Wireshark

Autores:

Javier Martínez Montilla

Bryan Moreno Picamán

1. Introducción

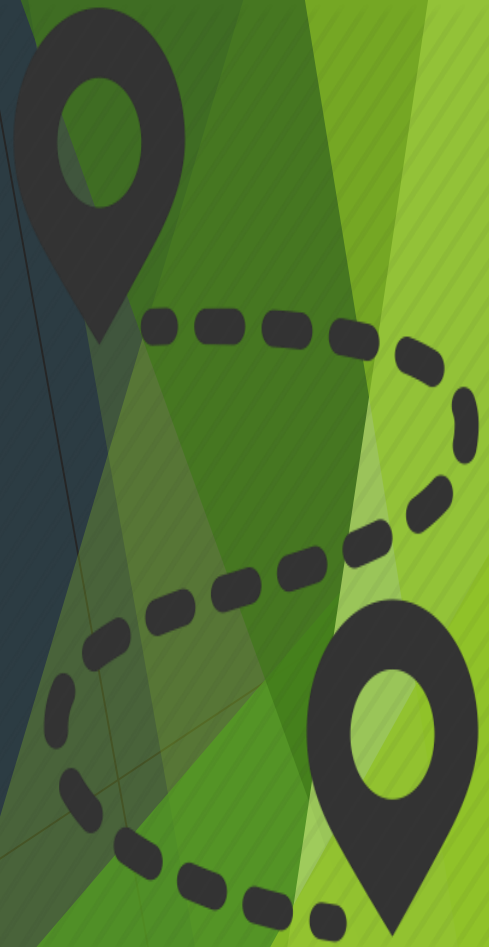
- Wireshark (Ethereal), es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica.

2. Finalidad de la aplicación

- Su utilidad principal es parecida a tcpdump, pero de forma gráfica, analizar el tráfico que circula por la red, además de permitir al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos por la red a la cual el ordenador está conectado.

  Permite observar de forma detalla las cabeceras de los protocolos que hemos estudiado teóricamente y con ello ayudarnos a comprender la utilidad y la función de cada uno de sus campos.

  Utilidad para realizar auditorias y ver información de terceros, por ejemplo, para intentar conectarse a una red Wi-Fi protegida con WEP.



3. Licencia

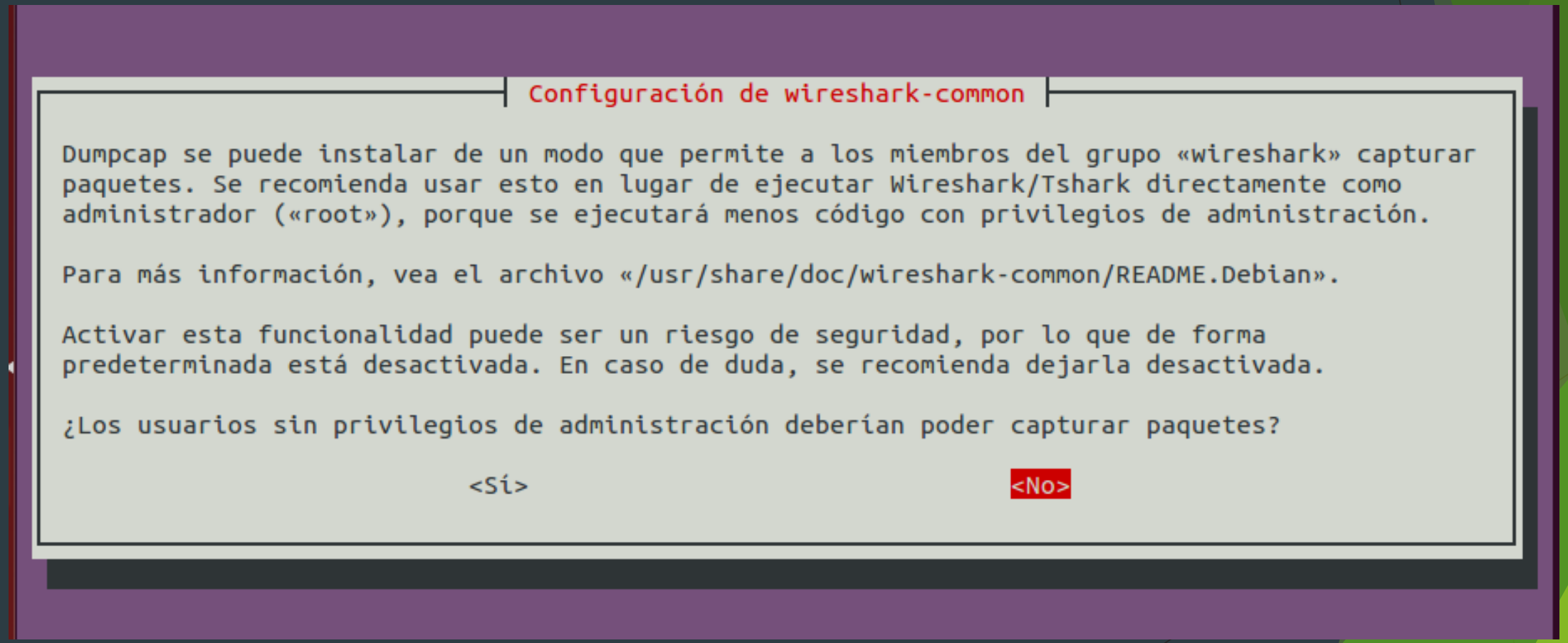
- Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android, y Mac OS X, así como en Microsoft Windows.

