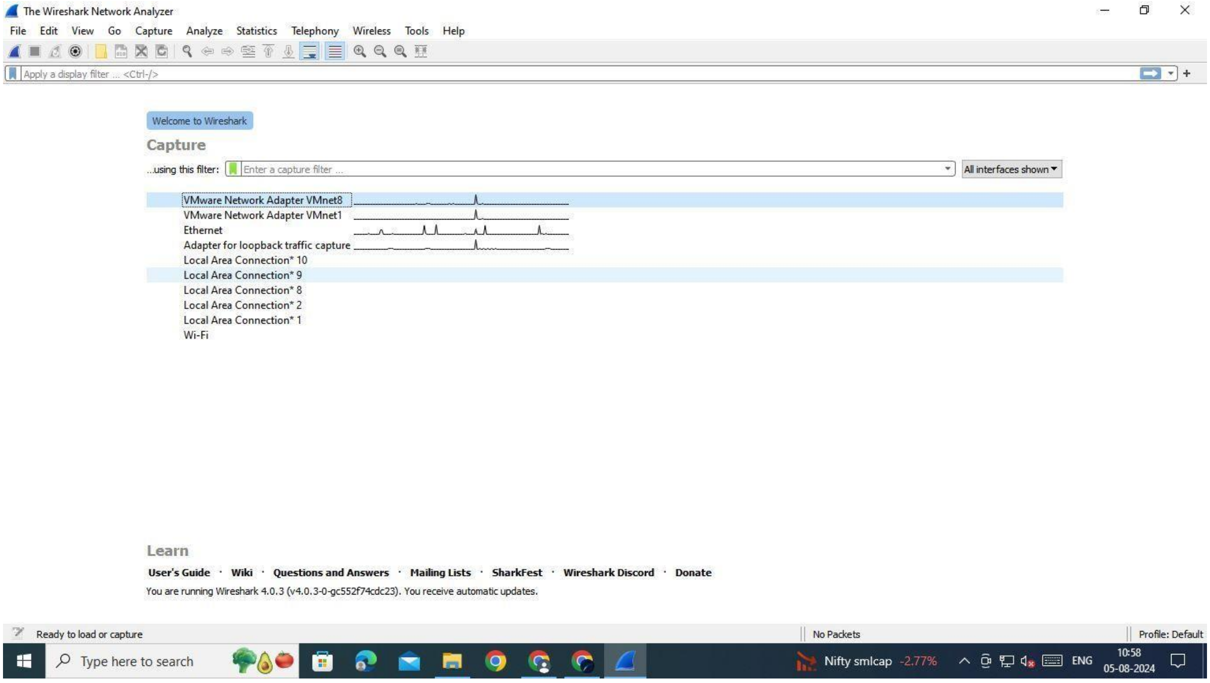
EX-NO : 05

DATE : 05 -08-2024 **EXPERIMENTS ON PACKET CAPTURE TOOL: WIRESHARK**

CAPTURING PACKETS:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Wi-Fi

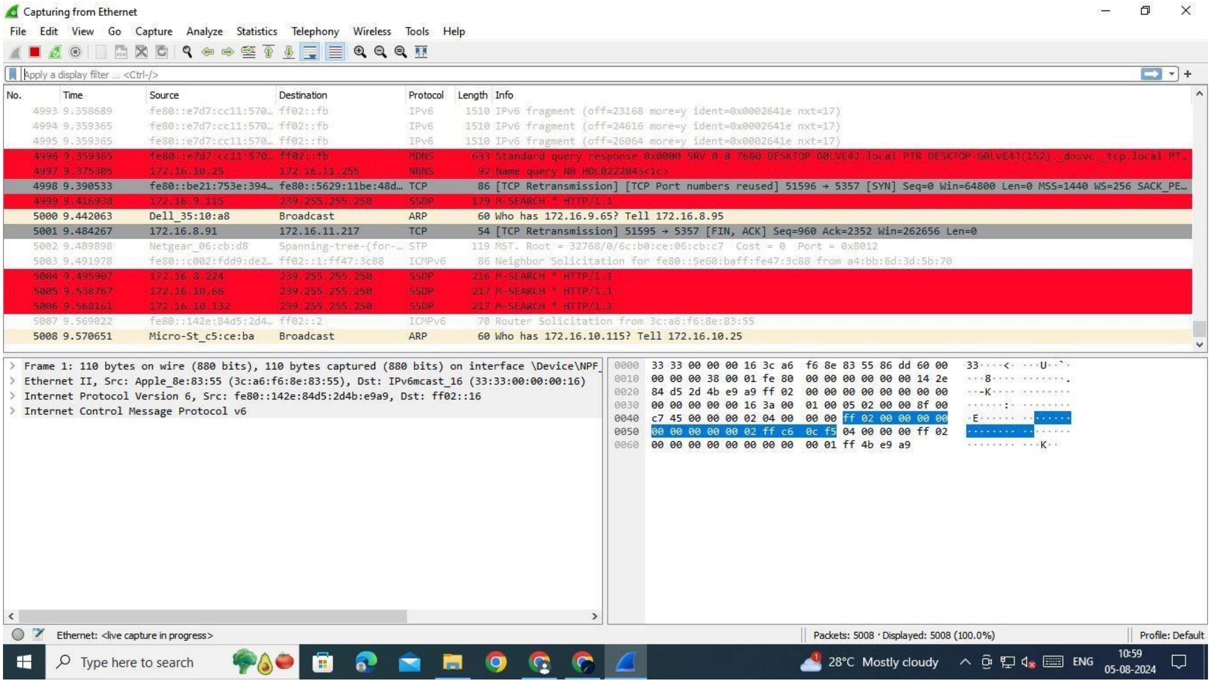
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

PACKET LISTS, DETAILS AND BYTES:


