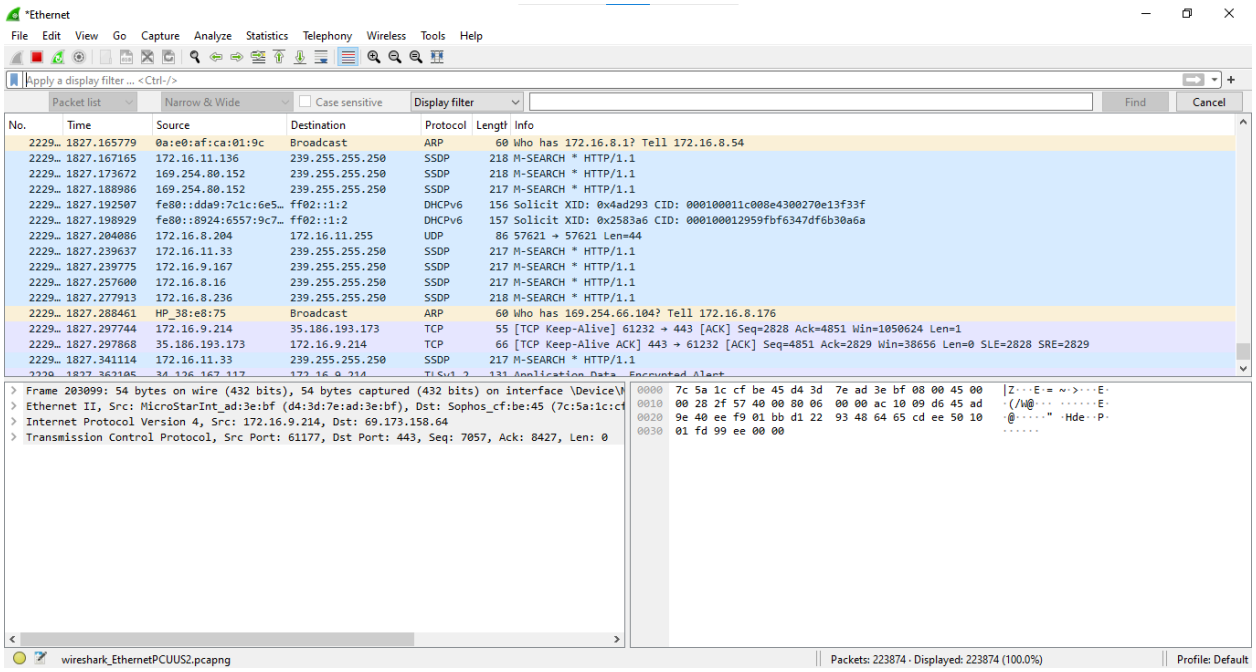
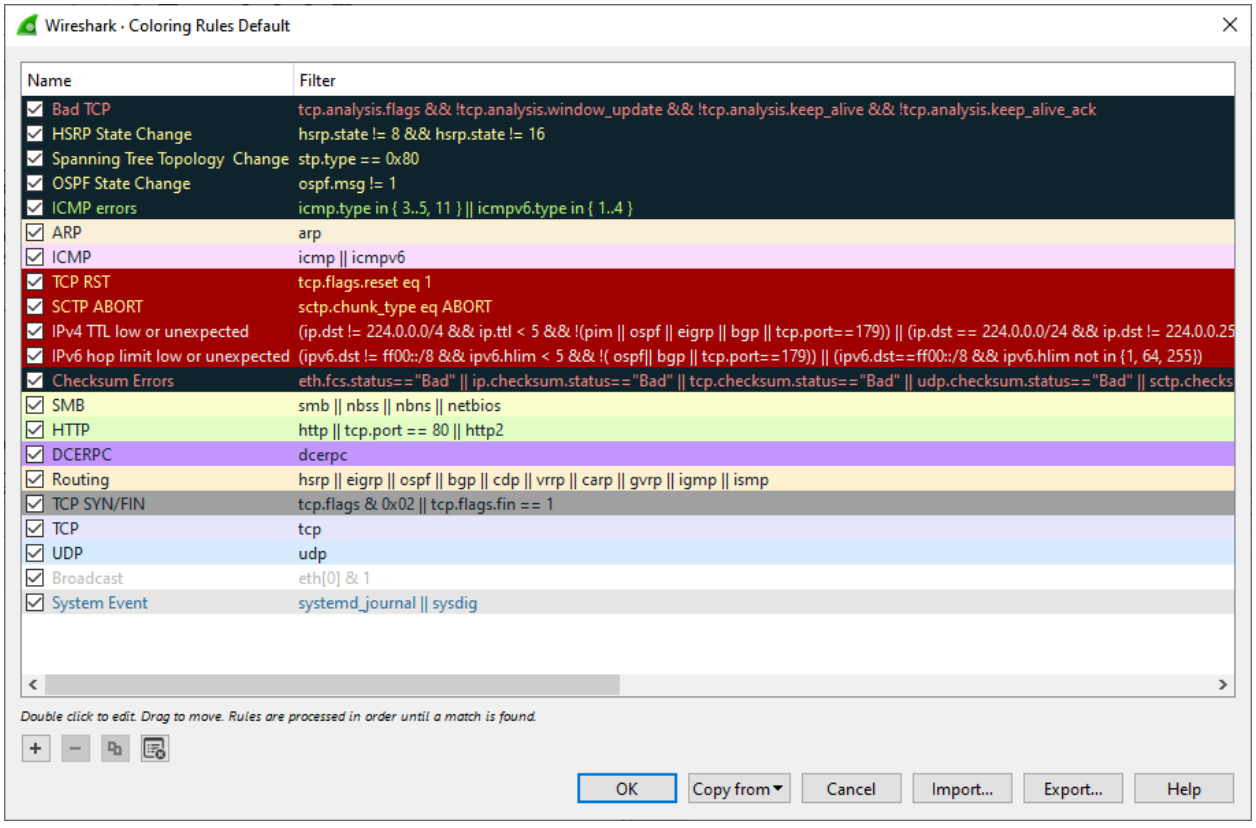
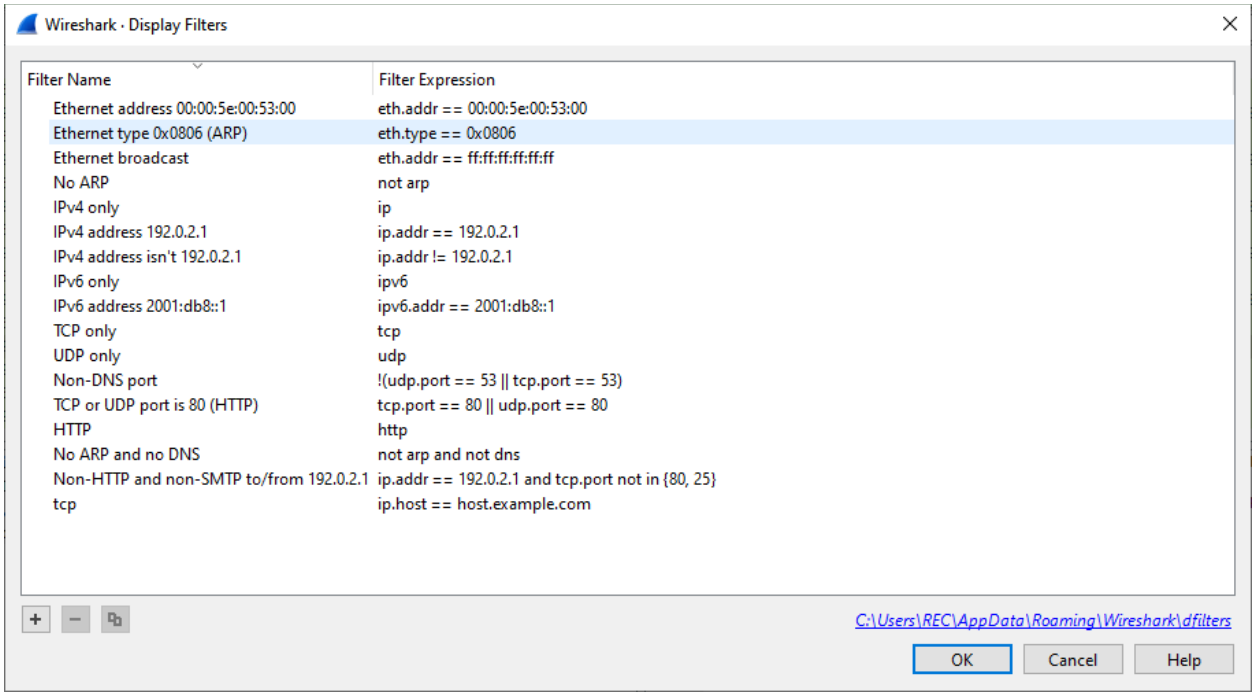
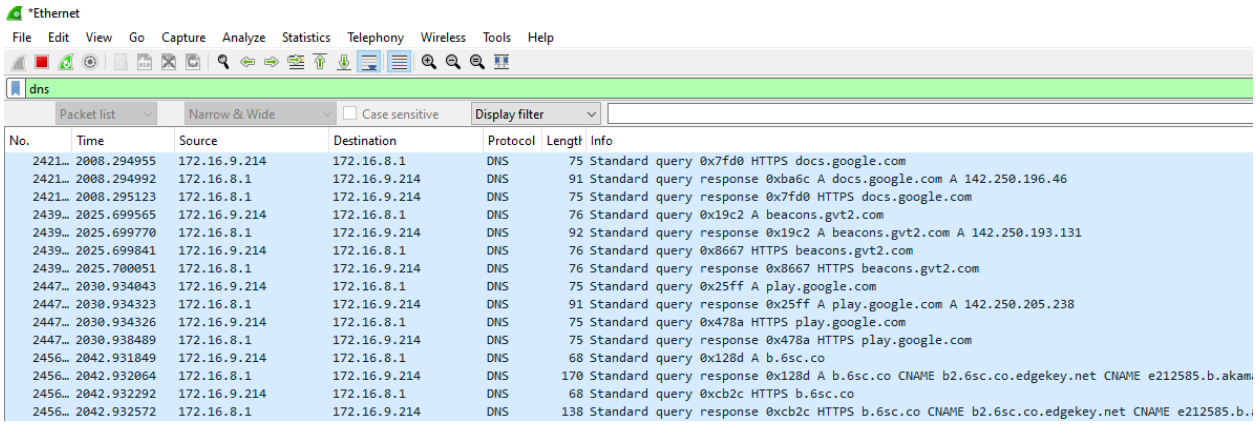
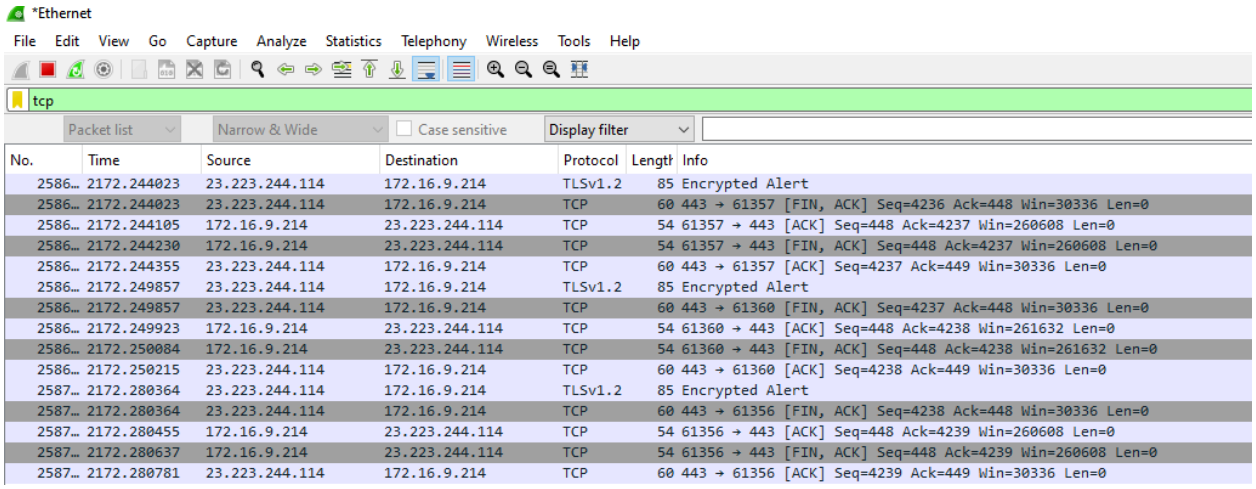
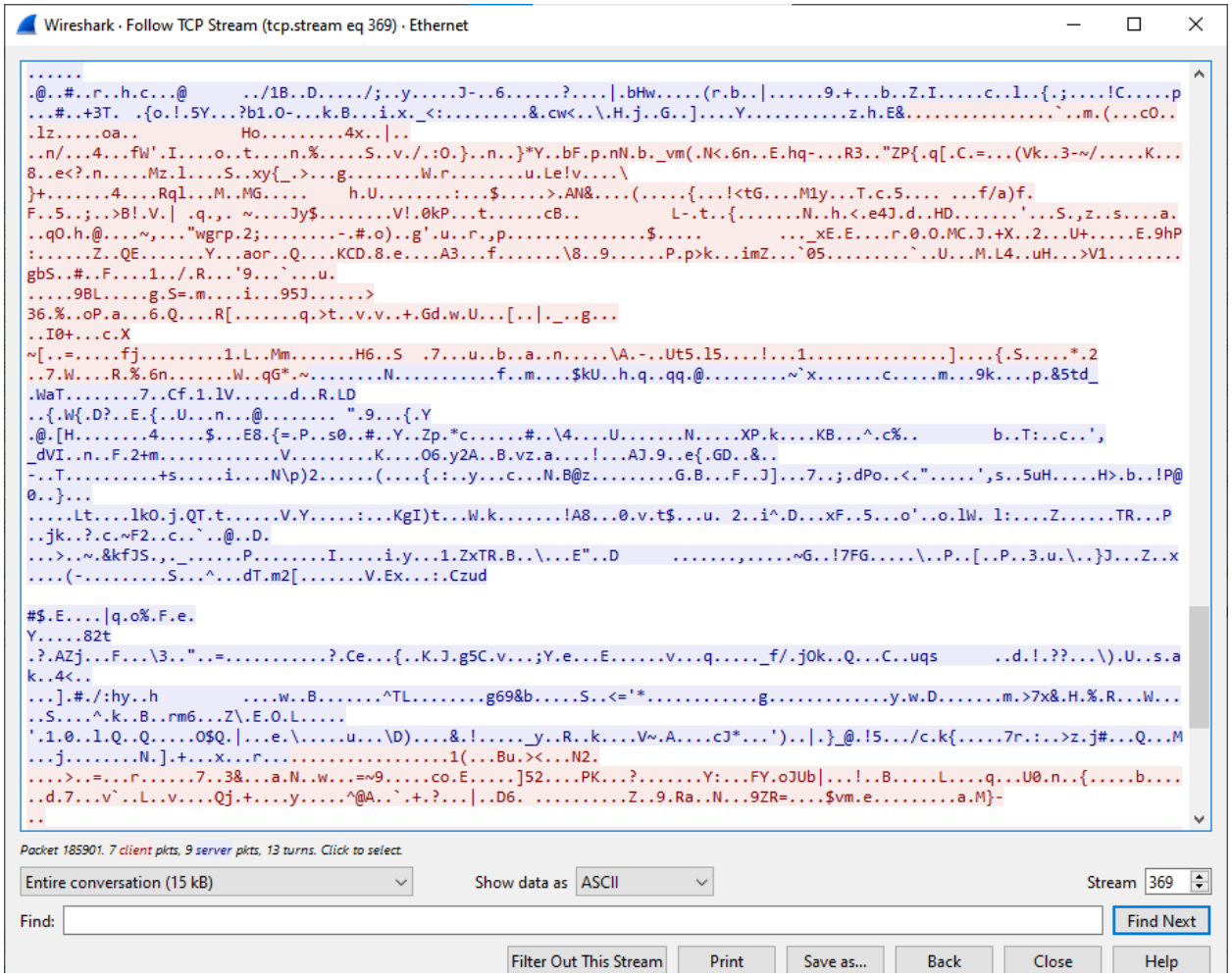

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list Narrow & Wide Case sensitive Display filter Find Cancel
No. Time Source Destination Protocol Length Info
2229… 1827.165779 0a:e0:af:ca:01:9c Broadcast ARP 60 Who has 172.16.8.1? Tell 172.16.8.54
2229… 1827.167165 172.16.11.136 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
2229… 1827.173672 169.254.80.152 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
2229… 1827.188986 169.254.80.152 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2229… 1827.192507 fe80::dda9:7c1c:6e5… ff02::1:2 DHCPv6 156 Solicit XID: 0x4ad293 CID: 000100011c008e4300270e13f33f
2229… 1827.198929 fe80::8924:6557:9c7… ff02::1:2 DHCPv6 157 Solicit XID: 0x2583a6 CID: 000100012959fbf6347df6b30a6a
2229… 1827.204086 172.16.8.204 172.16.11.255 UDP 86 57621 → 57621 Len=44
