Wireshark Command Cheat Sheet

GUI Shortcuts

Ctrl+E	Start capture.
Ctrl+E	Stop capture.
Ctrl+S or **Ctrl+Shift+S**	Save the current capture file.
Ctrl+O	Open a capture file (*.pcap*, *.pcapng*, etc.).
Ctrl+F	Search for a packet by string or display filter.
↓ / ↑	Move to the next or previous packet in the packet list.
Ctrl+↓ / Ctrl+↑	Jump to the next or previous packet in the same conversation.
Enter	Expand or collapse a tree item in the details pane.
Backspace	Jump to the parent node in the packet details pane.
Tab or **Shift+Tab**	Navigate between UI elements (e.g., filter bar, packet list).

Capture Filter Expressions

Capture all traffic from a host.	**src host 192.168.1.10**
Capture all traffic to a host.	**dst host 8.8.8.8**
Capture all traffic to and from a host.	**host 192.168.1.1**
Capture specific port traffic.	**port 443**
Only capture TCP traffic.	**tcp**
Only capture UDP traffic.	**udp**
Only capture DNS traffic (UDP port 53).	**udp port 53**
Capture ICMP (ping) traffic.	**icmp**
Capture HTTP traffic.	**tcp port 80**
Capture HTTPS traffic.	**tcp port 443**
Capture traffic from a network.	**net 192.168.1.0/24**
Exclude SSH traffic.	**not port 22**

Display Filter Expressions

Filter by IP	**ip.addr == 10.10.42.1**
Filter by Source IP	**ip.src == 10.10.42.1**
Filter by Destination IP	**ip.dst == 10.10.42.1**
Exclude IP	**!(ip.addr == 10.10.42.1)**
IP Range	**ip.addr >= 10.10.42.1 and ip.addr <= 10.10.42.100**
Subnet	**ip.addr == 10.10.42.1/24**
Protocol Filter	**http** or **ftp** or **ssh** or **icmp**
TCP port	**tcp.port == 25**
HTTP Host	**http.host == "example.com"**
IP and port	**ip.addr == 10.10.50.1 and tcp.port == 25**
Timestamp	**frame.time >= "2025-08-07 12:48:22"**
SYN flag	**tcp.flags.syn == 1 && tcp.flags.ack == 0**
Destination TCP port	**tcp.dst == 27**
Broadcast traffic	**eth.dst == ff:ff:ff:ff:ff:ff**
Multicast traffic	**(eth.dst[0] & 1)**
MAC address	**eth.addr == 00:10:f7:23:12:c5**

Display Filter Operators

Equal to	**==** or **eq**
Not equal to	**!=** or **ne**
Greater than	**>** or **gt**
Less than	**<** or **lt**
Greater than or equal to	**>=** or **ge**
Less than or equal to	**<=** or **le**
Logical AND	**and** or **&&**
Logical OR	**or** or **||**
Logical NOT	**not** or **!**

tshark Commands

tshark -D	List all available interfaces.
tshark -i enp0s3	Capture packets on a specific interface.
tshark -i enp0s3 -w file.pcapng	Save captured packets to a file.
tshark -a duration:30 -i enp0s3	Capture traffic for 30 seconds.
tshark -f "port 443" -i enp0s3	Apply a capture filter to only record HTTPS traffic.
tshark -Y "http" -r file.pcapng	Apply a display filter to show HTTP traffic from a saved file.
tshark -T fields -e ip.src -e ip.dst	Output only specific fields (the source and destination IP in this example).
tshark -z io,stat,1	Show I/O statistics in 1-second intervals.
tshark -z conv,tcp	Display TCP conversations.
tshark -i enp0s3 -c 100 -w file.pcapng	Capture 100 packets and stop automatically.
tshark -i enp0s3 -w file.pcapng -P	Show packets live in the terminal and write them to a file.
tshark -r file.pcapng -Y "http.request"	Filter and display only HTTP requests from a capture file.
tshark -r file.pcapng -T fields -e ip.src -e ip.dst -e frame.len	Display the selected fields (source IP, destination IP, frame size).
tshark -r file.pcapng -T fields -e ip.src -e ip.dst -E header=y -E separator=, > packets.csv	Export selected fields as a CSV file.
tshark -r file.pcapng -T json	Output data in a structured JSON format.
tshark -r file.pcapng -Y "dns" -T fields -e dns.qry.name	Extract domain names from DNS query packets.
tshark -i enp0s3 -f "tcp[tcpflags] & tcp-syn != 0" -c 10	Capture 10 TCP SYN packets to identify connection attempts.
tshark -i enp0s3 -f "host 192.168.1.10"	Capture traffic to and from the specified IP address.
tshark -qz io,stat,1 -i enp0s3 -a duration:60	Print packet counts per second over 60 seconds.
tshark -i enp0s3 -w file.pcapng &	Start a capture in the background.