Visit any http website while monitoring the network traffic. Now filter only the http packets. Observe the headers of any http request and response packet and explain how the layers are operating in this case.

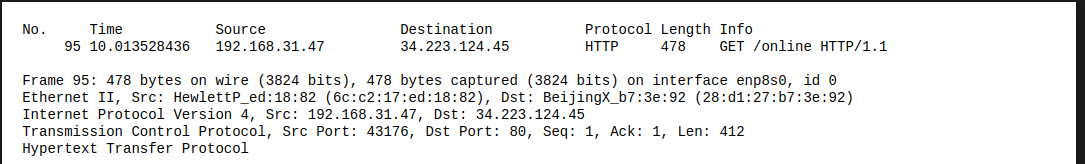
**Answer -** For this task, I have chosen a website that does not have https. The website I have chosen is [neverssl.com](http://neverssl.com), which only has some text on the website. [Here](https://drive.google.com/file/d/1XXoTJWP3TFiNNmdKPj7PsYMzSxC6nwsc/view) is the request captured from the wireshark while loading this website. After analysing the HTTP request, here is the report based on the OSI model.

The OSI model consists of seven layers. While conducting the analysis, I merged the layers and made it a TCP/IP model for better understanding. Here are the layers.

1. **Application Layer (HTTP)**: handles services and applications like web browsing.
2. **Transport Layer (TCP)**: ensures reliable data transfer between hosts.
3. **Network Layer (IP)**: Routing packages across different networks.
4. **Data Link Layer (Ethernet)**: Transfers data between directly connected devices.

As it can be noticed in the txt file, there are six HTTP requests captured by the wireshark, and each of them has a separate packet number. Among them, I will analyse two packets, which are packet 95 and packet 99. Here, packet 95 is a request packet, and packet 97 is the response to it.

#### **Packet 95: HTTP GET Request**



**Headers and Layers:**

* **Application Layer:**
  + **HTTP**:
    - Method: GET
    - URI: /online
    - Version: HTTP/1.1

It is the actual request specifying what the client wants to retrieve from the server; in this case, it is retrieving the content located at the “/online” path. Not only that, but it also contains the version number of the HTTP protocol being used.

* **Transport Layer:**
  + **TCP**:
    - Source Port: 43176
    - Destination Port: 80
    - Sequence Number: 1
    - Acknowledgment Number: 1
    - Length: 412

This layer is trying to transport data reliably from the client to the server, in this case the client device, to the website server. Here it has a client device port of 4317 and a destination port of 80 because it is an HTTP request. The sequence number indicates the starting number of bytes in this segment of data, and the acknowledgment number confirms receipt of the previous segment of data. 412 is the length of the TCP segment payload.

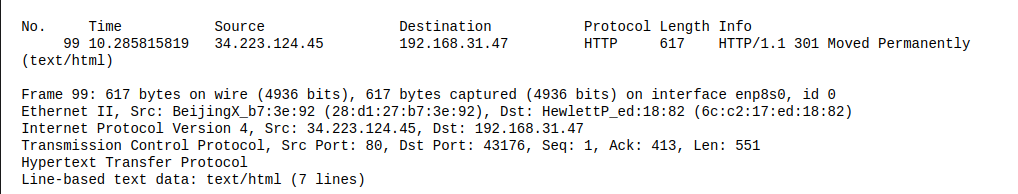
* **Network Layer:**
  + **IP**:
    - Source IP: 192.168.31.47
    - Destination IP: 34.223.124.45

This layer is trying to access the website from the local device; the source IP is the IP of the client device, and the destination IP is the IP of the website.

* **Data Link Layer:**
  + **Ethernet**:
    - Source MAC: HewlettP\_ed:18:82 (6c:c2:17:ed:18:82)
    - Destination MAC: BeijingX\_b7:3e:92 (28:d1:27:b7:3e:92)

This layer just transfers data from the local device to the next-hop device, here in this case HP laptop to the Xiaomi router.

#### **Packet 99: HTTP 301 Moved Permanently Response**



**Headers and Layers:**

* **Application Layer:**
  + **HTTP**:
    - Status: 301 Moved Permanently
    - Content-Type: text/html

The server responded with 301, which means the website the client was looking for is moved to a new URL and tells the client to update its records and make future requests to the new URL.

* **Transport Layer:**
  + **TCP**:
    - Source Port: 80
    - Destination Port: 43176
    - Sequence Number: 1
    - Acknowledgment Number: 413
    - Length: 551

As it is a response, it is coming from port 80, which is the port of the http response. The destination port is the port of the client's PC. The sequence number, acknowledgment number, and length indicate the same thing as the request.

* **Network Layer:**
  + **IP**:
    - Source IP: 34.223.124.45
    - Destination IP: 192.168.31.47

The source IP and destination IP are the same but reversed in the context of the request; from this, it can be noticed that the client is receiving something from the server.

* **Data Link Layer:**
  + **Ethernet**:
    - Source MAC: BeijingX\_b7:3e:92 (28:d1:27:b7:3e:92)
    - Destination MAC: HewlettP\_ed:18:82 (6c:c2:17:ed:18:82)

In this layer, the client PC is receiving the data from the Xiaomi router to the HP laptop.

In short, the client requested a website, but the server replied that the address of the requested website changed.