INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

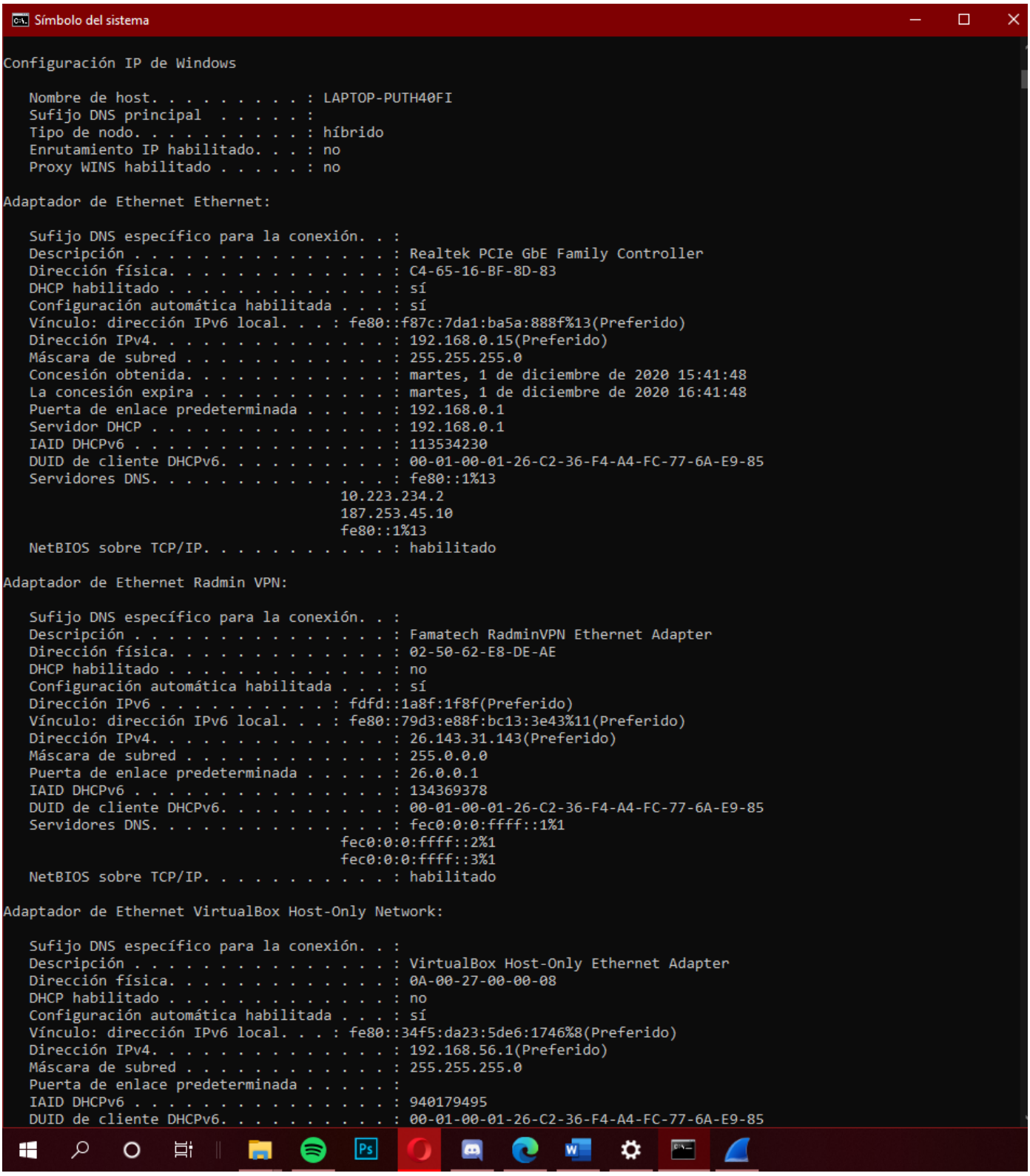
N.º De Actividad: Laboratorio 12

Nombre Del Alumno: Vazquez Canto Andres Omar

