eth.addr eth.en eth.src eth.lg eth.raller eth.traller eth.lg eth.		WIRESHARK DISPLAY FILTERS					
eth.addr eth.dst eth.lg eth.lg eth.lg eth.railer eth.lg eth.railer eth.lg eth.railer eth.lg eth.railer eth.lg eth.railer eth.lg eth.railer  eth.lg eth.railer   ARP  arp.dst.hw_mac arp.proto.se arp.broto.jpv4 arp.proto.type arp.src.hw_mac arp.hwsbe arp.src.proto_ipv4 arp.opcode  FEE 802.IQ  vlan.cfi vlan.dd vlan.priorty vlan.trailer  1Pv4  ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragment.toolongfragment ip.checksum_bad ip.fragments ip.dsfield ip.dsfield ip.dsfield ip.dsfield.dscp ip.dsfield ip.dsfield.dscp ip.dsfield ip.dsfield.ec ip.dsfield ip.dsfield.ec ip.dsfield ip.dsfield.ec ip.dsfield ip.src ip.flags ip.src ip.flags ip.src ip.flags ip.src ip.flags.mf ip.tos.cost ip.flags.mf ip.tos.cost ip.flags.mf ip.fragment.multpretais ip.fragment.overlap							
eth.ig eth.multicast eth.type  ARP  arp.dst.hw_mac arp.proto.sse arp.dst.proto_ipv4 arp.proto.type arp.hwsbe arp.src.hw_mac arp.src.hw_mac arp.opcode  EEE 802.IQ  vlan.cfi vlan.d vlan.d vlan.priority vlan.etype vlan.len vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragment.sip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield.ee ip.id ip.dsfield.ee ip.id ip.dsfield.et ip.proto ip.dsfield.et ip.proto ip.dst_len ip.fragment.overlap.conflict ip.fragment.sip.fragments ip.fragments ip.fragment.overlap.conflict ip.nost ip.src_host ip.src ip.src ip.src_host ip.dsfield.et ip.proto ip.dst_len ip.src_host ip.flags_ip.flags_fl ip.src_host ip.flags_fl ip.flos_cost ip.flags_fl ip.flos_cost ip.flags_flos_flos_tost ip.frag_offset ip.tos_precedence ip.fragment.multipretais ip.tos_precedence ip.fragment.multipretais ip.tos_repealer ip.fragment.multipretais ip.trs_ ip.res_breedence ip.fragment.multipretais ip.trs_ ip.ves_breedence ip.fragment.multipretais ip.trs_ ip.ves_breedence ip.fragment.overlap  ipv66ddr ipv66ddr		ملده		ernet	ath and		
eth.ig eth.multicast eth.type  ARP  arp.dst.hw_mac arp.proto.see arp.dst.proto_ipv4 arp.hwsee arp.hwsee arp.src.hym_mac arp.src.proto_ipv4  arp.opcode  FEEE 802.IQ  vlan.cfi vlan.d vlan.priority vlan.etype vlan.len vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.fragments ip.fragments ip.checksum ip.fragments ip.checksum good ip.host ip.len ip.dsfield.dscp ip.len ip.dsfield.dscp ip.dsfield.et ip.proto ip.dsfield ip.src_host ip.src_ ip.src							
arp.dst.hw_mac arp.proto.see arp.dst.proto_ipv4 arp.hwsee arp.src.hw_mac arp.src.hw_mac arp.src.proto_ipv4 arp.hwsee arp.src.proto_ipv4 arp.hwsee arp.src.proto_ipv4 arp.src.proto_ipv4 arp.src.proto_ipv4 arp.opcode    EEE 802.IQ	etn.ust	etii	.ıg		eth.trailer		
arp.dst.hw_mac arp.proto.see arp.dst.proto_ipv4 arp.proto.type arp.hwsee arp.src.hw_mac arp.hwtype arp.src.proto_ipv4 arp.opcode  EEE 802.IQ  Vlan.cfi vlan.d vlan.priorty vlan.etype vlan.en vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.fragments ip.checksum_bad ip.fragments ip.checksum_bad ip.fragments ip.dsfield ip.host ip.dsfield.ee ip.dsfield.ee ip.dsfield.ee ip.gragment ip.dsfield.ee ip.gragment ip.gragment ip.dsfield.ee ip.gragment ip.tos.cost ip.flags.rb ip.flags.rb ip.tos.delay ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.muttipletais ip.ttl ipfragment.muttipletais ip.ttl ipfragment.overlap ipvesion	eth.ig	eth	.multicast		eth.type		
arp.dst.proto_ipv4 arp.hwsee arp.src.hw_mac arp.nycpcode    FEEE 802.IQ			Al	RP			