2229… 1827.239637 172.16.11.33 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2229… 1827.239775 172.16.9.167 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2229… 1827.257600 172.16.8.16 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2229… 1827.277913 172.16.8.236 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
2229… 1827.288461 HP_38:e8:75 Broadcast ARP 60 Who has 169.254.66.104? Tell 172.16.8.176
2229… 1827.297744 172.16.9.214 35.186.193.173 TCP 55 [TCP Keep-Alive] 61232 → 443 [ACK] Seq=2828 Ack=4851 Win=1050624 Len=1
2229… 1827.297868 35.186.193.173 172.16.9.214 TCP 66 [TCP Keep-Alive ACK] 443 → 61232 [ACK] Seq=4851 Ack=2829 Win=38656 Len=0 SLE=2828 SRE=2829
2229… 1827.341114 172.16.11.33 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
Frame 203099: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\
Ethernet II, Src: MicroStarInt_ad:3e:bf (d4:3d:7e:ad:3e:bf), Dst: Sophos_cf:be:45 (7c:5a:1c:c
Internet Protocol Version 4, Src: 172.16.9.214, Dst: 69.173.158.64
Transmission Control Protocol, Src Port: 61177, Dst Port: 443, Seq: 7057, Ack: 8427, Len: 0
0000 7c 5a 1c cf be 45 d4 3d 7e ad 3e bf 08 00 45 00
0010 00 28 2f 57 40 00 80 06 00 00 ac 10 09 d6 45 ad
0020 9e 40 ee f9 01 bb d1 22 93 48 64 65 cd ee 50 10
0030 01 fd 99 ee 00 00
wireshark_EthernetPCUUS2.pcapng
Packets: 223874 · Displayed: 223874 (100.0%)
