Wireshark Intro Lab Report

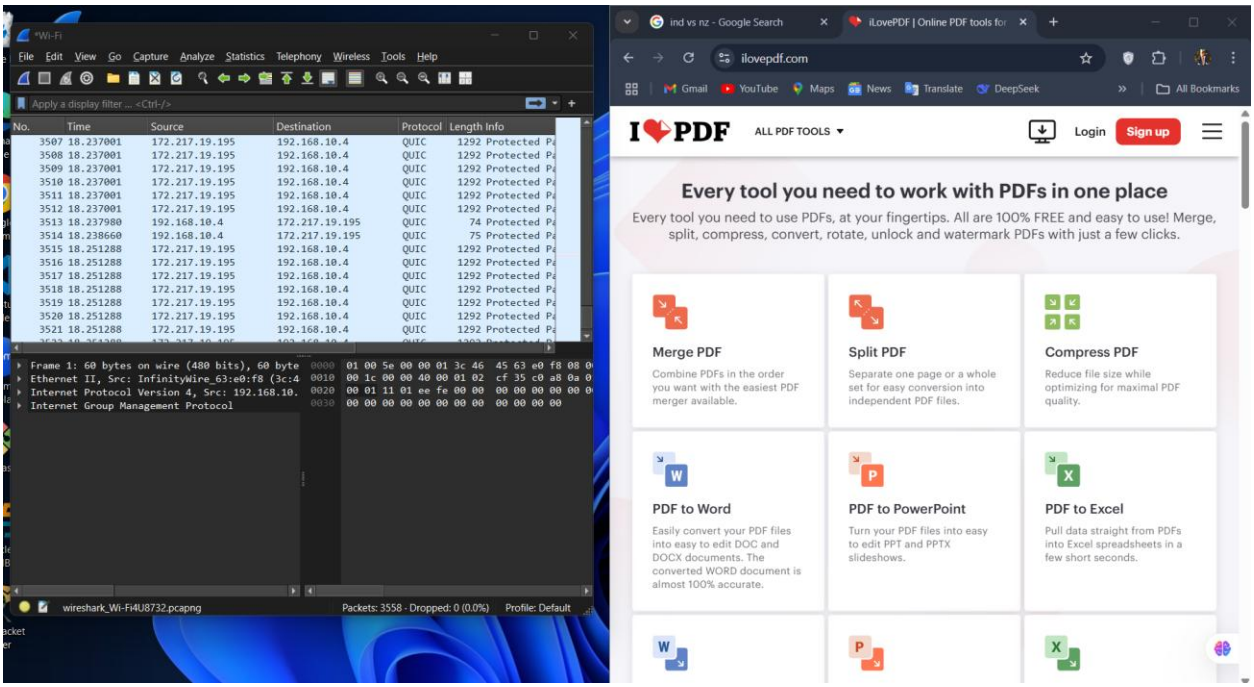
Name: Muhammad Shoaib Ahmad (BSDSF22A028)
Date: 31-03-2025
Instructor: Dr. Nadeem Majeed

---

1. Capturing Network Traffic

1. Open Wireshark and start packet capture on your active network interface.
2. Perform basic network activity, such as visiting `www.google.com`.
3. Stop the capture after 30-60 seconds.

Wireshark capturing packets (Show the main Wireshark window with packets captured).

