G3 – M7 _ Seguridad en redes de datos

Informe de Análisis de Vulnerabilidades y Comportamiento de Red

Autor: Carlos Aliendres

25 de agosto de 2025

Introducción:

El objetivo de este informe es documentar y analizar el comportamiento de la red corporativa de Desafío Latam desde el punto de vista de la seguridad. Se emplean herramientas de escaneo y captura de trafico para identificar posibles vulnerabilidades, el estado de la conectividad en la red y patrones de tráfico anómalos.

Para lograr el objetivo se emplearon las siguientes herramientas:

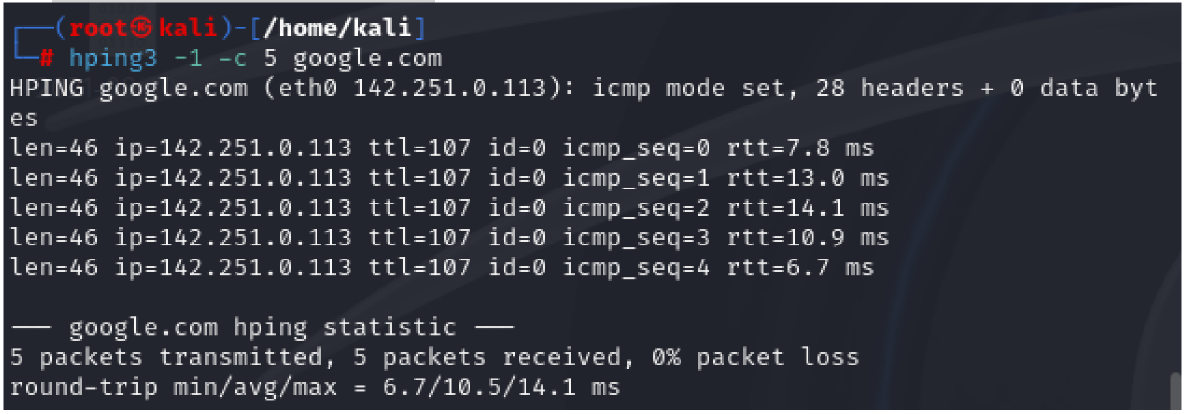
- Hping3
- Wireshark
- Entorno de laboratorio Kali Linux

Además, se realizan una secuencia de pruebas de conectividad, análisis del tráfico generado y se documentan los hallazgos.

Desarrollo:

Uso de **hping3** para envió de diferentes tipos de paquetes a un host objetivo (puede ser google.com o la puerta de enlace local):

- **ICMP** ping normal
  - hping3 -1 -c 5 google.com

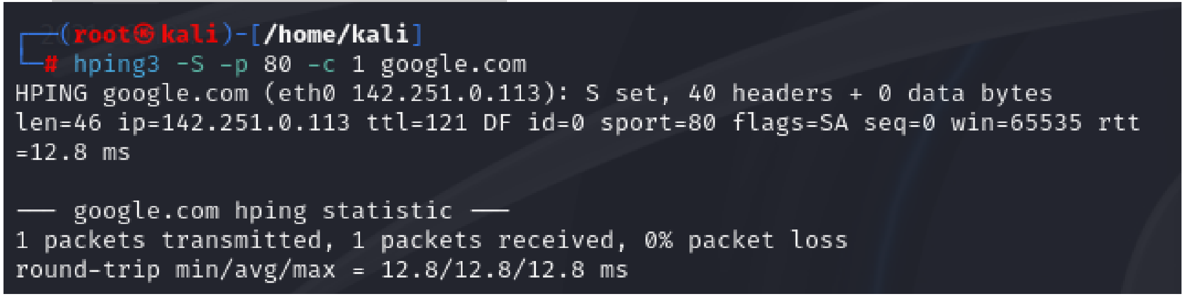


```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -1 -c 5 google.com
HPING google.com (eth0 142.251.0.113): icmp mode set, 28 headers + 0 data byt
es
len=46 ip=142.251.0.113 ttl=107 id=0 icmp_seq=0 rtt=7.8 ms
len=46 ip=142.251.0.113 ttl=107 id=0 icmp_seq=1 rtt=13.0 ms
len=46 ip=142.251.0.113 ttl=107 id=0 icmp_seq=2 rtt=14.1 ms
len=46 ip=142.251.0.113 ttl=107 id=0 icmp_seq=3 rtt=10.9 ms
len=46 ip=142.251.0.113 ttl=107 id=0 icmp_seq=4 rtt=6.7 ms

—— google.com hping statistic ——
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 6.7/10.5/14.1 ms
```

