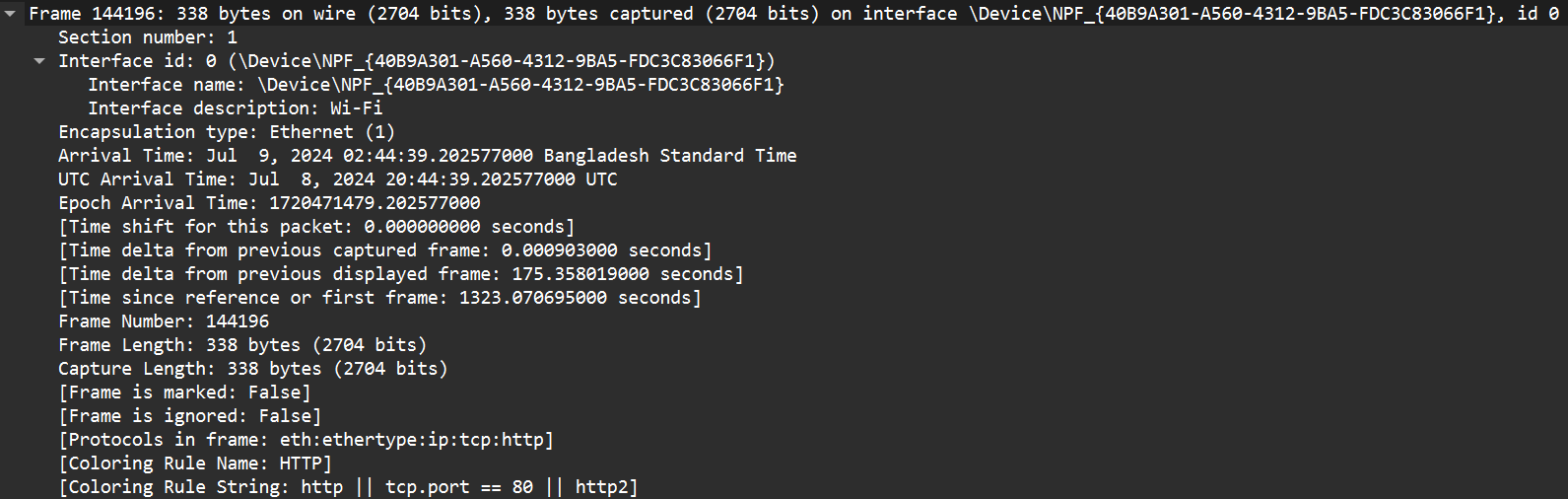
**TASK 1 : Wireshark**

**HTTP Request**

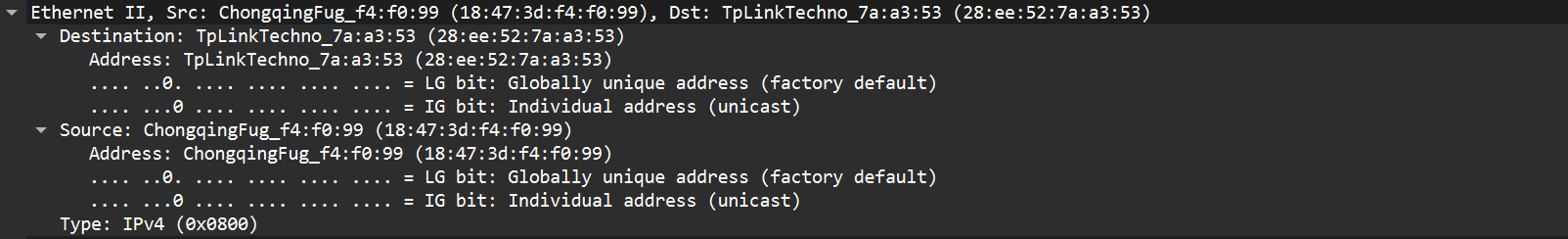
**Header 1 : Frame**

Frame = 144196 contains data from the application layer which has been encapsulated in the transport layer and later carried over to the network layer. Frames are the PDU of the data link layer. A header and trailer is added with the frame. Send this frame straight to the destination device.



