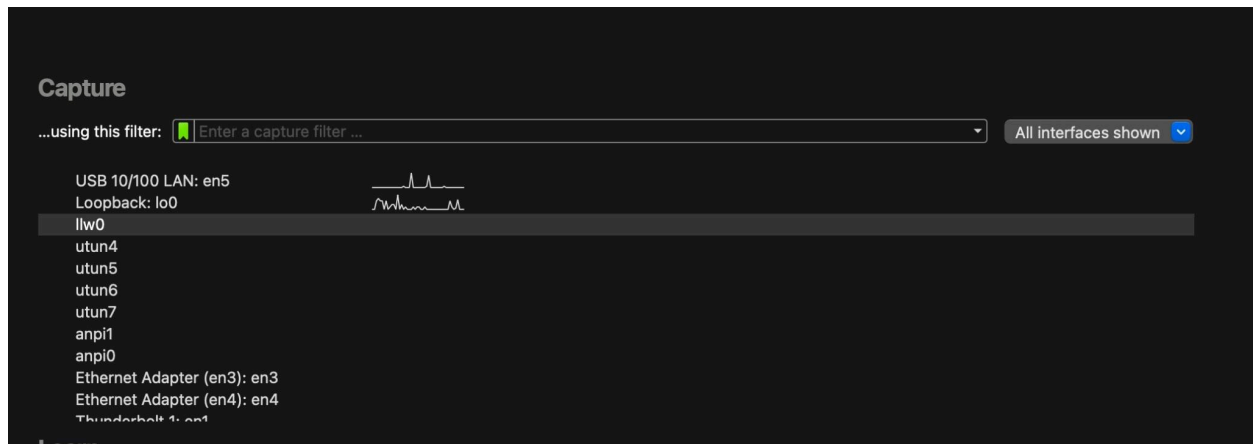
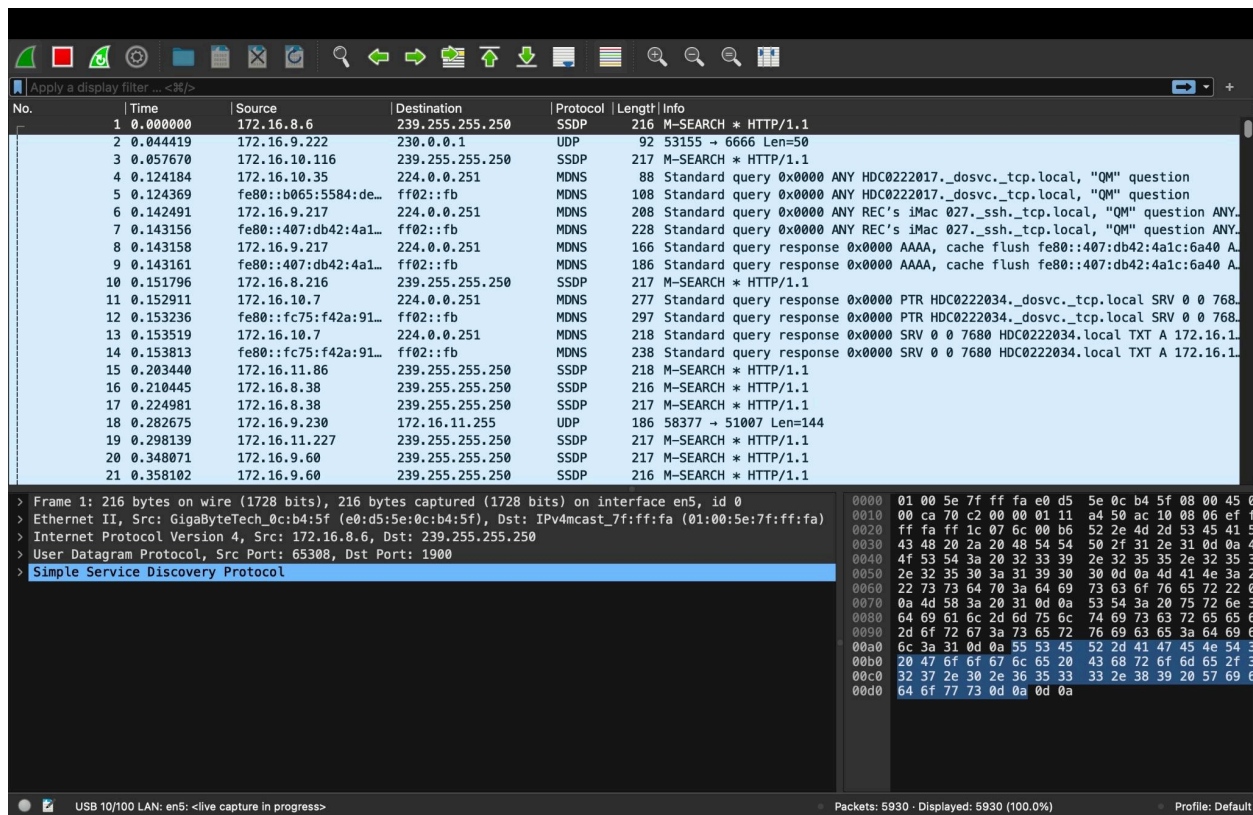


