Network-traffic-capture-and-analysis-with-Wireshark

AIM:

To capture and analyze network traffic using Wireshark in order to observe protocols, packets, and potential anomalies.

DESIGN STEPS:

Step 1:

Install Wireshark using the command:

Step 2:

Launch Wireshark and select the appropriate network interface for live traffic capture.

Step 3:

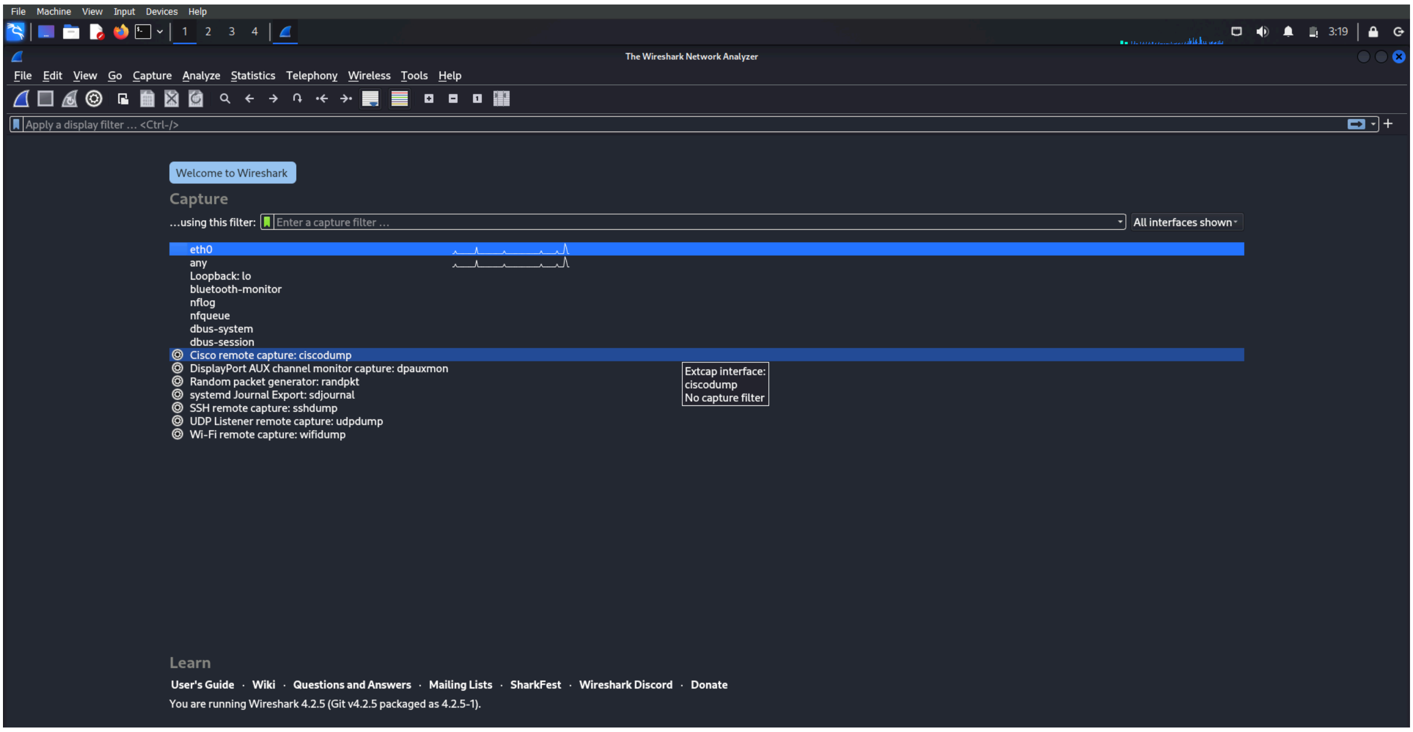
Start the capture, apply filters (like http, tcp, ip.addr == x.x.x.x) to analyze specific traffic, and stop the capture after observing relevant data.

