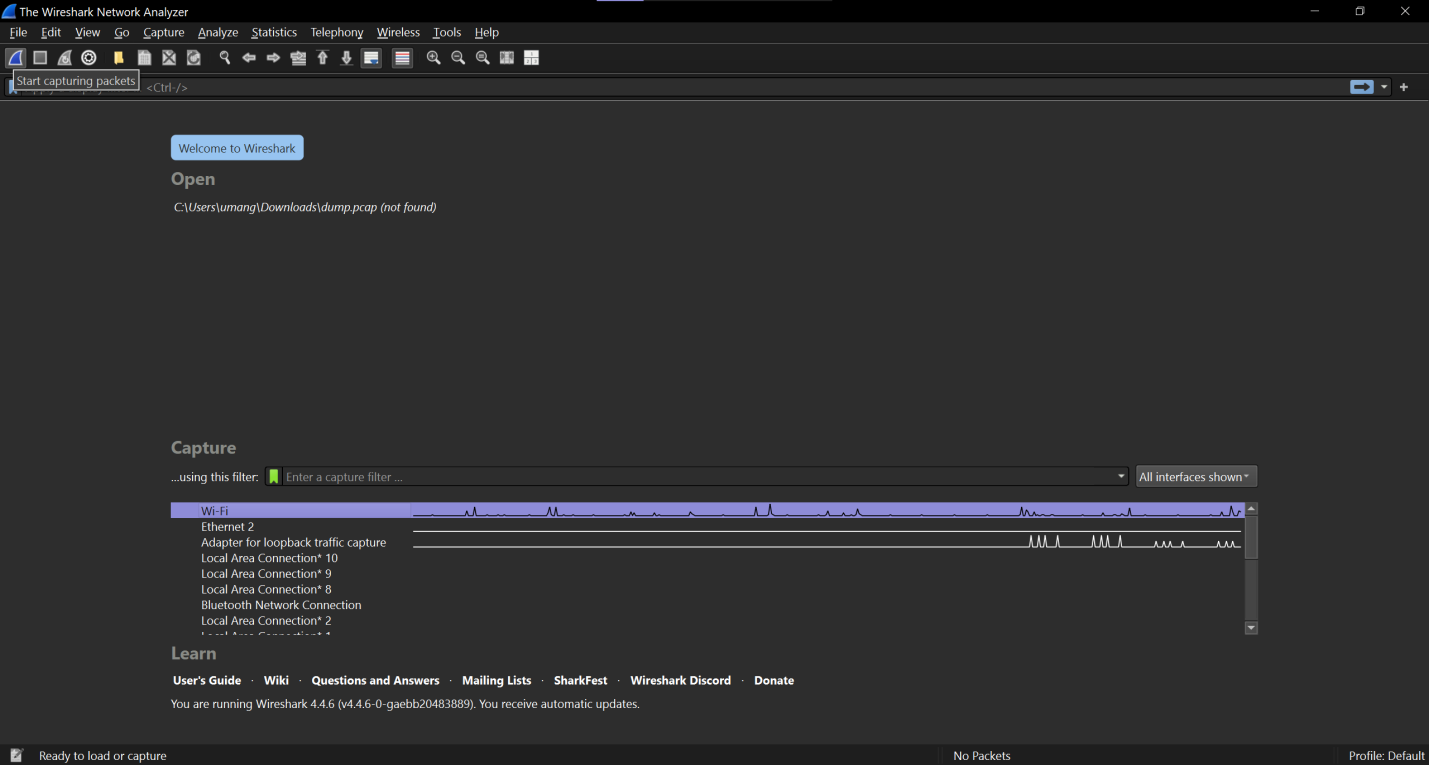
**Steps to Perform the Capture**

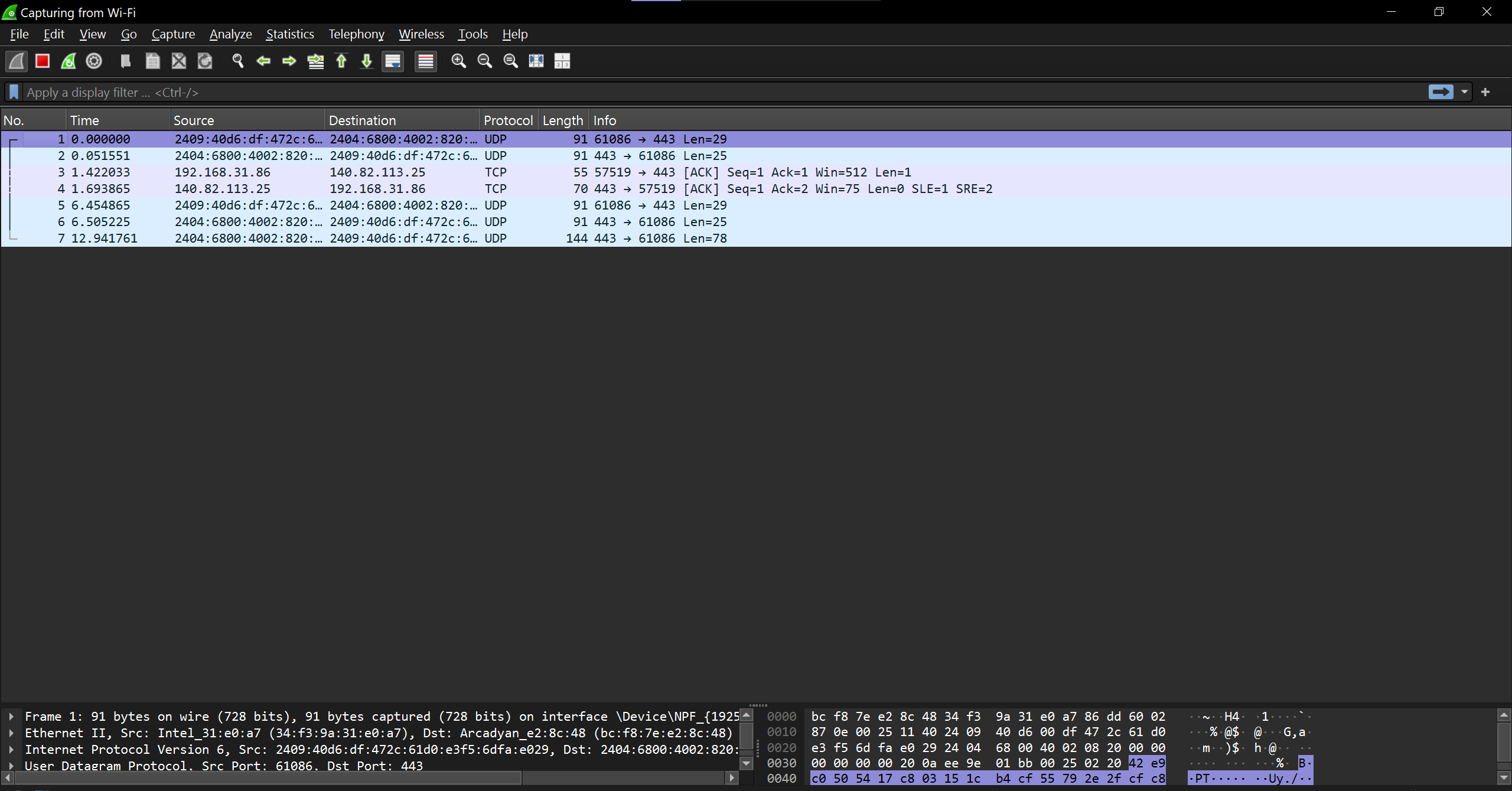
**1. Install Wireshark**

Download and install Wireshark from the official website.