Profile: Default


Wireshark · Coloring Rules Default
Name Filter
Bad TCP tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
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 || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.25
IPv6 hop limit low or unexpected (ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 64, 255})
Checksum Errors eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checks
SMB smb || nbss || nbns || netbios
HTTP http || tcp.port == 80 || http2
DCERPC dcerpc
Routing hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
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


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}
tcp
ip.host == host.example.com
C:\Users\REC\AppData\Roaming\Wireshark\dfilters
OK
Cancel
Help


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Packet list
Narrow & Wide
Case sensitive
Display filter
No. Time Source Destination Protocol Length Info
2421... 2008.294955 172.16.9.214 172.16.8.1 DNS 75 Standard query 0x7fd0 HTTPS docs.google.com
2421... 2008.294992 172.16.8.1 172.16.9.214 DNS 91 Standard query response 0xba6c A docs.google.com A 142.250.196.46
2421... 2008.295123 172.16.8.1 172.16.9.214 DNS 75 Standard query response 0x7fd0 HTTPS docs.google.com
2439... 2025.699565 172.16.9.214 172.16.8.1 DNS 76 Standard query 0x19c2 A beacons.gvt2.com
2439... 2025.699770 172.16.8.1 172.16.9.214 DNS 92 Standard query response 0x19c2 A beacons.gvt2.com A 142.250.193.131
2439... 2025.699841 172.16.9.214 172.16.8.1 DNS 76 Standard query 0x8667 HTTPS beacons.gvt2.com
2439... 2025.700051 172.16.8.1 172.16.9.214 DNS 76 Standard query response 0x8667 HTTPS beacons.gvt2.com
2447... 2030.934043 172.16.9.214 172.16.8.1 DNS 75 Standard query 0x25ff A play.google.com
2447... 2030.934323 172.16.8.1 172.16.9.214 DNS 91 Standard query response 0x25ff A play.google.com A 142.250.205.238
2447... 2030.934326 172.16.9.214 172.16.8.1 DNS 75 Standard query 0x478a HTTPS play.google.com
2447... 2030.938489 172.16.8.1 172.16.9.214 DNS 75 Standard query response 0x478a HTTPS play.google.com
2456... 2042.931849 172.16.9.214 172.16.8.1 DNS 68 Standard query 0x128d A b.6sc.co
2456... 2042.932064 172.16.8.1 172.16.9.214 DNS 170 Standard query response 0x128d A b.6sc.co CNAME b2.6sc.co.edgekey.net CNAME e212585.b.akam
2456... 2042.932292 172.16.9.214 172.16.8.1 DNS 68 Standard query 0xcb2c HTTPS b.6sc.co
