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
2229 1827.362105	34.126.167.117	172.16.9.214	TLSv1.2	131	Application Data, Encrypted Alert

> Frame 203099: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\N
> Ethernet II, Src: MicroStarInt_ad:3e:bf (d4:3d:7e:ad:3e:bf), Dst: Sophos_cf:be:45 (7c:5a:1c:cf
> 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   |Z···E·= ~·>···E·
0010  00 28 2f 57 40 00 80 06  00 00 ac 10 09 d6 45 ad   ·(/W@··· ······E·
0020  9e 40 ee f9 01 bb d1 22  93 48 64 65 cd ee 50 10   ·@····" ·Hde··P·
0030  01 fd 99 ee 00 00                                   ······
```

Packets: 223874 · Displayed: 223874 (100.0%)   Profile: Default
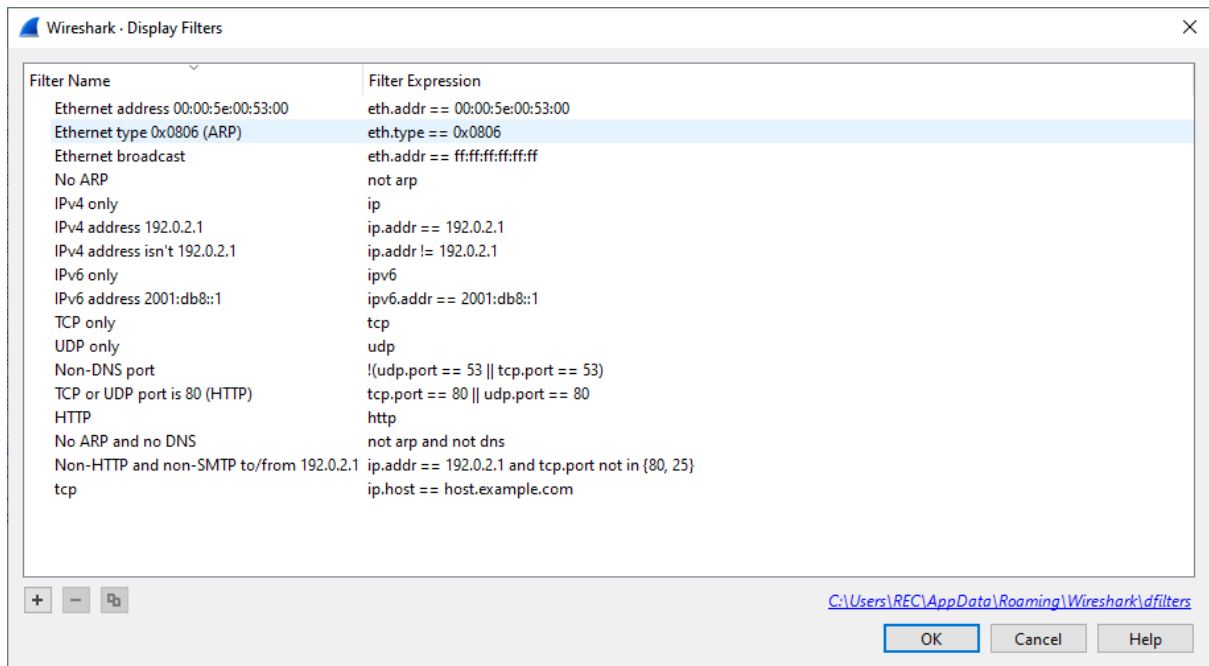
wireshark_EthernetPCUUS2.pcapng

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