**2. Start Capturing**

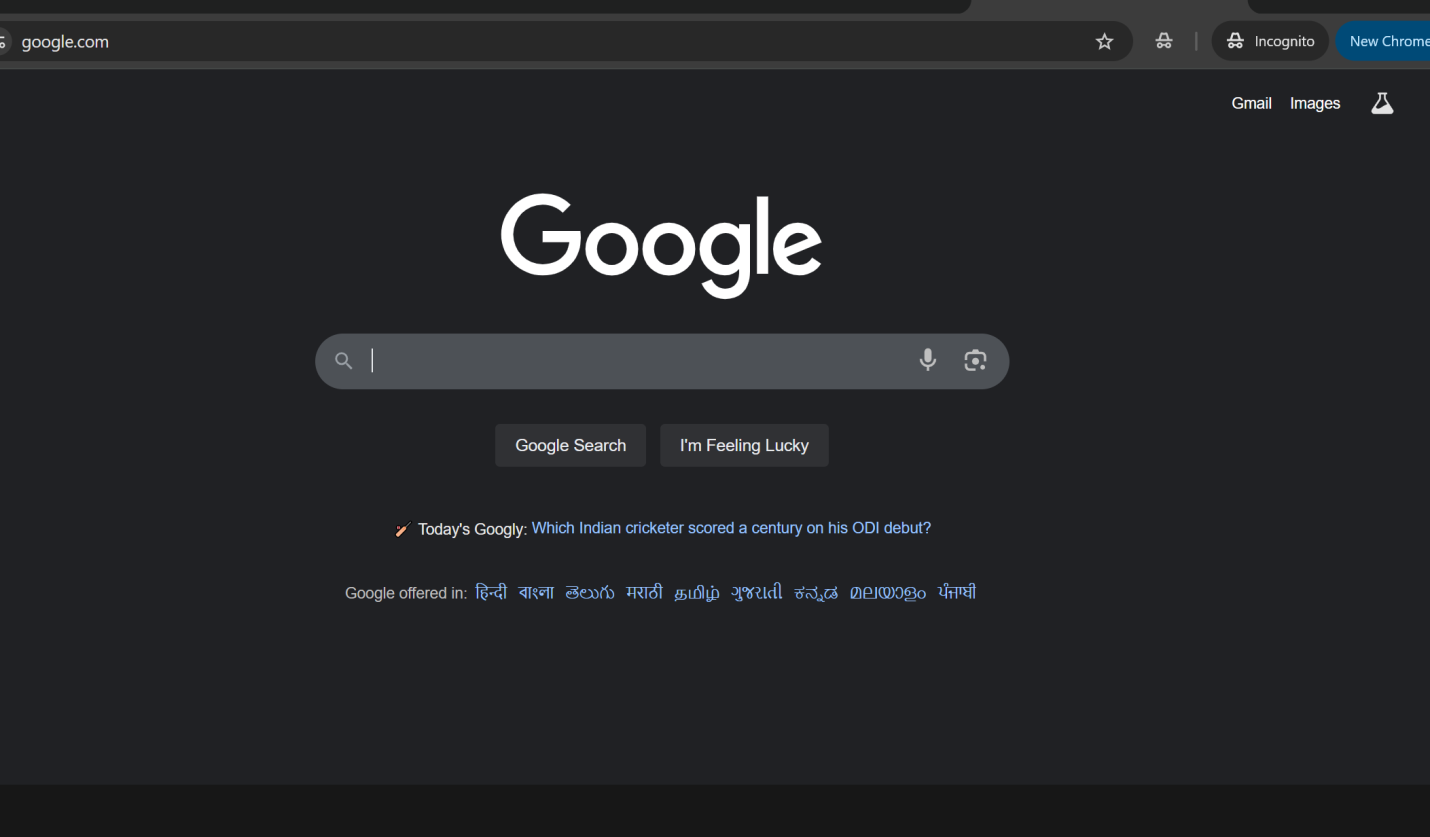
* Open Wireshark.
* Select your active network interface (usually Wi-Fi or Ethernet).
* Click the blue **shark fin** icon to start the capture.

