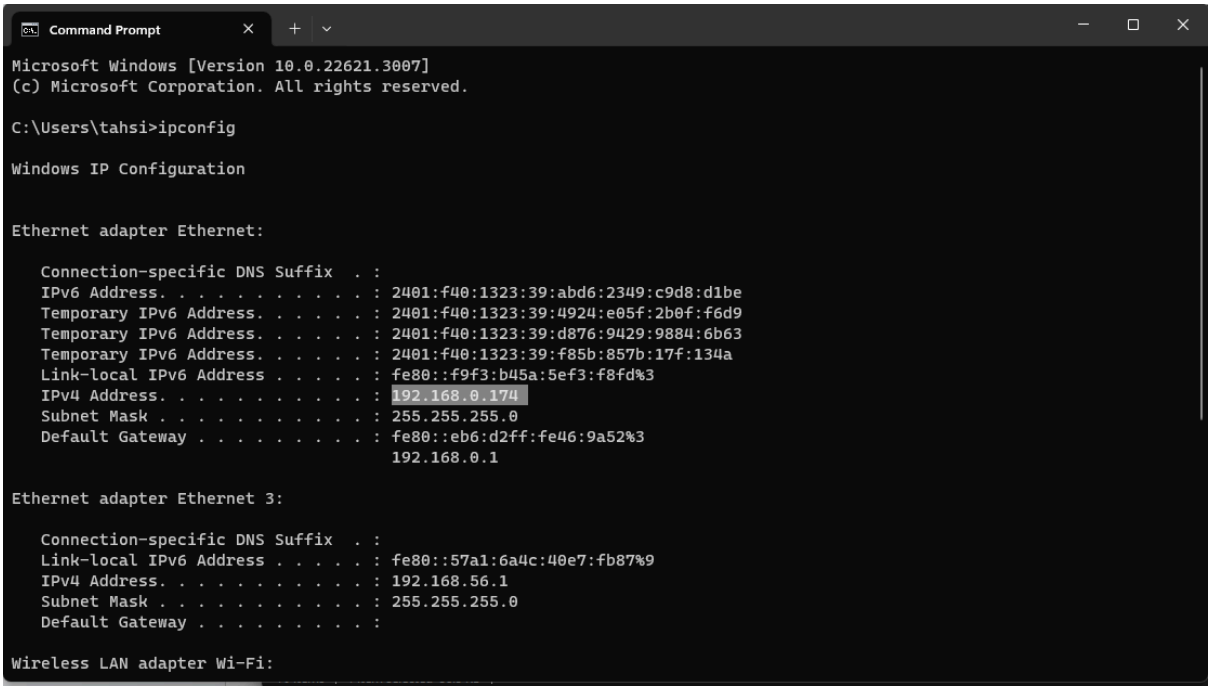
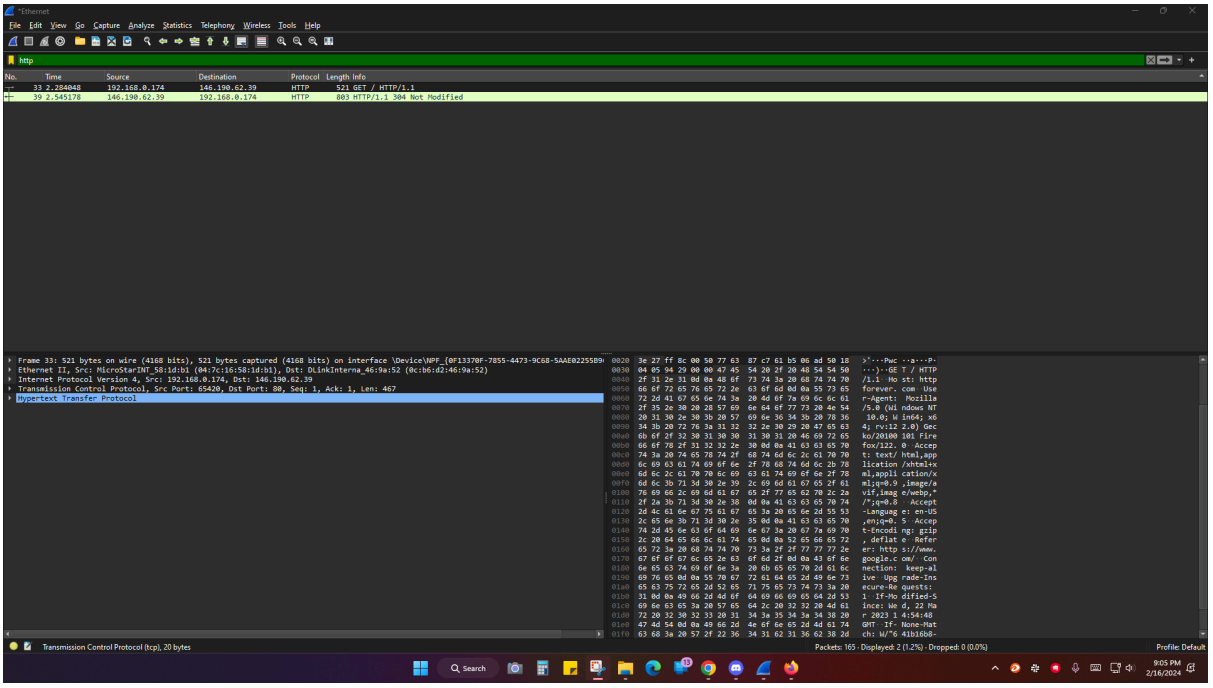
CSE421 Lab 2
Tahsin Ashrafee Susmit
ID:20301088



