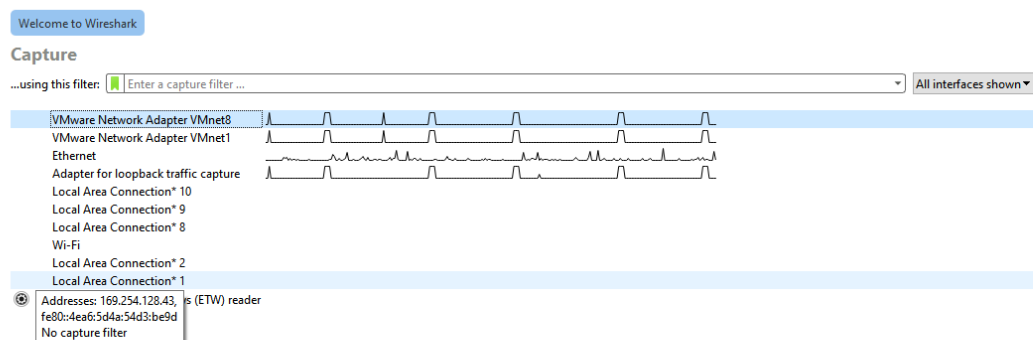


CAPTURING PACKETS OVER NETWORKS



PACKETS IN REAL TIME

97	394.442995	192.168.38.1	224.0.0.251	NBNS	81 Standard query 0x0000 AAAA TLPR3HDC0013074.local, "QI" question
98	394.443157	fe80::ef90:8862:4a1...ff02::1b		NBNS	101 Standard query 0x0000 AAAA TLPR3HDC0013074.local, "QI" question
99	394.918150	192.168.38.1	192.168.38.255	NBNS	92 Name query NB DESKTOP-8G77M1D<1c>
100	395.682301	192.168.38.1	192.168.38.255	NBNS	92 Name query NB DESKTOP-8G77M1D<1c>
101	395.853309	fe80::ef90:8862:4a1...ff02::1c		SSDP	189 M-SEARCH * HTTP/1.1
102	395.853699	192.168.38.1	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
103	413.715044	192.168.38.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
104	414.724746	192.168.38.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
105	415.691105	192.168.38.1	192.168.38.255	BROWSER	216 Get Backup List Request
106	415.691306	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
107	415.737083	192.168.38.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
108	416.452371	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
109	416.751256	192.168.38.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
110	417.204672	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
111	418.969177	192.168.38.1	192.168.38.255	BROWSER	216 Get Backup List Request
112	418.969264	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
113	419.733865	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
114	420.497047	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>

114	420.497047	192.168.38.1	192.168.38.255	NBNS	92 Name query NB WORKGROUP<1b>
-----	------------	--------------	----------------	------	--------------------------------

> Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF{...}

> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

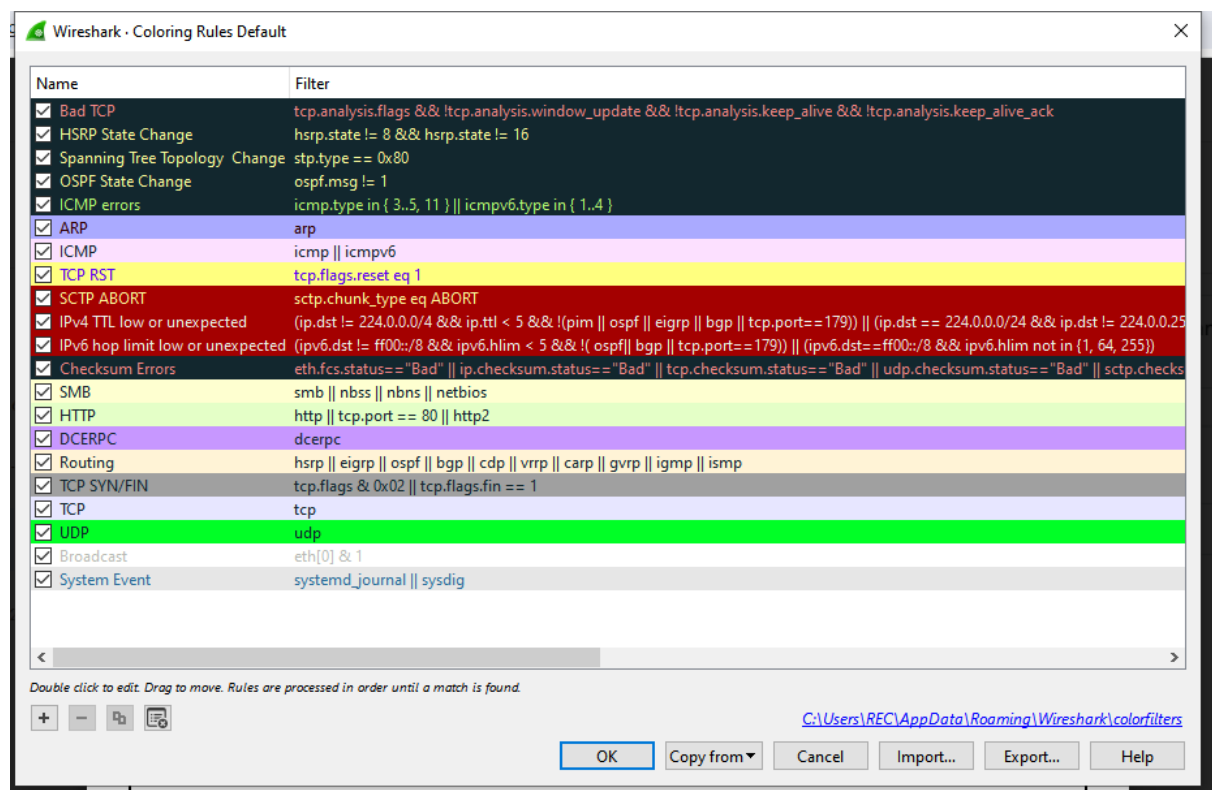
> Internet Protocol Version 4, Src: 192.168.38.1, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 61711, Dst Port: 1900

> Simple Service Discovery Protocol

0000	01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00	..^...P V.....E..
0010	00 ca 06 90 00 00 01 11 db ef c0 a8 26 01 ef ff	...&...
0020	ff fa f1 0f 07 6c 00 b6 2d a8 4d 2d 53 45 41 52l..-M-SEAR
0030	43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48	CH * HTTP/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:discover"
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-multicast
0090	2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61	-org:service:dia
00a0	6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a	l:1..USER-AGENT:
00b0	20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 31	Google Chrome/1
00c0	32 37 2e 30 2e 36 35 33 33 2e 38 39 20 57 69 6e	27.0.653 3.89 Win
00d0	64 6f 77 73 0d 0a 0d 0a	dows...

COLOR CODING



APPLY AS FILTER

ws.col.info == "M-SEARCH * HTTP/1.1"						
No.	Time	Source	Destination	Protocol	Length	Info
10536	50.606402	172.16.11.123	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10543	50.688926	172.16.10.8	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10544	50.700405	172.16.8.211	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10548	50.778363	172.16.9.232	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10550	50.788938	172.16.10.172	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10551	50.802997	172.16.9.115	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
10553	50.822540	172.16.8.66	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10554	50.838048	172.16.8.75	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10560	50.937289	172.16.10.196	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10563	51.146115	172.16.9.176	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10564	51.148673	172.16.10.173	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10578	51.281598	172.16.10.151	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10580	51.343546	172.16.9.137	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10584	51.412580	172.16.8.218	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10586	51.413248	172.16.9.235	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10593	51.419185	172.16.9.75	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10594	51.419185	172.16.9.75	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1

FLOW GRAPH



DNS

No.	dns	Source	Destination	Protocol	Length	Info
4280	dnsserver	172.16.8.100	172.16.8.1	DNS	75	Standard query 0x4880 A play.google.com
4282	23.320640	172.16.8.100	172.16.8.1	DNS	75	Standard query 0x2a50 HTTPS play.google.com
4283	23.320760	172.16.8.1	172.16.8.100	DNS	91	Standard query response 0x4880 A play.google.com A 142.250.193.174
4284	23.320987	172.16.8.1	172.16.8.100	DNS	75	Standard query response 0x2a50 HTTPS play.google.com

