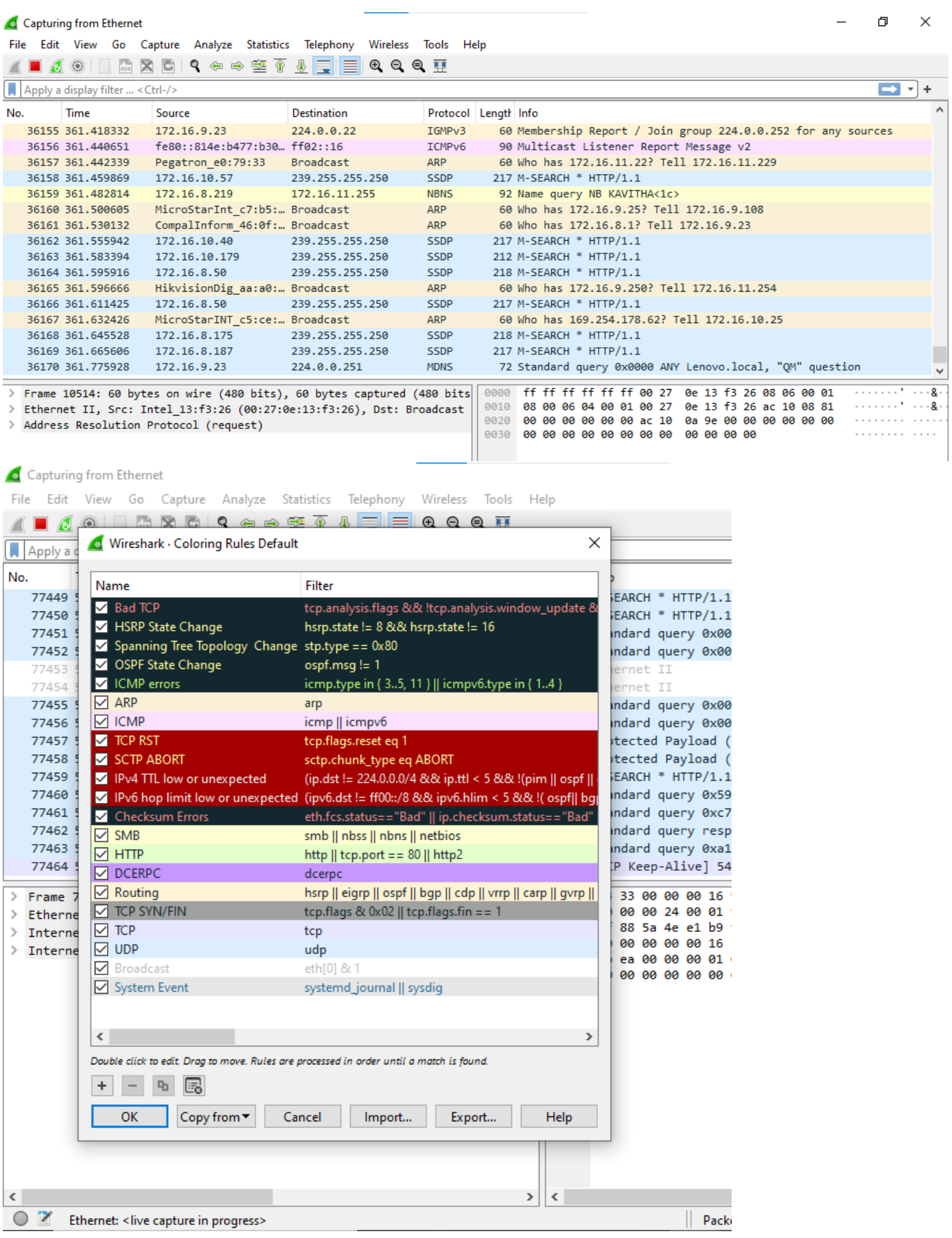
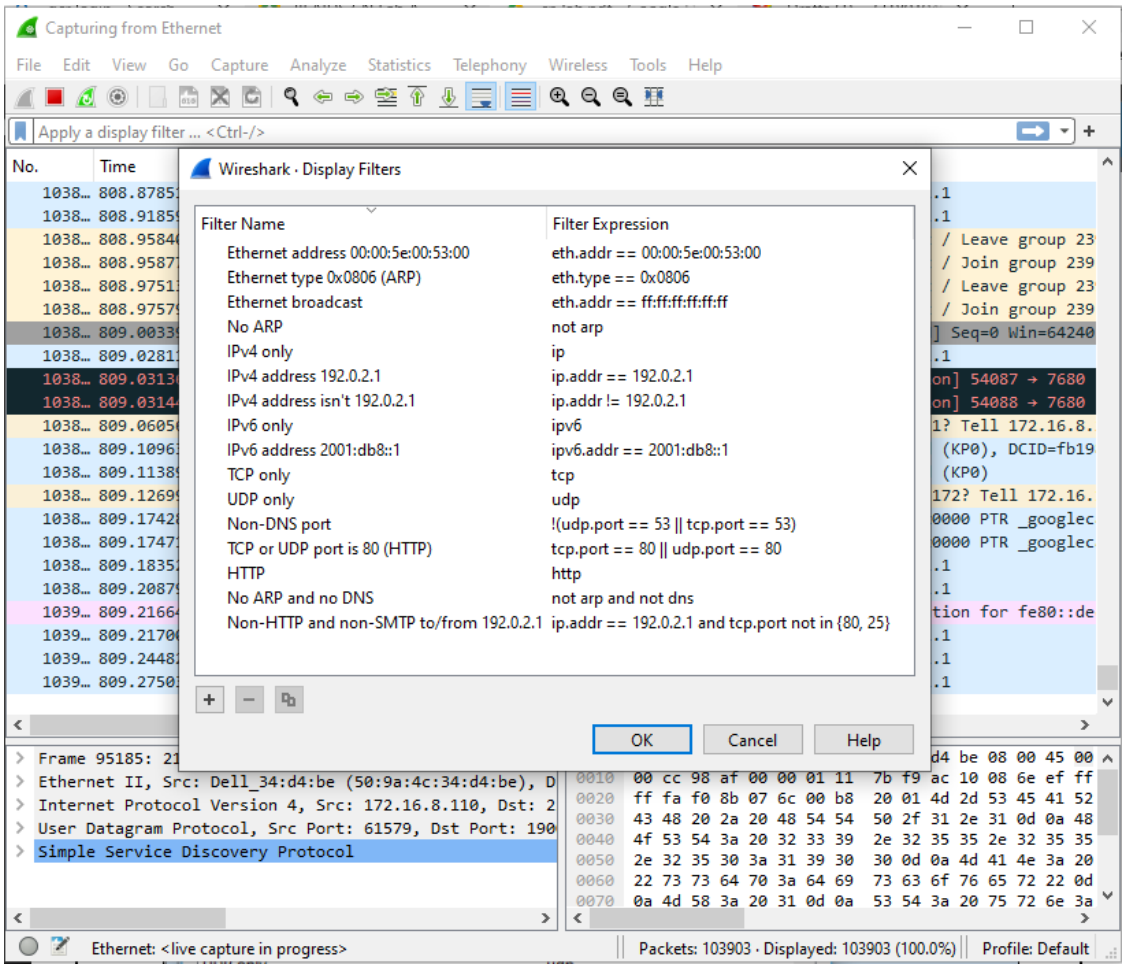
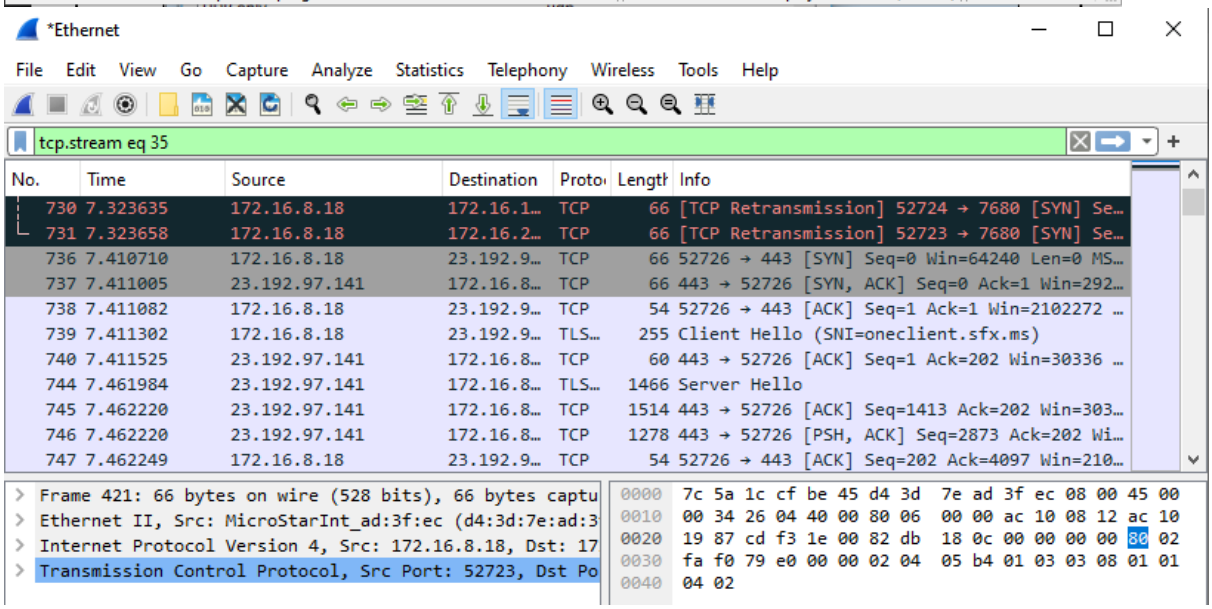
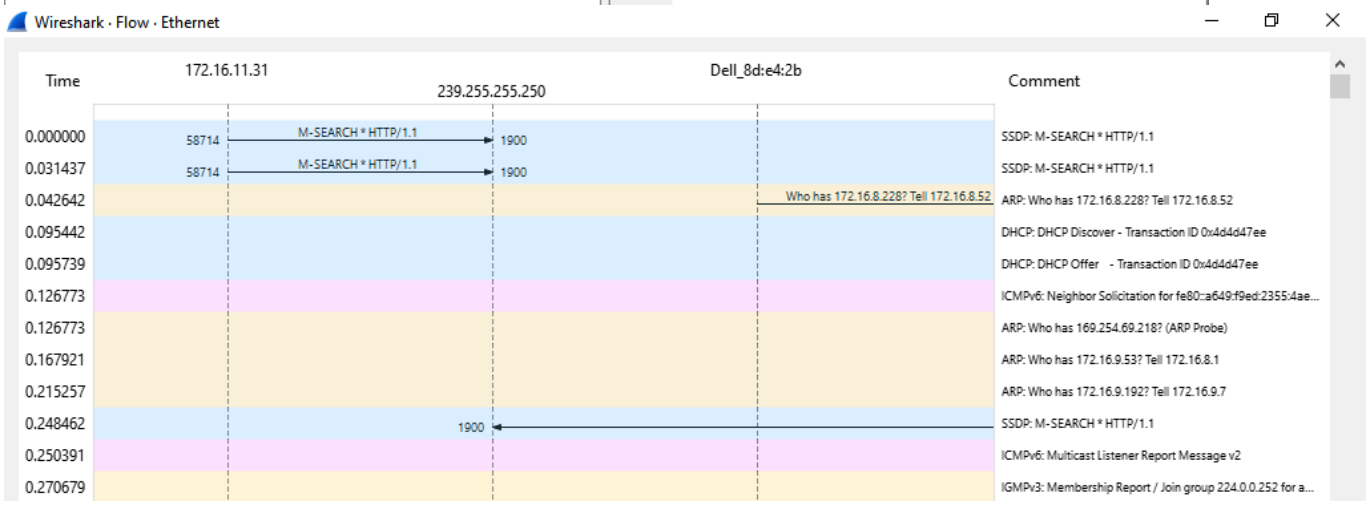
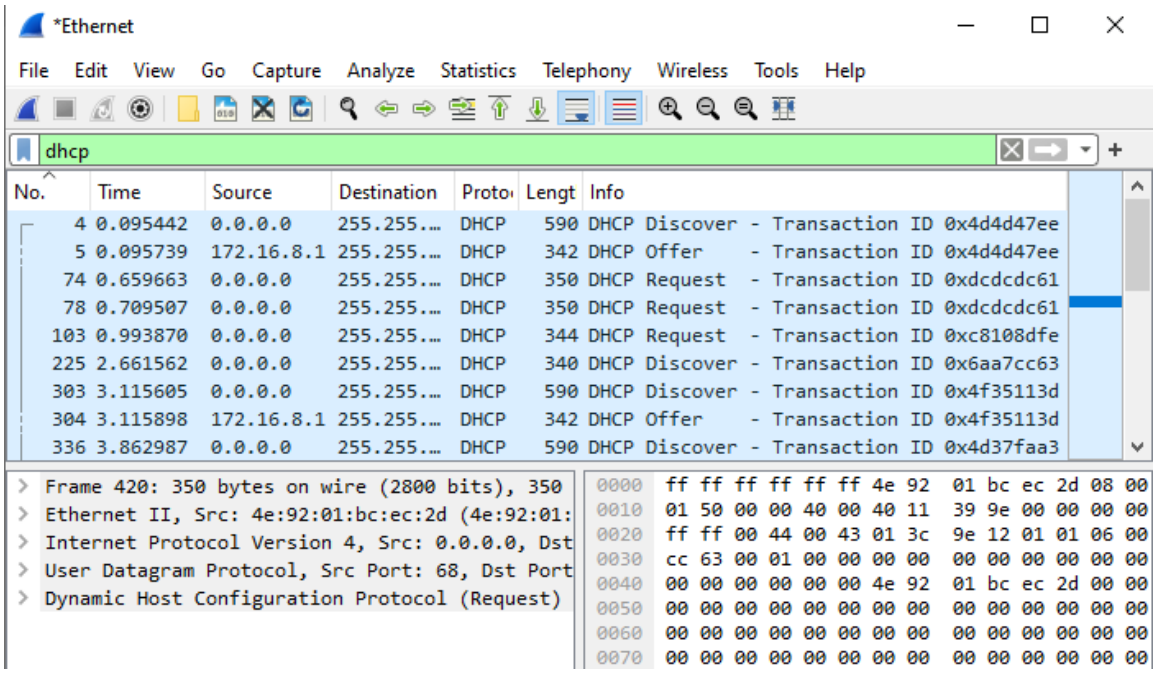

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
36155 361.418332 172.16.9.23 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
36156 361.440651 fe80::814e:b477:b30… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
36157 361.442339 Pegatron_e0:79:33 Broadcast ARP 60 Who has 172.16.11.22? Tell 172.16.11.229
36158 361.459869 172.16.10.57 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
36159 361.482814 172.16.8.219 172.16.11.255 NBNS 92 Name query NB KAVITHA<1c>
36160 361.500605 MicroStarInt_c7:b5:… Broadcast ARP 60 Who has 172.16.9.25? Tell 172.16.9.108
36161 361.530132 CompalInform_46:0f:… Broadcast ARP 60 Who has 172.16.8.1? Tell 172.16.9.23
36162 361.555942 172.16.10.40 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
36163 361.583394 172.16.10.179 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
36164 361.595916 172.16.8.50 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
