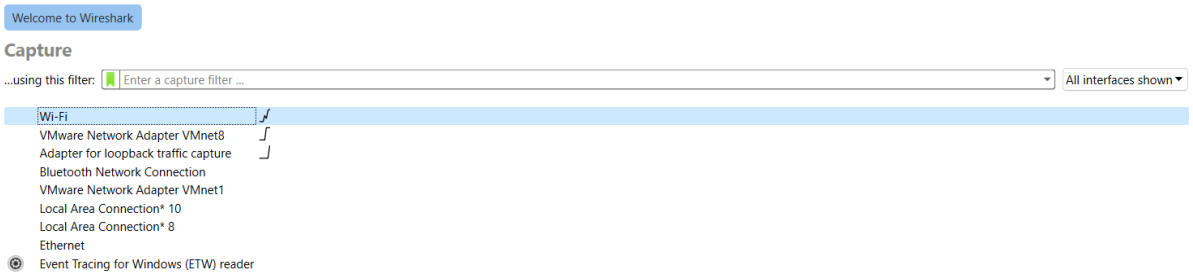
02 Capture and Analyze ICMP (Ping) Traffic in Wireshark

Step 1: Open Wireshark

- Open Wireshark on your computer.
- Select your **Wi-Fi****



**

Step 2: Open Command Prompt or Terminal

- **Windows:** Press `Windows + R`, type `cmd`, and hit Enter.

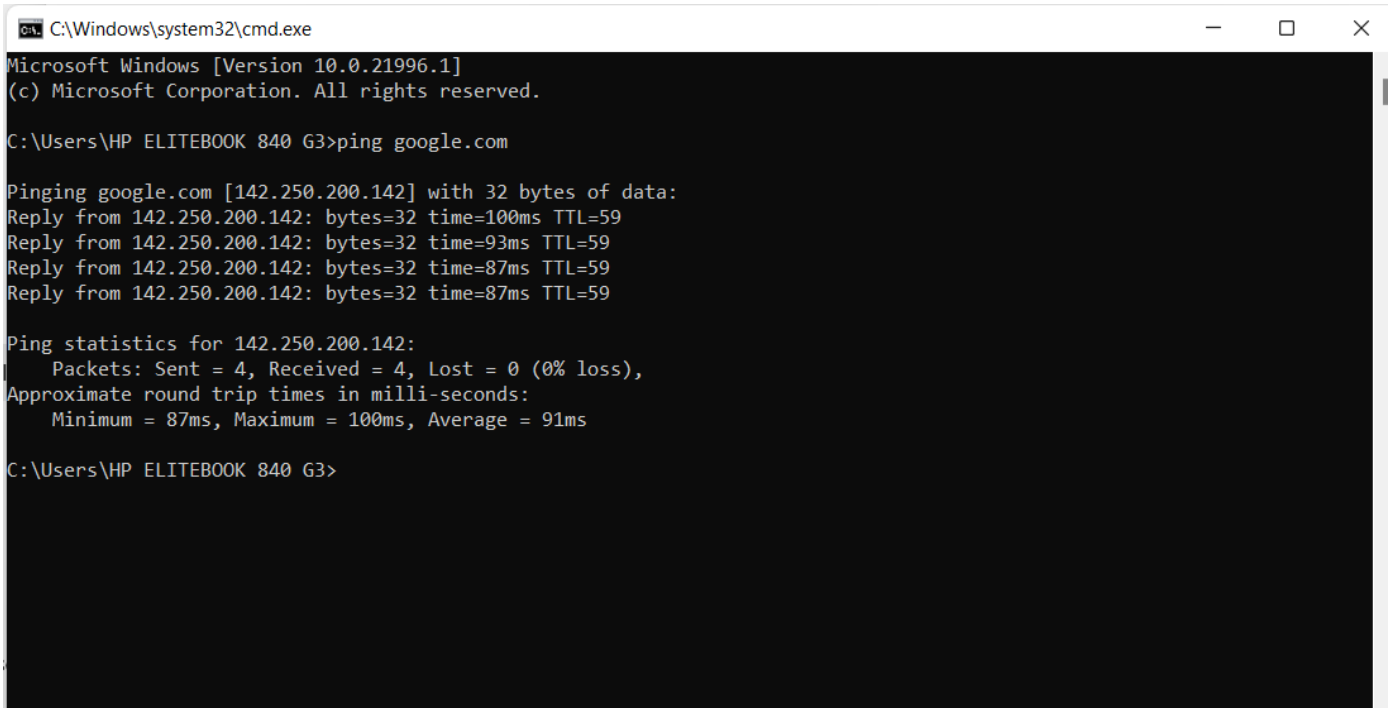
Step 3: Run the Ping Command

In the command prompt or terminal, type:

```
ping google.com
```

and press **Enter**.

