

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 (<https://qu.edu.sa>) website.

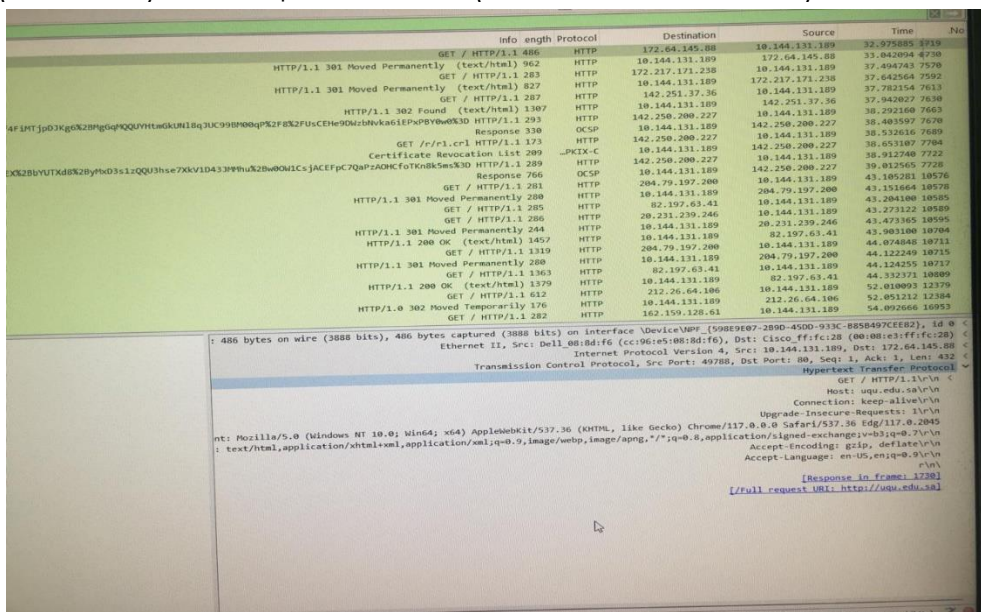
Step 5: After the website has fully loaded, stop capturing packets by clicking the red stop button in Wireshark.

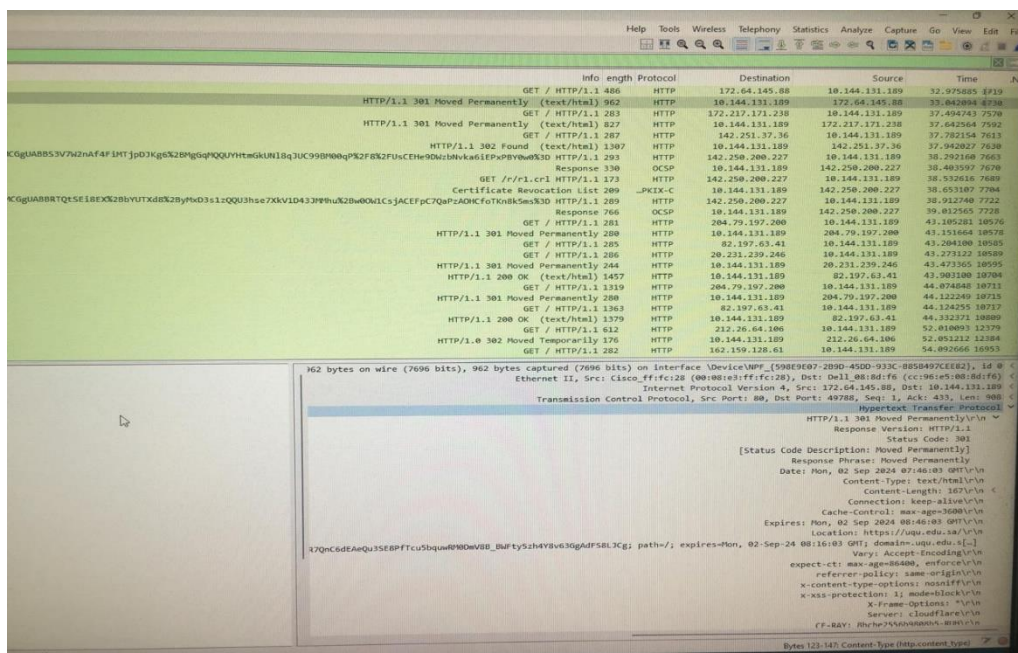
Task 2: Filter HTTP packets and analyze them.

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.