PROGRAM:

Wireshark Packet Capture and Filter Usage

OUTPUT:

- Captured Packets with Protocol Analysis and Detailed Packet Info

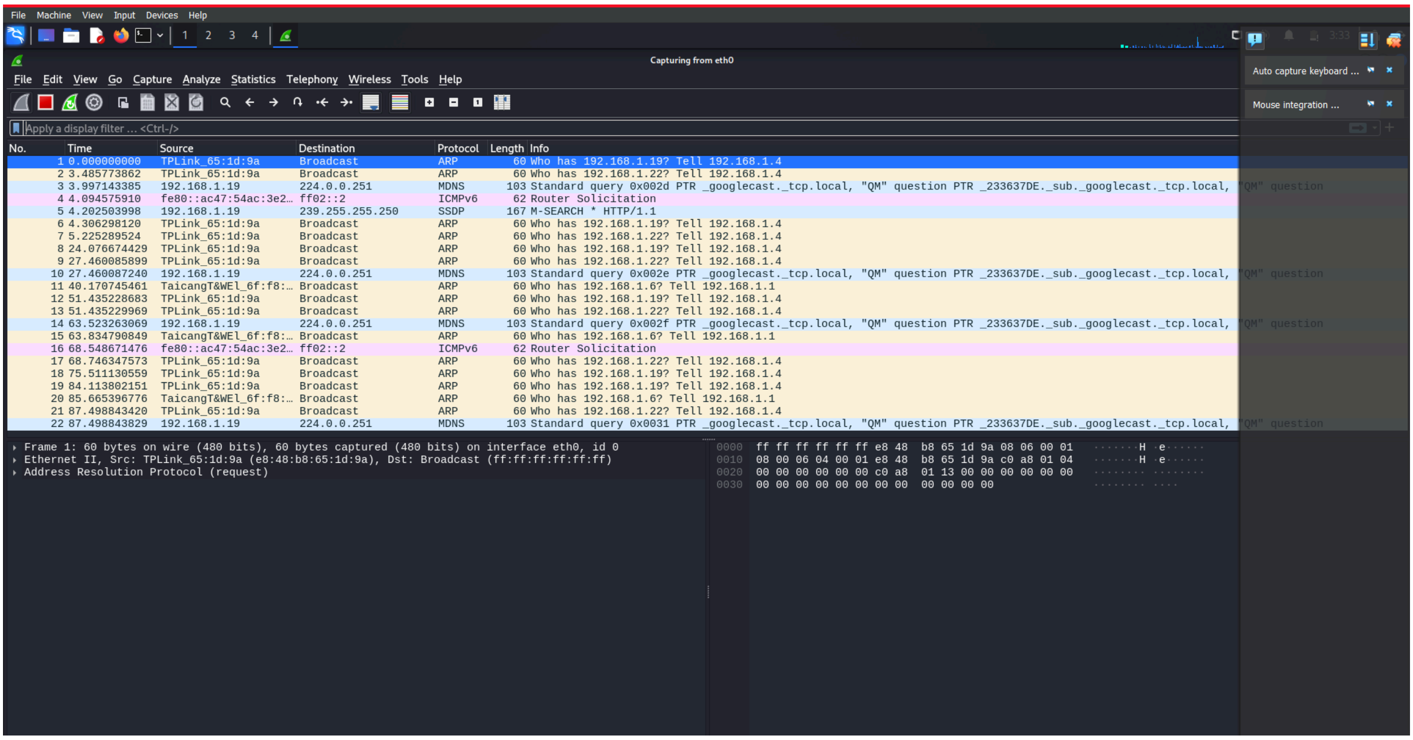

File Machine View Input Devices Help
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Extcap interface:
ciscodump
No capture filter
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.5 (Git v4.2.5 packaged as 4.2.5-1).

- **Start Capturing Packets**

• Click the blue shark fin icon or double-click the interface.

• Wireshark will start capturing all real-time traffic.


File Machine View Input Devices Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Auto capture keyboard …
Mouse integration …

