

## 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.

	<b>Last Device</b>	<b>At Device</b>	<b>Type</b>
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.

(sec)	Last Device	At Device	Type	Info
--	PC1	Switch 0	DNS	[Red Square]
--	PC1	Switch 0	ARP	[Green Square]
	PC1	Switch0	ARP	[Green Square]
	Switch0	PC0	ARP	[Green Square]
	Switch0	Switch1	ARP	[Green Square]

- 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?

**Answer:** HTTP request packet

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

**Answer:** SRC IP:192.168.10.3 , DST IP:192.168.10.11  
Source Port: 80, Destination Port: 1025  
Sequence number = 1 and Acknowledge number = 1

HTTP Data:Accept-Language: en-us  
Accept: \*/\*  
Connection: close  
Host:

**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?

**Answer:**

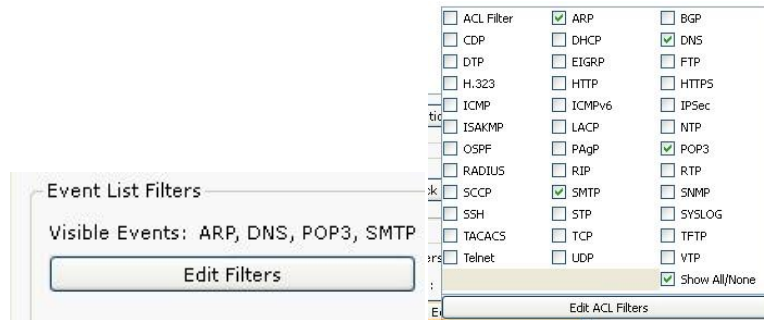
HTTP Data:Connection: close  
Content-Length: 151  
Content-Type: text/html  
Server: PT-Server/5.2

HTTP response packet

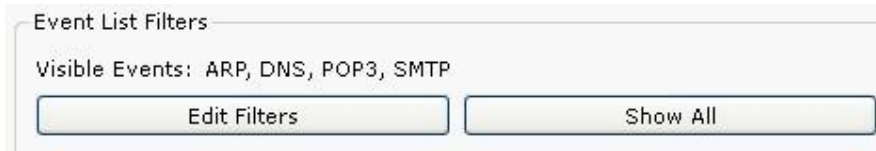
**Task 2: Observe email traffic exchange between a client and email server using SMTP and POP3.**

**Step 1 – Run the simulation and capture the traffic.**

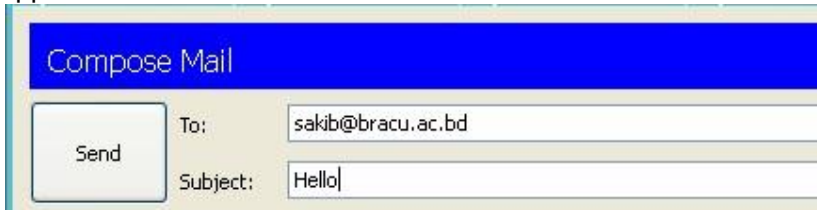
- On the Event List window click “Reset Simulation” button. All previous packets will disappear.
- At the bottom of the Event List window, there is a filter which filters the protocols that we want to see. Click Edit filters. Another window appears showing different protocols, unclick HTTP and click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

**Answer:** The purpose of the DNS packet is to find the Bracu email server’s IP address.

**For packet 5& 6::**

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

**Answer:** PC1 sends an SMTP packet to send the email message to Bracu Email Server, which then responds with an SMTP packet to acknowledge the successful receipt of the email.

**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?

**Answer:** This DNS packet is used to get the IP address of the Bracu Email Server. With this information, PC0 can locate the server to send the POP3 request.

**For packet 7&8::**

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

**Answer:** PC0 sends a POP3 packet to the email server to check for any new incoming emails. In response, the email server sends a POP3 packet containing the requested email data or a message indicating the status of the inbox.