Wireshark

Default columns in a packet capture output

No.	Frame/Packet number in the packet capture.
Time	Time at which the packet was captured (in Second).
Source	Source IP address or MAC address (IPv4/ IPv6/ Ethernet address).
Destination	Destination IP address or MAC address.
Protocol	Protocol used in the packet (e.g., TCP, UDP, ICMP).
Length	Length of the packet in bytes.
Info	Additional information about the packet, such as protocol-specific details or any alerts.

Wireshark Capturing modes

Standrad Mode	Default real-time packet capture from the network interface.
Promiscuous Mode	Captures all packets on the network segment, regardless of destination.
Non-Promiscuous Mode	Only captures packets specifically addressed to the capturing system.
Monitor Mode	Captures wireless network traffic on specified channels.
Remote Capture Mode	Captures packets remotely from another system over the network.

Miscellaneous

Ctrl + E	Start / Stop Capturing.
Slice Operator	[:] -- Range of values
Membership Operator	{ } – In (filters packets based on whether a value belongs to a specified list or set.)

Filter Types

Ethernet, tcp & udp, http, dns, fddi, ip, arp, rarp, decnt, lat, sca, moprc, moprc, mopdl

Filter Types

Capture Filter	applied during live packet capture to select packets
Display Filter	used post-capture to filter and analyze captured packets.

Capture Filter Syntex

Syntax	Protocol	Direction	Hosts	Value	Logical Operator	Expressions
Test_Case	Tcp	Src	192.168.1.1	80	And	Tcp sdt 202.168.24.1

Display Filter Syntex

Syntax	Protocol	String 1	String 2	Comparison Operator	Vaue	Logical Operator	Expressions
Test_Case	http	dest	ip	==	192.168.1.1	and	tcp port

Logical Operators

Operator	Description	Example
and or &&	Logical AND	All the conditions should match
or or ||	Logical OR	Either all or one of the condition should match
xor or ^^	Logical XOR	Exclusive alternation (Only one of the two conditions should match not both)
not or !	NOT (Negation)	Not equal to
[n] [....]	Substring operator	Filter a specific keyword

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 > 100
lt or <	Less than	frame.len < 100
ge or >=	Greater than or Equal	frame.len >= 100
Le or <=	Less than or Equal	frame.len <= 100

Wireshark

Default columns in a packet capture output

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

Common Filtering Commands

Usage	Filter syntax	Usage	Filter syntax
Filter by IP address	ip.addr == 192.168.0.100	Filter by Packet Length	frame.len > 100
Filter by Source IP	ip.src == 192.168.1.100	Filter by Time Stamp	frame.time >= "March 18,2024 16:12:40"
Filter by Destination IP	ip.dst == 192.168.1.100	Filter by URL	http.host == "host name"
Filter by MAC address	eth.addr == 00:11:22:33:44:55	Filter by Host Name	ip.host = host name
Filter by Source MAC address	eth.src == 00:11:22:33:44:55	Filter SYN flag	tcp.flags.syn == 1
Filter by Destination MAC address	eth.dst == 00:11:22:33:44:55	Filter by UDP length	udp.length > 100
Filter by Packet Payload	data contains "keyword"	Wireshark Beacon Filter	wlan.fc.type_subtype = 0x08
Filter by IP range	ip.addr >= 192.168.1.1 and ip.addr <= 192.168.1.100	Wireshark Multicast Filter	(eth.dst[0] & 1)
Filter by Multiple IP's	ip.addr == 192.168.1.10 and ip.addr == 192.168.1.100	Filter by VLAN ID	vlan.id == 10
Filter out IP address	!(ip.addr == 192.168.1.10)	Filter by DHCP traffic	bootp
Filter Subnet	ip.addr == 192.168.1.1/24	RST flag filter	tcp.flags.reset == 1
Filter by port	tcp.port==25	Filter by TCP Window Size	tcp.window_size >= 1024
Filter by Destination port	tcp.dstport == 80	Filter by IP Version (IPv4 or IPv6)	ip.version == 4
Filter by IP address and port	ip.addr == 192.168.1.10 and tcp.port == 60	RST flag filter	tcp.flag.reset == 1

Main Toolbar Item in Wreshark

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	Restarts active capture session
	Options	Capture → Options	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	View → Reload	Reloads 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 to the width