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

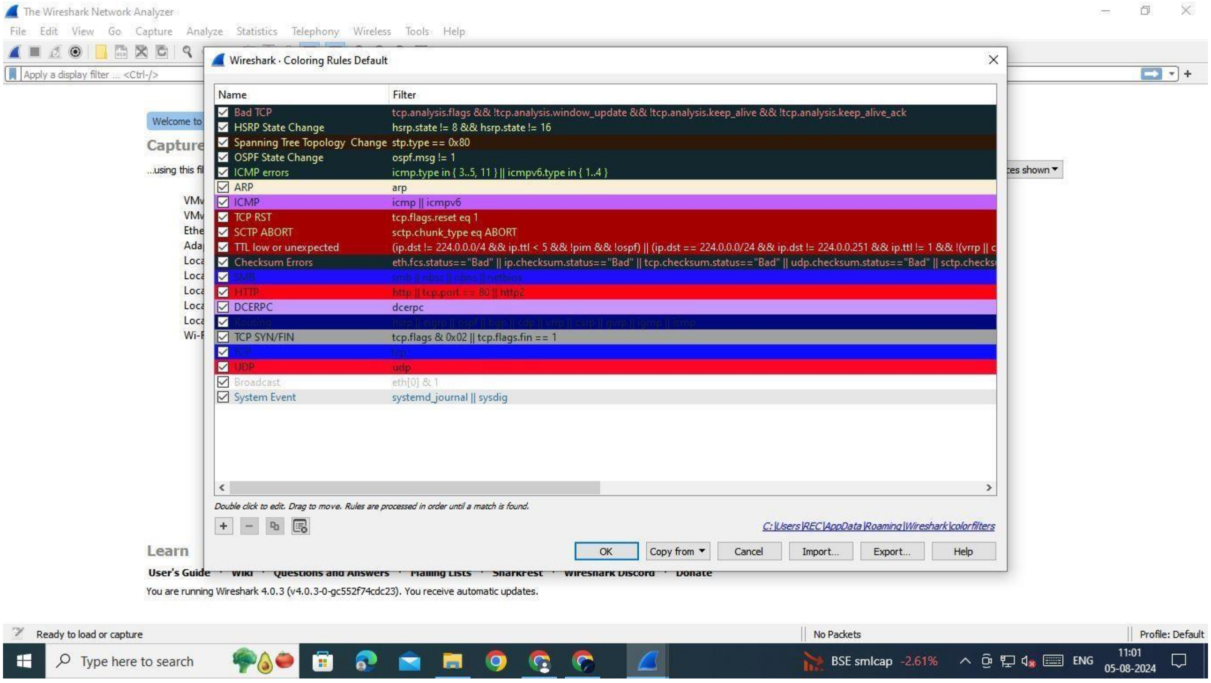
```
No.  Time       Source                  Destination             Protocol  Length Info
4993 9.358689   fe80::e7d7:cc11:570…    ff02::fb                IPv6      1510 IPv6 fragment (off=23168 more=y ident=0x0002641e nxt=17)
4994 9.359365   fe80::e7d7:cc11:570…    ff02::fb                IPv6      1510 IPv6 fragment (off=24616 more=y ident=0x0002641e nxt=17)
4995 9.359365   fe80::e7d7:cc11:570…    ff02::fb                IPv6      1510 IPv6 fragment (off=26064 more=y ident=0x0002641e nxt=17)
4996 9.359365   fe80::e7d7:cc11:570…    ff02::fb                MDNS       633 Standard query response 0x0000 SRV 0 0 7680 DESKTOP-G0LVE4J.local PTR DESKTOP-G0LVE4J(152)._dosvc._tcp.local PT…
4997 9.375305   172.16.10.25            172.16.11.255           NBNS        92 Name query NB HDC0222043<1c>
4998 9.390533   fe80::be21:753e:394…    fe80::5629:11be:48d…    TCP         86 [TCP Retransmission] [TCP Port numbers reused] 51596 → 5357 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PE…
4999 9.416938   172.16.9.115            239.255.255.250         SSDP       179 M-SEARCH * HTTP/1.1
5000 9.442063   Dell_35:10:a8           Broadcast               ARP         60 Who has 172.16.9.65? Tell 172.16.8.95
5001 9.484267   172.16.8.91             172.16.11.217           TCP         54 [TCP Retransmission] 51595 → 5357 [FIN, ACK] Seq=960 Ack=2352 Win=262656 Len=0
5002 9.489898   Netgear_06:cb:d8        Spanning-tree-(for-…    STP        119 MST. Root = 32768/0/6c:b0:ce:06:cb:c7  Cost = 0  Port = 0x8012
5003 9.491978   fe80::c002:fdd9:de2…    ff02::1:ff47:3c88       ICMPv6      86 Neighbor Solicitation for fe80::5e60:baff:fe47:3c88 from a4:bb:6d:3d:5b:70
5004 9.495907   172.16.8.224            239.255.255.250         SSDP       216 M-SEARCH * HTTP/1.1
5005 9.538767   172.16.10.66            239.255.255.250         SSDP       217 M-SEARCH * HTTP/1.1
5006 9.568161   172.16.10.132           239.255.255.250         SSDP       217 M-SEARCH * HTTP/1.1
5007 9.569022   fe80::142e:84d5:2d4…    ff02::2                 ICMPv6      70 Router Solicitation from 3c:a6:f6:8e:83:55
5008 9.570651   Micro-St_c5:ce:ba       Broadcast               ARP         60 Who has 172.16.10.115? Tell 172.16.10.25
```

```
> Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_
> Ethernet II, Src: Apple_8e:83:55 (3c:a6:f6:8e:83:55), Dst: IPv6mcast_16 (33:33:00:00:00:16)
> Internet Protocol Version 6, Src: fe80::142e:84d5:2d4b:e9a9, Dst: ff02::16
> Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 16 3c a6  f6 8e 83 55 86 dd 60 00   33····<· ···U··`·
0010  00 00 00 38 00 01 fe 80  00 00 00 00 00 00 14 2e   ···8···· ·······.
0020  84 d5 2d 4b e9 a9 ff 02  00 00 00 00 00 00 00 00   ··-K···· ········
0030  00 00 00 00 00 16 3a 00  01 00 05 02 00 00 8f 00   ······:· ········
0040  c7 45 00 00 00 02 04 00  00 00 ff 02 00 00 00 00   ·E······ ········
0050  00 00 00 00 00 02 ff c6  0c f5 04 00 00 00 ff 02   ········ ········
0060  00 00 00 00 00 00 00 00  00 01 ff 4b e9 a9         ········ ··K··
```

Ethernet: <live capture in progress> | Packets: 5008 · Displayed: 5008 (100.0%) | Profile: Default

COLORING RULES:



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
☑ TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || c
☑ 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

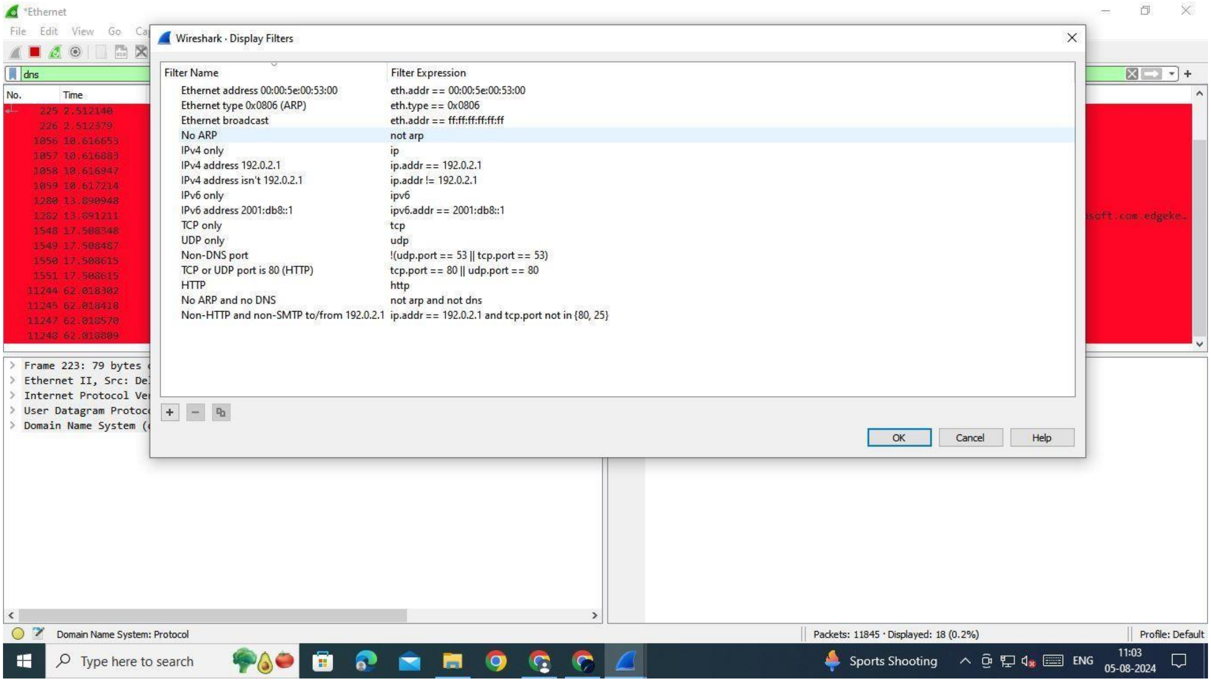
Double click to edit. Drag to move. Rules are processed in order until a match is found.

C:\Users\REC\AppData\Roaming\Wireshark\colorfilters

You are running Wireshark 4.0.3 (v4.0.3-0-gc552f74cdc23). You receive automatic updates.