36165 361.596666 HikvisionDig_aa:a0:… Broadcast ARP 60 Who has 172.16.9.250? Tell 172.16.11.254
36166 361.611425 172.16.8.50 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
36167 361.632426 MicroStarINT_c5:ce:… Broadcast ARP 60 Who has 169.254.178.62? Tell 172.16.10.25
36168 361.645528 172.16.8.175 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
36169 361.665606 172.16.8.187 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
36170 361.775928 172.16.9.23 224.0.0.251 MDNS 72 Standard query 0x0000 ANY Lenovo.local, "QM" question
Frame 10514: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
Ethernet II, Src: Intel_13:f3:26 (00:27:0e:13:f3:26), Dst: Broadcast
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 27 0e 13 f3 26 08 06 00 01
0010 08 00 06 04 00 01 00 27 0e 13 f3 26 ac 10 08 81
0020 00 00 00 00 00 00 ac 10 0a 9e 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00

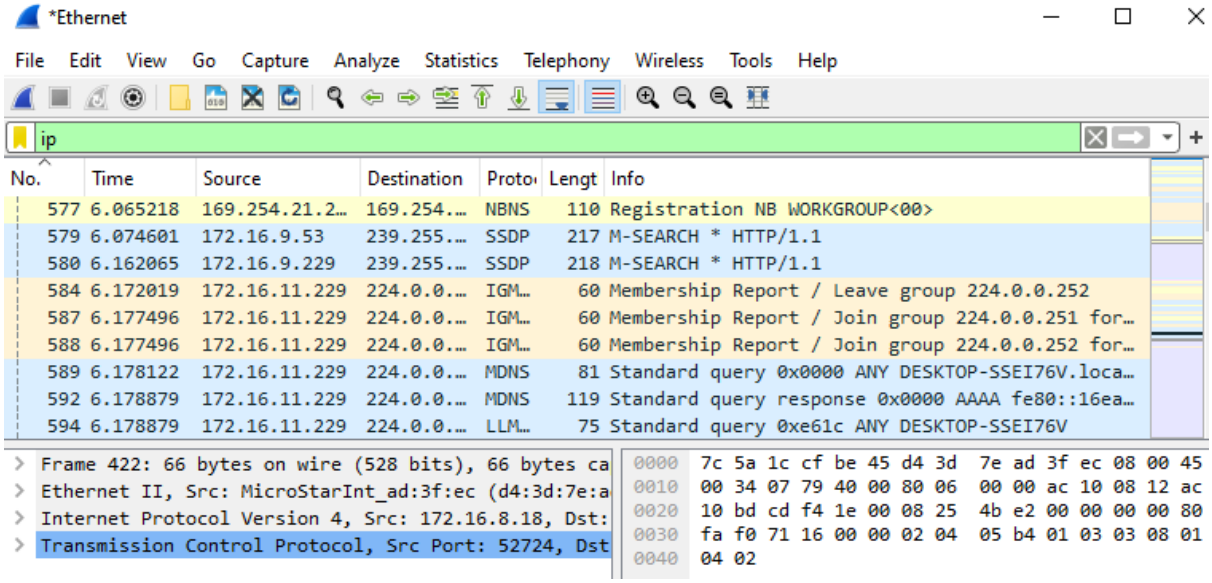
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Coloring Rules Default
Name Filter
Bad TCP tcp.analysis.flags && !tcp.analysis.window_update &
