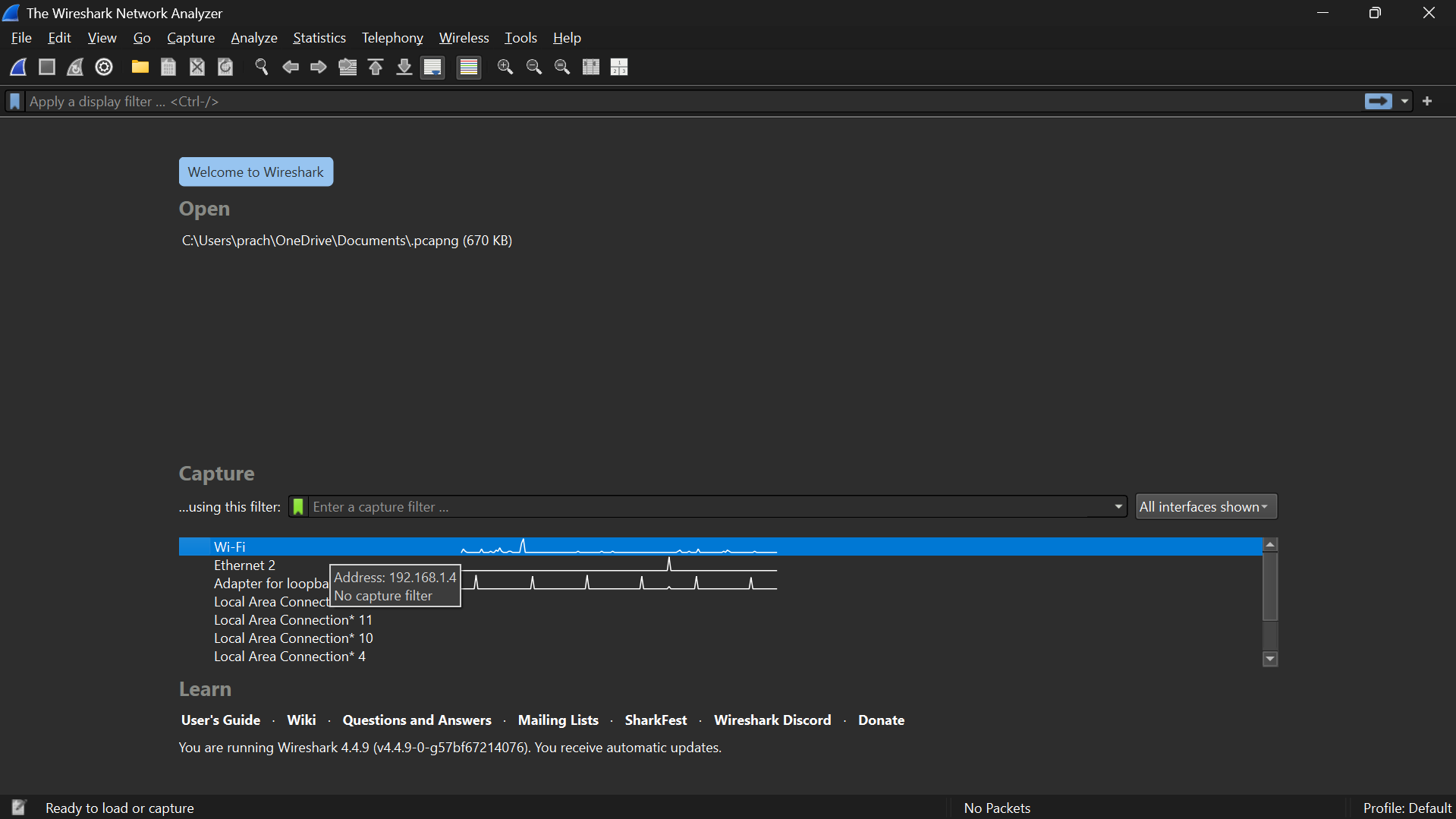
Cyber Security Task-5.

