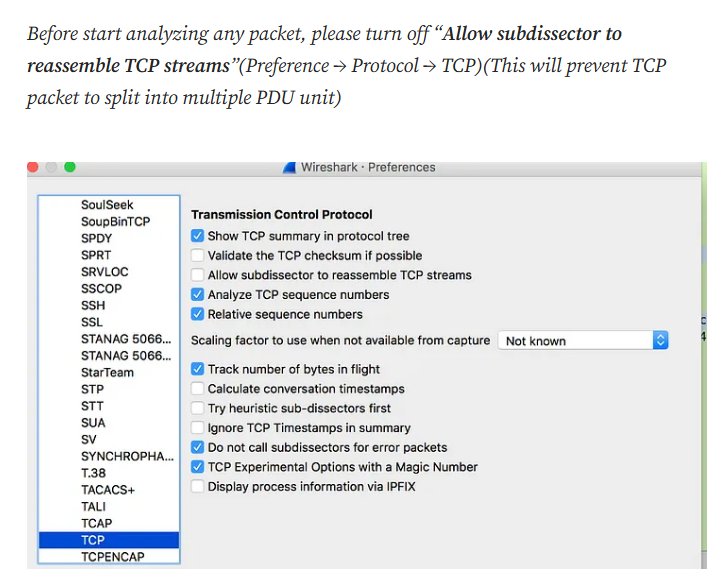
<https://youtu.be/cQ6RsLhJCP4?si=78lPQv4zpm4lvla5>

  
  
sudo apt update  
sudo apt upgrade  
sudo apt dist-upgrade  
Step 1: Start

* Begin by installing Wireshark, a tool used to analyze network traffic.

Step 2: Install Wireshark

* Open the terminal on your Ubuntu system. This is where you type commands to interact with your computer's operating system.
* To install Wireshark, which helps us capture and analyze network traffic, type the following command:

Copy code

**sudo apt install wireshark**

* After typing the command, press Enter. You may be prompted to enter your password. When typing your password, you won't see anything on the screen, but it's still registering your input. After entering your password, press Enter again.
* The installation will begin. Follow the prompts on the screen. Type "Y" and then press Enter when asked if you want to continue with the installation.

Step 3: Start Wireshark

* Now that Wireshark is installed, type the following command in the terminal to start it:

Copy code

**sudo tcpdump -i eth0 -w http\_traffic.pcap 'port 80'**

* Again, you may need to enter your password. This command opens Wireshark with administrative privileges, allowing us to capture network traffic.

Step 4: Analyze the Difference Between HTTP vs HTTPS

* In Wireshark, we can analyze the difference between unencrypted HTTP and encrypted HTTPS traffic.
* HTTP typically uses port 80, while HTTPS uses port 443.

Step 5: Capture HTTP and HTTPS Traffic

* To capture HTTP traffic, we use a tool called **tcpdump**. Let's capture HTTP traffic first:

Copy code: **sudo tcpdump -i eth0 -w https\_traffic.pcap 'port 443'**

* + Replace **eth0** with the name of your network interface. This command captures HTTP traffic on port 80 and saves it to a file named **http\_traffic.pcap**.
* To capture HTTPS traffic, use a similar command, but for port 443:

Copy code

**sudo tcpdump -i eth0 -w https\_traffic.pcap 'port 443'**

* + This command captures HTTPS traffic on port 443 and saves it to a file named **https\_traffic.pcap**.

Step 6: View Server Output

* After capturing traffic, we can open the captured files in Wireshark to analyze them.
* To view the HTTP traffic, use the following command:

Copy code

**wireshark -r http\_traffic.pcap**

* Similarly, to view the HTTPS traffic, use this command:

Copy code

**wireshark -r https\_traffic.pcap**

* These commands open Wireshark and load the respective captured traffic files for analysis.

Step 7: Stop

* After analyzing the traffic, you can close Wireshark by simply closing its window. Additionally, you can stop capturing packets by pressing Ctrl+C in the terminal window where **tcpdump** is running.