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to
Capture
…using this fi
VMw
VMw
Ethe
Ada
Loca
Loca
Loca
Loca
Loca
Wi-F
ces shown
+ −
OK
Copy from
Cancel
Import…
Export…
Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Ready to load or capture
No Packets
Profile: Default
Type here to search
BSE smlcap -2.61%
ENG
11:01
05-08-2024

BUILDING DISPLAY FILTER EXPRESSIONS:



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}

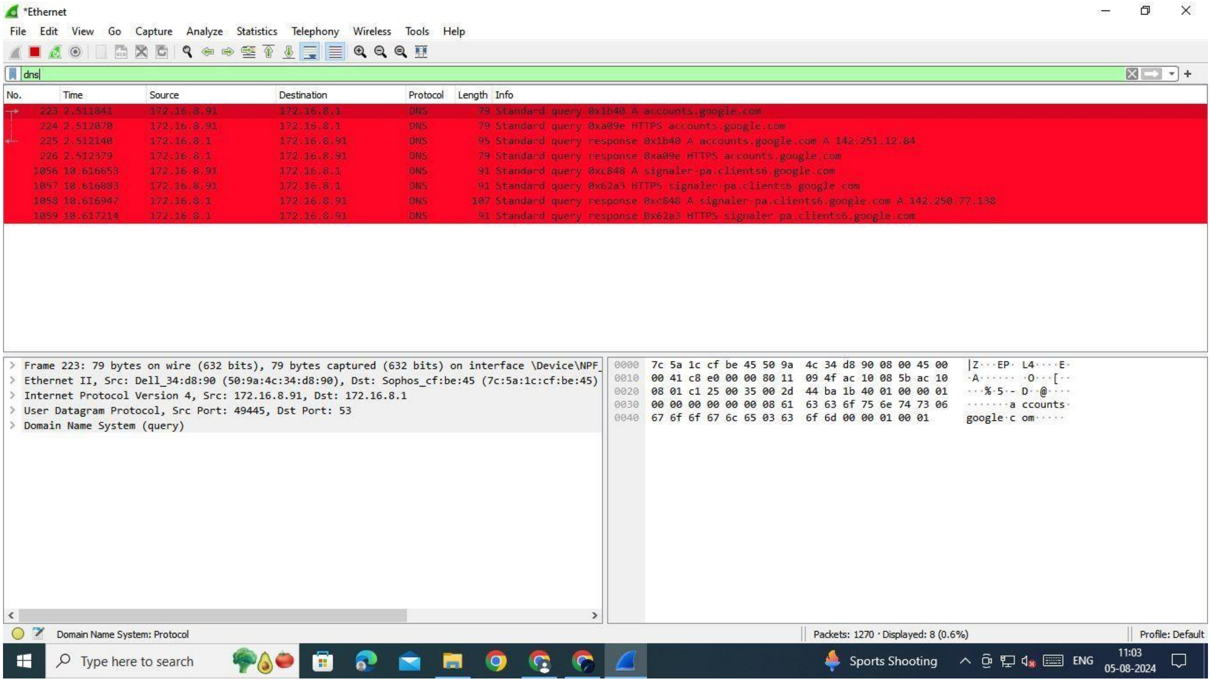
```
No.   Time
  225 2.512140
  226 2.512379
 1056 10.616653
 1057 10.616883
 1058 10.616947
 1059 10.617214
 1280 13.090948
 1282 13.091211
 1548 17.508348
 1549 17.508487
 1550 17.508615
 1551 17.508615
11244 62.018302
11245 62.018418
11247 62.018570
11248 62.018889
```

```
> Frame 223: 79 bytes
> Ethernet II, Src: De
> Internet Protocol Ve
> User Datagram Protoco
> Domain Name System (
```

Domain Name System: Protocol

Packets: 11845 · Displayed: 18 (0.2%)

FILTERING PACKETS:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Domain Name System: Protocol
Packets: 1270 · Displayed: 8 (0.6%)
Profile: Default
Type here to search
Sports Shooting
ENG
11:03
05-08-2024

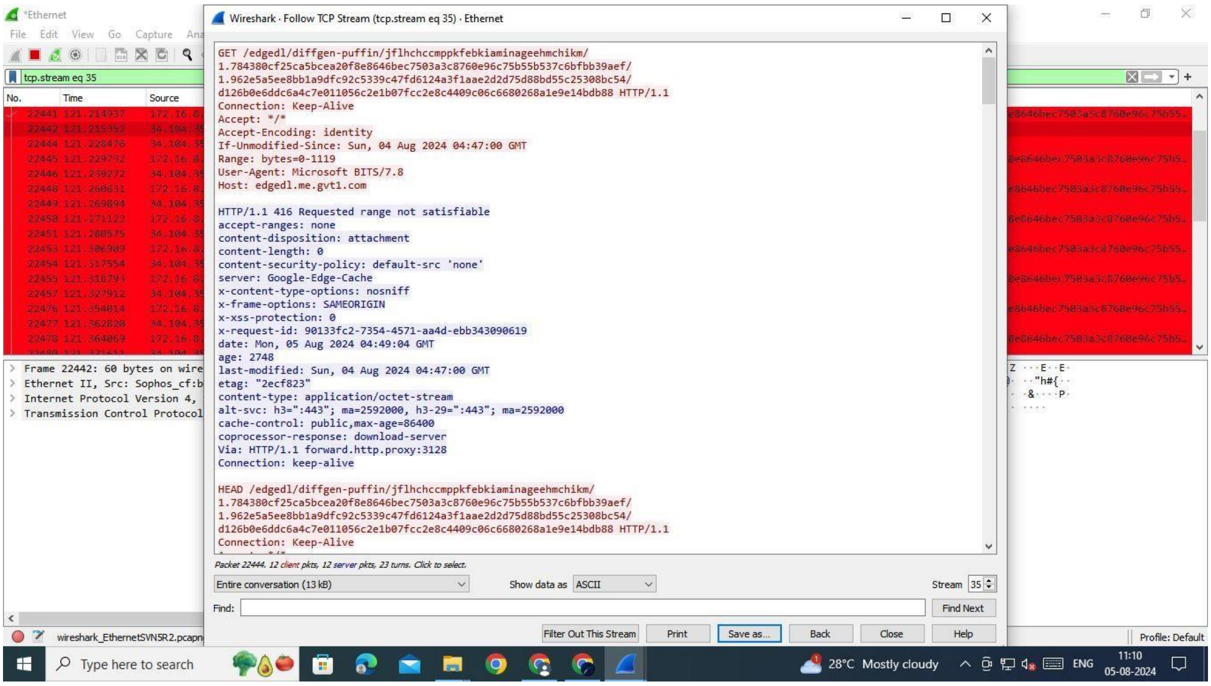
dns

```
No.   Time       Source        Destination   Protocol Length Info
  223 2.511841   172.16.8.91   172.16.8.1    DNS       79 Standard query 0x1b40 A accounts.google.com
  224 2.512070   172.16.8.91   172.16.8.1    DNS       79 Standard query 0xa09e HTTPS accounts.google.com
  225 2.512140   172.16.8.1    172.16.8.91   DNS       95 Standard query response 0x1b40 A accounts.google.com A 142.251.12.84
  226 2.512379   172.16.8.1    172.16.8.91   DNS       79 Standard query response 0xa09e HTTPS accounts.google.com
 1056 10.616653  172.16.8.91   172.16.8.1    DNS       91 Standard query 0xc848 A signaler-pa.clients6.google.com
 1057 10.616883  172.16.8.91   172.16.8.1    DNS       91 Standard query 0x62a3 HTTPS signaler-pa.clients6.google.com
 1058 10.616947  172.16.8.1    172.16.8.91   DNS      107 Standard query response 0xc848 A signaler-pa.clients6.google.com A 142.250.77.138
 1059 10.617214  172.16.8.1    172.16.8.91   DNS       91 Standard query response 0x62a3 HTTPS signaler-pa.clients6.google.com
```

```
> Frame 223: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_
> Ethernet II, Src: Dell_34:d8:90 (50:9a:4c:34:d8:90), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.8.91, Dst: 172.16.8.1
> User Datagram Protocol, Src Port: 49445, Dst Port: 53
> Domain Name System (query)
```

```
0000  7c 5a 1c cf be 45 50 9a  4c 34 d8 90 08 00 45 00   |Z···EP· L4····E·
0010  00 41 c8 e0 00 00 80 11  09 4f ac 10 08 5b ac 10   ·A······ ·O···[··
0020  08 01 c1 25 00 35 00 2d  44 ba 1b 40 01 00 00 01   ···%·5·- D··@····
0030  00 00 00 00 00 00 08 61  63 63 6f 75 6e 74 73 06   ·······a ccounts·
0040  67 6f 6f 67 6c 65 03 63  6f 6d 00 00 01 00 01      google·c om·····
```

