Wireshark Cheat Sheet

Cyber Writes

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

Filter Types

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

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 AA	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 ==	Logical AND	ip.dest 192.168.1.1
ne or !=	Logical OR	ip.dest != 192.168.1.1
gt or >	Logical XOR	frame.len > 10
it or <	Not (Negation)	frame.len 10
ge or >=	Substring operator	frame.len >> 10
le or <=	Substring operator	frame.len <= 10

Wireshark Capturing Modes

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

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
Tab or Shift+Tab	Move between screen elements, e.g. from the toolbars. to the packet list to the packet detail.
Tab or Shift+Tab	Move to the next packet or detail item.
Tab or Shift+Tab	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).

Accelerator	Description
Alt+ or Optio	Move to the next packetin the selection history.
	In the packet detail, opens the selected tree item.
Shift+-	In the packet detail, opens the selected tree items and all of its subtrees.
Ctrl+	In the packet detail, opens all tree items.
Ctrl++	In the packet detail, closes all the tree
Backspace	in the packet detail, jumps to the parent node.
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