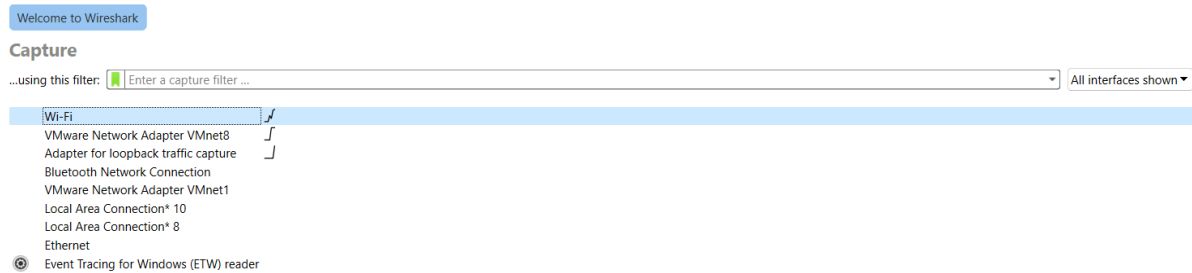


02 Capture and Analyze ICMP (Ping) Traffic in Wireshark

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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP ELITEBOOK 840 G3>ping google.com

Pinging google.com [142.250.200.142] with 32 bytes of data:
Reply from 142.250.200.142: bytes=32 time=100ms TTL=59
Reply from 142.250.200.142: bytes=32 time=93ms TTL=59
Reply from 142.250.200.142: bytes=32 time=87ms TTL=59
Reply from 142.250.200.142: bytes=32 time=87ms TTL=59

Ping statistics for 142.250.200.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 87ms, Maximum = 100ms, Average = 91ms

C:\Users\HP ELITEBOOK 840 G3>
```

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).

The screenshot shows the Wireshark interface with the filter bar at the top set to 'icmp'. The packet list pane displays several ICMP Echo (ping) requests and replies, as well as a 'Destination unreachable' message. The packet details pane shows the structure of an ICMP Echo request, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol fields.

No.	Time	Source	Destination	Protocol	Length	Info
320	16.781779	192.168.100.251	mad41s14-in-f14.1e1...	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 321)
321	16.875043	mad41s14-in-f14.1e1...	192.168.100.251	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=59 (request in 320)
328	17.801893	192.168.100.251	mad41s14-in-f14.1e1...	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 329)
329	17.891260	mad41s14-in-f14.1e1...	192.168.100.251	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=59 (request in 328)
384	18.822510	192.168.100.251	mad41s14-in-f14.1e1...	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 385)
385	18.910766	mad41s14-in-f14.1e1...	192.168.100.251	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=59 (request in 384)
387	19.835629	192.168.100.251	mad41s14-in-f14.1e1...	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 388)
388	19.924145	mad41s14-in-f14.1e1...	192.168.100.251	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=59 (request in 387)
772	40.457734	102.216.203.1	192.168.100.251	ICMP	110	Destination unreachable (Network unreachable)

Step 6: Analyze ICMP Packets

Packet Type	What You Should See
Echo (ping) request	A packet from your computer to <code>google.com</code> (Type 8 - Echo Request).
Echo (ping) reply	A packet from <code>google.com</code> 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)

> Frame 328: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{618B3613-...}

> Ethernet II, Src: Intel_54:57:0e (e4:a4:71:54:57:0e), Dst: HuaweiTechno_4f:f9:95 (84:3e:92:4f:f9:95)

> Internet Protocol Version 4, Src: 192.168.100.251 (192.168.100.251), Dst: mad41s14-in-f14.1e100.net (142...)

> Internet Control Message Protocol

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4d55 [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 6 (0x0006)
- Sequence Number (LE): 1536 (0x0600)
- [\[Response frame: 329\]](#)

> Data (32 bytes)