Wireshark filters cheat-sheet

Lesson 3

Protocols	
Filter by protocol	http
IP	
Filter by src ip	ip.src == 192.168.0.1
Filer by dst ip	ip.dst == 192.168.0.1
Filter by any ip	ip.addr == 192.168.0.1
Port	
Filter by src port	tcp.srcport == 80
Filter by dst port	tcp.dstport == 80
Filter by any port	tcp.port == 80
Text	
Filter by text	frame contains "GET"

Logic operators		
Equals	==, eq	tcp.port == 12
Not equals	!=, ne	ip.src != 101.1.1.2
Or	||, or	http **or** dns
and	&&, and	tcp.port == 80 **and** ip.dst == 12.12.2.2
not	!, not	!http

Inspect TCP Stream	Right click a packet -> Follow -> TCP Stream. Client's data will be colored red. Server's data will be colored blue. When done, remember to clear the display filter.