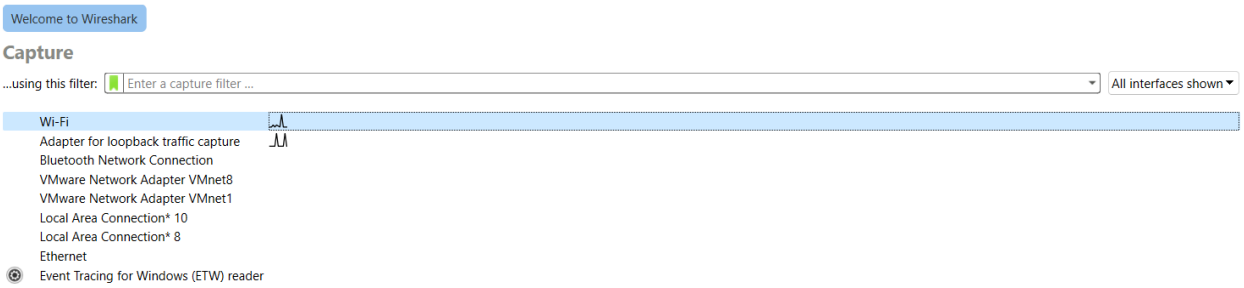
Capture and Analyze the TCP Three-Way Handshake in Wireshark

Step 1: Open Wireshark

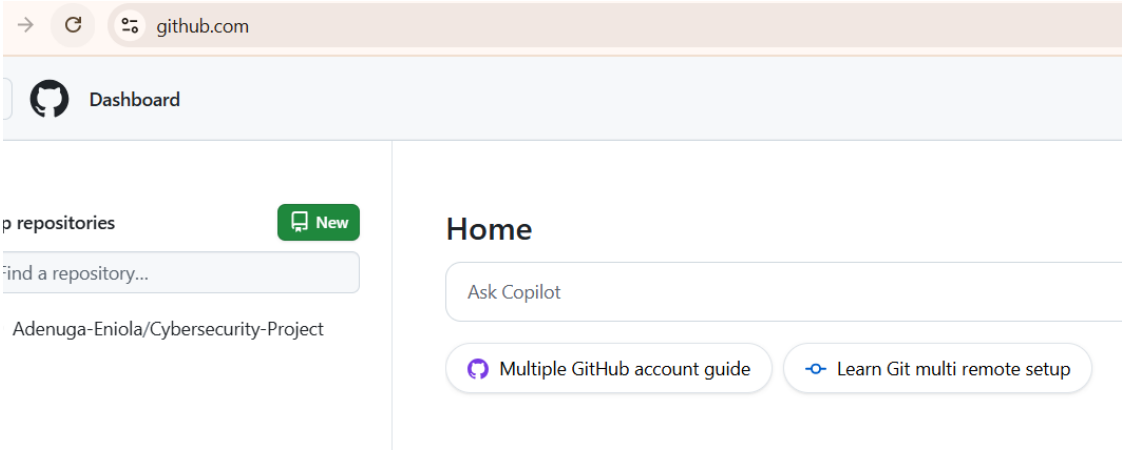
- Open Wireshark.
- Select your **Wi-Fi****



**

Step 2: Open a New Connection

- While Wireshark is capturing, **open a completely new website** that you have not visited recently.
  Examples:
  - `www.github.com`



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!

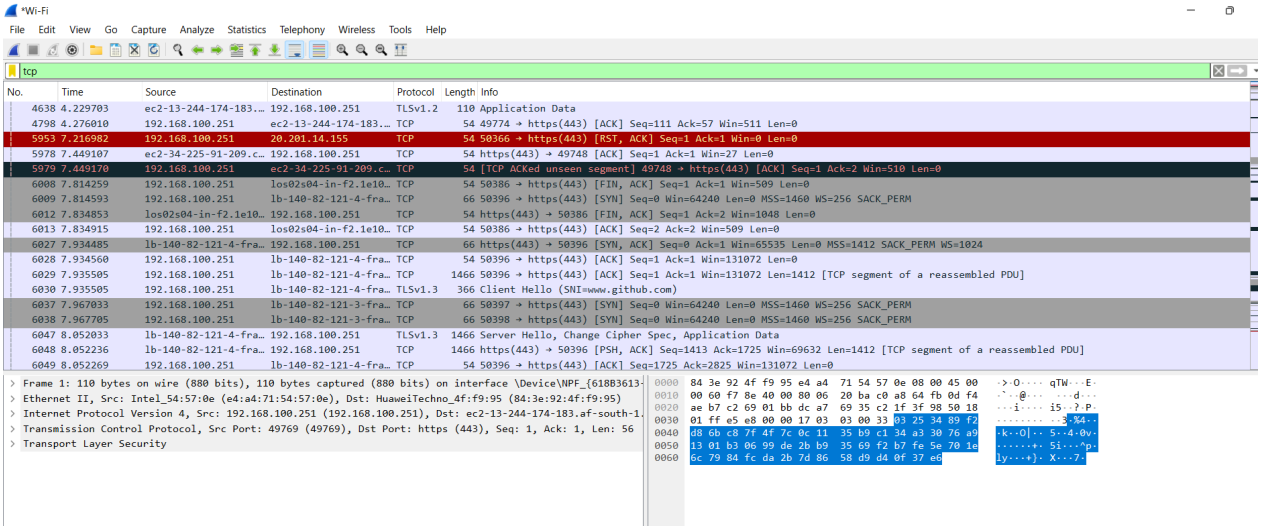
<img src="_resources/8c8594dd34b54005b220519befee7229.png"
alt="b9f85a27f99765a92fe76a2eac3bf9b0.png" width="578"
height="259" class="jop-noMdConv">
````

- ## 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 `SYN` |
| SYN-ACK | Something like `SYN, ACK` |
| ACK | Something like `ACK` |




### Step 5: Bonus - Follow the TCP Stream

- Right-click on any TCP request packet.
````

- Click **"Follow" > "TCP Stream"**.