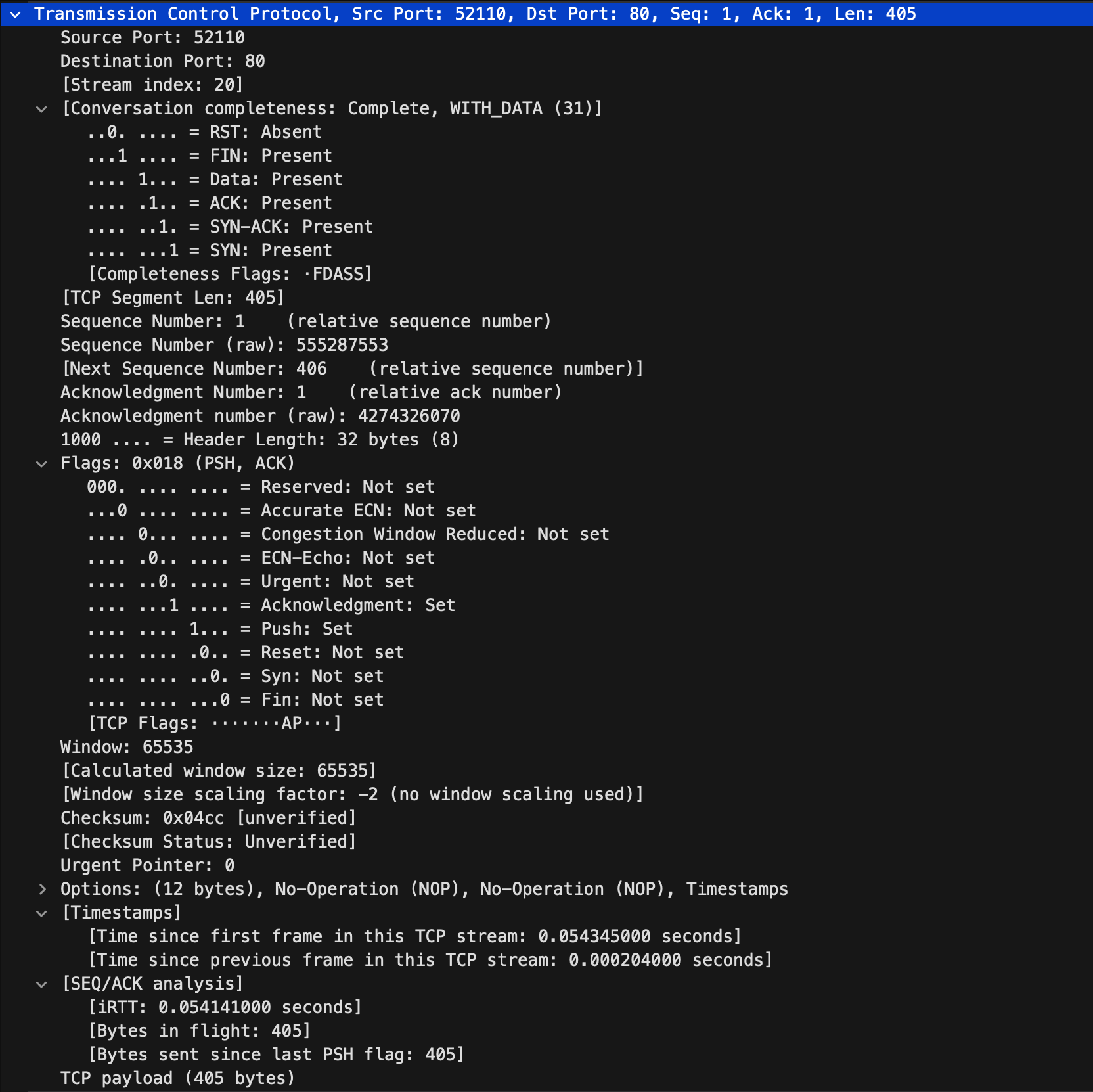
This layer uses the protocol of the **Datalink Layer.** This Ethernet frame establishes communication between the **source device** (Apple\_b2:d1:d2, MAC address a0:78:17:b2:d1:d2) and the **destination device** (HuaweiTechno\_90:a9:0b, MAC address c0:f6:ec:90:a9:0b). Both MAC addresses are globally unique and represent **individual (unicast) addresses**, ensuring one-to-one communication. The frame encapsulates an IPv4 packet (Type: 0x0800) as the payload, which will be further processed at the network layer.