APPLY FILTERS:



tcp.stream eq 35

```
No.    Time        Source
22441  121.214937  172.16.8.
22442  121.215352  34.104.35
22444  121.228476  34.104.35
22445  121.229732  172.16.8.
22446  121.239272  34.104.35
22448  121.260631  172.16.8.
22449  121.269894  34.104.35
22450  121.271122  172.16.8.
22451  121.280575  34.104.35
22453  121.306909  172.16.8.
22454  121.317554  34.104.35
22455  121.318793  172.16.8.
22457  121.327912  34.104.35
22476  121.354014  172.16.8.
22477  121.362820  34.104.35
22478  121.364069  172.16.8.
```

```
> Frame 22442: 60 bytes on wire
> Ethernet II, Src: Sophos_cf:b
> Internet Protocol Version 4,
> Transmission Control Protocol
```

```
GET /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageehmchikm/
1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c75b55b537c6bfbb39aef/
1.962e5a5ee8bb1a9dfc92c5339c47fd6124a3f1aae2d2d75d88bd55c25308bc54/
d126b0e6ddc6a4c7e011056c2e1b07fcc2e8c4409c06c6680268a1e9e14bdb88 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
If-Unmodified-Since: Sun, 04 Aug 2024 04:47:00 GMT
Range: bytes=0-1119
User-Agent: Microsoft BITS/7.8
Host: edgedl.me.gvt1.com

HTTP/1.1 416 Requested range not satisfiable
accept-ranges: none
content-disposition: attachment
content-length: 0
content-security-policy: default-src 'none'
server: Google-Edge-Cache
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-xss-protection: 0
x-request-id: 90133fc2-7354-4571-aa4d-ebb343090619
date: Mon, 05 Aug 2024 04:49:04 GMT
age: 2748
last-modified: Sun, 04 Aug 2024 04:47:00 GMT
etag: "2ecf823"
content-type: application/octet-stream
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000
cache-control: public,max-age=86400
coprocessor-response: download-server
Via: HTTP/1.1 forward.http.proxy:3128
Connection: keep-alive

HEAD /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageehmchikm/
1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c75b55b537c6bfbb39aef/
1.962e5a5ee8bb1a9dfc92c5339c47fd6124a3f1aae2d2d75d88bd55c25308bc54/
d126b0e6ddc6a4c7e011056c2e1b07fcc2e8c4409c06c6680268a1e9e14bdb88 HTTP/1.1
Connection: Keep-Alive
```

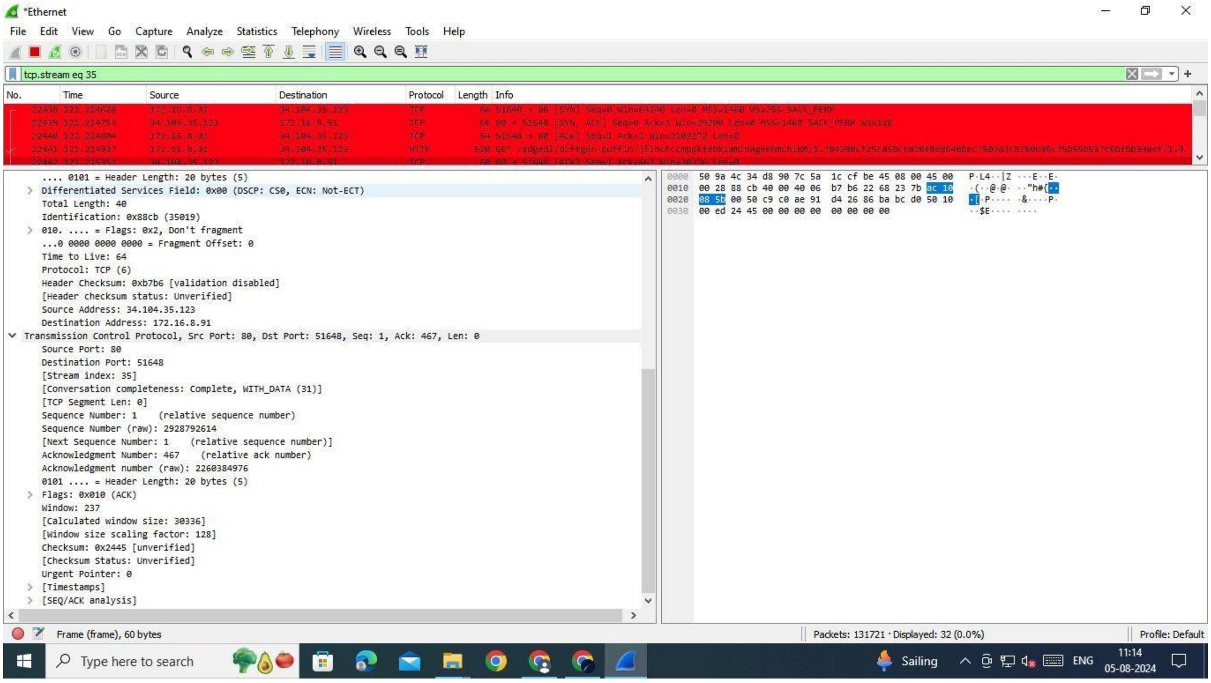
Packet 22444. 12 client pkts, 12 server pkts, 23 turns. Click to select.

Entire conversation (13 kB)

Show data as: ASCII

Stream: 35

INSPECTING AND FILTERING PACKETS:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

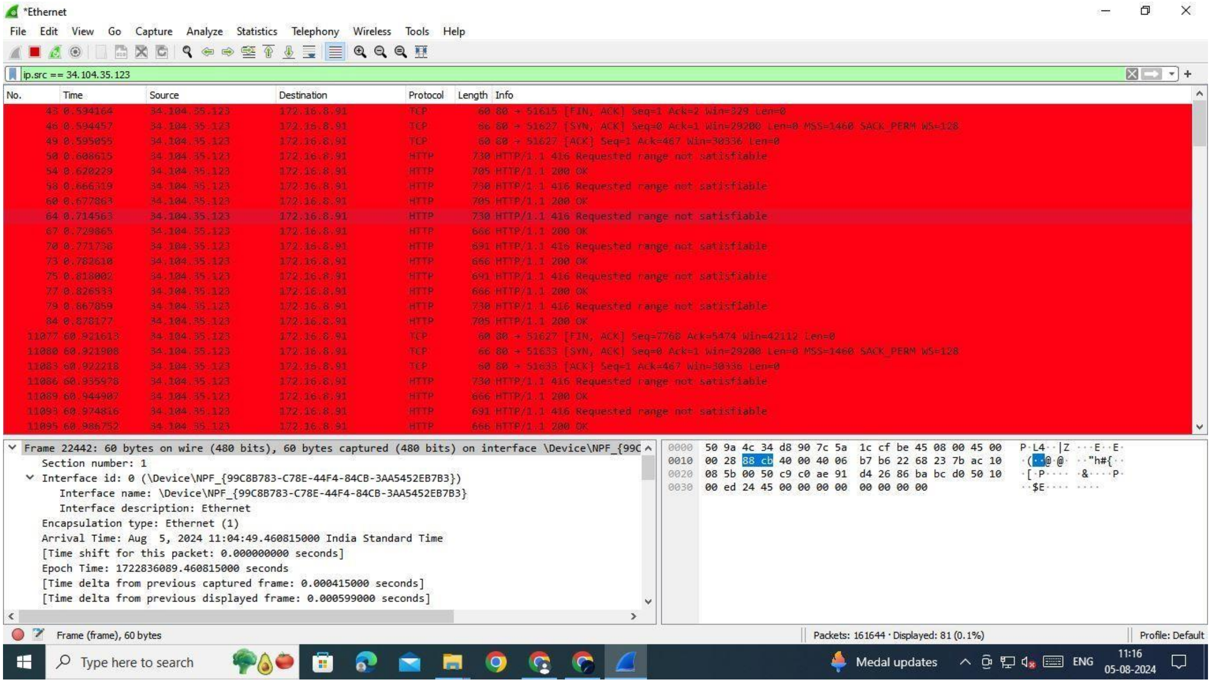
```
No.   Time        Source         Destination    Protocol Length Info
22438 121.214628  172.16.8.91    34.104.35.123  TCP      66 51648 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22439 121.214753  34.104.35.123  172.16.8.91    TCP      66 80 → 51648 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
22440 121.214804  172.16.8.91    34.104.35.123  TCP      54 51648 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
22441 121.214937  172.16.8.91    34.104.35.123  HTTP    520 GET /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c75b55b537c6bfbb39aef/1.9.
22442 121.215352  34.104.35.123  172.16.8.91    TCP      60 80 → 51648 [ACK] Seq=1 Ack=467 Win=30336 Len=0
```

