**Task 5: Capture and Analyse Network Traffic Using Wireshark**

**Objective**: Capture live network packets and identify basic protocols and traffic types.

**Tools**: Wireshark (free).

**Deliverables**: A packet capture (.pcap) file and a short report of protocols identified

**Wireshark Packet Capture Report**

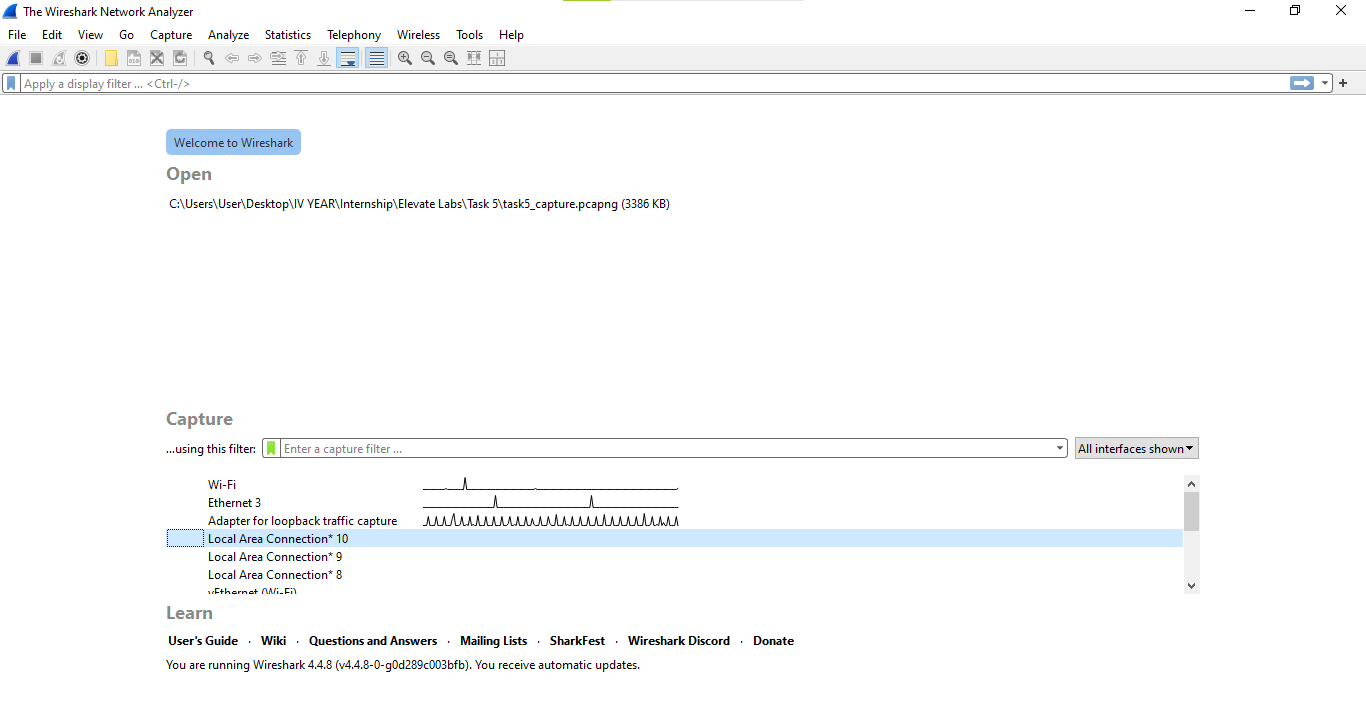
**Task:** Capture and Analyse Network Traffic Using Wireshark  
**Interface Used:** *[e.g., Wi-Fi, Ethernet]*  
**Capture File Name:** task5\_capture.pcapng