## A VIEW OF ALL NETWORKS



## VIEW OF ALL PACKETS INCOMING AND OUTGOING



## COLOR FILTERS AVAILABLE FOR NETWORKS

The image shows the Wireshark interface with the 'Wireshark - Coloring Rules Default' dialog box open. The dialog lists various network protocols and their corresponding color filters. The background shows a packet capture list with various protocols like ARP, ICMP, TCP, UDP, and SMB.

Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis...
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
SCPT ABORT	scpt.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 == 224.0.0.0/4 && ip.ttl < 5 && !(pim    ospf    eigrp    bgp    tcp.port==179))
IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf    bgp    tcp.port==179))    (ipv6.dst == ff00::/8 && ipv6.hlim < 5 && !(ospf    bgp    tcp.port==179))
Checksum Errors	eth.fcs.status=="Bad"    ip.checksum.status=="Bad"    tcp.checksum.status=="Bad"    udp.checksum.status=="Bad"
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.

Buttons: +, -, Copy from, Export..., Import..., Help, Cancel, OK

URL: [/Users/hhv/config/wireshark/colorfilters](#)

USB 10/100 LAN: en5: <live capture in progress> Packets: 1679 - Displayed: 1679 (100.0%) Profile: Default

## FILTERING THE PROTOCOL OF NETWORK

The image shows the Wireshark interface with a packet capture filtered by 'dns'. The packet list shows various DNS queries and responses. The packet details pane shows the structure of a DNS query packet.

No.	Time	Source	Destination	Protocol	Length	Info
460	3.323501	172.16.11.122	172.16.8.1	DNS	86	Standard query 0x3d86 A waa-pa.clients6.google.com
461	3.323786	172.16.8.1	172.16.11.122	DNS	86	Standard query response 0x4d3c HTTPS waa-pa.clients6.google.com
463	3.324051	172.16.8.1	172.16.11.122	DNS	102	Standard query response 0x3d86 A waa-pa.clients6.google.com A 142.250.196.16
4835	19.157631	172.16.11.122	172.16.8.1	DNS	78	Standard query 0xa53b HTTPS gateway.icloud.com
4836	19.157761	172.16.11.122	172.16.8.1	DNS	78	Standard query 0x604a A gateway.icloud.com
4837	19.158147	172.16.8.1	172.16.11.122	DNS	117	Standard query response 0xa53b HTTPS gateway.icloud.com CNAME gateway.fe2.a
4838	19.158149	172.16.8.1	172.16.11.122	DNS	165	Standard query response 0x604a A gateway.icloud.com CNAME gateway.fe2.apple
4839	19.158704	172.16.11.122	172.16.8.1	DNS	85	Standard query 0x1de7 HTTPS gateway.fe2.apple-dns.net
4840	19.158975	172.16.8.1	172.16.11.122	DNS	85	Standard query response 0x1de7 HTTPS gateway.fe2.apple-dns.net
16394	81.848013	172.16.11.122	172.16.8.1	DNS	80	Standard query 0x6f21 HTTPS weatherkit.apple.com
16395	81.848272	172.16.11.122	172.16.8.1	DNS	80	Standard query 0x6913 A weatherkit.apple.com
16396	81.848602	172.16.8.1	172.16.11.122	DNS	209	Standard query response 0x6f21 HTTPS weatherkit.apple.com CNAME weather-dat
16397	81.848792	172.16.8.1	172.16.11.122	DNS	353	Standard query response 0x6913 A weatherkit.apple.com CNAME weather-data.ap
16398	81.849454	172.16.11.122	172.16.8.1	DNS	84	Standard query 0x91bf HTTPS a2047.dscapi9.akamai.net
16399	81.849785	172.16.8.1	172.16.11.122	DNS	84	Standard query response 0x91bf HTTPS a2047.dscapi9.akamai.net
16770	86.993363	172.16.11.122	172.16.8.1	DNS	78	Standard query 0x6d5a HTTPS gateway.icloud.com
16771	86.993488	172.16.11.122	172.16.8.1	DNS	78	Standard query 0xd7e7 A gateway.icloud.com
16772	86.993789	172.16.8.1	172.16.11.122	DNS	117	Standard query response 0x6d5a HTTPS gateway.icloud.com CNAME gateway.fe2.a
16773	86.994015	172.16.8.1	172.16.11.122	DNS	165	Standard query response 0xd7e7 A gateway.icloud.com CNAME gateway.fe2.apple
16774	86.994492	172.16.11.122	172.16.8.1	DNS	85	Standard query 0xa584 HTTPS gateway.fe2.apple-dns.net
16776	86.994843	172.16.8.1	172.16.11.122	DNS	85	Standard query response 0xa584 HTTPS gateway.fe2.apple-dns.net

