Tabela de Filtros Wireshark

ip.addr == 8.8.8.8	Endereço IP específico
ip.src == 192.168.0.100	Endereço IP origem
ip.dst == 192.168.0.1	Endereço IP destino
eth.dst == 00:11:22:33:44:55	Endereço MAC de destino especifico
icmp && ip.addr == 8.8.8.8	Protocolo ICMP e Endereço IP
dns.qry.name == "example.com"	Consulta de nome de domínio DNS
dns.time < 0.1	Tempo de resposta DNS Ideal menor que 100ms
dns.time > 0.2 && dns	Tempo de resposta DNS delay maior que 200ms
dns.flags.response == 0	Somente consulta DNS
dns.flags.response == 1	Somente resposta DNS
tcp.flags.syn == 1 && tcp.flags.ack == 0	Segmento TCP com flag SYN
tcp.flags.syn == 1 && tcp.flags.ack == 1	Segmento TCP com flag SYN/ACK
tcp.flags.ack == 1	Segmento TCP com flag ACK
tcp.flags.reset == 1	Segmento TCP com flag RST
tcp.flags.push == 1	Segmento TCP com flag PUSH (Real Time Env)
tcp.flags.fin == 1	egmento TCP com flag FIN
tcp.time_delta > 1	Tempo de resposta maior que 1 segundo
tcp.port == 443	Somente porta TCP especifica
udp.port == 53	Somente porta UDP especifica
tcp.srcport < 1024	Somente portas menores que 1024
tcp.analysis.flags	Exibe segmento com problemas
tcp.analysis.lost_segment	Segmento perdido “perda de pacotes”
tcp.analysis.retransmission	Retransmissão “perda de pacotes”
tcp.analysis.window_update	Identificar gargalos de buffer no Servidor HTTP
http.time > 1	Tempo de resposta HTTP maior que 1 segundo
http.request	Requisições HTTP
http contains "string"	Dados HTTP com uma string especifica
http.request.uri == "https://nic.br/"	Domínio específico
http.request.method == "GET"	Método HTTP para recuperar dados
http.request.method == "POST"	Método HTTP para enviar dados
http.response.code == 400	Códigos de status HTTP
tls.handshake.type == 1	Domínios HTTPS/TLS

https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Reference/Status