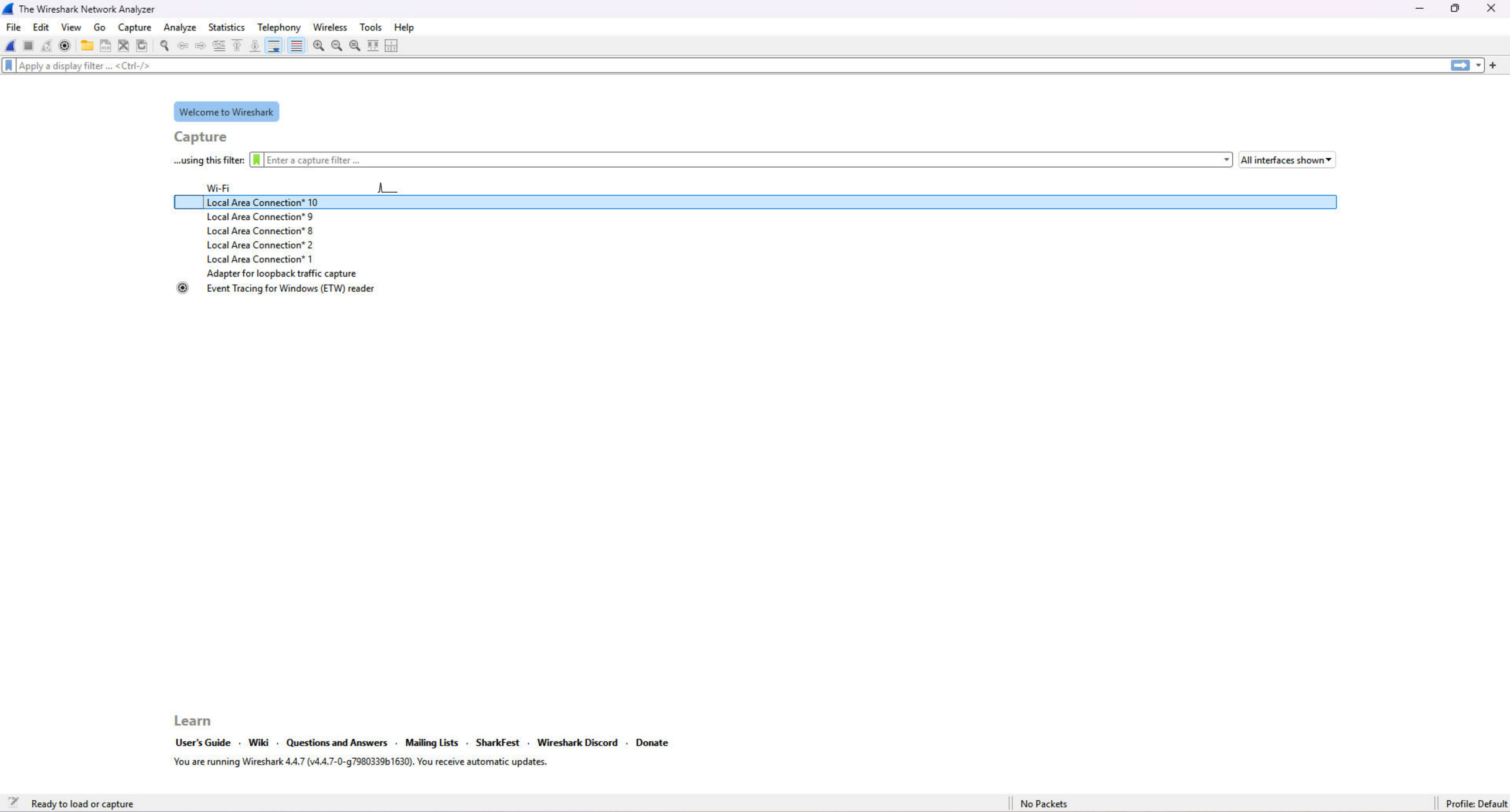
Wireshark is a widely used network protocol analyzer that allows individuals to see and capture data packets as they flow over the network. It is an open-source tool used by network admins, cybersecurity professionals, and teachers for discovering and repairing network problems. The software gives you a lot of information on network traffic, which is important for figuring out what went wrong and how different protocols work (Sanders, 2017).

People use Wireshark for lots of things, like figuring out why a thing isn't working so well, discovering unauthorized activity, or figuring out how networks talk to each other. Wireshark is a useful cybersecurity tool as it might identify suspicious traffic and malware communications. It helps pupils see how network protocols work in real life in schools (Orebaugh et al., 2007). Its ability to record and filter data in real time makes it a powerful and useful tool for anyone who works with network data.

References:

Sanders, C. (2017). *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* (3rd ed.). No Starch Press. https://nostarch.com/packetanalysis3

Orebaugh, A., Ramirez, G., & Beale, J. (2007). *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress. https://www.amazon.com/Wireshark-Ethereal-Protocol-Analyzer-Security/dp/1597490733


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
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.7 (v4.4.7-0-g7980339b1630). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

Announcements

This area will be used by the ins

Search forums

Separate groups: Group 0003

Discussion

- Important Announcement
- Welcome to week 1
- Welcome to CS 4404 - Adv AY2025-T5!

