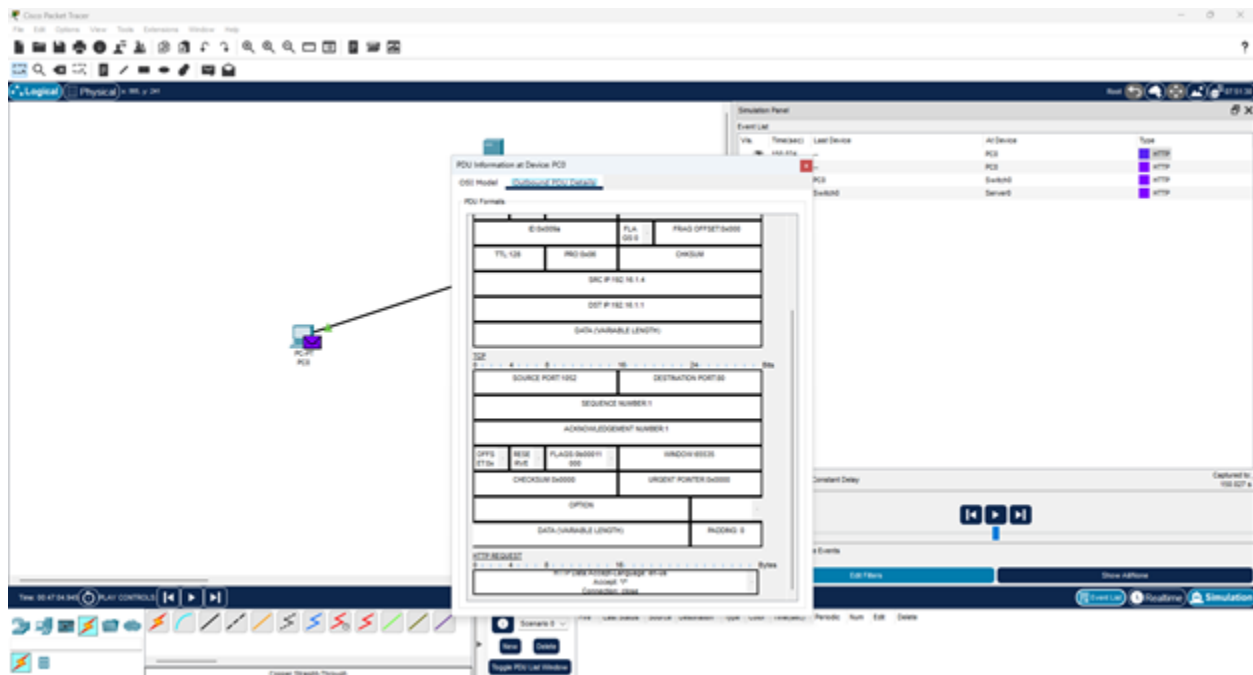


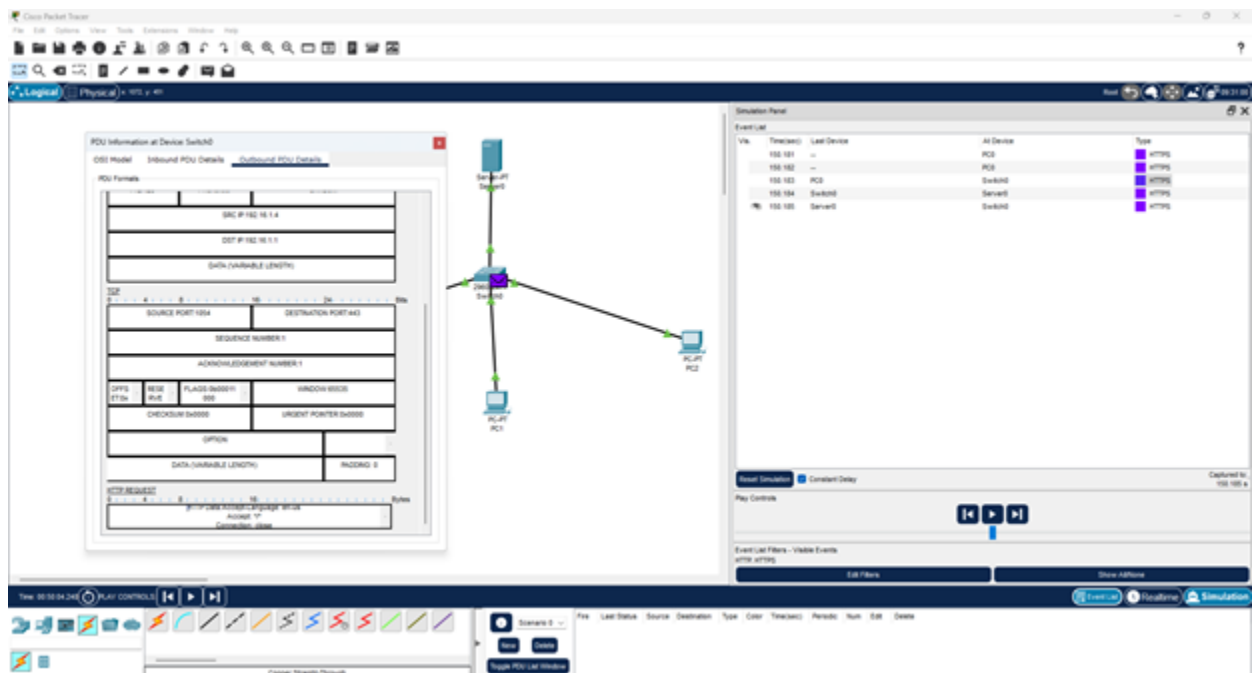