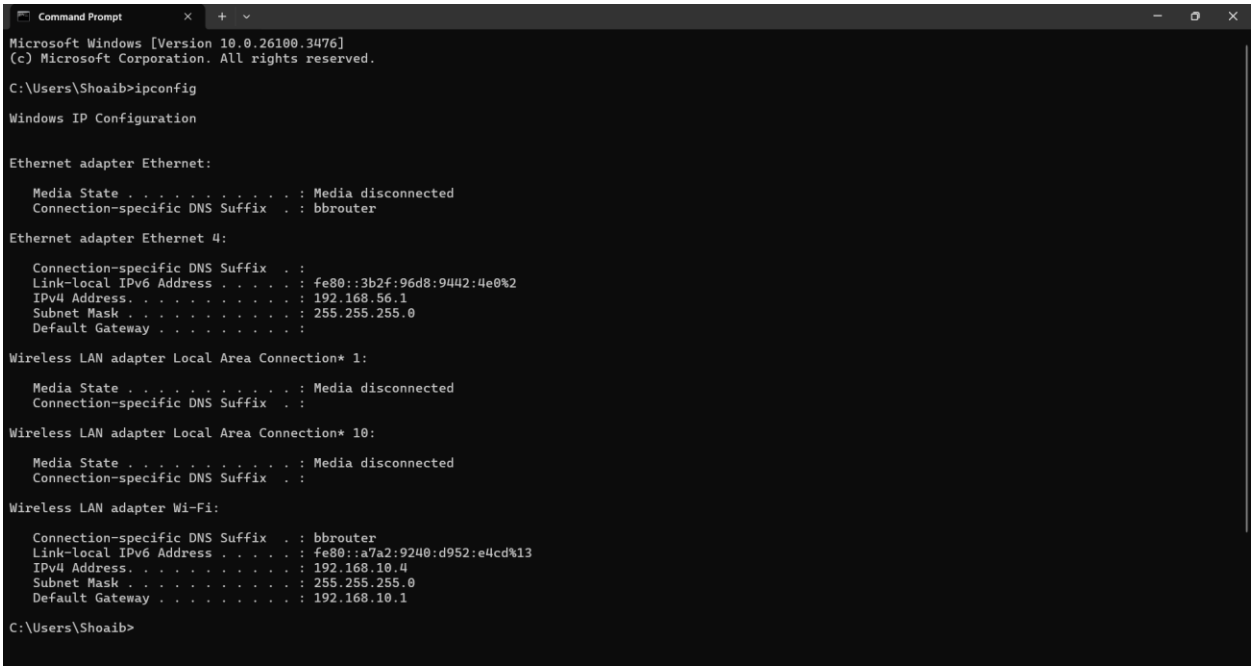


---

2. Identifying Your IP Address

1. Open a terminal or command prompt.
   - Windows: Run `ipconfig`
   - Mac/Linux: Run `ifconfig` or `ip a`
2. Note your IP address.

Output of `ipconfig` / `ifconfig` showing your IP address.

