**DEPARTMENT OF INFORMATION TECHNOLOGY**

**COMPUTER NETWORKING LAB**

**LAB3: 18/11/2022**

**Marks : 10 Marks**

**Objective**

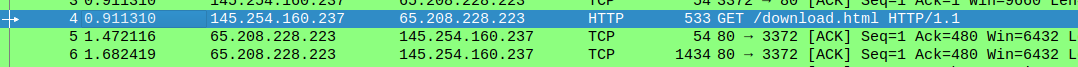
To understand the concept Packet headers at various layers

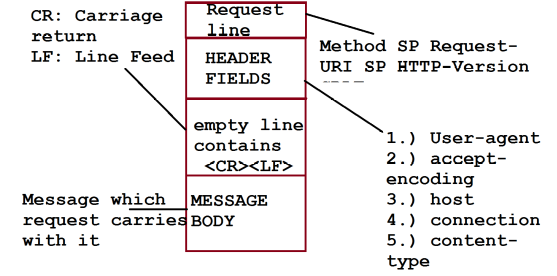
----------------------------------------------------------------------------------------

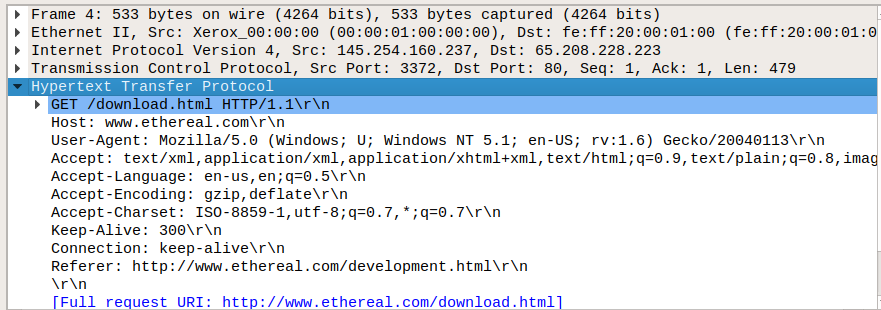
Download the http.pcap file from moodle.

Open the file and note down and understand the following things.

Click on following http request to understand the headers :

http request header 





**Q1. Note down the following from Message of HTTP request: [2 marks]**

Request Header :

GET /download.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /download.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /download.html

Request Version: HTTP/1.1

Header fields:

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.6) Gecko/20040113\r\n

Accept:text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,image/jpeg,image/gif;q=0.2,\*/\*;q=0.1\r\n

Accept-Language: en-us,en;q=0.5\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Reference: http://www.ethereal.com/development.html\r\n

\r\n

[Full request URI: http://www.ethereal.com/download.html]

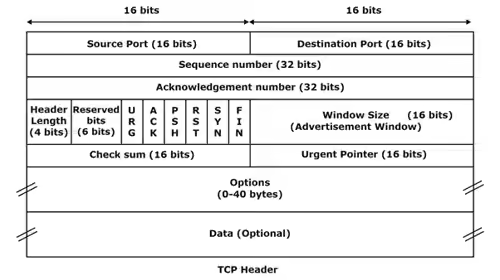
[HTTP request 1/1]

[Response in frame: 38]

**Q2: Write the relevance of these header fields in HTTP request. [2 marks]**

The HTTP request is sent to Transport Layer and TCP layer adds its own header for communication.

The format of TCP header is as follows:



**A2.**

The relevance of the header files in HTTP request are as follows:

**User Agent:** The user agent is an HTTP header that web browsers and other web applications use to identify themselves and their capabilities. User-Agent string is often used for content negotiation, where the origin server selects suitable content or operating parameters for the response. The web web security software captures and logs user agent data when users browse the Internet.