HSRP State Change hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change stp.type == 0x80
OSPF State Change ospf.msg != 1
ICMP errors icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP arp
ICMP icmp || icmpv6
TCP RST tcp.flags.reset eq 1
SCTP ABORT sctp.chunk_type eq ABORT
IPv4 TTL low or unexpected (ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf ||
IPv6 hop limit low or unexpected (ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bg
Checksum Errors eth.fcs.status=="Bad" || ip.checksum.status=="Bad"
SMB smb || nbss || nbns || netbios
HTTP http || tcp.port == 80 || http2
DCERPC dcerpc
Routing hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp ||
TCP SYN/FIN tcp.flags & 0x02 || tcp.flags.fin == 1
TCP tcp
UDP udp
Broadcast eth[0] & 1
System Event systemd_journal || sysdig
Double click to edit. Drag to move. Rules are processed in order until a match is found.
OK Copy from Cancel Import... Export... Help
Ethernet: <live capture in progress>

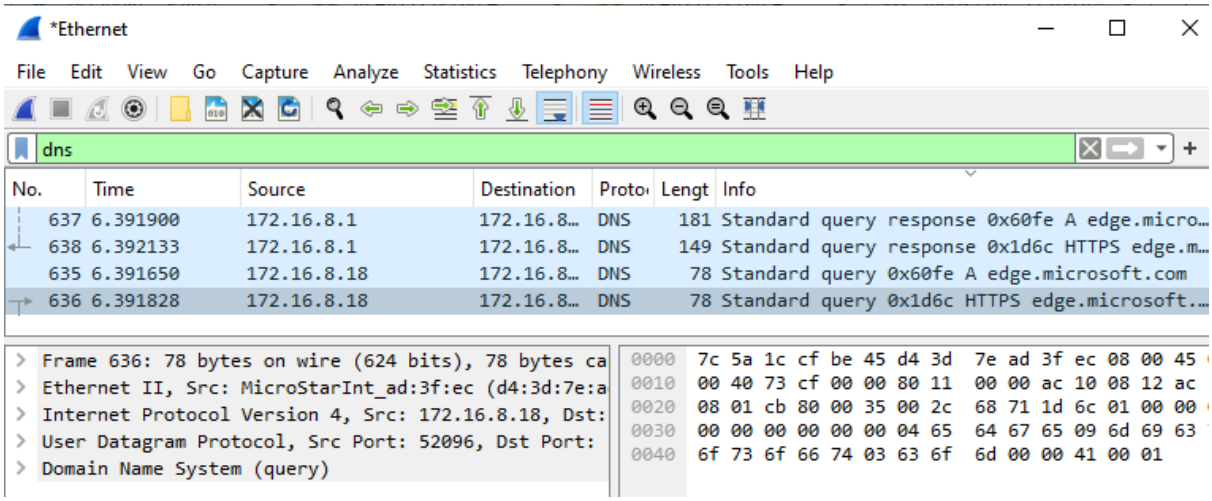

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1
ip.addr != 192.0.2.1
IPv6 only
ipv6
IPv6 address 2001:db8::1
ipv6.addr == 2001:db8::1