Frame 458: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface en5, id 0

Ethernet II, Src: RealtekSemic\_36:10:60 (00:e0:4c:36:10:60), Dst: Sophos\_cf:be:45 (7c:5a:1c:cf:be:45)

Internet Protocol Version 4, Src: 172.16.11.122, Dst: 172.16.8.1

User Datagram Protocol, Src Port: 61547, Dst Port: 53

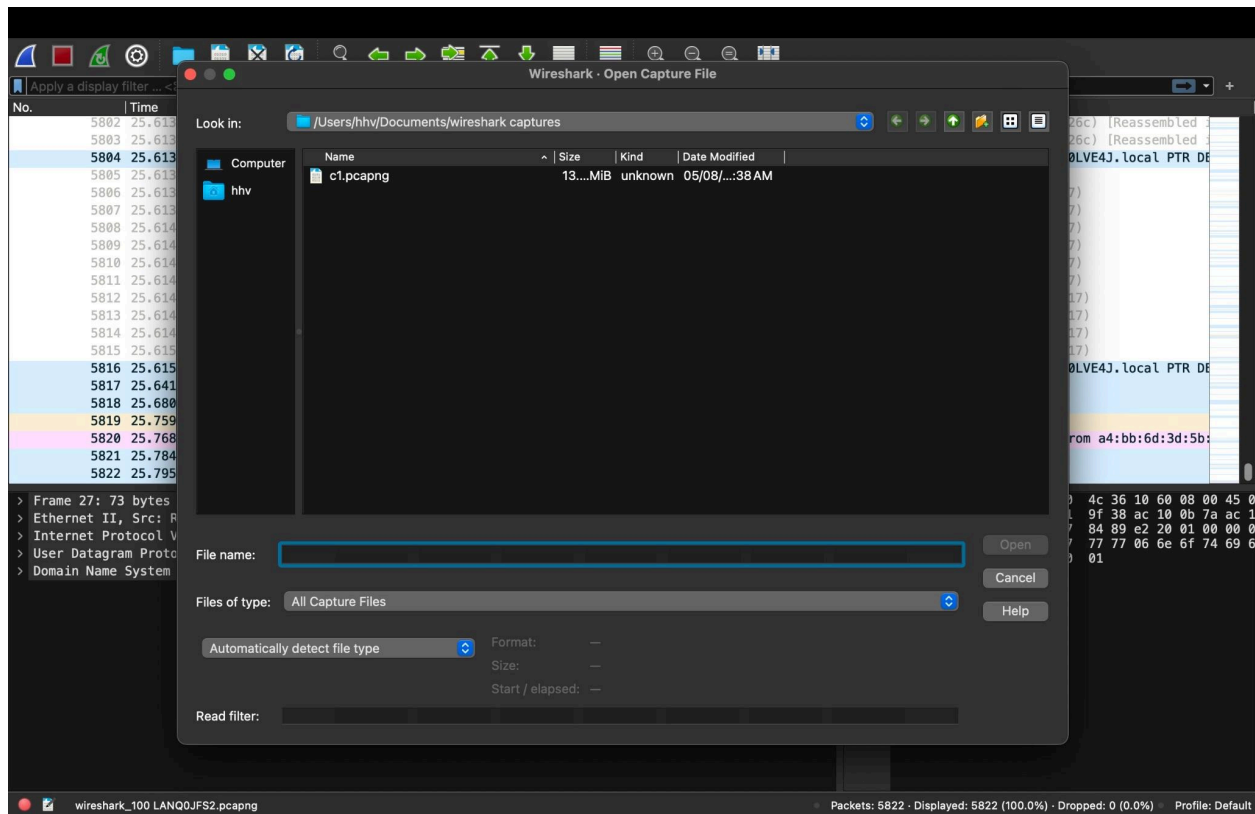
Domain Name System (query)

