Packet display rules

Packet display rules or filters as their name imply, allow you to control which packets are displayed by tshark when performing live network capture or when tshark is reading a capture file. The selection criteria is specified using the -R flag and a display filter expression. This is a simple example :
[crayon-6a9d5844f37f8610638851/]
This example displays only IP packets that are issued by or in destination to the IP address 192.168.0.1.

The filter expression can be a logical combination of other filter expressions. Here is a list of various display filters for your reference (do *man wireshark-filters* for more details of display filters):

«Ethernet address 00:08:15:00:08:15»	eth.addr == 00:08:15:00:08:15
«Ethernet type 0×0806 (ARP)»	eth.type == 0×0806
«Ethernet broadcast»	eth.addr == ff:ff:ff:ff:ff:ff
«No ARP»	not arp
«IP only»	ip
«IP address 192.168.0.1»	ip.addr == 192.168.0.1
«IP address isn’t 192.168.0.1, don’t use != for this!»	!(ip.addr == 192.168.0.1)
«IPX only»	ipx
«TCP only»	tcp
«UDP only»	udp
«UDP port isn’t 53 (not **DNS**), don’t use != for this!»	!(tcp.port == 53)
«TCP or UDP port is 80 (**HTTP**)»	tcp.port == 80 || udp.port == 80

«**HTTP**«	http
«No ARP and no **DNS**«	not arp and not (udp.port == 53)
«Non-**HTTP** and non-**SMTP** to/from 192.168.0.1˝	not (tcp.port == 80) and not (tcp.port == 25) and ip.addr == 192.168.0.1