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

--------------------------------------------------------

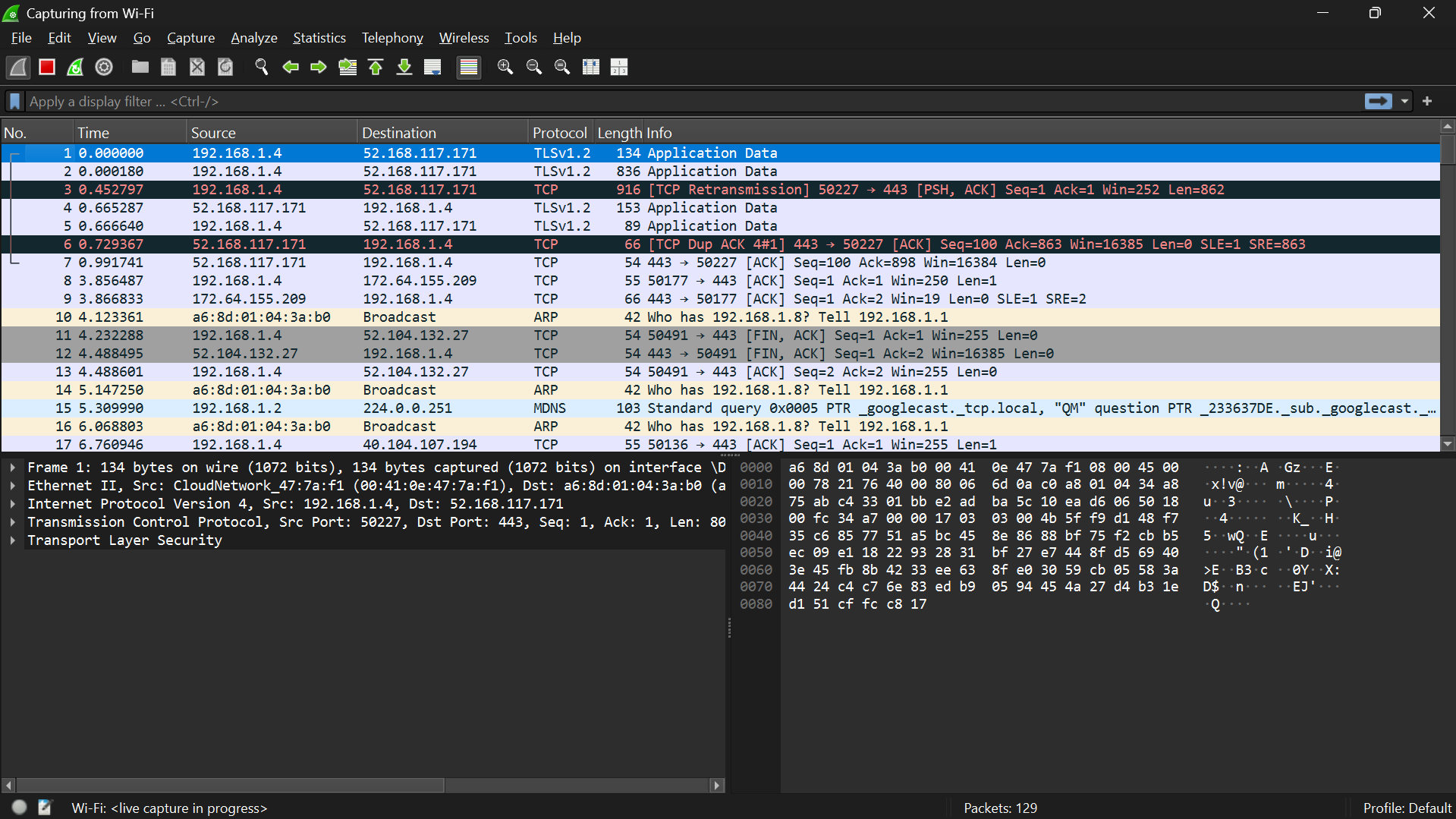
1. Install Wireshark.

I downloaded and installed Wireshark from the official website. After installation, I launched the application, which presented the home screen with a list of available network interfaces.



1. Capturing on the Active Network Interface.

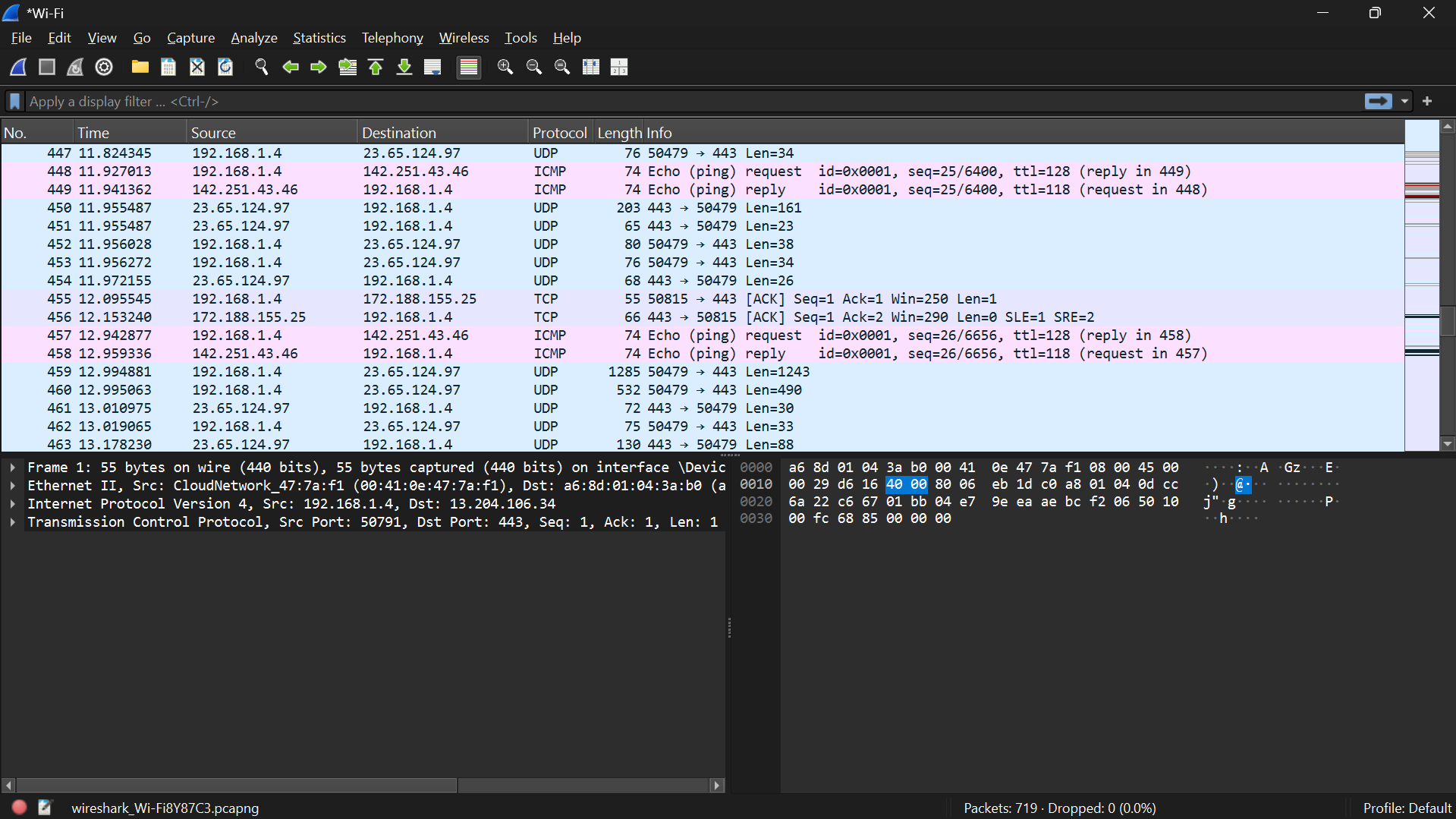
I selected the active network interface (Wi-Fi) and started the capture. Wireshark began recording all network traffic passing through my computer.