arp.dst.proto_ipv4 arp.hwsee arp.src.hw_mac arp.nycpcode    FEEE 802.IQ	arp.dst.hw mac		arp.proto.si	re			
arp.hwsize arp.hwtype arp.src.hw_mac arp.src.proto_ipv4  arp.opcode  EEE 802.IQ  vlan.cfi vlan.id vlan.priority vlan.etype vlan.len vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.fragments ip.fragments ip.fragments ip.fragments ip.deksum_bad ip.fragments ip.host ip.defield.ee ip.lid ip.defield.ee ip.lid ip.defield.ee ip.groto ip.defield.ee ip.src_ ip.src_ ip.flags_ ip.src_ ip.flags_ ip.src_ ip.flags_ ip.src_ ip.flags_ i							
arp.nytype arp.src.proto_ipv4  arp.opcode    FEE 802.IQ							
Van.cfi vlan.d vlan.priority  vlan.etype vlan.len vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragments ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield.ce ip.id ip.dsfield.ce ip.len ip.dsfield.ect ip.proto ip.dsfield.ect ip.proto ip.dst ip.reassembled_in ip.dst_losst ip.src ip.flags ip.src_host ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.precedence ip.fragment ip.fragment ip.frag.offset ip.tos.precedence ip.fragment ip.fragment.error ip.tos.troughput ip.fragment.multipletais ip.ttl ipfragment.overlap  IPv6  ipv6addr ipv6hop_opt	arn hwtyne						
vlan.cfi vlan.id vlan.priority vlan.etype vlan.len vlan.trailer  IPv4  ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragments ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield.ce ip.lost ip.lost ip.dsfield.dec ip.lost ip.len ip.dsfield.ect ip.proto ip.dst ip.reassembled_in ip.src ip.flags ip.src host ip.src ip.flags.df ip.flags.df ip.flags.mf ip.flags.mf ip.flags.mf ip.tos.cost ip.frag.mf ip.frag.mf ip.tos.recedence ip.fragment ip.tos.precedence ip.fragment ip.tos.precedence ip.fragment.multipletais ip.ttl ip.fragment.multipletais ip.ttl ip.tros.overlap  Ipv6  ipv6addr ipv6hop_opt	arp.opcode						
ip.addr ip.addr ip.checksum ip.checksum_bad ip.checksum_good ip.hdr_len ip.dsfield.ce ip.dsfield.ect ip.dsfield.ect ip.dsfield.ect ip.flags ip.flags.mf ip.flags.mf ip.flags.mf ip.flags.mf ip.flags.mf ip.flags.mf ip.fragment ip.fragment ip.tos.cost ip.fragment ip.tos.cedence ip.fragment ip.tos.cedence ip.fragment ip.tos.reliability ip.fragment.multipletais ip.vesion  1Pv6  ipv6addr  ipv6hop_opt			EEE 8	02.IQ			
ip.addr ip.checksum ip.checksum ip.checksum_bad ip.fragment.toolongfragment ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield ip.dsfield.ce ip.dsfield.ce ip.dsfield.ect ip.dsfield.ect ip.proto ip.dst ip.dst ip.fragment ip.dst ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment ip.fragment.error ip.fragment.multpletais ip.fragment.overlap ip.fragment.overlap ip.fragment ip.ves.oof ip.fragment ip.ves.oof ip.fragment.ooverlap ip.fragment.ooverlap ip.ves.oof	vlan.cfi	vla	n.id		vlan.priority		
ip.addr ip.fragment.overlap.conflict ip.checksum ip.fragment.toolongfragment ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield ip.host ip.dsfield.ce ip.id ip.dsfield.dscp ip.len ip.dsfield.ect ip.proto ip.dsfield.ect ip.fragment ip.src ip.frags ip.src_host ip.src ip.flags ip.src_host ip.src ip.flags ip.src_host ip.flags.mf ip.tos.cost ip.flags.mf ip.tos.cost ip.fragment ip.fragment ip.fragment.error ip.fragment.error ip.fragment.error ip.fragment.multipletals ip.fragment.overlap ipv6hop_opt	vlan.etype	vla	n.len		vlan.trailer		