2456... 2042.932572 172.16.8.1 172.16.9.214 DNS 138 Standard query response 0xcb2c HTTPS b.6sc.co CNAME b2.6sc.co.edgekey.net CNAME e212585.b.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Packet list
Narrow & Wide
Case sensitive
Display filter
No. Time Source Destination Protocol Length Info
2586... 2172.244023 23.223.244.114 172.16.9.214 TLSv1.2 85 Encrypted Alert
2586... 2172.244023 23.223.244.114 172.16.9.214 TCP 60 443 → 61357 [FIN, ACK] Seq=4236 Ack=448 Win=30336 Len=0
2586... 2172.244105 172.16.9.214 23.223.244.114 TCP 54 61357 → 443 [ACK] Seq=448 Ack=4237 Win=260608 Len=0
2586... 2172.244230 172.16.9.214 23.223.244.114 TCP 54 61357 → 443 [FIN, ACK] Seq=448 Ack=4237 Win=260608 Len=0
2586... 2172.244355 23.223.244.114 172.16.9.214 TCP 60 443 → 61357 [ACK] Seq=4237 Ack=449 Win=30336 Len=0
2586... 2172.249857 23.223.244.114 172.16.9.214 TLSv1.2 85 Encrypted Alert
2586... 2172.249857 23.223.244.114 172.16.9.214 TCP 60 443 → 61360 [FIN, ACK] Seq=4237 Ack=448 Win=30336 Len=0
2586... 2172.249923 172.16.9.214 23.223.244.114 TCP 54 61360 → 443 [ACK] Seq=448 Ack=4238 Win=261632 Len=0
2586... 2172.250084 172.16.9.214 23.223.244.114 TCP 54 61360 → 443 [FIN, ACK] Seq=448 Ack=4238 Win=261632 Len=0
