

DEPARTMENT OF INFORMATION TECHNOLOGY

COMPUTER NETWORKING LAB

LAB3: 18/11/2022

Marks : 10 Marks

Objective

To understand the concept Packet headers at various layers

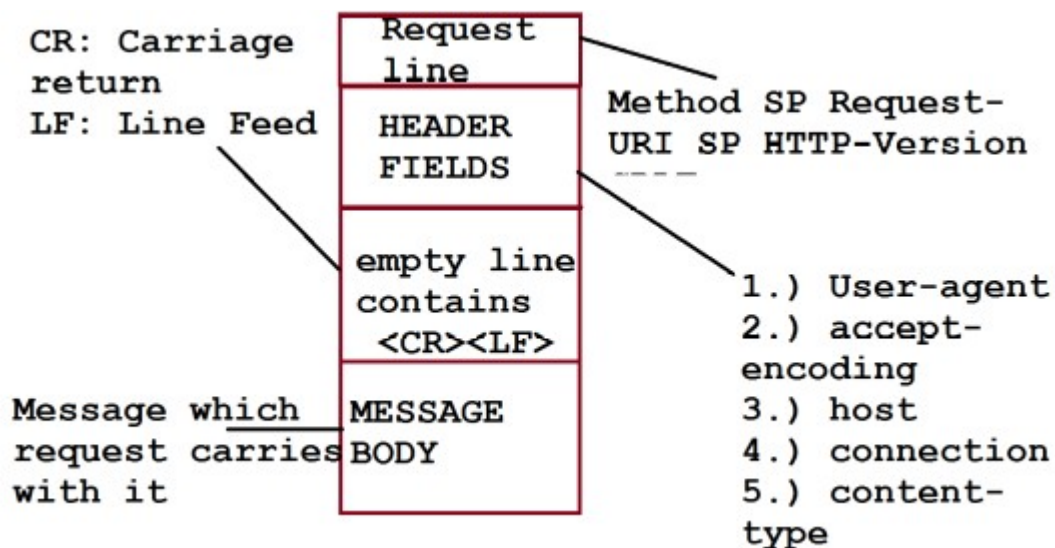
Download the http.pcap file from moodle.

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

Click on following http request to understand the headers :

3	0.911310	145.254.160.237	65.208.228.223	TCP	54 3372 → 80 [ACK] Seq=1 Ack=1 Win=5000 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533 GET /download.html HTTP/1.1
5	1.472116	65.208.228.223	145.254.160.237	TCP	54 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0

http request header



```

▶ Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
▶ Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▶ Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
▶ Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
▼ Hypertext Transfer Protocol
  ▶ GET /download.html HTTP/1.1\r\n
    Host: www.ethereal.com\r\n
    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;q=0.7\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
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
    [Full request URI: http://www.ethereal.com/download.html]

```

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

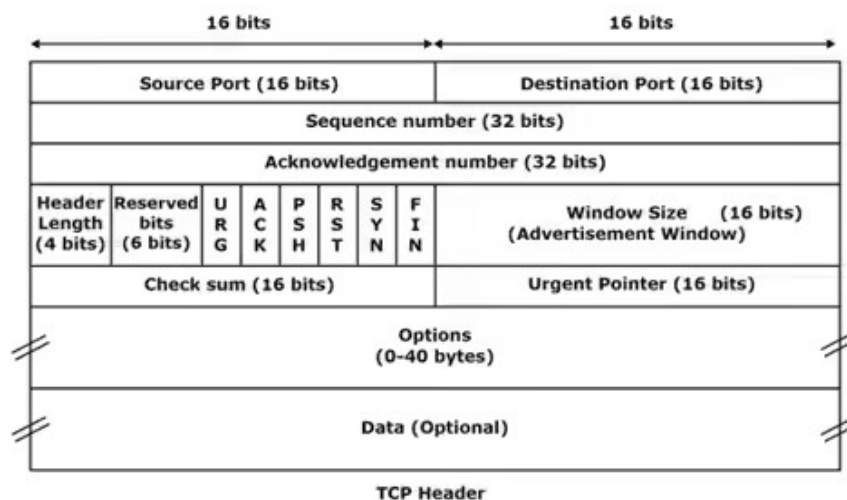
Request Header :