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x88cb (35019)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb7b6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 34.104.35.123
    Destination Address: 172.16.8.91
v Transmission Control Protocol, Src Port: 80, Dst Port: 51648, Seq: 1, Ack: 467, Len: 0
    Source Port: 80
    Destination Port: 51648
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2928792614
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 467    (relative ack number)
    Acknowledgment number (raw): 2260384976
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0x2445 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
```

```
0000  50 9a 4c 34 d8 90 7c 5a  1c cf be 45 08 00 45 00   P·L4··|Z ···E··E·
0010  00 28 88 cb 40 00 40 06  b7 b6 22 68 23 7b ac 10   ·(··@·@· ··"h#{··
0020  08 5b 00 50 c9 c0 ae 91  d4 26 86 ba bc d0 50 10   ·[·P···· ·&····P·
0030  00 ed 24 45 00 00 00 00  00 00 00 00               ··$E···· ····
```

Frame (frame), 60 bytes | Packets: 131721 · Displayed: 32 (0.0%) | Profile: Default

Type here to search
Sailing
ENG
11:14
05-08-2024


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 34.104.35.123

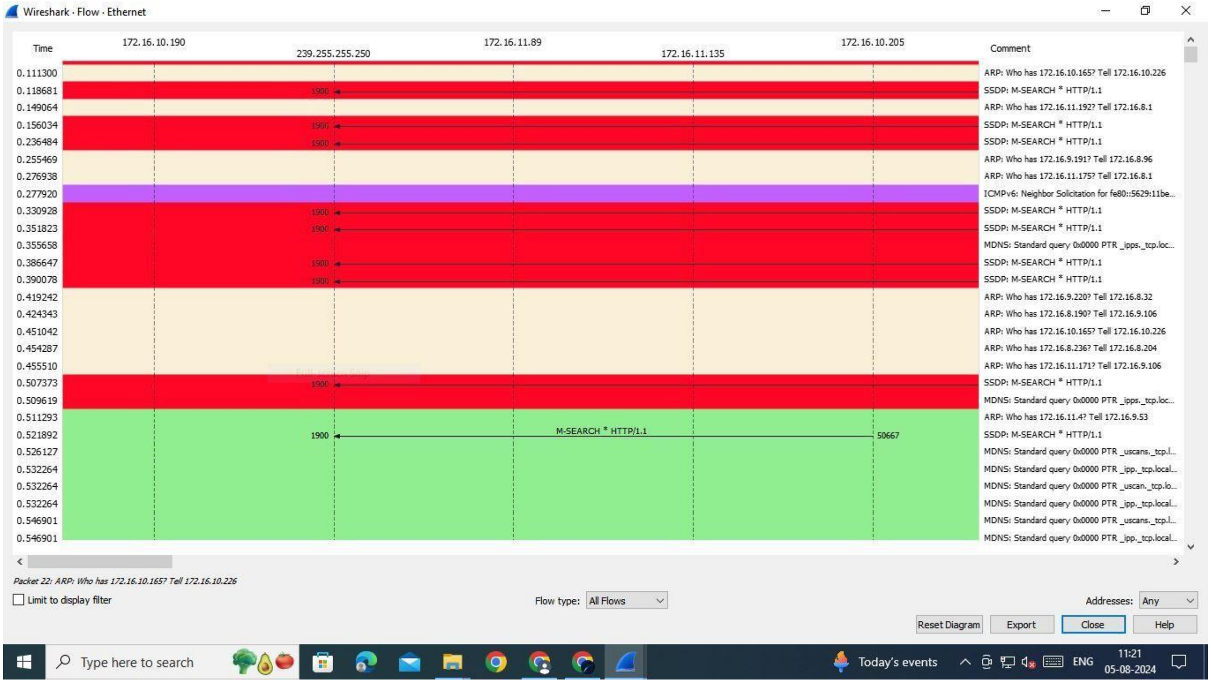
```
No.   Time        Source         Destination  Protocol Length Info
   43 0.594164    34.104.35.123  172.16.8.91  TCP      60 80 → 51615 [FIN, ACK] Seq=1 Ack=2 Win=329 Len=0
   46 0.594457    34.104.35.123  172.16.8.91  TCP      66 80 → 51627 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
   49 0.595055    34.104.35.123  172.16.8.91  TCP      60 80 → 51627 [ACK] Seq=1 Ack=467 Win=30336 Len=0
   50 0.608615    34.104.35.123  172.16.8.91  HTTP    730 HTTP/1.1 416 Requested range not satisfiable
   54 0.620229    34.104.35.123  172.16.8.91  HTTP    705 HTTP/1.1 200 OK
   58 0.666319    34.104.35.123  172.16.8.91  HTTP    730 HTTP/1.1 416 Requested range not satisfiable
   60 0.677863    34.104.35.123  172.16.8.91  HTTP    705 HTTP/1.1 200 OK
   64 0.714563    34.104.35.123  172.16.8.91  HTTP    730 HTTP/1.1 416 Requested range not satisfiable
   67 0.729865    34.104.35.123  172.16.8.91  HTTP    666 HTTP/1.1 200 OK
   70 0.771738    34.104.35.123  172.16.8.91  HTTP    691 HTTP/1.1 416 Requested range not satisfiable
   73 0.782610    34.104.35.123  172.16.8.91  HTTP    666 HTTP/1.1 200 OK
   75 0.818002    34.104.35.123  172.16.8.91  HTTP    691 HTTP/1.1 416 Requested range not satisfiable
   77 0.826533    34.104.35.123  172.16.8.91  HTTP    666 HTTP/1.1 200 OK
   79 0.867859    34.104.35.123  172.16.8.91  HTTP    730 HTTP/1.1 416 Requested range not satisfiable
   84 0.878177    34.104.35.123  172.16.8.91  HTTP    705 HTTP/1.1 200 OK
11077 60.921613   34.104.35.123  172.16.8.91  TCP      60 80 → 51627 [FIN, ACK] Seq=7768 Ack=5474 Win=42112 Len=0
11080 60.921908   34.104.35.123  172.16.8.91  TCP      66 80 → 51633 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
11083 60.922218   34.104.35.123  172.16.8.91  TCP      60 80 → 51633 [ACK] Seq=1 Ack=467 Win=30336 Len=0
11086 60.935978   34.104.35.123  172.16.8.91  HTTP    730 HTTP/1.1 416 Requested range not satisfiable
11089 60.944907   34.104.35.123  172.16.8.91  HTTP    666 HTTP/1.1 200 OK
11093 60.974816   34.104.35.123  172.16.8.91  HTTP    691 HTTP/1.1 416 Requested range not satisfiable
11095 60.986752   34.104.35.123  172.16.8.91  HTTP    666 HTTP/1.1 200 OK
```

```
v Frame 22442: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{99C
    Section number: 1
  v Interface id: 0 (\Device\NPF_{99C8B783-C78E-44F4-84CB-3AA5452EB7B3})
      Interface name: \Device\NPF_{99C8B783-C78E-44F4-84CB-3AA5452EB7B3}
      Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  5, 2024 11:04:49.460815000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1722836089.460815000 seconds
    [Time delta from previous captured frame: 0.000415000 seconds]
    [Time delta from previous displayed frame: 0.000599000 seconds]
```