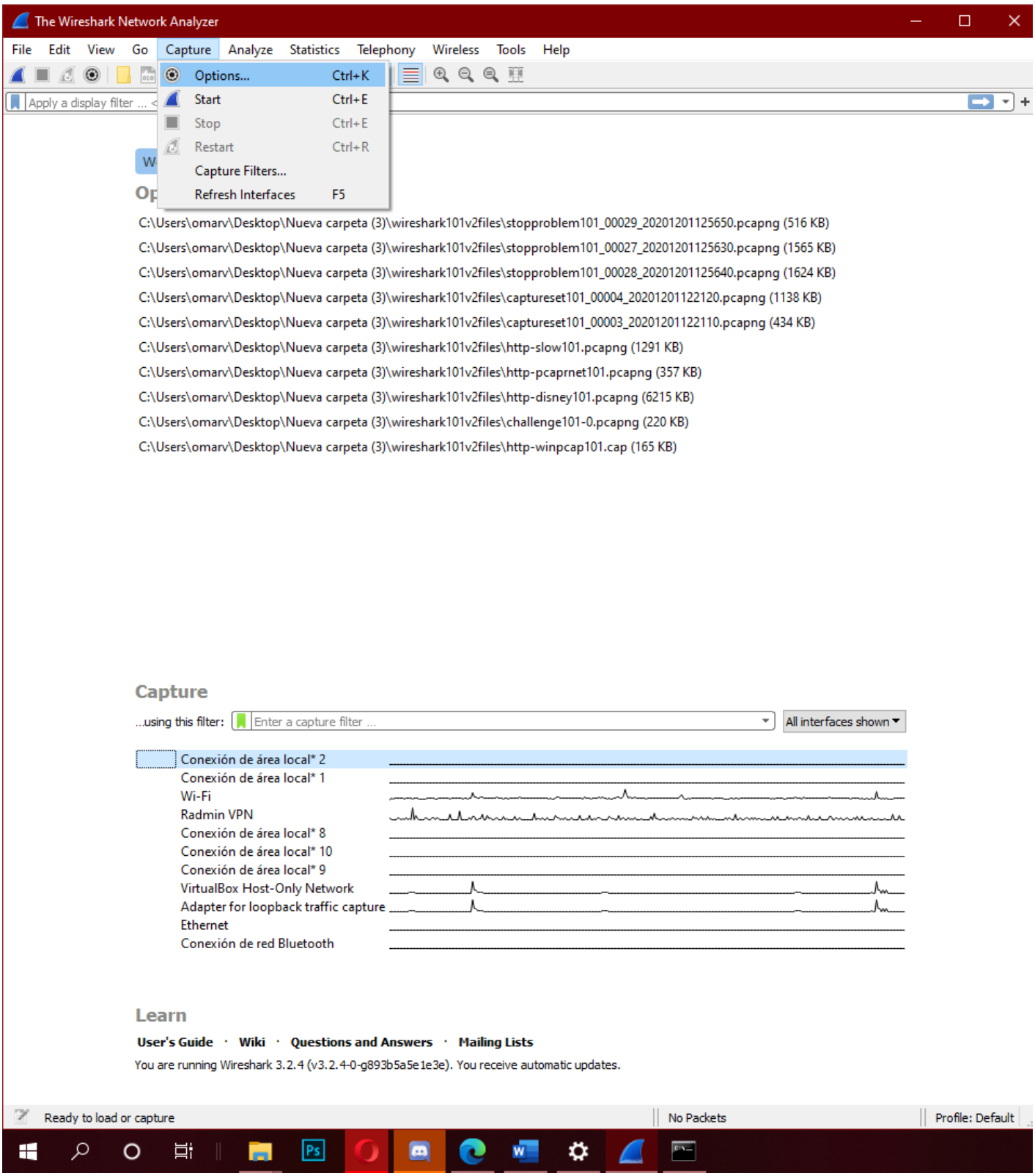
N.º De Control: 17530439

Lab 12: Capture only Traffic to or from Everyone else´s Mac Adress

Paso 1:

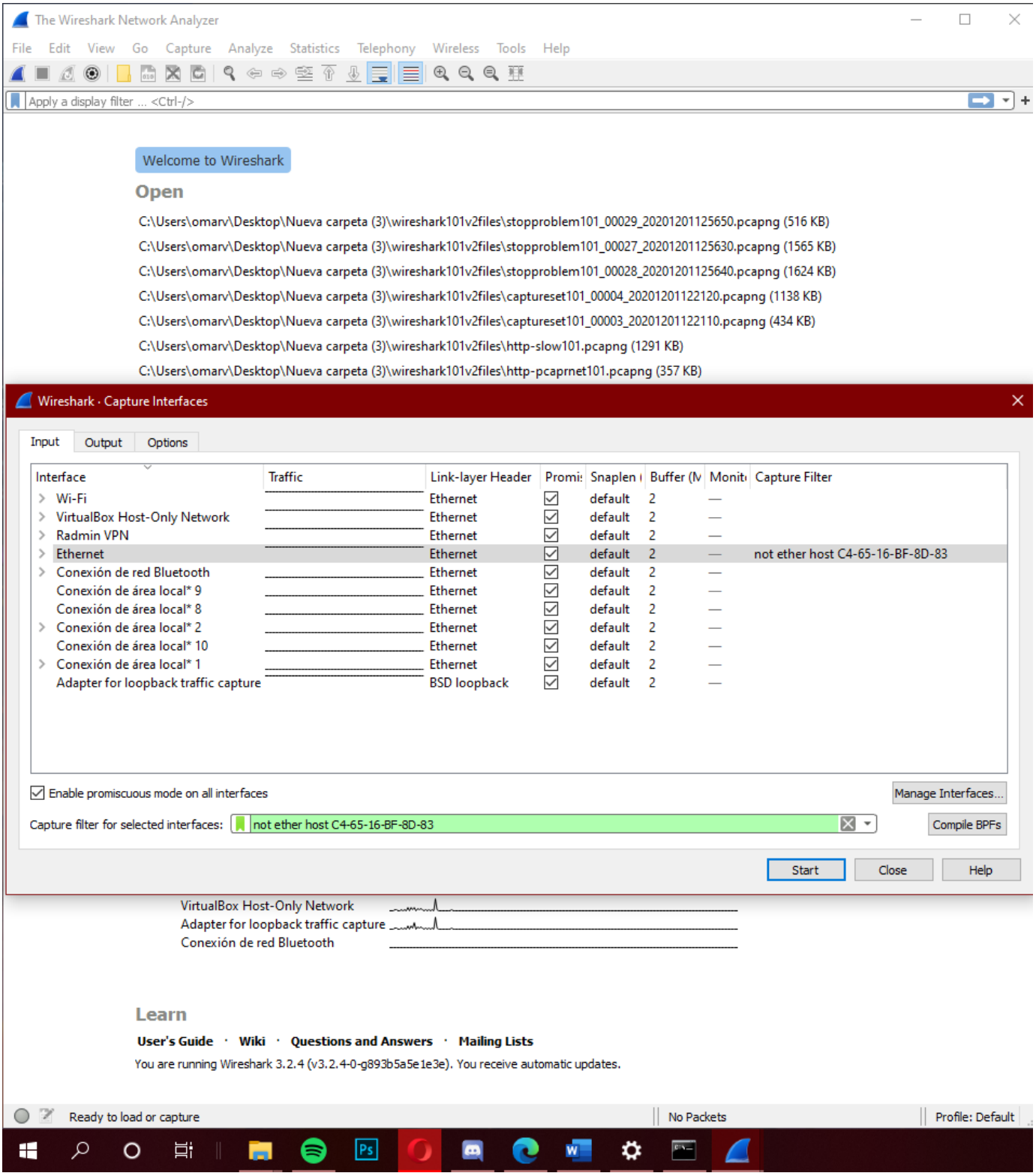


Paso 2:

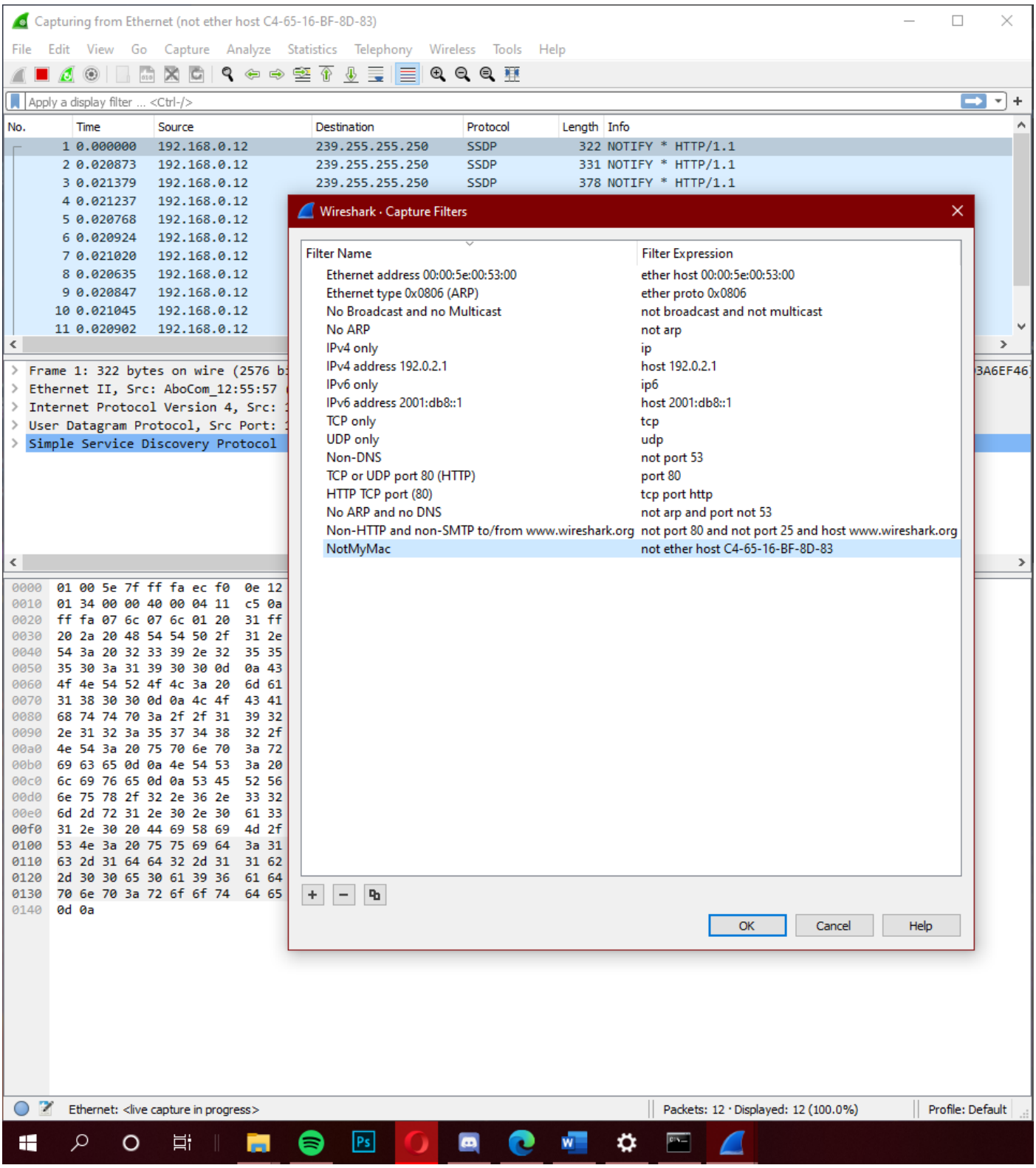


Paso 3: ordenar la sección de interface

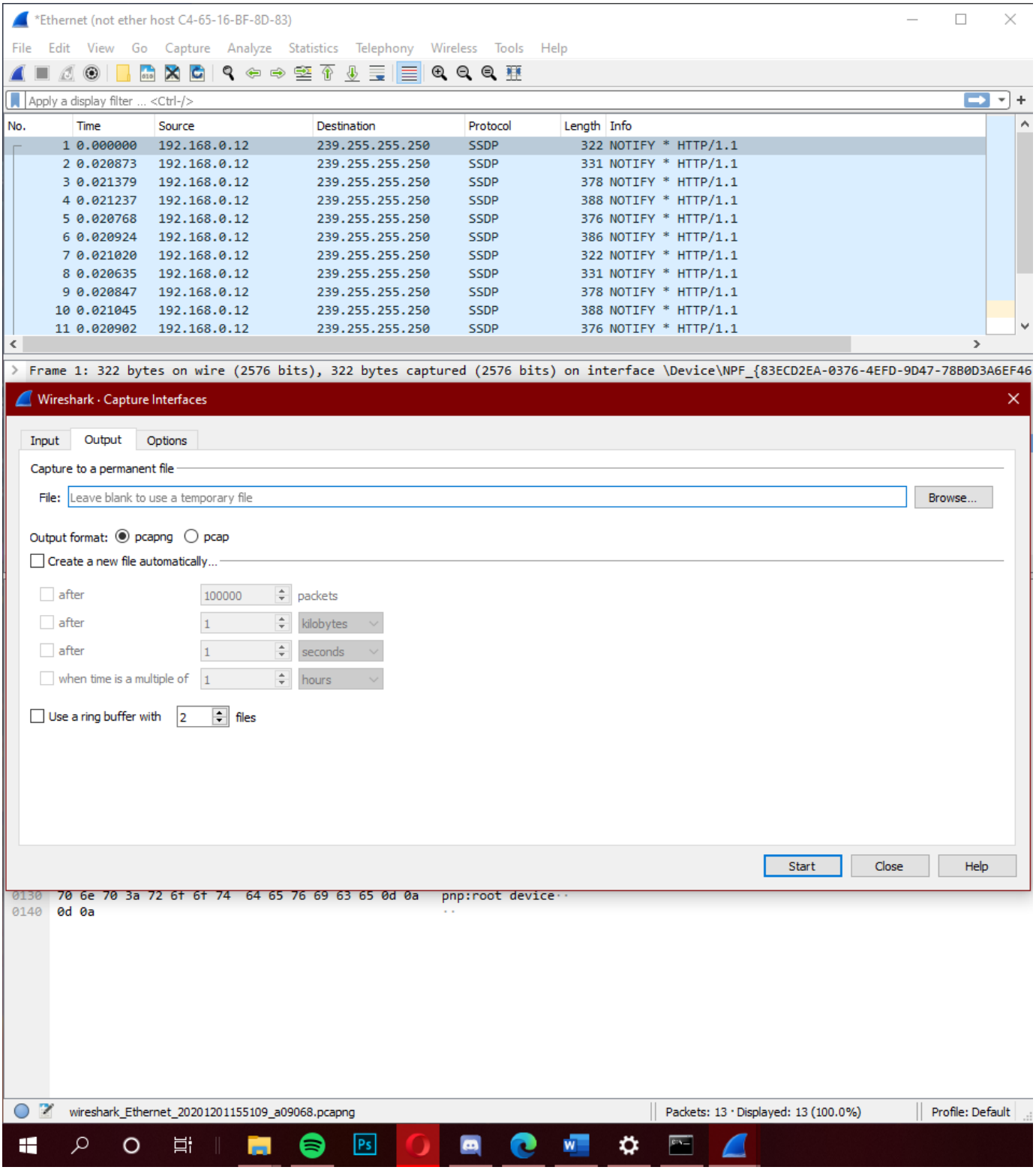
Paso 4:


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00027_20201201125630.pcapng (1565 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00028_20201201125640.pcapng (1624 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00004_20201201122120.pcapng (1138 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-slow101.pcapng (1291 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pcaprnet101.pcapng (357 KB)
Wireshark · Capture Interfaces
Input Output Options
Interface Traffic Link-layer Header Promi: Snaplen (Buffer (M Monit Capture Filter
Wi-Fi Ethernet default 2
VirtualBox Host-Only Network Ethernet default 2
Radmin VPN Ethernet default 2
Ethernet Ethernet default 2 not ether host C4-65-16-BF-8D-83
Conexión de red Bluetooth Ethernet default 2
Conexión de área local* 9 Ethernet default 2
Conexión de área local* 8 Ethernet default 2
Conexión de área local* 2 Ethernet default 2
Conexión de área local* 10 Ethernet default 2
Conexión de área local* 1 Ethernet default 2
Adapter for loopback traffic capture BSD loopback default 2
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: not ether host C4-65-16-BF-8D-83
Compile BPFs
Start Close Help
VirtualBox Host-Only Network
Adapter for loopback traffic capture
Conexión de red Bluetooth
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.4 (v3.2.4-0-g893b5a5e1e3e). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