-------------------------------------------------------------------------

1. Generating Network Traffic.

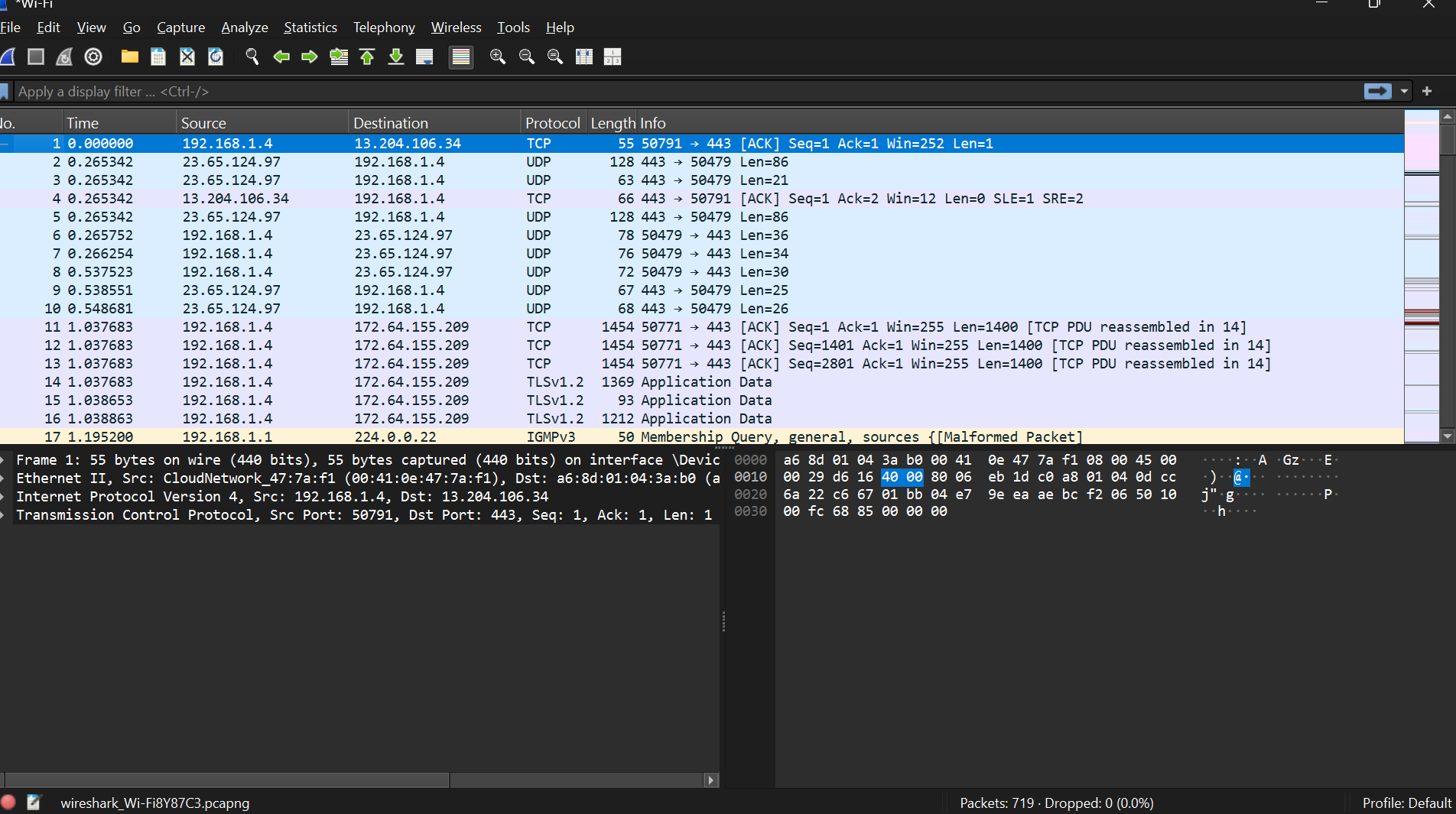
To generate packets, I performed two actions: browsing a website and pinging google.com from the command prompt. This generated HTTP, DNS, and ICMP traffic in the capture.



-------------------------------------------------------------------------

1. Stopping the Capture.

After approximately one minute of capturing traffic, I stopped the session. Wireshark displayed all recorded packets for analysis.



