Wireshark filters

Ethernet

eth.addr - address
eth.dst - destination
eth.ig - IG bit
eth.len - length
eth.lg - LG bit
eth.src - source
eth.trailer - trailer
eth.type - type

ARP Address resolution Protocol

arp.dst.hw_mac -Target MAC address
arp.dst.proto_ipv4 – Target IP address
arp.hw.size - Hardware size
arp.hw.type - Hardware type
arp.opcode - Opcode
arp.proto.size - Protocol size
arp.proto.type - Protocol type
arp.src.hw_mac - Sender MAC address
arp.src.proto_ipv4 – Sender IP address

IPv4

ip.addr - Source or Destination Address
ip.checksum - Header checksum
ip.checksum_bad - Bad
ip.checksum_good - Good
ip.dsfield - Diffrentiated Services Field
ip.dsfield.ce - ECN-CE
ip.dsfield.dscp - Diferrentiated Services Codepoint
ip.dsfield.ect - ECT Capable Transport
ip.dst - Destination
ip.dst_host - Destination host
ip.flags - Flags
ip.flags.df - Don’t fragment
ip.flags.mf - More fragments
ip.flags.rb - Reserved bits
ip.frag_offset - Fragment offset
ip.fragment - IPv4 Fragment

ip.fragment.error -Defragmentation error
ip.fragment.multipletails - Multiple tail fragment found
ip.fragment.overlap - Fragment overlap
ip.fragment.overlap.conflict - Confliting data in fragment overlap
ip.fragment.toolongfragment - Fragment too long
ip.fragments - IPv4 fragments
ip.hdr_len - Header length
ip.host - Source or Destination Host
ip.id - Identification
ip.len - Total length
ip.proto - Protocol
ip.reassembled_in - Reassembled IPv4 in frame
ip.src - Source
ip.src_host - Source host
ip.tos - Type of Service
ip.tos.cost - Cost
ip.tos.delay - Delay
ip.tos.precedence - Precedence
ip.tos.reliability - Reliability
ip.tos.throughput - Throughtput
ip.ttl - Time to live
ip.version - Version

IPv6

ipv6.addr - Source or Destination Address
ipv6.class - Traffic class
ipv6.dst - Destination
ipv6.dst_host - Destination host
ipv6.dst_opt - Destination Option
ipv6.flow - Flow label
ipv6.fragment IPv6 Fragment
ipv6.fragment.error - Defragmentation Error
ipv6.fragment.id - Identification
ipv6.fragment.more - More Fragment
ipv6.fragment.multipletails - Multiple tail fragment found
ipv6.fragment.offset - Offset
ipv6.fragment.overlap - Fragment overlap
ipv6.fragment.overlap.conflict -Confliting data in fragment overlap
ipv6.fragment.toolongfragment - Fragment too long
ipv6.fragments - IPv6 Fragments
ipv6.hlim - Hop limit
ipv6.hop_opt - Hop-by-hop option

ipv6.host - Source or destination host
ipv6.mipv6_home_address - Home address
ipv6.mipv6_length - option length
ipv6.mipv6_type - Option type
ipv6.nxt - Next header
ipv6.opt.pad1 - Pad1
ipv6.opt.padn - PadN
ipv6.plen - Payload lenght
ipv6.reassembled_in - Reassembled in Frame
ipv6.routing_hdr - Routing header type
ipv6.routing_hdr.addr - Address
ipv6.routing_hdr.left - Segments left
ipv6.routing_hdr.type - Type
ipv6.src - Source
ipv6.src_host - Source host
Ipv6.version - Version

TCP

tcp.ack - Anknowlegment number
tcp.checksum - Checksum
tcp.checksum_bad - Bad checksum
tcp.checksum_good - Good checksum
tcp.continuation_to - This is a contiuation to the PDU in frame
tcp.dstport - Destination Port
tcp.flags - Flags
tcp.flags.ack - Acknolegment
tcp.flags.cwr - Congestion Window reduced
tcp.flags.ecn - ECN-Echo
tcp.flags.fin - Fin
tcp.flags.push - Push
tcp.flags.reset - Reset
tcp.flags.syn - Syn
tcp.flags.urg - Urgent
tcp.hdr_len - Header length
tcp.len - TCP Sgment Len
tcp.nxtseq - Next sequent number
tcp.options - TCP options
tcp.options.cc - TCP CC Options
tcp.options.ccecho - TCP CC Echo Option
tcp.options.ccnew - TCP CC New option
tcp.options.echo - TCP echo option
tcp.options.echo_reply - TCP Echo Reply option
tcp.options.md5 - TCP MD5 option