**(iii) Internet Protocol/Network layer:**



This layer uses the protocol of the **Network layer.** This IPv4 packet establishes reliable communication between the source IP 10.100.37.195 and destination IP 103.230.106.202 using the TCP protocol. It is configured with the **Don't Fragment flag**, ensuring the packet remains intact during transmission, which is crucial for certain applications or networks. The **Time to Live (TTL)** is set to 64, which limits the packet's lifetime to prevent looping in the network.

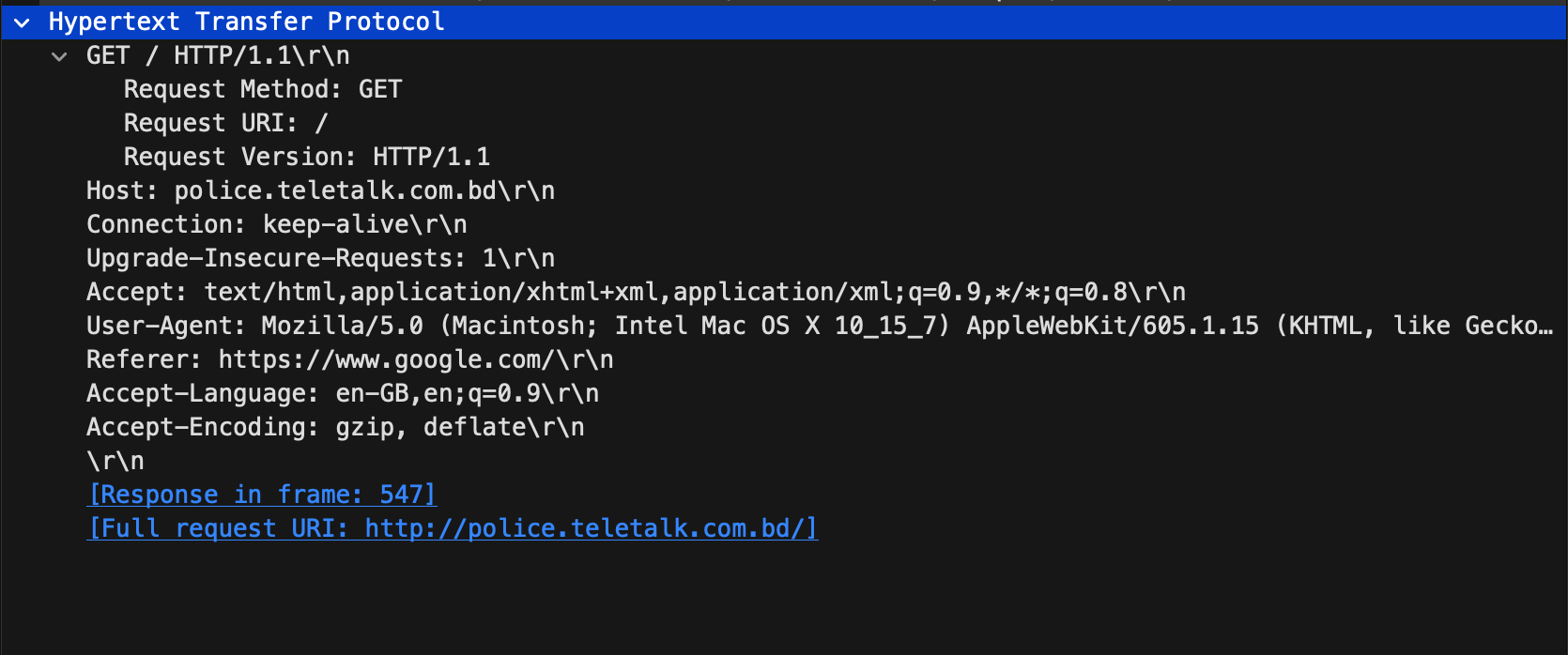
**(iv)Transmission Control Protocol/Transport Layer:**



This layer uses the protocol of the **Transport Layer.**  A TCP packet has been sent from source port 52110 to destination port 80(HTTP). This is because the request is being made from a private computer to a webpage and so the source port is **dynamic**, whereas the destination port falls under the range of **well known** port address.

