Wireshark Documentation

Introduction

Wireshark is a widely-used network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network. It is an essential tool for network troubleshooting, analysis, software development, and security auditing.

Features

- Deep inspection of hundreds of protocols.
- Live capture and offline analysis.
- Standard three-pane packet browser.
- Rich display filters to isolate relevant traffic.
- Coloring rules for intuitive packet analysis.
- Ability to read/write in multiple capture file formats.
- Exporting data for reports and further analysis.
- VoIP analysis and decryption support (with appropriate keys).

Installation

Wireshark is available for Windows, macOS, and Linux.

Windows/macOS:

1. Download from https://www.wireshark.org/download.html
2. Follow the installation wizard.

Linux (Debian/Ubuntu):

sudo apt update

sudo apt install wireshark

Optional: Add user to 'wireshark' group for non-root access:

sudo usermod -aG wireshark $USER

newgrp wireshark

Usage

To launch Wireshark, open it from your applications menu or run:

wireshark

Select a network interface to start capturing packets. You can apply filters like:

- http
- ip.addr == 192.168.1.1
- tcp.port == 80

Captured packets appear in real-time. Click on a packet for detailed analysis in the lower panes.

To save captures:

File > Save As (.pcap format)

To analyze saved captures:

Open Wireshark and use File > Open.

Disclaimer

Wireshark should only be used to capture and analyze traffic on networks you own or are authorized to monitor. Capturing data from unauthorized networks may be illegal and unethical. Always ensure your actions comply with laws and organizational policies.

Conclusion

Wireshark is a powerful and versatile network protocol analyzer suitable for beginners and experts alike. Its detailed insights and flexible features make it indispensable for network administrators, developers, and cybersecurity professionals.