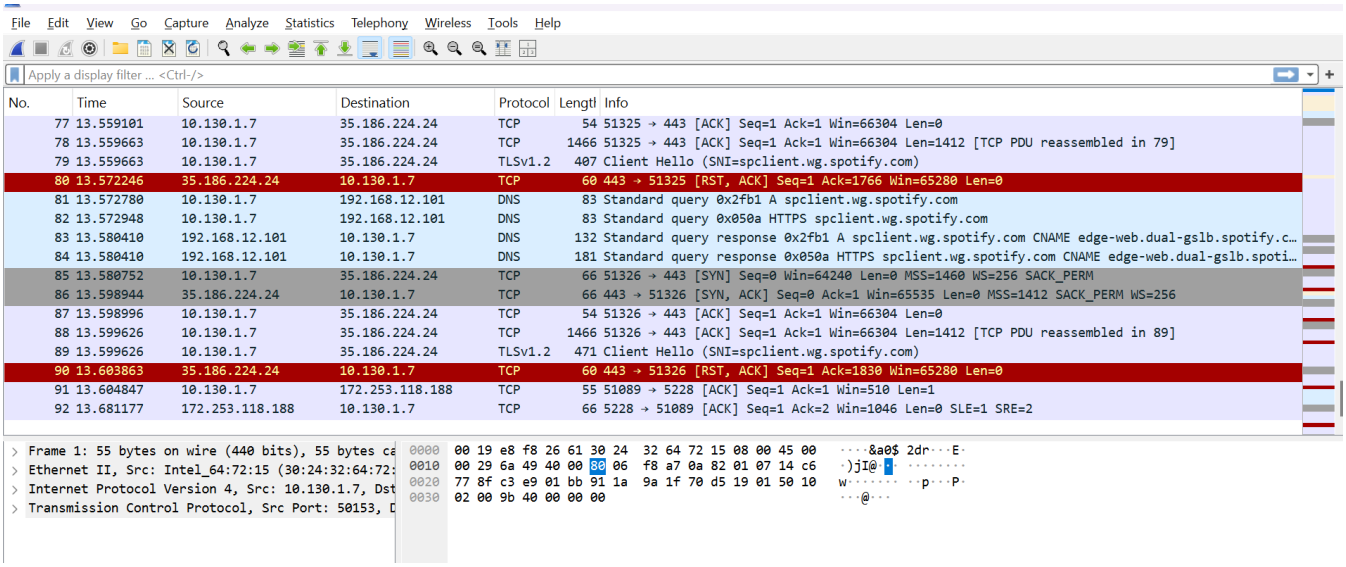
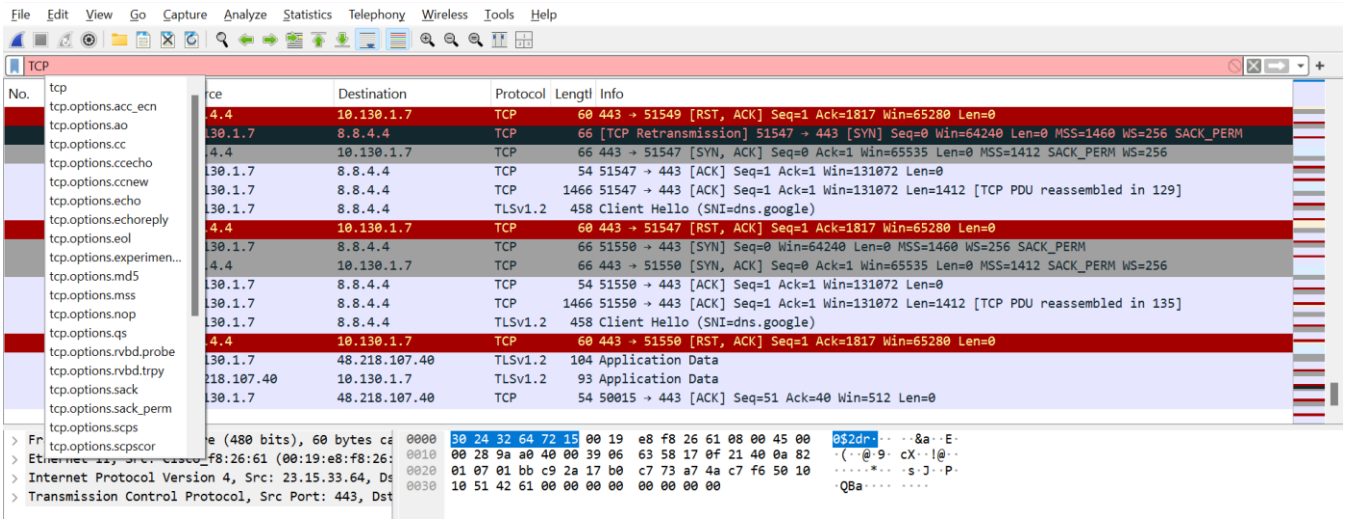
Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	**Date: 17/11/2024**	**Enrolment No: 92200133029**