The SYN, ACK, FIN flags are present, indicating that acknowledgements are sent/received for successful synchronization and finishing. The mentioned TCP segment length is 405, and so the next segment is 406. This means the current TCP segment has transmitted **405 bytes** of data starting from sequence number **1**. The next segment will start from sequence number **406**, which is the byte immediately following the last byte of this segment and so the size of the Payload is 405 bytes.

**(v) Hypertext Transfer Protocol/Application Layer:**



The HTTP request works as the foundation of a connection. This layer uses the protocol of the **Application Layer.**

**GET / HTTP/1.1\r\n**

Here, the request method is **GET**, which is used to request data from a specified source.

**HTTP/1.1** specifies the version of HTTP protocol being used.

**\r\n** represents a carriage return and a newline character, which are used to specify the end of the HTTP header request. Host, Connection, Accept, User-Agent, Referer, Accept-Language, Accept-Encoding are the **Header field names** of the header lines and the associated results are defined as **values**.

**Host: police.teletalk.com.bd\r\n**

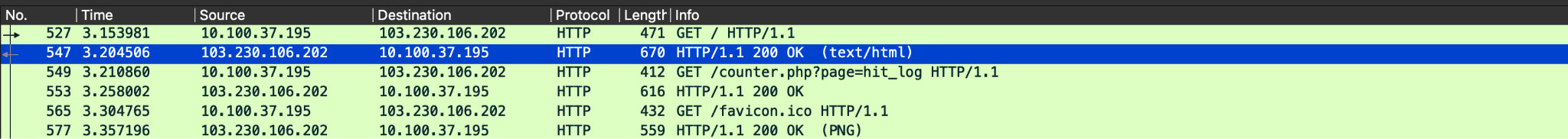
The host specifies the domain name of the server from which the request is being sent. police.teletalk is the **domain name**, .com.bd is the **top-level domain name** of the requested address. The domain address is sent to the DNS server to fetch the IP Address.

**Connection: keep-alive\r\n**

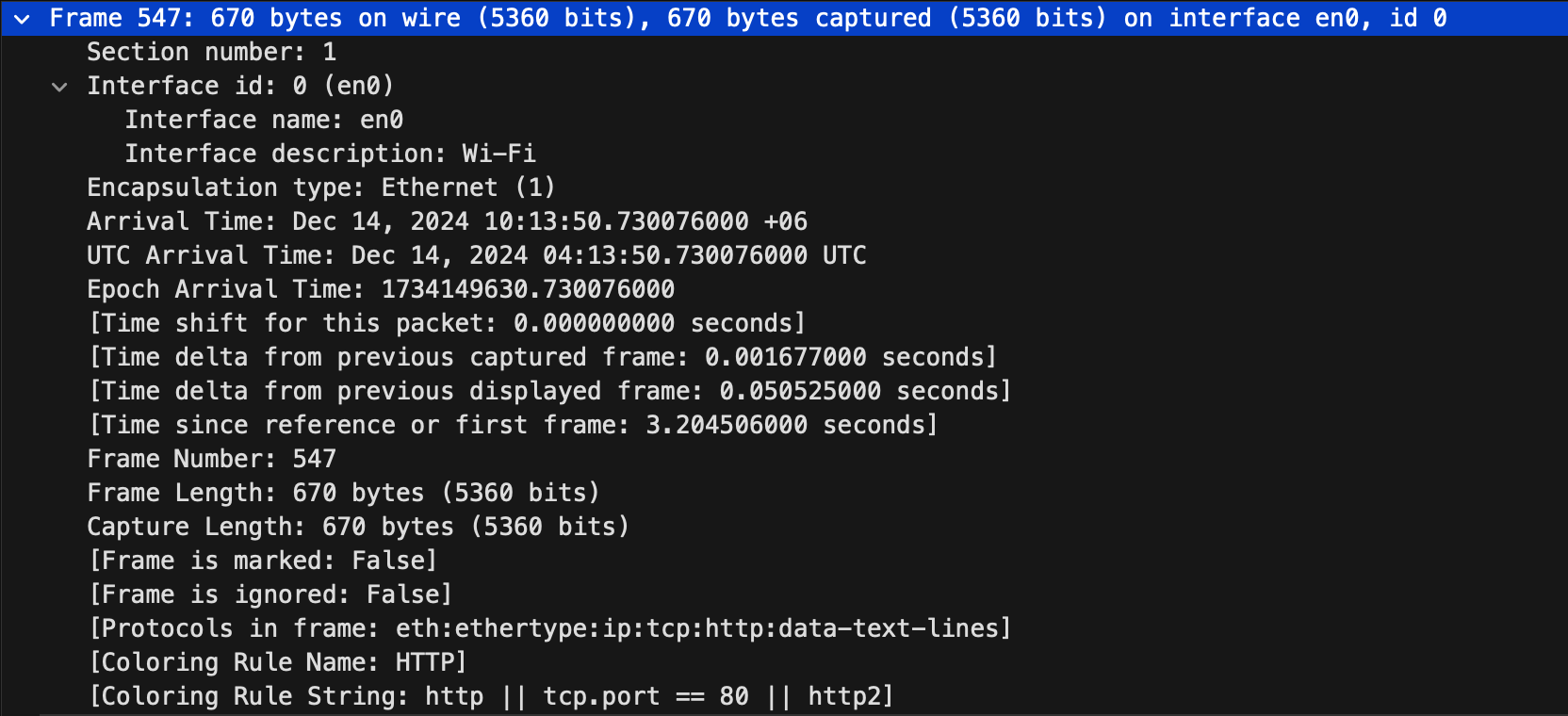
The value keep-value instructs the server to maintain the connection open even after the current request cycle completes. As a result, the same TCP connection is used for multiple HTTP requests instead of opening a new connection for every single request pair. Also, the header also indicates that the connection is capable of providing a secure connection.

