**Wireshark**

**Request**

**Application Layer:**

The GET is a method which means requesting data from a specific file path from the Host in the next line.

Host: The Host is the server pc that will receive the request from the line.

Connection: This field signifies whether the connection is persistent or non-persistent. As the connection is keep-alive, it means that the connection is persistent.

User-Agent: This field explains which browser, browser version, OS and its architecture the client is using, therefore the server will be able to respond as per client’s browser and OS requirements.

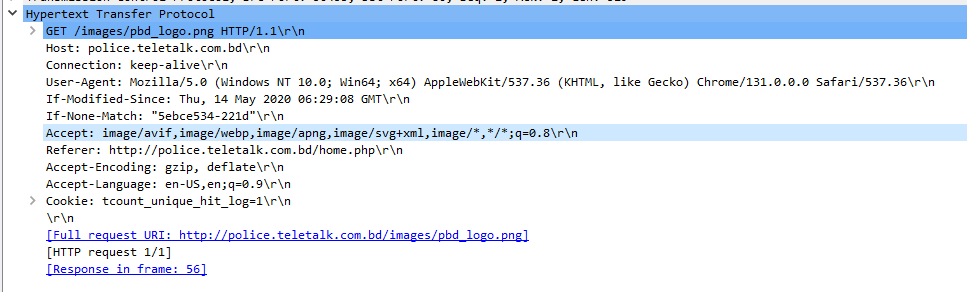
If-Modified-Since is the field to check for cookies. It is used by the proxy server to check if the requested data has been changed, if it is not changed then the proxy sends the client from its server. Otherwise, the proxy servers request the data from the actual server, then send it to the client.

If-None-Match: This header is used for cache validation. If the token does not match with sever then server will send the requested data. Otherwise, if matches, the client will use its cached data.

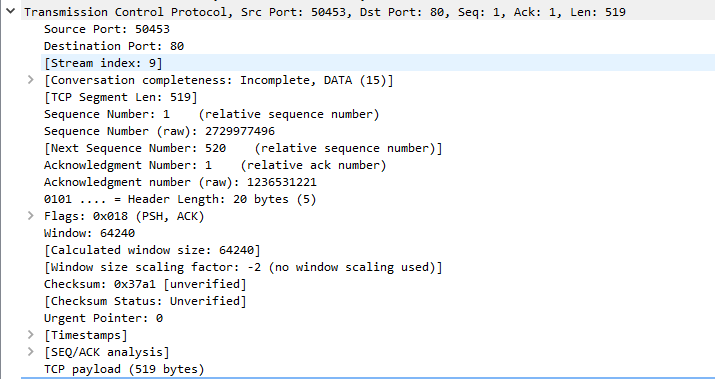
Accept-encoding: this field defines the type of encoding client support, thus if the server encode data, it will encode as per client’s requirement, therefore client will be able to decode accordingly

Accept Language: This field displays which language the client will accept thus the server will respond according to that language.

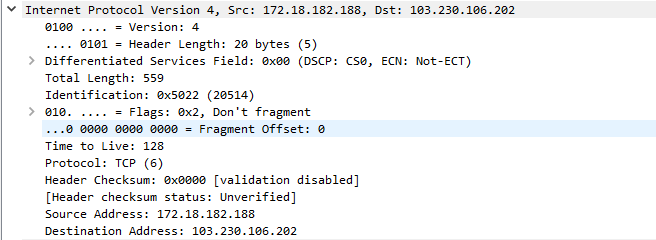
Cookie: This header is used to validate cookies. If the cookie is validated, then client will be able to use the data stored in cookie. Otherwise, it places a new cookie if expired