```
0000  50 9a 4c 34 d8 90 7c 5a  1c cf be 45 08 00 45 00   P·L4··|Z ···E··E·
0010  00 28 88 cb 40 00 40 06  b7 b6 22 68 23 7b ac 10   ·(··@·@· ··"h#{··
0020  08 5b 00 50 c9 c0 ae 91  d4 26 86 ba bc d0 50 10   ·[·P···· ·&····P·
0030  00 ed 24 45 00 00 00 00  00 00 00 00               ··$E···· ····
```

Frame (frame), 60 bytes | Packets: 161644 · Displayed: 81 (0.1%) | Profile: Default

WORKFLOW GRAPH:



Wireshark · Flow · Ethernet

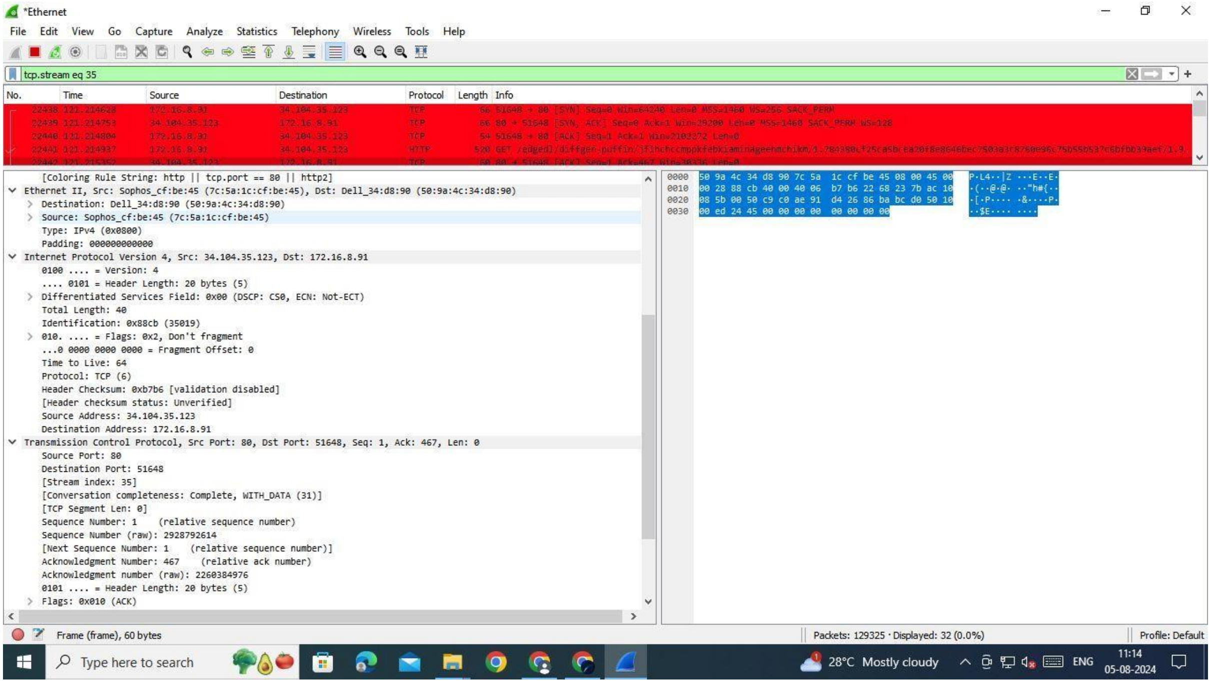
Time	172.16.10.190	239.255.255.250	172.16.11.89	172.16.11.135	172.16.10.205	Comment
0.111300						ARP: Who has 172.16.10.165? Tell 172.16.10.226
0.118681		1900				SSDP: M-SEARCH * HTTP/1.1
0.149064						ARP: Who has 172.16.11.192? Tell 172.16.8.1
0.156034		1900				SSDP: M-SEARCH * HTTP/1.1
0.236484		1900				SSDP: M-SEARCH * HTTP/1.1
0.255469						ARP: Who has 172.16.9.191? Tell 172.16.8.96
0.276938						ARP: Who has 172.16.11.175? Tell 172.16.8.1
0.277920						ICMPv6: Neighbor Solicitation for fe80::5629:11be...
0.330928		1900				SSDP: M-SEARCH * HTTP/1.1
0.351823		1900				SSDP: M-SEARCH * HTTP/1.1
0.355658						MDNS: Standard query 0x0000 PTR _ipps._tcp.loc...
0.386647		1900				SSDP: M-SEARCH * HTTP/1.1
0.390078		1900				SSDP: M-SEARCH * HTTP/1.1
0.419242						ARP: Who has 172.16.9.220? Tell 172.16.8.32
0.424343						ARP: Who has 172.16.8.190? Tell 172.16.9.106
0.451042						ARP: Who has 172.16.10.165? Tell 172.16.10.226
0.454287						ARP: Who has 172.16.8.236? Tell 172.16.8.204
0.455510						ARP: Who has 172.16.11.171? Tell 172.16.9.106
0.507373		1900				SSDP: M-SEARCH * HTTP/1.1
0.509619						MDNS: Standard query 0x0000 PTR _ipps._tcp.loc...
0.511293						ARP: Who has 172.16.11.4? Tell 172.16.9.53
0.521892		1900	M-SEARCH * HTTP/1.1		50667	SSDP: M-SEARCH * HTTP/1.1
0.526127						MDNS: Standard query 0x0000 PTR _uscans._tcp.l...
0.532264						MDNS: Standard query 0x0000 PTR _ipp._tcp.local...
0.532264						MDNS: Standard query 0x0000 PTR _uscan._tcp.lo...
0.532264						MDNS: Standard query 0x0000 PTR _ipp._tcp.local...
0.546901						MDNS: Standard query 0x0000 PTR _uscans._tcp.l...
0.546901						MDNS: Standard query 0x0000 PTR _ipp._tcp.local...

Packet 22: ARP: Who has 172.16.10.165? Tell 172.16.10.226

□ Limit to display filter

Flow type: All Flows

Addresses: Any



*Ethernet

tcp.stream eq 35

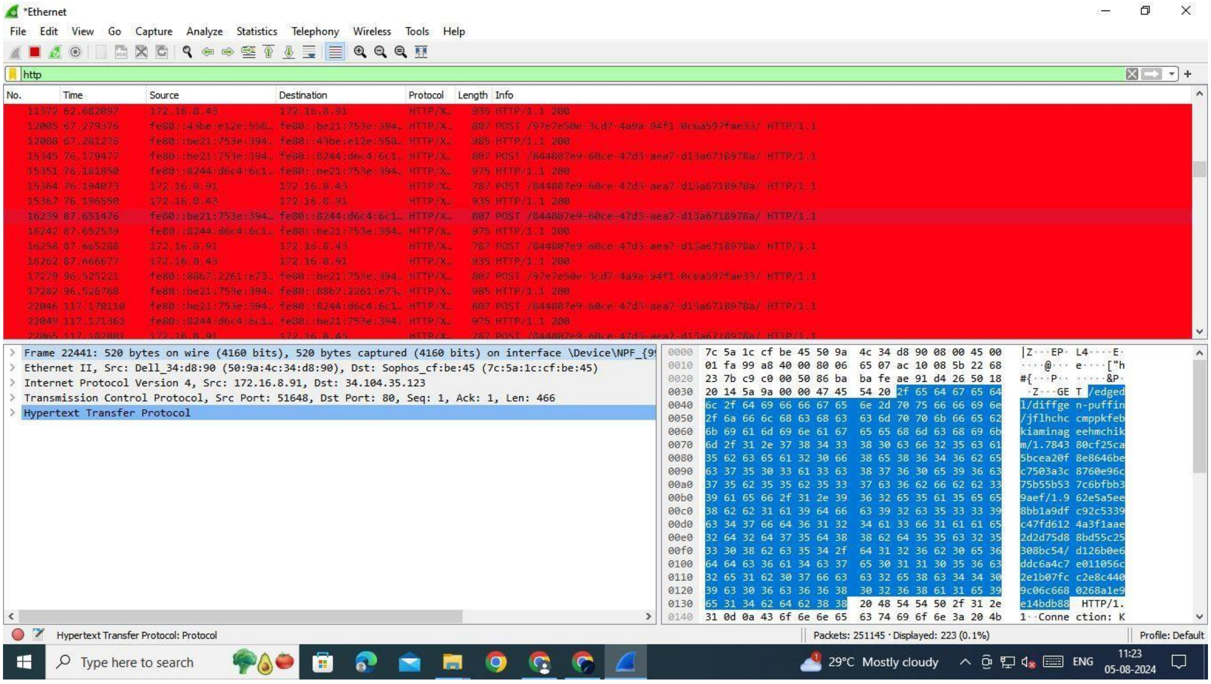
```
No.    Time        Source          Destination     Protocol  Length  Info
22438  121.214628  172.16.8.91     34.104.35.123   TCP       66      51648 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
22439  121.214753  34.104.35.123   172.16.8.91     TCP       66      80 → 51648 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
22440  121.214804  172.16.8.91     34.104.35.123   TCP       54      51648 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
22441  121.214937  172.16.8.91     34.104.35.123   HTTP      520     GET /edgedl/diffgen-puffin/jflhchccmppkfebkiaminageenmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c75b55b537c6bfbb39aef/1.9
22442  121.215352  34.104.35.123   172.16.8.91     TCP       60      80 → 51648 [ACK] Seq=1 Ack=467 Win=30336 Len=0
```