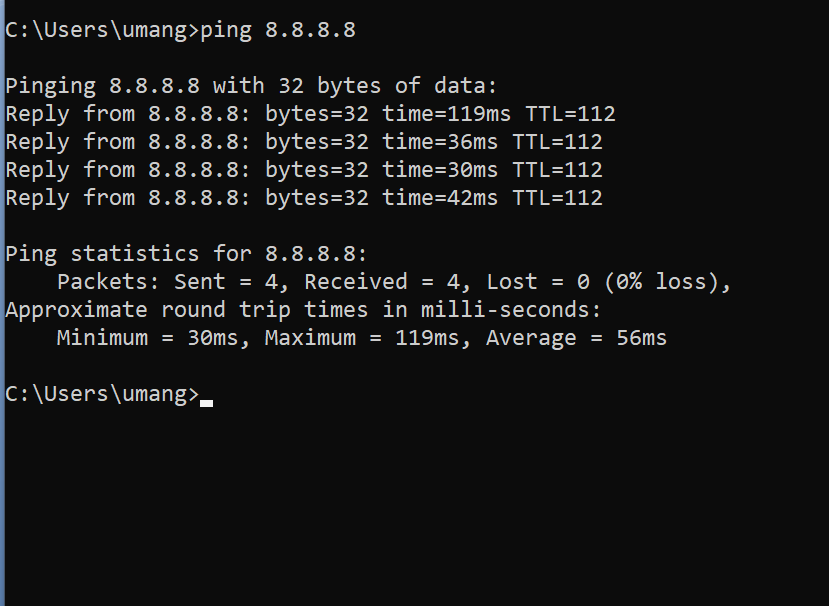




**3. Generate Traffic**

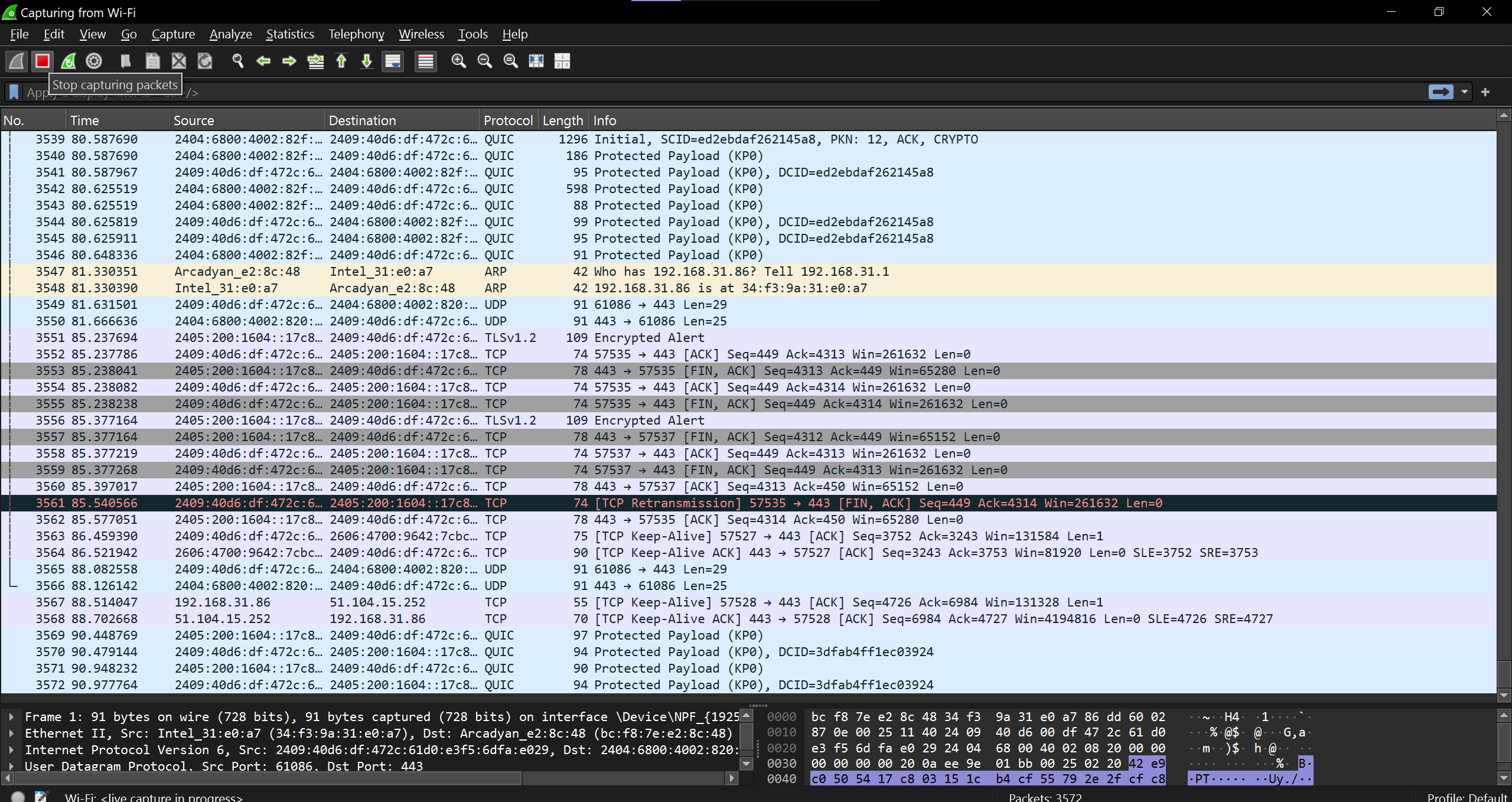
* Open a browser and visit a website like example.com or google.com.
* Open a terminal/command prompt and run a command like: ping 8.8.8.8





