Assignment-2:

Submitted by: GROUP 9_ Bhagyashree (120123027) | Harsh Deep(120123018)

We played Muffinstar game on onlinegames.com and analysed the packets sent and received using Wireshark.

Q1) List out all the protocols used by the application at different layers (only those which you can figure out from traces) and study their packet formats.

Solution 1:

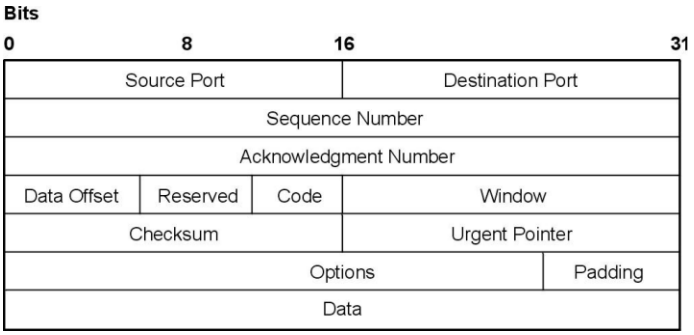
Protocols used :

HTTP - Hypertext Transfer Protocol

Packet format :

MAC Header	IP Header	TCP Header	Data

TCP - Transmission Control Protocol(Transport protocol)



TLSv1.2 - Transport layer cryptographic protocol to enhance the security of the layer

Q 2:

Highlight and explain the values of various fields of the protocols which you can see in the traces. Example, Source or destination IP address and port no., Ethernet address, protocol number, etc.

Solution 2:

TCP:

Source Port: sending port. (Value is 3128)

Destination Port: receiving port.(Value is 50437)

Acknowledgement Number: Acknowledge of packets which have successfully arrived. Then it will be the sequence number of the next packet ready to receive.

Flags: Contains 9, 1 bit flags. These are NS, CWR, ECE, URG, ACK, PSH, RST, SYN, FIN (Value is 0x010 i.e. ACK)

Sequence No:If the SYN flag is set i.e. 1, then the value is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence no plus 1.if the SYN flag is reset i.e. 0, then this is the accumulated sequence no of the first data byte of this segment for the current session.
Given to IP Packets when application's data is packaged into IP packets
Header Length: The total size of the header region in bytes (Value is 20bytes)
Checksum: 16 bit field for Error correction
TCP Segment Length: The total size of the tcp application data in bytes (Value is 1460 bytes)

HTTP :

Request Method : GET,POST,HEAD,PUT etc
HOST: The Host request-header field specifies the Internet host and port number of the resource being requested
Proxy-Connection: The Proxy-Connection general-header field allows the sender to specify options that are needed
Proxy-Authorization: Authorization of client for connecting to a proxy .
Accept-Encoding: The Accept-Encoding request-header field restricts the list of content accepted
Accept-Language: The Accept-Language request-header field restricts the set of languages

TLSv1.2:

Host – Domain name of the server
Connection – Control options for the current connection and list of hop-by-hop request fields.
Proxy Authorization – Authorization credentials for connecting to a proxy
Accept – Content type that are acceptable for the response

Q 3:
Explain the sequence of messages exchanged by the application for using several functionalities available in the application. For example, upload, download, play, pause, stop and so on. Check and explain if any handshaking sequence occurs or not.

Solution 3 :
When the game starts/stops/pauses i.e. it is not being played , lot of messages in the form of TCP Packets are getting sent for establishing the connections and exchanging of the data properly to ensure the current state is communicated . When the game is being played(up/ down /jump mode) HTTP requests and TCP packets are sent to server. Some TLSv1.2 protocol packets are also sent to ensure secure connection .

HANDSHAKING SEQUENCE takes place

Q 4:

Explain how a particular protocol is relevant for functioning of the application

Solution 4:

Every packet has its own importance for the game to function properly and hence every protocol is of importance in its own way

HTTP: The HTTP protocol is a request/response protocol based on the client/server based architecture. The client initiates an HTTP request message, which is serviced through a HTTP response message in return by the server.Thus HTTP decides action to be performed using methods like GET and POST

TCP: It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control and provide error-free data transmission-handles.

TLSv1.2: These are cryptographic protocols designed for network security.