ip.checksum ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield ip.dsfield.ce ip.dsfield.dscp ip.dsfield.ect ip.gragment ip.src ip.dst_host ip.src ip.flags ip.flags.mf ip.flags.rb ip.flags.rb ip.fragment ip.tos.cost ip.fragment ip.fragment.multipletais ip.fragment.multipletais ip.fragment.overlap  ip.fragment.overlap  ip.fragment.sip.fragment ip.v6hop_opt							
ip.checksum_bad ip.fragments ip.checksum_good ip.hdr_len ip.dsfield ip.dsfield.ce ip.dsfield.ce ip.dsfield.dscp ip.len ip.dsfield.ect ip.groto ip.dst ip.src ip.flags ip.src_host ip.flags.df ip.flags.mf ip.tos.cost ip.flags.rb ip.frag_offset ip.fragment ip.fragment.multipletais ipfragment.overlap ip.v6  ip.fragment.overlap ip.frag.ofte	•						
ip.checksum_good ip.hdr_len ip.dsfield ip.host ip.dsfield.ce ip.id ip.dsfield.dscp ip.len ip.dsfield.dscp ip.proto ip.dsfield.ect ip.proto ip.dst ip.dst_host ipreassembled_in ip.src ip.flags ip.src_host ip.flags.df iptos ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment.error ip.tragment.multipletais ip.ttl ipfragment.overlap ipv6hop_opt							
ip.dsfield.ce ip.dsfield.dscp ip.dsfield.ect ip.dsfield.ect ip.dstield.ect ip.dst ip.dst_host ip.dst_host ip.src ip.flags ip.src_host ip.flags.mf ip.flags.rb ip.frag_offset ip.fragment.error ip.fragment.error ip.fragment.multipletais ipfragment.overlap  ip.frag ip.fos. ip.fos. ip.fos. ip.fos. ip.fos.rb ip.fos.reliability ip.fragment.overlap  ip.fragment.overlap  ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ip.fragment.overlap ipv6hop_opt	ipioneonoum_baa						
ip.dsfield.ce ip.dsfield.dscp ip.dsfield.ect ip.groto ip.dst ip.dst_host ip.dst_host ip.flags ip.flags.df ip.flags.mf ip.flags.rb ip.frag_offset ip.fragment.error ip.fragment.multipletais ip.fragment.overlap ip.v6shop_opt ip.v6shop_opt	ip.checksum_good						
ip.dsfield.dscp ip.dsfield.ect ip.proto ip.dst ip.dst ip.dst ip.eassembled_in ip.dst_host ip.src ip.flags ip.src_host ip.flags.df ip.flags.mf ip.tos.cost ip.flags.rb ip.frag_offset ip.fragment ip.fragment.error ip.fragment.multipletais ipfragment.overlap ipv6addr ipv6hop_opt			ip.host				
ip.dsfield.ect ip.proto ip dst ipreassembled_in ip.dst_host ip.src ip.flags ip.src_host ip.flags.df iptos ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletais ip.ttl ip fragment.overlap ipversion  1Pv6				-			
ip.dst ipreassembled_in ip.dst_host ip.src ip.flags ip.src_host ip.flags.df iptos ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletails ip.ttl ipfragment.overlap ipv6hop_opt							
ip.dst_host ip.flags ip.src_host ip.flags.df ip.tos ip.flags.mf ip.tos.cost ip.flags.rb ip.frag_offset ip.tos.precedence ip.fragment ip.fragment.error ip.fragment.multipletais ipfragment.overlap  ipv6addr ipv6hop_opt							
ip.flags ip.src_host ip.flags.df iptos ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletails ip.ttl ipfragment.overlap ip.version  1Pv6	•						
ip.flags.mf ip.tos.cost ip.flags.rb ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletais ip.ttl ipfragment.overlap ip.version  1Pv6							
ip.flags.rb ip.frag_offset ip.tos.delay ip.frag_offset ip.tos.precedence ip.fragment ip.fragment.error ip.fragment.multipletaik ipfragment.overlap  ipv6addr ipv6addr ipv6hop_opt				· -			
ip.flags.rb ip.frag_offset ip.tos.precedence ip.fragment ip.fragment ip.tos.reliability ip.fragment.error ip.tragment.multipletais ip.ttl ipfragment.overlap  ip.version  1Pv6  ipv6addr ipv6hop_opt							
ip.frag_offset ip.tos.precedence ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletais ip.ttl ipfragment.overlap ip.version  1Pv6  ipv6addr ipv6hop_opt							