UoPeople Clock (GMT-5)

All activities close on Wednesdays at 11:55 PM, except for some activities which close on Thursdays at 11:55 PM. **Always follow the clock at the top of the page.**

Due dates/times *displayed* in activities will vary based on your time zone, however you are still required to follow the **11:55 PM GMT-5** deadline.

Capturing from Wi-Fi

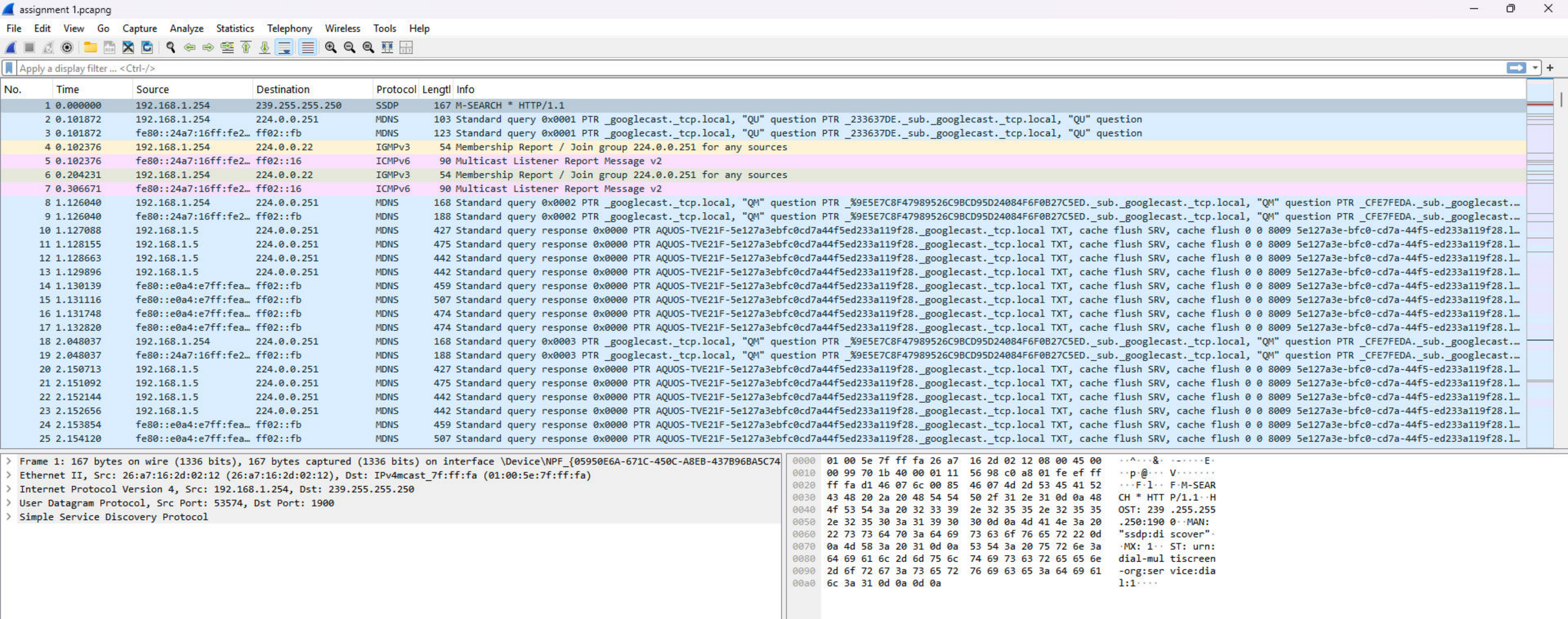
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengtl	Info
29757	131.132626	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=64295 Win=65280 Len=0
29758	131.133676	2.22.91.131	192.168.1.4	TCP	4434	443 → 50083 [PSH, ACK] Seq=64295 Ack=834 Win=64128 Le…
29759	131.133738	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=68675 Win=130816 Len=0
29760	131.134753	192.168.1.4	13.69.239.78	TCP	66	50084 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2…
29761	131.160329	38.106.231.208	192.168.1.4	TCP	60	443 → 50081 [ACK] Seq=164 Ack=4817 Win=39808 Len=0
29762	131.163456	2.22.91.131	192.168.1.4	TCP	2974	443 → 50083 [PSH, ACK] Seq=68675 Ack=834 Win=64128 Le…
29763	131.163529	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=71595 Win=130816 Len=0
29764	131.163592	2.22.91.131	192.168.1.4	TLSv1.3	4434	Application Data
29765	131.163612	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=75975 Win=130816 Len=0
29766	131.165892	2.22.91.131	192.168.1.4	TCP	2974	443 → 50083 [PSH, ACK] Seq=75975 Ack=834 Win=64128 Le…
29767	131.165892	38.106.231.208	192.168.1.4	TLSv1.2	388	Application Data
29768	131.166025	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=78895 Win=130816 Len=0
29769	131.166955	192.168.1.4	38.106.231.208	TCP	54	50081 → 443 [FIN, ACK] Seq=4817 Ack=498 Win=65024 Len…
29770	131.168962	2.22.91.131	192.168.1.4	TLSv1.3	2974	Application Data
29771	131.169028	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=81815 Win=130816 Len=0
29772	131.169082	2.22.91.131	192.168.1.4	TCP	4434	443 → 50083 [PSH, ACK] Seq=81815 Ack=834 Win=64128 Le…
29773	131.169106	192.168.1.4	2.22.91.131	TCP	54	50083 → 443 [ACK] Seq=834 Ack=86195 Win=130816 Len=0
29774	131.170136	2.22.91.131	192.168.1.4	TCP	4434	443 → 50083 [PSH, ACK] Seq=86195 Ack=834 Win=64128 Le…

```
> Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336
> Ethernet II, Src: 26:a7:16:2d:02:12 (26:a7:16:2d:02:12), Dst: IPv
> Internet Protocol Version 4, Src: 192.168.1.254, Dst: 239.255.255
> User Datagram Protocol, Src Port: 53574, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 26 a7  16 2d 02 12 08 00 45 00   ··^···&· ·-····E·
0010  00 99 70 1b 40 00 01 11  56 98 c0 a8 01 fe ef ff   ··p·@··· V·······
0020  ff fa d1 46 07 6c 00 85  46 07 4d 2d 53 45 41 52   ···F·l·· F·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····
```


