**Part 2 Wireshark Packet Analyzer (Marks: 10)**

**\*\*\*\*Submission: You have to submit your (Roll-No.docx) word file in a folder named Question 2. You should provide proper explanation along with screen shots. \*\*\*\***

**Part 1: \*\*\*Wireshark Session: Capture 1\*\*\* [4]**

1. Filter out all TCP packets which are either going to or coming from IP: 128.119.245.12 on Port: 80**.** Write your filter as answer

**Ip.addr==128.119.245.12 && tcp.port==80**

1. If we take the first filtered packet as Packet No. 1, with each successive packet increasing one in number, then what is the request made in Packet No. 20 and what is the response from the server?

**Req: HTTP GET /wireshark-labs/Intor-Wireshark-file1.html**

**Response: HTTP 304 Not Modified**

1. How many data containing TCP Segments are present between the request made and response received for the packet in question 2**?**

**No data containing TCP segments are present between Request and Response (Excluding the one in which the response came). Only acknowledgements packets**

1. What is the content (data) length in bits returned by the server in response to the request made in Packet No. 28 taking first filtered packet as Packet No. 1?

**209 Bytes \* 8 = 1672 bits**

**Part 2: \*\*\* Wireshark Session: Capture 2\*\*\* [4]**

1. FTP is an application protocol and uses TCP as a Transport Layer Protocol. Filter out all the FTP packets by applying the filter on specific ports used by File Transfer Protocol to make a connection or transfer the data. Write your filter as the answer

**Tcp.port == 21 || tcp .port == 20(you were asked to apply filter on specific ports used by FTP)**

1. In the packets filtered, client asks for data two times from the server on a specific port and IP Address because of which server opens a data connection on the corresponding socket and sends the data to client on that newly opened socket on the client side. Keeping the sequence of first two client requests with regards to IP and Port Number, what will be the request made by client to get the data for the third time from the server?

**Client-> Request:PORT 192,168,1,2,63,215**

1. In regard to the third request made by client in question 6, server will send the data to the client on which Port Number (client side), Port Number (server side), IP address (client side) and IP address (server side)?

**Client Port: 16343 (Most Important)**

**Server Port: 20**

**Client IP: 192.168.1.2**

**Server IP: 195.89.6.167**

1. Apply a filter to get all the UDP packets which are directed towards Port Number 53 either by client or by server. What filter did you apply? If we take the first filtered packet as Packet No. 1 with each successive packet increasing one in number, then what will be the acknowledgement number of the DNS request made in Packet No. 12? Also tell the sequence number of the packet in which the request is made?

**Udp.port == 53. No acknowledgements in UDP.**

**Part 3: \*\*\* Wireshark Session: Capture 3\*\*\* [2]**

1. In which packet (write packet number) we have received the acknowledgement for the TCP Segment being carried in the packet number 13? What is the acknowledgement number and sequence number in the packet received? Show clear calculations how the server has sent the corresponding acknowledgement number?

**Packet 17 , Seq=1, Ack=9013(1+565+1460+1460+1460+1460+1460+1147)**

1. In Packet No. 170, what is the value of Sequence Number? How will you explain the value of Sequence Number?

**Seq = 1. The main reason is that server is only receiving the data due to POST request by the client. Its sequence became 1 as a result of three way handshake.**