Aim : Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

Step – 1 : Open the wireshark. After opening Wireshark**,** you will see several options on your screen. Select the **Wi-Fi interface** to start capturing packets. Once the capture begins, you can observe various types of packets being routed, similar to those shown in the image.

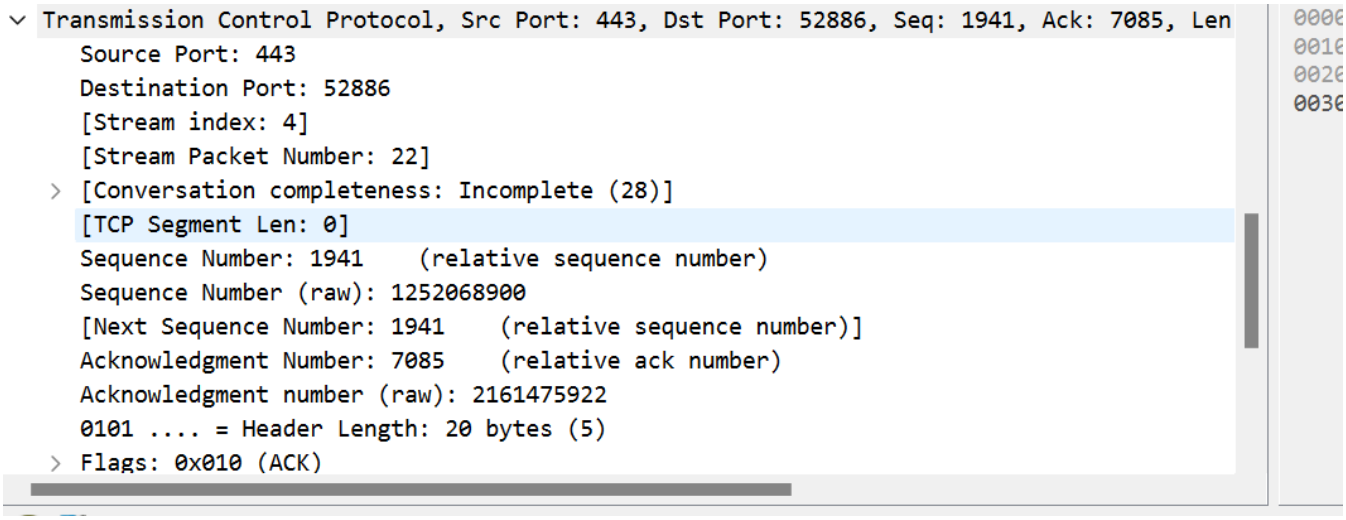


Step – 2 **:** Next, go to the **filter bar** in Wireshark and enter **tcp** as the filter. By applying this filter, you will see only the packets related to the **TCP protocol**, as shown in the image.