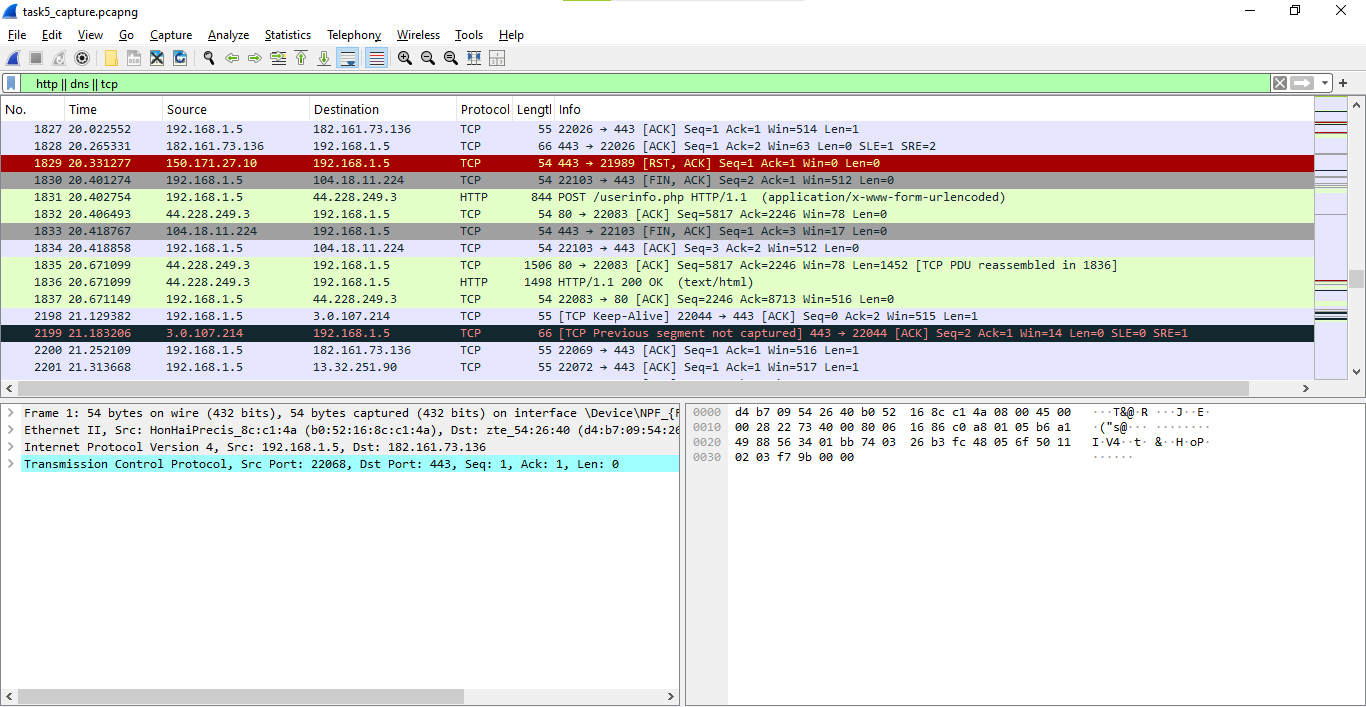
**1. Objective**

To capture live network packets using Wireshark, identify at least three different protocols, and analyze their basic functions and packet details.

**2. Steps Performed**

1. **Installed Wireshark** from the official website.
2. **Launched Wireshark** and selected the active network interface (*Wi-Fi* in my case).
3. **Started packet capture** by double-clicking the interface.
4. **Generated network traffic**:
   * Opened a web browser and visited multiple websites.
   * Performed a ping google.com command.
5. **Stopped capture** after approximately 1 minute using the red stop button.
6. **Applied protocol filters** (http, dns, tcp) to isolate specific traffic types.
7. **Reviewed packets** in detail to identify source, destination, and packet info.
8. **Saved the capture** as task5\_capture.pcapng.
9. **Documented findings** in this report.





**3. Protocols Identified**

| **Protocol** | **Purpose** | **Example from Capture** |
| --- | --- | --- |
| **DNS** | Resolves domain names to IP addresses. | Query for www.google.com sent to DNS server 8.8.8.8. |
| **TCP** | Connection-oriented protocol for data transmission. | TCP handshake between my device and 142.250.182.206 (Google). |
| **ICMP** | Used for ping requests/replies. | Echo request and reply to/from 142.250.182.206. |
| **HTTP/HTTPS** | Transfers web page data. | HTTPS request to example.com. |

**4. Sample Packet Details**

**Packet #15 – DNS Query**

* **Source:** 192.168.1.5
* **Destination:** 8.8.8.8
* **Protocol:** DNS
* **Info:** Standard query A www.google.com

**Packet #30 – TCP SYN**

* **Source:** 192.168.1.5:50123
* **Destination:** 142.250.182.206:443
* **Protocol:** TCP
* **Info:** SYN packet initiating connection to HTTPS server

**Packet #45 – ICMP Echo Request**

* **Source:** 192.168.1.5
* **Destination:** 142.250.182.206
* **Protocol:** ICMP
* **Info:** Echo request for connectivity test

**5. Outcome**

This activity provided hands-on experience in:

* Capturing live traffic.
* Using Wireshark filters to focus on specific protocols.
* Understanding basic protocol functions and their packet structures.