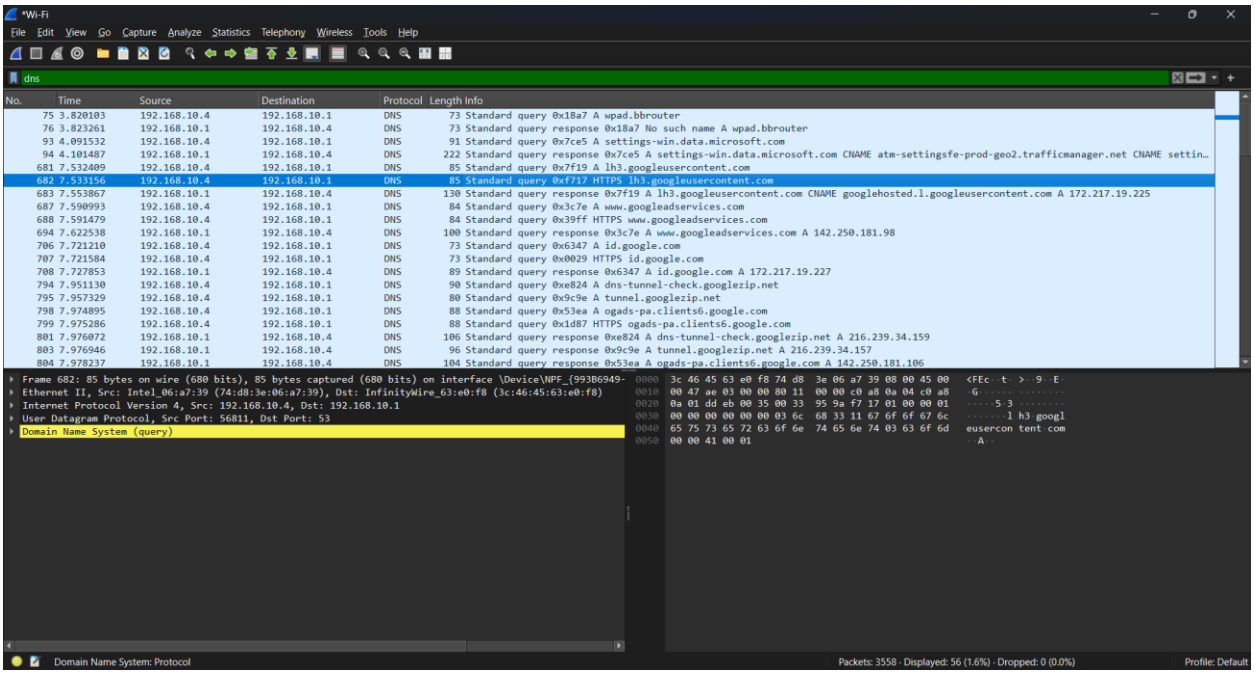


---

3. Filtering DNS Traffic

1. Apply the filter `dns` in Wireshark.
2. Identify DNS requests and responses for visited websites.

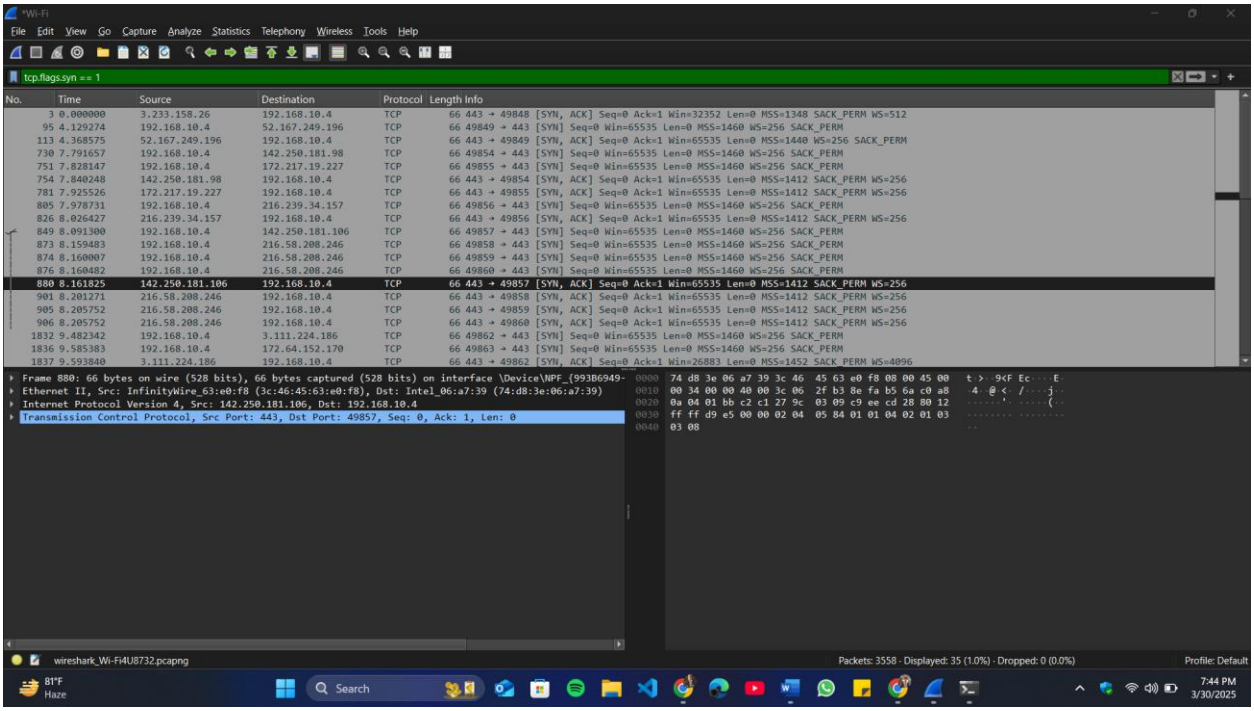
DNS query and response packets. Highlight the queried domain names.