-------------------------------------------------------------------------

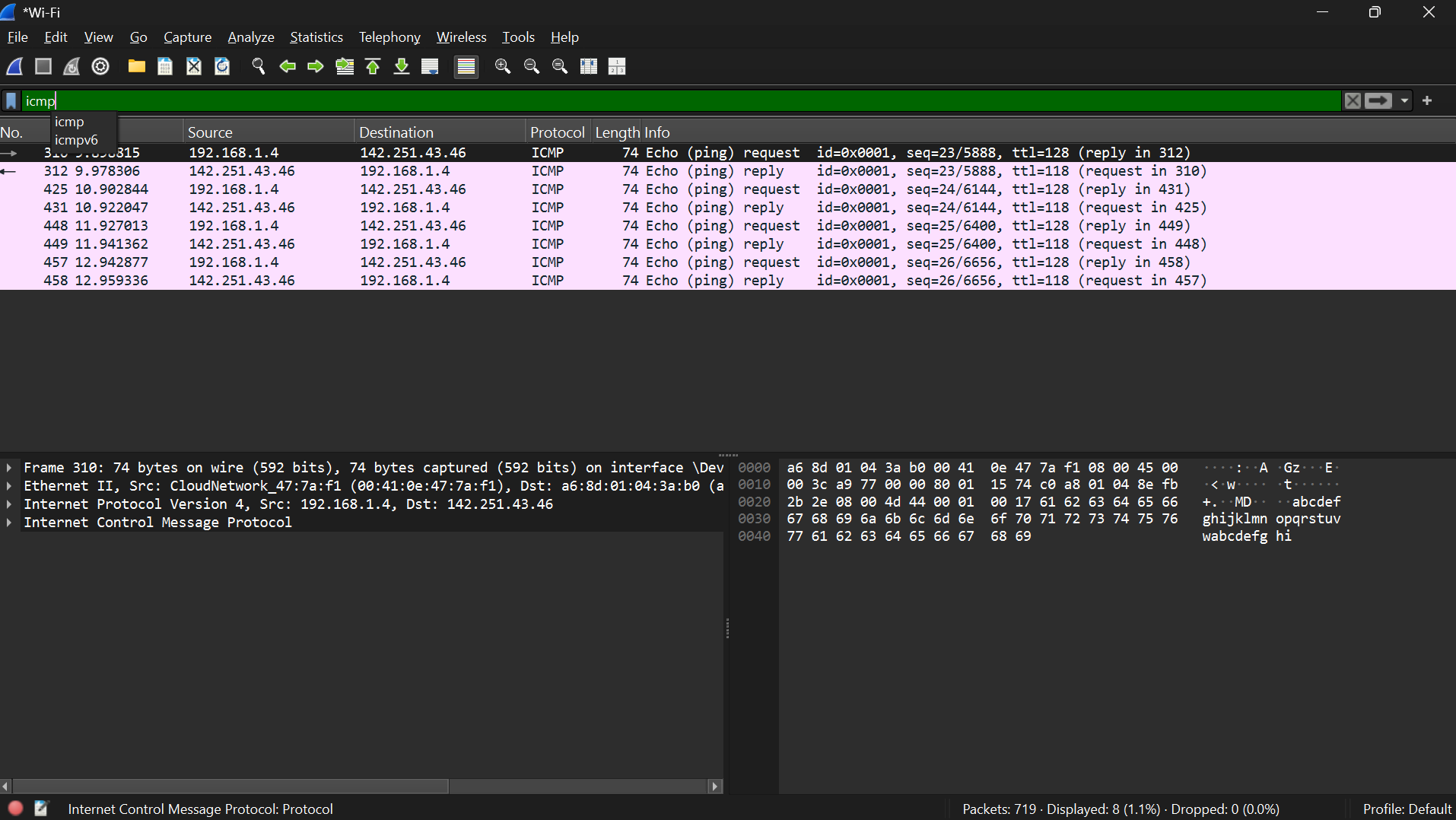
1. Filtering Captured Packets by Protocol.

I used protocol filters to analyze specific traffic types:

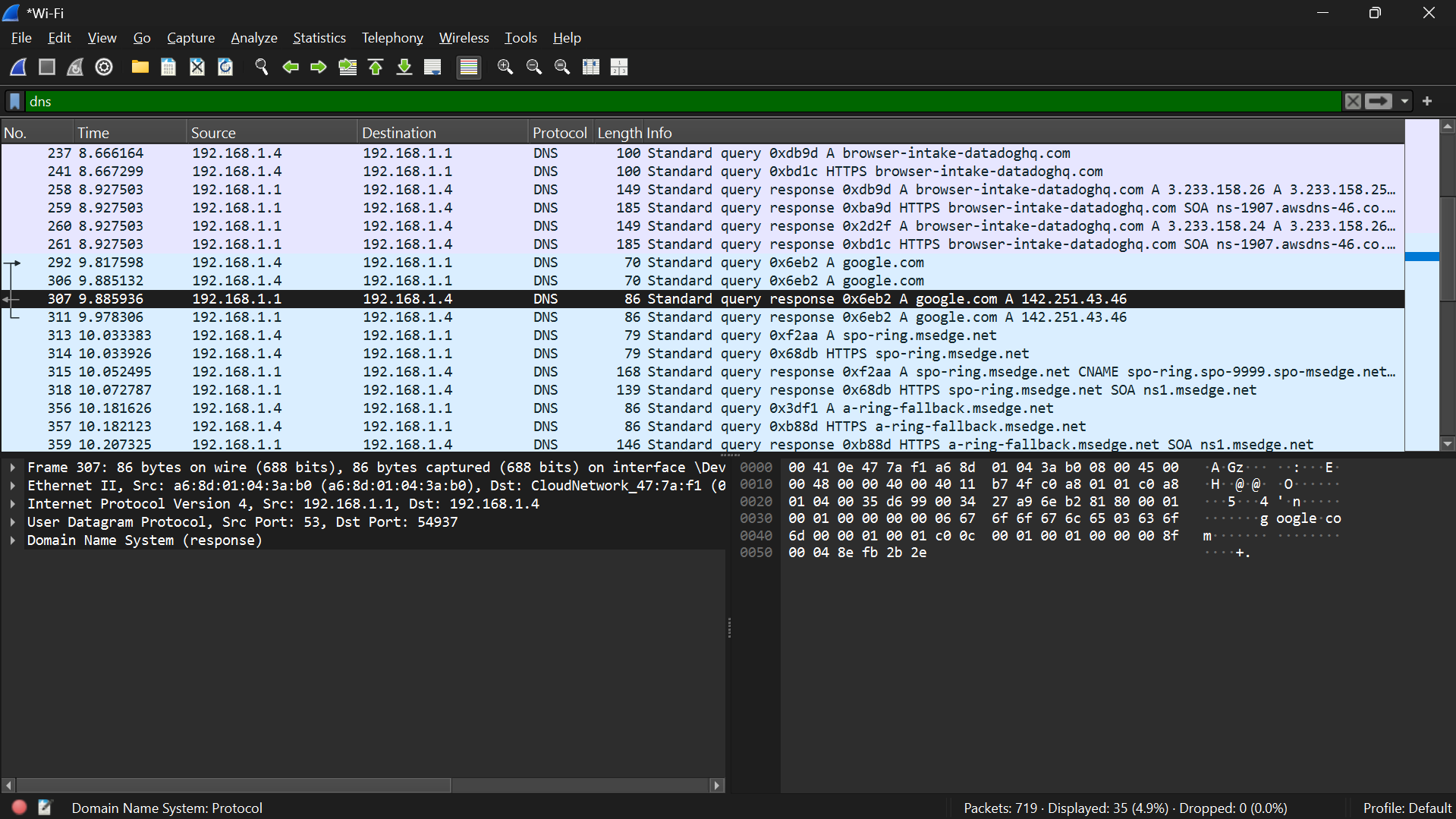
* icmp for ping requests and replies
* dns for domain name resolution queries and responses
* http for web browsing traffic