TCP only
tcp
UDP only
udp
Non-DNS port
!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)
tcp.port == 80 || udp.port == 80
HTTP
http
No ARP and no DNS
not arp and not dns
Non-HTTP and non-SMTP to/from 192.0.2.1
ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
OK
Cancel
Help
Ethernet: <live capture in progress>
Packets: 103903 · Displayed: 103903 (100.0%)
Profile: Default

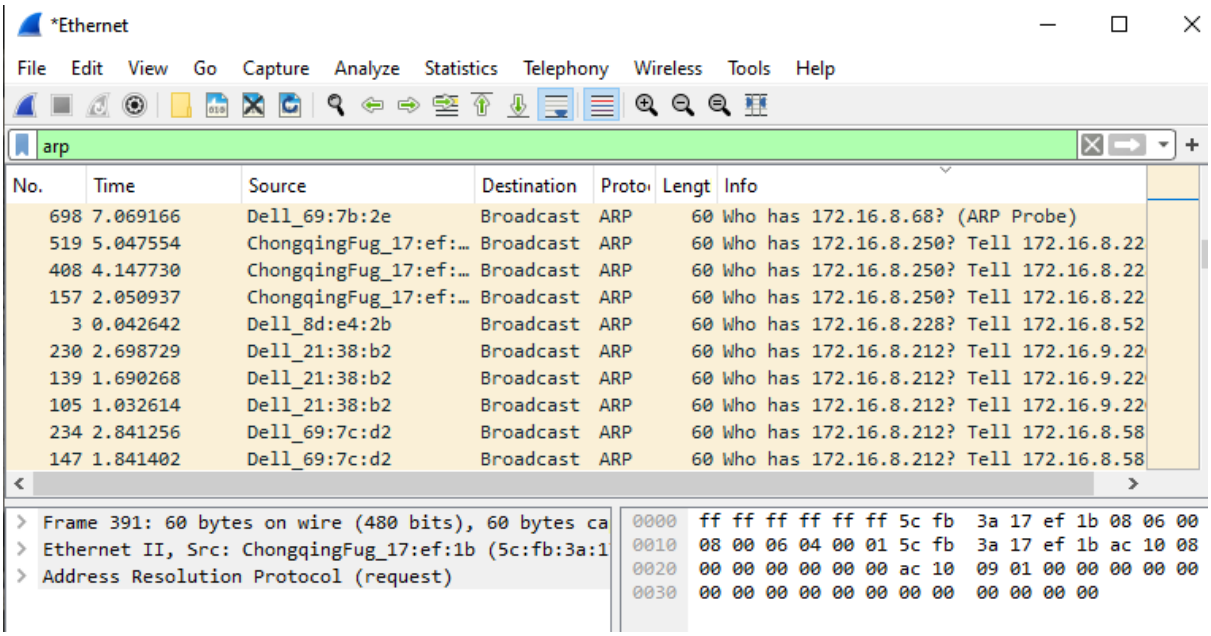

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 35
No. Time Source Destination Proto Length Info
730 7.323635 172.16.8.18 172.16.1… TCP 66 [TCP Retransmission] 52724 → 7680 [SYN] Se…
731 7.323658 172.16.8.18 172.16.2… TCP 66 [TCP Retransmission] 52723 → 7680 [SYN] Se…
736 7.410710 172.16.8.18 23.192.9… TCP 66 52726 → 443 [SYN] Seq=0 Win=64240 Len=0 MS…
737 7.411005 23.192.97.141 172.16.8… TCP 66 443 → 52726 [SYN, ACK] Seq=0 Ack=1 Win=292…
738 7.411082 172.16.8.18 23.192.9… TCP 54 52726 → 443 [ACK] Seq=1 Ack=1 Win=2102272 …
739 7.411302 172.16.8.18 23.192.9… TLS… 255 Client Hello (SNI=oneclient.sfx.ms)
740 7.411525 23.192.97.141 172.16.8… TCP 60 443 → 52726 [ACK] Seq=1 Ack=202 Win=30336 …