4. Instalación de wireshark

- Primero debemos añadir el repositorio y después procedemos con la instalación:

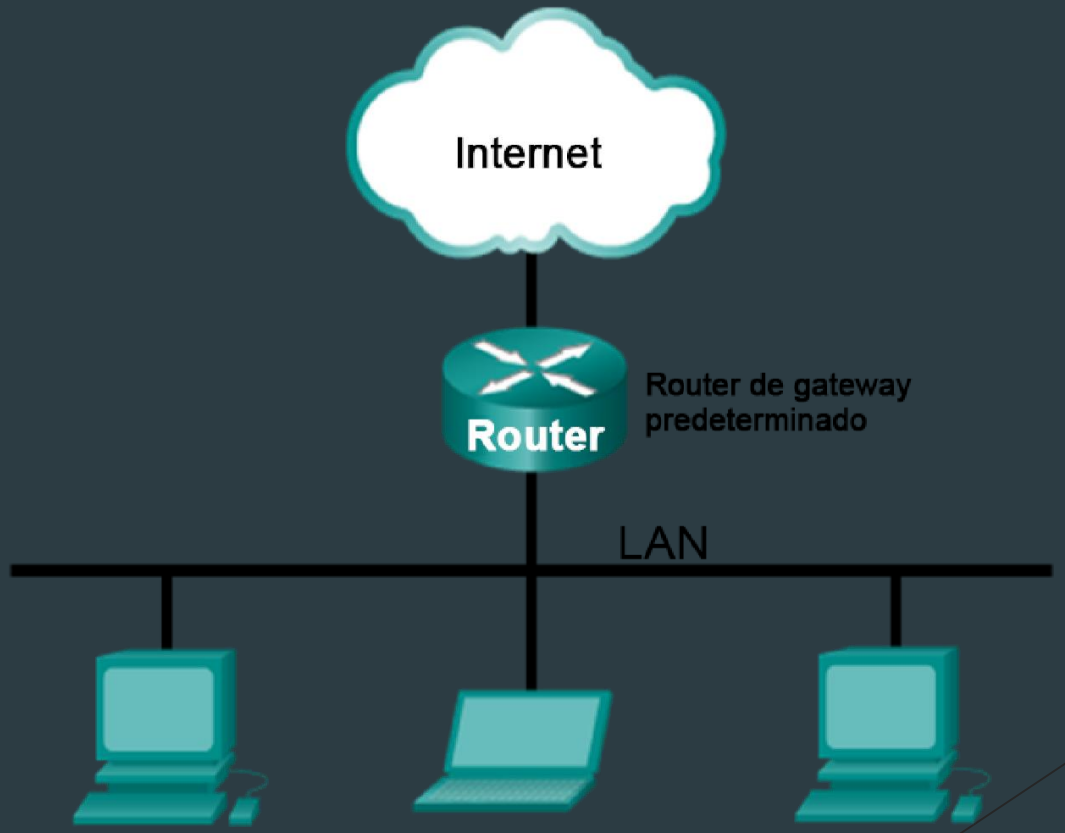
- sudo add-apt-repository ppa:pi-rho/security
- sudo apt-get update
- sudo apt-get install wireshark

4.1. Proceso de instalación



5. Uso de Wireshark

- A continuación, guiaremos paso a paso para empezar el análisis de los paquetes de la red:



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	216.58.201.142	192.168.1.130	TLSv1.2	325	Application Data

▶Frame 1: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface 0
▶Ethernet II, Src: 8c:e1:17:e5:da:2a (8c:e1:17:e5:da:2a), Dst: IntelCor_69:a7:44 (30:3a:64:69:a7:44)
▶Internet Protocol Version 4, Src: 216.58.201.142 (216.58.201.142), Dst: 192.168.1.130 (192.168.1.130)
▶Transmission Control Protocol, Src Port: 443 (443), Dst Port: 37062 (37062), Seq: 1, Ack: 1, Len: 259
▶Secure Sockets Layer