CN Lab 04

Class Activity 1:

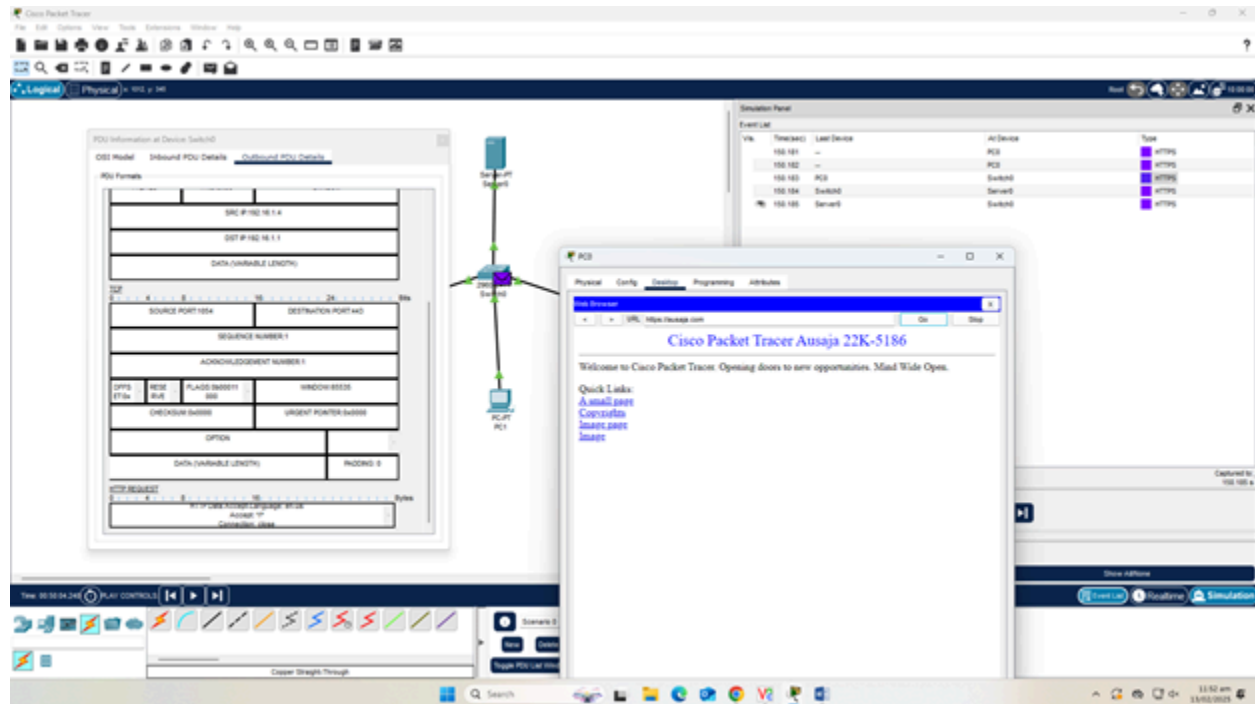
- For HTTP:



- For HTTPS:

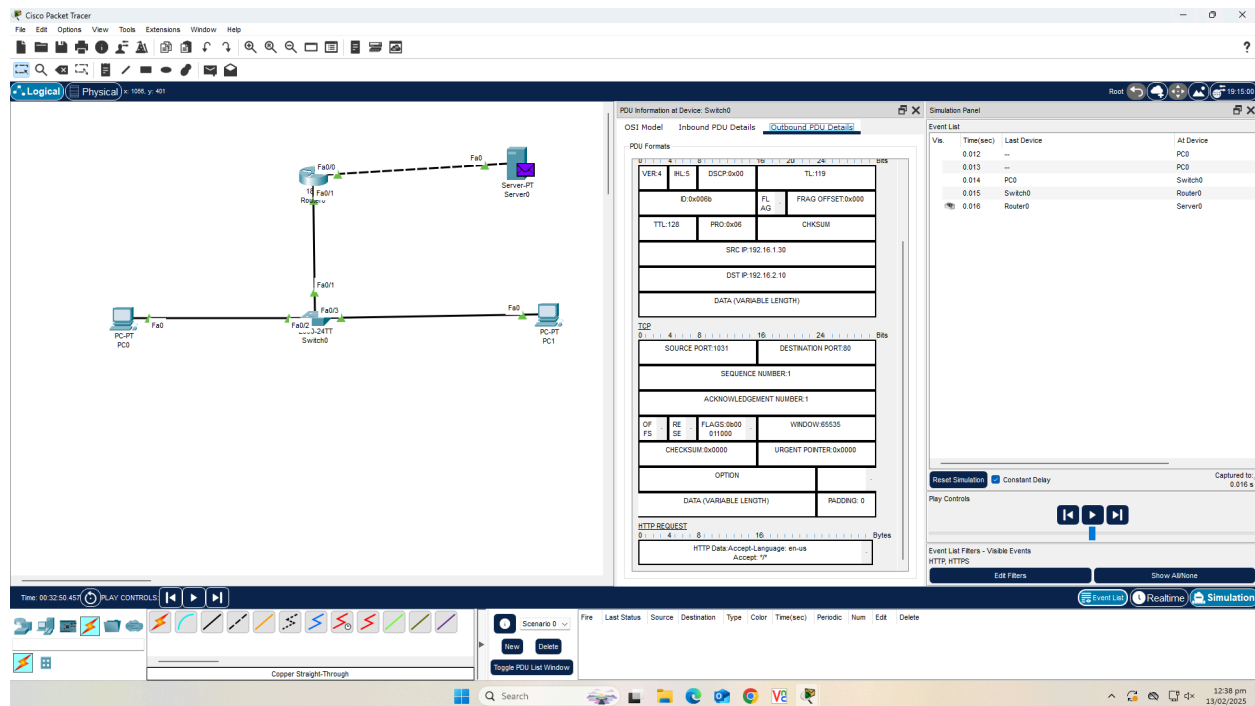


- For DNS:



Class Activity 2:

- For HTTP:



Class Activity:

- For HTTP:

The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a packet of 1342 bytes from 172.16.22.27 to 172.16.22.27. The packet details pane shows the following structure:

- Frame 1243: 702 bytes on wire (5616 bits), 702 bytes captured (5616 bits) on interface vDevice\VPF_{E829178A-D4FB-BA2A-3B2FE61E9}
- Ethernet II, Src: Dell_a1a1a0d (20:88:18:a1a1a0d), Dst: Cisco_45a7a76 (cc:98:91:45:a7:76)
- Internet Protocol Version 4, Src: 172.16.22.27, Dst: 172.16.22.27
- Transmission Control Protocol, Src Port: 54909, Dst Port: 80, Seq: 1204, Len: 640
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
- Form Name: "uname" = "Ausaja"
- Form Name: "pass" = "11234"

The packet bytes pane shows the raw data of the HTTP request, including the GET method, the URL, and the form data.

