CSE 421 **ID:** 22241163

Transport Layer Protocols (TCP) Examination Lab

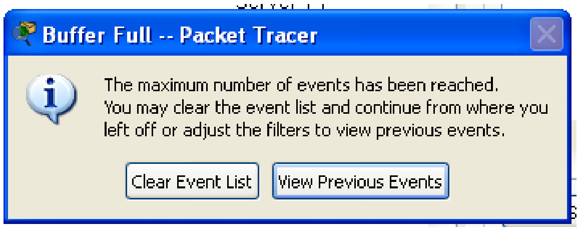
Objectives:

Capture traffic and observe the PDUS for TCP when a HTTP request is made.
.

Task 1: Observe TCP traffic exchange between a client and server.

Step 1 – Run the simulation and capture the traffic.

- Enter **Simulation** mode.
- Check that your Event List Filters shows only **HTTP** and **TCP**.
- Click on the PC1. Open the **Web Browser** from the **Desktop**.
- Enter **www.bracu.ac.bd** into the browser. Clicking on **Go** will initiate a web server request. Minimize the Web Client configuration window.
- A TCP packet appears in the **Event List**, as we will only focus on TCP the DNS and ARP packets are not shown.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.



The maximum number of events has been reached.
You may clear the event list and continue from where you left off or adjust the filters to view previous events.

- When the above message appears Click "View Previous Events".
- Click on PC1. The web browser displays a web page appears.

Step 2 – Examine the following captured traffic.

Our objective in this lab is only to observe TCP traffic.

	Last Device	**At Device**	**Type**
1.	PC1	Switch 0	TCP
2.	Local Web Server	Switch 1	TCP
3.	PC1	Switch 0	HTTP
4.	Local Web Server	Switch 1	HTTP
5.	PC1 (after HTTP response)	Switch 0	TCP
6.	Local Web Server	Switch 1	TCP
7.	PC1	Switch 0	TCP

- As before find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.

- When you click on the Info square for a packet in the event list the **PDU Information** window opens. If you click on these layers, the algorithm used by the device (in this case, the PC) is displayed. View what is going on at each layer.

For packet 1::

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header.

A. What is this TCP segment created by PC1 for? How do you know what is it for?

The first stage in three-way handshaking is the creation of TCP segments with

the server since the sequence number and acknowledgment number are both zero.

B. What control flags are visible?

000010 control flags are visible.

C. What are the sequence and acknowledgement numbers?

Both the sequence and acknowledgement numbers are 0.

For packet 2:

Click onto “Inbound PDU details” tab. Scroll down and observe the TCP header.

A. Why is this TCP segment created by the Local Web Server?

The local web server creates a TCP segment to transfer data. TCP segments can be transmitted between the client and server once a TCP connection has been established via the three-way handshake. TCP employs sequence numbers to confirm the proper delivery and sequencing of TCP segments in order to protect against the errors brought on by the unstable network.

B. What control flags are visible?

010010 control flags are visible.

C. Why is the acknowledgement number “ 1”?

The server asks the client to submit the following data, which has sequence number 1, for the second phase of the three-way handshaking. Making the ack 1.

For packet 3:

This HTTP PDU is actually the third packet of the “Three Way Handshake” process, along with the HTTP request.

A. Explain why control flags **ACK(Acknowledgement)** and **PSH (Push)** are visible in the TCP header?

PSH is visible because the data is sent right away rather than waiting because the ACK

flag, which is used for acknowledgement, must be visible to ensure that the server has received the earlier bits.

For packet 5:

After PC1 receives the HTTP response from the Local Web Server, it again sends a TCP packet to the Local Web server why?

PC1 sends another TCP packet to the local web server to close the TCP connection after receiving the HTTP response from the local web server.

Click onto "Inbound PDU details" tab. Scroll down and observe the TCP header.

A. What control flags are visible?

010001 control flags are visible.

B. Why the sequence number is 104 and acknowledge number 254? Note this packet is created after PC1 receives the HTTP response from the server.

The sequence number is used to establish a connection, while the acknowledgment number informs us about the package that needs to be synchronized with the rest of the data.

For packet 6:

Click onto "Inbound PDU details" tab. Scroll down and observe the TCP header.

What is this packet sent from the webserver to PC1 for?

The TCP header packet sent from the webserver to PC1 for closing the TCP Connection.

What control flags are visible?

010000 control flags are visible.

Why the sequence number is 254?

The sequence number is 254 because the client has sent the data till sequence number 253 already.