**4. Stop Capture**

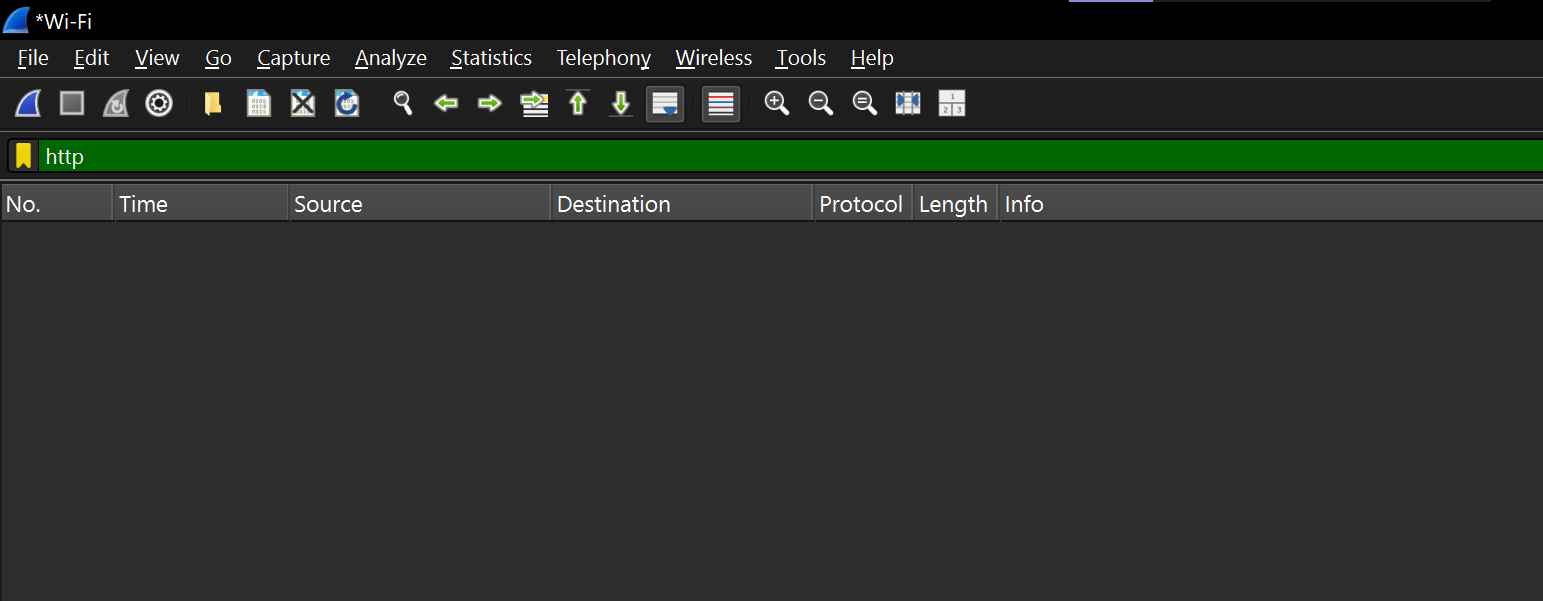
* Let the capture run for 30 seconds to 1 minute.
* Click the red square icon to stop the capture.

