Table of Contents

k Cheat Sheet: All the ds, Filters & Syntax

May 10, 2024 ▪ Nathan House

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

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**.

Sheet Search

t sheet to find the right cheat for the term you're looking
n the search bar and you'll receive the matching cheats

a Packet Capture Output

Level Up in Cyber Security: Join Our Membership Today!

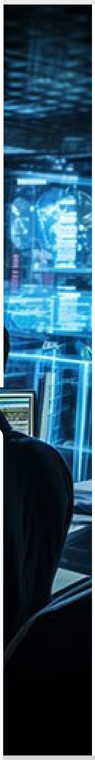
LEARN MORE

	TION
	umber from the beginning of the packet capture
	from the first frame
	ddress, 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

OPERATOR	DESCRIPTION	EXAMPLE
	Not equal to	
	Filter a specific word or text	



Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

Download the PDF Version of This Wireshark Cheat Sheet!

Want to keep this cheat sheet at your fingertips? Just enter your email address, and we'll send a PDF copy to your inbox.

First name

Email Address

DOWNLOAD →

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
it or <	less than	frame.len < 10
ge or >=	Greater than or equal	frame.len >= 10
le or <=	Less than or equal	frame.len <= 10

Filter Types

NAME	DESCRIPTION
	ter packets during capture
	de packets from a capture display

Modes

	N
	ce to capture all packets on a network segment to which it is to
	ireless interface to capture all traffic it can receive (Unix/ Linux

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

	DESCRIPTION
	[...] - Range of values
	{} - 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
	screen elements, olbars to the e packet detail.	**Alt+→ or Option→**	Move to the next packet in the selection history.
	xt packet or detail	**→**	In the packet detail, opens the selected tree item.
	vious packet or	**Shift+→**	In the packet detail, opens the selected tree items and all of its subtrees.
	xt packet, even if sn't focused.	**Ctrl+→**	In the packet detail, opens all tree items.
	vious packet, ket list isn't	**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.

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

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.add == 10.10.50.1

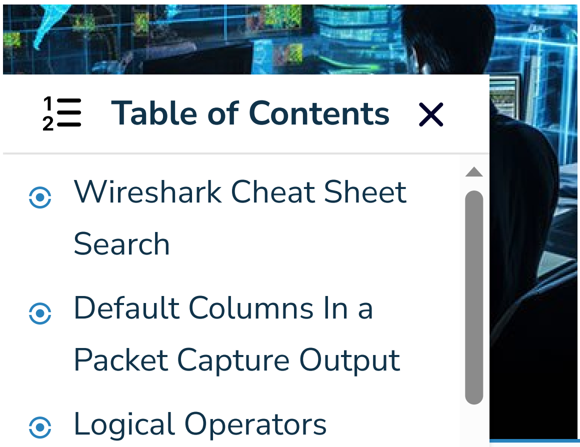
USAGE	FILTER SYNTAX
	ip.dest == 10.10.50.1
	ip.src == 10.10.50.1
	ip.addr >= 10.10.50.1 and ip.addr <=10.10.50.100
	ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100
	! (ip.addr == 10.10.50.1)
	ip.addr == 10.10.50.1/24
	tcp.port == 25
Filter by destination port	tcp.dstport == 23
	ip.addr == 10.10.50.1 and Tcp.port == 25
	http.host == "host name"
	frame.time >= "June 02, 2019 18:04:00"
	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

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

Download the PDF Version of This Wireshark Cheat Sheet!

Want to keep this cheat sheet at your fingertips? Just enter your email address, and



we'll send a PDF copy to your inbox.

First name

Email Address

DOWNLOAD →

and Generator

of trying to remember the exact syntax for your n our Wireshark Command Generator, you can simply say what you need Wireshark to do, and we will generate the command for you.

Generate

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

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

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

TOOLBAR ICON	TOOLBAR ITEM	MENU ITEM	DESCRIPTION
		File →open...	Opens "File open" dialog box to load a capture for viewing
		File → Save As...	Save current capture file
		File →Close	Close current capture file
		View → Reload	Reload current capture file
		Edit →Find Packet...	Find packet based on different criteria
		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
		View → Colorize	Colorize the packet list (or not)
		View → Zoom In	Zoom into the packet data (increase the font size)
		View → Zoom Out	Zoom out of the packet data (decrease the font size)
		View → Normal Size	Set zoom level back to 100%
		View → Resize Columns	Resize columns, so the content fits the width

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

erful 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 **StationX 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?

ilters used by Wireshark?

nito?

vith Wireshark?

kets in Wireshark?

h Wireshark?

earn Wireshark?

logs?

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

Guarantee Your Cyber Security Career with the StationX Master's Program!

Get real work experience and a job guarantee in the StationX Master's Program. Dive into tailored training, mentorship, and community support that accelerates your career.

- **Job Guarantee & Real Work Experience:** Launch your cybersecurity career with guaranteed placement and hands-on experience within our Master's Program.

- **30,000+ Courses and Labs:** Hands-on, comprehensive training covering all
excel in any role in the field.
- **ams:** Resources and exam simulations that help you
nce.
- **er Coaching:** Personalized advice, resume help, and
boost your career.
- Engage with a thriving community of peers and
oing support.
- **or Real-World Skills:** Courses and simulations
scenarios.
- **l Networking:** Join events and exclusive networking
opportunities to expand your connections.

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

P IN YOUR CAREER TODAY!

STER’S PROGRAM

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

nlocking

Read More »

OWASP ZAP Tutorial: Complete 2025 Guide

Read More »

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

How to Prevent Tailgating Attacks: The Five-Minute Guide

Read More »

Legal Notices

icy

ASSESSMENT

Penetration Testing

Vulnerability Scanning

Build Reviews

Source Code Review

Social Engineering

Audit & Compliance

Incident Response

Security Architecture

Risk Assessment

Security Training

Pro Bono Services

Table of Contents

Level Up in Cyber Security: Join Our Membership Today!

LEARN MORE

COPYRIGHT © 2025 STATIONX LTD. ALL RIGHTS RESERVED.

Nathan House