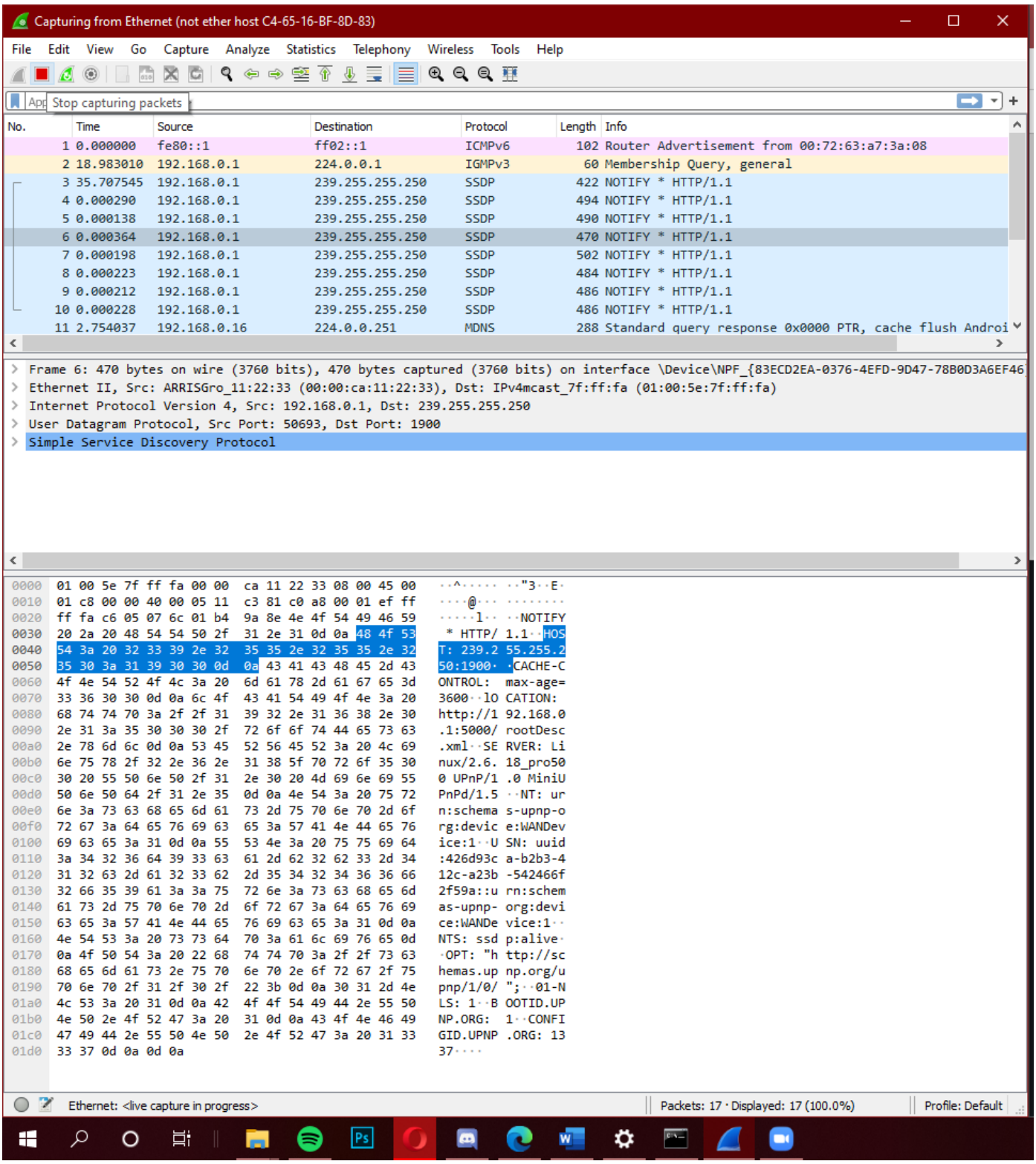
Paso 5:


Capturing from Ethernet (not ether host C4-65-16-BF-8D-83)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.12 239.255.255.250 SSDP 322 NOTIFY * HTTP/1.1
2 0.020873 192.168.0.12 239.255.255.250 SSDP 331 NOTIFY * HTTP/1.1
3 0.021379 192.168.0.12 239.255.255.250 SSDP 378 NOTIFY * HTTP/1.1
4 0.021237 192.168.0.12
5 0.020768 192.168.0.12
6 0.020924 192.168.0.12
7 0.021020 192.168.0.12
8 0.020635 192.168.0.12
9 0.020847 192.168.0.12
10 0.021045 192.168.0.12
11 0.020902 192.168.0.12
Frame 1: 322 bytes on wire (2576 b
Ethernet II, Src: AboCom_12:55:57
Internet Protocol Version 4, Src:
User Datagram Protocol, Src Port:
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa ec f0 0e 12
0010 01 34 00 00 40 00 04 11 c5 0a
0020 ff fa 07 6c 07 6c 01 20 31 ff
0030 20 2a 20 48 54 54 50 2f 31 2e
0040 54 3a 20 32 33 39 2e 32 35 35
0050 35 30 3a 31 39 30 30 0d 0a 43
0060 4f 4e 54 52 4f 4c 3a 20 6d 61
0070 31 38 30 30 0d 0a 4c 4f 43 41
0080 68 74 74 70 3a 2f 2f 31 39 32
0090 2e 31 32 3a 35 37 34 38 32 2f
00a0 4e 54 3a 20 75 70 6e 70 3a 72
00b0 69 63 65 0d 0a 4e 54 53 3a 20
00c0 6c 69 76 65 0d 0a 53 45 52 56
00d0 6e 75 78 2f 32 2e 36 2e 33 32
00e0 6d 2d 72 31 2e 30 2e 30 61 33
00f0 31 2e 30 20 44 69 58 69 4d 2f
0100 53 4e 3a 20 75 75 69 64 3a 31
0110 63 2d 31 64 64 32 2d 31 31 62
0120 2d 30 30 65 30 61 39 36 61 64
0130 70 6e 70 3a 72 6f 6f 74 64 65
0140 0d 0a
Wireshark · Capture Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
ether proto 0x0806
No Broadcast and no Multicast
not broadcast and not multicast
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
host 192.0.2.1
IPv6 only
ip6
IPv6 address 2001:db8::1
host 2001:db8::1
TCP only
tcp
UDP only
udp
Non-DNS
not port 53
TCP or UDP port 80 (HTTP)
port 80
HTTP TCP port (80)
tcp port http
No ARP and no DNS
not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org
not port 80 and not port 25 and host www.wireshark.org
NotMyMac
not ether host C4-65-16-BF-8D-83
OK
Cancel
Help
Ethernet: <live capture in progress>
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default

Paso 6, 7 y 8


*Ethernet (not ether host C4-65-16-BF-8D-83)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.12 239.255.255.250 SSDP 322 NOTIFY * HTTP/1.1
2 0.020873 192.168.0.12 239.255.255.250 SSDP 331 NOTIFY * HTTP/1.1
3 0.021379 192.168.0.12 239.255.255.250 SSDP 378 NOTIFY * HTTP/1.1
4 0.021237 192.168.0.12 239.255.255.250 SSDP 388 NOTIFY * HTTP/1.1
5 0.020768 192.168.0.12 239.255.255.250 SSDP 376 NOTIFY * HTTP/1.1
6 0.020924 192.168.0.12 239.255.255.250 SSDP 386 NOTIFY * HTTP/1.1
7 0.021020 192.168.0.12 239.255.255.250 SSDP 322 NOTIFY * HTTP/1.1
8 0.020635 192.168.0.12 239.255.255.250 SSDP 331 NOTIFY * HTTP/1.1
9 0.020847 192.168.0.12 239.255.255.250 SSDP 378 NOTIFY * HTTP/1.1
10 0.021045 192.168.0.12 239.255.255.250 SSDP 388 NOTIFY * HTTP/1.1
11 0.020902 192.168.0.12 239.255.255.250 SSDP 376 NOTIFY * HTTP/1.1
Frame 1: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface \Device\NPF_{83ECD2EA-0376-4EFD-9D47-78B0D3A6EF46
Wireshark · Capture Interfaces
Input Output Options
Capture to a permanent file
File: Leave blank to use a temporary file
Browse...
Output format: pcapng pcap
Create a new file automatically...
after 100000 packets
after 1 kilobytes
after 1 seconds
when time is a multiple of 1 hours
Use a ring buffer with 2 files
Start Close Help
0130 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a pnp:root device··
0140 0d 0a ··
wireshark_Ethernet_20201201155109_a09068.pcapng
Packets: 13 · Displayed: 13 (100.0%)
Profile: Default