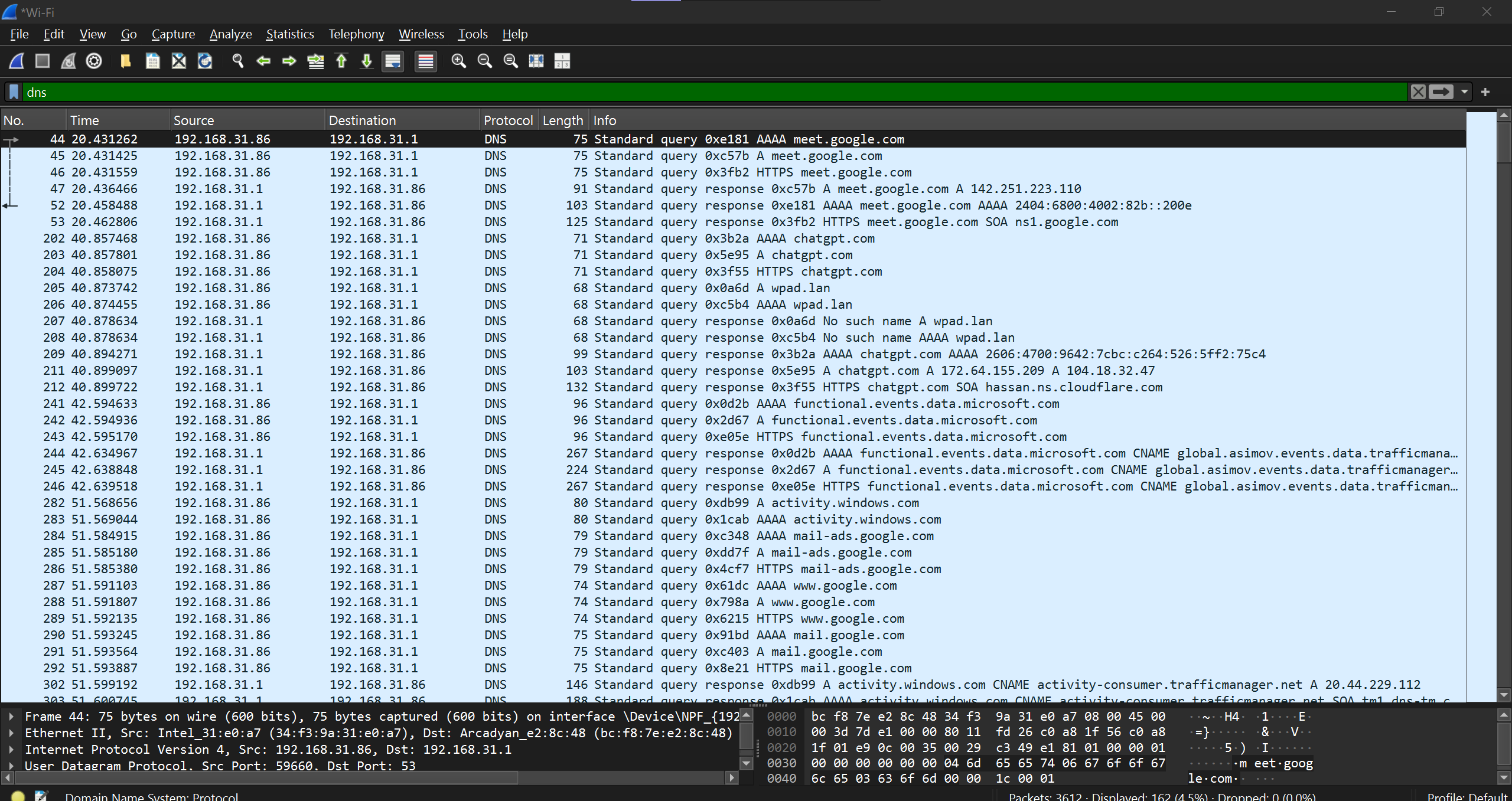


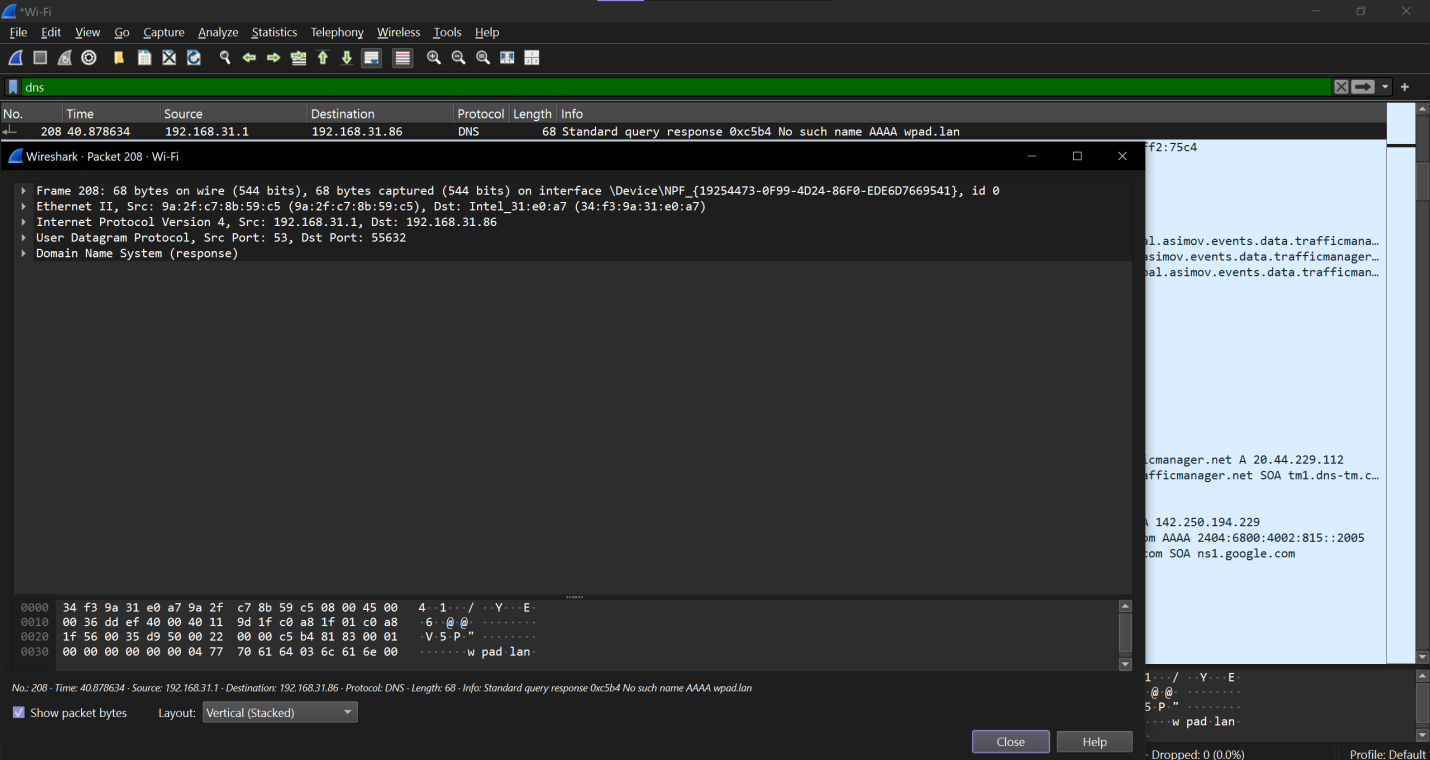
**5. Filter by