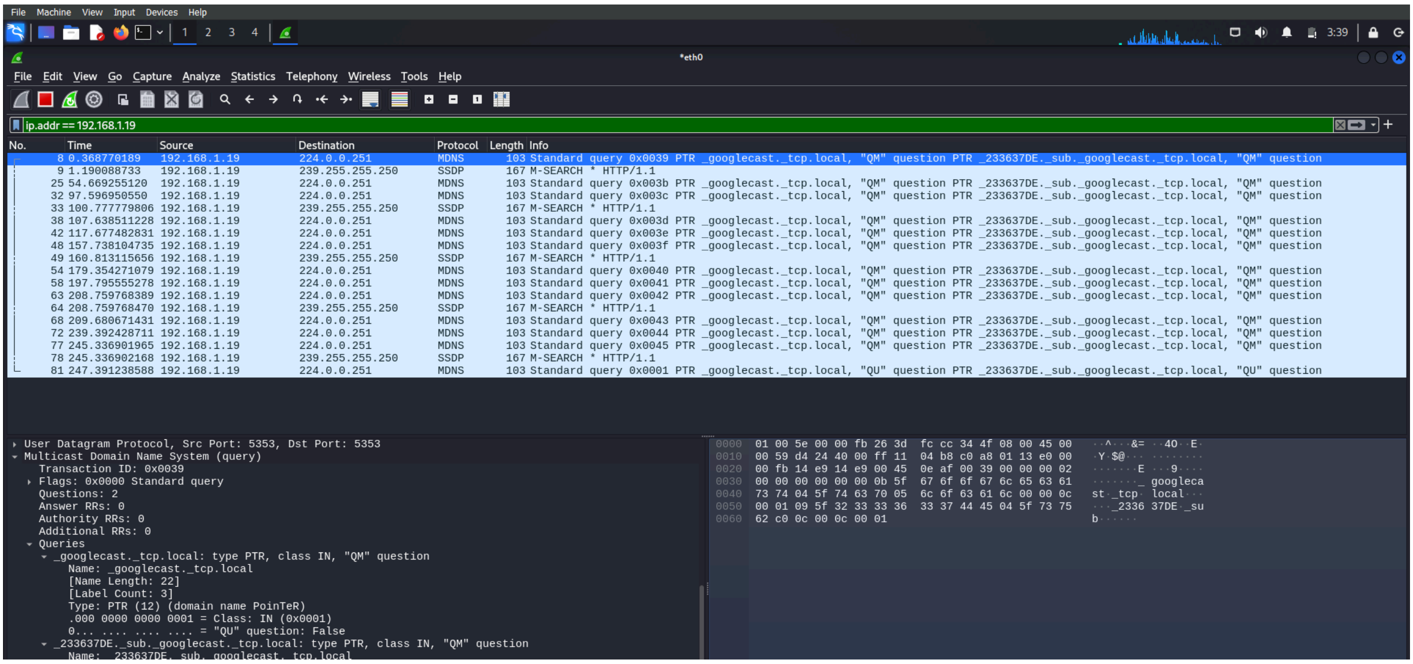
```
No.   Time          Source                Destination       Protocol Length Info
    1 0.000000000   TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
    2 3.485773862   TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
    3 3.997143385   192.168.1.19          224.0.0.251       MDNS      103 Standard query 0x002d PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
    4 4.094575910   fe80::ac47:54ac:3e2…  ff02::2           ICMPv6     62 Router Solicitation
    5 4.202503998   192.168.1.19          239.255.255.250   SSDP      167 M-SEARCH * HTTP/1.1
    6 4.306298120   TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
    7 5.225289524   TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
    8 24.076674429  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
    9 27.460085899  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
   10 27.460087240  192.168.1.19          224.0.0.251       MDNS      103 Standard query 0x002e PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
   11 40.170745461  TaicangT&WEl_6f:f8:…  Broadcast         ARP        60 Who has 192.168.1.6? Tell 192.168.1.1
   12 51.435228683  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
   13 51.435229969  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
   14 63.523263069  192.168.1.19          224.0.0.251       MDNS      103 Standard query 0x002f PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
