Wireshark Cheat Sheet

Default columns in a packet capture output

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

Logical operators

Operator	Discription	Example
and or &&	Logical AND	All the conditions should match
or or ||	Logical OR	Either all or one of the condtions should match
xor or ^^	Logical XOR	Exclusive alterations - only one of the two conditions should match not both
not ot !	Not (Negation)	Not equal to
[n] [...]	Substring operator	Filter a specific word or text

Filtering packets (Display Filters)

Operator	Discription	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

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

Wireshark Capturing Modes

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

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 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 Optio→	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.

Protocols - Values

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

Wireshark Cheat Sheet

Common Filtering commands

Usage	Filter syntax
Wireshark Filter by IP	ip.add == 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 adress	! (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
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 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

Common Filtering commands

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 ⟶ Optio...	Opens "Capture Options" dialog box
	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	File ⟶ 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
	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