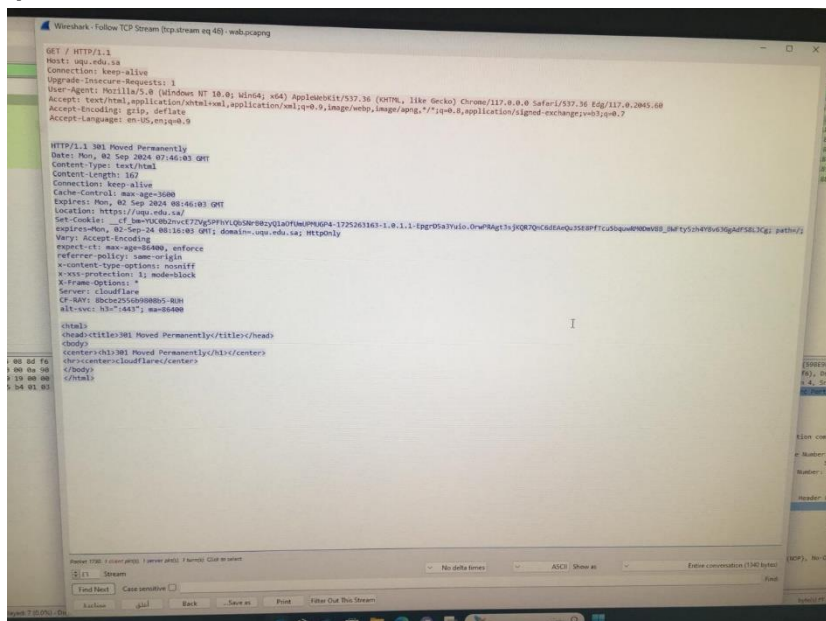
Task 1: Filter TCP packets

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 4: Look at the TCP termination process (FIN, ACK packets).

	Info	Length	Protocol	Destination	Source	Time
Seq=8988 ACK=11848 Win=131328 Len=0	[ACK] 443 > 49785 54	TCP	10.144.131.189	51.137.3.145	28.634315 1663	
	Application Data 990	TLSv1.3	10.144.131.189	51.137.3.145	28.634342 1664	
	Application Data 572	TLSv1.2	10.144.131.189	284.79.197.239	28.680435 1665	
	Application Data 92	TLSv1.2	10.144.131.189	284.79.197.239	28.680435 1666	
Seq=2557 ACK=8729 Win=131328 Len=0	[ACK] 443 > 49784 54	TCP	284.79.197.239	10.144.131.189	28.680440 1667	
	Application Data 137	TLSv1.3	28.189.173.25	10.144.131.189	28.695515 1668	
	Application Data 1892	TLSv1.3	28.189.173.25	10.144.131.189	28.695574 1669	
Seq=7476 ACK=7723 Win=4193280 Len=0	[ACK] 49780 > 443 60	TCP	10.144.131.189	28.189.173.25	30.772514 1670	
	Application Data 86	TLSv1.3	10.144.131.189	28.189.173.25	30.772514 1671	
Seq=7723 ACK=7508 Win=131328 Len=0	[ACK] 443 > 49780 54	TCP	28.189.173.25	10.144.131.189	30.826496 1672	
	Application Data 155	TLSv1.3	28.189.173.25	10.144.131.189	31.018014 1674	
	Application Data 155	TCP	28.189.173.25	10.144.131.189	31.018014 1687	
Seq=7723 ACK=7609 Win=131328 Len=0	[ACK] 443 > 49780 54	TCP	28.189.173.25	10.144.131.189	32.791423 1690	
Seq=0 Min=64240 Len=0 MSS=1460 MSO=256 SACK_PERM [SYN] 00 > 49780 60	[ACK] 443 > 49780 54	TCP	10.144.131.189	10.144.131.189	32.820549 1711	
Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=0 B192 [SYN, ACK] 49788 > 80 66	[ACK] 49788 > 80 66	TCP	10.144.131.189	172.64.145.88	32.820549 1711	
Seq=0 Ack=1 Win=131328 Len=0 MSS=1400 SACK_PERM=0 B192 [ACK] 80 > 49780 54	[ACK] 80 > 49780 54	TCP	172.64.145.88	10.144.131.189	32.820549 1712	
Seq=0 Min=64240 Len=0 MSS=1400 MSO=256 SACK_PERM [SYN] 443 > 49780 60	[ACK] 443 > 49780 54	TCP	10.144.131.189	10.144.131.189	32.820538 1713	
Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM=0 B192 [SYN, ACK] 49788 > 443 66	[ACK] 49788 > 443 66	TCP	10.144.131.189	10.144.131.189	32.820538 1714	
Seq=1 Ack=1 Win=131328 Len=0 [ACK] 443 > 49780 54	[ACK] 443 > 49780 54	TCP	10.144.131.189	10.144.131.189	32.820538 1715	
Client Hello (SHA256-dllupdate.dell.com) 230	TLSv1.2	10.144.131.189	10.144.131.189	32.986192 1716		
Seq=0 Min=64240 Len=0 MSS=1460 MSO=256 SACK_PERM [SYN] 80 > 49780 66	GET / HTTP/1.1 406	HTTP	172.64.145.88	10.144.131.189	32.979771 1719	
Seq=0 Min=64240 Len=0 MSS=1460 MSO=256 SACK_PERM [SYN] 80 > 49780 66	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1720	
Seq=1 ACK=177 Win=64128 Len=0 [ACK] 49789 > 443 60	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1721	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1722	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1723	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1724	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1725	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1726	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1727	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1728	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1729	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1730	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1731	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1732	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1733	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1734	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1735	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1736	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1737	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1738	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1739	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1740	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1741	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1742	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1743	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1744	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1745	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1746	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1747	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1748	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1749	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1750	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1751	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1752	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1753	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1754	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1755	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1756	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1757	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1758	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1759	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1760	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1761	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1762	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1763	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1764	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1765	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1766	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1767	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1768	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1769	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1770	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1771	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1772	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1773	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1774	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1775	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1776	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1777	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1778	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1779	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1780	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1781	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1782	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1783	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1784	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1785	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1786	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1787	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1788	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1789	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1790	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1791	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1792	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1793	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1794	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1795	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1796	
Seq=177 ACK=2921 Win=131328 Len=0 [ACK] 443 > 49789 54	Server Hello 1514	TCP	10.144.131.189	10.144.131.189	32.979771 1797	
Seq=17						