744 7.461984 23.192.97.141 172.16.8… TLS… 1466 Server Hello
745 7.462220 23.192.97.141 172.16.8… TCP 1514 443 → 52726 [ACK] Seq=1413 Ack=202 Win=303…
746 7.462220 23.192.97.141 172.16.8… TCP 1278 443 → 52726 [PSH, ACK] Seq=2873 Ack=202 Wi…
747 7.462249 172.16.8.18 23.192.9… TCP 54 52726 → 443 [ACK] Seq=202 Ack=4097 Win=210…
Frame 421: 66 bytes on wire (528 bits), 66 bytes captu
Ethernet II, Src: MicroStarInt_ad:3f:ec (d4:3d:7e:ad:3
Internet Protocol Version 4, Src: 172.16.8.18, Dst: 17
Transmission Control Protocol, Src Port: 52723, Dst Po
0000 7c 5a 1c cf be 45 d4 3d 7e ad 3f ec 08 00 45 00
0010 00 34 26 04 40 00 80 06 00 00 ac 10 08 12 ac 10
0020 19 87 cd f3 1e 00 82 db 18 0c 00 00 00 00 80 02
0030 fa f0 79 e0 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02


Wireshark · Flow · Ethernet
Time
172.16.11.31
239.255.255.250
Dell_8d:e4:2b
Comment
0.000000 58714 M-SEARCH * HTTP/1.1 1900 SSDP: M-SEARCH * HTTP/1.1
0.031437 58714 M-SEARCH * HTTP/1.1 1900 SSDP: M-SEARCH * HTTP/1.1
0.042642 Who has 172.16.8.228? Tell 172.16.8.52 ARP: Who has 172.16.8.228? Tell 172.16.8.52
0.095442 DHCP: DHCP Discover - Transaction ID 0x4d4d47ee