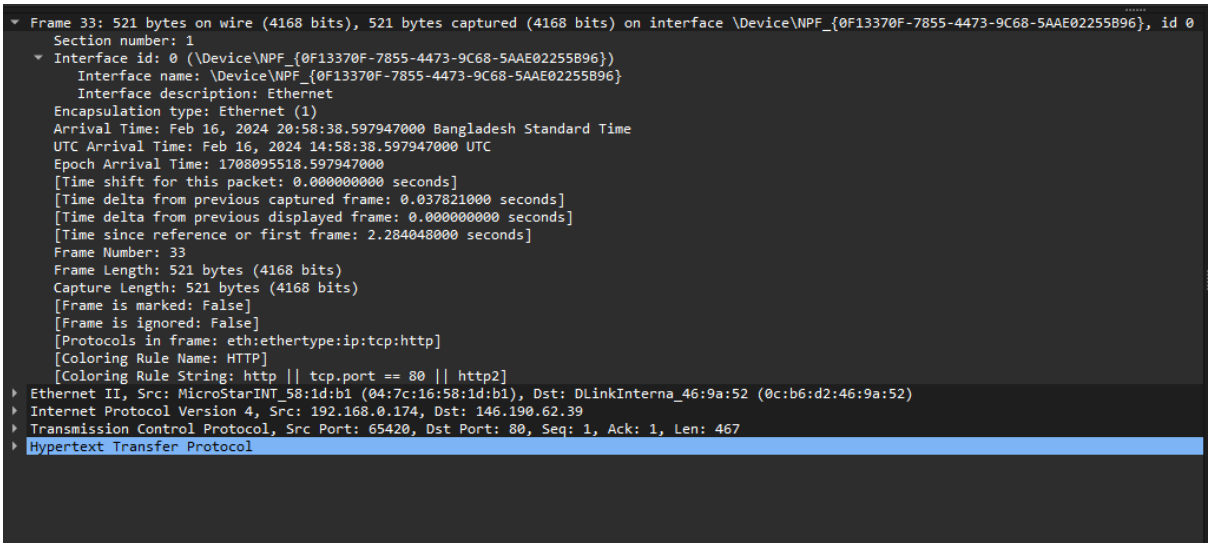
Wireshark



The IP address of my device is 192.168.0.174, and the IP address of HTTP Forever Website is 146.190.62.39