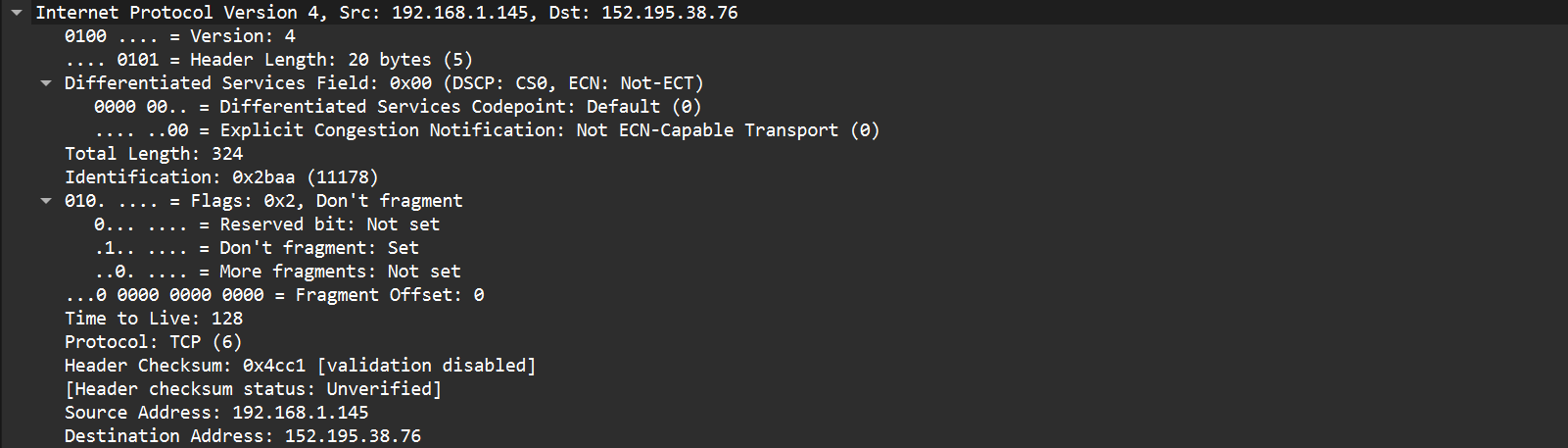
**Header 2: Ethernet II**

The data link layer contains the source MAC address = 18:47:3d:f4:f0:99 and destination MAC address = 28:ee:52:7a:a3:53 needed to identify the source and destination devices within a network.



