

Wireshark Cheat Sheet: All the Commands, Filters & Syntax

January 18, 2023 / By Nathan House

WIRESHARK CHEAT SHEET



 Listen to the article

Wireshark is arguably the most popular and powerful tool you can use to capture, analyze and troubleshoot network traffic. The only downside you will face when using a tool as verbose as Wireshark is memorizing all of the commands, flags, filters, and syntax. That's where we come in.

Whether you are a network administrator, a security professional, or just someone curious about how networks work, learning to use Wireshark is a valuable skill. This Wireshark cheat sheet will provide a solid foundation and reference for using Wireshark to monitor and analyze your network traffic.

Download a pdf copy for your records [here](#), and scroll below to find a list of the **common commands in Wireshark**.

Search cheats here



Default Columns In a Packet Capture Output

NAME	DESCRIPTION
No.	Frame number from the beginning of the packet capture
Time	Seconds from the first frame
Source (src)	Source address, commonly an IPv4, IPv6 or Ethernet address
Destination (dst)	Destination address
Protocol	Protocol used in the Ethernet frame, IP packet, or TC segment
Length	Length of the frame in bytes

Logical Operators

OPERATOR	DESCRIPTION	EXAMPLE
and or &&	Logical AND	All the conditions should match
or or	Logical OR	Either all or one of the conditions should match
xor or ^^	Logical XOR	Exclusive alterations – only one of the two conditions should match not both
not or !	Not (Negation)	Not equal to
[n] [...]	Substring operator	Filter a specific word or text

Filtering Packets (Display Filters)

OPERATOR	DESCRIPTION	EXAMPLE
eq or ==	Equal	ip.dest == 192.168.1.1
ne or !=	Not equal	ip.dest != 192.168.1.1
gt or >	Greater than	frame.len > 10
lt or <	less than	frame.len < 10
ge or >=	Greater than or equal	frame.len >= 10

OPERATOR	DESCRIPTION	EXAMPLE
le or <=	Less than or equal	frame.len <= 10

Filter Types

NAME	DESCRIPTION
Capture filter	Filter packets during capture
Display filter	Hide packets from a capture display

Wireshark Capturing Modes

NAME	DESCRIPTION
Promiscuous mode	Sets interface to capture all packets on a network segment to which it is associated to
Monitor mode	Setup the wireless interface to capture all traffic it can receive (Unix/ Linux only)

Miscellaneous

NAME	DESCRIPTION
Slice Operator	[...] – Range of values
Membership Operator	{ } – In
CTRL+E	Start/Stop Capturing

Capture Filter Syntax

SYNTAX	PROTOCOL	DIRECTION	HOSTS	VALUE	LOGICAL OPERATOR	EXPRESSIONS
Example	tcp	src	192.168.1.1	80	and	tcp dst 202.164.30.1

Display Filter Syntax

SYNTAX	PROTOCOL	STRING 1	STRING 2	COMPARISON OPERATOR	VALUE	LOGICAL OPERATOR	EXPRESSIONS
Example	http	dest	ip	==	192.168.1.1	and	tcp port

Keyboard Shortcuts – Main Display Window

ACCELERATOR	DESCRIPTION	ACCELERATOR	DESCRIPTION
Tab or Shift+Tab	Move between screen elements, e.g. from the toolbars to the packet list to the packet detail.	Alt+→ or Option→	Move to the next packet in the selection history.
↓	Move to the next packet or detail item.	→	In the packet detail, opens the selected tree item.
↑	Move to the previous packet or detail item.	Shift+→	In the packet detail, opens the selected tree items and all of its subtrees.
Ctrl+ ↓ or F8	Move to the next packet, even if the packet list isn't focused.	Ctrl+→	In the packet detail, opens all tree items.
Ctrl+ ↑ Or F7	Move to the previous packet, even if the packet list isn't focused	Ctrl+←	In the packet detail, closes all the tree
Ctrl+.	Move to the next packet of the conversation (TCP, UDP or IP).	Backspace	In the packet detail, jumps to the parent node.
Ctrl+,	Move to the previous packet of the conversation (TCP, UDP or IP).	Return or Enter	In the packet detail, toggles the selected tree item.

Want to Download All Our Premium Cheat Sheets?

No Problem! Just enter your email address, and we'll send you the PDF versions of all our top cheat sheets.