DISPLAY DEFAULT 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}

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

OK Cancel Help

ARP

No.	Time	Source	Destination	Protocol	Length	Info
15	0.104296	0a:e0:af:ae:4f:4f	Broadcast	ARP	60	Who has 172.16.37.149? Tell 172.16.8.44
16	0.104296	0a:e0:af:ae:4f:4f	Broadcast	ARP	60	Who has 172.16.50.120? Tell 172.16.8.44
25	0.160479	Dell_69:7b:90	Broadcast	ARP	60	Who has 172.16.8.203? Tell 172.16.11.123
180	0.504127	Micro-St_c5:c8:a2	Broadcast	ARP	60	Who has 172.16.9.173? Tell 172.16.10.87
181	0.523477	EliteGro_14:8a:37	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.10.181
193	0.651796	Dell_69:7b:26	Broadcast	ARP	60	Who has 172.16.11.77? Tell 172.16.8.42
194	0.657009	HonHaiPr_82:7f:d5	Broadcast	ARP	60	Who has 172.16.11.23? Tell 172.16.10.216
195	0.657009	HonHaiPr_82:7f:d5	Broadcast	ARP	60	Who has 172.16.11.23? Tell 172.16.10.216
211	0.892133	0a:e0:af:ae:4f:4f	Broadcast	ARP	60	Who has 172.16.37.149? Tell 172.16.8.44
212	0.892133	0a:e0:af:ae:4f:4f	Broadcast	ARP	60	Who has 172.16.50.120? Tell 172.16.8.44
213	0.982446	Giga-Byt_0c:b4:5f	Broadcast	ARP	60	Who has 172.16.11.16? Tell 172.16.8.6
220	1.054625	Hangzhou_aa:a0:4f	Broadcast	ARP	60	Who has 172.16.9.250? Tell 172.16.11.254
225	1.151692	Dell_69:7b:90	Broadcast	ARP	60	Who has 172.16.8.203? Tell 172.16.11.123
226	1.191829	Micro-St_c8:87:c3	Broadcast	ARP	60	Who has 172.16.11.42? Tell 172.16.9.74
227	1.204630	HonHaiPr_82:7f:d5	Broadcast	ARP	60	Who has 172.16.11.23? Tell 172.16.10.216
233	1.333814	Realtek5_42:be:b9	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.9.51
234	1.342572	EliteGro_15:e8:6c	Broadcast	ARP	60	Who has 172.16.10.43? Tell 172.16.10.173
236	1.430225	Dell_69:7b:26	Broadcast	ARP	60	Who has 172.16.11.77? Tell 172.16.8.42

ICMP

No.	Time	Source	Destination	Protocol	Length	Info
13	0.107735	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
17	0.107735	34.104.35.123	172.16.8.100	HTTP	666	HTTP/1.1 200 OK
18	0.127009	172.16.10.211	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
19	0.127009	172.16.10.211	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	0.132718	172.16.9.67	172.16.11.255	NBNS	92	Name query NB SUDHARSAN<1>
21	0.136815	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
22	0.144358	34.104.35.123	172.16.8.100	HTTP	691	HTTP/1.1 416 Requested range not satisfiable
23	0.145218	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
24	0.155546	34.104.35.123	172.16.8.100	HTTP	705	HTTP/1.1 200 OK
26	0.183354	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
27	0.191327	34.104.35.123	172.16.8.100	HTTP	691	HTTP/1.1 416 Requested range not satisfiable
28	0.192901	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
29	0.195878	172.16.8.177	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
30	0.201636	172.16.9.15	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
31	0.213360	34.104.35.123	172.16.8.100	HTTP	705	HTTP/1.1 200 OK
32	0.247472	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
33	0.257469	34.104.35.123	172.16.8.100	HTTP	730	HTTP/1.1 416 Requested range not satisfiable
34	0.259363	172.16.9.129	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

