TTHP Operational Architect

Designing efficiency, delivering success: Your operational architect.

LAB Capture and view network traffic

the process of capturing and viewing network traffic is often used in network troubleshooting, security analysis, and understanding network performance. There are various ways to do this, and one of the most common ways is to use a free and open-source tool called Wireshark.

Here are the steps to capture and view network traffic with Wireshark:

Step 1: Install Wireshark Wireshark is a free and open-source packet analyzer. You can download it from its official website. Be sure to download the version compatible with your operating system. After downloading the installer, run it, and follow the prompts to install Wireshark.

Step 2: Launch Wireshark Open Wireshark. You will see a simple interface with a list of the network interfaces on your computer.

Step 3: Select a Network Interface to Monitor In the Wireshark interface, you will see a list of network interfaces. Select the one through which the traffic you want to capture will go through. Usually, it's your main ethernet or wireless interface.

Step 4: Start Capturing Packets Click on the 'Start' button or double click the interface to start capturing packets on that interface. This will open a new window that starts to list all the packets being transmitted or received through the interface.

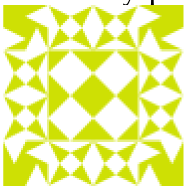
Step 5: Stop Capturing Packets When you think you've captured what you want, you can stop Wireshark from capturing more packets. Click on the 'Stop' button in the toolbar (or under the 'Capture' menu option) to stop the capture.

Step 6: Analyzing the Captured Packets You will now see a list of packets captured. Each packet displays the time it was captured, the source and destination IP addresses, the protocol used, the length of the packet, and information about the packet. Clicking on a packet will display more detailed information in the two sections below the packet list.

Step 7: Using Filters To help with analysis, Wireshark includes a powerful filtering language. At the top of the window is a filter bar where you can enter filter expressions. For example, typing "tcp" will display only packets that use the TCP protocol.

Step 8: Saving the Capture If you want to save the capture for future analysis or to share with others, go to 'File' > 'Save As' and give the capture a name. It will be saved with a .pcapng extension and can be opened later for further analysis.

Capturing network traffic may include sensitive data (like passwords) and can have legal implications, especially if the network is not owned by you. Always ensure you have the necessary permissions and legal rights to capture network traffic in any network environment.



Published by rhondamelo21

View all posts by rhondamelo21

June 11, 2023
Uncategorized

BLOG AT WORDPRESS.COM.

UP ↑