Register No:	**99220040570**
Name:	**K.Hanumaan**
Class/Section:	**8501 A/S06**
Ex.No:	**12**
Name of the Experiment	**Capture and Analyse HTTP packets**
Google Drive link of the packet tracer file **(give view permission):**	https://drive.google.com/drive/folders/1g0GjX7uZsXGddsaleVBZKMTCB5IX-W4z?usp=drive_link

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

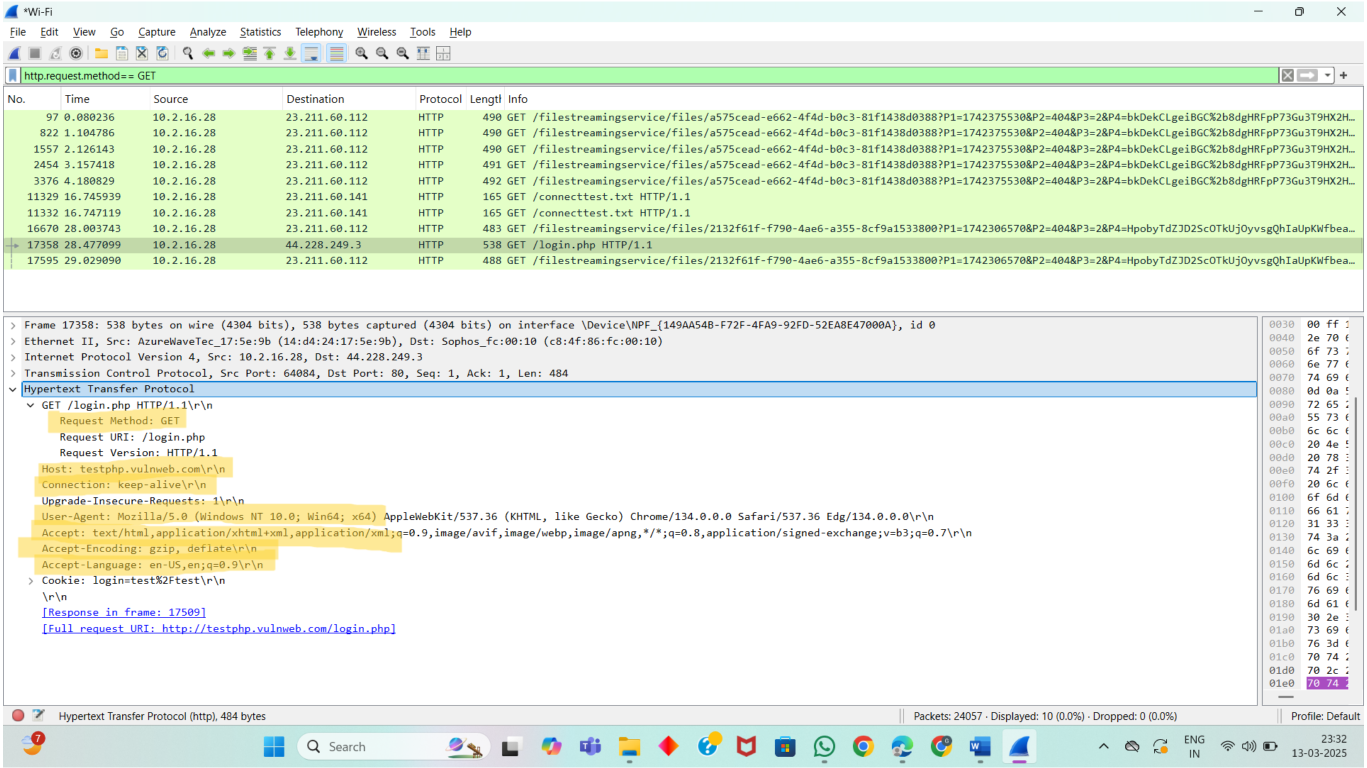
2. Fill the TCP connection segment details:

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:



http.request.method== GET

```
No.    Time       Source        Destination     Protocol Lengtl Info
   97 0.080236    10.2.16.28    23.211.60.112   HTTP     490 GET /filestreamingservice/files/a575cead-e662-4f4d-b0c3-81f1438d0388?P1=1742375530&P2=404&P3=2&P4=bkDekCLgeiBGC%2b8dgHRFpP73Gu3T9HX2H…
  822 1.104786    10.2.16.28    23.211.60.112   HTTP     490 GET /filestreamingservice/files/a575cead-e662-4f4d-b0c3-81f1438d0388?P1=1742375530&P2=404&P3=2&P4=bkDekCLgeiBGC%2b8dgHRFpP73Gu3T9HX2H…
 1557 2.126143    10.2.16.28    23.211.60.112   HTTP     490 GET /filestreamingservice/files/a575cead-e662-4f4d-b0c3-81f1438d0388?P1=1742375530&P2=404&P3=2&P4=bkDekCLgeiBGC%2b8dgHRFpP73Gu3T9HX2H…
 2454 3.157418    10.2.16.28    23.211.60.112   HTTP     491 GET /filestreamingservice/files/a575cead-e662-4f4d-b0c3-81f1438d0388?P1=1742375530&P2=404&P3=2&P4=bkDekCLgeiBGC%2b8dgHRFpP73Gu3T9HX2H…
 3376 4.180829    10.2.16.28    23.211.60.112   HTTP     492 GET /filestreamingservice/files/a575cead-e662-4f4d-b0c3-81f1438d0388?P1=1742375530&P2=404&P3=2&P4=bkDekCLgeiBGC%2b8dgHRFpP73Gu3T9HX2H…
11329 16.745939   10.2.16.28    23.211.60.141   HTTP     165 GET /connecttest.txt HTTP/1.1
11332 16.747119   10.2.16.28    23.211.60.141   HTTP     165 GET /connecttest.txt HTTP/1.1
16670 28.003743   10.2.16.28    23.211.60.112   HTTP     483 GET /filestreamingservice/files/2132f61f-f790-4ae6-a355-8cf9a1533800?P1=1742306570&P2=404&P3=2&P4=HpobyTdZJD2ScOTkUjOyvsgQhIaUpKWfbea…
17358 28.477099   10.2.16.28    44.228.249.3    HTTP     538 GET /login.php HTTP/1.1
17595 29.029090   10.2.16.28    23.211.60.112   HTTP     488 GET /filestreamingservice/files/2132f61f-f790-4ae6-a355-8cf9a1533800?P1=1742306570&P2=404&P3=2&P4=HpobyTdZJD2ScOTkUjOyvsgQhIaUpKWfbea…
```

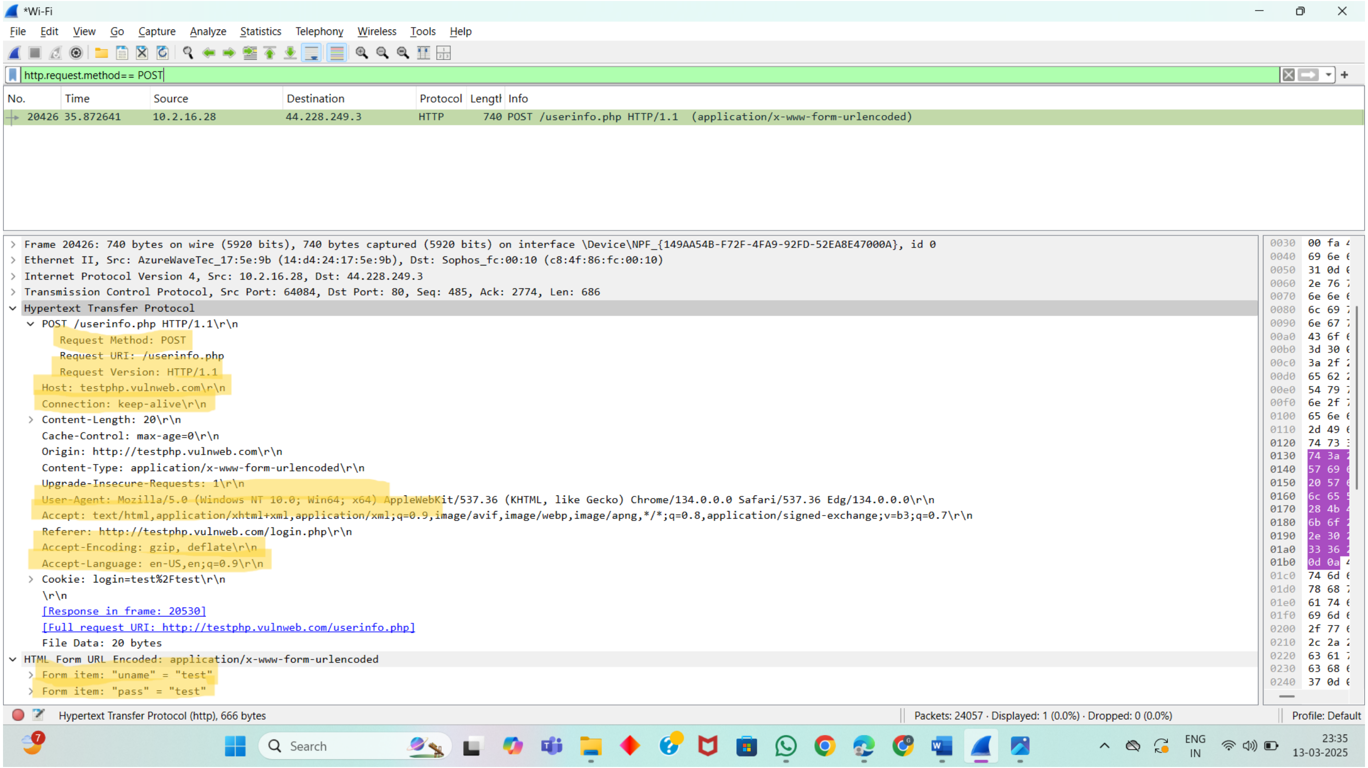
```
> Frame 17358: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EA8E47000A}, id 0
> Ethernet II, Src: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
> Internet Protocol Version 4, Src: 10.2.16.28, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 64084, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
v Hypertext Transfer Protocol
  v GET /login.php HTTP/1.1\r\n
      Request Method: GET
      Request URI: /login.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36 Edg/134.0.0.0\r\n
    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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: login=test%2Ftest\r\n
    \r\n
    [Response in frame: 17509]
    [Full request URI: http://testphp.vulnweb.com/login.php]
```

```
0030  00 ff
0040  2e 70
0050  6f 73
0060  6e 77
0070  74 69
0080  0d 0a
0090  72 65
00a0  55 73
00b0  6c 6c
00c0  20 4e
00d0  20 78
00e0  74 2f
00f0  20 6c
0100  6f 6d
0110  66 61
0120  31 33
0130  74 3a
0140  6c 69
0150  6d 6c
0160  6d 6c
0170  76 69
0180  6d 61
0190  30 2e
01a0  73 69
01b0  76 3d
01c0  70 74
01d0  70 2c
01e0  70 74
```