4. Analyzing TCP Three-Way Handshake

1. Use the filter `tcp.flags.syn == 1` to locate a SYN packet.
2. Right-click the SYN packet and "Follow TCP Stream" to view the handshake.

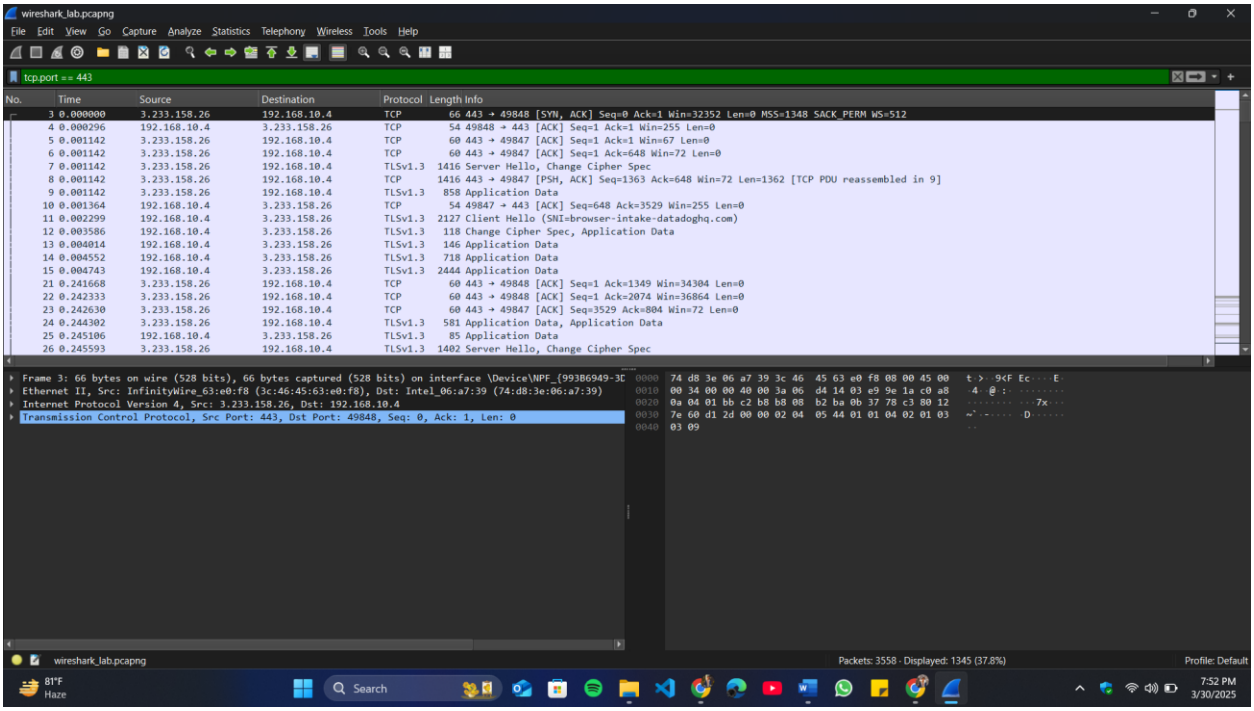
Attach Screenshot: Three-way handshake (SYN, SYN-ACK, ACK packets).



5. Examining HTTP Traffic

1. Apply the filter `http` in Wireshark.
2. Look at GET and POST requests to identify visited websites and request details.

Attach Screenshot: HTTP request headers showing requested URLs.



---

6. Saving and Submitting Capture File

1. Go to **File → Save As**, and save the file as `wireshark_lab.pcapng`
