CSE 320 **ID:** 19101573

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

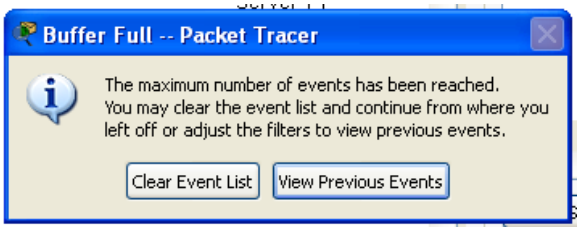
Objectives:

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

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.



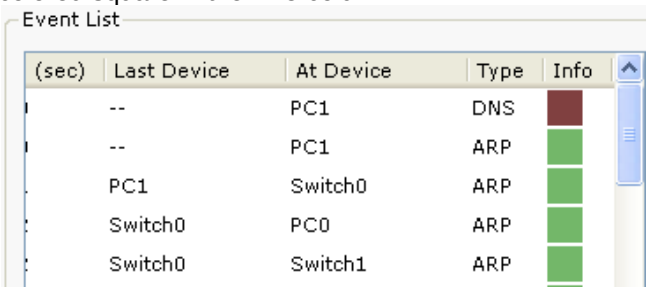
- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser displays a web page appears.

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?

HTTP request packet

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

In inbound PDU details, we see HTTP Response at the end where HTTP request message can be seen.

For packet 2:

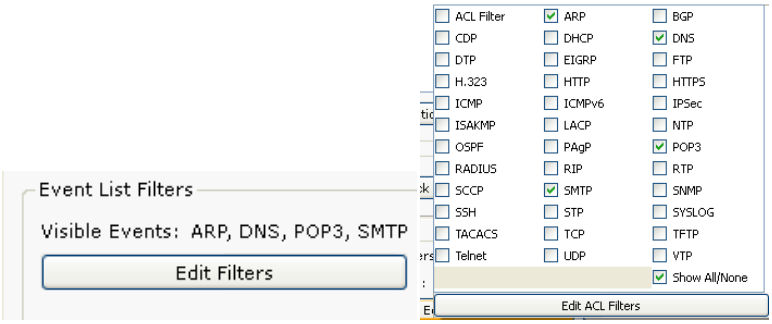
Click onto “Inbound PDU details” tab. Scroll down at the end, what do you see? What kind of HTTP packet is this?

Now, in inbound PDU details, we see HTTP Response at the end where HTTP connection is can be seen. Moreover, content-length and content type is shown as well.

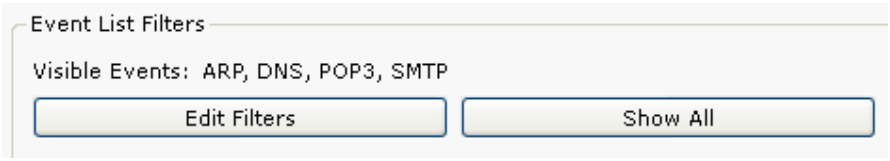
Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.

Step 1 – Run the simulation and capture the traffic.

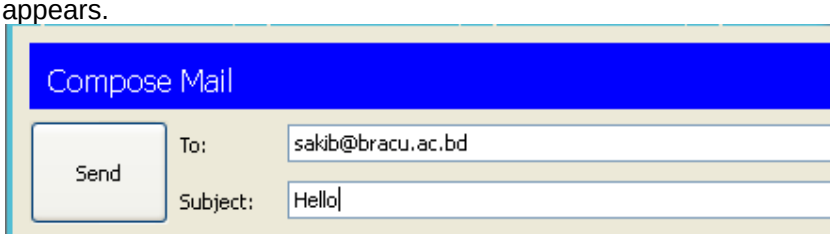
- On the Event List window click “Reset Simulation” button. All previous packets will disappear.
- At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click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

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.

For packet 4::

What is the purpose of this DNS packet?

DNS packet is sent to so that we can get the IP address of the email side server where SMTP Push method will be used.

For packet 5& 6::

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

SMTP is sent to the email server so that the server can get an confirmation that the email was sent. And after getting SMTP, the server reply back. This process mainly happens to get the confirmation.

Step 3 – Run the simulation and capture the traffic for POP.

- 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 – Examine the following captured traffic.

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.

For packet 6::

What is the purpose of this DNS packet?

getting the IP address of the email server.

For packet 7&8::

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

POP packet mainly carries the expected email(i.e.- sakib's) . So, POP packet was sent in email server to get the data of client side email and server sends a POP packet reply with the email data.

Homework Task:

Observe DHCP Traffic and write down the steps for the DHCP process.

- Reset simulation. Change the Event Filter to show **ARP** and **DHCP** only.
- Click to PC2. Go to the **Physical Tab** and turn on the PC by clicking the power button on the CPU shown.
- Then go to the **Desktop Tab** and then to **IP Configuration**. Click DHCP. Wait for a while. Then the IP address and other data will appear in the boxes for this PC.
- **Note:** If the IP addresses do not appear, click the static radio button and again click the dhcp radio button again.