Protocol filters

MAC Address
eth.addr == 23:23:23:ab:ab:ab
eth.src == aa:bb:cc:dd:ee:ff
eth.dst == 11:22:33:44:55:66

IP Address (address or CIDR notation)
ip.addr== 192.168.1.1
ip.dst== 192.168.1.0/24
ip.src== 192.168.1.2

TCP
tcp.port == 80
tcp.srcport== 80
tcp.dstport== 80

UDP
udp.port== 53
udp.srcport==123
udp.dstport==161

ICMP - all ICMP
icmp

ICMP TTL exceeded
icmp.type == 11

DNS Show all DNS packets
dns

DHCP Show all DHCP packets
dhcp

SMB - Show all SMB
smb

SMTP - Show SMTP packets
smtp

FTP - Show FTP packets
ftp && ftp-data

SIP - Show SIP packets
sip

ARP requests and replies
arp

Filter operators

Description	Symbol	Text
equals	==	eq
and	&&	and
or	||	or
not	!	not
not equal	!=	ne
matches		matches
contains		contains
greater than	>	gt
less than	<	lt
greater than or equal	>=	ge

Advanced Filter Examples

All traffic between two subnets
ip.addr==192.168.1.0/24 and ip.addr ==192.168.2.0/24

All packets with a selected text in the TCP data
tcp.segment_data contains “microsoft”

All HTTP requests and replies
http.request and http.request_in

HTTP gets
http.request.method == “GET”

HTTP posts
http.request.method == “POST”

HTTP redirects and errors
http.response.code > 200

Specific text (case sensitive)
tcp contains “password”

Specific text (not case sensitive)
tcp matches “password”

DHCP server declined - DHCPNAK
dhcp.option.dhcp == 6

DHCP client declined - DHCPDECLINE
dhcp.option.dhcp == 4

Wireshark Display Filters Cheat Sheet v1.1b

https://www.lanwan.ninja

Advanced Filter Examples - TLS, DHCP

Packets containing Certificates
tls.handshake.type == 11

Client Hello packets
tls.handshake.type == 1

Server Hello packets
tls.handshake.type == 2

TLS handshake failure packets
tls.alert_message.level

**** TLS troubleshooting ****
(tls.record.content_type || tls.handshake.type || tls.alert_message.level) && tls.record.content_type !=23

DHCP server is not what you expect -
Add your DHCP server to this query to see if any other DHCP servers are answering (notice the !=)

Advanced Filter Examples DNS, Frames

Show packets greater than packet #1500
frame.number > 1500

Show packets after 50 seconds of capture start
frame.time_relative > 50

Show only frames with comments
frame.comment

Specific DNS query
dns.qry.name == “www.lanwin.ninja”

DNS server cannot resolve - no such name
dns.flags.rcode != 0