HTTP

No.	Time	Source	Destination	Protocol	Length	Info
10	0.060740	34.104.35.123	172.16.8.100	HTTP	666	HTTP/1.1 200 OK
12	0.090136	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
13	0.090602	34.104.35.123	172.16.8.100	HTTP	691	HTTP/1.1 416 Requested range not satisfiable
14	0.099513	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
17	0.107735	34.104.35.123	172.16.8.100	HTTP	666	HTTP/1.1 200 OK
21	0.136815	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
22	0.144358	34.104.35.123	172.16.8.100	HTTP	691	HTTP/1.1 416 Requested range not satisfiable
23	0.145218	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
24	0.155546	34.104.35.123	172.16.8.100	HTTP	705	HTTP/1.1 200 OK
26	0.183354	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
27	0.191327	34.104.35.123	172.16.8.100	HTTP	691	HTTP/1.1 416 Requested range not satisfiable
28	0.192901	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
31	0.213360	34.104.35.123	172.16.8.100	HTTP	705	HTTP/1.1 200 OK
32	0.247472	172.16.8.100	34.104.35.123	HTTP	520	GET /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
33	0.257469	34.104.35.123	172.16.8.100	HTTP	730	HTTP/1.1 416 Requested range not satisfiable
35	0.260871	172.16.8.100	34.104.35.123	HTTP	500	HEAD /edgedl/diffgen-puffin/jflhchccmpkfebkiaminageehmchikm/1.784380cf25ca5bcea20f8e8646bec7503a3c8760e96c...
38	0.268156	34.104.35.123	172.16.8.100	HTTP	666	HTTP/1.1 200 OK
5403	36.470837	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	HTTP/XL	807	POST /4f44fb72-a560-4244-a7f6-9a21f42fcb7/ HTTP/1.1

TCP

No.	Time	Source	Destination	Protocol	Length	Info
5309	36.151731	172.16.8.49	172.16.8.208	TCP	66	62628 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5398	36.469325	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	86	51655 → 5357 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
5399	36.469500	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	TCP	86	5357 → 51655 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5401	36.470037	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	74	51655 → 5357 [ACK] Seq=1 Ack=1 Win=2108160 Len=0
5402	36.470037	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	314	51655 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=2108160 Len=240 [TCP segment of a reassembled PDU]
5403	36.470037	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	HTTP/XL	807	POST /4f44fb72-a560-4244-a7f6-9a21f42fcb7/ HTTP/1.1
5404	36.470183	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	TCP	74	5357 → 51655 [ACK] Seq=1 Ack=974 Win=2108160 Len=0
5406	36.473642	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	TCP	1514	5357 → 51655 [ACK] Seq=1 Ack=974 Win=2108160 Len=1440 [TCP segment of a reassembled PDU]
5407	36.473642	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	HTTP/XL	985	HTTP/1.1 200
5408	36.474135	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	74	51655 → 5357 [ACK] Seq=974 Ack=2352 Win=2108160 Len=0
5410	36.484537	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	74	51655 → 5357 [FIN, ACK] Seq=974 Ack=2352 Win=2108160 Len=0
5411	36.484706	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	TCP	74	5357 → 51655 [FIN, ACK] Seq=2352 Ack=975 Win=2108160 Len=0
5412	36.485149	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	74	51655 → 5357 [ACK] Seq=975 Ack=2353 Win=2108160 Len=0
6770	37.165987	172.16.8.49	172.16.8.208	TCP	66	[TCP Retransmission] 62628 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6956	39.182029	172.16.8.49	172.16.8.208	TCP	66	[TCP Retransmission] 62628 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7133	41.604733	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	86	51800 → 5357 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
7134	41.604829	fe80::43be:e12e:558...	fe80::c623:6ce2:33a...	TCP	86	5357 → 51800 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
7135	41.605189	fe80::c623:6ce2:33a...	fe80::43be:e12e:558...	TCP	74	51800 → 5357 [ACK] Seq=1 Ack=1 Win=263424 Len=0