- For HTTPS (via SSL/TLS):

The image shows a Wireshark packet capture of an HTTPS (SSL/TLS) handshake. The packet list on the left shows a packet of 2550 bytes from 172.16.22.27 to 172.16.22.27. The packet details pane shows the following structure:

- Frame 23: 2550 bytes on wire (20400 bits), 2550 bytes captured (20400 bits) on interface vDevice\VPF_{E829178A-D4FB-BA2A-3B2FE61E9}
- Ethernet II, Src: Dell_a1a1a0d (20:88:18:a1a1a0d), Dst: Cisco_45a7a76 (cc:98:91:45:a7:76)
- Internet Protocol Version 4, Src: 172.16.22.27, Dst: 172.16.22.27
- Transmission Control Protocol, Src Port: 54909, Dst Port: 443, Seq: 1, Ack: 1, Len: 2496
- Transport Layer Security
- TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
- Content Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 2491
- [Encrypted Application Data [truncated]]: 75ee8faaffefcdeba3435e72aec8b54348ac7b6933de93f5896481e69a563dc374954cb44dd677724a
- [Application Data Protocol: Hypertext Transfer Protocol]

The packet bytes pane shows the raw data of the TLS record, including the TLS version, content type, and the encrypted application data.

Task 1:**Part 1:**

The screenshot shows the Cisco Packet Tracer interface. On the left, a network topology is visible with a central switch connected to several PCs and servers. The main window displays the 'PDU Information at Device: Switch' for an inbound PDU. The PDU is an HTTP request from PC0 (192.168.1.2) to the switch (192.168.1.1). The packet details are as follows:

OSI Model	
Version: 4	Protocol: 60
Length: 128	Flags: 0x00
Source Port: 1028	Destination Port: 80
Sequence Number: 1	Acknowledgement Number: 1
Offset: 0	Window: 65535
Checksum: 0x0000	Urgent Pointer: 0x0000
Data: HTTP Data Accept-Language: en-us Accept: */*	

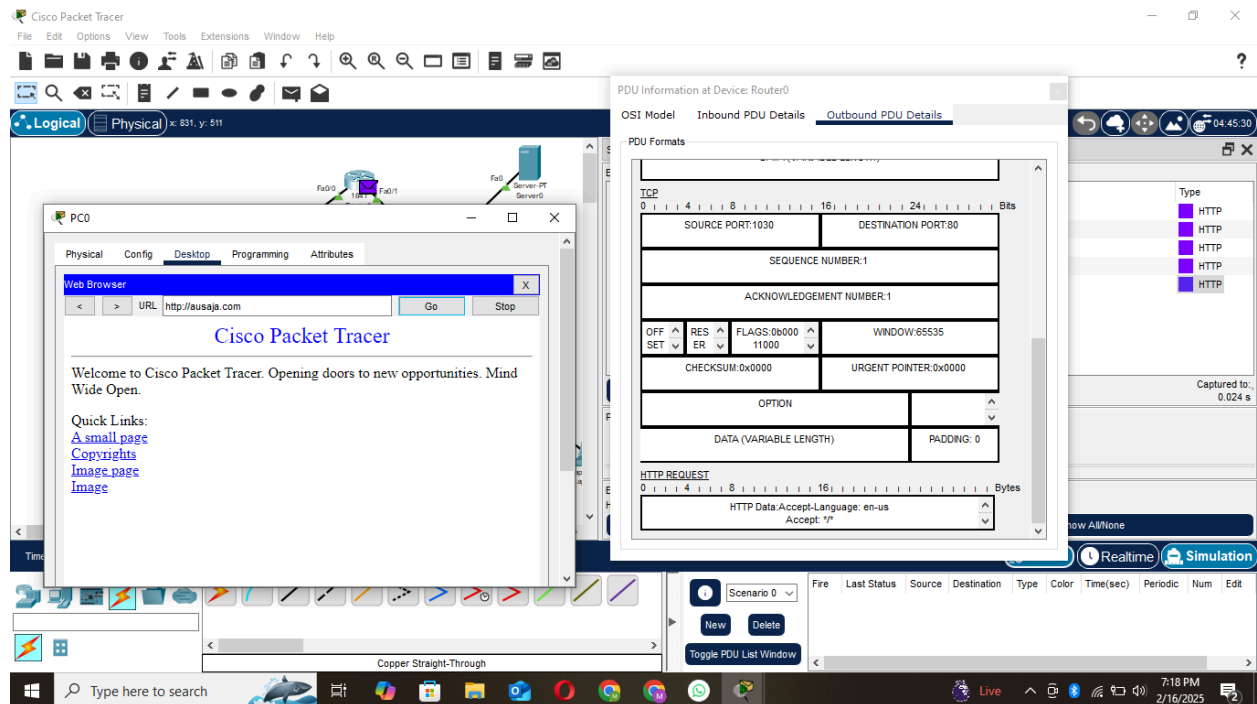
The Event List on the right shows the packet capture at the switch. The PC0 window shows a web browser with the URL 'http://ausaja.com'.