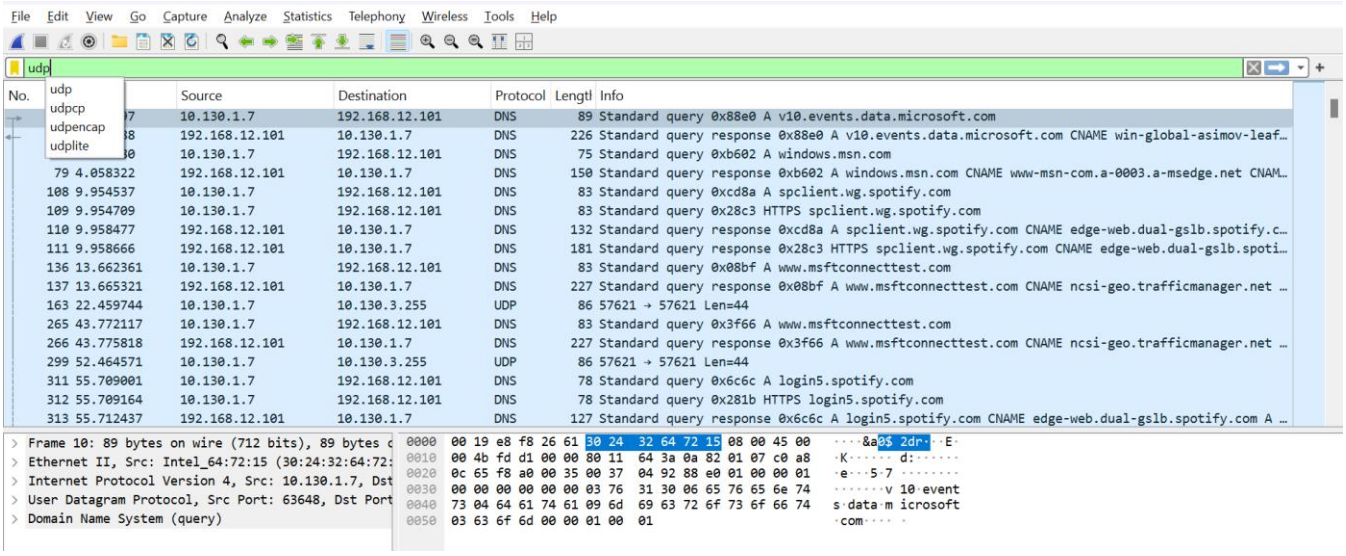


Here we can see detailed information of TCP that how it routes the packets and what ack it gives etc.

Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	**Date: 17/11/2024**	**Enrolment No: 92200133029**



Step – 3 : Now, in the **filter bar**, type **udp** and apply the filter. This will display only packets using the **UDP protocol**. In the image, you can see DNS packets because DNS (Domain Name System) typically operates over UDP for queries and responses, as it is faster and requires fewer resources compared to TCP.

