**GitHub Project Report: Wireshark Network Capture**

## **📘 Project Overview**

This project demonstrates how to use Wireshark, a network packet analyzer, to capture and analyze network traffic. The experiment involves monitoring a live network interface, generating packets, filtering them by protocol, and summarizing observed communication details.

## **🧰 Tools Used**

- Wireshark (Network Protocol Analyzer)  
- Web Browser or Command Prompt (for generating traffic)  
- Operating System: Windows/Linux

## ⚙️ Procedure

1. 1. Install Wireshark.
2. 2. Start capturing on your active network interface.
3. 3. Browse a website or ping a server to generate traffic.
4. 4. Stop capture after a minute.
5. 5. Filter captured packets by protocol (e.g., HTTP, DNS, TCP).
6. 6. Identify at least 3 different protocols in the capture.
7. 7. Export the capture as a .pcap file.
8. 8. Summarize your findings and packet details.

## 📊 Findings

During the capture session, three main protocols were identified:  
- \*\*HTTP:\*\* Handles communication between client browsers and web servers.  
- \*\*DNS:\*\* Resolves domain names into corresponding IP addresses.  
- \*\*TCP:\*\* Ensures reliable transmission of data packets between devices.

## 📦 Packet Summary

1. \*\*HTTP Packets:\*\* Displayed GET and POST requests, and 200 OK responses.  
2. \*\*DNS Packets:\*\* Showed A and AAAA record queries and responses.  
3. \*\*TCP Packets:\*\* Contained connection setup (SYN, SYN-ACK) and teardown (FIN, ACK) packets.

## ✅ Results Summary

The analysis successfully captured and categorized multiple network communication protocols. By applying protocol filters, the traffic could be inspected in detail, offering insights into how data travels across the internet at various layers of the OSI model.

## 🔍 Conclusion

Wireshark proved to be a powerful tool for understanding network communications. The experiment provided hands-on experience in capturing, filtering, and interpreting packets. This knowledge is essential for tasks like network troubleshooting, cybersecurity analysis, and performance monitoring.