CSE 421

ID: 24241370

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 tightandobservethepacketsflowingthroughthenetwork.

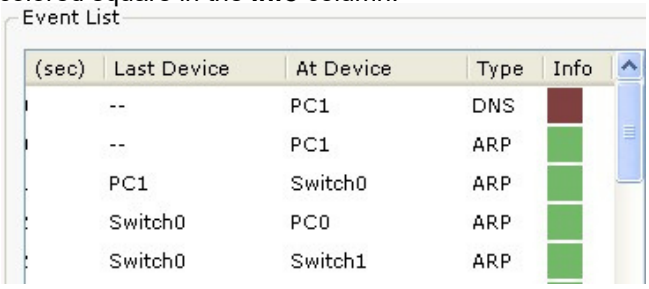
- When the above message appears Click “View Previous Events".
- Click on PC1. The web browser displays a web page appears.

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 onat 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?

This HTTP packet is a request or query packet

SRC IP: 192.168.10.11, DST IP: 192.168.10.3 SEQ NUM: 1, ACKNOWLEDGE NUMBER: 1

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

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?

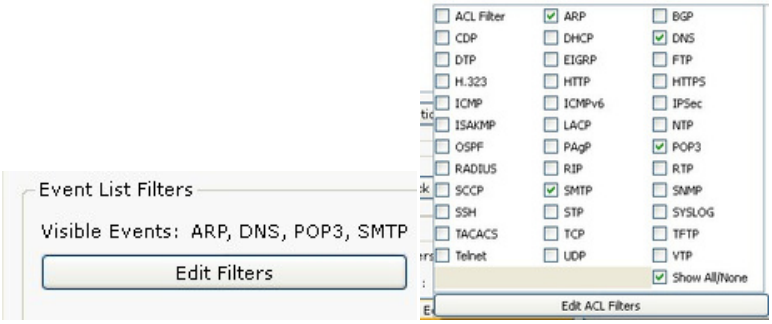
This HTTP packet is a response packet

SRC IP: 192.168.10.3, DST IP: 192.168.10.11 SEQ NUM: 1, ACKNOWLEDGE NUMBER: 105

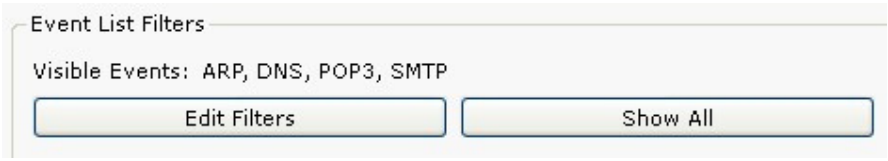
Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.

Step 1 – Run the simulation and capture the traffic.

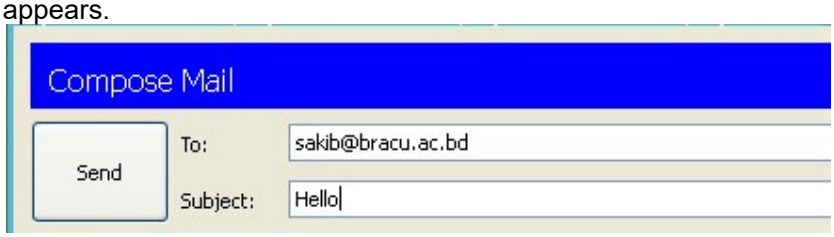
- On the Event List window click “Reset Simulation” button. All previous packets will disappear.
- At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click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



- Click a space anywhere outside the popup window, then it willdisappear.
- 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”, anotherwindow 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	**AtDevice**	**Type**
3.	PC1 PC1 Bracu	Switch 0	DNS
4.	Email Server	Switch 0	SMTP
5.		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?

The purpose of DNS packet is to get the IP address of BRACU email server

For packet 5& 6::

<u>Explain why SMTP</u> packet was sent to the email server and the server replied with an SMTP packet?

Featching the IP address, PC1 sent the email to the email server so that the server could send it to the recevuer and for the same reason, the server replied with an SMTP packet to send the PC0. Becuse push prortocl used by email sending which is SMPT

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	AtDevice	Type
6.	PC1 PC1 Bracu	Switch 0	DNS
7.	Email Server	Switch 0	POP3
8.		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?

PC1 used the DNS packet to get the IP address of the email server. PC0 needs to receive the email and it does not know the IP address of the email server, It will use the DNS packet to get 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?

After receving the IP address PC0 created a POP3 packet and sent it to the email server to ask if there were any possible email that it received and as an email was available for PC0 at the server sent it to PC0 through another POP3 packet