

## Worksheet Experiment 1

Student Name: RAJDEEP JAISWAL

Branch: CSE

Semester: 5<sup>th</sup> Sem

Subject Name: WMS Lab

UID: 20BCS2761

Section/Group: WM\_902/B

Date of Performance: 12<sup>th</sup> Aug, 2022

Subject Code: 20CSP-338

### 1. Aim/Overview of the practical:

Open any website on computer system and identify http packet on monitoring tool like Wireshark.

### 2. Objective:

To analyse http traffic.

### 3. Introduction:

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

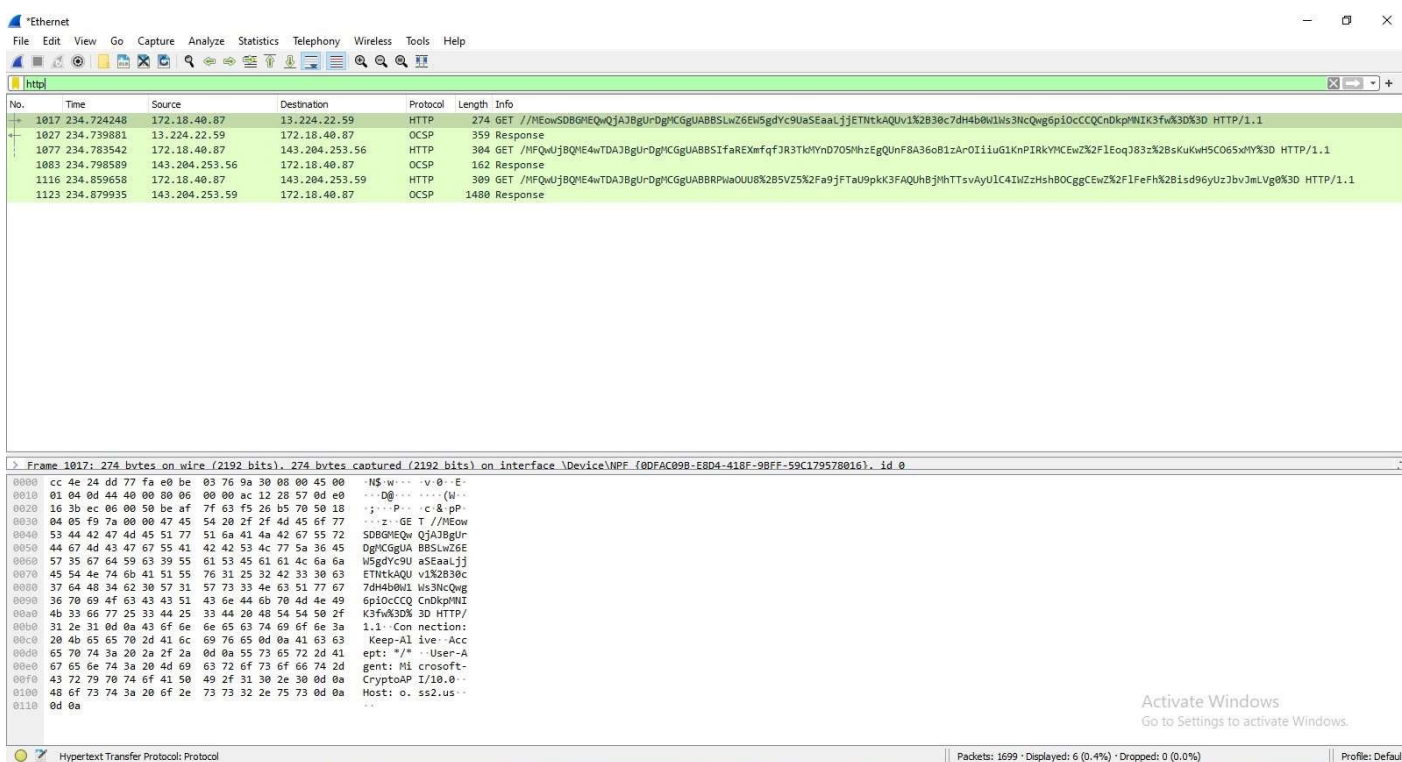
It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

### 4. Steps/Method:

1. Open Wireshark
2. Click on "Capture > Interfaces". A pop-up window will display.
3. You'll start capture traffic that goes through your ethernet driver.

4. Visit the URL that you wanted to capture the traffic from.
5. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
6. After the traffic capture is stopped, please save the captured traffic into a \*.pcap format file and attach it to your support ticket.

## 5. Outcomes:



The screenshot shows the Wireshark interface with a packet capture on the 'Ethernet' interface. The packet list shows several HTTP and OCSP requests and responses. The selected packet (No. 1017) is an HTTP GET request to a specific URL. The packet details pane shows the structure of the HTTP request, including the GET method, the URL, and the 'Host' header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1017	234.724248	172.18.40.87	13.224.22.59	HTTP	274	GET //MEowSDBGMEQwQjA3BgUrDgMCGUA... HTTP/1.1
1027	234.739881	13.224.22.59	172.18.40.87	OCSP	359	Response
1077	234.783542	172.18.40.87	143.204.253.56	HTTP	304	GET /HFQwUjBQME4wTDA3BgUrDgMCGUA... HTTP/1.1
1083	234.798589	143.204.253.56	172.18.40.87	OCSP	162	Response
1116	234.859658	172.18.40.87	143.204.253.59	HTTP	309	GET /HFQwUjBQME4wTDA3BgUrDgMCGUA... HTTP/1.1
1123	234.879935	143.204.253.59	172.18.40.87	OCSP	1488	Response

Frame 1017: 274 bytes on wire (2192 bits), 274 bytes captured (2192 bits) on interface \Device\NPF... id 0

Activate Windows  
Go to Settings to activate Windows.

Profile: Default

Learning outcomes (What I have learnt):

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe single small file (e.g., simple html file) request/response behavior and the request/response behavior for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behavior. Observe request/response behavior for a page that needs authentication.

Evaluation Grid:

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Student Performance (Conduct of experiment) objectives/Outcomes.		12
2.	Viva Voce		10
3.	Submission of Work Sheet (Record)		8
	Total		30