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

FILES

Ctrl + **O**
Open a capture file

Ctrl + **S**
Save the capture

NAVIGATION

Ctrl + **G**
Go to packet number

Ctrl + **Down** / **F8**
Next packet

Ctrl + **Up** / **F7**
Previous packet

Ctrl + **.**
Next packet in conversation

Ctrl + **,**
Previous packet in conversation

Up / **Down**
Previous / next row

PACKET DETAILS

Right
Open selected item

PACKET DETAILS (cont.)

Left
Close item, or jump to parent

Shift + **Right**
Expand item and subtrees

Ctrl + **Right**
Expand all

Ctrl + **Left**
Collapse all

FIND AND FILTER

Ctrl + **F**
Find packet

Ctrl + **N**
Find next

Ctrl + **B**
Find previous

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

MARKING AND TIME

Ctrl + **M**
Mark or unmark packet

Ctrl + **Shift** + **N**
Next marked packet

Ctrl + **D**
Ignore or unignore packet

VIEW

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

Ctrl + **-**
Zoom out