Email Address

DOWNLOAD

Protocols – Values

ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp

Common Filtering Commands






USAGE	FILTER SYNTAX
Wireshark Filter by IP	ip.addr == 10.10.50.1
Filter by Destination IP	ip.dest == 10.10.50.1
Filter by Source IP	ip.src == 10.10.50.1
Filter by IP range	ip.addr >= 10.10.50.1 and ip.addr <=10.10.50.100
Filter by Multiple Ips	ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
Filter out IP address	! (ip.addr == 10.10.50.1)
Filter subnet	ip.addr == 10.10.50.1/24
Filter by port	tcp.port == 25
Filter by destination port	tcp.dstport == 23

USAGE	FILTER SYNTAX
Filter by ip adress and port	ip.addr == 10.10.50.1 and Tcp.port == 25
Filter by URL	http.host == “host name”
Filter by time stamp	frame.time >= “June 02, 2019 18:04:00”
Filter SYN flag	Tcp.flags.syn == 1 and tcp.flags.ack ==0
Wireshark Beacon Filter	wlan.fc.type_subtype = 0x08
Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Wireshark multicast filter	(eth.dst[0] & 1)
Host name filter	ip.host = hostname
MAC address filter	eth.addr == 00:70:f4:23:18:c4
RST flag filter	tcp.flag.reset == 1

Main Toolbar Items

TOOLBAR ICON	TOOLBAR ITEM	MENU ITEM	DESCRIPTION
	Start	Capture → Start	Uses the same packet capturing options as the previous session, or uses defaults if no options were set
	Stop	Capture → Stop	Stops currently active capture
	Restart	Capture → Restart	Restart active capture session
	Options...	Capture → Options...	Opens “Capture Options” dialog box

TOOLBAR ICON	TOOLBAR ITEM	MENU ITEM	DESCRIPTION
	Open...	File →open...	Opens “File open” dialog box to load a capture for viewing
	Save As...	File → Save As...	Save current capture file
	Close	File →Close	Close current capture file
	Reload	View → Reload	Reload current capture file
	Find Packet...	Edit →Find Packet...	Find packet based on different criteria
	Go Back	Go → Go back	Jump back in the packet history
	Go Forward	Go → Go Forward	Jump forward in the packet history
	Go to Packet...	Go → Go to Packet...	Go to specific packet
	Go to First Packet	Go → Go to First Packet	Jump to first packet of the capture file
	Go to last Packet	Go → Go to last Packet	Jump to last packet of the capture file
	Auto Scroll in Live Capture	View → Auto Scroll in Live Capture	Auto scroll packet list during live capture

TOOLBAR ICON	TOOLBAR ITEM	MENU ITEM	DESCRIPTION
	Colorize	View → Colorize	Colorize the packet list (or not)
	Zoom In	View → Zoom In	Zoom into the packet data (increase the font size)
	Zoom Out	View → Zoom Out	Zoom out of the packet data (decrease the font size)
	Normal Size	View → Normal Size	Set zoom level back to 100%
	Resize Columns	View → Resize Columns	Resize columns, so the content fits the width

Conclusion

Wireshark is an incredibly powerful tool for analyzing and troubleshooting network traffic. It provides a wealth of information that can help you identify issues, track down problems, and understand how your network is being used.

We hope that with the knowledge and techniques covered in this Wireshark cheat sheet, you should now be able to confidently capture, filter, and analyze packets with Wireshark. You can also learn to [Master Wireshark in Five Days](#) or [Start Using Wireshark to Hack Like a Pro](#) with our VIP courses.

Frequently Asked Questions

⊖ What is Wireshark and how do you use it?

Wireshark advertises itself as, “the world’s foremost and widely-used network protocol analyzer.” By running a capture, you can grab traffic on your network and see not only the origin and destination of the packets, but often important information contained within.

⊕ Can Wireshark see texts?

- ⊕ What should I look for when using Wireshark?
- ⊕ What are the 2 types of filters used by Wireshark?
- ⊕ Can Wireshark see incognito?
- ⊕ Can you track someone with Wireshark?
- ⊕ How do you capture packets in Wireshark?
- ⊕ What can hackers do with Wireshark?
- ⊕ What is the best way to learn Wireshark?
- ⊕ How do I read Wireshark logs?

Grow your Cyber Security Skills





FIND OUT MORE

CATEGORIES

CHEAT SHEETS

HACKING

NETWORKING



Nathan House

Nathan House is the founder and CEO of StationX. He has over 25 years of experience in cyber security, where he has advised some of the largest companies in the world. Nathan is the author of the popular "The Complete Cyber Security Course", which has been taken by over half a million students in 195 countries. He is the winner of the AI "Cyber Security Educator of the Year 2020" award and finalist for Influencer of the year 2022.

Related Articles

NMAP CHEAT SHEET



Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

[Read More »](#)

LINUX CHEAT SHEET



Linux Command Line Cheat Sheet: All the Commands You Need

[Read More »](#)

SOCIAL ENGINEERING EXAMPLE



Social Engineering Example

[Read More »](#)



Movies for Hackers to Watch

[Read More »](#)

INFO

[Affiliates](#)

[Legal Notices](#)

[Privacy Policy](#)

[Site Map](#)

SECURITY ASSESSME NT

[Penetration](#)

[Testing](#)

[Vulnerability](#)

CONSULTI NG

[Audit &](#)

[Compliance](#)

[Incident](#)

[Response](#)



00:00

00:00

14



[Source Code](#)

[Review](#)

[Social](#)

[Engineering](#)

[Risk Assessment](#)

[Security Training](#)



00:00

00:00

1⚡