0.095739 DHCP: DHCP Offer - Transaction ID 0x4d4d47ee
0.126773 ICMPv6: Neighbor Solicitation for fe80::a649:f9ed:2355:4ae...
0.126773 ARP: Who has 169.254.69.218? (ARP Probe)
0.167921 ARP: Who has 172.16.9.53? Tell 172.16.8.1
0.215257 ARP: Who has 172.16.9.192? Tell 172.16.9.7
0.248462 1900 SSDP: M-SEARCH * HTTP/1.1
0.250391 ICMPv6: Multicast Listener Report Message v2
0.270679 IGMPv3: Membership Report / Join group 224.0.0.252 for a...


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Proto Lengt Info
4 0.095442 0.0.0.0 255.255.... DHCP 590 DHCP Discover - Transaction ID 0x4d4d47ee
5 0.095739 172.16.8.1 255.255.... DHCP 342 DHCP Offer - Transaction ID 0x4d4d47ee
74 0.659663 0.0.0.0 255.255.... DHCP 350 DHCP Request - Transaction ID 0xdcdcdc61
78 0.709507 0.0.0.0 255.255.... DHCP 350 DHCP Request - Transaction ID 0xdcdcdc61
103 0.993870 0.0.0.0 255.255.... DHCP 344 DHCP Request - Transaction ID 0xc8108dfe
225 2.661562 0.0.0.0 255.255.... DHCP 340 DHCP Discover - Transaction ID 0x6aa7cc63
303 3.115605 0.0.0.0 255.255.... DHCP 590 DHCP Discover - Transaction ID 0x4f35113d