Overall, this request is sent to the server police.teletalk.com.bd to retrieve the main page(/) over HTTP 1.1 while specifying preferences and source of the request.

**Response file:**

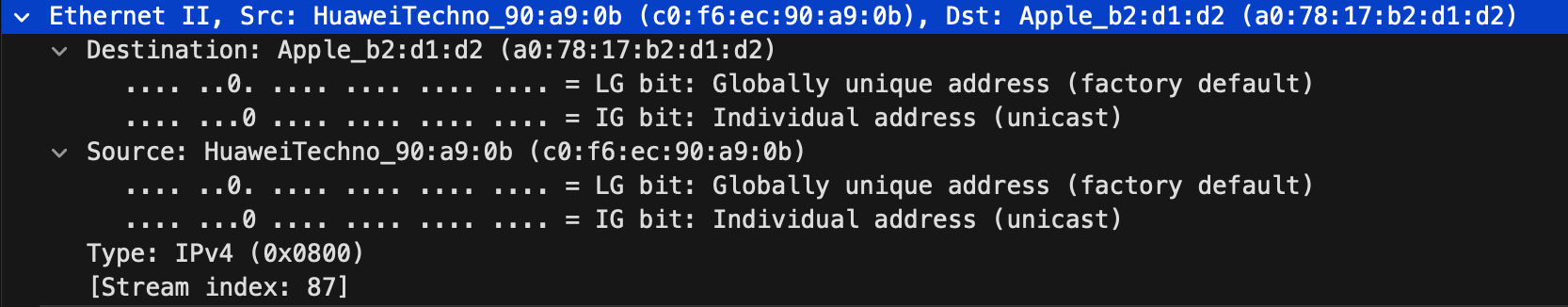


**(i) Frame 527/Physical Layer:**



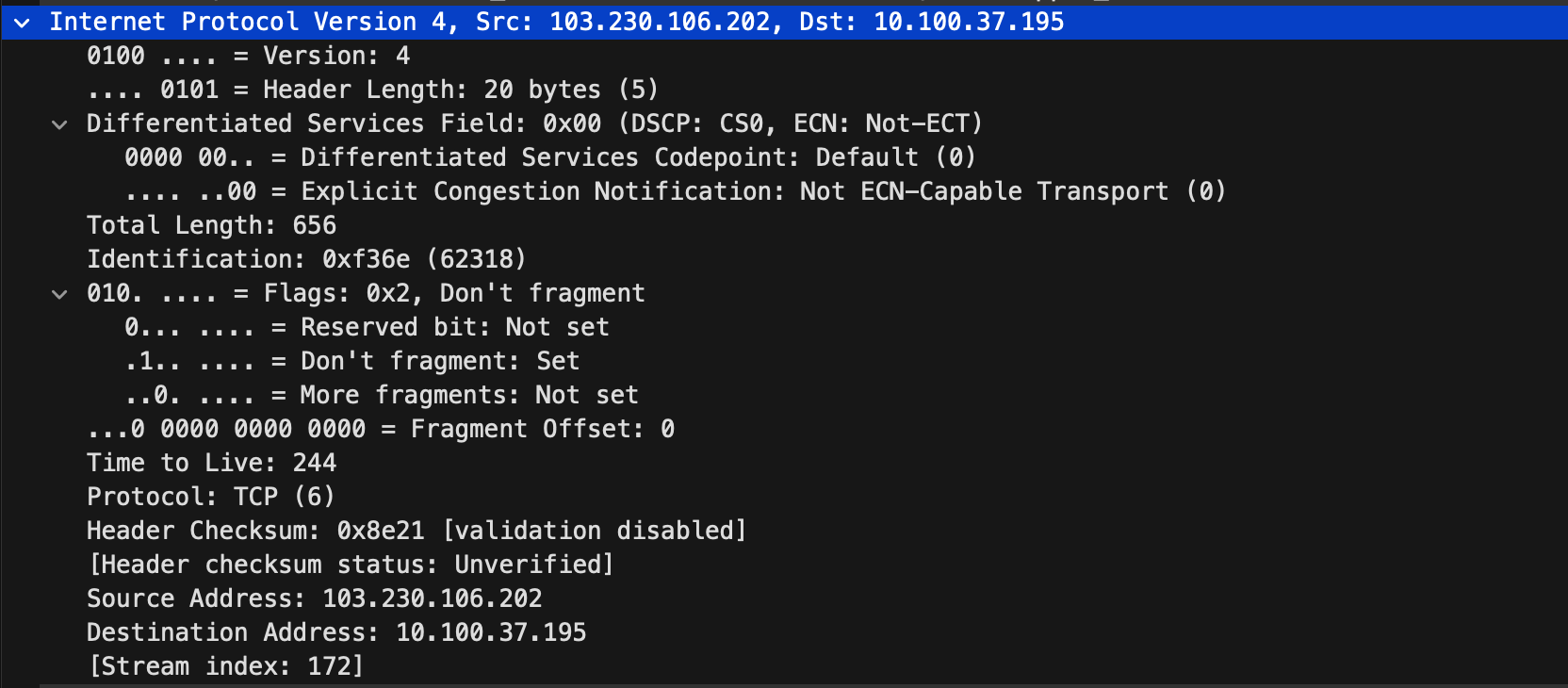
This layer uses the protocol of the **Physical Layer.** This Ethernet frame is part of an HTTP communication observed on interface en0, which indicates Wi-Fi interface. The arrival time is **December 14, 2024, 10:13:50.730076000 UTC+6** (local time).

**(ii) Ethernet II/Datalink Layer:**



This layer uses the protocol of the **Datalink Layer.** This Ethernet frame establishes communication between the **source device** (HuaweiTechno\_90:a9:0b, MAC address c0:f6:ec:90:a9:0b) and the **destination device** (Apple\_b2:d1:d2, MAC address a0:78:17:b2:d1:d2). Both MAC addresses are globally unique and represent **individual (unicast) addresses**, ensuring one-to-one communication. The frame encapsulates an IPv4 packet (Type: 0x0800) as the payload, which will be further processed at the network layer.

