Project Report

Network Traffic Capture Using Wireshark

Objective

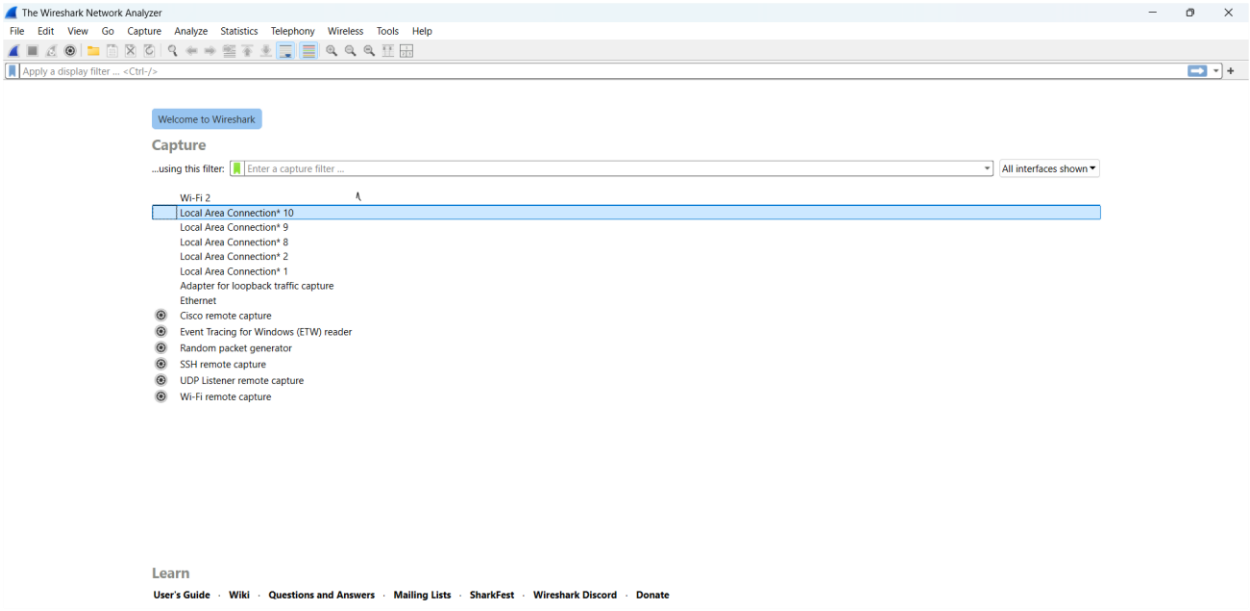
The objective of this project is to understand and analyze how data is transmitted over a network. Using Wireshark, a network protocol analyzer, we captured real-time traffic to inspect and learn about key protocols such as HTTP, DNS, and TCP. The project helps in visualizing how network communication works and detecting potential issues.

