Wireshark Packet analyzer GUI

CONCEPTS

> The display filter bar narrows what you see; the capture filter (set before starting) narrows what is recorded.

Packet list one row per packet
Packet details protocol tree
Packet bytes raw hex / ASCII

CAPTURE

Ctrl + K Open capture options

Ctrl + E Start or stop capture

Ctrl + R
Reload file / restart capture

F5 Refresh interface list

FILES

Ctrl + O Open a capture file

Ctrl + S Save the capture

Ctrl + Shift + S Save as

Ctrl + W Close the capture

Ctrl + P Print

Ctrl + Q Quit Wireshark

NAVIGATION

Ctrl + G Go to packet number

Ctrl + Down / F8
Next packet

Ctrl + Up / F7
Previous packet

Ctrl + Home First packet

Ctrl + End Last packet

Ctrl + .
Next packet in conversation

Ctrl + ,
Previous packet in conversation

Alt + Right
Next in selection history

Alt + Left
Previous in selection history

Tab / Shift + Tab
Move between panes and widgets

NAVIGATION (cont.)

Up / Down
Previous / next row

PACKET DETAILS

Right Open selected item

Left
Close item, or jump to parent

Shift + Right
Expand item and subtrees

Shift + Left Collapse subtrees

Ctrl + Right Expand all

Ctrl + Left Collapse all

Backspace
Jump to parent node

Enter Toggle selected item

FIND AND FILTER

Ctrl + F Find packet

Ctrl + N Find next

Ctrl + B Find previous

Ctrl + Shift + P Preferences

Display filter basics

Filter	Matches
`ip.addr == 10.0.0.1`	Either IP address
`tcp.port == 443`	Either TCP port
`http and !dns`	Combine with and / or / !
`frame contains "user"`	Raw bytes or string
`tcp.flags.syn == 1`	SYN set

More filter syntax

Syntax	Meaning
`tcp.port in {80, 8000..8100}`	Value in set or range
`http.host matches "a\.(com|net)"`	Regular expression
`eth.src[0:3] == 00:1a:2b`	Byte slice
`== != > < >= <=`	Compare (eq ne gt lt ge le)

MARKING AND TIME

Ctrl + M
Mark or unmark packet

Ctrl + Shift + M
Mark all displayed

Ctrl + Alt + M
Unmark all displayed

Ctrl + Shift + N
Next marked packet

Ctrl + Shift + B
Previous marked packet

Ctrl + D
Ignore or unignore packet

Ctrl + Shift + D
Ignore all displayed

Ctrl + Alt + D
Unignore all displayed

Ctrl + T
Set or unset time reference

Ctrl + Alt + T
Unset all time references

Ctrl + Shift + T Time shift

Ctrl + Alt + C
Add packet comment

VIEW

Ctrl + =
Zoom in (Ctrl++ also works)

Ctrl + - Zoom out

Ctrl + 0 Normal font size

Ctrl + Shift + R
Resize all columns

RECIPES

Isolate one TCP stream

```
# select a packet, then follow its conversation
Ctrl+.   next packet of the same conversation
# or filter by hand
tcp.stream == 3
```

Triage a slow connection

```
tcp.analysis.flags
tcp.analysis.retransmission
# then mark interesting ones
Ctrl+M  then  Ctrl+Shift+N
```

Spot DNS problems

```
dns.flags.rcode != 0
dns and !dns.flags.response
```