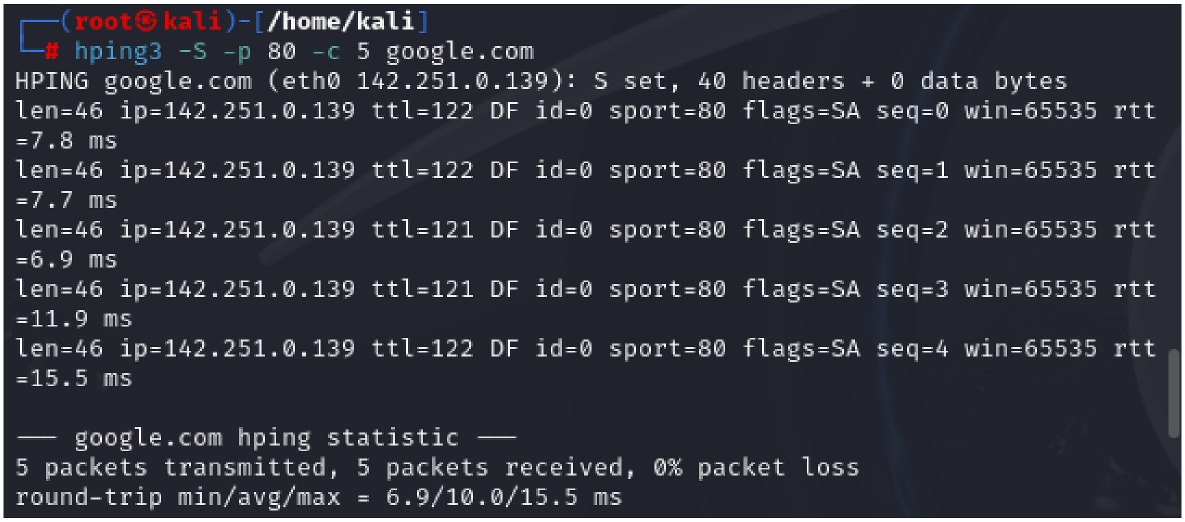
Este comando nos permite verificar la conectividad a un host, medir la latencia y determinar si el host se encuentra activo.

- TCP SYN a puerto 80
  - hping3 -S -p 80 -c 5 google.com



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 80 -c 1 google.com
HPING google.com (eth0 142.251.0.113): S set, 40 headers + 0 data bytes
len=46 ip=142.251.0.113 ttl=121 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt
=12.8 ms

—— google.com hping statistic ——
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.8/12.8/12.8 ms
```

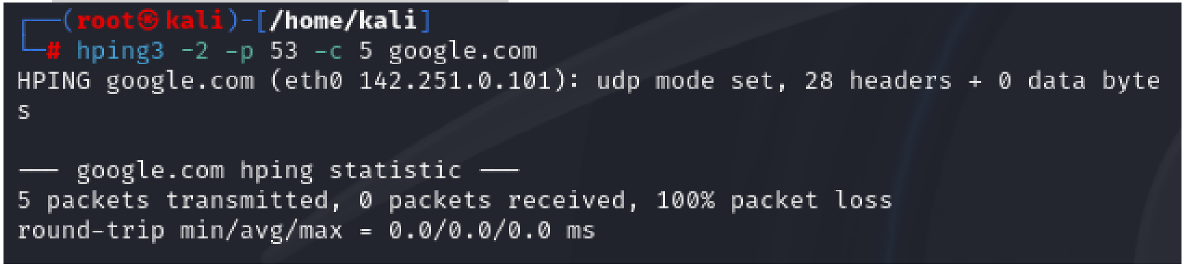


