Wireshark filters

Filter types:

Capture filters: This type of filter set before start capturing traffic in Wireshark. This type of filter can't change while capturing traffic. It is generally used for capturing a specific type of traffic.

Example:

- Capture only traffic to or from IP address 172.18.5.4:

  host 172.18.5.4

- Capture traffic to or from a range of IP addresses:

  net 192.168.0.0/24

Display Filters: This type of filter is used to reduce the packets which are showing in Wireshark. This type of filter can be changed while capturing traffic. It is generally used for hiding traffic to analyze the specific type of traffic.

Example:

- Display only traffic from port number 25 or ICMP packets

  tcp.port eq 25 or ICMP

- Display only traffic to or from IP address 192.168.0.87

  ip.addr == 192.168.0.87

❖ Display Filter comparison operators:

English	Alias	C-like	Description	Example
eq	any_eq	==	Equal (any if more than one)	`ip.src == 10.0.0.5`
ne	all_ne	!=	Not equal (all if more than one)	`ip.src != 10.0.0.5`
	all_eq	===	Equal (all if more than one)	`ip.src === 10.0.0.5`
	any_ne	!==	Not equal (any if more than one)	`ip.src !== 10.0.0.5`
gt		>	Greater than	`frame.len > 10`
lt		<	Less than	`frame.len < 128`
ge		>=	Greater than or equal to	`frame.len ge 0x100`
le		<=	Less than or equal to	`frame.len <= 0x20`
contains			Protocol, field or slice contains a value	`sip.To contains "a1762"`
matches		~	Protocol or text field matches a Perl-compatible regular expression	`http.host matches "acme\\.(org|com|net)"`

❖ Display Filter Logical Operations

English	C-like	Description	Example
and	&&	Logical AND	`ip.src==10.0.0.5 and tcp.flags.fin`
or	||	Logical OR	`ip.src==10.0.0.5 or ip.src==192.1.1.1`
xor	^^	Logical XOR	`tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
not	!	Logical NOT	`not llc`

Filter Examples:

❖ Protocal Filter

- ✓ If we need to filter packets from protocols like dns ,http,ftp,icmp,tcp,udp etc.... , Enter protocal name in display filter bar

❖ IPv4 address:

- ✓ **ip.addr == 192.168.0.1** – Display all packets whose source or destination is 192.168.0.1
- ✓ **ip.src==192.168.0.1** - Display all packets the source address is 192.168.0.1
- ✓ **ip.dst==192.168.0.1** – Display all packets the destination address is 192.168.0.1
- ✓ **ip.addr==192.168.0.0/16** – Display all packets in the 192.168 Class-B network
- ✓ **ip.addr == 10.10.50.1 and ip.addr == 10.10.50.100** - Filter by Multiple Ips

❖ Port Filter:

Syntax: Protocal (tcp|udp).port==PortNum

Example:

- ✓ **tcp.port==80 -** Display all packets whose source or destination port is 80 (http packets)
- ✓ **udp.srcport ==53** - Display all packets the source port is 53 (dns packets)
- ✓ **udp.dstport==53** – Display all packets the destination port is 53

when write this filter tcp.port in {80, 443, 8080} equal for
tcp.port == 80 || tcp.port == 443 || tcp.port == 8080

Note: if we don't know the service port is tcp or upd you can write this filter
tcp.port ==PortNum || udp.port==PortNum
Example: tcp.port==53 || upd.port==53

❖ Mac Filter:

- ✓ **eth.addr==00:af:85:aa:06:11** –Display all packets whose source or destination mac is 00:af:85:aa:06:11
- ✓ **eth.dst==00:af:85:aa:06:11** –Display all packets the destination mac is 00:af:85:aa:06:11
- ✓ **eth.src==00:af:85:aa:06:11** –Display all packets the source mac is 00:af:85:aa:06:11

❖ Search and match operators:

Syntax : protocol contains " String text"

Example:

- ✓ **dns contains "wireshark" –** Display all packets the protocol is dns and contains wireshark string.
- ✓ **http contains** " https://www.wireshark.org " – Display all packets the protocal is http and contains https://www.wireshark.org.
- ✓ **http.request.uri matches "(gif)$"** - Display all HTTP requests in which the uri ends with "gif".

❖ Other Examples:

- ✓ **http.request –** Display all HTTP requests.
- ✓ **http.request || http.response –** Display all HTTP request and responses.
- ✓ **tcp.len < 100 –** Display all TCP packets whose data length is less than 100 bytes.
- ✓ **dns.query.name == "www.google.com"** - Display all Dns queries for " www.google.com"
- ✓ **dns and not ip.addr==192.168.10.1** – Display all dns packets and source and destination address not equal 192.168.10.1
- ✓ **tcp.port eq 25 or icmp** - Show only SMTP (port 25) and ICMP traffic

- ✓ **http.request.method=="GET"** – Show only http traffic that used Get Method for request

- ✓ **tcp.port==23 and ip.host==10.0.0.5 -** Capturing all telnet traffic and from a particular host 10.0.0.5

- ✓ **ip.addr == 127.0.0.1 –** Display all IP packets whose source or destination is localhost

Best Wishes