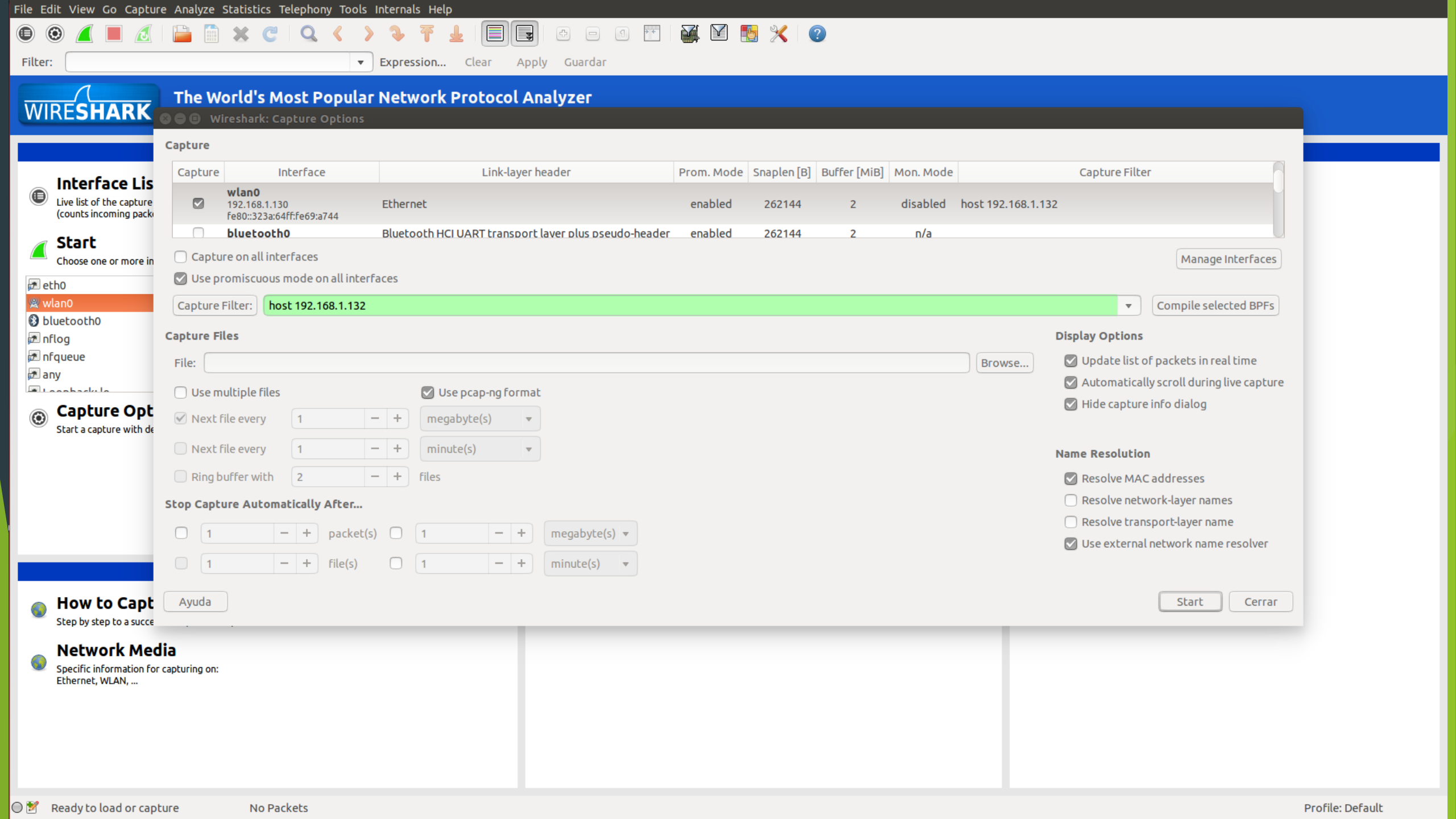
Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s
☐	eth0		none	0	0
☑	wlan0		192.168.1.130	111	0
☐	bluetooth0		none	96	0
☐	nflog		none	0	0
☐	nfqueue		none	0	0
☐	any		none	111	0
☐	lo		127.0.0.1	0	0

Ayuda Start Stop Options Cerrar

```
0000  30 3a 64 69 a7 44 8c e1  17 e5 da 2a 08 00 45 00   0:di.D.. ...*..E.
0010  01 37 ad 9b 00 00 39 06  6f 32 d8 3a c9 8e c0 a8   .7....9. o2.:....
0020  01 82 01 bb 90 c6 87 41  04 a2 b5 e7 61 a3 80 18   .......A ....a...
0030  06 56 a7 a1 00 00 01 01  08 0a 00 3a 91 5a ff ff   .V...... ...:.Z..
```

Frame (frame), 325 bytes Packets: 95 · Displayed: 95 (100,0%) · Dropped: 0 (0,0%) Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Guardar
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Wireshark: Capture Options
Capture
Capture
Interface
Link-layer header
Prom. Mode
Snaplen [B]
Buffer [MiB]
Mon. Mode
Capture Filter
wlan0
192.168.1.130
fe80::323a:64ff:fe69:a744
Ethernet
enabled
262144
2
disabled
host 192.168.1.132
bluetooth0
Bluetooth HCI UART transport layer plus pseudo-header
enabled
262144
2
n/a
Capture on all interfaces
Manage Interfaces
Use promiscuous mode on all interfaces
Capture Filter:
host 192.168.1.132
Compile selected BPFs
Capture Files
File:
Browse...
Use multiple files
Use pcap-ng format
Next file every
1
megabyte(s)
Next file every
1
minute(s)
Ring buffer with
2
files
Stop Capture Automatically After...
packet(s)
megabyte(s)
file(s)
minute(s)
Display Options
Update list of packets in real time
Automatically scroll during live capture
Hide capture info dialog
Name Resolution
Resolve MAC addresses
Resolve network-layer names
Resolve transport-layer name
Use external network name resolver
Ayuda
Start
Cerrar
Interface Lis
Live list of the capture
(counts incoming packe
Start
Choose one or more in
eth0
wlan0
bluetooth0
nflog
nfqueue
any
Capture Opt
Start a capture with de
How to Capt
Step by step to a succe
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

Capture filters

- - Captura el tráfico desde una dirección IP:
  - host 192.168.1.56
- Captura el tráfico de una subred completa:
  - net 192.168.1.0/24
- Captura desde un puerto concreto:
  - port 53 → Ejemplo DNS

¡Existen más filtros y combinaciones disponibles!