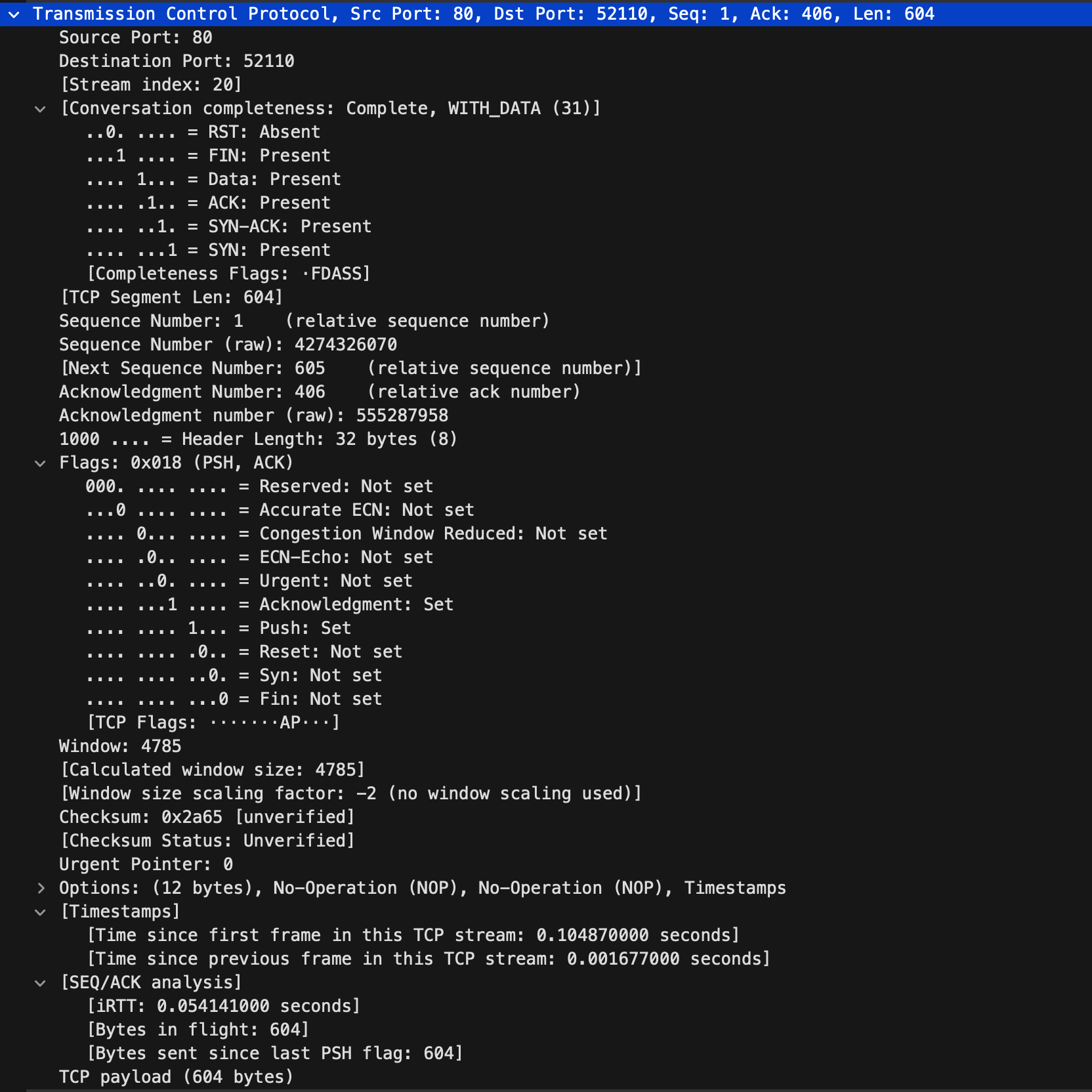
**(iii) Internet Protocol/Network layer:**



This layer uses the protocol of the **Network layer.** This IPv4 packet establishes reliable communication between the source IP 103.230.106.202 and destination IP 10.100.37.195 using the TCP protocol.

It is configured with the **Don't Fragment flag**, ensuring the packet extracts the exact way it was extracted throughout the transmission. The **Time to Live (TTL)** is set to 244, which limits the packet's lifetime to prevent looping in the network.

