Wireshark Display Filter

Logic

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

Operators

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

Layer 1-Frame

frame.time_relative	**frame**
frame.time	frame.ignored
frame.md5_hash	frame.number
frame.file_off	frame.time_delta
frame.time_invalid	frame.cap_len
frame.ref_time	frame.len
frame.marked	frame.p2p_dir
frame.coloring_rule.string	frame.time_delta_displayed
frame.time_epoch	frame.coloring_rule.name
frame.protocols	frame.link_nr

Layer 2

Frame Relay

fr.upper_dlci	fr.becn
fr.dc	fr.de
fr.third_dlci	fr.chdlctype
fr.cr	fr.dlci
fr.snaptype	fr.control
fr.control.u_modifier_resp	fr.dlcore_control
fr.snap.pid	fr.control.f
fr.control.u_modifier_cmd	fr.ea
fr.snap.oui	fr.control.ftype
fr.control.s_ftype	fr.fecn
fr.second_dlci	fr.control.n_r
fr.control.p	fr.lower_dlci
fr.nlpid	fr.control.n_s

MPLS

mpls.ttl	mpls.bottom
mpls.oam.bip16	mpls.oam.defect_location
mpls.oam.ttsi	mpls.cw.control
mpls.label	mpls.oam.defect_type
mpls.oam.function_type	mpls.cw.res
mpls.exp	mpls.oam.frequency

DTP

dtp.version	dtp.neighbor
dtp.tlv_len	dtp.tlv_type
	vtp.neighbor

VLAN Trunking Protocol

vtp.version	vtp.code
vtp.vlan_info.vlan_type	vtp.vlan_info.802_10_index
vtp.upd_ts	vtp.conf_rev_num
vtp.vlan_info.vlan_name_len	vtp.vlan_info.isl_vlan_id
vtp.upd_id	vtp.followers
vtp.vlan_info.vlan_name	vtp.vlan_info.len
vtp.start_value	vtp.md
vtp.vlan_info.tlv_type	vtp.vlan_info.mtu_size
vtp.seq_num	vtp.md5_digest
vtp.vlan_info.tlv_len	vtp.vlan_info.status.vlan_susp
	vtp.md_len

Ethernet

eth.type	eth.addr
eth.multicast	eth.len
eth.ig	eth.src
eth.trailer	eth.dst
	eth.lg

ARP

arp.opcode	arp.dst.hw_mac
arp.src.proto_ipv4	arp.proto.size
arp.hw.type	arp.dst.proto_ipv4
arp.src.hw_mac	arp.proto.type
	arp.hw.size

IEEE 802.1Q

vlan.trailer	vlan.cfi
vlan.len	vlan.id
vlan.etype	vlan.priority

PPP

ppp.address
ppp.direction
ppp.control
ppp.protocol

Layer 3

ICMPv6

icmpv6.type	icmpv6.all_comp
icmpv6.recursive_dns_serv	icmpv6.checksum
icmpv6.ra.router_lifetime	icmpv6.checksum_bad
icmpv6.ra.retrans_timer	icmpv6.code
icmpv6.ra.reachable_time	icmpv6.comp
icmpv6.ra.cur_hop_limit	icmpv6.haad.ha_addrs
icmpv6.option.type	icmpv6.identifier
icmpv6.option.rsa.key_hash	icmpv6.option
icmpv6.option.name_x501	icmpv6.option.cga
icmpv6.option.name_type.fqdn	icmpv6.option.length
	icmpv6.option.name_type

ICMP

icmp.redir_gw	icmp.checksum
icmp.code	icmp.ident
icmp.type	icmp.seq
icmp.mtu	icmp.checksum_bad

IPv4

ip.version	ip.addr
ip.ttl	ip.checksum
ip.tos.throughput	ip.checksum_bad
ip.tos.reliability	ip.checksum_good
ip.tos.precedence	ip.dsfield
ip.tos.delay	ip.dsfield.ce
ip.tos.cost	ip.dsfield.dscp
ip.tos	ip.dsfield.ect
ip.reassembled_in	ip.dst
ip.src_host	ip.dst_host
ip.src	ip.flags
ip.proto	ip.flags.df
ip.len	ip.flags.mf
ip.id	ip.flags.rb
ip.host	ip.frag_offset
ip.hdr_len	ip.fragment
ip.fragments	ip.fragment.error
ip.fragment.toolongfragment	ip.fragment.multipletails
ip.fragment.overlap.conflict	ip.fragment.overlap

