CSE 421 **ID:** 20101549

Application Layer Protocols (HTTP.SMTP/POP) Examination Lab

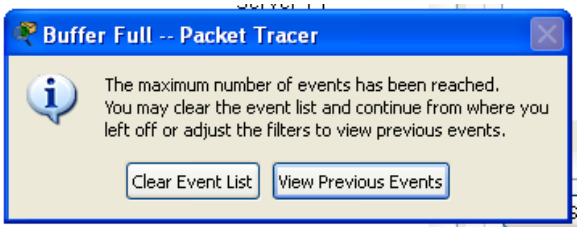
Objectives:

Capture traffic and observe the PDUS for HTTP, SMTP, POP.

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

Step 1 – Run the simulation and capture the traffic.

- Enter **Simulation** mode.
- 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.
- Two packets appear in the **Event List**, a DNS request needed to resolve the URL to the IP address of the web server and an ARP request needed to resolve the IP address of the server to its hardware MAC address.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.



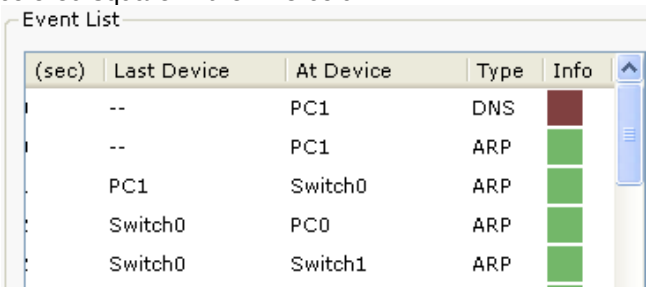
- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser displays a web page appears.

Step 2 – Examine the following captured traffic.

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

	Last Device	At Device	Type
1.	PC1	Switch 0	HTTP
2..	Local Web Server	Switch 1	HTTP

- 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.

- Examine the PDU information for the remaining events in the exchange.

For packet 1::

What kind of HTTP packet is packet no. 1?

Request HTTP packet (Non Persistent.)

Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see?

HTTP Data:Accept-Language: en-us
Accept: */*
Connection: close
Host: www.bracu.ac.bd

This is a HTTP request of 32 bytes and the language, accepting file type, connection and host is mentioned

For packet 2:

Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see? What kind of HTTP packet is this?

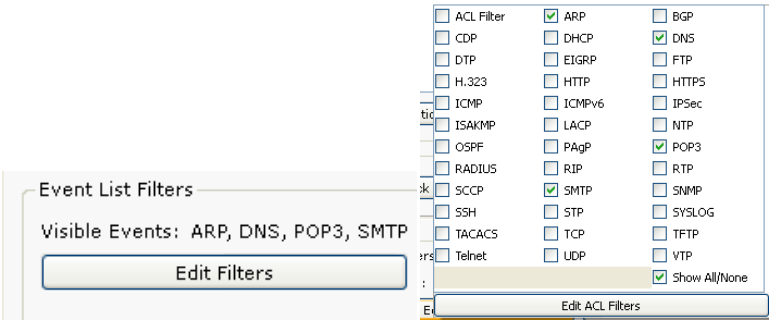
A 32 bytes HTTP response packet from the local web server. It contains connection state, content length and server.

HTTP Data:Connection: close
Content-Length: 151
Content-Type: text/html
Server: PT-Server/5.2

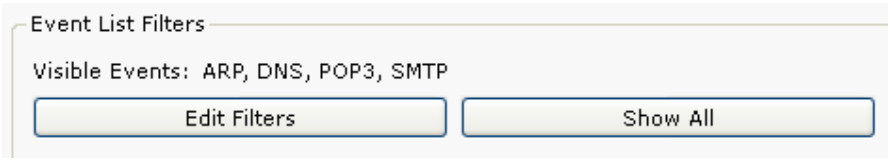
Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.

Step 1 – Run the simulation and capture the traffic.

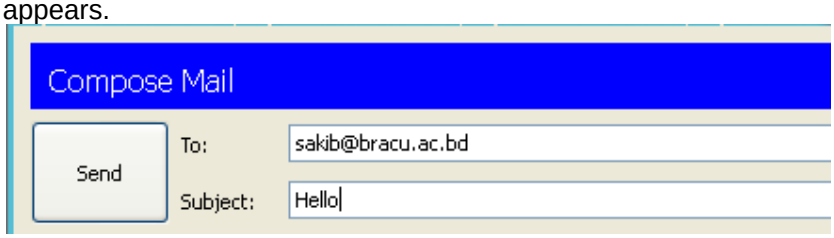
- On the Event List window click “Reset Simulation” button. All previous packets will disappear.
- At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click SMTP and POP3.



- Click a space anywhere outside the popup window, then it will disappear.
- Your Event List Filter should be as shown below:



- Now click on the PC1. Close the web browser window. Open the **Email** from the **Desktop**. A mail browser window will open. Click “compose”, another window appears.



- Fill the window as shown and press send.
- Minimize the client window .
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.
- This interaction is between the sender client and its email server.

Step 2 – <u>Examine the following captured traffic.</u>

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

	Last Device	**At Device**	**Type**
3.	PC1	Switch 0	DNS
4.	PC1	Switch 0	SMTP
5.	Bracu Email Server	Switch 1	SMTP

- Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
- Examine the PDU information.

<u>For packet 4::</u>

What is the purpose of this DNS packet?

To get the IP addresses and to resolve host names in TCP/IP network

<u>For packet 5& 6::</u>

Explain why SMTP packet was sent to the email server and the server replied with an SMTP packet?

SMTP is used to send emails. An SMTP server can relay emails through multiple hops to the recipient's email service's SMTP server. After sending an email, the server replies with an SMTP packet to confirm success or failure. Acknowledgment is received using an SMTP packet. The main reason is to send data in mail server and get acknowledgment .

Step 3 – <u>Run the simulation and capture the traffic for POP.</u>

- On the Event List window click “Reset Simulation” button. All previous packets will disappear.
- Now click on the PC0. Open the **Email** from the **Desktop**. A mail browser window will open. Click “**receive**”, minimize the window.
- Click the **Auto Capture / Play** button to run the simulation and capture events.
- Sit tight and observe the packets flowing through the network.
- This interaction is between the sender client and its email server.

Step 2 – <u>Examine the following captured traffic.</u>

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

	Last Device	**At Device**	**Type**
6.	PC1	Switch 0	DNS
7.	PC1	Switch 0	POP3
8.	Bracu Email Server	Switch 1	POP3

- Find the following packets given in the table above in the **Event List**, and click on the colored square in the **Info** column.
- Examine the PDU information.

<u>For packet 6::</u>

What is the purpose of this DNS packet?

The purpose of DNS packet here is to resolve and get IP addresses

<u>For packet 7&8::</u>

Explain why POP packet was sent to the email server and the server replied with a POP packet?

POP packets are used to verify if there's new mail in the email server for a user. The server responds with a POP packet to notify the user of any incoming emails. This process helps users stay updated on their email status and receive new messages. It checks and reply the response.