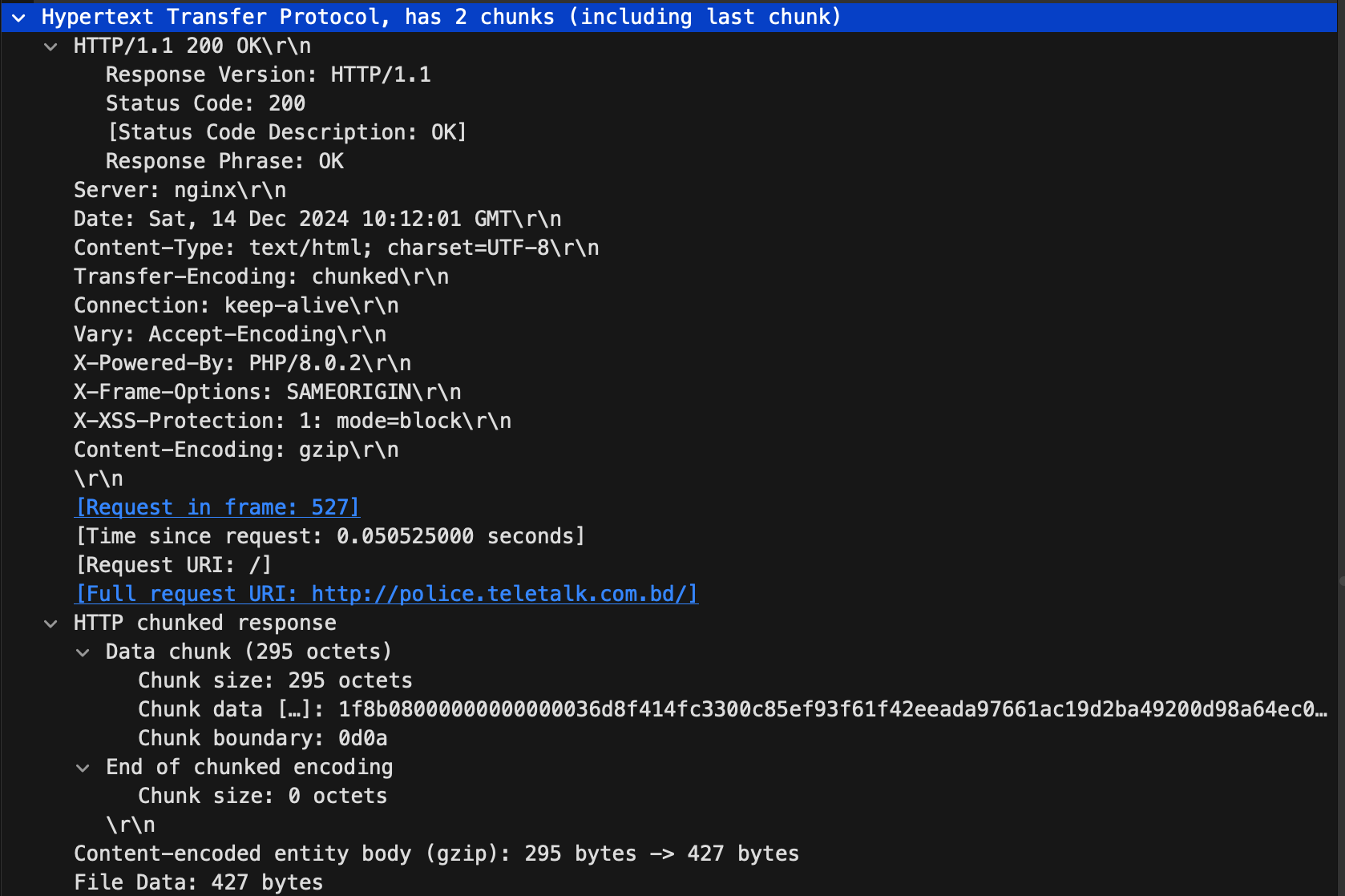
**(iv)Transmission Control Protocol/Transport Layer:**



This layer uses the protocol of the **Transport Layer.**  A TCP packet has been received from source port 80(HTTP) to destination port 52110 . This is because the request is sent to a private computer from a webpage and so the source port is a well **known** port address, whereas the destination port falls under the range of **dynamic** port address.

The SYN, ACK, FIN flags are present, indicating that acknowledgements are received for successful synchronization and finishing. The mentioned TCP segment length is 604, and so the next segment is 605. This means the current TCP segment has received **604 bytes** of data starting from sequence number **1**. The next segment will start from sequence number **605**, which is the byte immediately following the last byte of this segment and so the size of the Payload is 604 bytes.

**(v) Hypertext Transfer Protocol/Application Layer:**



This layer uses the protocol of the **Application Layer.**

**HTTP/1.1 200 OK\r\n**

Here, **HTTP/1.1** specifies the version of HTTP protocol being used. The OK and 200 indicates that the data has been received successfully. **\r\n** represents a carriage return and a newline character, which are used to specify the end of the HTTP header request.

Moreover, Server, Date, Content-Type, Transfer-Encoding, Connection etc are **Header field names** of the header lines and the associated results are defined as **values**.

**Date: Sat, 14 Dec 2024 10:12:01 GMT\r\n**

The date indicates when the response was received. It is used to compare where data is stale or updated while working with a proxy server.