tcp.options.mss - TCP MSS option
tcp.options.mss_val - MSS value
tcp.options.qs - TCP QS option
tcp.options.sack - TCP Sack option
tcp.options.sack_le - TCP Sack Left Edge
tcp.options.sack_perm - TCP Sack Permitted option
tcp.options.sack_re - TCP Sack Right Edge
tcp.options.time_stamp - TCP Timestamp value
tcp.options.wscale - TCP Window Scale option
tcp.options.wscale_val - TCP Window Scale Optin Value
tcp.pdu.last_frame - Last frame of the PDU
tcp.pdu.size - PDU size
tcp.pdu.time - Time until the last segment of this PDU
tcp.port - Source or Destination Port
tcp.reassembled_in - Reassembled PDU in frame
tcp.segment - TCP segment
tcp.segment.error - Reassembling error
tcp.segment.multipletails - Multiple tail segment found
tcp.segment.overlap - Segment ovelap
tcp.segment.overlap.conflict - Conflicting data in segment overlap
tcp.segment.toolongfragment - Segment too long
tcp.segments -Reassembled TCP segments
tcp.seq - Sequence number
tcp.srcport - Source port
tcp.time_delta - Time sence previous frame in the TCP stream
tcp.time_relative - Time since first frame in the TCP stream
tcp.urgent_pointer - Urgent pointer
tcp.window_size - Window size value

UDP

udp.checksum - Checksum
udp.checksum_bad - Bad checksum
udp.checksum_good - Good checksum
udp.dstport - Destination Port
udp.length - Length
udp.port - Source or Destination Port
udp.srcport - Source Port

ICMP

icmp.checksum - Checksum
icmp.checksum_bad - Bad checksum
icmp.code - Code
icmp.ident - Identifier
icmp.mtu - MTU

icmp.redir_gw - Gateway address
icmp.seq - sequence Number
icmp.type - Type

ICMPv6

icmpv6.all_comp - Component
icmpv6.checksum - Checksum
icmpv6.checksum_bad - Bad Checksum
icmpv6.code - Code
icmpv6.comp - Component
icmpv6.haad.ha_addrs - Home Agent Address
icmpv6.identifier - Identifier
icmpv6.option - ICMPv6 Option
icmpv6.option.cga - CGA
icmpv6.option.length - Length
icmpv6.option.name_type.fqdn - FQDN
icmpv6.option.name_x501 - DER Encoer X.501 name
icmpv6.option.rsa.key_hash - Key hash
icmpv6.option.type - Type
icmpv6.ra.cur_hop_limit - Cur hop limit
icmpv6.ra.reachable_time - Reachable time
icmpv6.ra.retrans_timer - Retrans timer
icmpv6.ra.router_lifetime - Router lifetime
icmpv6.recursive_dns_serv - Recursive DNS Server
Icmpv6.type- Type

HTTP

http.accept - Accept
http.accept_encoding - Accept encoding
http.accept_language - Accept language
http.authbasic - Credentials
http.authorization - Authorization
http.cache_control - Cache control
http.connection - Connection
http.content_encoding - Content encoding
http.content_length - Content length
http.content_type - Content type
http.cookie - Cookei
http.date - Date
http.host - Host
http.last_modified - Last modified
http.location - Location
http.notification - Notification
http.proxy_authenticate- Proxy authenticate

http.proxy_authorization - Proxy authorization
http.proxy_connect_host - Proxu connect hostname
http.proxy_connect_port - Proxy connect port
http.referer - Referer
http.request - Request
http.request.method - Request method
http.request.uri - Request URI
http.request.version - Request version
http.response - Response
http.response.code - Status code
http.server - Server
http.set_cookie - Set Cookie
http.transfer_encoding - transfer encoding
http.user_agent - user agent
http.www_authenticate - WWW-Authenticate
http.x_forwarded_for - X-Forwarded For

Operators

- eq or ==
- ne or !=
- gt or >
- lt or <
- ge or >=
- le or <=

Logic

- and or && Logical AND
- or or || Logical OR
- xor or ^^ Logical XOR
- not or ! Logical NOT
- [n] [...] Substring operator