



@hackinarticles



<https://github.com/ignitetechnologies>



<https://in.linkedin.com/company/hackingarticles>

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

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

Logic

Operators

Wireshark Display Filter

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_rulestring	frame.time_delta_displayed
frame.time_epoch	frame.coloring_rule.name
frame.protocols	frame.link_nr

Layer 2

Frame Relay		Ethernet	
fr.upper_dlcI	fr.been	eth.type	eth.addr
fr.dc	fr.de	eth.multicast	eth.len
fr.third_dlcI	fr.chdlctype	eth.ig	eth.src
fr.cr	fr.dlcI	eth.trailer	eth.dst
fr.snaptype	fr.control	eth.ig	
fr.control_u_modifier_resp	fr.dlcore_control		
fr.snap.pid	fr.control.f	ARP	
fr.control_u_modifier_cmd	fr.ea	arp.opcode	arp.dst.hw_mac
fr.snap.poui	fr.control.ftype	arp.src.proto_ipv4	arp.proto.size
fr.controls.ftype	fr.fcen	arp.hw.type	arp.dst.proto_ipv4
fr.second_dlcI	fr.control.n_r	arp.src.hw_mac	arp.proto.type
fr.control.p	fr.lower_dlcI	arp.hw.size	
fr.nlpid	fr.control.n_s	IEEE 802.1Q	
		vlan.trailer	vlan.cfi
		vlan.len	vlan.id
		vlan.type	vlan.priority
MPLS		PPP	
mpls.ttl	mpls.bottom	ppp.address	
mpls.oam.bip16	mpls.oam.defect_location	ppp.direction	
mpls.oam.ttsi	mpls.cw.control	ppp.control	
mpls.label	mpls.oam.defect_type	ppp.protocol	
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		

Layer 3

ICMPv6		IPv4	
icmpv6.type	icmpv6.all_comp	ip.version	ip.addr
icmpv6.recursive_dns_serv	icmpv6.checksum	ip.ttl	ip.checksum
icmpv6.ra.router_lifetime	icmpv6.checksum_bad	ip.tos.throughput	ip.checksum_bad
icmpv6.ra.retrans_timer	icmpv6.code	ip.tos.reliability	ip.checksum_good
icmpv6.ra.reachable_time	icmpv6.comp	ip.tos.precedence	ip.dsfield
icmpv6.ra.cur_hop_limit	icmpv6.haad.ha_addrs	ip.tos.delay	ip.dsfield.ce
icmpv6.option.type	icmpv6.identifier	ip.tos.cost	ip.dsfield.dscp
icmpv6.option.rsa_key_hash	icmpv6.option	ip.tos	ip.dsfield.dect
icmpv6.option.name_x501	icmpv6.option.cga	ip.reassembled_in	ip.dst
icmpv6.option.name_typefqdn	icmpv6.option.length	ip.src_host	ip.dst_host
	icmpv6.option.name_type	ip.src	ip.flags
ICMP		ip.proto	ip.flags.df
icmp.predir_gw	icmp.checksum	ip.len	ip.flags.mf
icmp.code	icmp.ident	ip.id	ip.flags.rb
icmp.type	icmp.seq	ip.host	ip.frag_offset
icmp.mtu	icmp.checksum_bad	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.padh	ipv6.fragment.multipletails		
ipv6.opt.padh1	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		TCP	
udp.srcport	udp.checksum	tcp.window_size	tcp.ack
udp.port	udp.checksum_bad	tcp.urgent_pointer	tcp.analysis.acks_frame
udp.length	udp.checksum_good	tcp.time_relative	tcp.analysis.ack_lost_segment
	udp.dstport	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.cs	tcp.checksum_good
		tcp.options.mss_val	tcp.continuation_to
		tcp.options.miss	tcp.dstport
		tcp.options.md5	tcp.flags
		tcp.options.echo_reply	tcp.flags.ack
		tcp.options.echo	tcp.flags.cwr
		tcp.options.cnew	tcp.flags.ecn
		tcp.options.cchecho	tcp.flags.fin
		tcp.options.cc	tcp.flags.push
		tcp.options	tcp.flags.reset
		tcp.nextseq	tcp.flags.syn
		tcp.len > 0 && (tcp.analysis.keep_alive == 1)	tcp.flags.urg
		tcp.len	tcp.hdr_len

Other/Suspicious		HTTP	
frame matches "join #"	smb2.cmd==3 or smb2.cmd==5	http.x_forwarded_for	http.accept
http.user_agent contains "Nmap"	Hated Apps:	http.www_authenticate	http.accept_encoding
ftp.request.command=="USER" && tcp.len>50	Frame offset 100-199 contains "nessus" in lc	http.user_agent	http.accept_language
frame[100-199] matches "nessus"	Frame offset 100-199 contains "nessus" in uc	http.transfer_encoding	http.authbasic
frame[100-199] contains "nessus"	Suspected nmap traffic (case sensitive):	http.set_cookie	http.authorization
	IRC Joins	http.server	http.cache_control
	Long FTP Username	http.response.code	http.connection
	tfip irc bittorrent	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
		bgp.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	
		ospfv2.router.isa.flags.w	ospf.adrouter
		ospfv2.router.isa.flags.v	ospf.dbd
		ospfv2.router.isa.flags.n	ospf.dbd.i
		ospfv2.router.isa.flags.e	ospf.dbd.m
		ospfv2.router.isa.flags.b	ospf.dbd.ms
		ospfv2.router.isa.flags	ospf.dbd.r
		ospfv2.options.o	ospf.fls.ext.options
		ospfv2.options.np	ospf.fls.ext.options.lr
		ospfv2.options.mt	ospf.fls.ext.options.rs
		ospfv2.options.mc	ospf.isa
		ospfv2.options.l	ospf.isa.asbr
		ospfv2.options.e	ospf.isa.asext
		ospfv2.options.dn	ospf.isa.attr
		ospfv2.options.dc	ospf.isa.member
		ospfv2.options	ospf.isa.mpls
		ospfv2.grace.reason	ospf.isa.network
		ospfv2.grace.period	ospf.isa.nssa
		ospfv2.grace.ip	ospf.isa.opaque
		ospfv2.grace	ospf.isa.router
		ospf.srcrouter	ospf.isa.summary
		ospf.oid.remote_node_id	ospf.isid.opaque_type
		ospf.oid.local_node_id	ospf.isid.te_isa.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