304 3.115898 172.16.8.1 255.255.... DHCP 342 DHCP Offer - Transaction ID 0x4f35113d
336 3.862987 0.0.0.0 255.255.... DHCP 590 DHCP Discover - Transaction ID 0x4d37faa3
Frame 420: 350 bytes on wire (2800 bits), 350
Ethernet II, Src: 4e:92:01:bc:ec:2d (4e:92:01:
Internet Protocol Version 4, Src: 0.0.0.0, Dst
User Datagram Protocol, Src Port: 68, Dst Port
Dynamic Host Configuration Protocol (Request)
0000 ff ff ff ff ff ff 4e 92 01 bc ec 2d 08 00
0010 01 50 00 00 40 00 40 11 39 9e 00 00 00 00
0020 ff ff 00 44 00 43 01 3c 9e 12 01 01 06 00
0030 cc 63 00 01 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 4e 92 01 bc ec 2d 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
No. Time Source Destination Proto Lengt Info
577 6.065218 169.254.21.2... 169.254.... NBNS 110 Registration NB WORKGROUP<00>
579 6.074601 172.16.9.53 239.255.... SSDP 217 M-SEARCH * HTTP/1.1
580 6.162065 172.16.9.229 239.255.... SSDP 218 M-SEARCH * HTTP/1.1
584 6.172019 172.16.11.229 224.0.0.... IGM... 60 Membership Report / Leave group 224.0.0.252
587 6.177496 172.16.11.229 224.0.0.... IGM... 60 Membership Report / Join group 224.0.0.251 for...