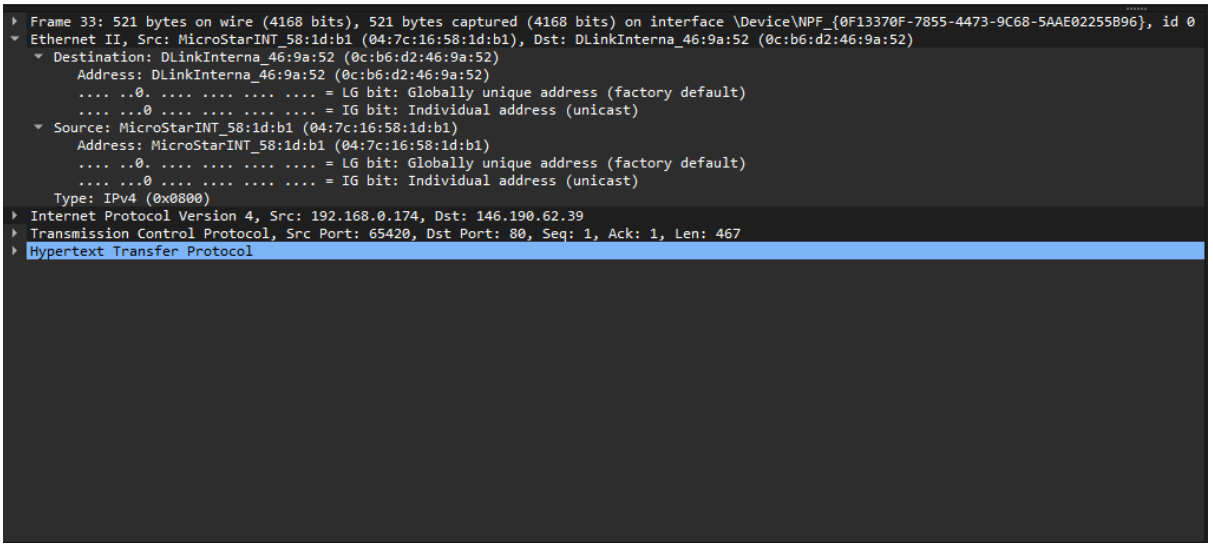
Request Packet

Frame:



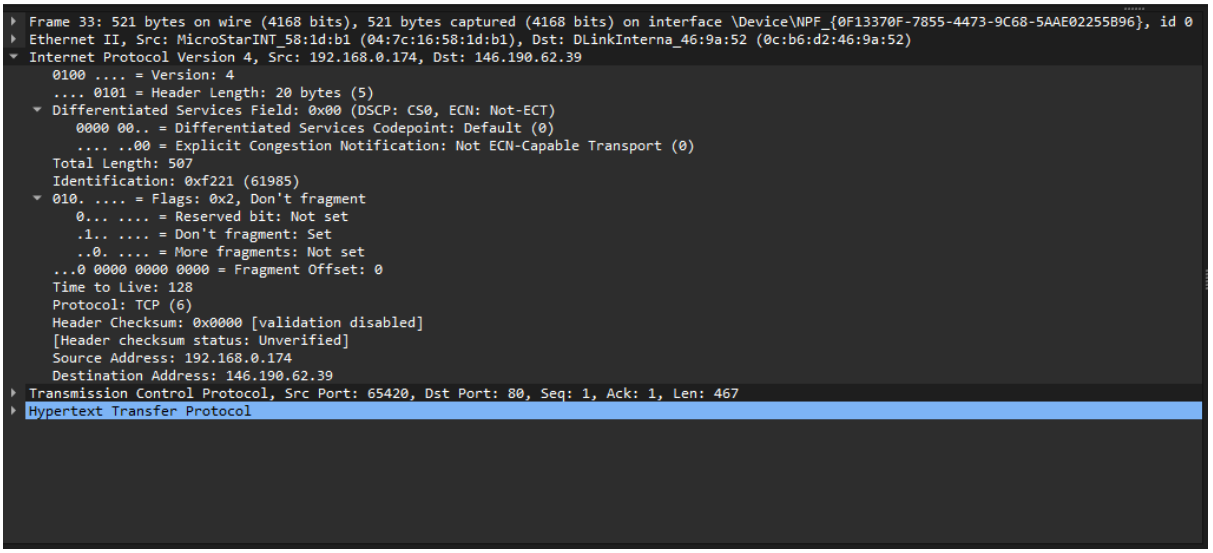
Frames reside at the Data Link Layer.

