

Wireshark

Cheatsheet

Wireshark Cheat Sheet					◆ Cyber Press		
Default Columns in a packet capture output					Logical operators		
No.	Frame number from the begining of the packet capture				Operator	Discription	Example
Time.	Seconds from the first frame				and or &&	Logical AND	All the conditions should match
Source (src).	Source address, commonly an IPv4, IPv6 or Ethernet address				or or	Logical OR	Either all or one of the condions should match
Destination (dst).	Destination adress				xor or AA	Logical XOR	Exclusive alterations only one of the two conditions should match not both
Protocol.	Protocol used in the Ethernet frame, IP packet, or TC segment				not ot !	Not (Negation)	Not equal to
Length.	Length of the frame in bytes				[n] [...]	Substring operator	Filter a specific word or text
Filter Types					Filtering packets (Display Filters)		
Capture Filter	Filter packets during capture				Operator	Discription	Example
Display filter	Hide packets from a capture display				eq or ==	Logical AND	ip.dest 192.168.1.1
Wireshark Capturing Modes					ne or !=	Logical OR	ip.dest != 192.168.1.1
Promiscuous mode	Sets interface to capture all packets on a network segment to which it is associated to Setup the wireless interface to capture all traffic it can receive (Unix/Linux only)				gt or >	Logical XOR	frame.len > 10
Monitor mode					it or <	Not (Negation)	frame.len 10
					ge or >=	Substring operator	frame.len >> 10
					le or <=	Substring operator	frame.len <= 10
					Miscellaneous		
					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 1	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 Optio	Move to the next packetin the selection history.		
Tab or Shift+Tab	Move to the next packet or detail item.				In the packet detail, opens the selected tree item.		
Tab or Shift+Tab	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.		
Protocols Values		ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp					

From:
<https://wiki.fortier-family.com/> - Warnaud's Wiki

Permanent link:
<https://wiki.fortier-family.com/cybersecurity/wireshark>

Last update: 2026/09/20 13:17