Filtering helped focus on relevant protocols for better understanding.

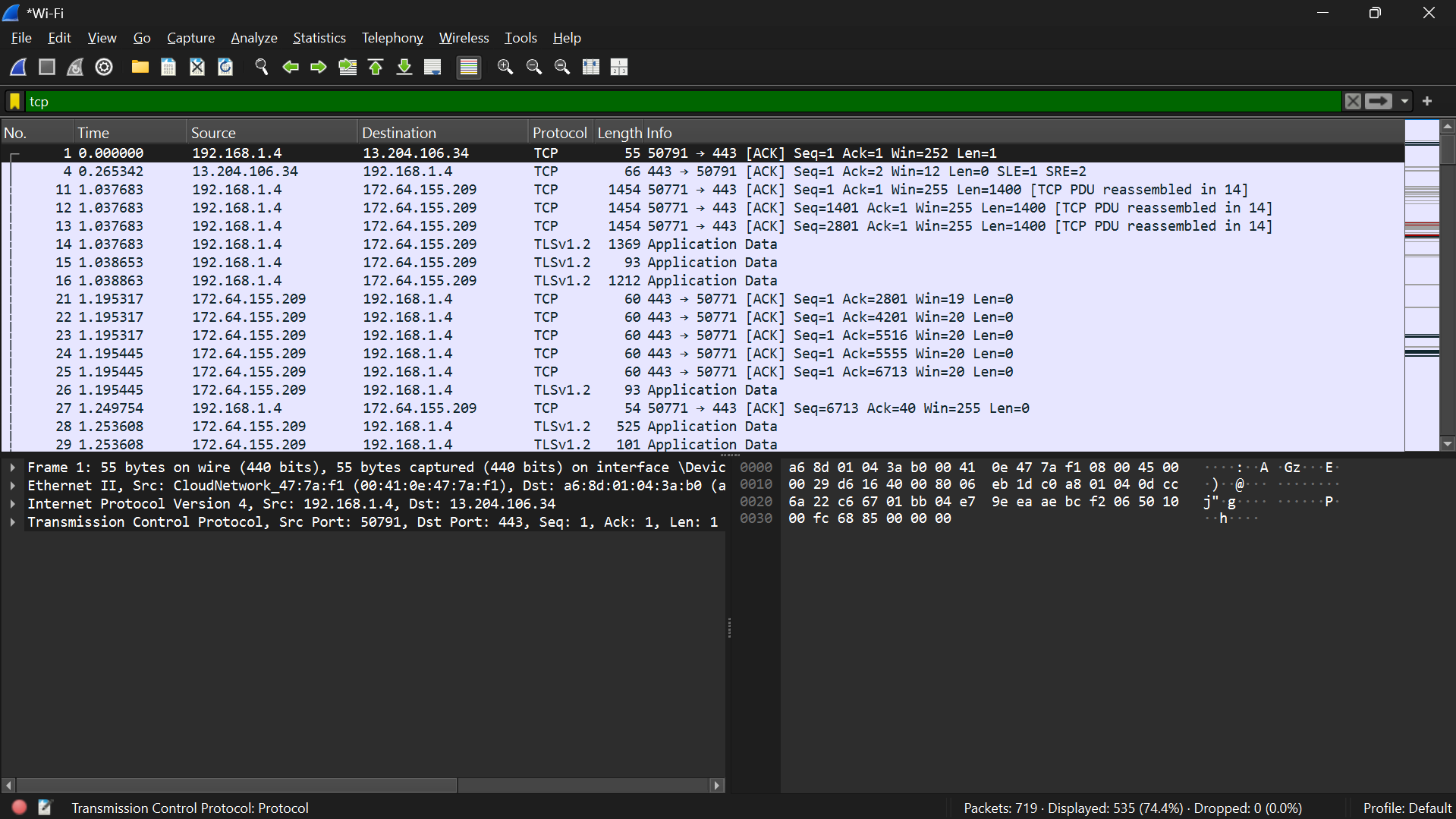
Icmp:



dns:



tcp:



