Wireshark Display Filter Cheat Sheet

www.cellstream.com www.netscionline.com

Operators and Logic

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

LAYER 1

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

LAYER 2

Ethernet

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

ARP

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

802.1Q VLAN

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

PPP

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

VLAN Trunking Protocol

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

DTP

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

MPLS

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

Frame Relay

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

LAYER 3

IP v4

- ip.addr
- ip.checksum
- ip.checksum_bad
- ip.checksum_good
- ip.dsfield
- ip.fragment.overlap.conflict
- ip.fragments
- ip.fragment.toolongfragment
- ip.hdr_len
- ip.host

IP v6

- ipv6.addr
- ipv6.class
- ipv6.dst
- ipv6.dst_host
- ipv6.dst_opt
- ipv6.hop_opt
- ipv6.host
- ipv6.mipv6_home_address
- ipv6.mipv6_length
- ipv6.mipv6_type

ip.dsfield.ce
ip.dsfield.dscp
ip.dsfield.ect
ip.dst
ip.dst_host
ip.flags
ip.flags.df
ip.flags.mf
ip.flags.rb
ip.fragment
ip.frag_offset
ip.fragment.error
ip.fragment.multipletails
ip.fragment.overlap

ip.id
ip.len
ip.proto
ip.reassembled_in
ip.src
ip.src_host
ip.tos
ip.tos.cost
ip.tos.delay
ip.tos.precedence
ip.tos.reliability
ip.tos.throughput
ip.ttl
ip.version

Filter out 192.168.1.1: !ip.addr==192.168.1.1

ICMP

icmp.checksum
icmp.checksum_bad
icmp.code
icmp.ident

icmp.mtu
icmp.redir_gw
icmp.seq
icmp.type

ipv6.flow
ipv6.fragment
ipv6.fragment.error
ipv6.fragment.id
ipv6.fragment.more
ipv6.fragment.multipletails
ipv6.fragment.offset
ipv6.fragment.overlap
ipv6.fragment.overlap.conflict
ipv6.fragment.toolongfragment
ipv6.fragments
ipv6.hlim

ipv6.nxt
ipv6.opt.pad1
ipv6.opt.padn
ipv6.plen
ipv6.reassembled_in
ipv6.routing_hdr
ipv6.routing_hdr.addr
ipv6.routing_hdr.left
ipv6.routing_hdr.type
ipv6.src
ipv6.src_host
ipv6.version

ICMPv6

icmpv6.all_comp
icmpv6.checksum
icmpv6.checksum_bad
icmpv6.code
icmpv6.comp
icmpv6.haad.ha_addrs
icmpv6.identifier
icmpv6.option
icmpv6.option.cga
icmpv6.option.length
icmpv6.option.name_type

icmpv6.option.name_type.fqdn
icmpv6.option.name_x501
icmpv6.option.rsa.key_hash
icmpv6.option.type
icmpv6.ra.cur_hop_limit
icmpv6.ra.reachable_time
icmpv6.ra.retrans_timer
icmpv6.ra.router_lifetime
icmpv6.recursive_dns_serv
icmpv6.type

LAYER 4

TCP

tcp.ack
tcp.analysis.ack_lost_segment
tcp.analysis.ack_rtt
tcp.analysis.acks_frame
tcp.analysis.bytes_in_flight
tcp.analysis.duplicate_ack
tcp.analysis.duplicate_ack_frame
tcp.analysis.duplicate_ack_num
tcp.analysis.fast_retransmissions
tcp.analysis.flags
tcp.analysis.keep_alive
tcp.analysis.keep_alive_ack
tcp.analysis.lost_segment
tcp.analysis.out_of_order
tcp.analysis.retransmission
tcp.analysis.reused_ports
tcp.analysis.rto
tcp.analysis.rto_frame
tcp.analysis.window_full
tcp.analysis.window_update
tcp.analysis.zero_window
tcp.analysis.zero_window_probe
tcp.analysis.zero_window_probe_ack
tcp.checksum
tcp.checksum_bad
tcp.checksum_good
tcp.continuation_to

tcp.flags.push
tcp.flags.reset
tcp.flags.syn
tcp.flags.urg
tcp.hdr_len
tcp.len > 0
tcp.nxtseq
tcp.options
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echo_reply
tcp.options.md5
tcp.options.mss
tcp.options.mss_val
tcp.options.qs
tcp.options.sack
tcp.options.sack_le
tcp.options.sack_perm
tcp.options.sack_re
tcp.options.time_stamp
tcp.options.wscale
tcp.options.wscale_val
tcp.pdu.last_frame
tcp.pdu.size
tcp.pdu.time