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
1536	127.1063160	216.58.214.163	192.168.1.130	TCP	66	[TCP Dup ACK 318#2] [TCP ACKed unseen segment] 443→47848 [ACK] Seq=1 Ack=2 Win=374 Len=0 TSval=1800506251 TSecr=4294947808
1537	127.1063270	216.58.201.131	192.168.1.130	TCP	66	[TCP Dup ACK 317#2] [TCP ACKed unseen segment] 443→59990 [ACK] Seq=1 Ack=2 Win=651 Len=0 TSval=1214309919 TSecr=4294947845
1538	127.7102850	8c:e1:17:e5:da:2a	IntelCor_69:a7:44	ARP	42	Who has 192.168.1.130? Tell 192.168.1.1
1539	127.7102950	IntelCor_69:a7:44	8c:e1:17:e5:da:2a	ARP	42	192.168.1.130 is at 30:3a:64:69:a7:44
1540	128.8826530	192.168.1.130	216.58.214.163	TCP	66	[TCP Dup ACK 319#2] 47802→443 [ACK] Seq=1 Ack=1 Win=1425 Len=0 TSval=26048 TSecr=1634979880
1541	128.8986630	216.58.214.163	192.168.1.130	TCP	66	[TCP Dup ACK 320#2] [TCP ACKed unseen segment] 443→47802 [ACK] Seq=1 Ack=2 Win=390 Len=0 TSval=1635024934 TSecr=4294948287
1542	129.0106490	192.168.1.130	216.58.201.138	TCP	66	[TCP Dup ACK 321#2] 38512→443 [ACK] Seq=1 Ack=1 Win=399 Len=0 TSval=26080 TSecr=83299596
1543	129.0258580	216.58.201.138	192.168.1.130	TCP	66	[TCP Dup ACK 322#2] [TCP ACKed unseen segment] 443→38512 [ACK] Seq=1 Ack=2 Win=357 Len=0 TSval=83344651 TSecr=4294948304
1544	129.1386570	192.168.1.130	216.58.201.129	TCP	66	[TCP Dup ACK 323#2] 47336→443 [ACK] Seq=1 Ack=1 Win=339 Len=0 TSval=26112 TSecr=1267525244
1545	129.1543800	216.58.201.129	192.168.1.130	TCP	66	[TCP Dup ACK 324#2] [TCP ACKed unseen segment] 443→47336 [ACK] Seq=1 Ack=2 Win=365 Len=0 TSval=1267570299 TSecr=4294948347
1546	129.6506570	192.168.1.130	216.58.201.129	TCP	66	[TCP Dup ACK 325#2] 46996→443 [ACK] Seq=1 Ack=1 Win=339 Len=0 TSval=26240 TSecr=1303850279
1547	129.6659110	216.58.201.129	192.168.1.130	TCP	66	[TCP Dup ACK 326#2] [TCP ACKed unseen segment] 443→46996 [ACK] Seq=1 Ack=2 Win=392 Len=0 TSval=1303895334 TSecr=4294948485
1548	129.7579110	162.125.18.133	192.168.1.130	TLSv1.2	323	Application Data
1549	129.7586500	192.168.1.130	216.58.201.142	TLSv1.2	192	Application Data
1550	129.7586850	192.168.1.130	216.58.201.142	TLSv1.2	1434	Application Data
1551	129.7590290	192.168.1.130	216.58.201.142	TCP	1434	[TCP segment of a reassembled PDU]
1552	129.7598730	192.168.1.130	162.125.18.133	TLSv1.2	1016	Application Data
1553	129.7605820	192.168.1.130	216.58.201.142	TLSv1.2	1434	Application Data
1554	129.7621170	192.168.1.130	216.58.201.142	TCP	1434	[TCP segment of a reassembled PDU]
1555	129.7644330	192.168.1.130	216.58.201.142	TLSv1.2	1434	Application Data
1556	129.7656380	192.168.1.130	216.58.201.142	TLSv1.2	181	Application Data
1557	129.7744220	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=55329 Ack=63448 Win=1622 Len=0 TSval=83108339 TSecr=26267
1558	129.7759310	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=55329 Ack=64816 Win=1617 Len=0 TSval=83108340 TSecr=26267
1559	129.7759460	216.58.201.142	192.168.1.130	TLSv1.2	112	Application Data
1560	129.7797050	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=55375 Ack=67552 Win=1617 Len=0 TSval=83108344 TSecr=26267
1561	129.7819330	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=55375 Ack=70288 Win=1617 Len=0 TSval=83108346 TSecr=26267
1562	129.8146390	192.168.1.130	216.58.201.142	TCP	66	36928→443 [ACK] Seq=70403 Ack=55375 Win=2415 Len=0 TSval=26281 TSecr=83108340
1563	129.8228470	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=55375 Ack=70403 Win=1622 Len=0 TSval=83108387 TSecr=26268
1564	129.8432790	216.58.201.142	192.168.1.130	TLSv1.2	154	Application Data
1565	129.8432930	192.168.1.130	216.58.201.142	TCP	66	36928→443 [ACK] Seq=70403 Ack=55463 Win=2415 Len=0 TSval=26288 TSecr=83108408
1566	129.8445810	216.58.201.142	192.168.1.130	TLSv1.2	1053	Application Data
1567	129.8446020	192.168.1.130	216.58.201.142	TCP	66	36928→443 [ACK] Seq=70403 Ack=56450 Win=2415 Len=0 TSval=26288 TSecr=83108408
1568	129.8446180	216.58.201.142	192.168.1.130	TLSv1.2	112	Application Data
1569	129.8446230	192.168.1.130	216.58.201.142	TCP	66	36928→443 [ACK] Seq=70403 Ack=56496 Win=2415 Len=0 TSval=26288 TSecr=83108408
1570	129.8449050	192.168.1.130	216.58.201.142	TLSv1.2	112	Application Data
1571	129.8604560	216.58.201.142	192.168.1.130	TCP	66	443→36928 [ACK] Seq=56496 Ack=70449 Win=1622 Len=0 TSval=83108425 TSecr=26288
1572	129.8824630	162.125.18.133	192.168.1.130	TCP	66	443→40654 [ACK] Seq=772 Ack=2851 Win=84 Len=0 TSval=1236242625 TSecr=26267