Ethernet II:



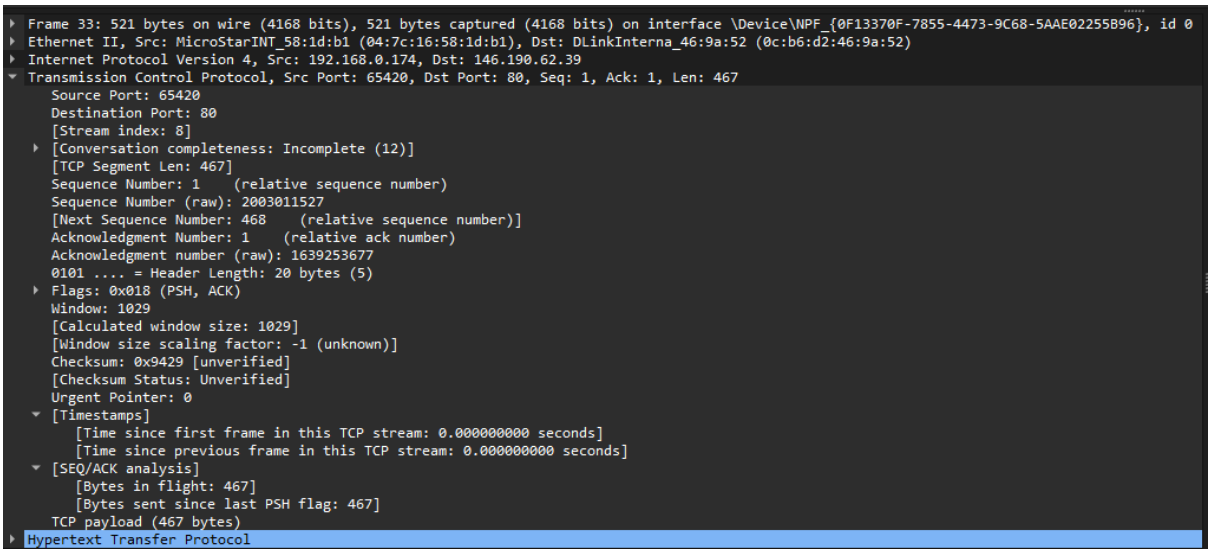
The Ethernet II also falls on the Data Link Layer. We can see the Destination Mac Address at first then the source Mac Address is evident. Also, it shows that data transfer is done via the IPv4 protocol.

IPV4:



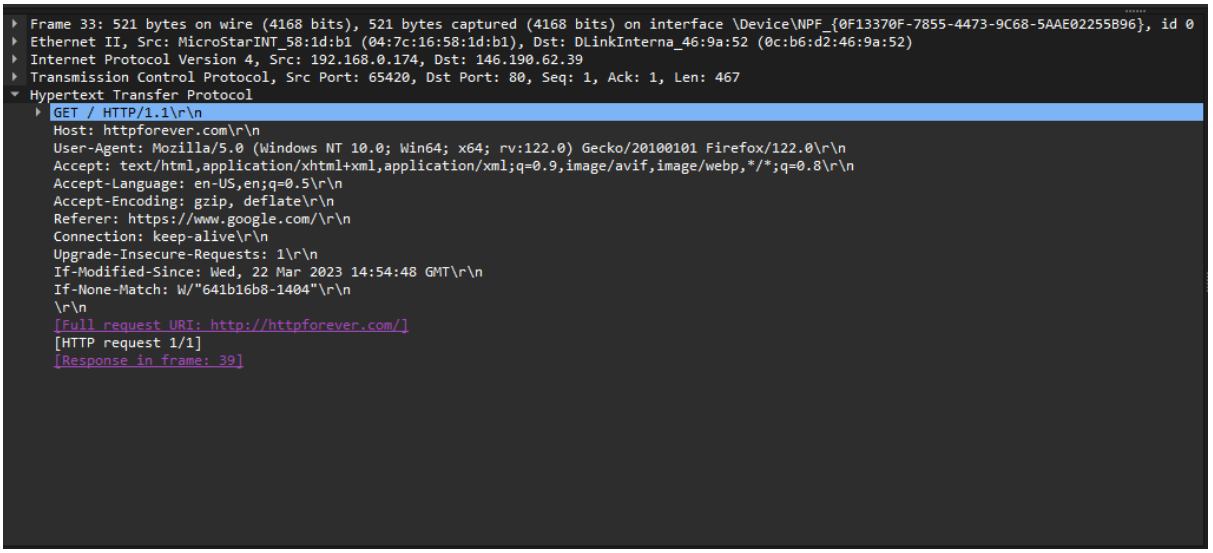
The IPV4 falls under Network Layer. The source is 192.168.0.174 meaning my PC, and the destination 146.190.62.39 meaning the website I searched for. The packet contains a header of 20 bytes, utilising TCP for data transmission. Its overall size is 507 bytes and includes a Time-to-Live (TTL) value 128.

TCP:



TCP operates within the transport layer. The destination port for the HTTP Forever website is 80, while the source port, originating from my PC, is designated as 65420. Both the sequence number and acknowledgment number are identified as 1. This signifies the successful initiation of the TCP communication session, where the sender has sent the initial segment of data with sequence number 1, and the receiver has acknowledged its receipt by confirming the sequence number as 1.

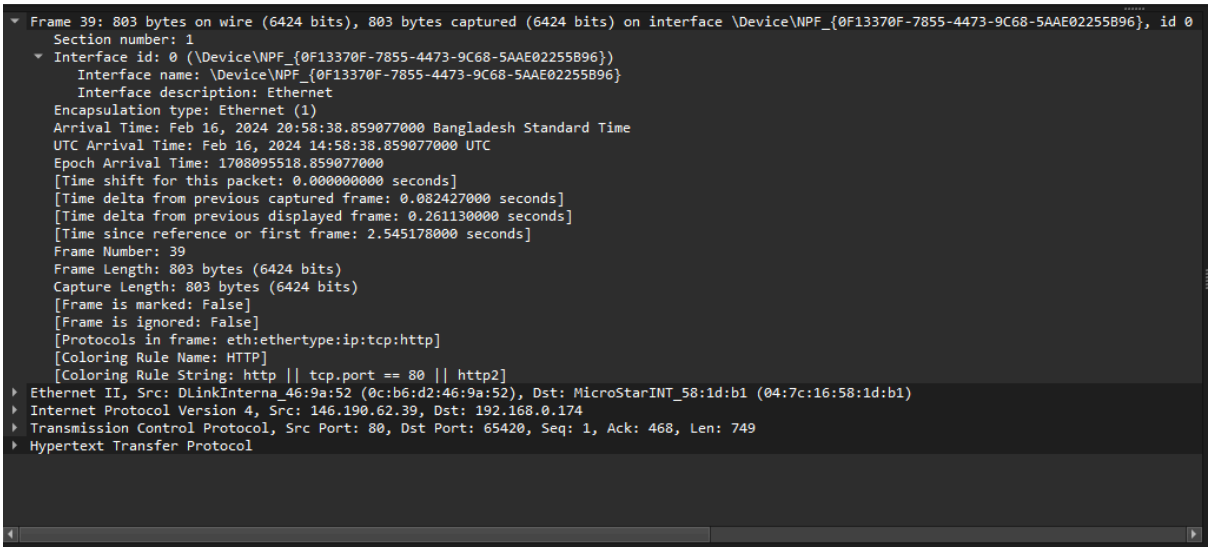
HTTP:



