Wireshark Setup

Example Display Filters

Host and port filters

1. `ip.addr==192.168.1.242`
2. `ip.src==192.168.1.242`
3. `ip.dst==10.1.2.3`
4. `tcp.port==80`
5. `tcp.dstport<=1024`

Host and port filters explanations

1. Display packets with source or destination IP 192.168.1.242
2. Display packets with source IP 192.168.1.242
3. Display packets with destination IP 10.1.2.3
4. Display packets with source or destination TCP port 80
5. Display packets with destination TCP port 1024 or less

TCP conversation filter

1. `(ip.addr eq 192.168.1.242 and ip.addr eq 10.1.2.3) and (tcp.port eq 51317 and tcp.port eq 80)`

TCP conversation filter explanation

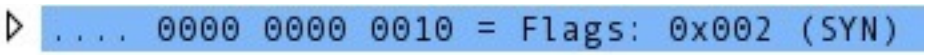
1. Display packets with source or destination IP 192.168.1.242 **and** with source or destination IP 10.1.2.3 **and** with source or destination TCP port 51317 **and** with source or destination TCP port 80

SYN packet filter

1. `tcp.flags==2`
2. `ip.src==192.168.1.242 and tcp.flags==2`

SYN packet filter explanation

1. Show new connection initiations. The value of the TCP flags with only the SYN bit set is 2



2. Display new connections from source IP 192.168.1.242

Other filters

1. `tcp.analysis.flags`
2. `tcp.port!=80`
3. `!tcp.port==80`

Other filters explanation

1. Display any packet with TCP expert infos e.g. Retransmission
2. Display any packet that has a TCP port that is not 80. This WILL display packets with port 80 unless both source and destination ports are 80
3. Do not display any packet with a source or destination TCP port 80

Filter Notes

- Use the Save button next to the filter input field to save often used Display filters
- Wireshark will attempt to auto-complete Display filters showing you what filters are available
- Click the Expression button next to the filter input field to search for filter expressions and build a filter

Further reading on Display Filters

- Wireshark Wiki on Display Filters
- Top 10 Wireshark Filters by Chris Greer