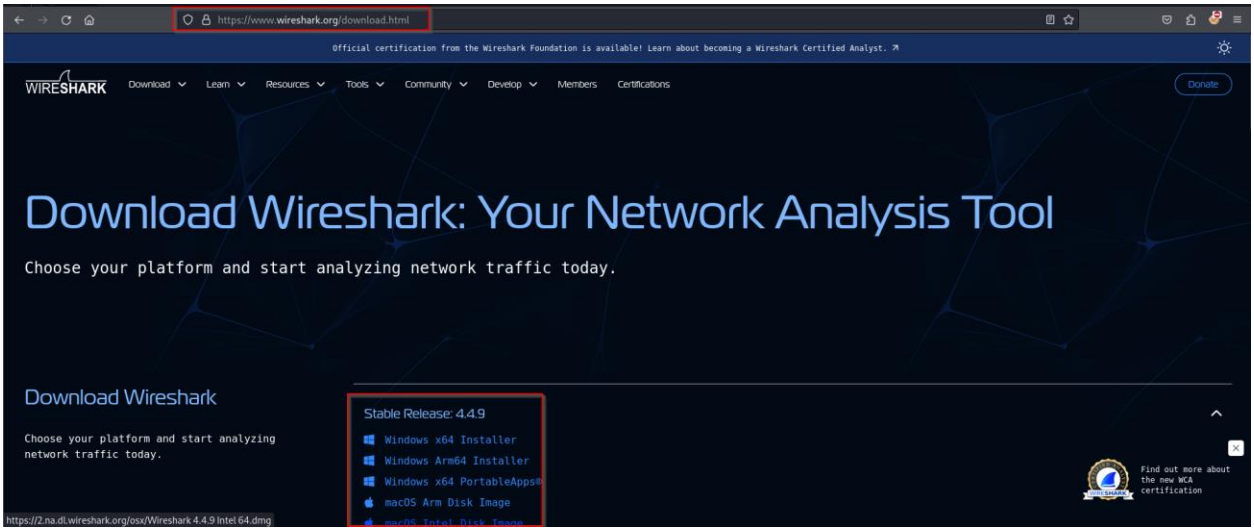
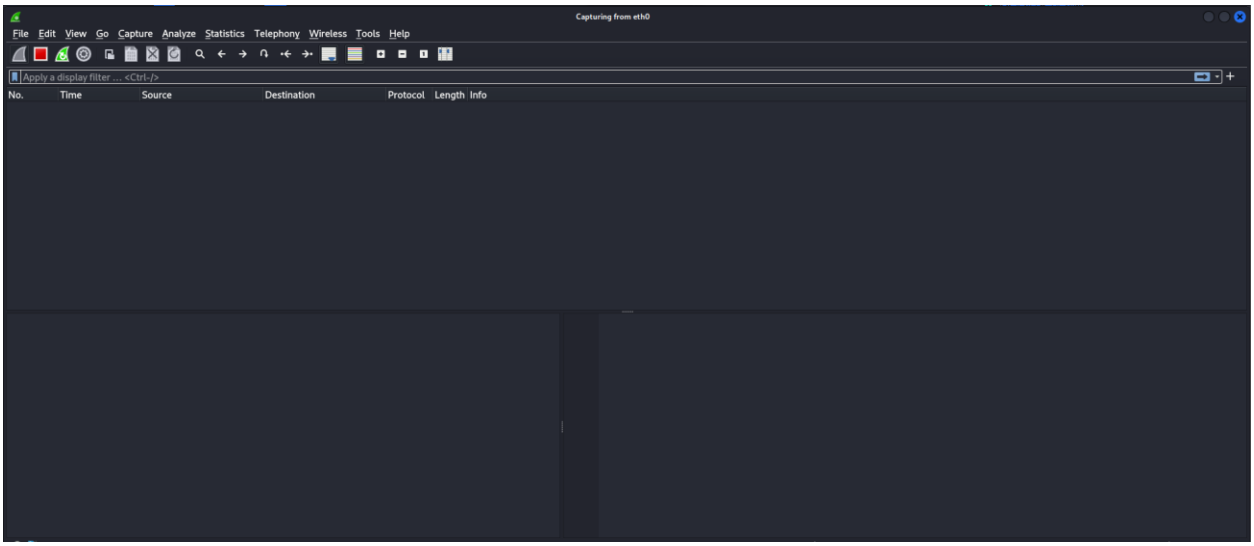
Task 5: Capture and Analyze Network Traffic Using Wireshark

