

Wireshark Display Filter Cheat Sheet

www.cellstream.com www.netscionline.com

DISPLAY FILTER SYNTAX

PROTOCOL.STRING1.STRING2 ComparisonOperator VALUE LogicalOperator SECOND EXPRESSION

ip.src==192.168.1.1 and ip.dst==192.168.1.2

Hint: use Right-Click to select Apply as a Filter

Green is good syntax, Red is bad syntax

COMPARISON OPERATORS and LOGICAL OPERATORS

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	

WIRESHARK KEYBOARD SHORTCUTS

Key Sequence	Action	Key Sequence	Action
Tab or Shift+Tab	Move between screen elements	Alt+Right Arrow or Option+Right Arrow	Move to next packet
Down Arrow	Move to next packet or detail item	Right Arrow	In Packet Detail, opens the selected tree item
Up Arrow	Move to previous packet or detail item	Shift+Right Arrow	In Packet Detail, opens selected tree item and all of its subtrees
CTRL+Down Arrow or F8	Move to next packet, even if packet list is not focused	Ctrl+Right Arrow	Opens all tree items in packet details
Ctrl+Up Arrow or F7	Move to previous packet, even if packet list is not focused	Ctrl+Left Arrow	Closes all tree items in packet details
Ctrl+.	Move to next (IP, TCP,UDP) packet in conversation	Backspace	Jumps to parent node in packet details
Ctrl+,	Move to previous (IP, TCP,UDP) packet in conversation	Return or Enter	Toggles selected tree item in packet details

EXAMPLE DISPLAY FILTERS

DEFAULT DISPLAY FILTERS		COMMONLY USED EXAMPLES	
Ethernet address 00:00:5e:00:53:0c	eth.addr == 00:00:5e:00:53:00	Wireshark Filter by IP	ip.addr == 10.10. 50.1
Ethernet type 0x0806 (ARP)	eth.type == 0x0806	Filter by Destination IP	ip.dst == 10.10. 50.1
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff	Filter by Source IP	ip.src == 10.10. 50.1
No ARP	not arp	Filter by IP range	ip.addr >= 10.10. 50.1 and ip.addr <= 10.10. 50.100
IPv4 only	ip	Filter by Multiple Ips	ip.addr == 10.10. 50.1 and ip.addr == 10.10. 50.100
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1	Filter out IP address	!(ip.addr == 10.10. 50.1)
IPv4 address isn't 192.0.2.1 (don't use != for this)	!(ip.addr == 192.0.2.1)	Filter subnet	ip.addr == 10.10. 50.1/ 24
IPv6 only	ipv6	Filter by port	tcp.port == 25
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1	Filter by destination port	tcp.dstport == 23
IPX only	ipx	Filter by ip address and port	ip.addr == 10.10. 50.1 and Tcp.port == 25
TCP only	tcp	Filter by URL	http.host == "host name"
UDP only	udp	Filter by time stamp	frame.time >= " June 02, 2019 18:04:00 "
Non-DNS	!(udp.port == 53 tcp.port == 53)	Filter SYN flag	Tcp.flags.syn == 1
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80	Filter SYN flag	Tcp.flags.syn == 1 and tcp.flags.ack == 0
HTTP	http	Wireshark Beacon Filter	wlan.fc.type_subtype == 0x08
No ARP and no DNS	not arp and !(udp.port == 53)	Wireshark broadcast filter	eth.dst == ff:ff:ff:ff:ff:ff
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.port in {80,25}	Wireshark multicast filter	(eth.dst[0] & 1)
		Host name filter	ip.host == hostname
		MAC address filter	eth.addr == 00:70:f4:23:18:c4
		RST flag filter	tcp.flag.reset == 1

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		ARP	
eth.addr	eth.multicast	arp.dst.hw_mac	arp.proto.size
eth.dst	eth.src	arp.dst.proto_ipv4	arp.proto.type
eth.ig	eth.trailer	arp.hw.size	arp.src.hw_mac
eth.len	eth.type	arp.hw.type	arp.src.proto_ipv4
eth.lg		arp.opcode	
802.1Q VLAN		PPP	
vlan.cfi	vlan.len	ppp.address	ppp.direction
vlan.etype	vlan.priority	ppp.control	ppp.protocol
vlan.id	vlan.trailer		
VLAN Trunking Protocol		DTP	
vtp.code	vtp.version	dtb.neighbor	dtb.tlv_type
vtp.conf_rev_num	vtp.vlan_info.802_10_index	dtb.tlv_len	dtb.version
vtp.followers	vtp.vlan_info.isl_vlan_id		
vtp.md	vtp.vlan_info.len	MPLS	
vtp.md5_digest	vtp.vlan_info.mtu_size	mpls.bottom	mpls.oam.defect_location
vtp.md_len	vtp.vlan_info.status.vlan_suspend	mpls.cw.control	mpls.oam.defect_type
vtp.neighbor	vtp.vlan_info.tlv_len	mpls.cw.res	mpls.oam.frequency
vtp.seq_num	vtp.vlan_info.tlv_type	mpls.exp	mpls.oam.function_type
vtp.start_value	vtp.vlan_info.vlan_name	mpls.label	mpls.oam.ttsi
vtp.upd_id	vtp.vlan_info.vlan_name_len	mpls.aom.bip16	mpls.ttl
vtp.upd_ts	vtp.vlan_info.vlan_type		
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 v6	
ip.addr	ip.fragment.overlap.conflict	ipv6.addr	ipv6.hop_opt
ip.checksum	ip.fragments	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	ICMPv6	