ip.fragment ip.tos.reliability ip.fragment.error ip.tos.throughput ip.fragment.multipletais ip.ttl ipfragment.overlap ip.version  1Pv6  ipv6addr ipv6hop_opt	•						
ip.fragment.error ip.tos.throughput ip.fragment.multipletails ip.ttl ipfragment.overlap ip.version  1Pv6  ipv6addr ipv6hop_opt				• •			
ip.tragment.multipletails ipfragment.overlap ip.version  1Pv6 ipv6addr ipv6hop_opt	ip.fragment.error						
ipfragment.overlap ip.version  1Pv6  ipv6addr ipv6hop_opt							
ipv6addr ipv6hop_opt	ipfragment.overlap						
Ιρνοπομ_ομι							
	ipv6addr			ipv6hop opt			
	ipv6class			ipv6host			

ipv6dst	ipv6mipv6_length
ipv6dst_opt	ipv6mipv6_type
ipv6flow	ipv6nxt
ipv6fragment	ipv6opt.padl
ipv6 fragment.error	ipv6opt.padn
ipv6fragmentmore	ipv6.penipv6
ipv6fragment.multipletails	.reassembled_in
ipv6fragment offset	ipv6.puting_hdr
ipv6fragment.overlap	ipv6.puting_hdr.addr
ipv6fragment.overlap.conflict	ipv6.puting_hdr.left
ipv6fragment.toolongfragment	ipv6.puting_hdr.type
ipv6fragments	ipv6src
ipv6fragmentid	ipv6src_host
ipv6hlim	ipv6version
TC	CP CP
tcp.ack	tcp.options.qs
tcp.checksum	tcp.options.sack
tcp.checksum_bad	tcp.options.sack_le
tcp.checksum_good	tcp.options.sack_perm
tcp.continuation_to	tcp.options.sack_re
tcp.dstport	tcp.options.time_stamp
tcp.flags	tcp.options.wscale
tcp.flagsack	tcp.options.wscale_val
tcp.flagscwr	tcp.pdu.last_frame
tcp.flagsecn	tcp.pdu.size
tcpflagsfin	tcppdutime
tcp.flags.push	tcp.port
tcp.flags.reset	tcp.reassembled_in
tcp.flagssyn	tcp.segment
tcp.flagsurg	tcp.ægment.error
tcp.hdr_len	tcp.segment.multipletails
tcp.len	tcp.ægment.overlap
tcp.nxtseq	tcp.segment.overlap.conflict tcp.segment.toobngfragment
tcp.options	
tcp.options.cc	tcp.segments
tcp.options.ccecho	tcp.seq
tcp.options.ccnew	tcp.srcport
tcp.options.echo	tcp.time_delta
tcp.options.echo_reply	tcp.time_relative
tcp.options.md5	tcp.urgent_pointer
tcp.options.mss	tcp.window_size
tcpoptionsmss_val	A.D.
UE	
udpchecksum	udpdstport
udpsrcport	udp.length

udp.checksum_bad	udp.port			
udp.checksum_good	00p.po.0			
	Relay			
fr.been	fr.de			
fr.chdlctype	fr.dlci			
fr.control	fr.dlcorecontrol			
fr.control.f	fr.ea			
fr.controlftype	fr.teen			
fr.control.nr	fr.lower dlci			
fr.control.ns	fr.nlpid			
fr.control.p	fr.seconddlci			
fr.controls_ftype	fr.snap.oui			
fr.controlu_modifier_cmd	fr.snap.pid			
fr.controlu_modifier_resp	fr.snaptype			
fr.er	fr.third dlci			
fr.de	tr.upper dlci			
	// Pv6			
i-may Call assess	icmpv6option.name_type fqdn			
icmpv6all_comp	icmpv6option.name_x501			
icmpv6checksum	icmpv6 option.rsa.key_hash			
icmpv6checksum_bad	icmpv6 option.type			
icmpv6code	icmpv6 .ra.cur_hop_limit			
icmpv6comp	icmpv6.ra.reachable_time			
icmpv6haad.ha_addrs icmpv6identifier	icmpv6.ra.retrans_timer			
icmpv6option	icmpv6.ra.router_lifetime			
icmpv6optionga	icmpv6.recursive_dns_serv			
icmpv6option.length	icmpv6type			
icmpv6option.name_type				
P	PP			
ppp.address	ppp.direction			
ppp.control	ppp.protocol			
	RIP			
wine with recognised	ripip			
ripauthpasswd	rip.auth.type			
riproute_tag	rip.routing_domain			
rip.metric rip.command	rip.netmask			
rip.version	rip.family			
·				
rip.next_hop MPLS				
malshattam	mplsoam_detect_location			
mplsbottom mplscw.control	mpls.oam.defect_type			
mplscw.control mplscw.res	mpls.oam.frequency			
mplsexp	mpls.oam.function_type			
mplsabel	mpls.oam.ttsi			
mplsoam.bip16	mpls.ttl			
IIIhispatti'nihto	Implated			