IPv6

ipv6.version	ipv6.addr
ipv6.src_host	ipv6.class
ipv6.src	ipv6.dst
ipv6.routing_hdr.type	ipv6.dst_host
ipv6.routing_hdr.left	ipv6.dst_opt
ipv6.routing_hdr.addr	ipv6.flow
ipv6.routing_hdr	ipv6.fragment
ipv6.reassembled_in	ipv6.fragment.error
ipv6.plen	ipv6.fragment.more
ipv6.opt.padn	ipv6.fragment.multipletails
ipv6.opt.pad1	ipv6.fragment.offset
ipv6.nxt	ipv6.fragment.overlap
ipv6.mipv6_type	ipv6.fragment.overlap.conflict
ipv6.mipv6_length	ipv6.fragment.toolongfragment
ipv6.mipv6_home_address	ipv6.fragments
ipv6.host	ipv6.fragment.id
ipv6.hop_opt	ipv6.hlim

Layer 4

UDP

udp.srcport	udp.checksum
udp.port	udp.checksum_bad
udp.length	udp.checksum_good
	udp.dstport

TCP

tcp.window_size	tcp.ack
tcp.urgent_pointer	tcp.analysis.acks_frame
tcp.time_relative	tcp.analysis.ack_lost_segment
tcp.time_delta	tcp.analysis.ack_rtt
tcp.srcport	tcp.analysis.bytes_in_flight
tcp.seq	tcp.analysis.duplicate_ack
tcp.segments	tcp.analysis.duplicate_ack_frame
tcp.segment.toolongfragment	tcp.analysis.duplicate_ack_num
tcp.segment.overlap.conflict	tcp.analysis.fast_retransmissions
tcp.segment.overlap	tcp.analysis.flags
tcp.segment.multipletails	tcp.analysis.keep_alive
tcp.segment.error	tcp.analysis.keep_alive_ack
tcp.segment	tcp.analysis.lost_segment
tcp.reassembled_in	tcp.analysis.out_of_order
tcp.port	tcp.analysis.retransmission
tcp.pdu.time	tcp.analysis.reused_ports
tcp.pdu.size	tcp.analysis.rto
tcp.pdu.last_frame	tcp.analysis.rto_frame
tcp.options.wscale_val	tcp.analysis.window_full
tcp.options.wscale	tcp.analysis.window_update
tcp.options.time_stamp	tcp.analysis.zero_window
tcp.options.sack_re	tcp.analysis.zero_window_probe
tcp.options.sack_perm	tcp.analysis.zero_window_probe_ack
tcp.options.sack_le	tcp.checksum
tcp.options.sack	tcp.checksum_bad
tcp.options.qs	tcp.checksum_good
tcp.options.mss_val	tcp.continuation_to
tcp.options.mss	tcp.dstport
tcp.options.md5	tcp.flags
tcp.options.echo_reply	tcp.flags.ack
tcp.options.echo	tcp.flags.cwr
tcp.options.ccnew	tcp.flags.ecn
tcp.options.ccecho	tcp.flags.fin
tcp.options.cc	tcp.flags.push
tcp.options	tcp.flags.reset
tcp.nxtseq	tcp.flags.syn
tcp.len>0&&!(tcp.analysis.keep_alive==1)	tcp.flags.urg
tcp.len	tcp.hdr_len

Layer 5

Other/Suspicious

frame matches "join #"	smb2.cmd==3 or smb2.cmd==5
http.user_agent contains "Nmap"	Hated Apps:
ftp.request.command=="USER" && tcp.len>50	Frame offset 100-199 contains "nessus" in lc:
frame[100-199] matches "nessus"	Frame offset 100-199 contains "nessus" in uc/lc:
frame[100-199] contains "nessus"	Suspected nmap traffic (case sensitive):
	IRC Joins
	Long FTP Username
	tftp || irc || bittorrent

TLS

tls.record.content_type == 22	tls
tls.record.content_type == 21	TLS Client Hello Packets
tls.handshake.type == 2	TLS contains "hack" in server name
tls.handshake.type == 1	TLS Encrypted Alert
tls.handshake.extensions_server_name contains "hack"	TLS Handshake Packets:
	TLS Server Hello Packets