Protocols**

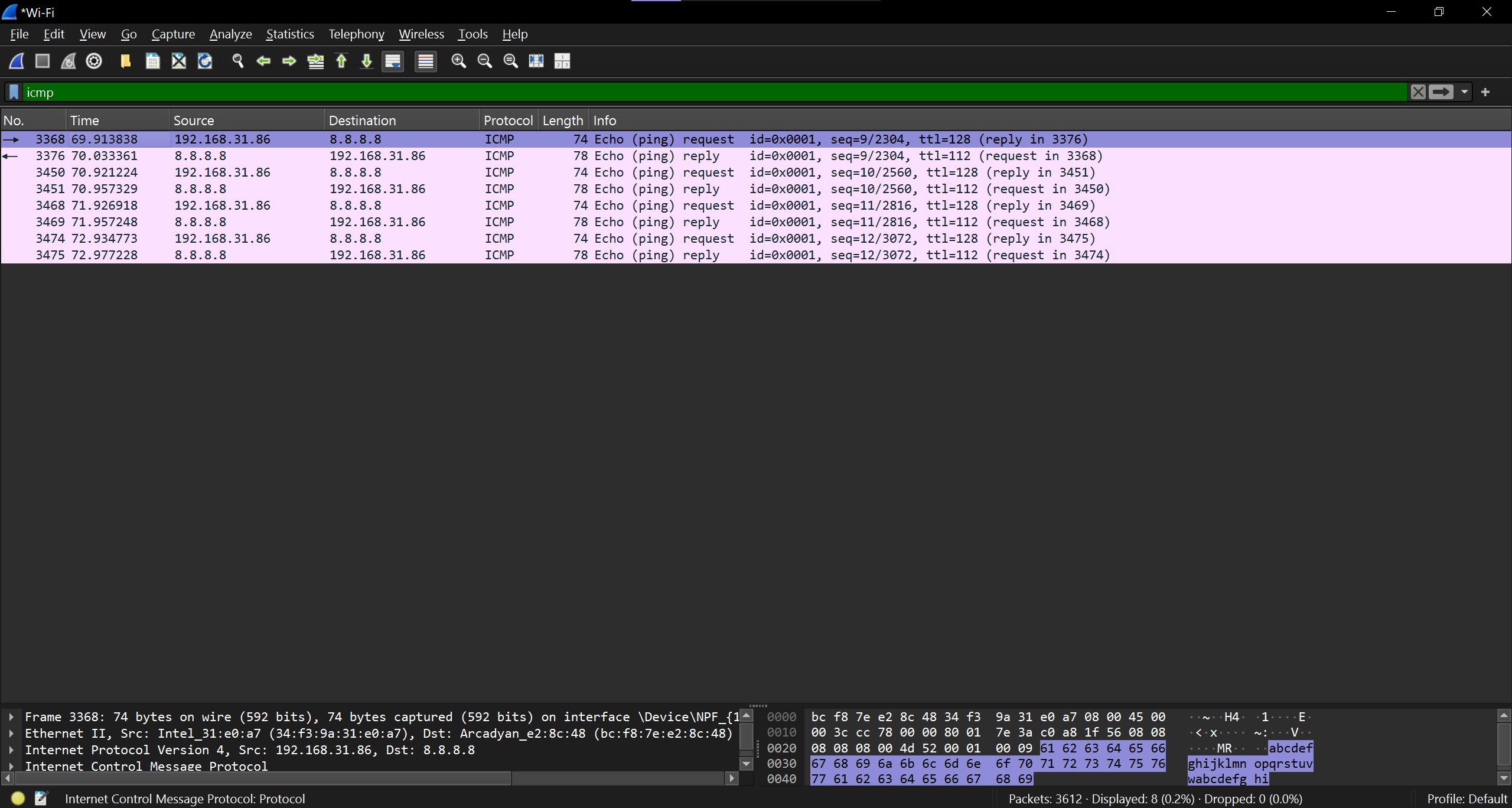
Use Wireshark filters to narrow down traffic:

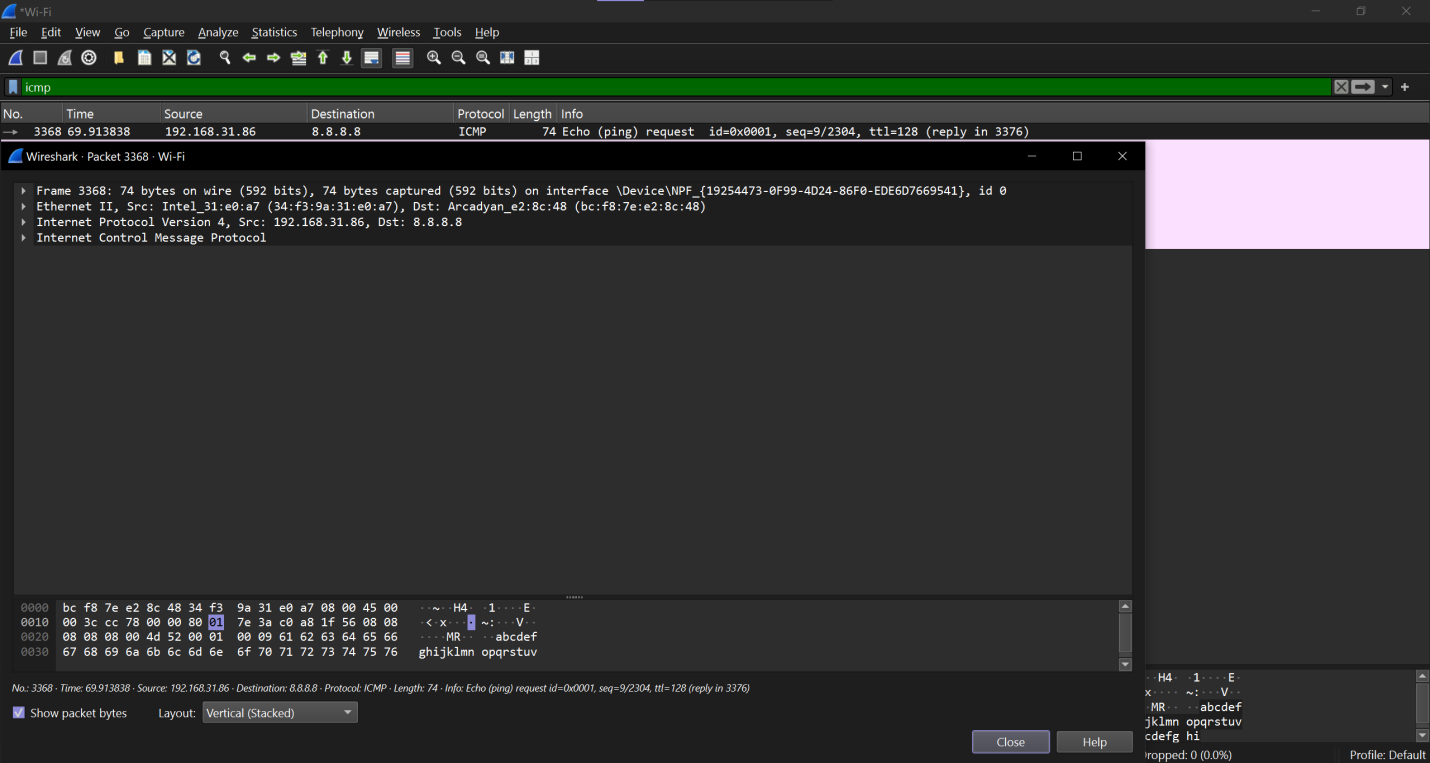
* http → HTTP requests and responses
* dns → Domain name lookups
* icmp → Ping/echo traffic
* tcp or udp → Transport layer protocols

