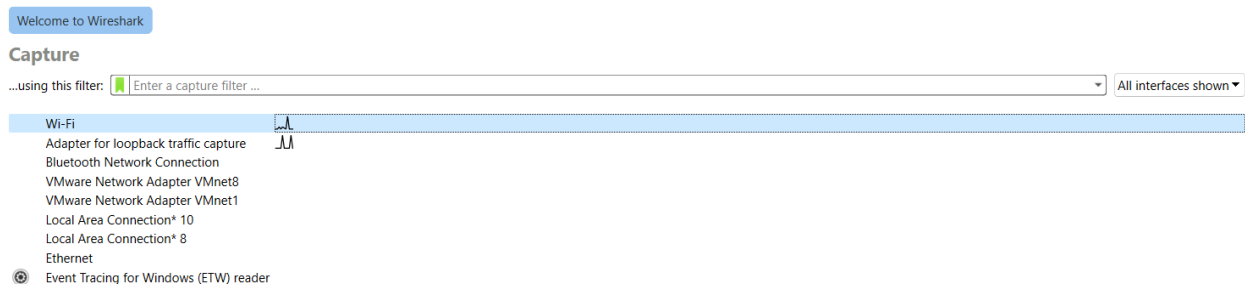


Capture and Analyze the TCP Three-Way Handshake in Wireshark

Step 1: Open Wireshark

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

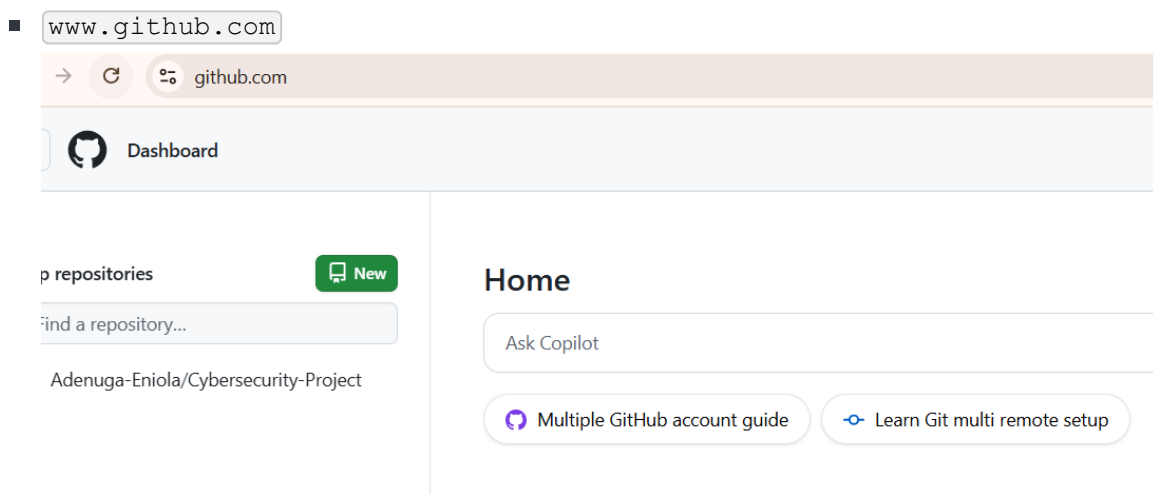


**

Step 2: Open a New Connection

- While Wireshark is capturing, **open a completely new website** that you have not visited recently.

Examples:



Step 3: Stop Capturing

- Once the page loads, go back to Wireshark.
- Click the **red square Stop button** to stop the capture.

■

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

````  
````

Step 4: Filter TCP Packets

````

`tcp`

and press **\*\*Enter\*\***.

Now you will only see TCP packets – much easier!

&nbsp;

  
````

■ Step 4: Find the Three-Way Handshake

Now look carefully:

- Look in the "Info" column for these patterns:

Packet Type	What You Will See
SYN	Something like <code>SYN</code>
SYN-ACK	Something like <code>SYN, ACK</code>
ACK	Something like <code>ACK</code>

Wireshark packet capture showing a TCP three-way handshake. The filter is set to 'tcp'. The packet list shows a SYN packet (No. 5953), a SYN-ACK packet (No. 5979), and an ACK packet (No. 6008). The packet details for the SYN-ACK packet show the 'Info' column with the text '54 [TCP ACKED unseen segment] 49748 -> https(443) [ACK] Seq=1 Ack=2 Win=510 Len=0'.

Step 5: Bonus - Follow the TCP Stream

- Right-click on any TCP request packet.

- Click "Follow" > "TCP Stream".

The image shows a Wireshark interface with a packet capture of a TCP stream. The packet list on the left shows frame 6009 selected. The packet details pane shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII. The packet bytes pane is currently displaying the raw data in hexadecimal.

Wireshark - Follow TCP Stream (tcp.stream eq 7) - Wi-Fi

File Edit View Go Capture Analyze

tcpstream eq 7

No.	Time	Source
6009	7.814593	192.168.100
6027	7.934485	1b-140-82-1
6028	7.934560	192.168.100
6029	7.935505	192.168.100
6030	7.935505	192.168.100
6047	8.052033	1b-140-82-1
6048	8.052236	1b-140-82-1
6049	8.052269	192.168.100
6050	8.052692	1b-140-82-1
6051	8.055756	192.168.100
6052	8.055941	192.168.100
6053	8.056101	192.168.100
6054	8.060300	1b-140-82-1
6055	8.060336	192.168.100
6084	8.182423	1b-140-82-1
6085	8.182423	1b-140-82-1
6086	8.182423	1b-140-82-1
6087	8.182423	1b-140-82-1

> Frame 6009: 66 bytes on wire (5
> Ethernet II, Src: Intel_54:57:0
> Internet Protocol Version 4, Sr
> Transmission Control Protocol,

20 client pkts, 113 server pkts, 13 turns.

Entire conversation (144 KB)

Show data as ASCII

Stream 7

Find:

Find Next

Filter Out This Stream Print Save as... Back Close Help

ed: 0 (0.0%) Profile: Default