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

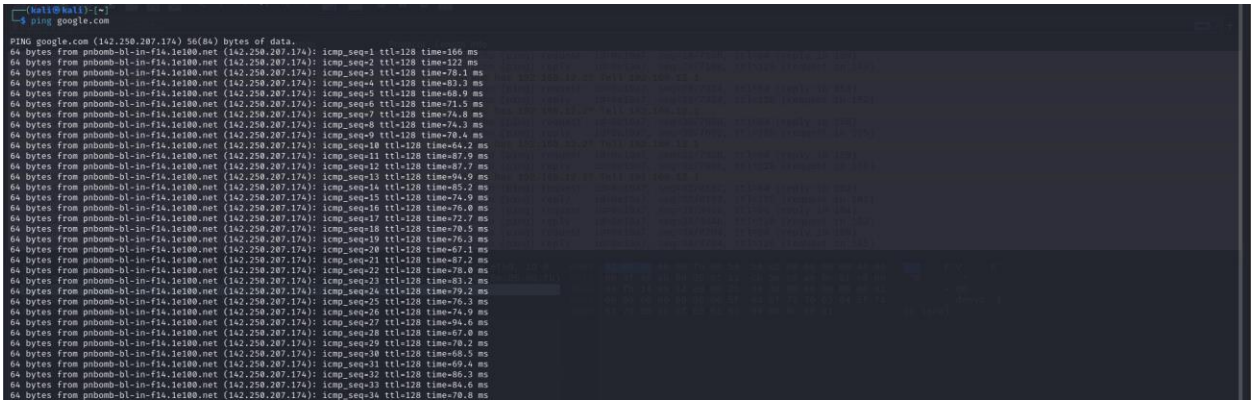
- **Step 1: Install Wireshark**
  - Download from: https://www.wireshark.org/download.html
  - Follow the installation instructions for your OS (Windows/Mac/Linux)



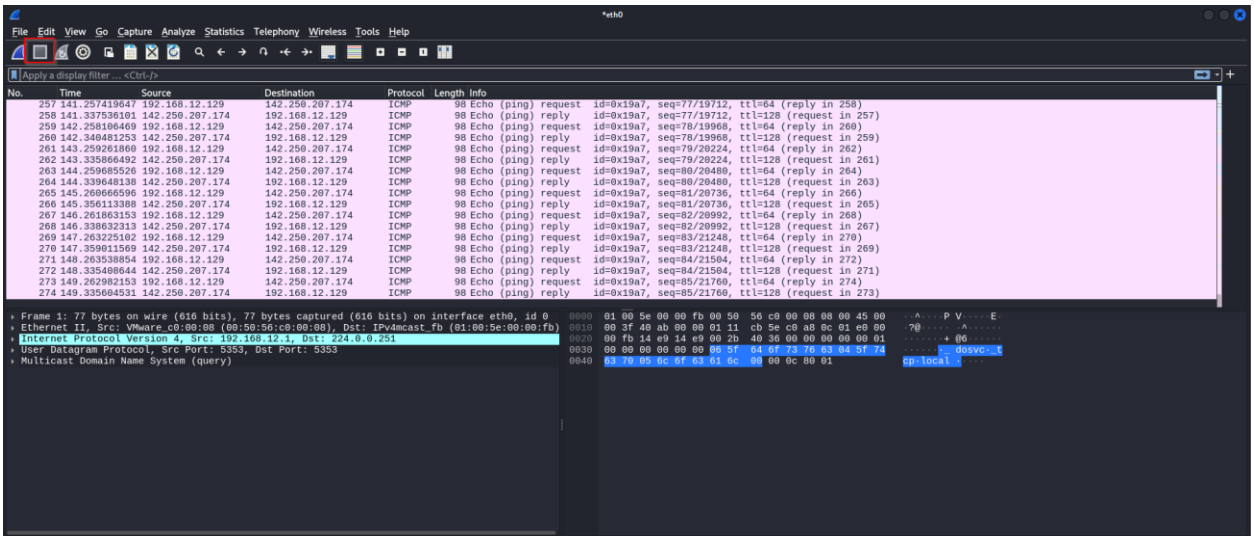
- **Step 2: Start Capturing on Active Network Interface**
  - Open Wireshark.
  - Select your **active network interface** (usually Ethernet or Wi-Fi).
  - Click the blue **shark fin icon** (top left) to start capturing.