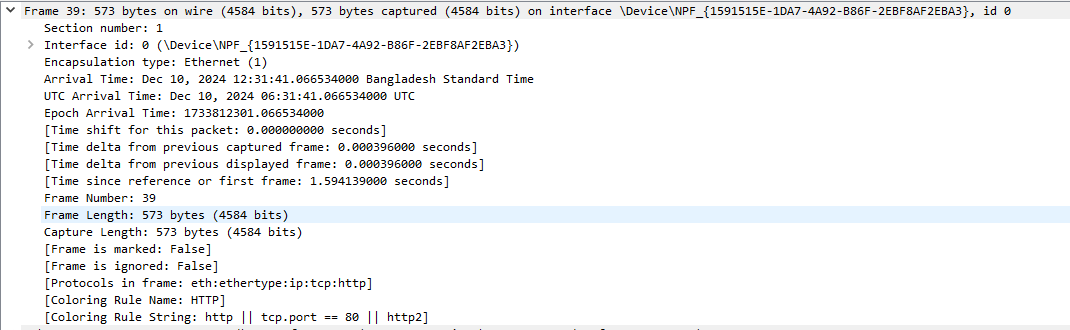
**Transport Layer**: This header is from the client’s transport layer, which sends the segment along with its sequence number acknowledgement number. Through this header, the server knows which data to send next, also knows the destination computer as well. This header also signifies the current state of buffer, in addition to this, it also mentions whether the packet is urgent. The checksum is used to validate the segment whether its corrupted or not. If corrupted, then the packet will be dropped, and it will request the packet again



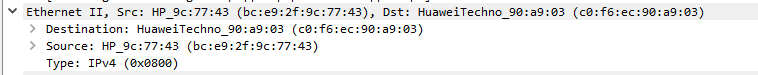
**Network Layer:** This header signifies the source and destination IP. The IP helps identify the unique source and destination. As the IP has two version, the header includes the version as well to identify the IP as per its version. TTL field signifies the validation of time of a single packet. Checksum will identify whether the packet is corrupted or not



**Data-Link Layer:** This header file contains necessary information for the data-link layer. The frame number signifies the number of frames of a data, and its length represents the size. Protocols mentioned which protocols were used in transport and application layer.



**Physical Layer:** This field contains data for the physical layer. It contains information about next hop’s MAC address. For each jump in the hop, the mac address changes. Also, it mentions the version of IP as well.



**Response**

**Application Layer:**

First Line: Version of HTTP is mentioned, and the request Status code and phrase. Not modified means the data is the same as before and the client will be able to use its cached data.

Server: This field mentions the software the server is using.

Date: This field describes the date and time of server response.

Last-Modified: This field is used to check from the client side whether its modified. The client check from if modified field to match with last-modified. If matches, it uses data from proxy sever else it requests the data again from the sever

Connection: This field signifies whether the connection is persistent or non-persistent. As the connection is keep-alive, it means that the connection is persistent.

Cookie: This header is used to validate cookies. If the cookie is validated, then client will be able to use the data stored in cookie. Otherwise, it will place a new cookie if expired.

E-tag: This field is used for cache validation to determine if the resource has changed.

Expires: Specifies the time at which the cached resource is considered stale. After this time, the client must revalidate the resource with the server.

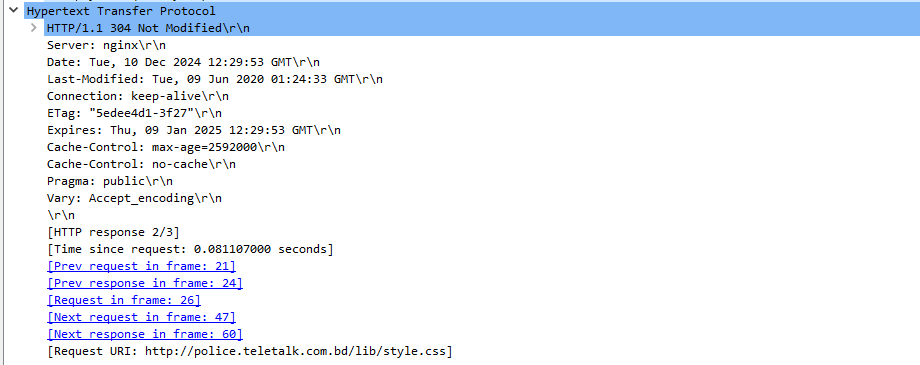
Cache-Control: Specifies the maximum amount of time in seconds that the cache is valid. After that it becomes stale

Pragma: this is a legacy HTTP header indicating that the response can be cached by both browsers and proxy servers.