This will start sending **ICMP Echo Request** packets to Google's server and getting **ICMP Echo Reply** back.



Step 4: Stop Capturing in Wireshark

- Go back to Wireshark.
- Click the **red square "Stop" button** to stop capturing packets.

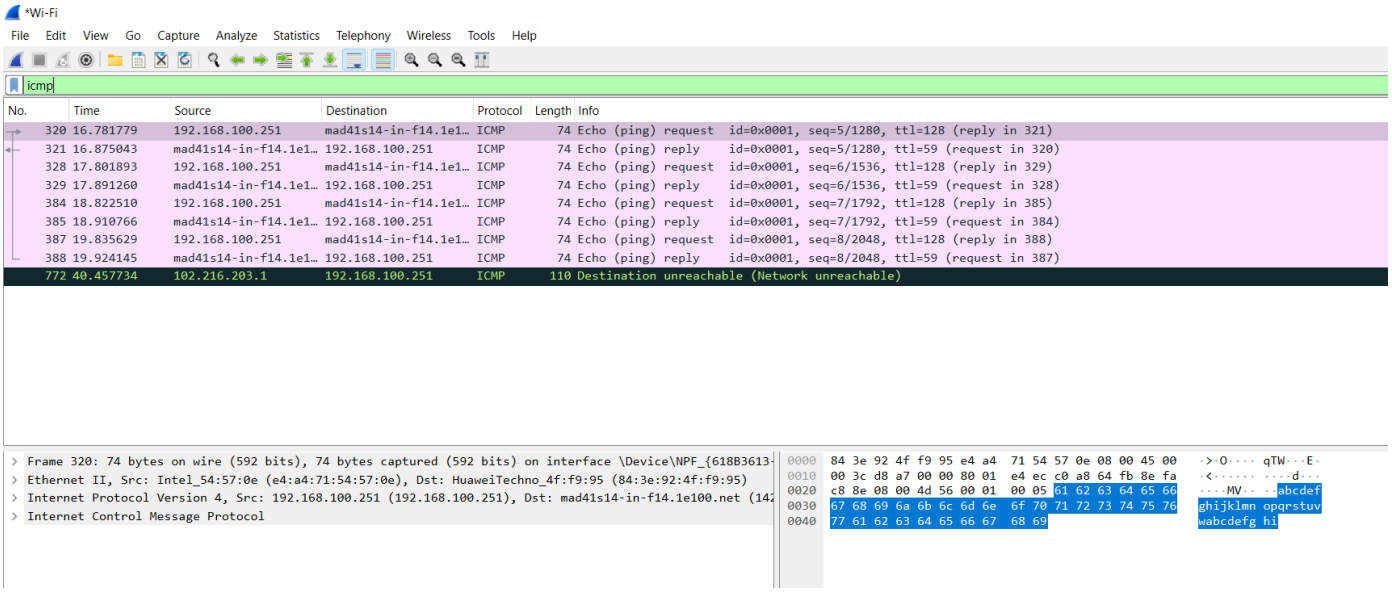
Step 5: Filter for ICMP Packets

- In the Wireshark filter bar at the top, type:

`icmp`

and press **Enter**.

Now, Wireshark will **only show ICMP traffic** (your ping packets).



Step 6: Analyze ICMP Packets

Packet Type	What You Should See
Echo (ping) request	A packet from your computer to `google.com` (Type 8 - Echo Request).
Echo (ping) reply	A packet from `google.com` back to your computer (Type 0 - Echo Reply).

Expand the packet details:

- You will see inside the ICMP section:
  - **Type:** 8 for Request
  - **Type:** 0 for Reply
  - **Identifier** and **Sequence Number** (they match between Request and Reply)