ip.fragment.overlap	ip.version
Filter out 192.168.1.1:	!ip.addr==192.168.1.1

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.analysis.ack_lost_segment	tcp.flags.reset
tcp.analysis.ack_rtt	tcp.flags.syn
tcp.analysis.acks_frame	tcp.flags.urg
tcp.analysis.bytes_in_flight	tcp.hdr_len
tcp.analysis.duplicate_ack	tcp.len > 0
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
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

tcp.segment.overlap.conflict	tcp.srcport
tcp.time_delta > 1	tcp.time_delta
tcp.len > 0 && !(tcp.analysis.keep_alive==1)	tcp.time_relative
tcp.segment.toolongfragment	tcp.urgent_pointer
tcp.segments	tcp.window_size
tcp.seq	

Examples:

Just SYN Packets:

TCP with PSH set:

TCP connection refusal/ACK scan:

SYN/ACK (Bitwise):

SYN and non-zero ACK#:

Port 443 or 4430 or 4434:

Data in Urgent Field:

(tcp.flags.syn == 1) && (tcp.flags.ack == 0)
tcp.flags.psh==1
tcp.flags.reset==1 && tcp.flags.ack==1 && tcp.seq==1 && tcp.ack==1
tcp.flags & 0x12
tcp.flags.syn==1 && tcp.flags.ack==0 && tcp.ack==0
tcp.port in {443 4430..4434}
tcp.urgent_pointer>0

Get the TCP Profile:

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

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

LAYER 5 – Applications and Routing Protocols			
HTTP		RIPv2	

http.accept	http.proxy_authorization
http.accept_encoding	http.proxy_connect_host
http.accept_language	http.proxy_connect_port
http.authbasic	http.referer

rip.auth.passwd	rip.netmask
rip.auth.type	rip.next_hop
rip.command	rip.route_tag
rip.family	rip.routing_domain

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
 HTTP Redirections
 HTTP .exe,.zip,.jar objects
 HTTP PUT and POST messages

frame contains "GET" && !tcp.port==80
 http.response.code>299 && http.response.code<400
 http.request.uri matches "\.(exe|zip|jar)\$"
 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
ospf.lsa.asbr	ospf.v2.grace
ospf.lsa.asext	ospf.v2.grace.ip
ospf.lsa.attr	ospf.v2.grace.period
ospf.lsa.member	ospf.v2.grace.reason
ospf.lsa.mpls	ospf.v2.options
ospf.lsa.network	ospf.v2.options.dc
ospf.lsa.nssa	ospf.v2.options.dn
ospf.lsa.opaque	ospf.v2.options.e
ospf.lsa.router	ospf.v2.options.l
ospf.lsa.summary	ospf.v2.options.mc
ospf.lsid_opaque_type	ospf.v2.options.mt
ospf.lsid_te_lsa.instance	ospf.v2.options.np
ospf.mpls.bc	ospf.v2.options.o
ospf.mpls.linkcolor	ospf.v2.router.lsa.flags
ospf.mpls.linkid	ospf.v2.router.lsa.flags.b
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	

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.v3.lls.ext.options.tlv	ospf.v3.options.l
ospf.v3.lls.fsf.tlv	ospf.v3.options.mc
ospf.v3.lls.relay.added	ospf.v3.options.n
ospf.v3.lls.relay.options	ospf.v3.options.r
ospf.v3.lls.relay.options.a	ospf.v3.options.v6
ospf.v3.lls.relay.options.n	ospf.v3.prefix.options
ospf.v3.lls.relay.tlv	ospf.v3.prefix.options.la
ospf.v3.lls.rf.tlv	ospf.v3.prefix.options.mc
ospf.v3.lls.state.options	ospf.v3.prefix.options.nu
ospf.v3.lls.state.options.a	ospf.v3.prefix.options.p
ospf.v3.lls.state.options.n	ospf.v3.router.lsa.flags
ospf.v3.lls.state.options.r	ospf.v3.router.lsa.flags.b
ospf.v3.lls.state.scs	ospf.v3.router.lsa.flags.e
ospf.v3.lls.state.tlv	ospf.v3.router.lsa.flags.v
ospf.v3.lls.willingness	ospf.v3.router.lsa.flags.w

Other/Suspicious

smb2.cmd==3 or smb2.cmd==5	
Hated Apps:	tfpt 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

You can check out our Wireshark Profile Repository here:

<https://www.cellstream.com/resources/wireshark-profiles-repository>

Also check out our Wireshark videos on YouTube:

<https://www.youtube.com/playlist?list=PL-nDeWT9WTjEwyPqQvKupmW9V9DZD3Jiq>