-------------------------------------------------------------------------

1. Identify at least 3 different protocols.

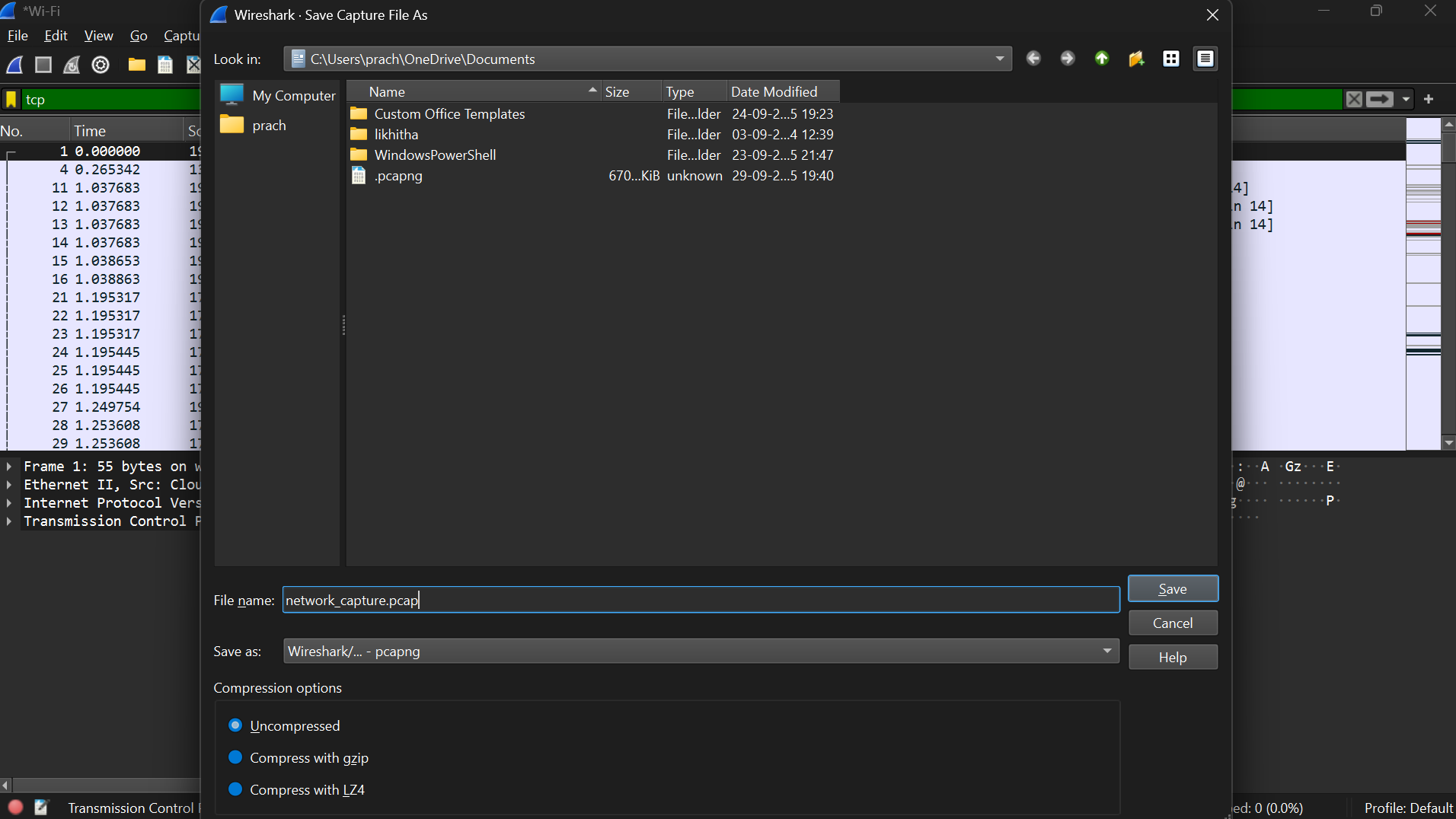
Even using CMD, I observed:

* **ICMP:** Ping requests and replies.
* **DNS:** Queries and responses resolving google.com.
* **TCP:** Some background traffic (for example, system updates or other network connections).

**-**------------------------------------------------------------------------

1. Exporting the Capture.

The entire capture session was exported as a .pcap file by navigating to **File → Save As** and naming it network\_capture.pcap. This file contains all captured packets and can be reopened in Wireshark for further analysis.