Paso 9 y 10


Capturing from Ethernet (not ether host C4-65-16-BF-8D-83)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets
No. Time Source Destination Protocol Length Info
1 0.000000 fe80::1 ff02::1 ICMPv6 102 Router Advertisement from 00:72:63:a7:3a:08
2 18.983010 192.168.0.1 224.0.0.1 IGMPv3 60 Membership Query, general
3 35.707545 192.168.0.1 239.255.255.250 SSDP 422 NOTIFY * HTTP/1.1
4 0.000290 192.168.0.1 239.255.255.250 SSDP 494 NOTIFY * HTTP/1.1
5 0.000138 192.168.0.1 239.255.255.250 SSDP 490 NOTIFY * HTTP/1.1
6 0.000364 192.168.0.1 239.255.255.250 SSDP 470 NOTIFY * HTTP/1.1
7 0.000198 192.168.0.1 239.255.255.250 SSDP 502 NOTIFY * HTTP/1.1
8 0.000223 192.168.0.1 239.255.255.250 SSDP 484 NOTIFY * HTTP/1.1
9 0.000212 192.168.0.1 239.255.255.250 SSDP 486 NOTIFY * HTTP/1.1
10 0.000228 192.168.0.1 239.255.255.250 SSDP 486 NOTIFY * HTTP/1.1
11 2.754037 192.168.0.16 224.0.0.251 MDNS 288 Standard query response 0x0000 PTR, cache flush Androi
Frame 6: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface \Device\NPF_{83ECD2EA-0376-4EFD-9D47-78B0D3A6EF46}
Ethernet II, Src: ARRISGro_11:22:33 (00:00:ca:11:22:33), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 50693, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 00 00 ca 11 22 33 08 00 45 00 ..^..... ..”3..E.
0010 01 c8 00 00 40 00 05 11 c3 81 c0 a8 00 01 ef ff ....@... ....
0020 ff fa c6 05 07 6c 01 b4 9a 8e 4e 4f 54 49 46 59 .....l.. ..NOTIFY
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/ 1.1..HOS
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.2
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900. .CACHE-C
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ONTROL: max-age=
0070 33 36 30 30 0d 0a 6c 4f 43 41 54 49 4f 4e 3a 20 3600..lO CATION:
0080 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36 38 2e 30 http://1 92.168.0
0090 2e 31 3a 35 30 30 30 2f 72 6f 6f 74 44 65 73 63 .1:5000/ rootDesc
00a0 2e 78 6d 6c 0d 0a 53 45 52 56 45 52 3a 20 4c 69 .xml..SE RVER: Li
00b0 6e 75 78 2f 32 2e 36 2e 31 38 5f 70 72 6f 35 30 nux/2.6. 18_pro50
00c0 30 20 55 50 6e 50 2f 31 2e 30 20 4d 69 6e 69 55 0 UPnP/1 .0 MiniU
00d0 50 6e 50 64 2f 31 2e 35 0d 0a 4e 54 3a 20 75 72 PnPd/1.5 ..NT: ur
00e0 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f n:schema s-upnp-o
00f0 72 67 3a 64 65 76 69 63 65 3a 57 41 4e 44 65 76 rg:devic e:WANDev
0100 69 63 65 3a 31 0d 0a 55 53 4e 3a 20 75 75 69 64 ice:1..U SN: uuid
0110 3a 34 32 36 64 39 33 63 61 2d 62 32 62 33 2d 34 :426d93c a-b2b3-4
0120 31 32 63 2d 61 32 33 62 2d 35 34 32 34 36 36 66 12c-a23b -542466f
0130 32 66 35 39 61 3a 3a 75 72 6e 3a 73 63 68 65 6d 2f59a::u rn:schem
0140 61 73 2d 75 70 6e 70 2d 6f 72 67 3a 64 65 76 69 as-upnp- org:devi
0150 63 65 3a 57 41 4e 44 65 76 69 63 65 3a 31 0d 0a ce:WANDe vice:1..
0160 4e 54 53 3a 20 73 73 64 70 3a 61 6c 69 76 65 0d NTS: ssd p:alive.
0170 0a 4f 50 54 3a 20 22 68 74 74 70 3a 2f 2f 73 63 .OPT: "h ttp://sc
0180 68 65 6d 61 73 2e 75 70 6e 70 2e 6f 72 67 2f 75 hemas.up np.org/u
0190 70 6e 70 2f 31 2f 30 2f 22 3b 0d 0a 30 31 2d 4e pnp/1/0/ ";..01-N
01a0 4c 53 3a 20 31 0d 0a 42 4f 4f 54 49 44 2e 55 50 LS: 1..B OOTID.UP
01b0 4e 50 2e 4f 52 47 3a 20 31 0d 0a 43 4f 4e 46 49 NP.ORG: 1..CONFI
01c0 47 49 44 2e 55 50 4e 50 2e 4f 52 47 3a 20 31 33 GID.UPNP .ORG: 13
01d0 33 37 0d 0a 0d 0a 37....
Ethernet: <live capture in progress>
Packets: 17 · Displayed: 17 (100.0%)
Profile: Default