Wireshark Packet analyzer GUI

START HERE

- **Ctrl** + **K** Capture options
- **Ctrl** + **D** Ignore a packet
- **Ctrl** + **E** Start / stop capture
- **Ctrl** + **Shift** + **R** Resize columns
- **Ctrl** + **F** Find a packet
- **Ctrl** + **M** Mark a packet
- **Ctrl** + **G** Go to packet number
- **Ctrl** + **.** Next in conversation

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

CONCEPTS

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

View > Internals > Keyboard Shortcuts lists every shortcut of the main window. On macOS, Ctrl is mostly Cmd.

CAPTURE

- **Ctrl** + **K** Open capture options
- **Ctrl** + **E** Start or stop capture
- **Ctrl** + **R** Reload file / restart capture
  Restart a live capture, or reload the open file.
- **F5** Refresh interface list
- **Ctrl** + **Shift** + **F** Reload as file format/capture

FILES

- **Ctrl** + **O** Open a capture file
- **Ctrl** + **S** Save the capture
- **Ctrl** + **Shift** + **S** Save as

FILES (cont.)

- **Ctrl** + **W** Close the capture
- **Ctrl** + **H** Export packet dissections
- **Ctrl** + **P** Print
- **Ctrl** + **Q** Quit Wireshark

NAVIGATION

- **Ctrl** + **G** Go to packet number
- **Ctrl** + **Down** / **F8** Next packet
  Works even when the packet list is not focused.
- **Ctrl** + **Up** / **F7** Previous packet
- **Ctrl** + **Home** First packet
- **Ctrl** + **End** Last packet
- **Ctrl** + **.** Next packet in conversation
  Follows the TCP, UDP or IP conversation of the selected packet.
- **Ctrl** + **,** Previous packet in conversation
- **Alt** + **Right** Next in selection history

NAVIGATION (cont.)

- **Alt** + **Left** Previous in selection history
- **Tab** / **Shift** + **Tab** Move between panes and widgets
- **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

FIND AND FILTER (cont.)

- **Ctrl** + **N** Find next
- **Ctrl** + **B** Find previous
- **Ctrl** + **Shift** + **A** Configuration profiles
- **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 expressio
`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** + **Alt** + **N** Next time reference
- **Ctrl** + **Alt** + **B** Previous time reference
- **Ctrl** + **Shift** + **T** Time shift

MARKING AND TIME (cont.)

- **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
```