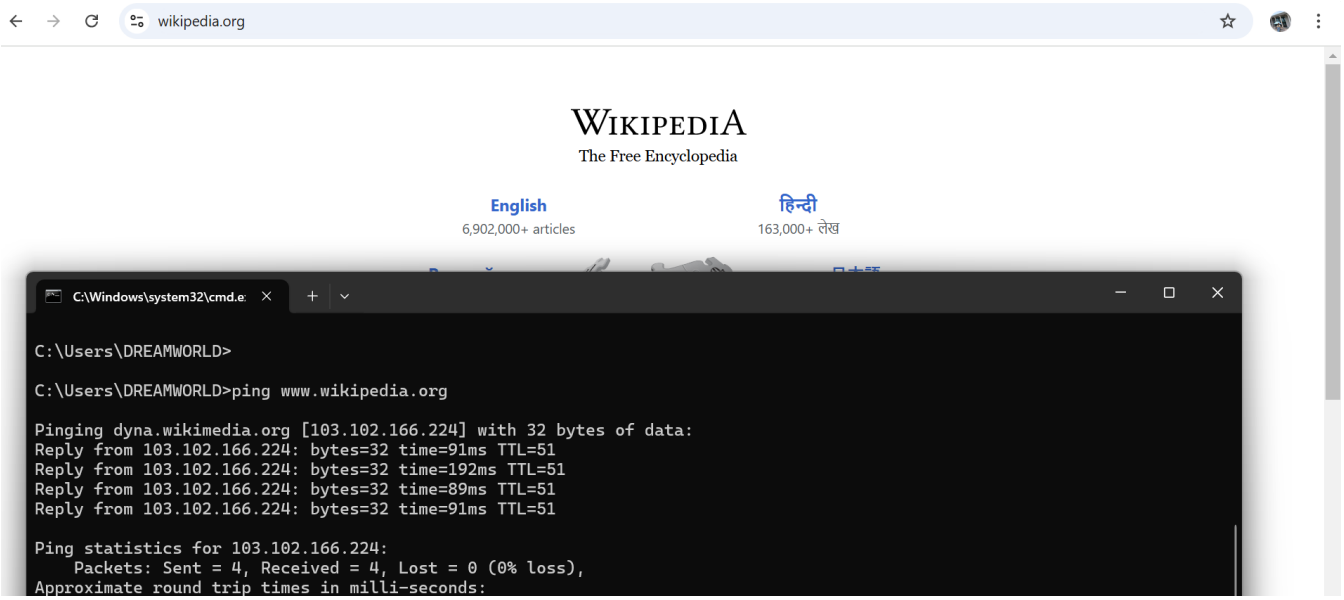


Here you can see various information about udp like udppayload and flags etc.

Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	**Date: 17/11/2024**	**Enrolment No: 92200133029**

```
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (48 bytes)
v Domain Name System (query)
    Transaction ID: 0x9afd
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 56]
```

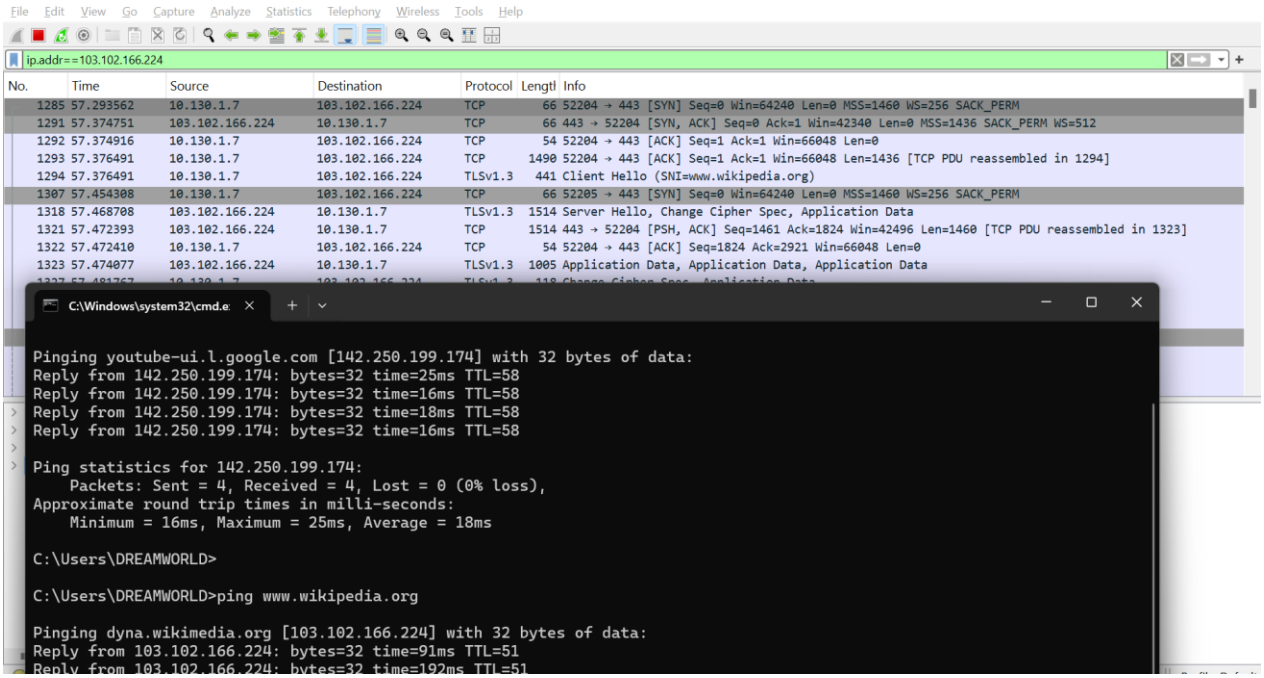
Step – 4 : To view the **IP protocol in action**, I opened the **Wikipedia website** and launched the **Command Prompt**. I then used the **ping command**, which is commonly used to check the routing of packets and measure the response time between your device and the target server. From this command, I was able to retrieve the **IP address of Wikipedia**.