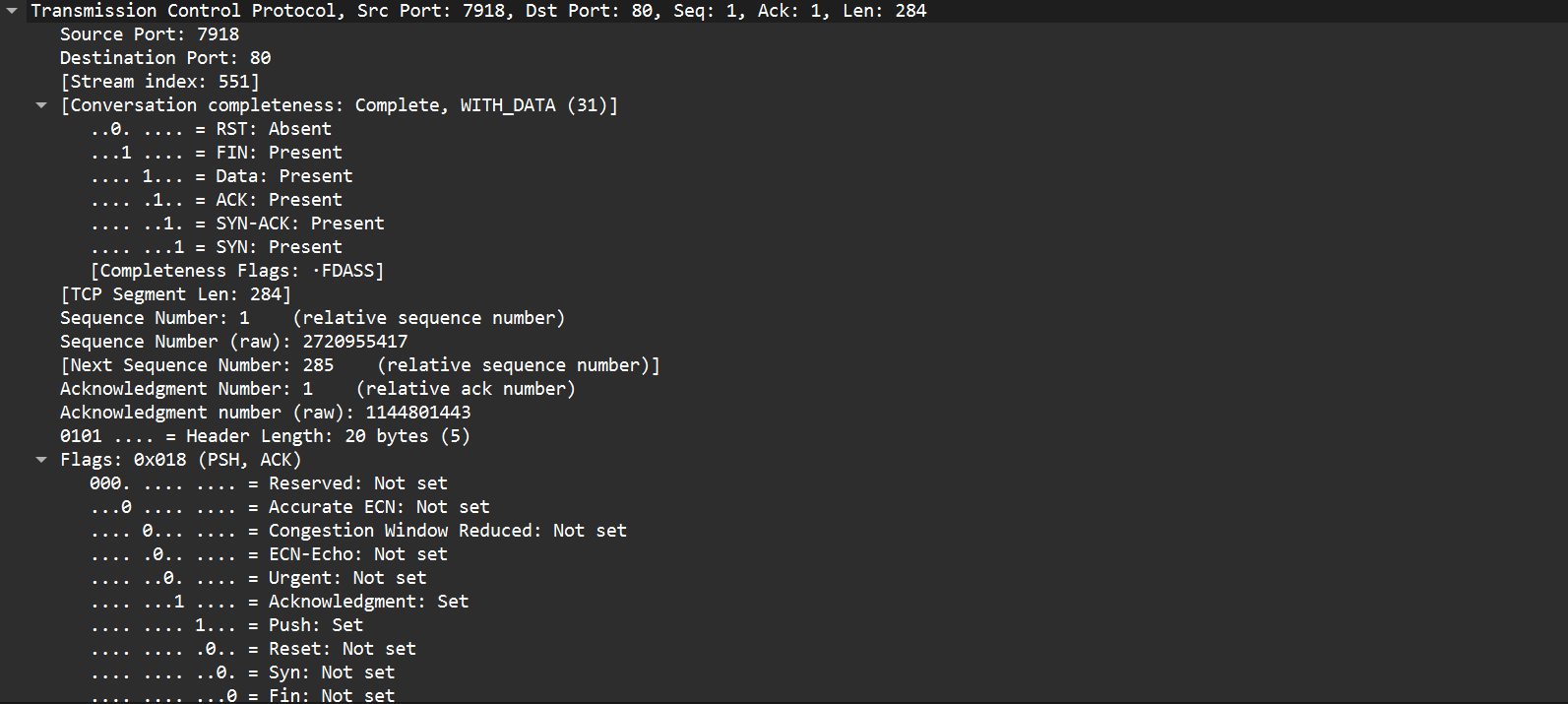
**Header 3: Internet Protocol**

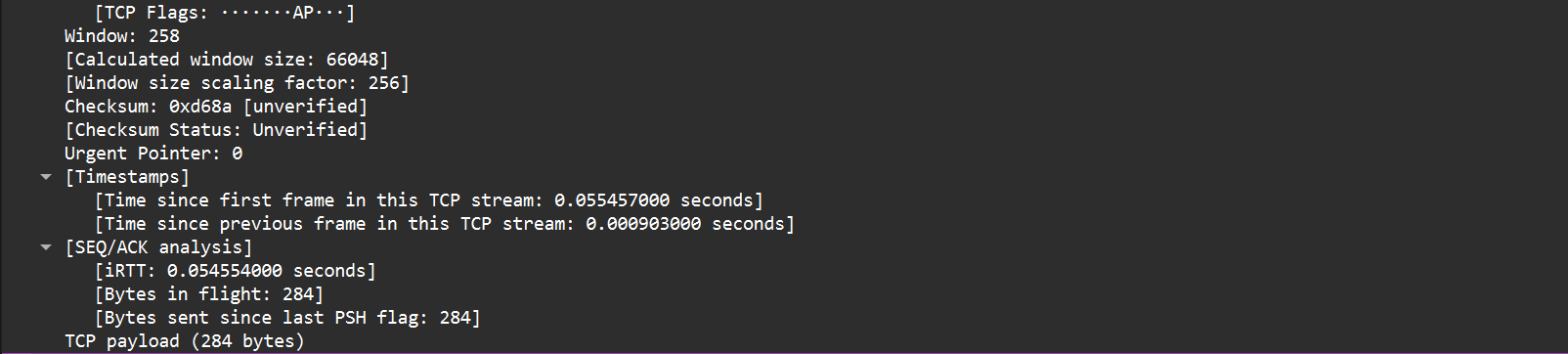
The network layer is using Internet Protocol. Source ip address = 192.168.1.145, Destination ip address = 152.195.38.76 are used to identify a device uniquely. This is responsible for routing and sending packets from source to destination.