-------------------------------------------------------------------------

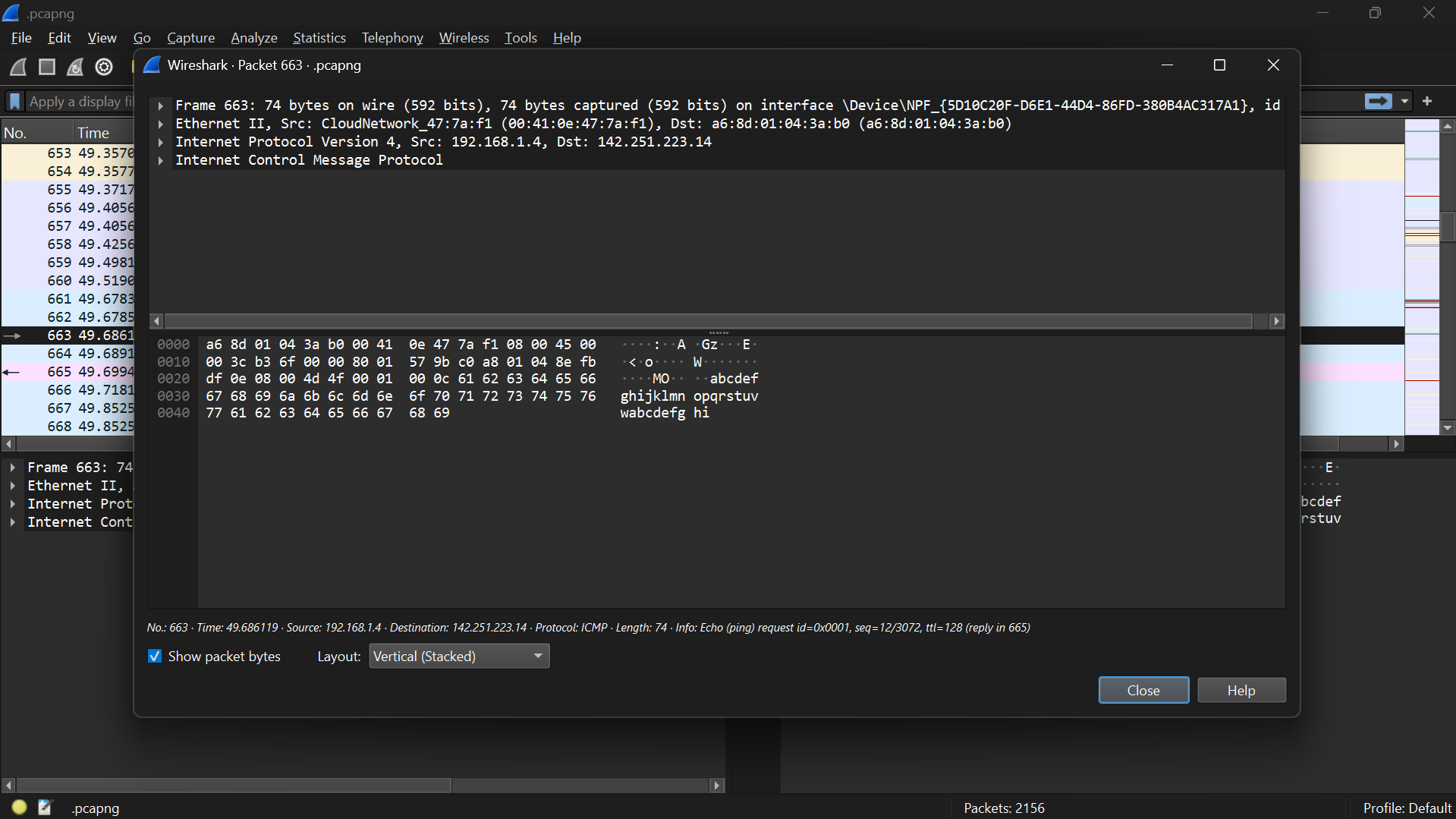
1. Summary of Findings.

The captured traffic illustrates real-time communication between my computer and external servers. Key observations include:

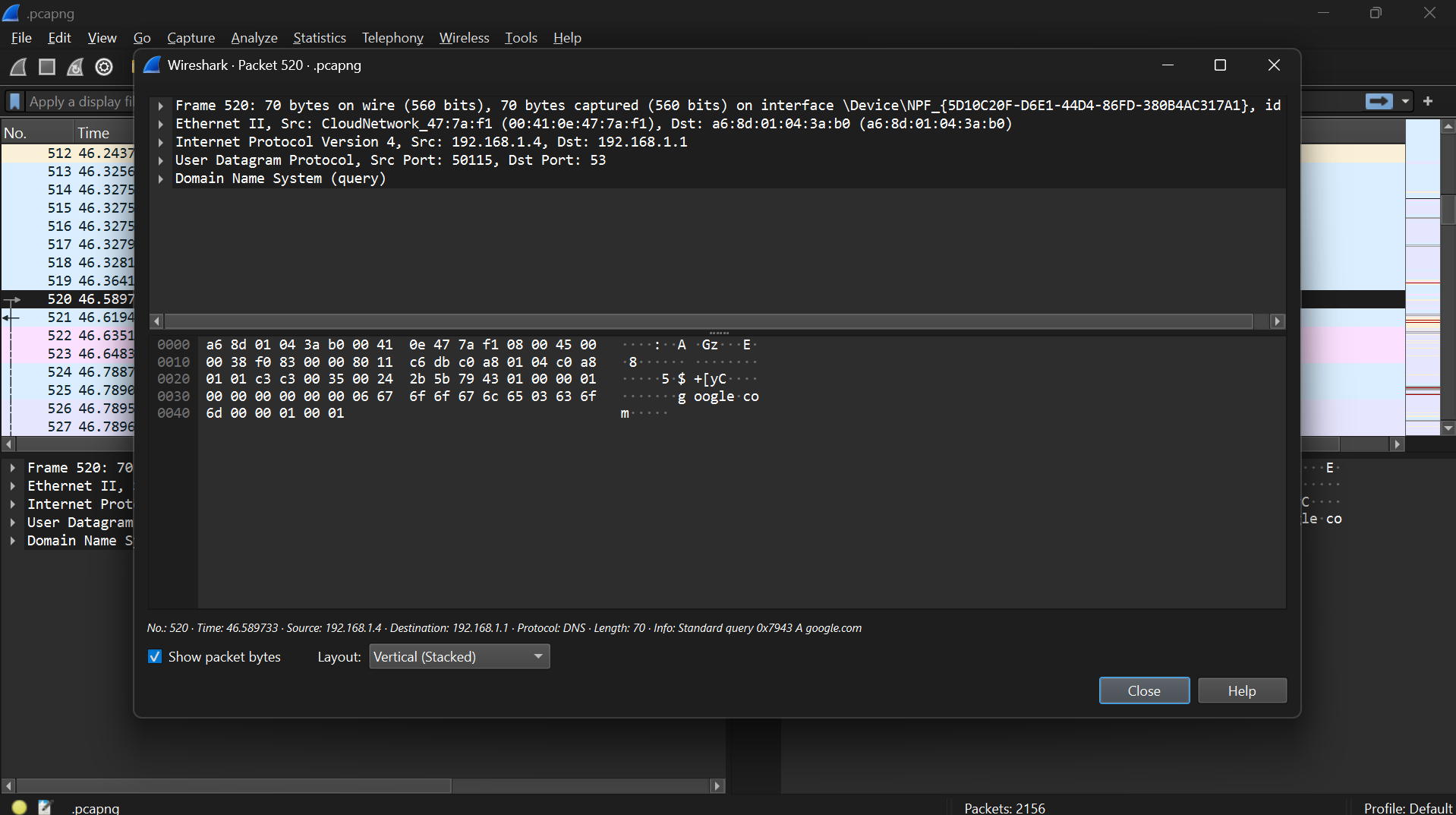
* **ICMP packets:** Confirmed successful network connectivity with response times.
* **DNS packets:** Demonstrated domain resolution, showing the mapping between domain names and IP addresses.
* **HTTP packets:** Revealed web page requests and responses, including source and destination IPs, ports, and other packet details.