TCP – continued

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

tcp.srcport
tcp.time_delta
tcp.time_relative
tcp.urgent_pointer
tcp.window_size

<u>Examples:</u>

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

UDP

udp.checksum
udp.checksum_bad
udp.checksum_good
udp.dstport

udp.length
udp.port
udp.srcport

tcp.dstport
tcp.flags
tcp.flags.ack
tcp.flags.cwr
tcp.flags.ecn
tcp.flags.fin
tcp.port
tcp.reassembled_in
tcp.segment
tcp.segment.error
tcp.segment.multipletails
tcp.segment.overlap

LAYER 5 – Applications and Routing Protocols

HTTP

http.accept
http.accept_encoding
http.accept_language
http.authbasic
http.authorization
http.cache_control
http.connection
http.content_encoding
http.content_length
http.content_type
http.cookie
http.date
http.host
http.last_modified
http.location
http.notification
http.proxy_authenticate
http.proxy_authorization
http.proxy_connect_host
http.proxy_connect_port
http.referer
http.request
http.request.method
http.request.uri
http.request.version
http.response
http.response.code
http.server
http.set_cookie
http.time > 1
http.transfer_encoding
http.user_agent
http.www_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.dbd
ospf.dbd.i
ospf.dbd.m
ospf.dbd.ms
ospf.dbd.r
ospf.lls.ext.options
ospf.lls.ext.options.lr
ospf.lls.ext.options.rs
ospf.lsa
ospf.lsa.asbr
ospf.lsa.asext
ospf.lsa.attr
ospf.lsa.member
ospf.lsa.mpls
ospf.lsa.network
ospf.lsa.nssa
ospf.lsa.opaque
ospf.lsa.router
ospf.lsa.summary
ospf.lsid_opaque_type
ospf.mpls.routerid
ospf.msg
ospf.msg.dbdesc
ospf.msg.hello
ospf.msg.lsack
ospf.msg.lsreq
ospf.msg.lsupdate
ospf.oid.local_node_id
ospf.oid.remote_node_id
ospf.srcrouter
ospf.v2.grace
ospf.v2.grace.ip
ospf.v2.grace.period
ospf.v2.grace.reason
ospf.v2.options
ospf.v2.options.dc
ospf.v2.options.dn
ospf.v2.options.e
ospf.v2.options.l
ospf.v2.options.mc
ospf.v2.options.mt

RIPv2

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

BGP

bgp.aggregator_as
bgp.aggregator_origin
bgp.as_path
bgp.cluster.identifier
bgp.cluster_list
bgp.community_as
bgp.community_value
bgp.local_pref
bgp.mp_nlri_tnl_id
bgp.mp_reach_nlri_ipv4_prefix
bgp.mp_unreach_nlri_ipv4_prefix
bgp.multi_exit_disc
bgp.next.hop
bgp.nlri_prefix
bgp.origin
bgp.originator_id
bgp.type
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.as.external.flags.e
ospf.v3.as.external.flags.f
ospf.v3.as.external.flags.t
ospf.v3.lls.drop.tlv
ospf.v3.lls.ext.options.lr
ospf.v3.lls.ext.options.rs
ospf.v3.lls.ext.options.tlv
ospf.v3.lls.fsf.tlv
ospf.v3.lls.relay.added
ospf.v3.lls.relay.options
ospf.v3.lls.relay.options.a
ospf.v3.lls.relay.options.n
ospf.v3.lls.relay.tlv
ospf.v3.lls.rf.tlf
ospf.v3.lls.state.options
ospf.v3.lls.state.options.a
ospf.v3.lls.state.options.n
ospf.v3.lls.willingness.tlv
ospf.v3.options
ospf.v3.options.af
ospf.v3.options.dc
ospf.v3.options.e
ospf.v3.options.f
ospf.v3.options.i
ospf.v3.options.l
ospf.v3.options.mc
ospf.v3.options.n
ospf.v3.options.r
ospf.v3.options.v6
ospf.v3.prefix.options
ospf.v3.prefix.options.la
ospf.v3.prefix.options.mc
ospf.v3.prefix.options.nu
ospf.v3.prefix.options.p
ospf.v3.router.lsa.flags

ospf.lsid_te_lsa.instance
ospf.mpls.bc
ospf.mpls.linkcolor
ospf.mpls.linkid
ospf.mpls.linktype
ospf.mpls.local_addr
ospf.mpls.local_id
ospf.mpls.remote_addr
ospf.mpls.remote_id

ospf.v2.options.np
ospf.v2.options.o
ospf.v2.router.lsa.flags
ospf.v2.router.lsa.flags.b
ospf.v2.router.lsa.flags.e
ospf.v2.router.lsa.flags.n
ospf.v2.router.lsa.flags.v
ospf.v2.router.lsa.flags.w

ospf.v3.lls.state.options.r
ospf.v3.lls.state.scs
ospf.v3.lls.state.tlv
ospf.v3.lls.willingness

ospf.v3.router.lsa.flags.b
ospf.v3.router.lsa.flags.e
ospf.v3.router.lsa.flags.v
ospf.v3.router.lsa.flags.w

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

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