Wireshark Display Filter Cheat Sheet

Operators and Logic

eq or ==	lt or <	and or && Logical AND	not or ! Logical NOT
ne or !=	ge or >=	or or || Logical OR	[n] [_] Substring operator
gt or >	le or <=	xor or ^^ Logical XOR	

LAYER 1

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

LAYER 2

Ethernet

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

ARP

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

802.1Q VLAN

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

PPP

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

VLAN Trunking Protocol

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

DTP

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

MPLS

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

Frame Relay

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

LAYER 3

IP v4

ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragments

IP v6

ipv6.addr	ipv6.hop_opt
ipv6.class	ipv6.host

ip.checksum_bad	ip.fragment.toolongfragment	ipv6.dst	ipv6.mipv6_home_address
ip.checksum_good	ip.hdr_len	ipv6.dst_host	ipv6.mipv6_length
ip.dsfield	ip.host	ipv6.dst_opt	ipv6.mipv6_type
ip.dsfield.ce	ip.id	ipv6.flow	ipv6.nxt
ip.dsfield.dscp	ip.len	ipv6.fragment	ipv6.opt.pad1
ip.dsfield.ect	ip.proto	ipv6.fragment.error	ipv6.opt.padn
ip.dst	ip.reassembled_in	ipv6.fragment.id	ipv6.plen
ip.dst_host	ip.src	ipv6.fragment.more	ipv6.reassembled_in
ip.flags	ip.src_host	ipv6.fragment.multipletails	ipv6.routing_hdr
ip.flags.df	ip.tos	ipv6.fragment.offset	ipv6.routing_hdr.addr
ip.flags.mf	ip.tos.cost	ipv6.fragment.overlap	ipv6.routing_hdr.left
ip.flags.rb	ip.tos.delay	ipv6.fragment.overlap.conflict	ipv6.routing_hdr.type
ip.fragment	ip.tos.precedence	ipv6.fragment.toolongfragment	ipv6.src
ip.frag_offset	ip.tos.reliability	ipv6.fragments	ipv6.src_host
ip.fragment.error	ip.tos.throughput	ipv6.hlim	ipv6.version
ip.fragment.multipletails	ip.ttl		
ip.fragment.overlap	ip.version		

Filter out 192.168.1.1:   !ip.addr==192.168.1.1

ICMPv6	
icmpv6.all_comp	icmpv6.option.name_type.fqdn
icmpv6.checksum	icmpv6.option.name_x501
icmpv6.checksum_bad	icmpv6.option.rsa.key_hash
icmpv6.code	icmpv6.option.type
icmpv6.comp	icmpv6.ra.cur_hop_limit
icmpv6.haad.ha_addrs	icmpv6.ra.reachable_time
icmpv6.identifier	icmpv6.ra.retrans_timer
icmpv6.option	icmpv6.ra.router_lifetime
icmpv6.option.cga	icmpv6.recursive_dns_serv
icmpv6.option.length	icmpv6.type
icmpv6.option.name_type	

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

LAYER 4

TCP		TCP – continued	
tcp.ack	tcp.flags.push	tcp.segment.overlap.conflict	tcp.srcport
tcp.analysis.ack_lost_segment	tcp.flags.reset	tcp.time_delta > 1	tcp.time_delta
tcp.analysis.ack_rtt	tcp.flags.syn	tcp.len > 0 && !(tcp.analysis.keep_alive==1)	tcp.time_relative
tcp.analysis.acks_frame	tcp.flags.urg	tcp.segment.toolongfragment	tcp.urgent_pointer
tcp.analysis.bytes_in_flight	tcp.hdr_len	tcp.segments	tcp.window_size
tcp.analysis.duplicate_ack	tcp.len > 0	tcp.seq	
tcp.analysis.duplicate_ack_frame	tcp.nxtseq		
tcp.analysis.duplicate_ack_num	tcp.options		
tcp.analysis.fast_retransmissions	tcp.options.cc		
tcp.analysis.flags	tcp.options.ccecho		
tcp.analysis.keep_alive	tcp.options.ccnew		
tcp.analysis.keep_alive_ack	tcp.options.echo		
tcp.analysis.lost_segment	tcp.options.echo_reply		
tcp.analysis.out_of_order	tcp.options.md5		
tcp.analysis.retransmission	tcp.options.mss		
tcp.analysis.reused_ports	tcp.options.mss_val		
tcp.analysis.rto	tcp.options.qs		
tcp.analysis.rto_frame	tcp.options.sack		
tcp.analysis.window_full	tcp.options.sack_le		
tcp.analysis.window_update	tcp.options.sack_perm		

Examples:

Just SYN Packets:	(tcp.flags.syn == 1) && (tcp.flags.ack ==0)
TCP with PSH set:	tcp.flags.psh==1
TCP connection refusal/ACK scan:	tcp.flags.reset==1 && tcp.flags.ack==1 && tcp.seq==1 && tcp.ack==1
SYN/ACK (Bitwise):	tcp.flags & 0x12
SYN and non-zero ACK#:	tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.ack==0
Port 443 or 4430 or 4434:	tcp.port in {443 4430..4434}
Data in Urgent Field:	tcp.urgent_pointer>0

