

# Wireshark

Command-line packet analyzer

Linux, macOS, Windows (via WinDump)

Quick capture and filtering of packets

Text output or .pcap files

System/network administrators, security analysts comfortable with CLI

# tcpdump

Graphical packet analyzer

Linux, macOS, Windows

In-depth packet inspection and visualization

Graphical display of .pcap files

Network engineers, analysts, learners who prefer GUI

## Similarities

- Network protocol analyzers

Open source and free