588 6.177496 172.16.11.229 224.0.0.... IGM... 60 Membership Report / Join group 224.0.0.252 for...
589 6.178122 172.16.11.229 224.0.0.... MDNS 81 Standard query 0x0000 ANY DESKTOP-SSEI76V.loca...
592 6.178879 172.16.11.229 224.0.0.... MDNS 119 Standard query response 0x0000 AAAA fe80::16ea...
594 6.178879 172.16.11.229 224.0.0.... LLM... 75 Standard query 0xe61c ANY DESKTOP-SSEI76V
Frame 422: 66 bytes on wire (528 bits), 66 bytes ca
Ethernet II, Src: MicroStarInt_ad:3f:ec (d4:3d:7e:a
Internet Protocol Version 4, Src: 172.16.8.18, Dst:
Transmission Control Protocol, Src Port: 52724, Dst
0000 7c 5a 1c cf be 45 d4 3d 7e ad 3f ec 08 00 45
0010 00 34 07 79 40 00 80 06 00 00 ac 10 08 12 ac
0020 10 bd cd f4 1e 00 08 25 4b e2 00 00 00 00 80
0030 fa f0 71 16 00 00 02 04 05 b4 01 03 03 08 01
0040 04 02


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Proto Lengt Info
637 6.391900 172.16.8.1 172.16.8... DNS 181 Standard query response 0x60fe A edge.micro...
638 6.392133 172.16.8.1 172.16.8... DNS 149 Standard query response 0x1d6c HTTPS edge.m...
635 6.391650 172.16.8.18 172.16.8... DNS 78 Standard query 0x60fe A edge.microsoft.com
636 6.391828 172.16.8.18 172.16.8... DNS 78 Standard query 0x1d6c HTTPS edge.microsoft....
Frame 636: 78 bytes on wire (624 bits), 78 bytes ca
Ethernet II, Src: MicroStarInt_ad:3f:ec (d4:3d:7e:a
Internet Protocol Version 4, Src: 172.16.8.18, Dst:
User Datagram Protocol, Src Port: 52096, Dst Port:
Domain Name System (query)
0000 7c 5a 1c cf be 45 d4 3d 7e ad 3f ec 08 00 45
0010 00 40 73 cf 00 00 80 11 00 00 ac 10 08 12 ac
0020 08 01 cb 80 00 35 00 2c 68 71 1d 6c 01 00 00
0030 00 00 00 00 00 00 04 65 64 67 65 09 6d 69 63
0040 6f 73 6f 66 74 03 63 6f 6d 00 00 41 00 01


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Source Destination Proto Lengt Info
698 7.069166 Dell_69:7b:2e Broadcast ARP 60 Who has 172.16.8.68? (ARP Probe)
519 5.047554 ChongqingFug_17:ef:… Broadcast ARP 60 Who has 172.16.8.250? Tell 172.16.8.22
408 4.147730 ChongqingFug_17:ef:… Broadcast ARP 60 Who has 172.16.8.250? Tell 172.16.8.22
157 2.050937 ChongqingFug_17:ef:… Broadcast ARP 60 Who has 172.16.8.250? Tell 172.16.8.22
3 0.042642 Dell_8d:e4:2b Broadcast ARP 60 Who has 172.16.8.228? Tell 172.16.8.52
230 2.698729 Dell_21:38:b2 Broadcast ARP 60 Who has 172.16.8.212? Tell 172.16.9.22
139 1.690268 Dell_21:38:b2 Broadcast ARP 60 Who has 172.16.8.212? Tell 172.16.9.22
105 1.032614 Dell_21:38:b2 Broadcast ARP 60 Who has 172.16.8.212? Tell 172.16.9.22
234 2.841256 Dell_69:7c:d2 Broadcast ARP 60 Who has 172.16.8.212? Tell 172.16.8.58
147 1.841402 Dell_69:7c:d2 Broadcast ARP 60 Who has 172.16.8.212? Tell 172.16.8.58
Frame 391: 60 bytes on wire (480 bits), 60 bytes ca
Ethernet II, Src: ChongqingFug_17:ef:1b (5c:fb:3a:1
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 5c fb 3a 17 ef 1b 08 06 00
0010 08 00 06 04 00 01 5c fb 3a 17 ef 1b ac 10 08
0020 00 00 00 00 00 00 ac 10 09 01 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00