

<b>CS471 – Web Technologies (Laboratory)</b>		<b>Lab 1</b>  <b>The Internet Protocols</b>
--	--	---

This lab session covers the usage of the Wireshark application to monitor and capture the outgoing and incoming packets from a network connection (WIFI, ethernet, etc.). Specifically, students should be able to analyze HTTP, HTTPS, TCP/IP, and UDP protocols using Wireshark, a network protocol analyzer, and draw conclusions.

### Pre-lab Preparation:

1. Review the basics and the structure of HTTP, TCP/IP, and UDP protocols,
2. Install Wireshark and ensure it is running on your computer,
3. Create an online, *publically accessible* Git repository to host and upload your work in the labs. We recommend you use GitHub or GitLab.

### Lab Activities:

#### Part 1: Capturing HTTP Traffic.

##### Task 1: Start Wireshark and capture packets.

- Step 1: Open Wireshark.
- Step 2: Select the network interface connected to the internet (e.g., Ethernet or Wi-Fi).
- Step 3: Click the "Start Capturing Packets" button (the shark fin icon).
- Step 4: Open your favorite web browser and navigate to (<http://neverssl.com/>) website.
- Step 5: After the website has fully loaded, stop capturing packets by clicking the red stop button in Wireshark.

##### Task 2: Filter HTTP packets and analyze them.

- Step 1: In the filter bar, type http and press Enter. This filters out only the HTTP packets from the capture.
- Step 2: Select any HTTP packet to view its details.
- Step 3: Observe the HTTP request and response messages. Note the method (GET, POST), URL, response codes (200 OK, 404 Not Found), etc.

#### Part 2: Analyzing TCP/IP Traffic.

##### Task 1: Filter TCP packets

- Step 1:** Clear the previous filter and type TCP to focus on TCP packets.
- Step 2:** Select a TCP packet related to your HTTP request/response.
- Step 3:** Right-click on the packet and select "Follow" -> "TCP Stream".
- Step 4:** This shows the entire conversation between the client and server.

##### Task 2: Analyze TCP handshake and investigate Data Transfer and Termination

- Step 1:** Find and select packets related to the TCP three-way handshake:
- SYN: Initiates a connection.
  - SYN-ACK: Acknowledges and responds to the SYN.
  - ACK: Acknowledges the SYN-ACK and establishes the connection.
- Step 2:** Note the sequence and acknowledgment numbers. Screenshot and upload your image to your online git repository.
- Step 3:** Observe the data packets exchanged between the client and server. Take a screenshot and upload it to your online git repo.
- Step 4:** Look at the TCP termination process (FIN, ACK packets).

### Part 3: Capturing and Analyzing UDP Traffic

#### Task 1: Generate UDP traffic and capture packets

**Step 1:** Open a network application that uses UDP (e.g., streaming video, VoIP software, or custom script).

**Step 2:** Start the application to generate UDP traffic.

**Step 3:** Start capturing packets in Wireshark while the UDP application is running.

**Step 4:** After sufficient traffic is generated, stop capturing packets.

#### Task 2: Filter and analysis UDP Packets

**Step 1:** In the filter bar, type UDP and press Enter.

**Step 2:** This filters out only the UDP packets from the capture.

**Step 3:** Select any UDP packet to view its details.

**Step 4:** Observe the source and destination ports, length, and data.

**Step 5:** Compare the simplicity of UDP headers with TCP headers.

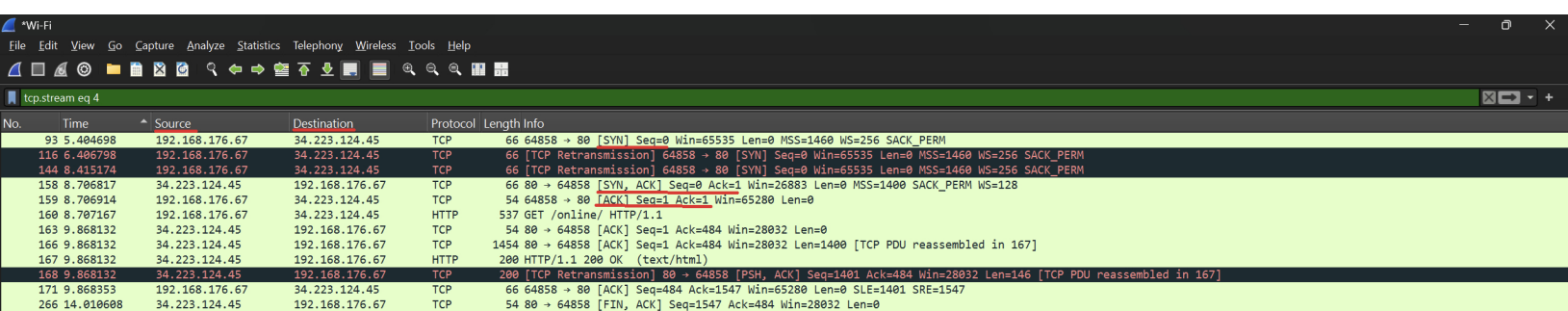
### Part 4: Comparing TCP and UDP by filling in the following tables. Save your work (e.g., in an MS Word document), and upload it to your online git repo.

#### Task 1: Fill in the following table and provide reasons.

	TCP or UDP	Reasons
Reliability and Connection Establishment	TCP	It's more reliable because it uses Three-Way Handshake. Also, if a packet is lost, it will resend it.
Data Integrity and Ordering	TCP	It uses sequence numbers which ensures integrity, and it delivers data in order

#### Task 2: Identify the use Cases and Performance of TCP and UDP.

	TCP	UDP
Use cases	Web Browsing using (HTTP/HTTPS)	Video Streaming
Performance	Higher latency (slower) due to reliability, order guarantees	Lower latency (faster) but packets may lost or disorder possible.



No.	Time	Source	Destination	Protocol	Length	Info
93	5.404698	192.168.176.67	34.223.124.45	TCP	66	64858 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
116	6.406798	192.168.176.67	34.223.124.45	TCP	66	[TCP Retransmission] 64858 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
144	8.415174	192.168.176.67	34.223.124.45	TCP	66	[TCP Retransmission] 64858 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
158	8.706817	34.223.124.45	192.168.176.67	TCP	66	80 → 64858 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1400 SACK_PERM WS=128
159	8.706914	192.168.176.67	34.223.124.45	TCP	54	64858 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
160	8.707167	192.168.176.67	34.223.124.45	HTTP	537	GET /online/ HTTP/1.1
163	9.868132	34.223.124.45	192.168.176.67	TCP	54	80 → 64858 [ACK] Seq=1 Ack=484 Win=28032 Len=0
166	9.868132	34.223.124.45	192.168.176.67	TCP	1454	80 → 64858 [ACK] Seq=1 Ack=484 Win=28032 Len=1400 [TCP PDU reassembled in 167]
167	9.868132	34.223.124.45	192.168.176.67	HTTP	200	HTTP/1.1 200 OK (text/html)
168	9.868132	34.223.124.45	192.168.176.67	TCP	200	[TCP Retransmission] 80 → 64858 [PSH, ACK] Seq=1401 Ack=484 Win=28032 Len=146 [TCP PDU reassembled in 167]
171	9.868353	192.168.176.67	34.223.124.45	TCP	66	64858 → 80 [ACK] Seq=484 Ack=1547 Win=65280 Len=0 SLE=1401 SRE=1547
266	14.010608	34.223.124.45	192.168.176.67	TCP	54	80 → 64858 [FIN, ACK] Seq=1547 Ack=484 Win=28032 Len=0