CSE 421 **ID:** 19301023

Transport Layer Protocols (TCP) Examination Lab

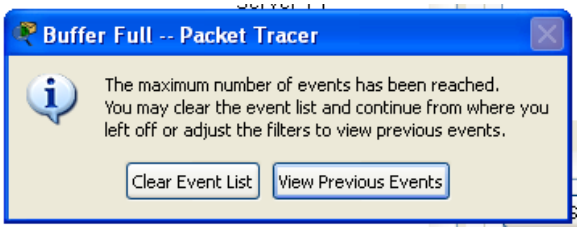
Objectives:

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?

This TCP segment has been created by PC1 for establishing a connection with the web server.

We know what it is for by looking at the flags in the header where the SYN bit is turned on.

B. What control flags are visible?

Only the SYN control flag is visible as the flags value is 0b00000010.

C. What are the sequence and acknowledgement numbers?

Both the sequence and the acknowledgement number 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?

This TCP packet is the second packet of the three way handshake. Through this packet the web server is asking the client if they are sure that they want to establish a connection between them.

B. What control flags are visible?

Both the SYN and ACK control flags are visible as the flags value is 0b00010010.

C. Why is the acknowledgement number “ 1”?

The reason why the acknowledgement number is 1 is the web server has received the first byte for connection from PC1 and is expecting the next byte which starts from 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?

To let the server know about the acknowledgement of the previous data PC1 has set ACK as 1.

Again, reason for PSH being 1 is that the data that is going to be sent by PC1 has to be processed right away and sent to the upper layer.

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?

It again sends a TCP packet for closing the connection with the Local Web Server.

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

A. What control flags are visible?

The ACK and the FIN control flags are visible as the flags value is 0b00010001.

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 because the server mentioned in the HTTP response message that it has received till 103 bytes from PC1 and has acknowledged that. Again, the acknowledgement number is 254 because PC1 has received till 253 bytes from the server and is expecting from byte number 254 now.

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?

It is to acknowledge that the server has received the connection close request message from PC1 and asking PC1 if it really wants to close the connection.

What control flags are visible?

Both the ACK and FIN control flags are visible as the flags value is 0b00010001.

Why the sequence number is 254?

The reason why the sequence number is 254 is that PC1 has received till byte number 253 and has acknowledged that. In addition, PC1 is now expecting from byte number 254. So, the server is now sending data from byte number 254.