**Accept Language:** The Accept-Language request HTTP header indicates the natural language and locate that the client is present. Accept Language tells the server about all the languages the client can understand

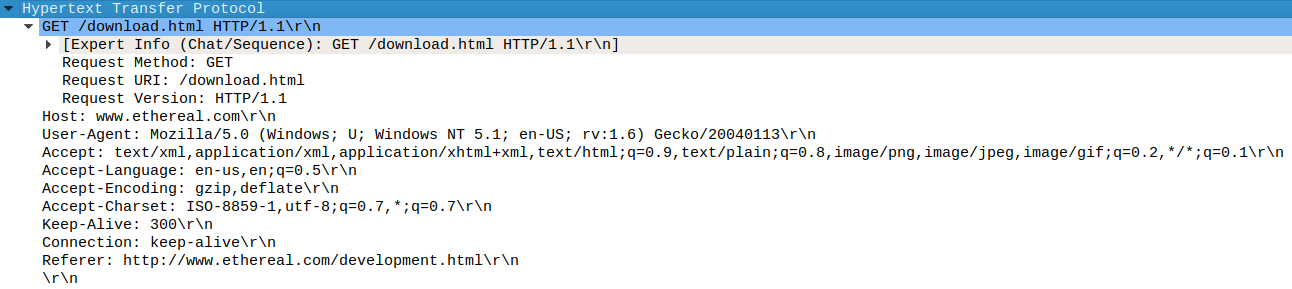
**Accept Encoding:** The accept encoding request HTTP header indicates the content encoding(usually a compression algorithm) that the client can understand. The accept- encoding restricts the content-codings that are acceptable in the response.

**Accept Charset:** The HTTP Accept-Charset is a request type header. This header is used to indicate what character set are acceptable for the response from the server. The accept-charset header specifies the character encodings which are accepted by the client and this header also allows a user-agent to specify the charsets it supports.

**Q3. From the pcap file click on Transmission Control protocol and identify the TCP header fields. Write its relevance in the header. Fill the table with details as shown for first field. [2 marks]**

| **Source Port: 3372** | | | | | | | | **Destination port: 80** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Sequence Number: 1** | | | | | | | | |
| **Acknowledge number: 1** | | | | | | | | |
| HL:  20 bytes | RES  000 | URG  0 | ACK  1 | PSH  1 | RST  0 | SYN  0 | FIN  0 | **Window Size: 9660** |
| **Checksum: 0xa958 [unverified]** | | | | | | | | **Urgent pointer: 0** |
| **Options:** | | | | | | | | |
| **Data:**  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 2f 64 65 76 65 6c 6f 70 6d 65 6e 74 2e 68 74 6d 6c 0d 0a 0d 0a | | | | | | | | |

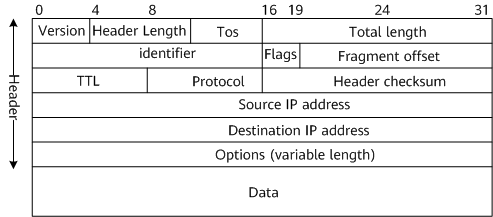
The data part in ASCII is as follows:

Find the relevance of each field and write at least one or two sentence about it. 

**Answer:**

After the TCP header is attached, The segment is sent to Network layer and It attaches header for routing.

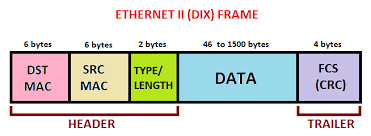
The format of IPv4 is as follows:



**Q4: Find the IPv4 fields for HTTP request and find their relevance [2marks]**

| **Version:**  **4** | | | **Header Length:**  **20 bytes (5)** | | | | | **ToS:**  **0x00** | | | **Total Length: 519** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Identifier: 0x0f45 (3909)** | | | | | | | | | | | **Flags: 0x40** | **Fragment Offset: 0** |
| **TTL: 128** | | | | | **Protocol: TCP(6)** | | | | | | **Header Checksum: 0x9010** | |
| **Source IP Address**  **145.254.160.237** | | | | | | | | | | | | |
| **Destination IP Address**  **65.208.228.223** | | | | | | | | | | | | |
| **Source Port: 3372** | | | | | | | | | | | **Destination port: 80** | |
| **Sequence Number: 1** | | | | | | | | | | | | |
| **Acknowledge number: 1** | | | | | | | | | | | | |
| HL:  20 bytes | RES  000 | URG  0 | | ACK  1 | | PSH  1 | RST  0 | | SYN  0 | FIN  0 | **Window Size: 9660** | |
| **Checksum: 0xa958** | | | | | | | | | | | **Urgent pointer: 0** | |
| **Options:** | | | | | | | | | | | | |
| **Data:**  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 2f 64 65 76 65 6c 6f 70 6d 65 6e 74 2e 68 74 6d 6c 0d 0a 0d 0a | | | | | | | | | | | | |

After The packet formation, the packet is sent to Data link layer and Ethernet protocol is used here.