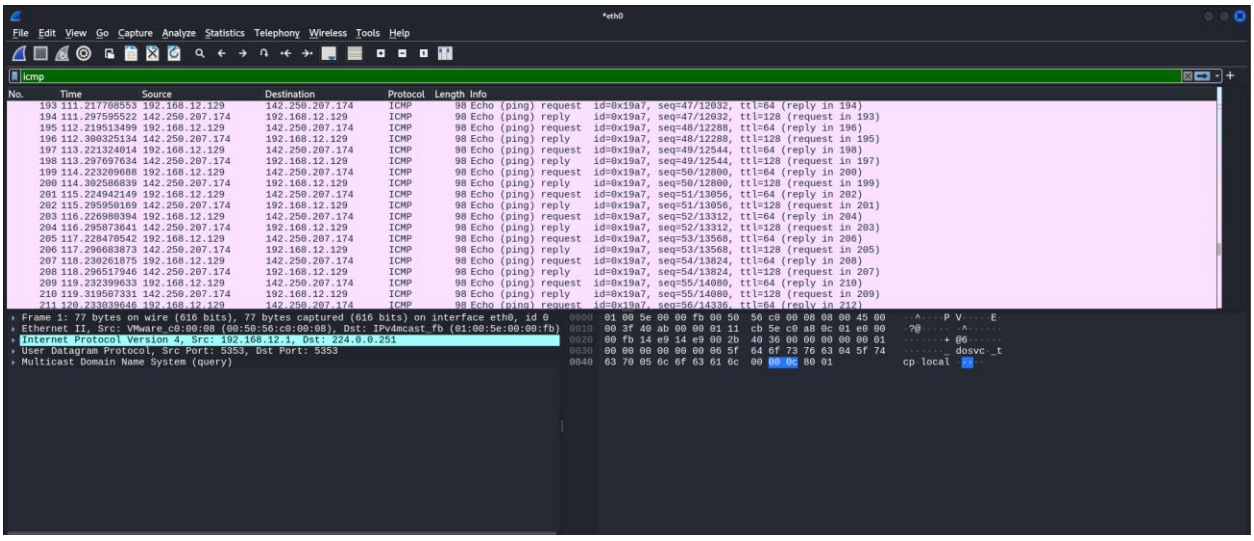
- **Step 3: Browse a Website or Ping a Server**
  - Open a browser and go to a website like example.com.
  - Or, open the terminal/command prompt and run: ping google.com



- **Step 4: Stop Capture After a Minute**
  - Wait ~60 seconds.
  - Click the red **stop icon** (top left) in Wireshark.



- **Step 5: Filter Captured Packets by Protocol**
  - Use the filter bar at the top.
  - Try these filters:
    - http → for HTTP traffic
    - dns → for DNS queries
    - tcp → for general TCP packets
    - icmp → for ping (if you used ping)



- **Step 7: Export as .pcap File**
  - Go to **File > Export Specified Packets...**

- Save as:
  your_capture_name.pcap