В	GP	
bgp.aggregator_as	bgp.mp_reach_nlri_ipv4_prefix	
	bgp.mp_unreach_nlri_ipv4_pretix	
bgp aggregator_origin bgp.as_path	bgp.multi_exit_disc	
	bgp.next_hop	
bgp.cluster_identifier	bgp.nlri_prefix	
bgp.cluster_list	bgporigin	
bgp.community_as	bgp.originator_id	
bgp.community_value	bgp.type	
bgp.local_pref		
bgp.mp_nlri_tnl_id	bgp.withdrawn_prefix	
IC	MP	
icmpchecksum	icmpident	
icmp.seq	cmp.checksum_bad	
icmpmtu	icmp.type	
icmpcode	icmpredir_gw	
DTP		
dta nairhhau	dtp.tlv_type	
dtp.neighbor	· · ·	
vtp.neighbor	dtp.tlv_len	
dtp.version	TP	
V	TP	
vtp.code	vtpvlan_info.802_10_index	
vtp.conf_rev_num	vtpvlan_into.len	
vtpvlan_info.lsl vlan_id	vtp vlan_into. mtu_siæ	
vtp.followers	vtpvlan_info.status.vlan_susp	
vtp.md	vtpvlan_info.tlv_len	
vtp.mdS_digest	vtpvlan_info.tlv_type	
	vtp.vlan info.vlan name	
vtp.md_len	vtpvlan_info.vlan_name_len	
vtp.seq_num		
vtp.start_value	vtpvlan_info.vlan_type	
vtp.upd_id		
vtp.upd_ts		
vtp.version vtp.version		
п	ТТР	
http.accept	http.proxy_authorization	
http.accept_encoding	http.proxy_connect_host	
http.accept_language http.authbasic	httpproxy_connect_port http.referer	
http authorization	httprequest	
http.cache_control	http.request. method	
http.connection	http.request.uri http.request.version	
http.content_encoding http.content_length	http.response	
http.content_type	http.responsecode	
http.cookie	httpserver	

http.date	http.set cookie					
http.host	httptransfer encoding					
http.last_modified	http.user agenthttp					
http.location	www authenticate					
http.notification	http.x forwarded for					
	Tittp.x_forwarded_for					
http.proxy_authenticate						
Intrusion & Ma	Intrusion & Malware Detection					
http.request. Uri contains ".exe"	# Executable downloads					
ton flags syn == 1 and ton flags ack == $0$	# SYN scan detection					
tcp.flags.syn == 1 and tcp.flags.ack == 0 frame contains "cmd.exe"	# Shell command traces					
dns.gry.name contains "malicious.com"						
ansiqiy.name contains mandous.com	# C2 domain lookup					
http.user_agent contains "curl"	# CLI downloader detection					
smtp.req.parameter	# Email credential leakage					
	_					
tcp.analysis.retransmission	# Flood/DoS activity					
IoT Prot	ocol Filters					
mqtt	#GeneralMQTTtraffic					
mqtt.msgtype == 1	#MQTTCONNECTmessages					
coap	#CoAPprotocol					
eth.addr == aa:bb:cc:dd:ee:ff	#SpedificIoTMACaddress					
http.user agent contains "esp8266"	#ESP device fingerprint					
nttp.user_agent contains espozoo	TTP Analysis					
DINS & FI	I IP Alidiysis					
duc any nama	#ViewDNSqueries					
dns.qry.name	#Failed DNS responses					
dns.flags.rcode > 0	#Fameu Divisiespoises #Form/data-submissions					
http.request.method == "POST"						
http.set_cookie	#Inspect cookies					
http.response.code >= 400	#HTTP error responses					
tls.handshake.extensions_server_name	#ExtractSNI					
VOIP & KI	P/SIP Trattic					
sip	#Session Initiation Protocol					
rtp	#Real-time Transport Protocol					
sip.Call-ID	#TrackSIPsessions					
rtp.marker == 1	#RTPstreamboundary					
Protoco						
Protocol Operators						
	HE-role (Net an ele					
==, !=	#Equals/Notequals					
>,<	#Greater/Lessthan					
contains	#Substring match					
and, or	#LogicalAND/OR					
not	#Negation					
eq or	andor&& Logical AND					
ne or!=	oror11 LogicalOR					
ators	xoror''' LogicalXOR					
gtor>	· ·					
lt or<	not or ! LogicalNOT					
geor>= leor<=	n] [1Substring operator					
IDOT/-						