

Register No:	99220040772
Name:	V Vishwaradhya
Class/Section:	9312/S24
Ex.No:	12c
Name of the Experiment	Capture and Analyse HTTP protocol
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1f7XAe6zNuTQ44mz4BRV6XpfhIxyex7-?usp=sharing

1. Visit any one website by opening a browser fill your machine details (attach relevant screenshots).

Parameter	Value
Your Machine IP Address.	10.2.16.28
Your Machine MAC Address	14:d4:24:17:5e:9b
Default Gateway address	10.2.0.1
Website URL	http://testphp.vulnweb.com/login.php
Website IP Address	44.228.249.3

2. Fill the TCP connection segment details:

Field Name	Field Length (no of bits)	Field value
Destination MAC address	48 bits	c8:4f:86:fc:00:10
Source MAC address	48 bits	14:d4:24:17:5e:9b
Destination IP address	32 bits	44.228.249.3
Source IP Address	32 bits	10.2.16.28

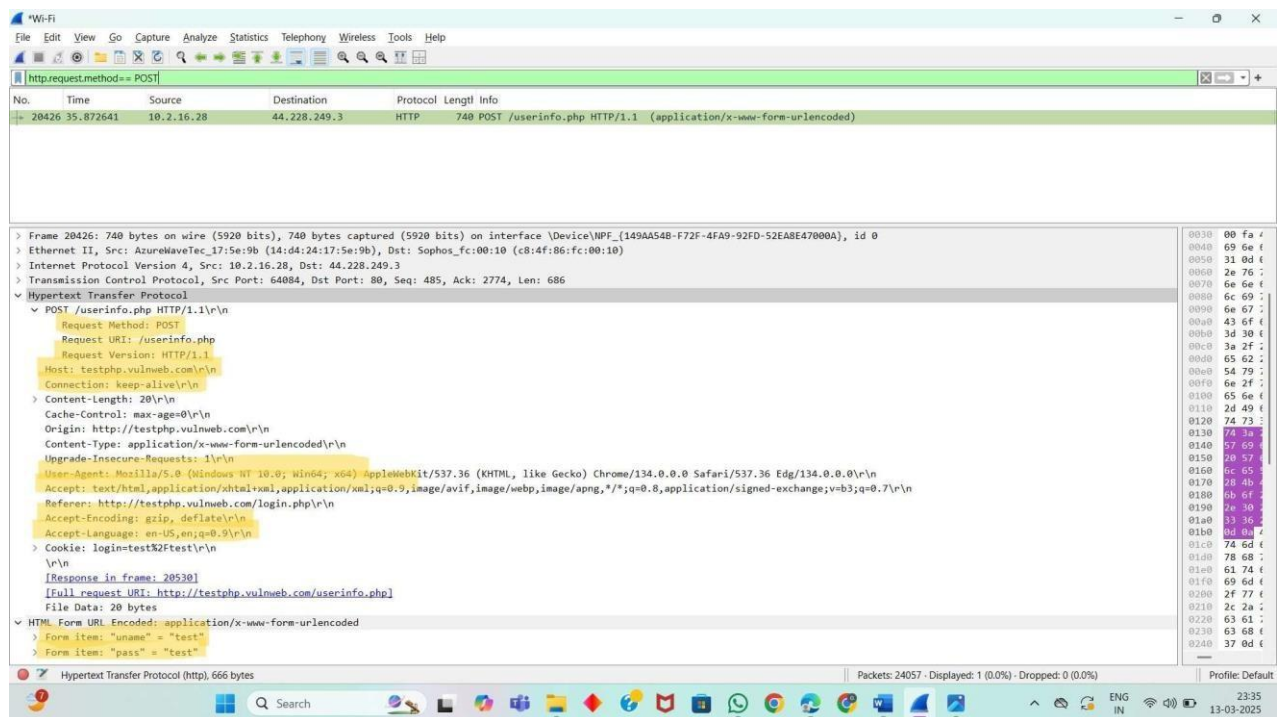
Destination TCP port	16 bits	80
Source TCP port	16 bits	64084

3. HTTP Request Message Details.

Field Name	Field Length (# of Bits)	Field Value (Binary or Hexa value)
Method	Variable (Usually 3 Bytes)	GET (0x474554 in Hex)
Host	Variable	Testphp.vulnweb.com\r\n (Hex: 546573747068702E76756C6E7765622E636F6D0D0A)
Accept	Variable	text/html, application/xhtml+xml
User-Agent	Variable	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Accept-Language	Variable	en-US, en; q=0.9\r\n
Accept-Encoding	Variable	gzip, deflate\r\n
Connection	Variable	Keep-alive\r\n

Paste the HTTP Response Screenshot:

The screenshot displays a Wireshark capture of an HTTP GET request. The packet list at the top shows a GET request from 10.2.16.28 to 23.211.60.112. The packet details pane on the left shows the request structure: GET /login.php HTTP/1.1, Host: testphp.vulnweb.com, Connection: keep-alive, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7, Accept-Encoding: gzip, deflate, Accept-Language: en-US,en;q=0.9, Cookie: login=test123test. The packet bytes pane on the right shows the raw data of the request.



Rubrics for Wireshark labs: (To be Filled by the Class Teacher)

Rubrics	Excellent	Fair	Poor	Marks
Understanding (2)	Understand the Concept very well. (2)	Understand the Concept (1)	Poor Understand the Concept (0)	
Usage of filters (3)	Identified and applied the filter correctly (3)	Identified the filter, but not applied correctly (2-1)	Couldn't identify and apply the filter. Just captured the packets (1)	
Attach relevant Screenshots (3)	clearly Highlighted the answers and attached the screenshots (3)	attached the screenshots, but not highlighted. (2-1)	Did not attach the screenshots (0)	
On time Submission (2)	Early or on time submission (2)	Submitted after deadline (1)	Did not Submit (0)	
Total				