Help

Tools

Wireless

Telephony

Statistics

Analyze

Capture

Go View

Edit

File

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

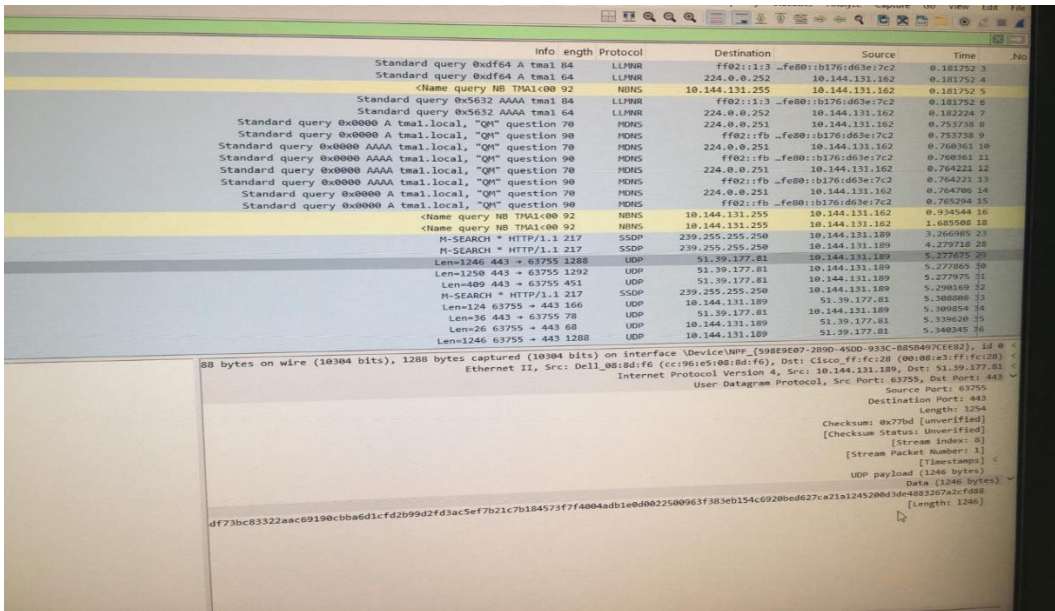
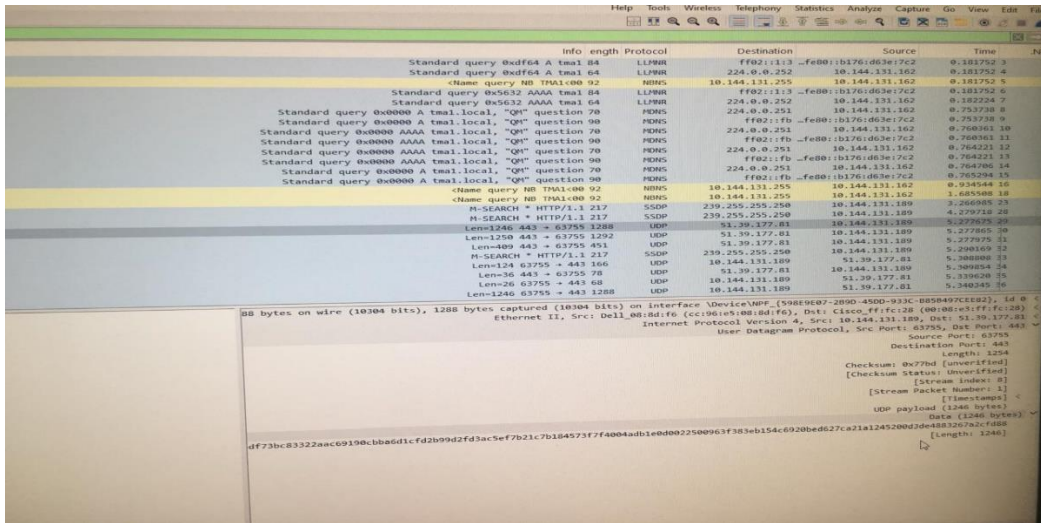
Step 1: In the filter bar, type UDP and press Enter.

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		
Data Integrity and Ordering		

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

	TCP	UDP
Use cases		
Performance		