Part 2:

The screenshot shows the Cisco Packet Tracer interface. On the left, a network topology is visible with a central switch connected to several PCs and servers. The main window displays the 'PDU Information at Device: PC0' for an outbound PDU. The PDU is an HTTP request from PC0 (192.168.1.2) to the switch (192.168.1.1). The packet details are as follows:

OSI Model	
Version: 4	Protocol: 60
Length: 128	Flags: 0x00
Source Port: 1028	Destination Port: 80
Sequence Number: 1	Acknowledgement Number: 1
Offset: 0	Window: 65535
Checksum: 0x0000	Urgent Pointer: 0x0000
Data: HTTP Data Accept-Language: en-us Accept: */*	

The Event List on the right shows the packet capture at PC0. The PC0 window shows a web browser with the URL 'http://ausaja.com'.

Task 2:

1.

Age Header: describes how long a response has been cached since it was retrieved from the server.

Expires Header: describes when cached information should not be used (i.e. will become old)

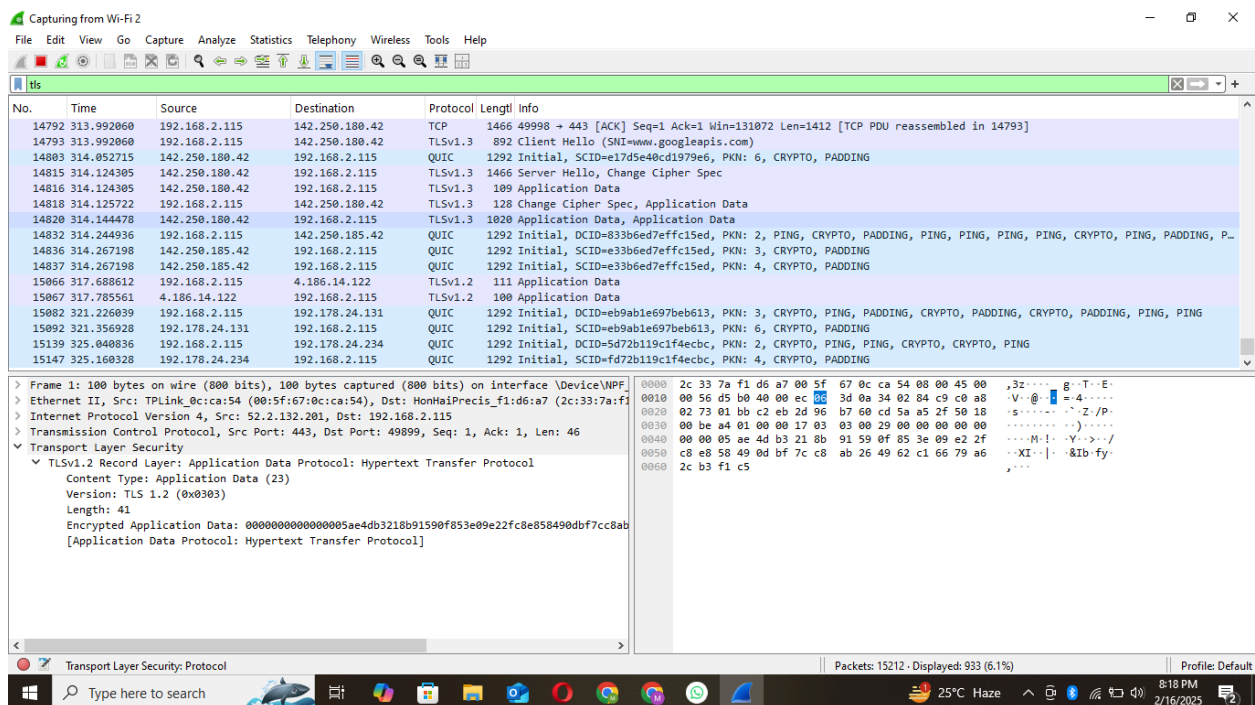
2. Four groupings of HTTP Headers:

- **General Headers:** provides general information about the request.
- **Request Headers:** provides additional information about the request.
- **Response Headers:** provides metadata about the response, and is usually sent by the server.
- **Entity Headers:** provides information about the body of the message.

Wireshark Lab Exercise:

1.

Logging in <http://testphp.vulnweb.com/>. It encrypts the data, and is secure.



2.

HTTP: The data remains unencrypted, and can be easily read by anyone. Hence, making it less secure.

The image shows a Wireshark packet capture of HTTP traffic. The top pane displays a list of packets, with packet 20535 selected. The middle pane shows the details of the selected packet, which is an HTTP POST request to /userinfo.php. The bottom pane shows the raw data of the packet, which is the HTML form URL encoded data. The form contains the fields 'uname' and 'pass', both with the value 'test'.

No.	Time	Source	Destination	Protocol	Length	Info
18437	432.119795	192.168.2.115	192.168.2.115	HTTP	165	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
18439	432.146644	192.168.2.115	192.168.2.115	HTTP	303	GET /c/msdownload/update/others/2025/02/42835581_a12f68d2e580456b12d5e0cc6a8732c35e8e627d.cab HTTP/1.1
18456	432.407351	192.168.2.115	192.168.2.115	HTTP	303	GET /c/msdownload/update/others/2025/02/42835860_bfaf69a420a5cdfd22c72ba0868963aeca4b7666.cab HTTP/1.1
18482	432.576306	192.168.2.115	192.168.2.115	HTTP	879	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
18484	432.578063	192.168.2.115	192.168.2.115	HTTP	303	GET /c/msdownload/update/others/2025/02/42835681_3fcl95f3d58a0d64a1b3bd62eb5589e89857eb.cab HTTP/1.1
18512	432.750266	192.168.2.115	192.168.2.115	HTTP	876	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
18566	433.556302	192.168.2.115	44.228.249.3	HTTP	738	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
18592	433.824015	44.228.249.3	192.168.2.115	HTTP	93	HTTP/1.1 200 OK (text/html)
18973	437.580702	192.168.2.115	58.65.192.225	HTTP	420	GET /d/msdownload/update/software/defu/2025/02/am_delta_patch_1.421.1925.0_bb13a8f8f0998ff1a573b724f28700a73730.. HTTP/1.1
18976	437.850631	58.65.192.225	192.168.2.115	HTTP	568	HTTP/1.1 206 Partial Content
18977	437.852554	192.168.2.115	58.65.192.225	HTTP	425	GET /d/msdownload/update/software/defu/2025/02/am_delta_patch_1.421.1925.0_bb13a8f8f0998ff1a573b724f28700a73730.. HTTP/1.1
19478	451.422729	58.65.192.225	192.168.2.115	HTTP	1488	HTTP/1.1 206 Partial Content
20044	489.968111	192.168.2.115	44.228.249.3	HTTP	609	GET /login.php HTTP/1.1
20048	490.255168	44.228.249.3	192.168.2.115	HTTP	1387	HTTP/1.1 200 OK (text/html)
20535	516.193873	192.168.2.115	44.228.249.3	HTTP	738	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
20539	516.462248	44.228.249.3	192.168.2.115	HTTP	93	HTTP/1.1 200 OK (text/html)

Frame 20535: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits) on interface \Device\NPF{...} Ethernet II, Src: HonHaiPrecis_f1:d6:a7 (2c:33:7a:f1:d6:a7), Dst: TPLink_0c:ca:54 (08:5f:67:00:0c:ca:54) Internet Protocol Version 4, Src: 192.168.2.115, Dst: 44.228.249.3 Transmission Control Protocol, Src Port: 50004, Dst Port: 80, Seq: 1240, Ack: 5693, Len: 684 Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "uname" = "test"
- Form item: "pass" = "test"

Raw data: 01b0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,application/x-www-form-urlencoded; charset=UTF-8

HTTPS: The data is encrypted, and cannot be read easily. Hence, making it more secure.