```
......
.@..#..r..h.c...@      ../1B..D...../;..y.....J-..6......?....|.bHw.....(r.b..|......9.+...b..Z.I.....c..l..{.;....!C.....p
...#..+3T. .{o.!.5Y..?b1.0-...k.B...i.x._<:.........&.cw<..\.H.j..G..]....Y.............z.h.E&................`..m.(...cO..
.lz.....oa..         Ho.........4x..|.
..n/...4...fW'.I...o..t....n.%....S..v./.:O.}..n..}*Y..bF.p.nN.b._vm(.N<.6n..E.hq-...R3.."ZP{.q[.C.=...(Vk..3-~/.....K...
8..e<?.n.....Mz.l....S..xy{_.>...g.......W.r.......u.Le!v....\
}+.......4...Rql...M..MG.....    h.U.........:..$.....>.AN&....(.....{...!<tG....M1y...T.c.5.... .../f/a)f.
F..5..;..>B!.V.| .q.,. ~....Jy$........V!.0kP...t.....cB..        L-.t..{.......N..h.<.e4J.d..HD.......'...S.,z..s....a.
..qO.h.@....~,..."wgrp.2;.........-.#.o)..g'.u..r.,p................$.....        ...xE.E....r.0.O.MC.J.+X..2...U+.....E.9hP
:......Z..QE.......Y..aor..Q...KCD.8.e....A3...f......\8..9......P.p>k...imZ..`05.........`..U...M.L4..uH...>V1.........
gbS..#..F....1../.R.."9...`...u.
.....9BL.....g.S=.m....i...95J......>
36.%..oP.a...6.Q....R[.......q.>t..v.v..+.Gd.w.U...[..|._..g...
..I0+...c.X
~[..=.....fj..........1.L..Mm......H6..S .7...u..b..a..n.....\A.-..Ut5.l5....!...1.................]...{.S.....*.2
..7.W....R.%.6n........W..qG*.~.......N........f..m...$kU..h.q..qq.@.........~`x.......c....m...9k...p.&5td_
.WaT........7..Cf.1.lV......d..R.LD
..{.W{.D?..E.{..U...n...@........ ".9...{.Y
.@.[H........4....$...E8.{=.P..s0..#..Y..Zp.*c.....#..\4....U.......N....XP.k...KB...^.c%..      b..T:..c..',
_dVI..n..F.2+m...........V.......K....O6.y2A..B.vz.a...!...AJ.9..e{.GD..&..
-..T...........+s.....i...N\p)2.....(....{.:..y...c...N.B@z.......G.B...F..J]...7..;.dPo..<."....',s..5uH.....H>.b..!P@
0..}...
.....Lt....lkO.j.QT.t......V.Y....:...KgI)t...W.k.......!A8...0.v.t$...u. 2..i^.D...xF..5...o'..o.lW. l:...Z.....TR...P
..jk..?.c.~F2..c..`..@..D.
...>..~.&kfJS.,._.....P.......I.....i.y...1.ZxTR.B..\...E"..D      .......,....~G..!7FG....\..P..[..P..3.u.\..}J...Z..x
....(-........S...^...dT.m2[.......V.Ex...:.Czud

#$.E....|q.o%.F.e.
Y.....82t
.?.AZj..F...\3.."...=.............?.Ce...{..K.J.g5C.v...;Y.e...E......v...q....._f/.jOk..Q...C..uqs      ..d.!.??...\).U..s.a
k..4<..
...].#./:hy..h       ....w..B......^TL.......g69&b.....S..<='*...........g..........y.w.D......m.>7x&.H.%.R...W...
..S....^.k..B..rm6...Z\.E.O.L.....
'.1.0..l.Q..Q.....O$Q.|...e.\.....u...\D)....&.!....._y..R..k....V~.A....cJ*...')..|.}_@.!5.../c.k{.....7r.:..>z.j#...Q...M
...j.......N.]+...x...r...............1(..Bu.><...N2.
....>..=...r.......7..3&...a.N..w...=~9.....co.E....]52....PK...?.......Y:...FY.oJUb|...!..B.....L....q...U0.n..{.....b....
..d.7...v`..L..v....Qj.+....y.....^@A..`.+.?...|..D6. ..........Z..9.Ra..N...9ZR=....$vm.e.........a.M}-
..
```

Packet 185901. 7 client pkts, 9 server pkts, 13 turns. Click to select.

Entire conversation (15 kB) ▾   Show data as ASCII ▾   Stream 369 ▾

Find: [   ]   Find Next

[Filter Out This Stream] [Print] [Save as...] [Back] [Close]   [Help]

```
        [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)
```