Hypertext Transfer Protocol (http), 484 bytes

Packets: 24057 · Displayed: 10 (0.0%) · Dropped: 0 (0.0%)

Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Search
ENG IN
23:35
13-03-2025

```
http.request.method== POST

No.   Time       Source      Destination   Protocol Lengtl Info
20426 35.872641  10.2.16.28  44.228.249.3  HTTP        740 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)

> Frame 20426: 740 bytes on wire (5920 bits), 740 bytes captured (5920 bits) on interface \Device\NPF_{149AA54B-F72F-4FA9-92FD-52EA8E47000A}, id 0
> Ethernet II, Src: AzureWaveTec_17:5e:9b (14:d4:24:17:5e:9b), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
> Internet Protocol Version 4, Src: 10.2.16.28, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 64084, Dst Port: 80, Seq: 485, Ack: 2774, Len: 686
v Hypertext Transfer Protocol
  v POST /userinfo.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
  > Content-Length: 20\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36 Edg/134.0.0.0\r\n
    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\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: login=test%2Ftest\r\n
    \r\n
    [Response in frame: 20530]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 20 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "test"
  > Form item: "pass" = "test"

0030  00 fa
0040  69 6e
0050  31 0d
0060  2e 76
0070  6e 6e
0080  6c 69
0090  6e 67
00a0  43 6f
00b0  3d 30
00c0  3a 2f
00d0  65 62
00e0  54 79
00f0  6e 2f
0100  65 6e
0110  2d 49
0120  74 73
0130  74 3a
0140  57 69
0150  20 57
0160  6c 65
0170  28 4b
0180  6b 6f
0190  2e 30
01a0  33 36
01b0  0d 0a
01c0  74 6d
01d0  78 68
01e0  61 74
01f0  69 6d
0200  2f 77
0210  2c 2a
0220  63 61
0230  63 68
0240  37 0d

Hypertext Transfer Protocol (http), 666 bytes    Packets: 24057 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Paste the Wireshark File with view permission:

Google Drive Link:https://drive.google.com/drive/folders/1g0GjX7uZsXGddsaleVBZKMTCB5IXW4z?usp=drive_link

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				

Result: Thus the Capture and analyse HTTP packets has been implemented and it was successfully verified.