
Wireshark Quick Start Guide: Your First Packet Capture & Basic Commands

Goal: Get up and running with Wireshark and capture your first packets, plus learn essential commands for quick analysis.

Before You Begin Your Capture:

- **Install Wireshark:** Ensure that Wireshark is correctly installed on your laptop or device.
- **Identify Your Goal:** What are you trying to observe or troubleshoot? (e.g., "Is my computer connecting to a specific website?", "Why is my network slow?", "What's this device doing?").
- **Choose the Right Interface:**
    - **Ethernet:** Select your wired network adapter (e.g., Ethernet, en0, eth0).
    - **Wi-Fi:** Select your wireless adapter (e.g., Wi-Fi, wlan0, en1).
    - **Loopback:** Use Loopback or lo0 for traffic generated on your local machine (e.g., testing local applications).
    - *Tip: Look for the interface with the most active traffic (green graph).*

Capturing Packets:

1. **Start Capture:**
    - Click the **blue shark fin icon** (usually top left) or go to Capture > Start.
    - *Tip: Wireshark will immediately start collecting all traffic on the selected interface.*
2. **Perform Your Action:**
    - Do the specific action you want to capture (e.g., open a website, ping a server, launch an application).
3. **Stop Capture:**
    - Click the **red square icon** (usually located in the top left corner) or go to Capture > Stop.
    - *Tip: Stopping the capture limits the amount of data you have to sift through.*
4. **Save Your Capture (Optional, but Recommended):**
    - Go to File > Save As...
    - Choose a descriptive filename (e.g., MyAppTrouble_2025-06-26.pcapng).
    - Select .pcapng as the file type (the modern default, which preserves more information).

Basic Commands & Filters (Display Filters):

Use the **Display Filter Bar** (located at the top, above the packet list) to narrow down what you see quickly. Hit Enter after typing a filter.

- **See All Traffic To/From an IP Address:**
  - ip.addr == 192.168.1.1 (Replace with your desired IP)
- **See Traffic To a Specific IP Address:**
  - ip.dst == 192.168.1.1
- **See Traffic From a Specific IP Address:**
  - ip.src == 192.168.1.1
- **Filter by Port Number:**
  - tcp.port == 80 (For HTTP web traffic)
  - udp.port == 53 (For DNS traffic)
- **Filter by Specific Protocol:**
  - http (Web requests and responses)
  - DNS (Domain Name System queries/responses)
  - icmp (Ping messages)
  - ARP (Address Resolution Protocol)
  - dhcp (Dynamic Host Configuration Protocol)
- **Combine Filters (AND / OR):**
  - ip.addr == 192.168.1.1 and tcp.port == 443 (Traffic to/from IP AND port 443)
  - http or dns (Either HTTP OR DNS traffic)
- **Exclude Traffic (NOT):**
  - !icmp (Show everything *except* ICMP traffic)
- **Finding Specific Text (Case-Insensitive):**
  - Frame contains "example.com" (Searches entire packet for text)
- **"Follow TCP Stream" (Powerful!):**
  - Right-click on a **TCP packet** in the packet list.
  - Select Follow > TCP Stream. This will display the entire conversation between two devices.

Quick Troubleshooting Tips:

- **No packets showing up?** Double-check that you selected the correct network interface.
- **Too much noise?** Start with a specific filter right away (e.g., host 192.168.1.1 as a *capture filter* before you hit start) to limit the data collected.
- **Looking for delays?** Pay attention to the "Time" column in the packet list.

Keep Exploring! Wireshark is incredibly powerful. This guide gets you started, but there's always more to learn!