▶Frame 278: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▶Ethernet II, Src: IntelCor_69:a7:44 (30:3a:64:69:a7:44), Dst: 8c:e1:17:e5:da:2a (8c:e1:17:e5:da:2a)
▶Internet Protocol Version 4, Src: 192.168.1.130 (192.168.1.130), Dst: 216.58.201.142 (216.58.201.142)
▶Transmission Control Protocol, Src Port: 36928 (36928), Dst Port: 443 (443), Seq: 18226, Ack: 5509, Len: 0

```
0000  8c e1 17 e5 da 2a 30 3a  64 69 a7 44 08 00 45 00   .....*0: di.D..E.
0010  00 34 e1 10 40 00 40 06  f5 bf c0 a8 01 82 d8 3a   .4..@.@. .......:
0020  c9 8e 90 40 01 bb 66 a7  11 5a 9c 77 ad c5 80 10   ...@..f. .Z.w....
0030  09 6f 0b ee 00 00 01 01  08 0a 00 00 05 c1 04 f2   .o...... ........
```

wlan0: <live capture in progress... Packets: 1572 · Displayed: 1572 (100,0%) Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 192.168.1.132 Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2	1.000754000	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	2.000864000	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	3.001806000	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
157	73.730189006	192.168.1.132	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
159	73.807260006	192.168.1.132	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
161	73.883695006	192.168.1.132	239.255.255.250	SSDP	535	NOTIFY * HTTP/1.1
163	73.959080006	192.168.1.132	239.255.255.250	SSDP	549	NOTIFY * HTTP/1.1
165	74.027400006	192.168.1.132	239.255.255.250	SSDP	547	NOTIFY * HTTP/1.1
167	74.107209006	192.168.1.132	239.255.255.250	SSDP	563	NOTIFY * HTTP/1.1
172	76.732200006	192.168.1.132	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
174	76.810483006	192.168.1.132	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
176	76.885181006	192.168.1.132	239.255.255.250	SSDP	535	NOTIFY * HTTP/1.1
178	76.960144006	192.168.1.132	239.255.255.250	SSDP	549	NOTIFY * HTTP/1.1
180	77.027580006	192.168.1.132	239.255.255.250	SSDP	547	NOTIFY * HTTP/1.1
182	77.107903006	192.168.1.132	239.255.255.250	SSDP	563	NOTIFY * HTTP/1.1
198	79.733750006	192.168.1.132	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
200	79.811350006	192.168.1.132	239.255.255.250	SSDP	492	NOTIFY * HTTP/1.1
202	79.885715006	192.168.1.132	239.255.255.250	SSDP	535	NOTIFY * HTTP/1.1
204	79.961712006	192.168.1.132	239.255.255.250	SSDP	549	NOTIFY * HTTP/1.1
208	80.028789006	192.168.1.132	239.255.255.250	SSDP	547	NOTIFY * HTTP/1.1
210	80.109074006	192.168.1.132	239.255.255.250	SSDP	563	NOTIFY * HTTP/1.1
347	108.703400006	192.168.1.132	192.168.1.255	BROWSER	243	Host Announcement MSI-SERSOKER, Workstation, Server, NT Workstation, Potential Browser
350	120.009076006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
351	121.010168006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
352	122.010696006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
353	123.010745006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
800	240.011488006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
801	241.012163006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
802	242.012705006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
803	243.013524006	192.168.1.132	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