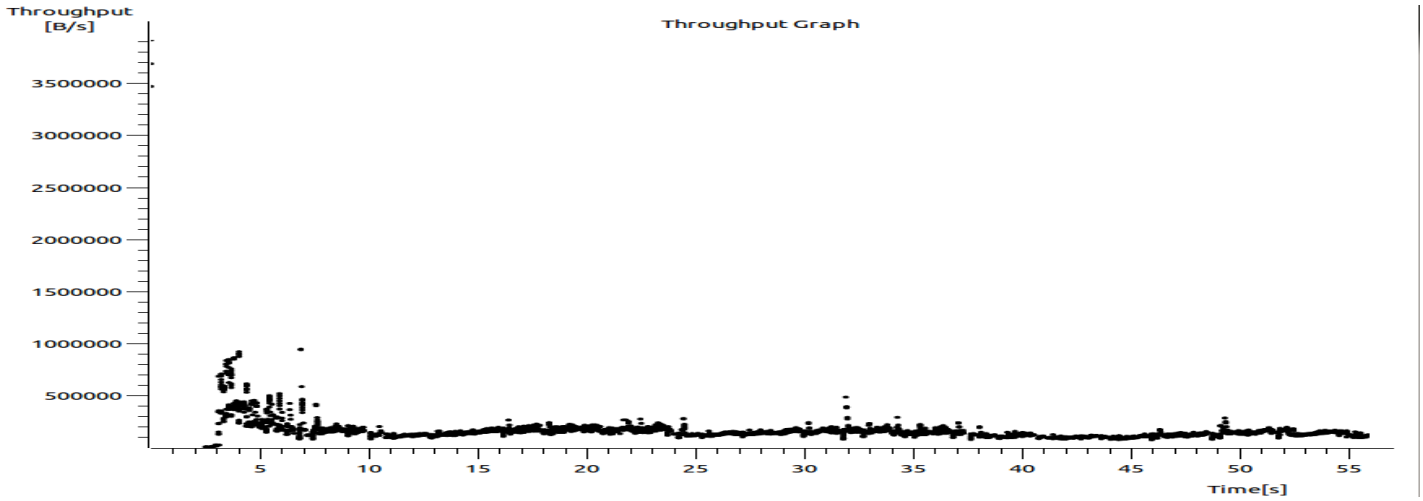
Q5. Calculate the following statistics from your traces when you perform experiment at different times of the day: Throughput, RTT, Packet size, No. of packets lost, number of UDP & TCP packets, number of responses received with respect to one request sent.

Solution 5:

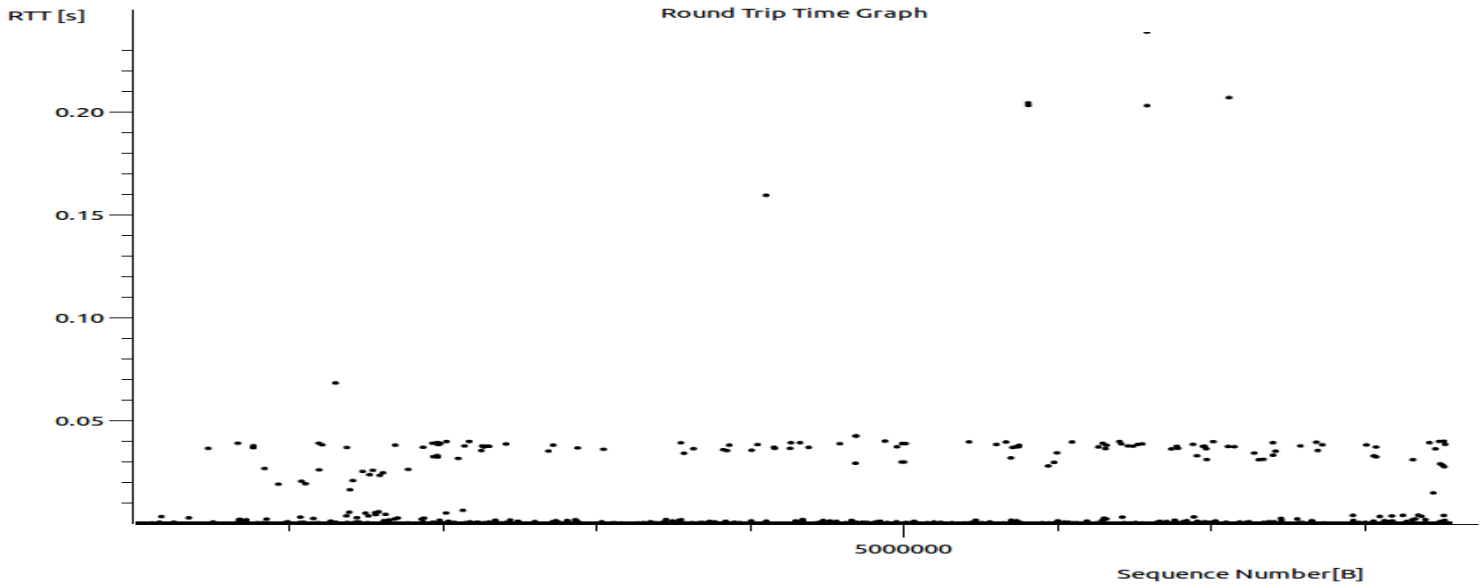
Time : 0730 , 1730, 2330 hrs using hostel server and IITG_WIFI

Total packets obtained = ~12k
TCP Packets = ~5k
Packet Loss is 0% in the captured packets.

Throughput Graph



Round Trip Time Graph



Number of responses wrt one request:
HTTP requests
TCP protocols .
TLSv1.2 protocols

Q6. Check if the whole content is being sent from same location/source. List out the IP addresses of content providers if there exist multiple sources and explain the reason behind it.

Solution 6:
The source is either 10.16.21.41(ip address of the computer used) or 202.141.80.20(proxy server authorized in IIT campus for students) Since we use the filtered the data by using proxy authentication (202.141.80.20) all the packets come in and go through this proxy Hence we cannot get the ip addresses of the original source.