CSE 421 **ID: _____**

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.

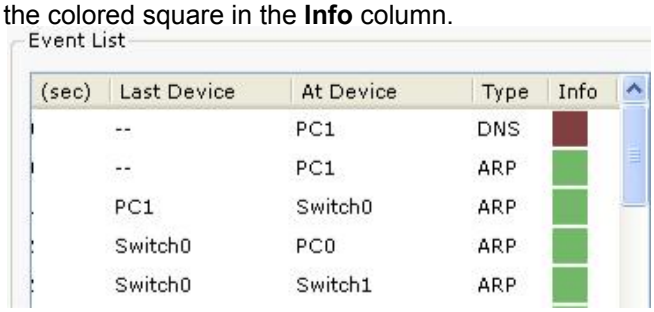
- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser displays a web page appears.

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?

_____ The packet 1 is Request Get HTTP kind. (Non-Persistent.)_____

_____

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

_____HTTP Data:Accept-Language: en-us Accept: */*, which indicates the natural language and locale that the client prefers. And accept: */* simply means that any data of whatever mimetype is accepted and the server may choose what to return to the requesting client._____

_____

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?

HTTP Data:Connection: close
Content-Length: 151
Content-Type: text/html
Server: PT-Server/5.2.
HTTP packet type: Response HTTP packet(Non-persistent)_____

_____

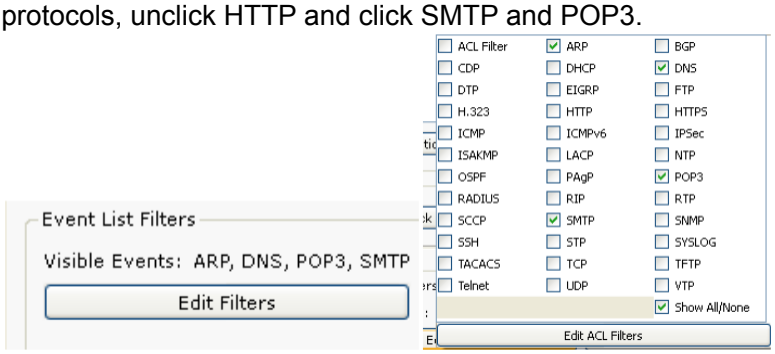
_____

_____

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

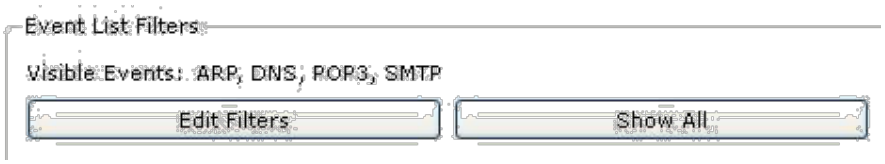
Step 1 – Run the simulation and capture the traffic.

- 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 resolve 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?

_____ The SMTP protocol is used to send emails, that is why SMTP packet is used here. One SMTP server can send email to another SMTP server, relay it to the destination through several hops. The SMTP server then sends the email to the recipient's email service's SMTP server. Here email was sent using a SMTP so the server replied back to the user with SMTP packet telling the email sending was successful or not. So, for acknowledgement of receiving the packets SMTP packet was sent to the email server and the server replied with an SMTP packet _____

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 IP addresses. Here the DNS client needs to find the IP Address of a computer known by its FQDN that is why it queries DNS servers to get the IP Address with the help of DNS packets._____

_____

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

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

_____ As POP packet is used to receive email, when the email is gone to pop3 server , the email is stored there until the receiver opens his email account. The POP packet sends a signal to the email server to check if there is any email for the user and the server then replies back using pop packet to user. Finally, user will be able to see if there is any new email. As it sends a POP request to the server so the replied with POP packet. So basically POP packet was sent to the email server and the server replied with a POP packet to check if

there is any new email that came to the email server and for delivering new email to the client._____

_____

_____

-