▶ Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
▶ Ethernet II, Src: 78:0c:b8:e3:86:54 (78:0c:b8:e3:86:54), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.1.132 (192.168.1.132), Dst: 239.255.255.250 (239.255.255.250)
▶ User Datagram Protocol, Src Port: 61117 (61117), Dst Port: 1900 (1900)
▶ Hypertext Transfer Protocol

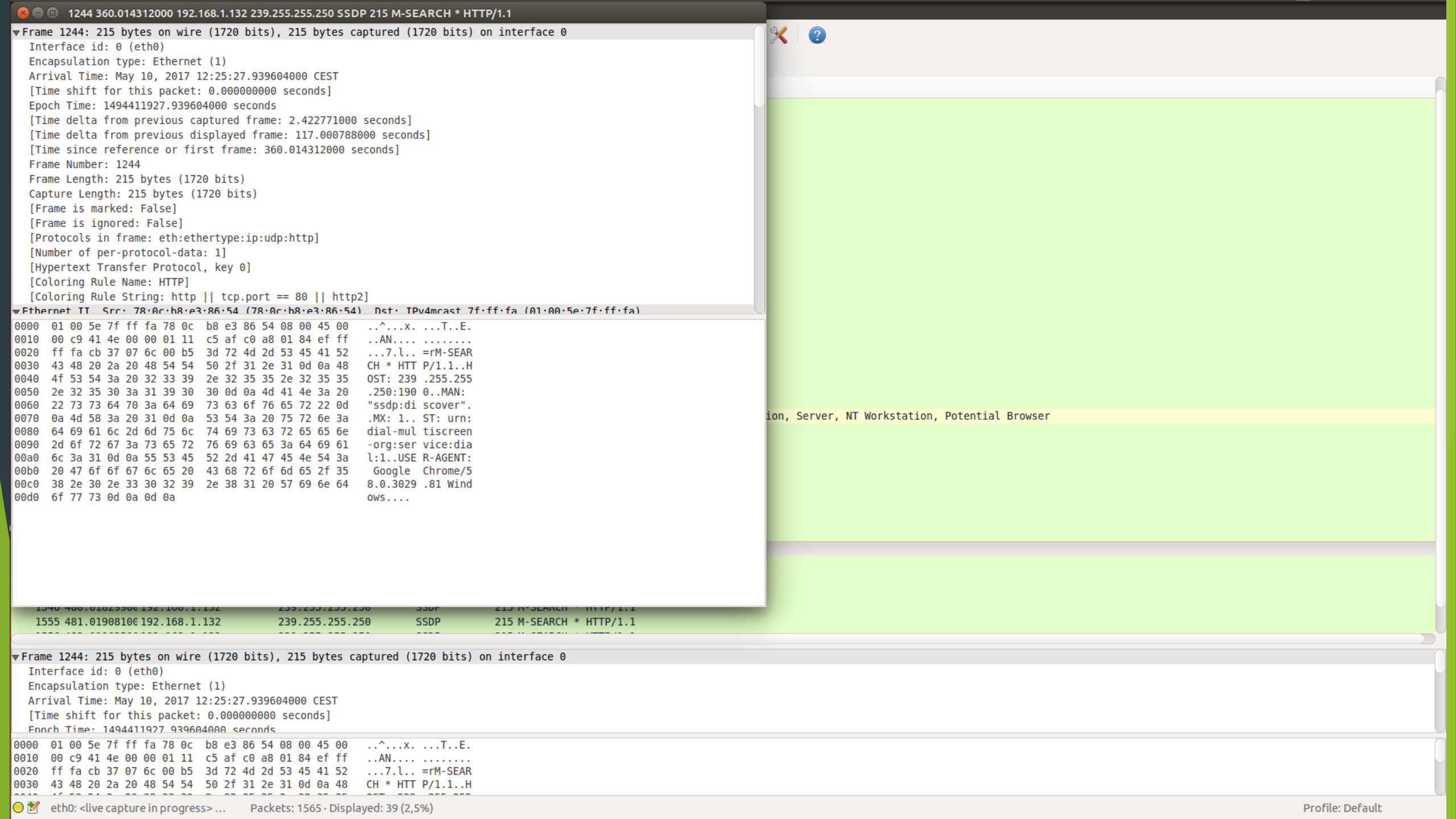
```
0000  01 00 5e 7f ff fa 78 0c  b8 e3 86 54 08 00 45 00   ..^...x. ...T..E.
0010  00 c9 41 30 00 00 01 11  c5 cd c0 a8 01 84 ef ff   ..A0.... ........
0020  ff fa ee bd 07 6c 00 b5  19 ec 4d 2d 53 45 41 52   .....l.. ..M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1..H
```

eth0: <live capture in progress> ... Packets: 1105 · Displayed: 31 (2,8%) Profile: Default

Display filters

- Filtrar tráfico de un puerto:
  - tcp.port eq 25
- Filtrar tráfico de una dirección específica:
  - Ip.addr == 192.168.1.46
- Filtrar por contenido en el header:
  - sip.To contains “a1762”

¡También existen más filtros y combinaciones entre sí!


