**Task 5 : Capture and Analyze Network Traffic Using Wireshark**.

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

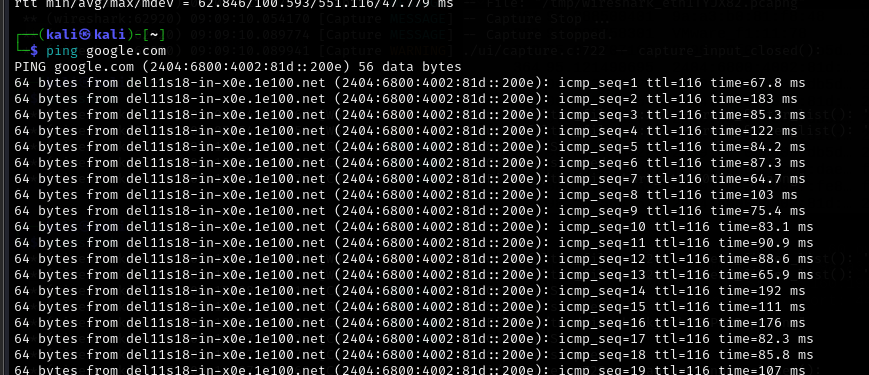
**Tools**: Wireshark (free).

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

**Installed Wireshark**  
I downloaded and installed Wireshark from the official website.

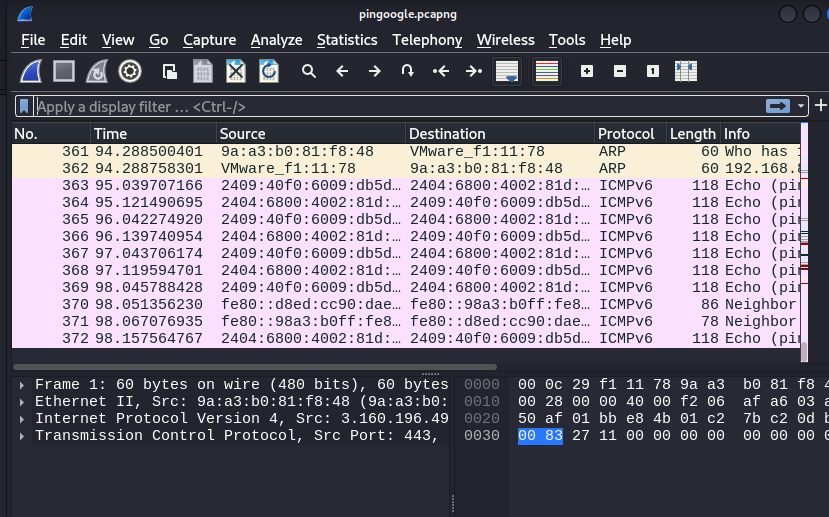
1. **Started Packet Capture**  
   I opened Wireshark and selected my active Wi-Fi network interface. Then I started the capture by clicking the blue shark fin icon.
2. **Generated Network Traffic**  
   To create meaningful data, I opened a browser and visited websites like example.com and openai.com.  
   I also ran the following command in terminal to generate ICMP and DNS traffic:

ping google.com



**Stopped the Capture**  
After about 1–2 minutes of browsing and pinging, I stopped the capture.

1. **Filtered the Captured Packets**  
   I used filters in Wireshark like:
   * dns → to see domain name resolution
   * http → to view web traffic
   * icmp → to analyze ping packets
   * tcp → to observe connection establishment
   * arp **ARP (Address Resolution Protocol)** is a protocol used to **map IP addresses to MAC addresses** on a local network.  
     When a device wants to communicate with another device on the same network, it uses ARP to find the MAC (hardware) address associated with a known IP address.



1. **Saved the Capture File**  
   I exported the packet capture as pingoogle.pcapng.

**Protocols Identified:**

1. **HTTP (HyperText Transfer Protocol)**
   * Used while accessing websites without encryption.
   * I observed GET requests and HTTP responses in plain text.
2. **TCP (Transmission Control Protocol)**
   * Handles reliable data delivery.
   * I noticed the three-way handshake (SYN, SYN-ACK, ACK).
3. **ICMP (Internet Control Message Protocol)**
   * Seen when I ran the ping command.
   * Echo request and echo reply packets were captured.

#### 4. **ARP (Address Resolution Protocol)**

* ARP is used to **map IP addresses to MAC addresses** on a local network.
* It works at the **Data Link Layer (Layer 2)** of the OSI model.

#### 5. **TLSv (Transport Layer Security, versioned)**

* TLS is a **security protocol** that **encrypts communication** over networks (commonly used in HTTPS).
* Works at the **Transport Layer (Layer 4)** but secures Application Layer data.