Get the TCP Profile:

https://www.cellstream.com/resources/wireshark-profiles-repository/262-a-wireshark-tcp-troubleshooting-profile/file

tcp.analysis.zero_window	tcp.options.sack_re
tcp.analysis.zero_window_probe	tcp.options.time_stamp
tcp.analysis.zero_window_probe_ack	tcp.options.wscale
tcp.checksum	tcp.options.wscale_val
tcp.checksum_bad	tcp.pdu.last_frame
tcp.checksum_good	tcp.pdu.size
tcp.continuation_to	tcp.pdu.time
tcp.dstport	tcp.port
tcp.flags	tcp.reassembled_in
tcp.flags.ack	tcp.segment
tcp.flags.cwr	tcp.segment.error
tcp.flags.ecn	tcp.segment.multipletails
tcp.flags.fin	tcp.segment.overlap

UDP

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

LAYER 5 – Applications and Routing Protocols

HTTP

http.accept	http.proxy_authorization
http.accept_encoding	http.proxy_connect_host
http.accept_language	http.proxy_connect_port
http.authbasic	http.referer
http.authorization	http.request
http.cache_control	http.request.method
http.connection	http.request.uri
http.content_encoding	http.request.version
http.content_length	http.response
http.content_type	http.response.code
http.cookie	http.server
http.date	http.set_cookie
http.host	http.time > 1
http.last_modified	http.transfer_encoding
http.location	http.user_agent
http.notification	http.www_authenticate
http.proxy_authenticate	http.x_forwarded_for

HTTP Get not on port 80	frame contains "GET" && !tcp.port==80
HTTP Redirections	http.response.code>299 && http.response.code<400
HTTP .exe,.zip,.jar objects	http.request.uri matches "\.(exe|zip|jar)$"
HTTP PUT and POST messages	http.request.method in {PUT POST}

OSPF and OSPFv2

ospf.advrouter	ospf.mpls.routerid
ospf.dbd	ospf.msg
ospf.dbd.i	ospf.msg.dbdesc
ospf.dbd.m	ospf.msg.hello
ospf.dbd.ms	ospf.msg.lsack
ospf.dbd.r	ospf.msg.lsreq
ospf.lls.ext.options	ospf.msg.lsupdate
ospf.lls.ext.options.lr	ospf.oid.local_node_id
ospf.lls.ext.options.rs	ospf.oid.remote_node_id
ospf.lsa	ospf.srcrouter

RIPv2

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

BGP

bgp.aggregator_as	bgp.mp_reach_nlri_ipv4_prefix
bgp.aggregator_origin	bgp.mp_unreach_nlri_ipv4_prefix
bgp.as_path	bgp.multi_exit_disc
bgp.cluster.identifier	bgp.next.hop
bgp.cluster_list	bgp.nlri_prefix
bgp.community_as	bgp.origin
bgp.community_value	bgp.originator_id
bgp.local_pref	bgp.type
bgp.mp_nlri_tnl_id	bgp.withdrawn_prefix

TLS

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

OSPFv3 (IP v6)

ospf.v3.as.external.flags	ospf.v3.lls.willingness.tlv
ospf.v3.as.external.flags.e	ospf.v3.options
ospf.v3.as.external.flags.f	ospf.v3.options.af
ospf.v3.as.external.flags.t	ospf.v3.options.dc
ospf.v3.lls.drop.tlv	ospf.v3.options.e
ospf.v3.lls.ext.options.lr	ospf.v3.options.f
ospf.v3.lls.ext.options.rs	ospf.v3.options.i

ospf.lsa.asbr	ospf.v2.grace	ospf.v3.lls.ext.options.tlv	ospf.v3.options.l
ospf.lsa.asext	ospf.v2.grace.ip	ospf.v3.lls.fsf.tlv	ospf.v3.options.mc
ospf.lsa.attr	ospf.v2.grace.period	ospf.v3.lls.relay.added	ospf.v3.options.n
ospf.lsa.member	ospf.v2.grace.reason	ospf.v3.lls.relay.options	ospf.v3.options.r
ospf.lsa.mpls	ospf.v2.options	ospf.v3.lls.relay.options.a	ospf.v3.options.v6
ospf.lsa.network	ospf.v2.options.dc	ospf.v3.lls.relay.options.n	ospf.v3.prefix.options
ospf.lsa.nssa	ospf.v2.options.dn	ospf.v3.lls.relay.tlv	ospf.v3.prefix.options.la
ospf.lsa.opaque	ospf.v2.options.e	ospf.v3.lls.rf.tlf	ospf.v3.prefix.options.mc
ospf.lsa.router	ospf.v2.options.l	ospf.v3.lls.state.options	ospf.v3.prefix.options.nu
ospf.lsa.summary	ospf.v2.options.mc	ospf.v3.lls.state.options.a	ospf.v3.prefix.options.p
ospf.lsid_opaque_type	ospf.v2.options.mt	ospf.v3.lls.state.options.n	ospf.v3.router.lsa.flags
ospf.lsid_te_lsa.instance	ospf.v2.options.np	ospf.v3.lls.state.options.r	ospf.v3.router.lsa.flags.b
ospf.mpls.bc	ospf.v2.options.o	ospf.v3.lls.state.scs	ospf.v3.router.lsa.flags.e
ospf.mpls.linkcolor	ospf.v2.router.lsa.flags	ospf.v3.lls.state.tlv	ospf.v3.router.lsa.flags.v
ospf.mpls.linkid	ospf.v2.router.lsa.flags.b	ospf.v3.lls.willingness	ospf.v3.router.lsa.flags.w
ospf.mpls.linktype	ospf.v2.router.lsa.flags.e		
ospf.mpls.local_addr	ospf.v2.router.lsa.flags.n		
ospf.mpls.local_id	ospf.v2.router.lsa.flags.v		
ospf.mpls.remote_addr	ospf.v2.router.lsa.flags.w		
ospf.mpls.remote_id			

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