```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 80 -c 5 google.com
HPING google.com (eth0 142.251.0.139): S set, 40 headers + 0 data bytes
len=46 ip=142.251.0.139 ttl=122 DF id=0 sport=80 flags=SA seq=0 win=65535 rtt
=7.8 ms
len=46 ip=142.251.0.139 ttl=122 DF id=0 sport=80 flags=SA seq=1 win=65535 rtt
=7.7 ms
len=46 ip=142.251.0.139 ttl=121 DF id=0 sport=80 flags=SA seq=2 win=65535 rtt
=6.9 ms
len=46 ip=142.251.0.139 ttl=121 DF id=0 sport=80 flags=SA seq=3 win=65535 rtt
=11.9 ms
len=46 ip=142.251.0.139 ttl=122 DF id=0 sport=80 flags=SA seq=4 win=65535 rtt
=15.5 ms

—— google.com hping statistic ——
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 6.9/10.0/15.5 ms
```

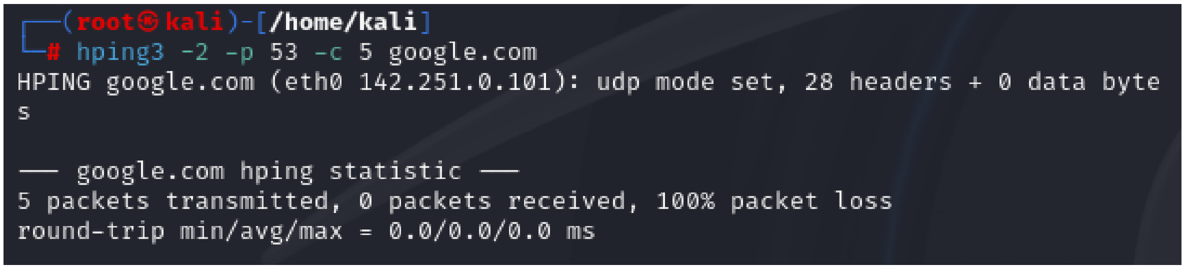
Este comando nos permite identificar que puertos TCP están abiertos en un host y mapear que servicios se ejecutan en el puerto 80

- UDP a puerto 53
    - hping3 -2 -p 53 -c 1 google.com



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -2 -p 53 -c 5 google.com
HPING google.com (eth0 142.251.0.101): udp mode set, 28 headers + 0 data byte
s

--- google.com hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

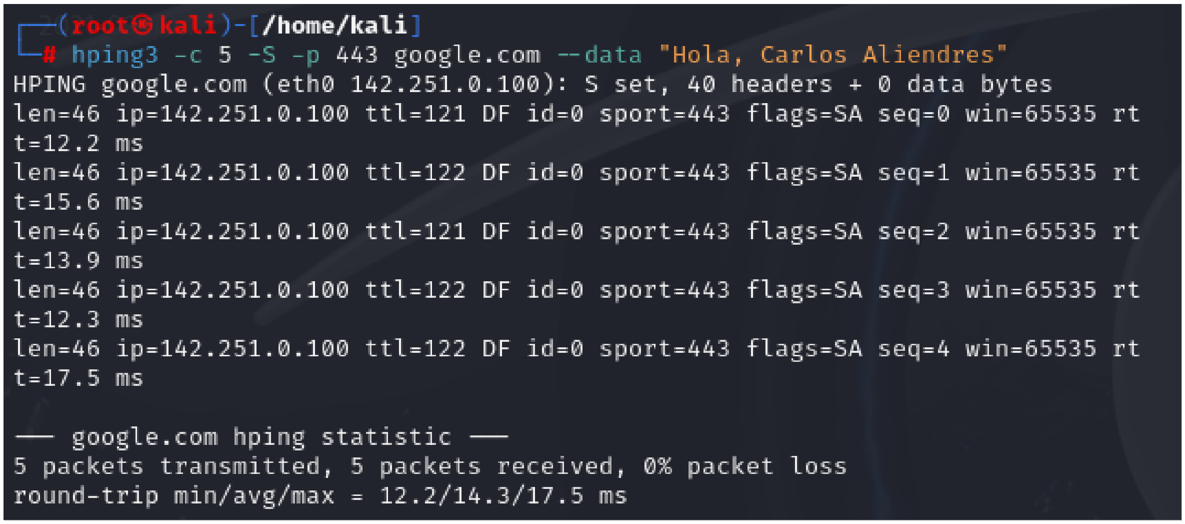