```
    [Coloring Rule String: http || tcp.port == 80 || http2]
v Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: Dell_34:d8:90 (50:9a:4c:34:d8:90)
  > Destination: Dell_34:d8:90 (50:9a:4c:34:d8:90)
  > Source: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
    Type: IPv4 (0x0800)
    Padding: 000000000000
v Internet Protocol Version 4, Src: 34.104.35.123, Dst: 172.16.8.91
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x88cb (35019)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xb7b6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 34.104.35.123
    Destination Address: 172.16.8.91
v Transmission Control Protocol, Src Port: 80, Dst Port: 51648, Seq: 1, Ack: 467, Len: 0
    Source Port: 80
    Destination Port: 51648
    [Stream index: 35]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2928792614
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 467    (relative ack number)
    Acknowledgment number (raw): 2260384976
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
```

```
0000  50 9a 4c 34 d8 90 7c 5a  1c cf be 45 08 00 45 00   P·L4··|Z ···E··E·
0010  00 28 88 cb 40 00 40 06  b7 b6 22 68 23 7b ac 10   ·(··@·@· ··"h#{··
0020  08 5b 00 50 c9 c0 ae 91  d4 26 86 ba bc d0 50 10   ·[·P···· ·&····P·
0030  00 ed 24 45 00 00 00 00  00 00 00 00               ··$E···· ····
```

Frame (frame), 60 bytes | Packets: 129325 · Displayed: 32 (0.0%) | Profile: Default

DISPLAY HTTP PACKETS:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
29°C Mostly cloudy
ENG
11:23
05-08-2024

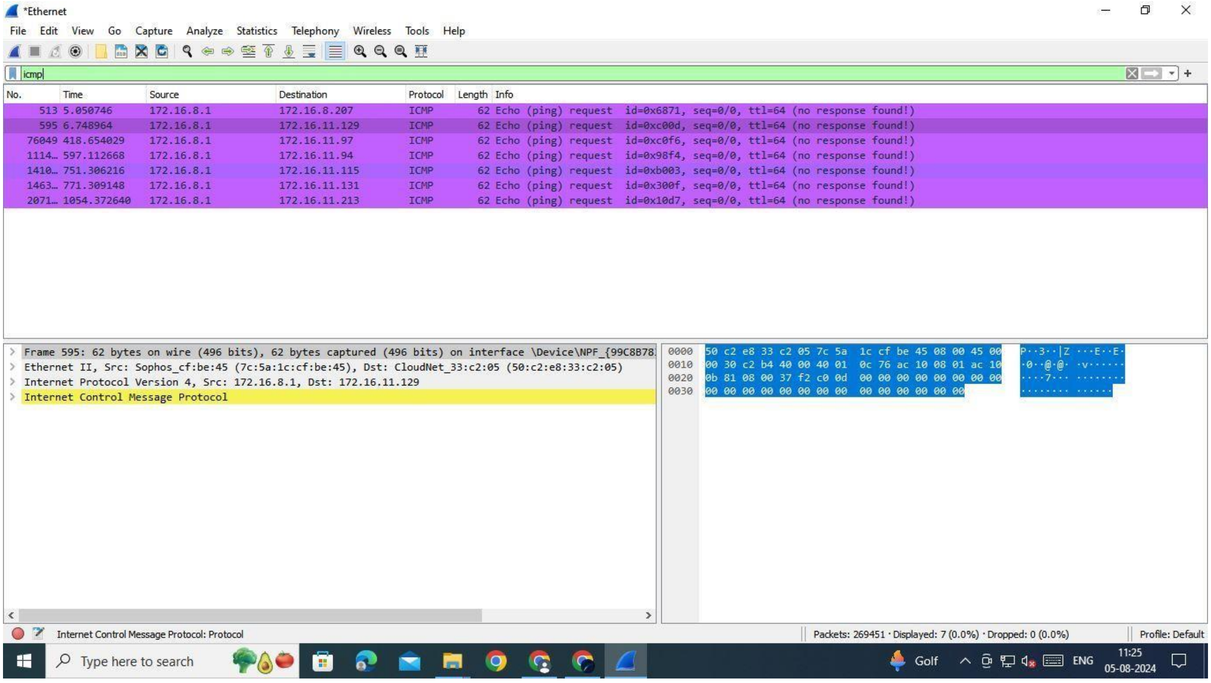
```
http

No.   Time        Source                  Destination             Protocol  Length Info
11372 62.682097   172.16.8.43             172.16.8.91             HTTP/X…   935 HTTP/1.1 200
12005 67.279376   fe80::43be:e12e:558…    fe80::be21:753e:394…    HTTP/X…   807 POST /97e7e50e-3cd7-4a9a-94f1-0c6a597fae33/ HTTP/1.1
12008 67.281276   fe80::be21:753e:394…    fe80::43be:e12e:558…    HTTP/X…   985 HTTP/1.1 200
15345 76.179477   fe80::be21:753e:394…    fe80::8244:d6c4:6c1…    HTTP/X…   807 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
15351 76.181850   fe80::8244:d6c4:6c1…    fe80::be21:753e:394…    HTTP/X…   975 HTTP/1.1 200
15364 76.194073   172.16.8.91             172.16.8.43             HTTP/X…   787 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
15367 76.196550   172.16.8.43             172.16.8.91             HTTP/X…   935 HTTP/1.1 200
16239 87.651476   fe80::be21:753e:394…    fe80::8244:d6c4:6c1…    HTTP/X…   807 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
16242 87.652539   fe80::8244:d6c4:6c1…    fe80::be21:753e:394…    HTTP/X…   975 HTTP/1.1 200
16258 87.665288   172.16.8.91             172.16.8.43             HTTP/X…   787 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
16262 87.666677   172.16.8.43             172.16.8.91             HTTP/X…   935 HTTP/1.1 200
17279 96.525221   fe80::88b7:2261:e73…    fe80::be21:753e:394…    HTTP/X…   807 POST /97e7e50e-3cd7-4a9a-94f1-0c6a597fae33/ HTTP/1.1
17282 96.526768   fe80::be21:753e:394…    fe80::88b7:2261:e73…    HTTP/X…   985 HTTP/1.1 200
22046 117.170110  fe80::be21:753e:394…    fe80::8244:d6c4:6c1…    HTTP/X…   807 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
22049 117.171362  fe80::8244:d6c4:6c1…    fe80::be21:753e:394…    HTTP/X…   975 HTTP/1.1 200
22065 117.182801  172.16.8.91             172.16.8.43             HTTP/X…   787 POST /844807e9-60ce-47d3-aea7-d13a6718978a/ HTTP/1.1
```

```
> Frame 22441: 520 bytes on wire (4160 bits), 520 bytes captured (4160 bits) on interface \Device\NPF_{9!
> Ethernet II, Src: Dell_34:d8:90 (50:9a:4c:34:d8:90), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.8.91, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 51648, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
> Hypertext Transfer Protocol
```

```
0000  7c 5a 1c cf be 45 50 9a  4c 34 d8 90 08 00 45 00   |Z···EP· L4····E·
0010  01 fa 99 a8 40 00 80 06  65 07 ac 10 08 5b 22 68   ····@··· e····["h
0020  23 7b c9 c0 00 50 86 ba  ba fe ae 91 d4 26 50 18   #{···P·· ·····&P·
0030  20 14 5a 9a 00 00 47 45  54 20 2f 65 64 67 65 64    ·Z···GE T /edged
0040  6c 2f 64 69 66 66 67 65  6e 2d 70 75 66 66 69 6e   l/diffge n-puffin
0050  2f 6a 66 6c 68 63 68 63  63 6d 70 70 6b 66 65 62   /jflhchc cmppkfeb
0060  6b 69 61 6d 69 6e 61 67  65 65 68 6d 63 68 69 6b   kiaminag eehmchik
0070  6d 2f 31 2e 37 38 34 33  38 30 63 66 32 35 63 61   m/1.7843 80cf25ca
0080  35 62 63 65 61 32 30 66  38 65 38 36 34 36 62 65   5bcea20f 8e8646be
0090  63 37 35 30 33 61 33 63  38 37 36 30 65 39 36 63   c7503a3c 8760e96c
00a0  37 35 62 35 35 62 35 33  37 63 36 62 66 62 62 33   75b55b53 7c6bfbb3
00b0  39 61 65 66 2f 31 2e 39  36 32 65 35 61 35 65 65   9aef/1.9 62e5a5ee
00c0  38 62 62 31 61 39 64 66  63 39 32 63 35 33 33 39   8bb1a9df c92c5339
00d0  63 34 37 66 64 36 31 32  34 61 33 66 31 61 61 65   c47fd612 4a3f1aae
00e0  32 64 32 64 37 35 64 38  38 62 64 35 35 63 32 35   2d2d75d8 8bd55c25
00f0  33 30 38 62 63 35 34 2f  64 31 32 36 62 30 65 36   308bc54/ d126b0e6
0100  64 64 63 36 61 34 63 37  65 30 31 31 30 35 36 63   ddc6a4c7 e011056c
0110  32 65 31 62 30 37 66 63  63 32 65 38 63 34 34 30   2e1b07fc c2e8c440
0120  39 63 30 36 63 36 36 38  30 32 36 38 61 31 65 39   9c06c668 0268a1e9
0130  65 31 34 62 64 62 38 38  20 48 54 54 50 2f 31 2e   e14bdb88  HTTP/1.
0140  31 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   1··Conne ction: K
```