**Header 4: Transmission Control Protocol**

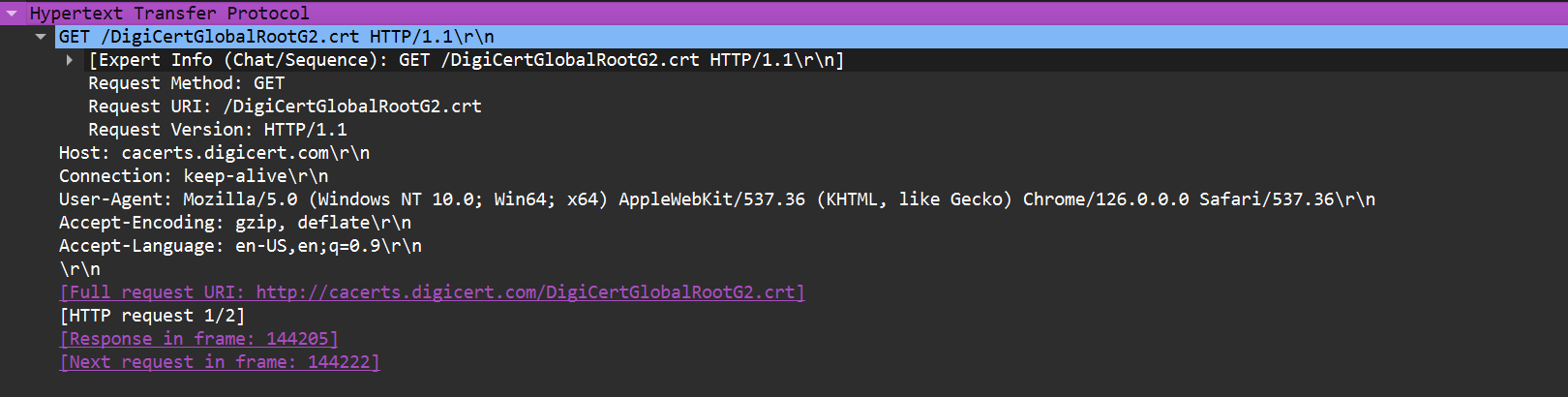
The transport layer is using TCP as its protocol with source port = 7918, destination port = 80 (web server), sequence number = 1, acknowledgement number = 1. The control flags are set accordingly. Port address is used for process-to-process data transmission. Port address is used for process-to-process data transmission





**Header 5: Hypertext Transfer Protocol**

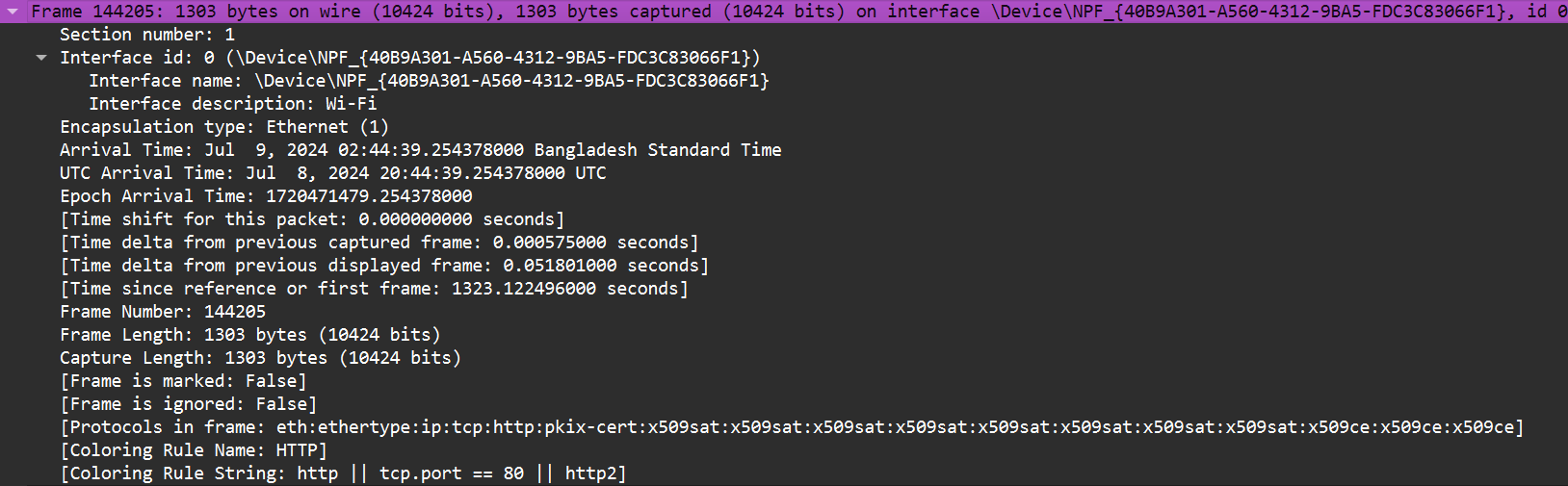
This header is for the application layer which tells the server the app / web the client wants to interact with. The GET method is used to fetch the data from the Request URI of the server by the client, where the Request URI = /DigiCertGlobalRootG2.crt contains the resource path for which the client is requesting for. Here, HTTP version 1.1 is used as the HTTP protocol which uses persistent HTTP connection. Host contains the hostname of the server with which the client wants to be connected. \r indicates the cursor to move back to the beginning to the current line. \n indicates the cursor to move to the beginning of the new line. Connection is set at keep-alive so that re-establishment of connection is avoided and the connection remains open.