HTTP falls under the Application Layer. Using the Get Method the client (My PC) is requesting data from the website HTTPforever.com. HTTP/1.1: is the version of the HTTP protocol being used. “\r\n” means 'Carriage Return' to the print head back to the start of line. Host: httpforever.com: specifies the host to which the request is being sent. It informs the server of the domain it should process the request for. Then the browser along with its version is specified. After that the acceptance of media type, language and encoding is declared. Then the Connection: keep-alive indicates the fact of Persistent Transmission. After that for the cache and proxy servers, the conditional get, IF-Modified-Since indicates when it was last updated and if required to be updated or not. Lastly, the server's response to that request is likely to contain 39 frames of data.

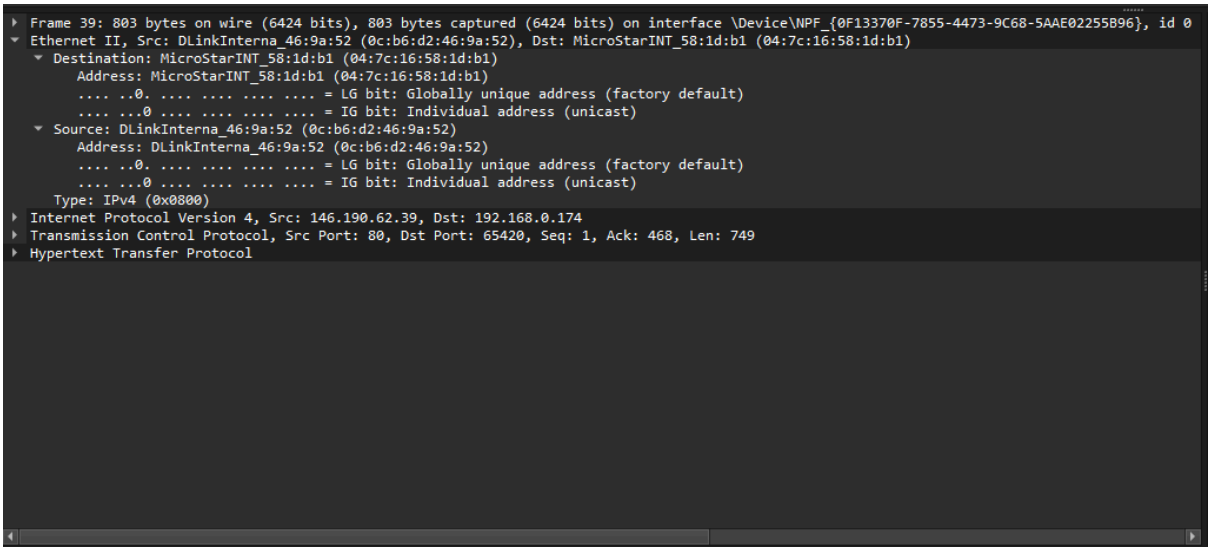
Response Packet

Frame:



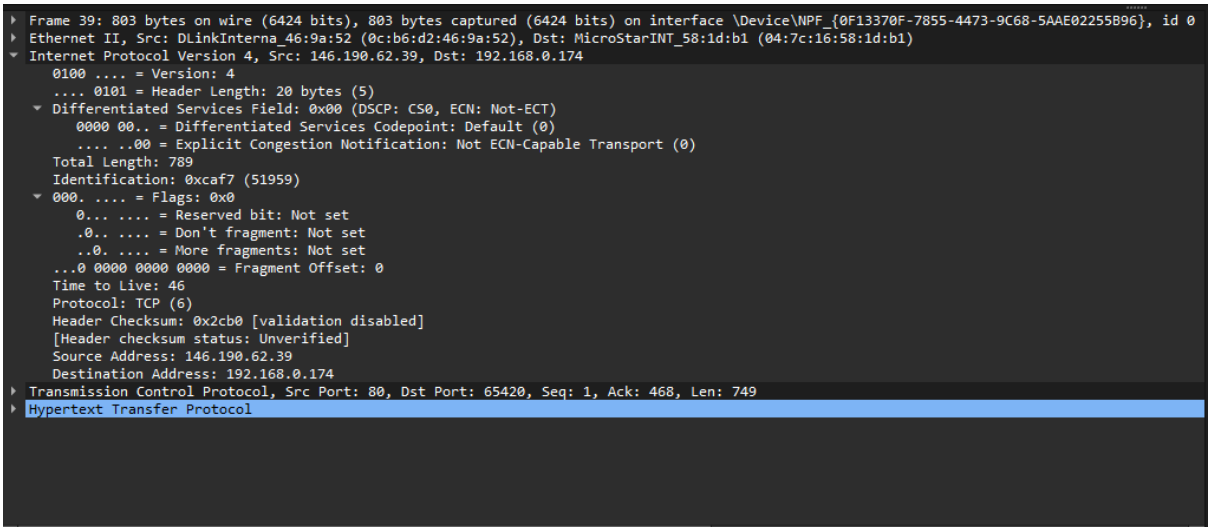
Frames reside at the Data Link Layer.

Ethernet II:



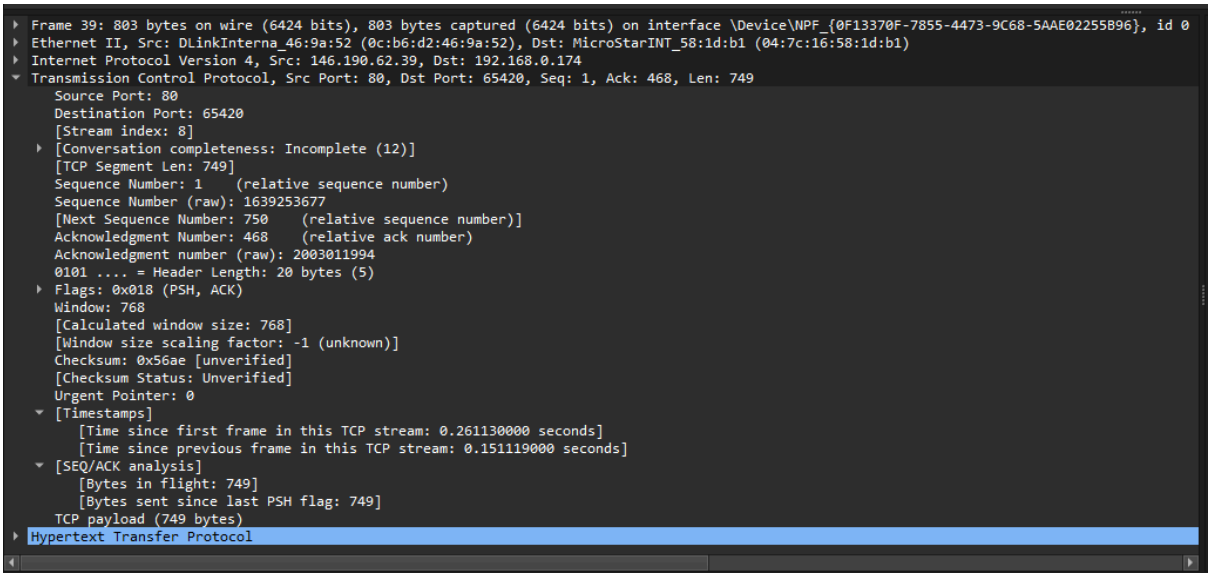
The Ethernet II also falls on the Data Link Layer. We can see the Destination Mac Address at first then the source Mac Address is evident. Also, it shows that data transfer is done via the IPv4 protocol.

