Name:- Chikkeri Chinmaya
Roll Number:- 211IT017

Question 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

Question 2

- **Request headers: It contain more information about the resource to be fetched, or about the client requesting the resource. Host: Specifies the domain name of the server (for virtual hosting), and (optionally) the TCP port number on which the server is listening.**

- **User-Agent: The User-Agent request header is a characteristic string that lets servers and network peers identify the application, operating system, vendor, and/or version of the requesting user agent. Accept: Informs the server about the types of data that can be sent back.**

- **Accept-Encoding: The encoding algorithm, usually a compression algorithm, that can be used on the resource sent back. Accept-Language: Informs the server about the human language the server is expected to**

send back. This is a hint and is not necessarily under the full control of the user: the server should always pay attention not to override an explicit user choice (like selecting a language from a dropdown).

- **Accept-Charset: The Accept-Charset request HTTP header was a header that advertised a client's supported character encodings. It is no longer widely used.**

- **Connection: Controls whether the network connection stays open after the current transaction finishes.**

- **Keep-Alive: Controls how long a persistent connection should stay open**

- **Referer: The address of the previous web page from which a link to the currently requested page was followed.**

Question 3

Source Port: 3372	Destination port: 80
Sequence Number: 1	
Acknowledge number:1	

HL:	RES	URG	ACK	PSH	RST	SYN	FIN	Window Size: 9660
20 Bytes	000.	….	….	….	….	….	….	
	….	..0.	…1	….	….	….	….	
	….	….	….	…1	.0..	..0.	…0	

Checksum: 0xa9958	Urgent pointer:0

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
```

The transmission control protocol (TCP) is the internet standard ensuring the successful exchange of data packets between devices over a network. TCP is the underlying communication protocol for a wide variety of applications, including web servers and websites, email applications, FTP and peer-to-peer apps.

• **Source port:** this is a 16 bit field that specifies the port number of the sender.

• **Destination port**: this is a 16 bit field that specifies the port number of the receiver.

• **Sequence number**: the sequence number is a 32 bit field that indicates how much data is sent during the TCP session. When you establish a new TCP connection (3 way handshake) then the initial sequence number is a random 32 bit value. The receiver will use this sequence number and sends back an acknowledgment. Protocol analyzers like wireshark will often use a relative sequence number of 0 since it's easier to read than some high random number.

• **Acknowledgment number**: this 32 bit field is used by the receiver to request the next TCP segment. This value will be the sequence number incremented by 1.

• **DO:** this is the 4 bit data offset field, also known as the header length. It indicates the length of the TCP header so that we know where the actual data begins.

• **RSV:** these are 3 bits for the reserved field. They are unused and are always set to 0.

• **Flags:** there are 9 bits for flags, we also call them control bits. We use them to establish connections, send data and terminate connections:

• **URG**: urgent pointer. When this bit is set, the data should be treated as priority over other data.
• **ACK:** used for the acknowledgment.

• **PSH:** this is the push function. This tells an application that the data should be transmitted immediately and that we don't want to wait to fill the entire TCP segment.

• **RST:** this resets the connection, when you receive this you have to terminate the connection right away. This is only used when there are unrecoverable errors and it's not a normal way to finish the TCP connection.

• **SYN**: we use this for the initial three way handshake and it's used to set the initial sequence number.

• **FIN:** this finish bit is used to end the TCP connection. TCP is full duplex so both parties will have to use the FIN bit to end the connection. This is the normal method how we end an connection.

• **Window:** the 16 bit window field specifies how many bytes the receiver is willing to receive. It is used so the receiver can tell the sender that it would like to receive more data than what it is currently receiving. It does so by specifying the number of bytes beyond the sequence number in the acknowledgment field.

• **Checksum**: 16 bits are used for a checksum to check if the TCP header is OK or not.

• **Urgent pointer**: these 16 bits are used when the URG bit has been set, the urgent pointer is used to indicate where the urgent data ends.

• **Options**: this field is optional and can be anywhere between 0 and 320 bits

74 2e 68 74 6d   6c 0d 0a 0d 0a

Question 4

Version 4	Header Length 20 Byets	ToS	Total Length;- 519	
Identifier:0x0f45			Flags 0x4000	Fragment Offset
TTL 128	Protocol TCP (6)		Header Checksum: 0x9010	
Source IP Address 145.254.168.237				
Destination IP Address 65.208.228.223				
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				

- **VERSION:** Version of the IP protocol (4 bits), which is 4 for IPv4

• **Header Length** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.

• **Type of Service (ToS):** Low Delay, High Throughput, Reliability (8 bits)

• **Total Length (TTL):** Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

• **Identification:** Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

• **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

• **Fragment Offset**: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 byte.

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): Xerox_00:00:01:00:00:00
Type/Length : IPv4 0x0800
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

- **Destination Address** – This is 6-Byte field which contains the MAC address of machine for which data is destined.

- **Source Address –** This is a 6-Byte field which contains the MAC address of source machine. As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.

- **Length –** Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 Bytes because of some own limitations of Ethernet.