**HTTP Response**

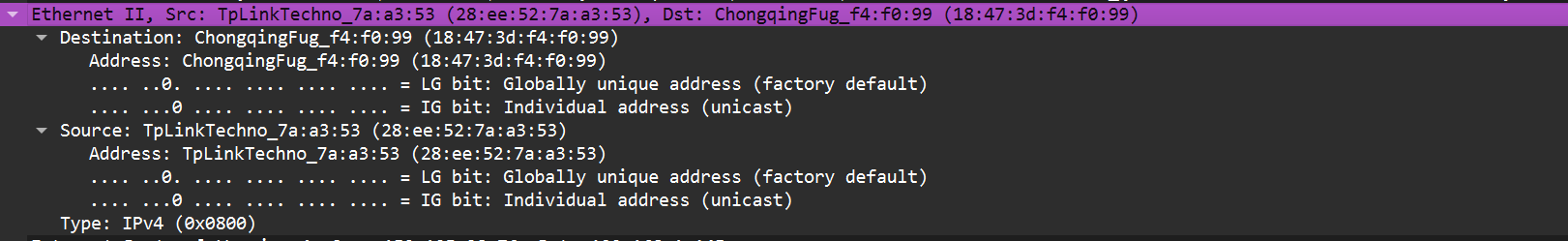
**Header 1: Frame**

Frame = 144205 contains data from the application layer which has been encapsulated in the transport layer and later carried over to the network layer. Frames are the PDU of the data link layer. A header and trailer is added with the frame. Here, Frame size is of 1303 bytes. This header tells whether or not the captured packet is responding to the request.