IPV4:



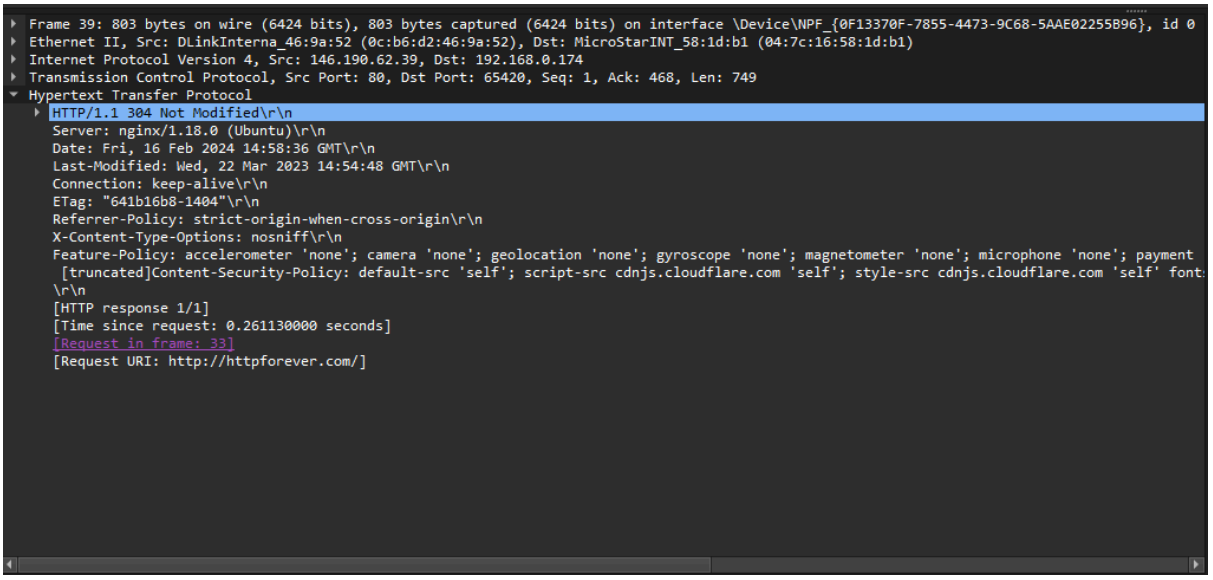
The IPV4 falls under the Network Layer. The source is 146.190.62.39 meaning the website HTTPforever.com, and the destination 192.168.0.174 meaning my PC. The packet contains a header of 20 bytes, utilising TCP for data transmission. Its overall size is 789 bytes and includes a Time-to-Live (TTL) value set at 46.

TCP:



TCP operates within the transport layer. The source port for the HTTP Forever website is 80, while the destination port, originating from my PC, is designated as 65420. The sequence number 1 represents the sequence number of the first byte of data in this TCP segment and acknowledgment number 468 acknowledges receipt of data up to sequence number 468. It's a relative acknowledgment number. TCP Segment Len: 749 indicates the data payload carried within this TCP segment, which is 749 bytes in size.

HTTP:



HTTP falls under the Application Layer. HTTP/1.1: Indicates the version of the HTTP protocol used. Then 304 Not Modified means that the requested resource has not been modified since the last requested time, and therefore, there is no need to resend the resource. Next the server lies on ubuntu. After that it is evident that the response was generated on 16th February 2024 with exact time and also when the requested resources were last modified, that is on 22 March 2023. Then the Connection: keep-alive indicates the fact of Persistent Transmission. Lastly, the server's response contains 33 frames of data.