Analyzing these packets provided a clear view of network behavior, protocol functions, and traffic patterns. This exercise enhanced my understanding of network protocols and packet analysis using Wireshark.

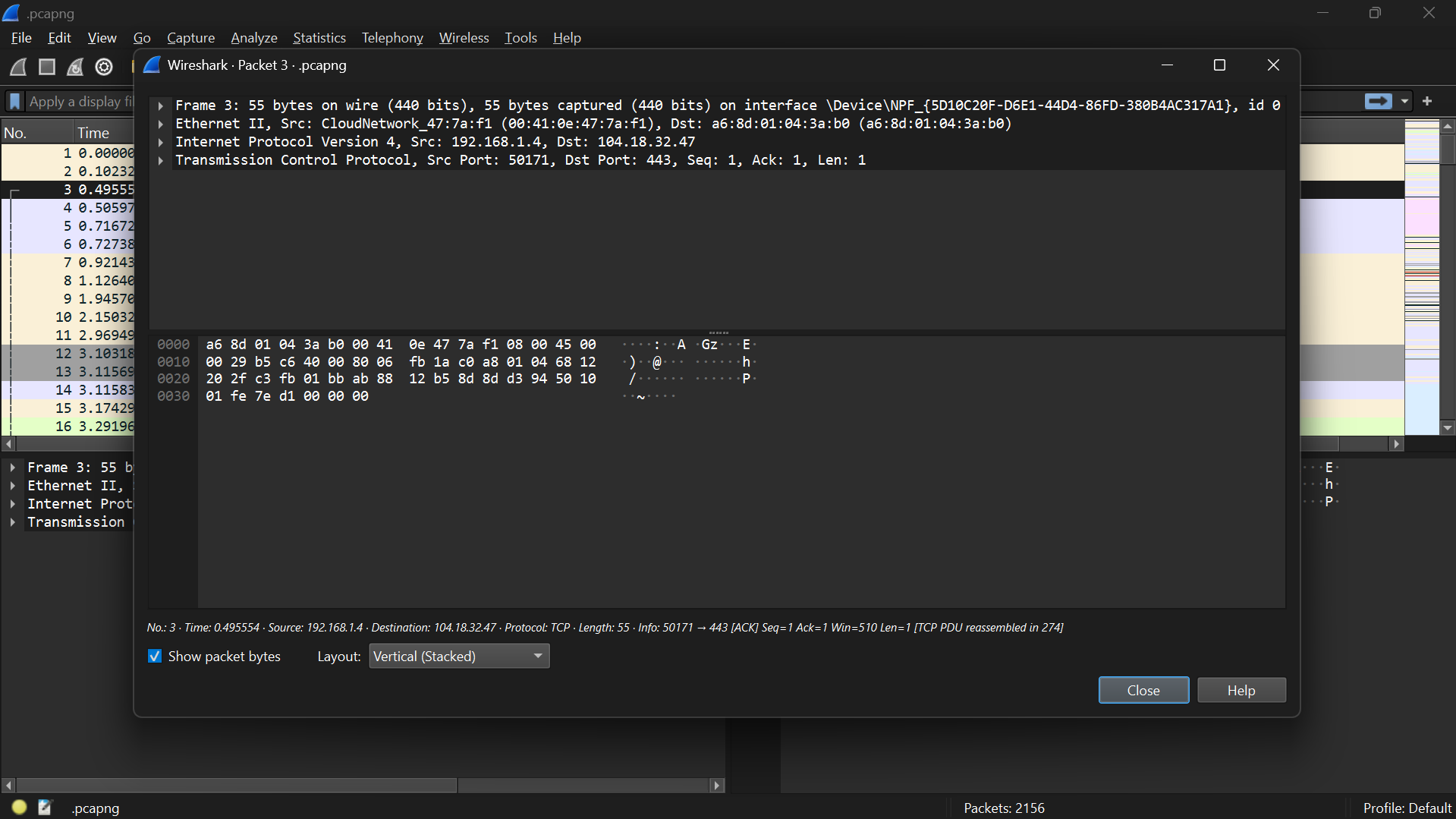
ICMP packet details:



DNS packet details:



TCP packet details:



--------------------------------------------------------