****

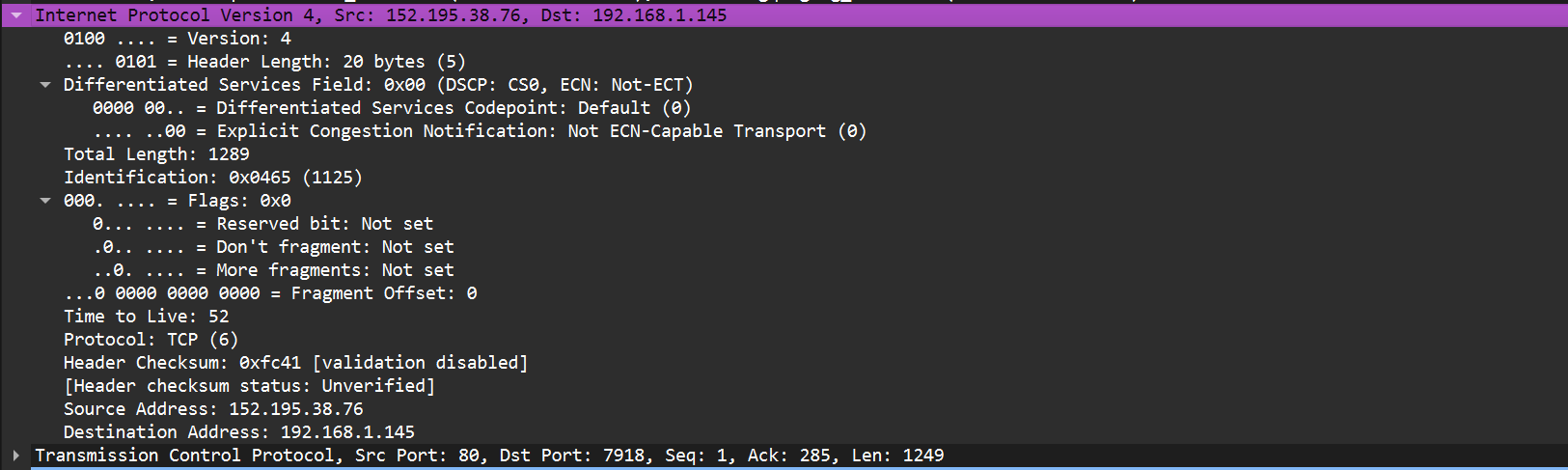
**Header 2: Ethernet II**

The data link layer contains the source MAC address = 28:ee:52:7a:a3:53 and destination MAC address = 18:47:3d:f4:f0:99 needed to identify the source and destination devices. This header makes sure that the data has been correctly and accurately sent to the destination.