```
Hypertext Transfer Protocol: Protocol        Packets: 251145 · Displayed: 223 (0.1%)        Profile: Default
```

DISPLAYING ICMP PACKETS:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
Golf
ENG
11:25
05-08-2024

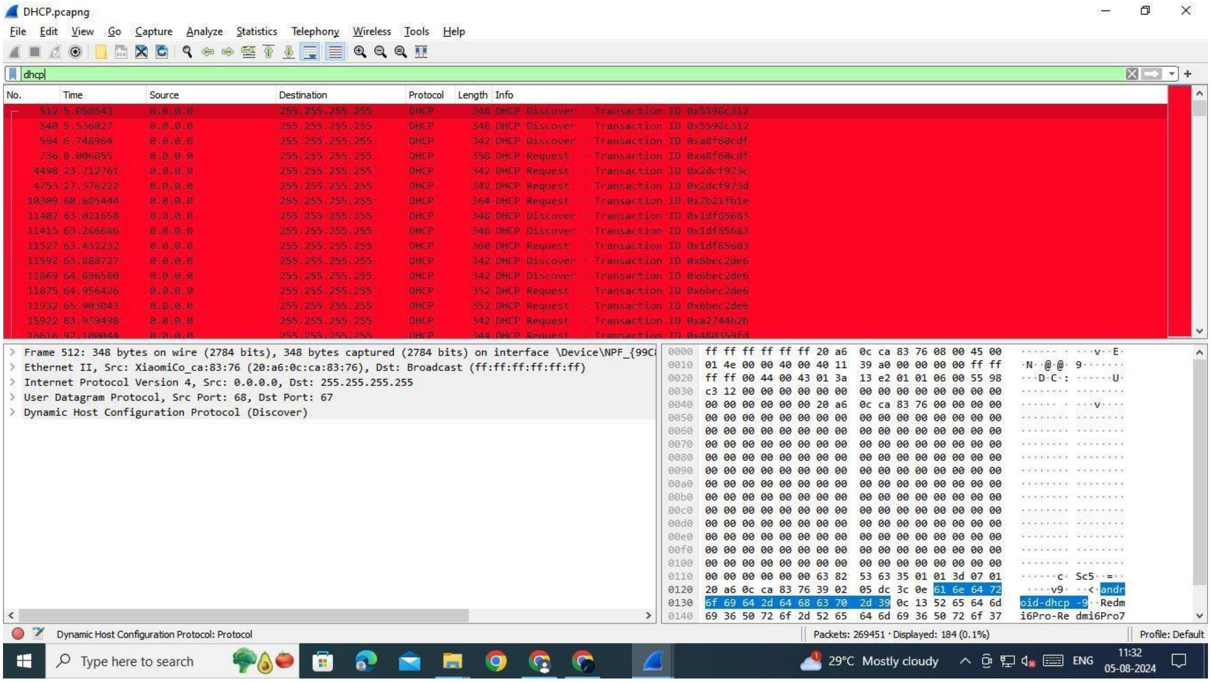
```
icmp

No.   Time         Source       Destination    Protocol  Length Info
  513 5.050746     172.16.8.1   172.16.8.207   ICMP      62 Echo (ping) request  id=0x6871, seq=0/0, ttl=64 (no response found!)
  595 6.748964     172.16.8.1   172.16.11.129  ICMP      62 Echo (ping) request  id=0xc00d, seq=0/0, ttl=64 (no response found!)
76049 418.654029   172.16.8.1   172.16.11.97   ICMP      62 Echo (ping) request  id=0xc0f6, seq=0/0, ttl=64 (no response found!)
1114… 597.112668   172.16.8.1   172.16.11.94   ICMP      62 Echo (ping) request  id=0x98f4, seq=0/0, ttl=64 (no response found!)
1410… 751.306216   172.16.8.1   172.16.11.115  ICMP      62 Echo (ping) request  id=0xb003, seq=0/0, ttl=64 (no response found!)
1463… 771.309148   172.16.8.1   172.16.11.131  ICMP      62 Echo (ping) request  id=0x300f, seq=0/0, ttl=64 (no response found!)
2071… 1054.372640  172.16.8.1   172.16.11.213  ICMP      62 Echo (ping) request  id=0x10d7, seq=0/0, ttl=64 (no response found!)
```

```
> Frame 595: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{99C8B78
> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: CloudNet_33:c2:05 (50:c2:e8:33:c2:05)
> Internet Protocol Version 4, Src: 172.16.8.1, Dst: 172.16.11.129
> Internet Control Message Protocol
```

```
0000  50 c2 e8 33 c2 05 7c 5a  1c cf be 45 08 00 45 00   P··3··|Z ···E··E·
0010  00 30 c2 b4 40 00 40 01  0c 76 ac 10 08 01 ac 10   ·0··@·@· ·v······
0020  0b 81 08 00 37 f2 c0 0d  00 00 00 00 00 00 00 00   ····7··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00         ········ ······
```

```
Internet Control Message Protocol: Protocol        Packets: 269451 · Displayed: 7 (0.0%) · Dropped: 0 (0.0%)        Profile: Default
```

DISPLAYING DHCP PACKETS:



dhcp

No.	Time	Source	Destination	Protocol	Length	Info
512	5.050543	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x5598c312
540	5.536027	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x5598c312
594	6.748964	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa8f60cdf
736	8.006855	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0xa8f60cdf
4498	23.712761	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2dcf973c
4753	27.378222	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2dcf973d
10309	60.685444	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7b21fb1e
11402	63.021658	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x1df85683
11415	63.266686	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x1df85683
11527	63.432232	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x1df85683
11592	63.888727	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6bec2de6
11869	64.896580	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6bec2de6
11875	64.956426	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6bec2de6
11932	65.903043	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6bec2de6
15922	83.939498	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xa2744b2b
16616	92.100044	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0x480359fd

```
> Frame 512: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{99C
> Ethernet II, Src: XiaomiCo_ca:83:76 (20:a6:0c:ca:83:76), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000  ff ff ff ff ff ff 20 a6  0c ca 83 76 08 00 45 00   ······ · ···v··E·
0010  01 4e 00 00 40 00 40 11  39 a0 00 00 00 00 ff ff   ·N··@·@· 9·······
0020  ff ff 00 44 00 43 01 3a  13 e2 01 01 06 00 55 98   ···D·C·: ······U·
0030  c3 12 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 20 a6  0c ca 83 76 00 00 00 00   ······ · ···v····
0050  00 00 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 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 3d 07 01   ······c· Sc5··=··
0120  20 a6 0c ca 83 76 39 02  05 dc 3c 0e 61 6e 64 72    ····v9· ··<·andr
0130  6f 69 64 2d 64 68 63 70  2d 39 0c 13 52 65 64 6d   oid-dhcp -9··Redm
0140  69 36 50 72 6f 2d 52 65  64 6d 69 36 50 72 6f 37   i6Pro-Re dmi6Pro7
```

Dynamic Host Configuration Protocol: Protocol

Packets: 269451 · Displayed: 184 (0.1%)

Profile: Default