OSPF v3 (IPv6)

ospf.v3.router.lsa.flags.w	ospf.v3.as.external.flags
ospf.v3.router.lsa.flags.v	ospf.v3.as.external.flags.e
ospf.v3.router.lsa.flags.e	ospf.v3.as.external.flags.f
ospf.v3.router.lsa.flags.b	ospf.v3.as.external.flags.t
ospf.v3.router.lsa.flags	ospf.v3.lls.drop.tlv
ospf.v3.prefix.options.p	ospf.v3.lls.ext.options.lr
ospf.v3.prefix.options.nu	ospf.v3.lls.ext.options.rs
ospf.v3.prefix.options.mc	ospf.v3.lls.ext.options.tlv
ospf.v3.prefix.options.la	ospf.v3.lls.fsf.tlv
ospf.v3.prefix.options	ospf.v3.lls.relay.added
ospf.v3.options.v6	ospf.v3.lls.relay.options
ospf.v3.options.r	ospf.v3.lls.relay.options.a
ospf.v3.options.n	ospf.v3.lls.relay.options.n
ospf.v3.options.mc	ospf.v3.lls.relay.tlv
ospf.v3.options.l	ospf.v3.lls.rf.tlf
ospf.v3.options.i	ospf.v3.lls.state.options
ospf.v3.options.f	ospf.v3.lls.state.options.a
ospf.v3.options.e	ospf.v3.lls.state.options.n
ospf.v3.options.dc	ospf.v3.lls.state.options.r
ospf.v3.options.af	ospf.v3.lls.state.scs
ospf.v3.options	ospf.v3.lls.state.tlv
ospf.v3.lls.willingness.tlv	ospf.v3.lls.willingness

HTTP

http.x_forwarded_for	http.accept
http.www_authenticate	http.accept_encoding
http.user_agent	http.accept_language
http.transfer_encoding	http.authbasic
http.set_cookie	http.authorization
http.server	http.cache_control
http.response.code	http.connection
http.response	http.content_encoding
http.request.version	http.content_length
http.request.uri	http.content_type
http.request.method	http.cookie
http.request	http.date
http.referer	http.host
http.proxy_connect_port	http.last_modified
http.proxy_connect_host	http.location
http.proxy_authorization	http.notification
	http.proxy_authenticate

RIP

rip.version	rip.auth.passwd
rip.routing_domain	rip.auth.type
rip.route_tag	rip.command
rip.next_hop	rip.family
rip.netmask	rip.ip
	rip.metric

BGP

gp.withdrawn_prefix	bgp.aggregator_as
bbgp.type	bgp.aggregator_origin
bgp.originator_id	bgp.as_path
bgp.origin	bgp.cluster_identifier
bgp.nlri_prefix	bgp.cluster_list
bgp.next_hop	bgp.community_as
bgp.multi_exit_disc	bgp.community_value
bgp.mp_unreach_nlri_ipv4_prefix	bgp.local_pref
bgp.mp_reach_nlri_ipv4_prefix	bgp.mp_nlri_tnl_id

OSPF and OSPFv2

ospf.v2.router.lsa.flags.w	ospf.advrouter
ospf.v2.router.lsa.flags.v	ospf.dbd
ospf.v2.router.lsa.flags.n	ospf.dbd.i
ospf.v2.router.lsa.flags.e	ospf.dbd.m
ospf.v2.router.lsa.flags.b	ospf.dbd.ms
ospf.v2.router.lsa.flags	ospf.dbd.r
ospf.v2.options.o	ospf.lls.ext.options
ospf.v2.options.np	ospf.lls.ext.options.lr
ospf.v2.options.mt	ospf.lls.ext.options.rs
ospf.v2.options.mc	ospf.lsa
ospf.v2.options.l	ospf.lsa.asbr
ospf.v2.options.e	ospf.lsa.asext
ospf.v2.options.dn	ospf.lsa.attr
ospf.v2.options.dc	ospf.lsa.member
ospf.v2.options	ospf.lsa.mpls
ospf.v2.grace.reason	ospf.lsa.network
ospf.v2.grace.period	ospf.lsa.nssa
ospf.v2.grace.ip	ospf.lsa.opaque
ospf.v2.grace	ospf.lsa.router
ospf.srcrouter	ospf.lsa.summary
ospf.oid.remote_node_id	ospf.lsid_opaque_type
ospf.oid.local_node_id	ospf.lsid_te_lsa.instance
ospf.msg.lsupdate	ospf.mpls.bc
ospf.msg.lsreq	ospf.mpls.linkcolor
ospf.msg.lsack	ospf.mpls.linkid
ospf.msg.hello	ospf.mpls.linktype
ospf.msg.dbdesc	ospf.mpls.local_addr
ospf.msg	ospf.mpls.local_id
ospf.mpls.routerid	ospf.mpls.remote_addr
	ospf.mpls.remote_id