   15 63.834790849  TaicangT&WEl_6f:f8:…  Broadcast         ARP        60 Who has 192.168.1.6? Tell 192.168.1.1
   16 68.548671476  fe80::ac47:54ac:3e2…  ff02::2           ICMPv6     62 Router Solicitation
   17 68.746347573  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
   18 75.511130559  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
   19 84.113802151  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.19? Tell 192.168.1.4
   20 85.665396776  TaicangT&WEl_6f:f8:…  Broadcast         ARP        60 Who has 192.168.1.6? Tell 192.168.1.1
   21 87.498843420  TPLink_65:1d:9a       Broadcast         ARP        60 Who has 192.168.1.22? Tell 192.168.1.4
   22 87.498843829  192.168.1.19          224.0.0.251       MDNS      103 Standard query 0x0031 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: TPLink_65:1d:9a (e8:48:b8:65:1d:9a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff e8 48  b8 65 1d 9a 08 06 00 01   ·······H ·e······
0010  08 00 06 04 00 01 e8 48  b8 65 1d 9a c0 a8 01 04   ·······H ·e······
0020  00 00 00 00 00 00 c0 a8  01 13 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

- **Apply Filters to Focus on Specific Traffic**

• Use filters like http, ip.addr == 192.168.1.1, or tcp.port == 80 in the top filter bar to narrow down results.


File Machine View Input Devices Help
1 2 3 4
3:39
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

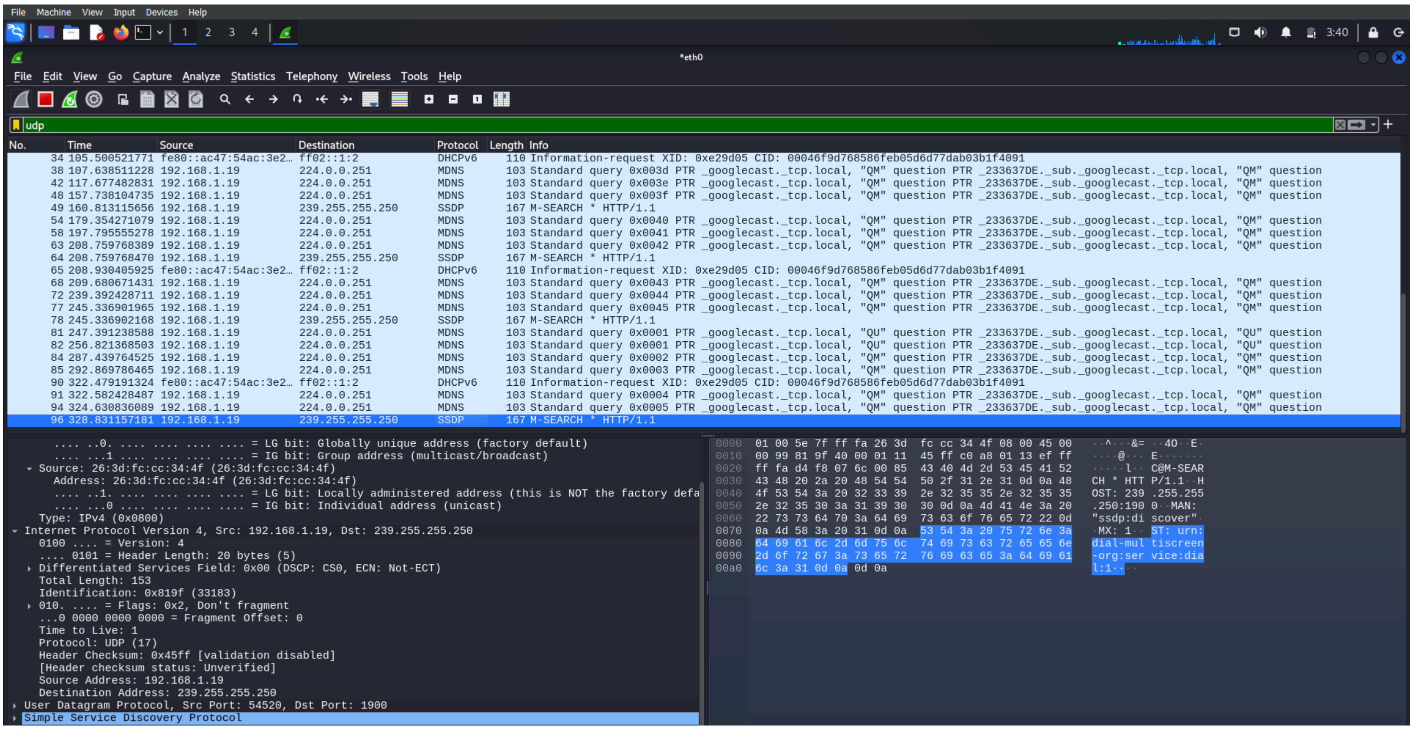
```
ip.addr == 192.168.1.19

