



TCP Sequencing & Handshake

Wireshark & TCP

- » What is the TCP handshake, and why is it so important?
- » How can I use Wireshark to capture and analyze this communication traffic?
 - Placement
 - Filters
 - Flow graph

Wireshark & TCP

The screenshot displays the Wireshark network protocol analyzer interface. The top toolbar contains various icons for file operations, search, and analysis. Below the toolbar, the 'Filter' bar is set to 'tcp.analysis'. The main window is divided into three panes:

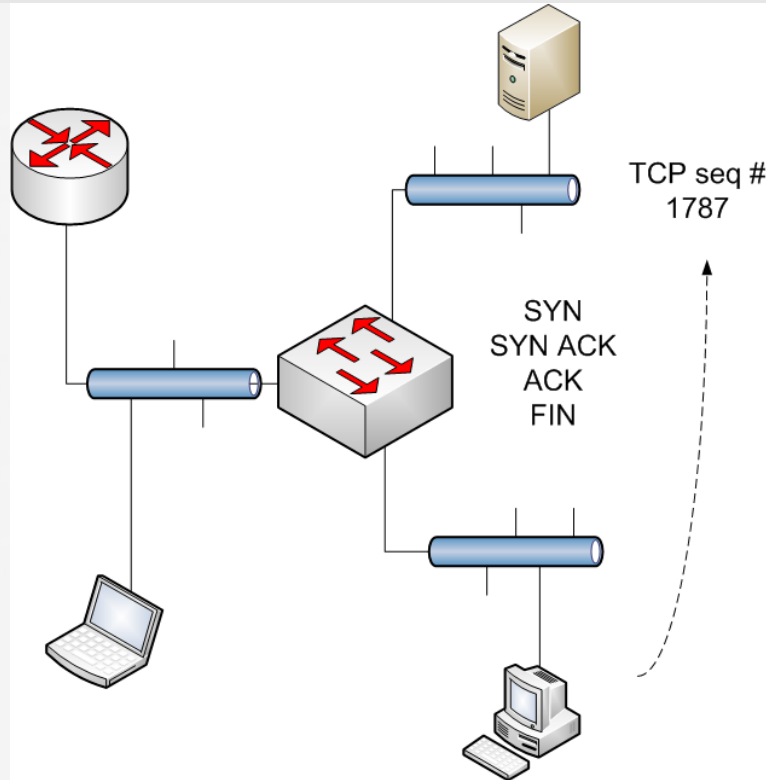
- Packet List:** Shows a list of captured packets with columns for No., Time, Source, and Destination. Packet 363 is highlighted in green.
- Packet Details:** Shows the structure of the selected packet (No. 363). It includes fields like 'Acknowledgment number: 1377', 'Header length: 32 bytes', 'Flags: 0x010 (ACK)', 'window size value: 61', 'Checksum: 0x5b58', and 'Options: (12 bytes), No-Operation (NOP), No-Operation (OFS), No-Operation (OFS), No-Operation (OFS)'. The 'SEQ/ACK analysis' section is expanded, showing '[This is an ACK to the segment in frame: 361]', '[The RTT to ACK the segment was: 0.000244s]', '[TCP Analysis Flags]', '[This is a TCP duplicate ack]', '[Duplicate ACK #: 1]', '[Duplicate to the ACK in frame: 363]', and '[Expert Info (Note/Sequence): Duplicate ACK (Message: Duplicate ACK (#1)) [Severity level: Note]]'.
- Filter Expression Dialog:** A modal dialog box titled 'Wireshark: Filter Expression - Profile: Custom' is open. It has three columns: 'Field name', 'Relation', and 'Value (Unsigned integer, 4 bytes)'. The 'Field name' column lists various TCP-related fields. The 'Relation' column lists operators like 'is present', '==', '!=', '>', '<', '>=', and '<='. The 'Value' column contains the number '3452'. A 'Predefined values' section is empty. At the bottom, there are 'OK' and 'Cancel' buttons.

Wireshark & TCP

» Wireshark can assist with

- Finding latency
- Out-of-order packets
- Retransmissions
- Fragmentation
- More

Network Lab



Questions?