1244 360.014312000 192.168.1.132 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
Frame 1244: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: May 10, 2017 12:25:27.939604000 CEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1494411927.939604000 seconds
[Time delta from previous captured frame: 2.422771000 seconds]
[Time delta from previous displayed frame: 117.000788000 seconds]
[Time since reference or first frame: 360.014312000 seconds]
Frame Number: 1244
Frame Length: 215 bytes (1720 bits)
Capture Length: 215 bytes (1720 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:http]
[Number of per-protocol-data: 1]
[Hypertext Transfer Protocol, key 0]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: 78:0c:b8:e3:86:54 (78:0c:b8:e3:86:54), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
0000 01 00 5e 7f ff fa 78 0c b8 e3 86 54 08 00 45 00 ..^...x. ...T..E.
0010 00 c9 41 4e 00 00 01 11 c5 af c0 a8 01 84 ef ff ..AN.... ....
0020 ff fa cb 37 07 6c 00 b5 3d 72 4d 2d 53 45 41 52 ...7.l.. =rM-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 55 53 45 52 2d 41 47 45 4e 54 3a l:1..USE R-AGENT:
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 35 Google Chrome/5
00c0 38 2e 30 2e 33 30 32 39 2e 38 31 20 57 69 6e 64 8.0.3029 .81 Wind
00d0 6f 77 73 0d 0a 0d 0a ows....
ion, Server, NT Workstation, Potential Browser
1555 481.0190810 192.168.1.132 239.255.255.250 SSDP 215 M-SEARCH * HTTP/1.1
Frame 1244: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: May 10, 2017 12:25:27.939604000 CEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1494411927.939604000 seconds
0000 01 00 5e 7f ff fa 78 0c b8 e3 86 54 08 00 45 00 ..^...x. ...T..E.
0010 00 c9 41 4e 00 00 01 11 c5 af c0 a8 01 84 ef ff ..AN.... ....
0020 ff fa cb 37 07 6c 00 b5 3d 72 4d 2d 53 45 41 52 ...7.l.. =rM-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
eth0: <live capture in progress> ...
Packets: 1565 · Displayed: 39 (2,5%)
Profile: Default

```
▼ Frame 367: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on interface 0
    Interface id: 0 (eth0)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 10, 2017 12:21:43.168639000 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1494411703.168639000 seconds
    [Time delta from previous captured frame: 10.475409000 seconds]
    [Time delta from previous displayed frame: 10.475409000 seconds]
    [Time since reference or first frame: 135.243347000 seconds]
    Frame Number: 367
    Frame Length: 185 bytes (1480 bits)
    Capture Length: 185 bytes (1480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:db-lsp-disc]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
▶ Ethernet II, Src: Micro-St_47:87:ad (44:8a:5b:47:87:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Internet Protocol Version 4, Src: 192.168.1.135 (192.168.1.135), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header Length: 20 bytes
  ▼ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 171
    Identification: 0xc378 (50040)
  ▼ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
  ▼ Header checksum: 0xb49a [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 192.168.1.135 (192.168.1.135)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 17500 (17500), Dst Port: 17500 (17500)
    Source Port: 17500 (17500)
    Destination Port: 17500 (17500)
    Length: 151
  ▼ Checksum: 0xd636 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 1]
▼ Dropbox LAN sync Discovery Protocol
    Text: {"host_int": 190851060612576816485335171291773514628, "version": [2, 0], "displayname": "", "port": 17500, "namespaces": [546836497, 80566589]}
```

```
0020  ff ff 44 5c 44 5c 00 97  d6 36 7b 22 68 6f 73 74   ..D\D\.. .6{"host
0030  5f 69 6e 74 22 3a 20 31  39 30 38 35 31 30 36 30   _int": 1 90851060
0040  36 31 32 35 37 36 38 31  36 34 38 35 33 33 35 31   61257681 64853351
0050  37 31 32 39 31 37 37 33  35 31 34 36 32 38 2c 20   71291773 514628,
```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 150.214.191.176 Expression... Clear Apply Guardar