Header fields: like User_Agent, Accept: Accept Language: Accept encoding, Accept-charset, Keep alive, Connection , Reference: etc

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:



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:
Sequence Number:								
Acknowledge number:								
HL:	RES	URG	ACK	PSH	RST	SYN	FIN	Window Size:
Checksum:								Urgent pointer:
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

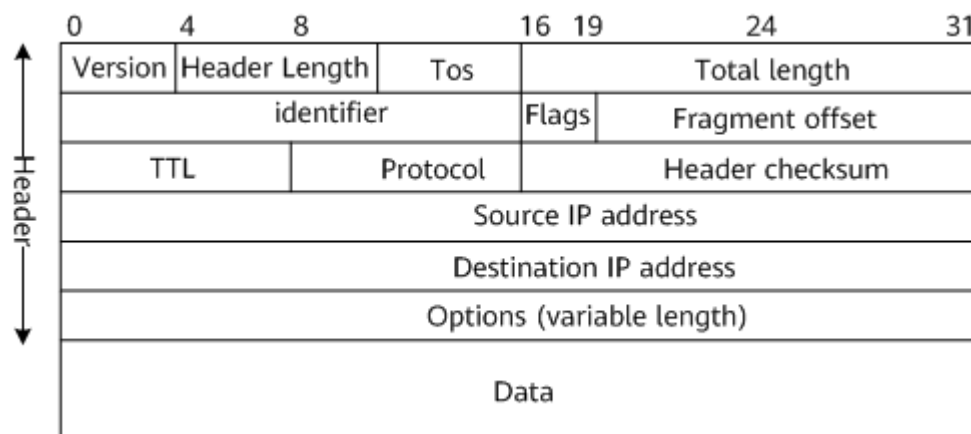
The data part in ASCII is as follows:

```
▼ Hypertext Transfer Protocol
▼ 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
    Host: www.ethereal.com\r\n
    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
    Referer: http://www.ethereal.com/development.html\r\n
    \r\n
```

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

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]

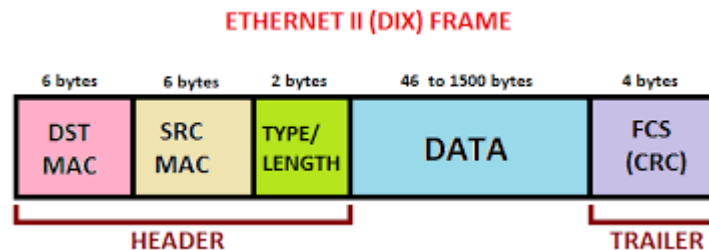
Version		Header Length		ToS		Total Length					
Identifier:						Flags		Fragment Offset			
TTL		Protocol				Header Checksum:					
Source IP Address											
Destination IP Address											
Source Port: 3372						Destination port:					
Sequence Number:											
Acknowledge number:											
HL:	RES	URG	ACK	PSH	RST	SYN	FIN	Window Size:			
Checksum:						Urgent pointer:					
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.



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

Destination MAC (48 bits)			
Source MAC (48 bits):			
Type/Length : IPv4 0x0800			
Version	Header Length	ToS	Total Length

Identifier:								Flags	Fragment Offset
TTL		Protocol						Header Checksum:	
Source IP Address									
Destination IP Address									
Source Port: 3372								Destination port:	
Sequence Number:									
Acknowledge number:									
HL:	RES	URG	ACK	PSH	RST	SYN	FIN	Window Size:	
Checksum:								Urgent pointer:	
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									