****

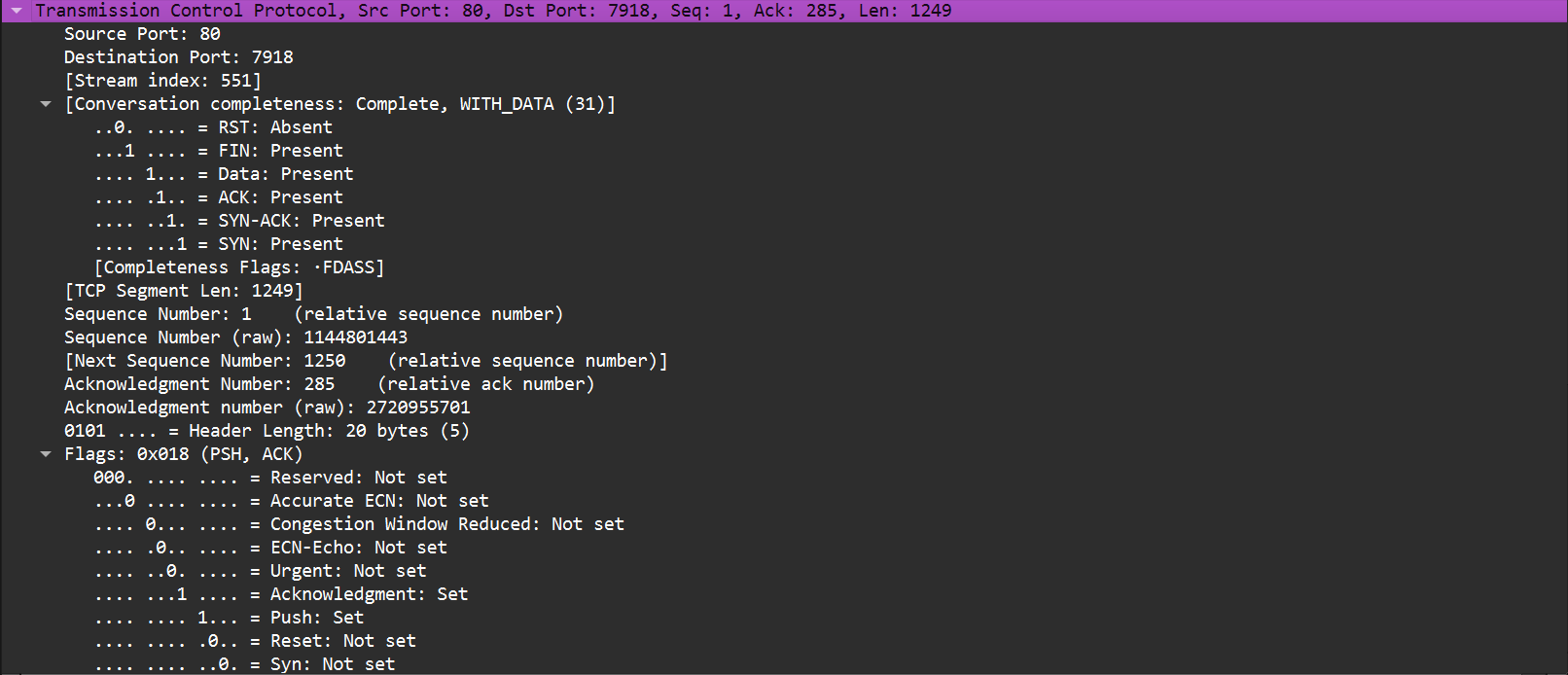
**Header 3: Internet Protocol**

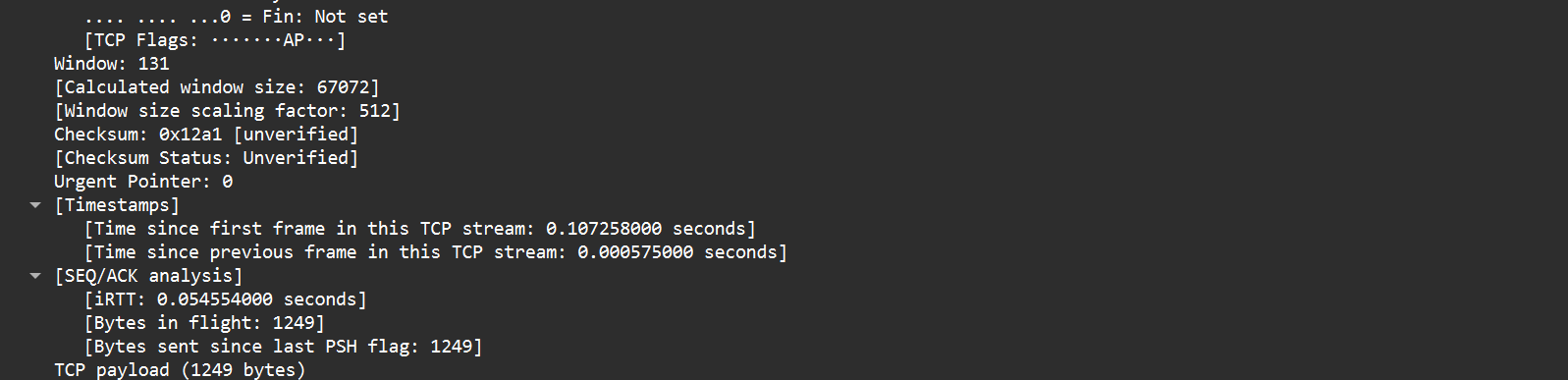
The network layer is using Internet Protocol. Source ip address = 152.195.38.76, Destination ip address = 192.168.1.145 are used to identify a device uniquely. This header checks whether the source and destination has been accurately identified for response purpose and the delivery of information is accurate.

****

**Header 4: Transmission Control Protocol**

The transport layer is using TCP as its protocol with source port = 80, destination port = 7918, sequence number = 1, next sequence number = 1250, acknowledgement number = 285, HLEN=20 bytes and the control flags are set accordingly. Port address is used for process-to-process data transmission. This header again checks for accurate data delivery and includes acknowledgements, sequence number and necessary error controls (such as checksum).





**Header 5: Hypertext Transfer Protocol**

Here, Response Version = HTTP version 1.1 is used as the HTTP protocol which uses persistent HTTP connection. Status code = 200 (OK) means the request was successful. \r indicates the cursor to move back to the beginning to the current line. \n indicates the cursor to move to the beginning of the new line. This header ensures that a response is sent to the client to tell whether or not the request was successful. It also contains response related contents as well.