The image shows a Wireshark packet capture of HTTPS traffic. The top pane displays a list of packets, with packet 20527 selected. The middle pane shows the details of the selected packet, which is a TLSv1.3 Record Layer. The bottom pane shows the raw data of the packet, which is the encrypted application data. The data is encrypted using TLSv1.3 and is not readable.

No.	Time	Source	Destination	Protocol	Length	Info
35960	705.846263	157.240.227.60	192.168.2.115	TLSv1.3	153	Application Data
35961	705.874731	23.158.56.120	192.168.2.115	BT-DHT	187	Announce_peer Info_hash=281170f0023a63d8bdc83a4bf7191396cc97f3b
35962	705.874999	192.168.2.115	23.158.56.120	BT-DHT	112	Response
35963	705.896936	192.168.2.115	157.240.227.60	TCP	54	50031 → 443 [ACK] Seq=275932 Ack=1732714 Win=131072 Len=0
35964	706.064762	192.168.2.115	54.226.184.164	TLSv1.2	196	Application Data
35965	706.129867	192.168.2.115	157.240.227.60	TLSv1.3	202	Application Data
35966	706.151694	157.240.227.60	192.168.2.115	TCP	54	443 → 50031 [ACK] Seq=1732714 Ack=276080 Win=399104 Len=0
35967	706.264067	54.226.184.164	192.168.2.115	TLSv1.2	157	Application Data
35968	706.275188	192.168.2.115	157.240.227.60	TLSv1.3	203	Application Data
35969	706.296161	157.240.227.60	192.168.2.115	TCP	54	443 → 50031 [ACK] Seq=1732714 Ack=276229 Win=399104 Len=0
35970	706.308692	192.168.2.115	54.226.184.164	TCP	54	49927 → 443 [ACK] Seq=7247 Ack=79855 Win=132352 Len=0
35971	706.339563	157.240.227.60	192.168.2.115	TLSv1.3	152	Application Data
35972	706.386667	192.168.2.115	157.240.227.60	TCP	54	50031 → 443 [ACK] Seq=276229 Ack=1732812 Win=130816 Len=0
35973	706.398448	185.236.203.100	192.168.2.115	BT-DHT	159	Get_peers Info_hash=28160044a1d47f8dc22ed4ebda92c09c582ba1c
35974	706.398820	192.168.2.115	185.236.203.100	BT-DHT	361	Response Nodes=8
35975	706.481363	157.240.227.60	192.168.2.115	TLSv1.3	153	Application Data

Frame 20527: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF{...} Ethernet II, Src: HonHaiPrecis_f1:d6:a7 (2c:33:7a:f1:d6:a7), Dst: TPLink_0c:ca:54 (08:5f:67:00:0c:ca:54) Internet Protocol Version 4, Src: 192.168.2.115, Dst: 3.161.104.31 Transmission Control Protocol, Src Port: 50025, Dst Port: 443, Seq: 3452, Ack: 874, Len: 31 Transport Layer Security

TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

- Opaque Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 26
- Encrypted Application Data: d6c9c8c18fda21effac092fe8f00e9791103a9310611c9470ce [Application Data Protocol: Hypertext Transfer Protocol]

Raw data: 0000 00 5f 67 0c ca 54 2c 33 7a f1 d6 a7 00 00 45 00 .G.T,3 z.....E-
0010 00 47 02 68 40 00 00 06 c9 6d c0 a0 02 73 03 a1 6.h.....m.s.s..
0020 68 f1 c3 69 01 bb 25 44 0c 7c 2e fc 1f 75 50 18 h.....ND.....uP
0030 02 02 f0 b5 00 00 17 03 03 00 1a d6 c9 c8 c1 8f
0040 da 21 ef fa c0 92 fe 8f 00 e9 97 91 10 3a 93 10
0050 61 1c 94 70 ce a.p.