0000 7c 5a 1c cf be 45 00 e0 4c 36 10 60 08 00 45 00  
0010 00 48 7e 10 00 00 40 11 90 f9 ac 10 0b 7a ac 1  
0020 08 01 f0 6b 00 35 00 34 9d 46 4d 3c 01 00 00 0  
0030 00 00 00 00 00 00 06 77 61 61 2d 70 61 08 63 6  
0040 69 65 6e 74 73 36 06 67 6f 6f 67 6c 65 03 63 6  
0050 6d 00 00 41 00 01

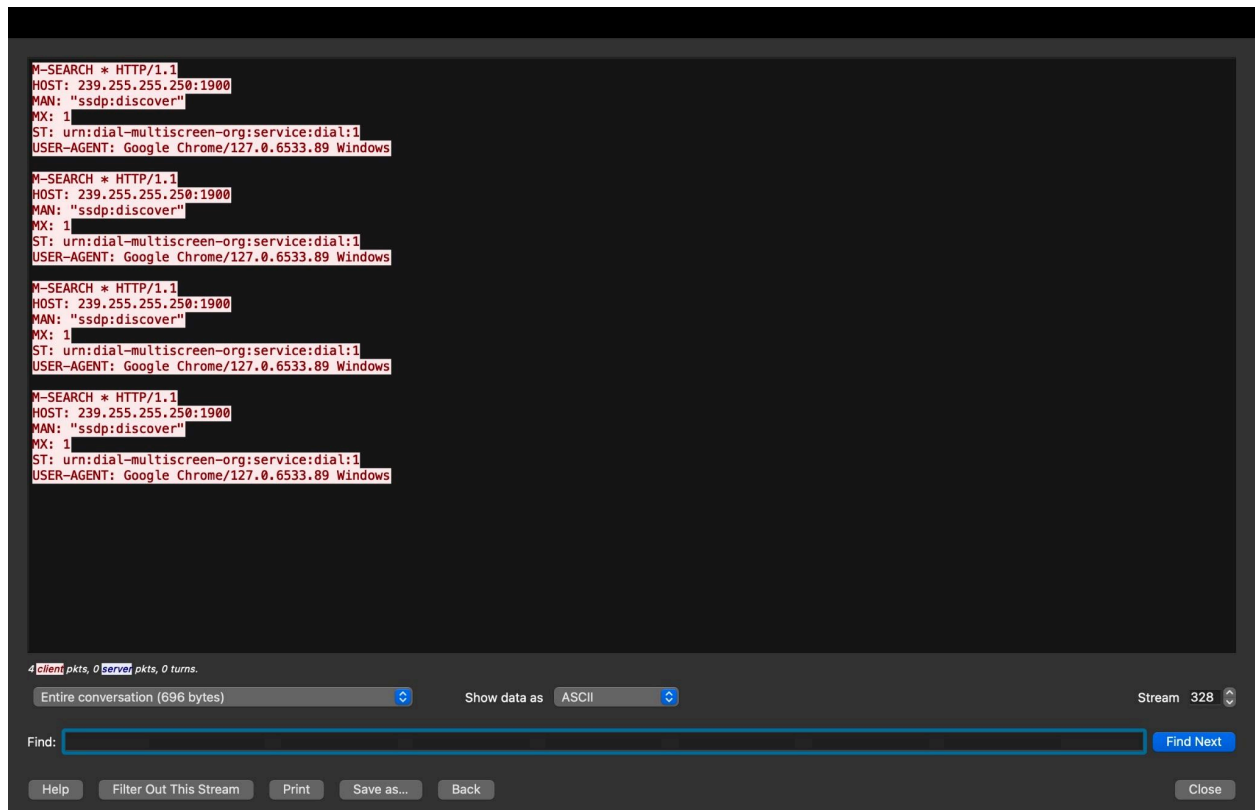
## DISPLAY FILTERS OF NETWORK



## SAVING A SAMPLE CAPTURE



## UDP FOLLOW UP





## THE FRAME INFORMATION OF A PACKET

Wireshark packet list and packet details view. The packet list shows 21 packets. The packet details view shows the frame information for packet 1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Pegatron_e0:87:9b	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.9.129
2	0.015348	HikvisionDig_aa:a0:4f	Broadcast	ARP	60	Who has 172.16.9.251? Tell 172.16.11.254
3	0.078980	fe80::280b:7dcd:dd...	ff02::1:2	DHCPv6	157	Solicit XID: 0xb6c67b CID: 0001000127e2333fd43d7ec7b51c
4	0.085034	Dell_37:fa:ce	Broadcast	ARP	60	Who has 172.16.9.184? Tell 172.16.8.90
5	0.117052	172.16.8.37	172.16.11.255	NBNS	92	Name query NB DESKTOP-1K98A14<1c>
6	0.150192	172.16.9.169	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
7	0.152800	172.16.11.137	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8	0.171656	172.16.9.45	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9	0.205574	172.16.9.38	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
10	0.206243	fe80::b89d:a9dc:57...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
11	0.216463	172.16.8.215	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	0.250519	172.16.8.177	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
13	0.264747	172.16.9.84	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
14	0.267524	Sophos_cf:be:45	Broadcast	ARP	60	Who has 172.16.10.238? Tell 172.16.8.1
15	0.282618	EliteGroupCo_14:72...	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.10.172
16	0.296294	172.16.11.135	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
17	0.301134	172.16.10.44	224.0.0.251	MDNS	217	Standard query response 0x0000 PTR HDC0222053._dosvc._tcp.local SRV 0 0
18	0.301136	fe80::b43d:a58b:dd...	ff02::fb	MDNS	237	Standard query response 0x0000 PTR HDC0222053._dosvc._tcp.local SRV 0 0
19	0.301493	172.16.10.44	224.0.0.251	MDNS	88	Standard query 0x0000 ANY HDC0222053._dosvc._tcp.local, "QM" question
20	0.301495	fe80::b43d:a58b:dd...	ff02::fb	MDNS	108	Standard query 0x0000 ANY HDC0222053._dosvc._tcp.local, "QM" question
21	0.311518	172.16.8.99	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en5, id 0

Section number: 1

Interface id: 0 (en5)