**A4.**

The IPv4 fields and their relevance are:

**Version:** The first header field is a 4-bit version indicator. In the case of IPv4, the value of its four bits is set to 0100, which indicates 4 in binary.

**Header Length:** IHL is the 2nd field of an IPv4 header, and it is of 4 bits in size. This header component is used to show how many 32-bit words are present in the header.

**Type of Service:** ToS is also called Differentiated Services Code Point or DSCP. This field is used to provide features related to service quality, such as for data streaming or Voice over IP (VoIP) calls. It is used to specific how a datagram will be handled.

**Total Length:** This field’s size is 16 bit, and it is used to denote the size of the entire datagram.

**Identification:** The identification or ID field in a packet can identify an IP datagram’s fragments uniquely.

**Flags:** Flag in an IPv4 header is a three-bit field that is used to control and identify fragments.

**Fragment Offset:** This field is 13 bit long in length, and it is measured by blocks that units of 8-byte blocks. These are used to specify the offset of a fragment relative to the start of the IP datagram, which when it was not fragmented.

**Time to live:** Time to live (or TTL in short) is an 8-bit field to indicate the maximum time the datagram will be live in the internet system.

**Protocol:** This is a filed in the IPv4 header reserved to denote which protocol is used in the later (data) portion of the datagram.

**The header’s checksum:** The checksum field is of 16-bit length, and it is used to check the header for any errors. The header is compared to the value of its checksum at each hop, and in case the header checksum is not matching, the packet is discarded.

**Source Address:** It is a 32-bit address of the source of the IPv4 packet.

**Destination Address:** the destination address is also 32 bit in size, and it contains the receiver’s address.

**Options**: This is an optional field of the IPv4 header. It is used only when the value of IHL is set to more than 5. These options contain values and settings for things related to security, Record route and time stamp etc.

**Q5: Find the Ethernet II frame fields for HTTP request and find their relevance [2 marks]**

| **Destination MAC (48 bits): fe:ff:20:00:01:00** | | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Source MAC (48 bits): 00:00:01:00:00:00** | | | | | | | | | | | | |
| **Type/Length : IPv4 0x0800** | | | | | | | | | | | | |
| **Version:**  **4** | | | **Header Length:**  **20 bytes (5)** | | | | | **ToS:**  **0x00** | | | **Total Length: 519** | |
| **Identifier: 0x0f45 (3909)** | | | | | | | | | | | **Flags: 0x40** | **Fragment Offset: 0** |
| **TTL: 128** | | | | | **Protocol: TCP (6)** | | | | | | **Header Checksum: 0x9010** | |
| **Source IP Address**  **145.254.160.237** | | | | | | | | | | | | |
| **Destination IP Address**  **65.208.228.223** | | | | | | | | | | | | |
| **Source Port: 3372** | | | | | | | | | | | **Destination port: 80** | |
| **Sequence Number: 1** | | | | | | | | | | | | |
| **Acknowledge number: 1** | | | | | | | | | | | | |
| HL:  20 bytes | RES  000 | URG  0 | | ACK  1 | | PSH  1 | RST  0 | | SYN  0 | FIN  0 | **Window Size: 9660** | |
| **Checksum: 0xa958** | | | | | | | | | | | **Urgent pointer: 0** | |
| **Options:** | | | | | | | | | | | | |
| **Data:**  47 45 54 20 2f 64 6f 77 6e 6c 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 74 65 78 74 2f 68 74 6d 6c 3b 71 3d 30 2e 39 2c 74 65 78 74 2f 70 6c 61 69 6e 3b 71 3d 30 2e 38 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 6a 70 65 67 2c 69 6d 61 67 65 2f 67 69 66 3b 71 3d 30 2e 32 2c 2a 2f 2a 3b 71 3d 30 2e 31 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 33 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 65 74 68 65 72 65 61 6c 2e 63 6f 6d 2f 64 65 76 65 6c 6f 70 6d 65 6e 74 2e 68 74 6d 6c 0d 0a 0d 0a | | | | | | | | | | | | |

**A5.**

The Ethernet II frame fields for HTTP request has an Ethernet header, which contains the destination and source MAC addresses.

MAC addresses are used to uniquely identify a computer on the LAN. It is an essential component required for network protocols like TCP/IP to function.

The primary importance of source and destination MAC addresses is to identify the physical source and destination devices (NICs) on the local network segment.