No.  Time          Source        Destination      Protocol Length Info
   8 0.368770189   192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0039 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
   9 1.190088733   192.168.1.19  239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  25 54.669255120  192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x003b PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  32 97.596950550  192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x003c PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  33 100.777779806 192.168.1.19  239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  38 107.638511228 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x003d PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  42 117.677482831 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x003e PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  48 157.738104735 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x003f PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  49 160.813115656 192.168.1.19  239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  54 179.354271079 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0040 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  58 197.795555278 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0041 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  63 208.759768389 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0042 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  64 208.759768470 192.168.1.19  239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  68 209.680671431 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0043 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  72 239.392428711 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0044 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  77 245.336901965 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0045 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  78 245.336902168 192.168.1.19  239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  81 247.391238588 192.168.1.19  224.0.0.251      MDNS     103 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" question
```

```
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▾ Multicast Domain Name System (query)
    Transaction ID: 0x0039
  ▸ Flags: 0x0000 Standard query
    Questions: 2
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ _googlecast._tcp.local: type PTR, class IN, "QM" question
        Name: _googlecast._tcp.local
        [Name Length: 22]
        [Label Count: 3]
        Type: PTR (12) (domain name PoinTeR)
        .000 0000 0000 0001 = Class: IN (0x0001)
        0... .... .... .... = "QU" question: False
    ▾ _233637DE._sub._googlecast._tcp.local: type PTR, class IN, "QM" question
        Name: _233637DE._sub._googlecast._tcp.local
```

```
0000  01 00 5e 00 00 fb 26 3d  fc cc 34 4f 08 00 45 00   ··^···&= ··4O··E·
0010  00 59 d4 24 40 00 ff 11  04 b8 c0 a8 01 13 e0 00   ·Y·$@··· ········
0020  00 fb 14 e9 14 e9 00 45  0e af 00 39 00 00 00 02   ·······E ···9····
0030  00 00 00 00 00 00 0b 5f  67 6f 6f 67 6c 65 63 61   ·······_ googleca
0040  73 74 04 5f 74 63 70 05  6c 6f 63 61 6c 00 00 0c   st·_tcp· local···
0050  00 01 09 5f 32 33 33 36  33 37 44 45 04 5f 73 75   ···_2336 37DE·_su
0060  62 c0 0c 00 0c 00 01                               b······
```

- **Analyze Packet Details**

• Click on a packet to view its detailed breakdown including frame, Ethernet,IP, TCP/UDP layers, and data payload.


File Machine View Input Devices Help
1 2 3 4
3:40
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp

No.  Time          Source              Destination      Protocol Length Info
  34 105.500521771 fe80::ac47:54ac:3e2… ff02::1:2       DHCPv6   110 Information-request XID: 0xe29d05 CID: 00046f9d768586feb05d6d77dab03b1f4091
  38 107.638511228 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x003d PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  42 117.677482831 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x003e PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  48 157.738104735 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x003f PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  49 160.813115656 192.168.1.19        239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  54 179.354271079 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0040 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  58 197.795555278 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0041 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  63 208.759768389 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0042 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  64 208.759768470 192.168.1.19        239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  65 208.930405925 fe80::ac47:54ac:3e2… ff02::1:2       DHCPv6   110 Information-request XID: 0xe29d05 CID: 00046f9d768586feb05d6d77dab03b1f4091
  68 209.680671431 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0043 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  72 239.392428711 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0044 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  77 245.336901965 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0045 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  78 245.336902168 192.168.1.19        239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
  81 247.391238588 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" question
  82 256.821368503 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" question
  84 287.439764525 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  85 292.869786465 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  90 322.479191324 fe80::ac47:54ac:3e2… ff02::1:2       DHCPv6   110 Information-request XID: 0xe29d05 CID: 00046f9d768586feb05d6d77dab03b1f4091
  91 322.582428487 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0004 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  94 324.630836089 192.168.1.19        224.0.0.251      MDNS     103 Standard query 0x0005 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local, "QM" question
  96 328.831157181 192.168.1.19        239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
```

```
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: 26:3d:fc:cc:34:4f (26:3d:fc:cc:34:4f)
      Address: 26:3d:fc:cc:34:4f (26:3d:fc:cc:34:4f)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory defa
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.1.19, Dst: 239.255.255.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 153
    Identification: 0x819f (33183)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x45ff [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.19
    Destination Address: 239.255.255.250
▸ User Datagram Protocol, Src Port: 54520, Dst Port: 1900
▸ Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 26 3d  fc cc 34 4f 08 00 45 00   ··^···&= ··4O··E·
0010  00 99 81 9f 40 00 01 11  45 ff c0 a8 01 13 ef ff   ····@··· E·······
0020  ff fa d4 f8 07 6c 00 85  43 40 4d 2d 53 45 41 52   ·····l·· C@M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 0d 0a                               l:1····
```

RESULT:

Network traffic was successfully captured and analyzed using Wireshark.