2586... 2172.250215 23.223.244.114 172.16.9.214 TCP 60 443 → 61360 [ACK] Seq=4238 Ack=449 Win=30336 Len=0
2587... 2172.280364 23.223.244.114 172.16.9.214 TLSv1.2 85 Encrypted Alert
2587... 2172.280364 23.223.244.114 172.16.9.214 TCP 60 443 → 61356 [FIN, ACK] Seq=4238 Ack=448 Win=30336 Len=0
2587... 2172.280455 172.16.9.214 23.223.244.114 TCP 54 61356 → 443 [ACK] Seq=448 Ack=4239 Win=260608 Len=0
2587... 2172.280637 172.16.9.214 23.223.244.114 TCP 54 61356 → 443 [FIN, ACK] Seq=448 Ack=4239 Win=260608 Len=0
2587... 2172.280781 23.223.244.114 172.16.9.214 TCP 60 443 → 61356 [ACK] Seq=4239 Ack=449 Win=30336 Len=0




```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: MicroStarInt_ad:3e:bf (d4:3d:7e:ad:3e:bf), Dst: Sophos_cf:be:45 (7c:5a:1c
> Internet Protocol Version 4, Src: 172.16.9.214, Dst: 34.104.35.123
v Transmission Control Protocol, Src Port: 61366, Dst Port: 80, Seq: 5473, Ack: 7702, Len: 0
    Source Port: 61366
    Destination Port: 80
    [Stream index: 576]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 5473    (relative sequence number)
    Sequence Number (raw): 382370088
    [Next Sequence Number: 5473    (relative sequence number)]
    Acknowledgment Number: 7702    (relative ack number)
```