ULTIMATE Wireshark COMMANDS CHEAT SHEET

awjunaid.com

Installation and Setup

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

Capturing Packets

Command	Description
wireshark	Start Wireshark GUI
tshark -i <interface>	Capture packets with tshark
tcpdump -i <interface> -w file.pcap	Capture packets with tcpdump (save to file)
tcpdump -i <interface> -w -	Print captured packets to stdout
tcpdump -r file.pcap	Read a pcap file with tcpdump
tcpdump -D	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
ip.addr == 192.168.0.1	Filter packets by source or destination IP
tcp.port == 80	Filter packets by source or destination port
http.request.method == "GET"	Filter HTTP GET requests
frame.number == 42	Filter by packet number
dns.qry.name == "example.com"	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

awjunaid.com

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.