assignment 1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengtl Info
1 0.000000 192.168.1.254 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
2 0.101872 192.168.1.254 224.0.0.251 MDNS 103 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" question
3 0.101872 fe80::24a7:16ff:fe2… ff02::fb MDNS 123 Standard query 0x0001 PTR _googlecast._tcp.local, "QU" question PTR _233637DE._sub._googlecast._tcp.local, "QU" question
4 0.102376 192.168.1.254 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.251 for any sources
5 0.102376 fe80::24a7:16ff:fe2… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
6 0.204231 192.168.1.254 224.0.0.22 IGMPv3 54 Membership Report / Join group 224.0.0.251 for any sources
7 0.306671 fe80::24a7:16ff:fe2… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
8 1.126040 192.168.1.254 224.0.0.251 MDNS 168 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub._googlecast.…
9 1.126040 fe80::24a7:16ff:fe2… ff02::fb MDNS 188 Standard query 0x0002 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub._googlecast.…
10 1.127088 192.168.1.5 224.0.0.251 MDNS 427 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
11 1.128155 192.168.1.5 224.0.0.251 MDNS 475 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
12 1.128663 192.168.1.5 224.0.0.251 MDNS 442 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
13 1.129896 192.168.1.5 224.0.0.251 MDNS 442 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
14 1.130139 fe80::e0a4:e7ff:fea… ff02::fb MDNS 459 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
15 1.131116 fe80::e0a4:e7ff:fea… ff02::fb MDNS 507 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
16 1.131748 fe80::e0a4:e7ff:fea… ff02::fb MDNS 474 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
17 1.132820 fe80::e0a4:e7ff:fea… ff02::fb MDNS 474 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
18 2.048037 192.168.1.254 224.0.0.251 MDNS 168 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub._googlecast.…
19 2.048037 fe80::24a7:16ff:fe2… ff02::fb MDNS 188 Standard query 0x0003 PTR _googlecast._tcp.local, "QM" question PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local, "QM" question PTR _CFE7FEDA._sub._googlecast.…
20 2.150713 192.168.1.5 224.0.0.251 MDNS 427 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
21 2.151092 192.168.1.5 224.0.0.251 MDNS 475 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
22 2.152144 192.168.1.5 224.0.0.251 MDNS 442 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
23 2.152656 192.168.1.5 224.0.0.251 MDNS 442 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
24 2.153854 fe80::e0a4:e7ff:fea… ff02::fb MDNS 459 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
25 2.154120 fe80::e0a4:e7ff:fea… ff02::fb MDNS 507 Standard query response 0x0000 PTR AQUOS-TVE21F-5e127a3ebfc0cd7a44f5ed233a119f28._googlecast._tcp.local TXT, cache flush SRV, cache flush 0 0 8009 5e127a3e-bfc0-cd7a-44f5-ed233a119f28.l…
Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF_{05950E6A-671C-450C-A8EB-437B96BA5C74
Ethernet II, Src: 26:a7:16:2d:02:12 (26:a7:16:2d:02:12), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 53574, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 26 a7 16 2d 02 12 08 00 45 00 ··^···&· ·-····E·
0010 00 99 70 1b 40 00 01 11 56 98 c0 a8 01 fe ef ff ··p·@··· V·····
0020 ff fa d1 46 07 6c 00 85 46 07 4d 2d 53 45 41 52 ···F·l·· F·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····