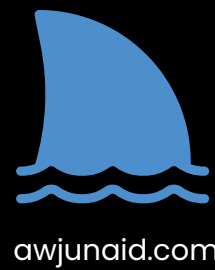


ULTIMATE Wireshark COMMANDS CHEAT SHEET



Installation and Setup

Command	Description
<code>sudo apt-get install wireshark</code>	Install Wireshark on Ubuntu/Debian
<code>brew install wireshark</code>	Install Wireshark on macOS (with Homebrew)
<code>yum install wireshark</code>	Install Wireshark on CentOS/RHEL

Capturing Packets

Command	Description
<code>wireshark</code>	Start Wireshark GUI
<code>tshark -i <interface></code>	Capture packets with tshark
<code>tcpdump -i <interface> -w file.pcap</code>	Capture packets with tcpdump (save to file)
<code>tcpdump -i <interface> -w -</code>	Print captured packets to stdout
<code>tcpdump -r file.pcap</code>	Read a pcap file with tcpdump
<code>tcpdump -D</code>	List available interfaces with tcpdump

Packet Details

Command	Description
Right-click > Follow > TCP Stream	View complete TCP stream
Right-click > Follow > HTTP Stream	View complete HTTP stream
Statistics > Protocol Hierarchy	Analyze protocols in the capture file

Display Filters

Command	Description
<code>ip.addr == 192.168.0.1</code>	Filter packets by source or destination IP
<code>tcp.port == 80</code>	Filter packets by source or destination port
<code>http.request.method == "GET"</code>	Filter HTTP GET requests
<code>frame.number == 42</code>	Filter by packet number
<code>dns.qry.name == "example.com"</code>	Filter DNS queries for a specific domain

Statistics and Analysis

Command	Description
Statistics > Conversations	View conversations in the capture file
Statistics > Endpoints	List all endpoints in the capture file
Statistics > Protocol Hierarchy	Analyze protocols in the capture file
Statistics > I/O Graphs	Graph I/O statistics

Preferences and Customization

Command	Description
Edit > Preferences	Access Wireshark preferences menu
Edit > Configuration Profiles	Manage configuration profiles
Edit > Custom Columns	Add custom columns to packet list

ULTIMATE Wireshark COMMANDS CHEAT SHEET



Expert Information

Command	Description
View > Coloring Rules	Customize packet coloring
View > Name Resolution	Resolve hostnames from IP addresses

Advanced Features

Command	Description
tshark	Command line version of Wireshark
tshark -i <interface>	Capture packets with tshark
tshark -r file.pcap	Read a pcap file with tshark
ssh user@remote tshark -i <interface>	Capture remotely with tshark
wireshark -o <protocol>.display_filter: <filter>	Apply display filter at startup

Exporting Data

Command	Description
File > Export Packet Dissections	Export packet details as plain text or in various formats
File > Export Objects	Extract files from captured traffic
File > Print	Print packet details or summaries

Note: This is not an exhaustive list, but it covers many of the essential commands and features of Wireshark. For more detailed information, consult the [Wireshark documentation](#) or use `man wireshark` and `man tshark` in your terminal.