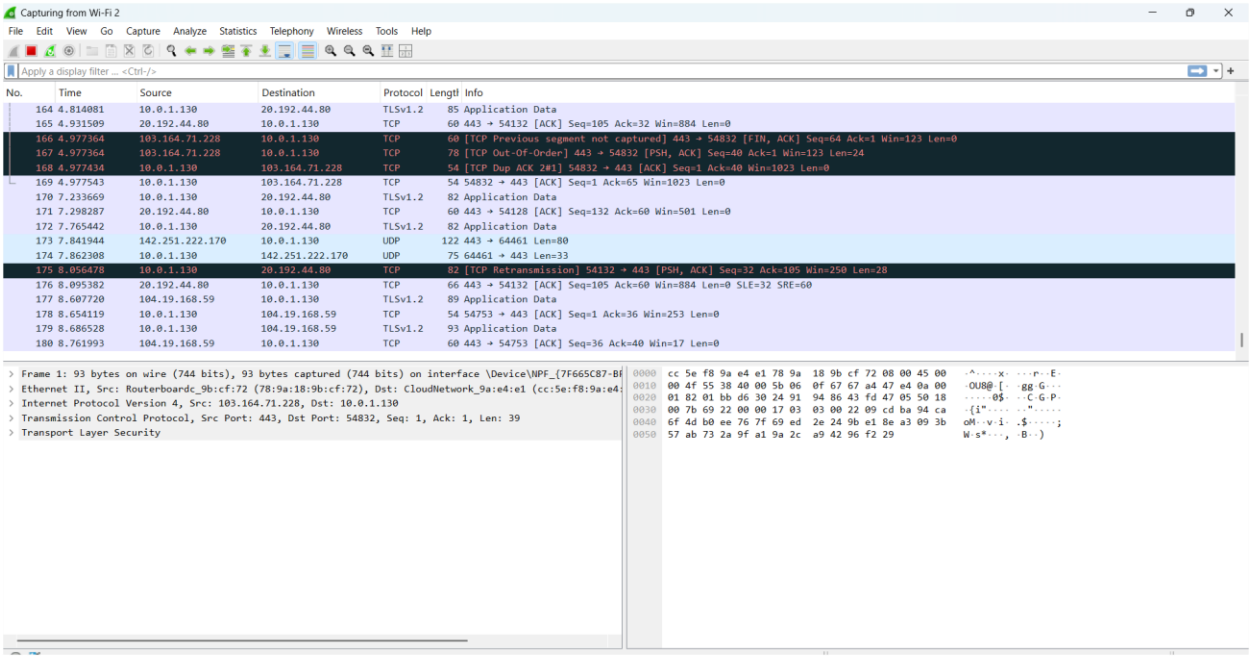
Tools Used

- **Wireshark** (Packet Capture Tool)
- **Web Browser** (to generate traffic)
- **Windows 10 / Linux OS**

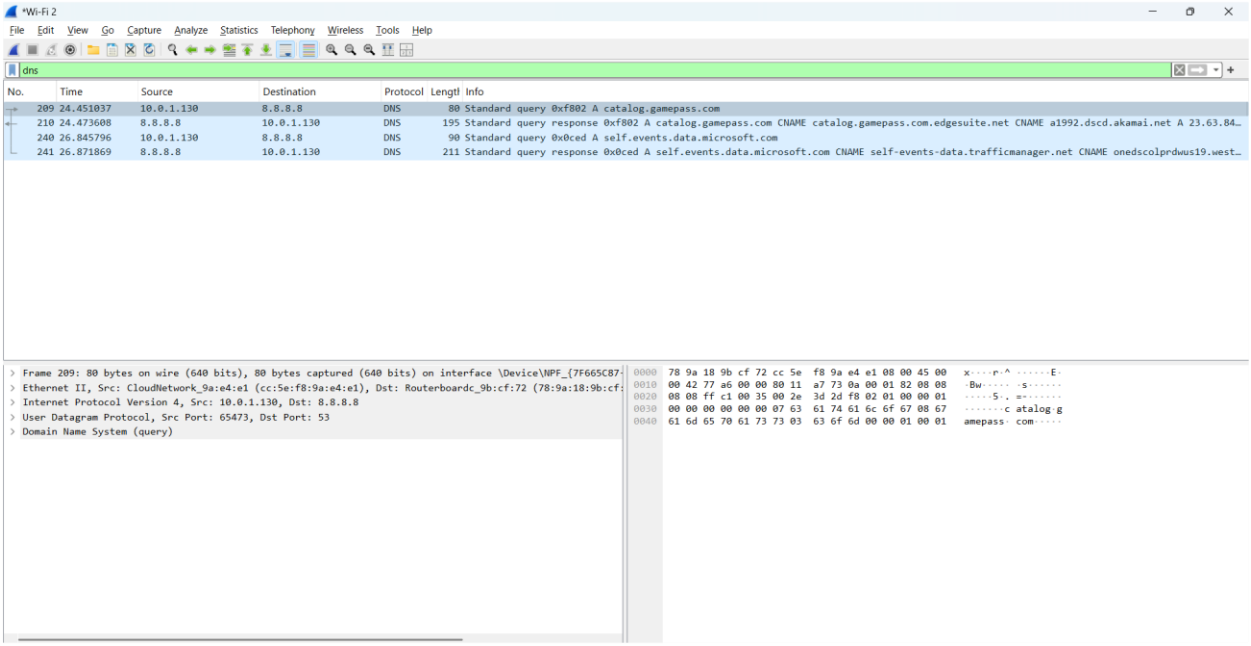
Steps Performed

1. Launched Wireshark and selected the active network interface (e.g., Wi-Fi).
2. Started capturing live traffic.
3. Opened a browser and visited websites like `https://www.wikipedia.org` to generate data.
4. Stopped the capture after generating enough traffic.
5. Applied filters like `http`, `dns`, and `tcp` to isolate specific protocol traffic.
6. Analyzed captured packets to study headers, source/destination IPs, and payload data.





- Screenshot : Full capture window



- Screenshot : Filtered DNS traffic

Conclusion

This project provided hands-on experience with capturing and analyzing network traffic using Wireshark. It improved understanding of how different protocols operate at various layers of the OSI model. By examining live packets, I learned how data is structured, routed, and responded to on a real network.