No.	Time	Source	Destination	Protocol	Length	Info
59	14.904777000	192.168.1.135	150.214.191.176	TCP	66	58258→80 [FIN, ACK] Seq=1 Ack=1 Win=620 Len=0 TSval=1100990 TSecr=1665672697
60	14.904793000	192.168.1.135	150.214.191.176	TCP	66	58260→80 [FIN, ACK] Seq=1 Ack=1 Win=321 Len=0 TSval=1100990 TSecr=1665672729
61	14.904849000	192.168.1.135	150.214.191.176	TCP	74	58262→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1100990 TSecr=0 WS=128
62	14.935992000	150.214.191.176	192.168.1.135	TCP	66	80→58258 [ACK] Seq=1 Ack=2 Win=253 Len=0 TSval=1665706524 TSecr=1100990
63	14.936007000	150.214.191.176	192.168.1.135	TCP	66	80→58260 [ACK] Seq=1 Ack=2 Win=235 Len=0 TSval=1665706524 TSecr=1100990
64	14.936226000	150.214.191.176	192.168.1.135	TCP	74	80→58262 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1665706525 TSecr=1100990 WS=128
65	14.936239000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1100998 TSecr=1665706525
66	14.936446000	192.168.1.135	150.214.191.176	HTTP	576	GET /~pw_25346371/redsocial/index.html HTTP/1.1
67	14.968373000	150.214.191.176	192.168.1.135	TCP	66	80→58262 [ACK] Seq=1 Ack=511 Win=30080 Len=0 TSval=1665706557 TSecr=1100998
68	14.970487000	150.214.191.176	192.168.1.135	HTTP	3867	HTTP/1.1 200 OK (text/html)
69	14.970496000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=511 Ack=3802 Win=36864 Len=0 TSval=1101007 TSecr=1665706557
70	19.249792000	192.168.1.135	150.214.191.176	HTTP	624	GET /~pw_25346371/redsocial/paginas/portada.html?usuario=Pepe&contrasenia=jejeje&inicio=Inicio HTTP/1.1
71	19.285388000	150.214.191.176	192.168.1.135	TCP	4410	[TCP segment of a reassembled PDU]
72	19.285406000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=1069 Ack=8146 Win=45568 Len=0 TSval=1102086 TSecr=1665710870
73	19.285614000	150.214.191.176	192.168.1.135	TCP	4410	[TCP segment of a reassembled PDU]
74	19.285619000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=1069 Ack=12490 Win=54272 Len=0 TSval=1102086 TSecr=1665710870
75	19.285621000	150.214.191.176	192.168.1.135	HTTP	1940	HTTP/1.1 200 OK (text/html)
76	19.285623000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=1069 Ack=14364 Win=57984 Len=0 TSval=1102086 TSecr=1665710871
82	24.287641000	150.214.191.176	192.168.1.135	TCP	66	80→58262 [FIN, ACK] Seq=14364 Ack=1069 Win=31232 Len=0 TSval=1665715876 TSecr=1102086
83	24.325316000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [ACK] Seq=1069 Ack=14365 Win=57984 Len=0 TSval=1103346 TSecr=1665715876
127	69.309356000	192.168.1.135	150.214.191.176	TCP	66	[TCP Keep-Alive] 58262→80 [ACK] Seq=1068 Ack=14365 Win=57984 Len=0 TSval=1114592 TSecr=1665715876
128	69.340689000	150.214.191.176	192.168.1.135	TCP	66	[TCP Keep-Alive ACK] 80→58262 [ACK] Seq=14365 Ack=1069 Win=31232 Len=0 TSval=1665760927 TSecr=1103346
137	72.657114000	192.168.1.135	150.214.191.176	TCP	66	58262→80 [FIN, ACK] Seq=1069 Ack=14365 Win=57984 Len=0 TSval=1115428 TSecr=1665760927
151	72.688445000	150.214.191.176	192.168.1.135	TCP	66	80→58262 [ACK] Seq=14365 Ack=1070 Win=31232 Len=0 TSval=1665764275 TSecr=1115428
208	82.406994000	192.168.1.135	150.214.191.176	ICMP	98	Echo (ping) request id=0x1d51, seq=1/256, ttl=64 (no response found!)
209	83.415520000	192.168.1.135	150.214.191.176	ICMP	98	Echo (ping) request id=0x1d51, seq=2/512, ttl=64 (reply in 210)
210	83.446952000	150.214.191.176	192.168.1.135	ICMP	98	Echo (ping) reply id=0x1d51, seq=2/512, ttl=54 (request in 209)
216	84.416841000	192.168.1.135	150.214.191.176	ICMP	98	Echo (ping) request id=0x1d51, seq=3/768, ttl=64 (no response found!)
217	85.423466000	192.168.1.135	150.214.191.176	ICMP	98	Echo (ping) request id=0x1d51, seq=4/1024, ttl=64 (no response found!)

▶ Frame 70: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits) on interface 0
▶ Ethernet II, Src: Micro-St_47:87:ad (44:8a:5b:47:87:ad), Dst: 8c:e1:17:e5:da:2a (8c:e1:17:e5:da:2a)
▶ Internet Protocol Version 4, Src: 192.168.1.135 (192.168.1.135), Dst: 150.214.191.176 (150.214.191.176)
▶ Transmission Control Protocol, Src Port: 58262 (58262), Dst Port: 80 (80), Seq: 511, Ack: 3802, Len: 558
▶ Hypertext Transfer Protocol

```
0000  8c e1 17 e5 da 2a 44 8a  5b 47 87 ad 08 00 45 00   .....*D. [G....E.
0010  02 62 21 61 40 00 40 06  fe 7e c0 a8 01 87 96 d6   .b!a@.@. .~......
0020  bf b0 e3 96 00 50 9f 14  ef e2 88 af 58 91 80 18   .....P.. ....X...
0030  01 20 a2 14 00 00 01 01  08 0a 00 10 d0 fd 63 48   . ...... ......cH
```

eth0: <live capture in progress> ... Packets: 317 · Displayed: 29 (9,1%) Profile: Default

Antes de la presentación en vivo….

¿alguna pregunta?