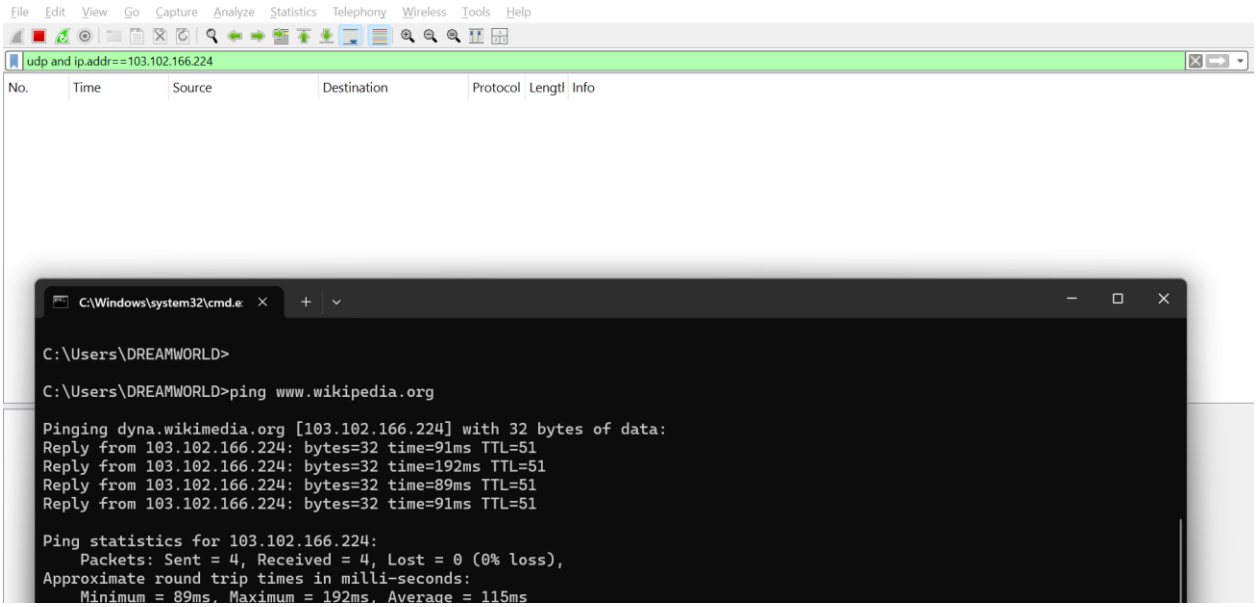
Step – 5 : Using the retrieved **IP address of Wikipedia**, go to the **filter bar** in Wireshark and type **ip.addr == [Wikipedia's IP address]** . This filter will show all the packets routed to and from the specified IP address, allowing you to analyze how the packets are being routed and the communication

Marwadi University Marwadi Chandarana Group	**Marwadi University** **Faculty of Engineering and Technology** **Department of Information and Communication Technology**	
Subject: Computer Networks (01CT0503)	**Aim:** Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	**Date: 17/11/2024**	**Enrolment No: 92200133029**

details.



Step – 6 : When you enter udp in the filter bar for the Wikipedia website, no packets are displayed because Wikipedia primarily uses the **TCP protocol** for communication. Websites like Wikipedia rely on **HTTP/HTTPS**, which are based on TCP, as TCP ensures reliable, ordered delivery of data. Since UDP is not used for this type of traffic, no UDP packets are captured for the Wikipedia website.



Conclusion :

In this Wireshark experiment, I analyzed network traffic using different protocols such as TCP, UDP, and IP. By applying filters for TCP and UDP, I observed how TCP ensures reliable, ordered data

transmission, making it ideal for applications like web browsing, while UDP, being faster and connectionless, is typically used for applications like DNS queries. I also observed the routing of IP packets when accessing a website like Wikipedia. Since Wikipedia uses the TCP protocol for its HTTP/HTTPS communication, no UDP packets were captured, highlighting the role of TCP in ensuring reliable web traffic. This experiment provided valuable insights into how different protocols function and interact within live networks.