CSE 421 **ID:** 18301221

Transport Layer Protocols (TCP) Examination Lab

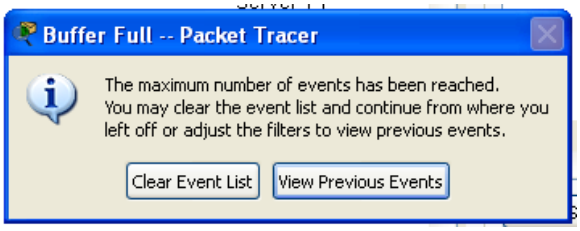
Objectives:

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.



- 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?

PC1 creates a TCP segment in order to perform the handshake that establishes the connection between the computer and the server. Both acknowladgement and sequence number are 0 and SYN bit enabled which is the first step of three way handshaking.

B. What control flags are visible?

SYN flag.

C. What are the sequence and acknowledgement numbers?

SEQUENCE NUMBER:0 & ACKNOWLEDGEMENT NUMBER: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?

TCP segment created by the Local Web Serverto reply the sync of three way handshake connection and send data.

B. What control flags are visible?

ACKNOWLEDGEMENT flag & SYN flag.

C. Why is the acknowledgement number “ 1”?

Web server is acknowledging the number from PC1 and that's why the acknowladge number 1'. It indicates that it will be able to establish a connection. It's the 2nd stage of three way handshaking.

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?

Because the connection was recently established, the ACK (Acknowledgement) control flag is visible, and the PSH (Push) control flag is visible for data communication because the data is flowing toward the server.

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?

To terminate the connection

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

A. What control flags are visible?

FIN & ACK

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 104 beacuse client expects 104th packet from the server

acknowledge number 254 beacuse it received up to 253 and expectiong 254.

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?

To close TCP connection and acknowladge last data.

What control flags are visible?

FIN & ACK

Why the sequence number is 254?

The sequence number is 254 because 253 segments just delivered by the sender and

it will send data from 254.