Wireshark

https://www.wireshark.org/

Written by Shad Brown || 🦋 @winterknight.net
Revised by Bronwen Aker

Wireshark is an incredible tool used to read and analyze network traffic coming in and out of an endpoint. Additionally, it can load previously captured traffic to assist with troubleshooting network issues or analyze malicious traffic to help determine what a threat actor is doing on your network.

Basic Usage

The most basic filtering Wireshark provides is by protocol. Simply type the protocol name:

- `dns`
- `http`
- `arp`
- `icmp`
- `tls`
- And many more!

Logical Operators

- Logical AND: `and` or `&&`
- Logical OR: `or` or `||`
- Logical NOT: `not` or `!`

Comparison Operators

- Equal to: `eq` or `==`
- Not Equal to: `ne` or `!=`
- Greater than: `gt` or `>`
- Less than: `lt` or `<`
- Greater than or equal to: `ge` or `>=`
- Less than or equal to: `le` or `<=`

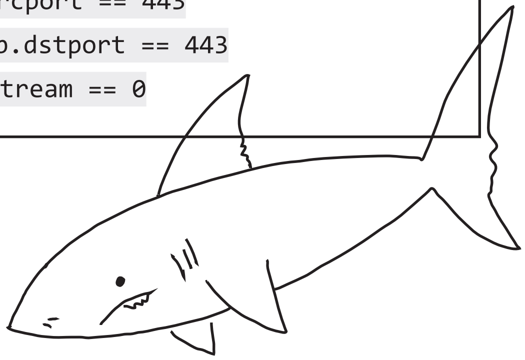
IP Filters

- Filter by IP (matches source or destination):
  `ip.addr == 192.168.0.1`
- Filter to source IP:
  `ip.src == 192.168.0.1` or `ip.src == 192.168.1.0/24`
- Filter to destination IP:
  `ip.dst == 192.168.0.1` or `ip.dst == 192.168.1.0/24`
- Exclude an IP:
  `ip.addr != 192.168.0.1`
- Filter to multiple IPs (any of them):
  `ip.addr == 192.168.0.1` or `ip.addr == 10.0.0.1`
- Filter for traffic between two specific IPs (both directions):
  `(ip.src == 192.168.0.1 and ip.dst == 10.0.0.1)` or
  `(ip.src == 10.0.0.1 and ip.dst == 192.168.0.1)`
- Filter by subnet:
  `ip.addr == 192.168.1.0/24`
- IP range filtering:
  `ip.addr >= 192.168.0.1 and ip.addr <= 192.168.0.100`

Transport Layer Filters

These also work for UDP!

- Port filtering: `tcp.port == 443`
- Source port filtering: `tcp.srcport == 443`
- Destination port filtering: `tcp.dstport == 443`
- TCP session tracking: `tcp.stream == 0`



Useful GUI Features

Wireshark's graphical interface has handy right-click options:

- **Apply as Filter:** Immediately applies the selected field as the display filter.
- **Prepare as Filter:** Constructs the filter expression in the text bar so you can edit it before running it.

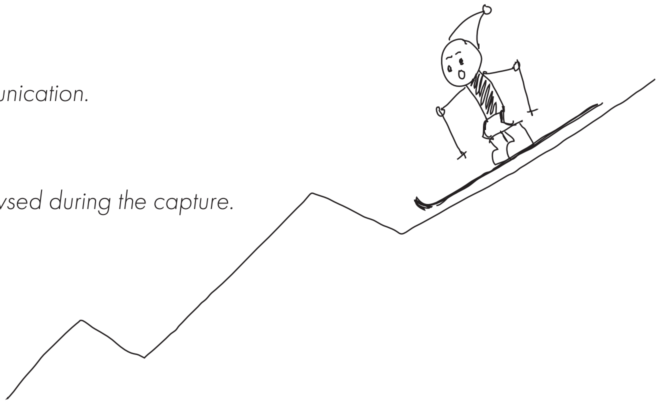
Wireshark also makes it easy to track individual conversations:

- Right-click a packet, then select **Follow > TCP Stream or Follow > UDP Stream**. This opens a window showing the conversation chronologically and applies the appropriate stream filter.

Useful Statistical Tools

Wireshark provides statistical summaries to help you analyze traffic:

- Statistics > IPv4 Statistics > Destinations and Ports
  - *Shows all IPs, transport protocols, and ports involved in communication. You can apply display filters here to narrow results.*
- Statistics > HTTP > Requests
  - *Displays web requests, including domains and endpoints browsed during the capture.*
- Statistics > Protocol Hierarchy
  - *Gives a tree breakdown of all protocols seen in the capture.*
- Statistics > IO Graphs
  - *Lets you visualize traffic volume over time with custom filters.*



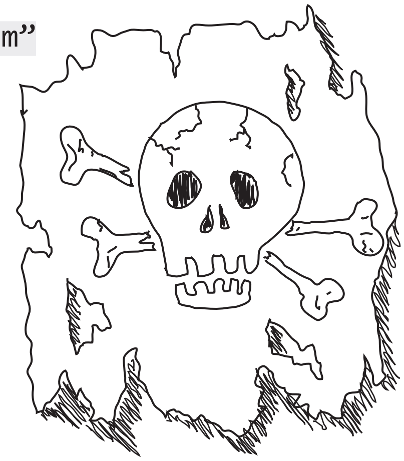
Other Useful Filters and Features

- Exclude local network noise:
  `not arp and not ssdp and not mdns`
- Filter packets by length:
  `frame.len > 500` or `frame.len > 1000`
- Find packets with TCP errors or analysis flags:
  `tcp.analysis.flags`
- Filter by MAC address:
  `eth.addr == aa:bb:cc:dd:ee:ff`
- HTTP host filter:
  `http.host == "example.com"`
- TLS SNI filter:
  `tls.handshake.extensions_server_name == "example.com"`
- Exclude an entire subnet:
  `not ip.addr == 192.168.1.0/24`

Exporting Objects

Wireshark can reassemble and export transferred files:

- File > Export Objects > HTTP
- File > Export Objects > SMB



Decryption Options

- Load SSL/TLS session keys to decrypt HTTPS traffic:
  - *Preferences > Protocols > TLS*
  - *Add your key log file.*
- For Wi-Fi traffic: WPA2 PSK decryption available with proper capture and passphrase.

Marking and Coloring

- Mark Packets: Right-click and choose Mark Packet.
- Coloring Rules: Define filters with custom colors to highlight traffic patterns.
  - *Found under View > Coloring Rules.*

Time Shift

- Edit > Time Shift lets you synchronize timestamps between multiple captures.

Name Resolution

- Toggle DNS, transport, and MAC name resolution:
  - *View > Name Resolution*
  - *Or in Preferences > Name Resolution for consistent display.*

Saving and Sharing Filters

- Use Manage Display Filters to save custom filters for frequent reuse.
- Export and share filter sets with your team.

Tip: If you're wondering what a button above the filter field does, just hover your cursor over it for a tooltip.