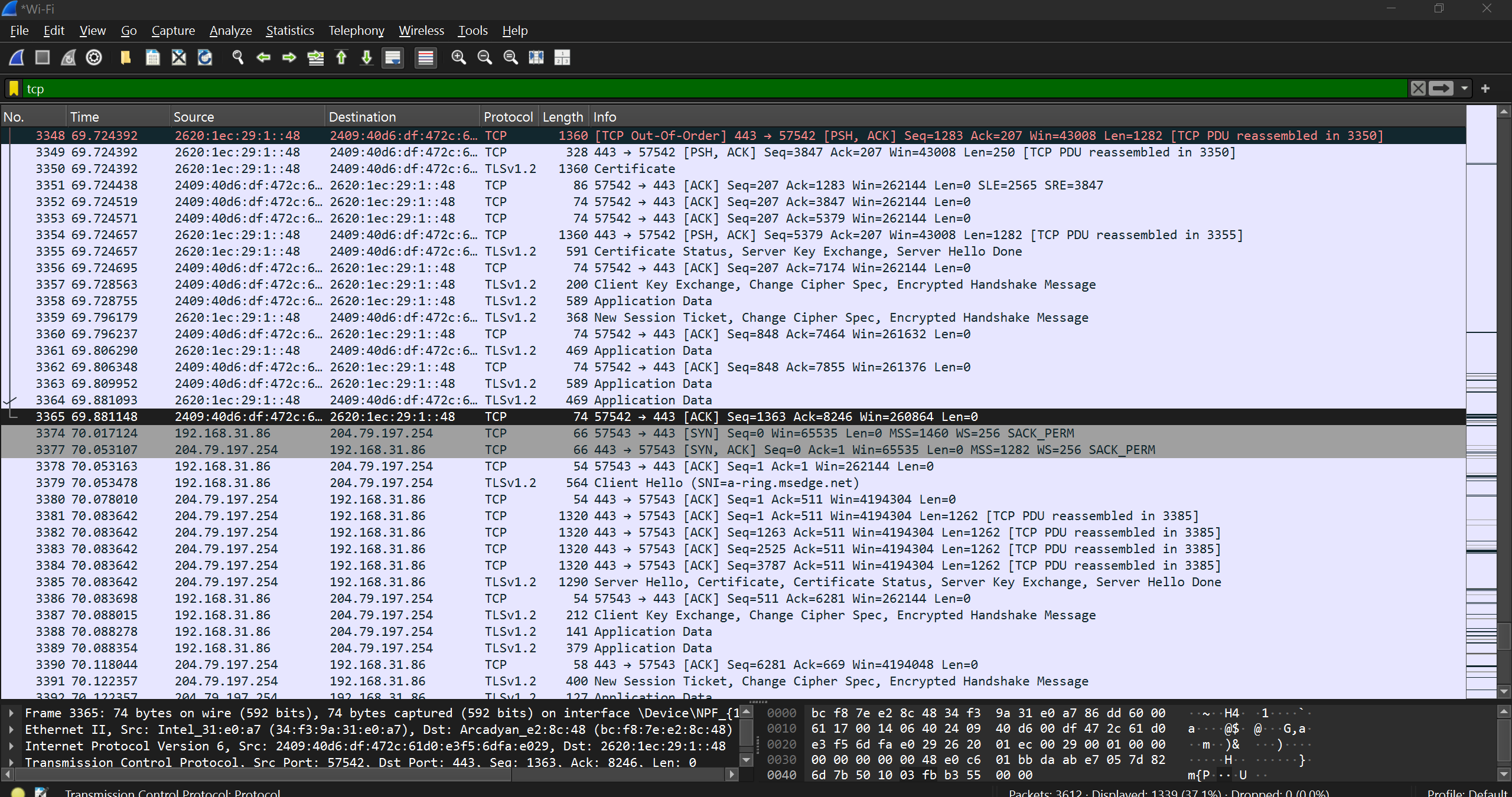


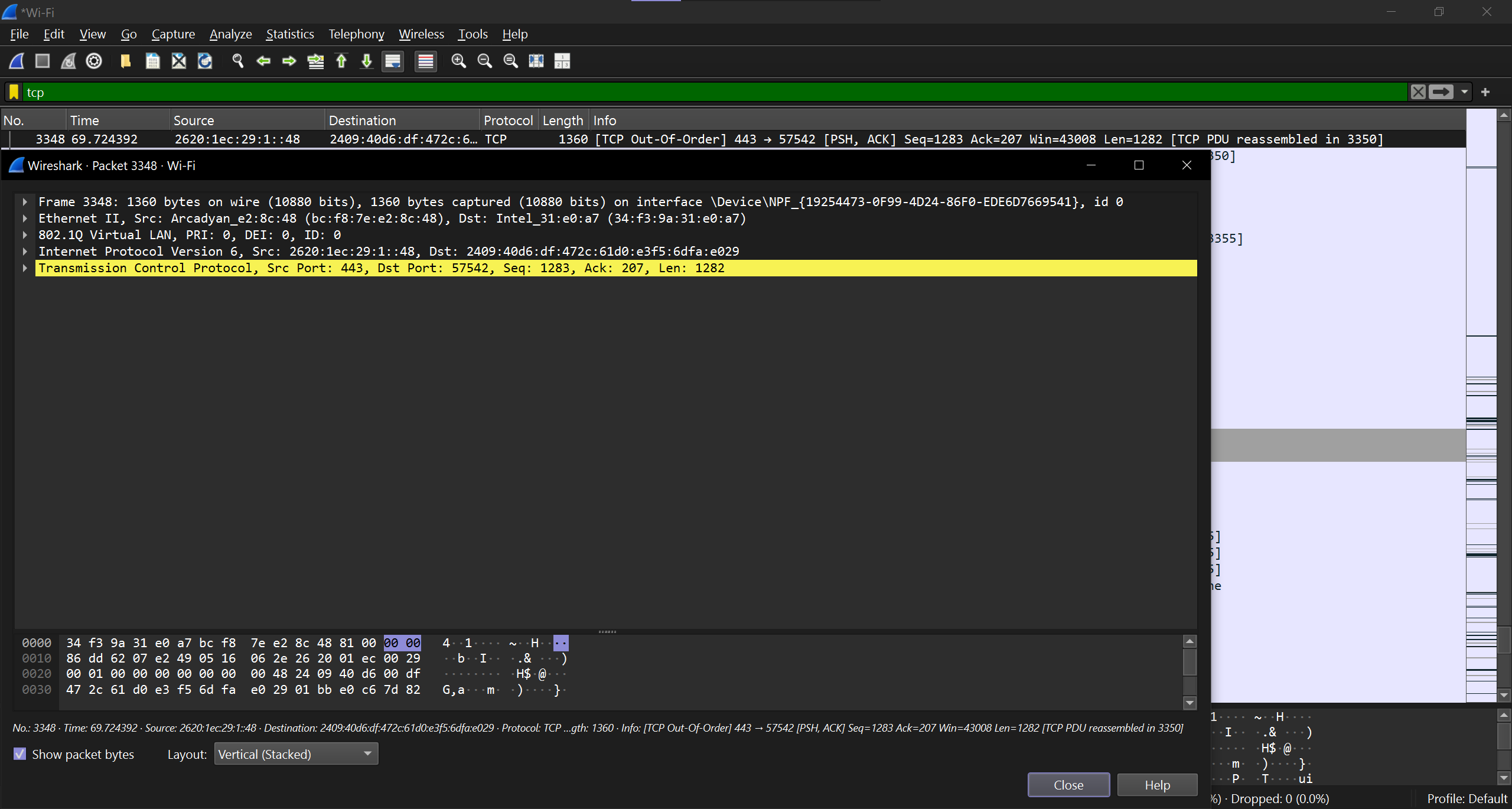












**Findings**

* Traffic captured included DNS lookups and ICMP echo requests.
* These are typical of common browsing and diagnostic activities.
* Each protocol plays a different role: DNS for name resolution and ICMP for connectivity checks.