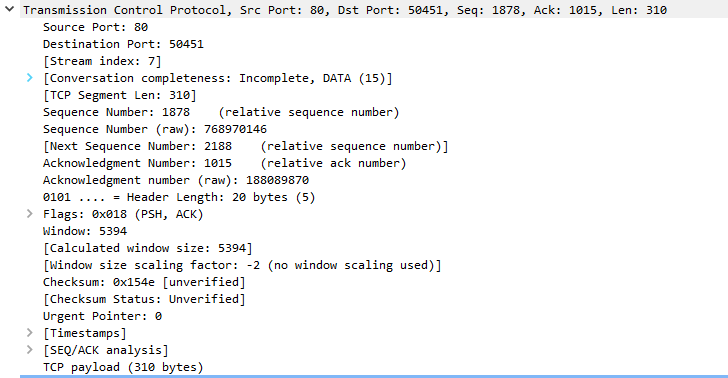
Vary: Specifies that the response may vary depending on the value of the Accept-Encoding header in the client request.

\r\n: Command line argument in each field separating each field so that computer is able to understand.

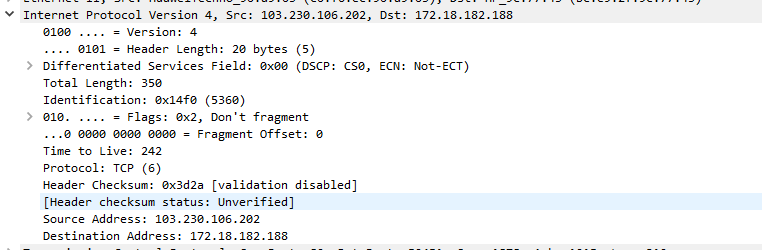
The rest is the additional information sent by the server to client.



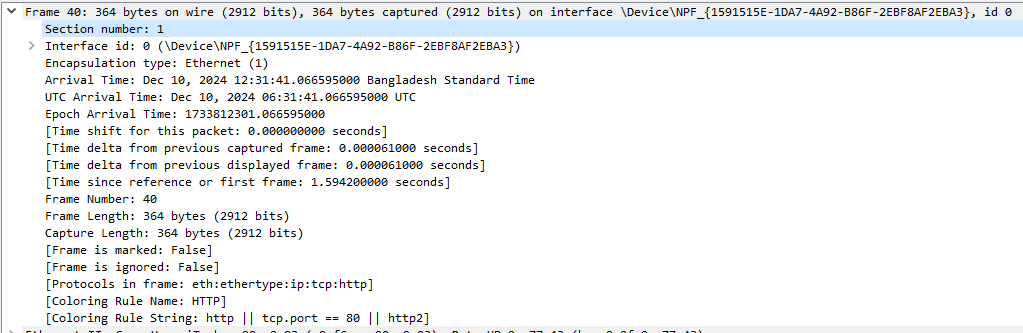
**Transport Layer**: This header is from the client’s transport layer, which sends the segment along with its sequence number acknowledgement number. Through this header, the server knows which data to send next, also knows the destination computer as well. This header also signifies the current state of buffer, in addition to this, it also mentions whether the packet is urgent. The checksum is used to validate the segment whether it’s corrupted or not. If corrupted, then the packet will be dropped, and it will request the packet again.



**Network Layer:** This header signifies the source and destination IP. The IP helps identify the unique source and destination. As the IP has two version, the header includes the version as well to identify the IP as per its version. TTL field signifies the validation of time of a single packet. Checksum will identify whether the packet is corrupted or not



**Data-Link Layer:** This header file contains necessary information for the data-link layer. The frame number signifies the number of frame of a data, and its length represents the size. Protocol is mentioned which protocols were used in transport and application layer.



**Physical Layer:** This field contains data for the physical layer. It contains information of next hop’s MAC address. For each jump in the hop, the mac address changes. Also, it mentions the version of IP as well.