Encapsulation type: Ethernet (1)

Arrival Time: Aug 5, 2024 11:07:35.772462000 IST

UTC Arrival Time: Aug 5, 2024 05:37:35.772462000 UTC

Epoch Arrival Time: 1722836255.772462000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 60 bytes (480 bits)

Capture Length: 60 bytes (480 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:arp]

## FLOW GRAPH

Wireshark flow graph view showing the flow of traffic between various hosts. The graph displays the sequence of packets and their destinations.

Time	Source	Destination	Comment
0.000000	Pegatron_e0:87:9b	Broadcast	Who has 169.254.169.254? Tell 172.16.9...
0.015348	HikvisionDig_aa:a0:4f	Broadcast	Who has 172.16.9.251? Tell 172.16.11.254
0.078980	fe80::280b:7dcd:dde7:ae31	546	Solicit XID: 0xb6c67b CID: 00010001...
0.085034	Dell_37:fa:ce	Broadcast	Who has 172.16.9.184? Tell 172.16.8.90
0.117052	172.16.8.37	172.16.11.255	NBNS: Name query NB DESKTOP-1K98A14<1c>
0.150192	172.16.9.169	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.152800	172.16.11.137	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.171656	172.16.9.45	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.205574	172.16.9.38	224.0.0.251	MDNS: Standard query 0x0000 PTR _googleca...
0.206243	fe80::b89d:a9dc:57...	ff02::fb	MDNS: Standard query 0x0000 PTR _googleca...
0.216463	172.16.8.215	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.250519	172.16.8.177	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.264747	172.16.9.84	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.267524	Sophos_cf:be:45	Broadcast	ARP: Who has 172.16.10.238? Tell 172.16.8.1
0.282618	EliteGroupCo_14:72...	Broadcast	ARP: Who has 169.254.169.254? Tell 172.16.10...
0.296294	172.16.11.135	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.301134	172.16.10.44	224.0.0.251	MDNS: Standard query response 0x0000 PTR ...
0.301136	fe80::b43d:a58b:dd...	ff02::fb	MDNS: Standard query response 0x0000 PTR ...
0.301493	172.16.10.44	224.0.0.251	MDNS: Standard query 0x0000 ANY HDC0222...
0.301495	fe80::b43d:a58b:dd...	ff02::fb	MDNS: Standard query 0x0000 ANY HDC0222...
0.311518	172.16.8.99	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.312894	172.16.9.169	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.342545	172.16.11.137	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.347278	172.16.9.45	239.255.255.250	SSDP: M-SEARCH * HTTP/1.1
0.357039	172.16.8.99	239.255.255.250	ARP: Who has 172.16.1.164? Tell 172.16.8.44

Packet 16: SSDP: M-SEARCH \* HTTP/1.1

Limit to display filter

Flow type: All Flows

Addresses: Any

Help Reset Diagram Export Close