```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -2 -p 53 -c 5 google.com
HPING google.com (eth0 142.251.0.101): udp mode set, 28 headers + 0 data byte
s

--- google.com hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Este comando se usa para realizar escaneos de puertos UDP, este no recibe confirmación de recepción por eso el 100% de paquetes perdidos

- TCP con datos personalizados
    - hping3 -c 5 -S -p 443 google.com --data "Hola, Carlos Aliendres"



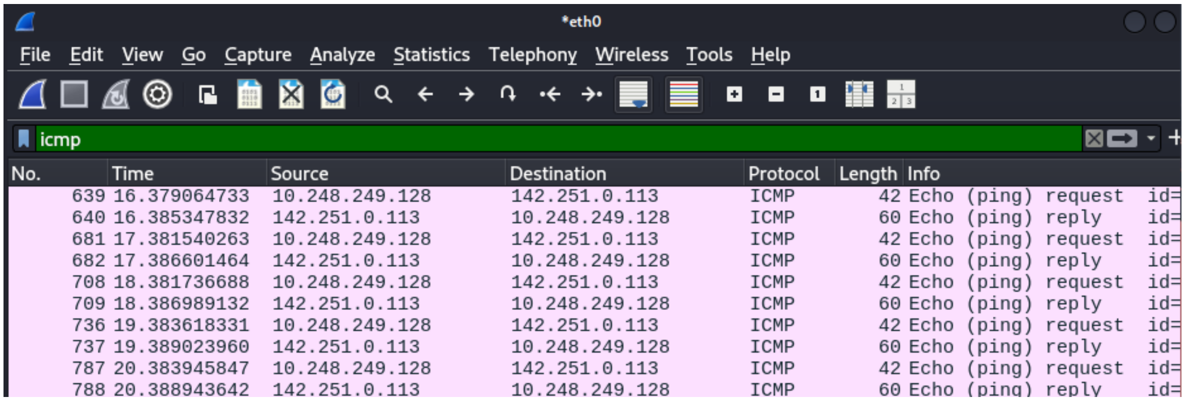
```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -c 5 -S -p 443 google.com --data "Hola, Carlos Aliendres"
HPING google.com (eth0 142.251.0.100): S set, 40 headers + 0 data bytes
len=46 ip=142.251.0.100 ttl=121 DF id=0 sport=443 flags=SA seq=0 win=65535 rt
t=12.2 ms
len=46 ip=142.251.0.100 ttl=122 DF id=0 sport=443 flags=SA seq=1 win=65535 rt
t=15.6 ms
len=46 ip=142.251.0.100 ttl=121 DF id=0 sport=443 flags=SA seq=2 win=65535 rt
t=13.9 ms
len=46 ip=142.251.0.100 ttl=122 DF id=0 sport=443 flags=SA seq=3 win=65535 rt
t=12.3 ms
len=46 ip=142.251.0.100 ttl=122 DF id=0 sport=443 flags=SA seq=4 win=65535 rt
t=17.5 ms

--- google.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 12.2/14.3/17.5 ms
```

Este comando permite probar si el servicio responde a datos personalizados.

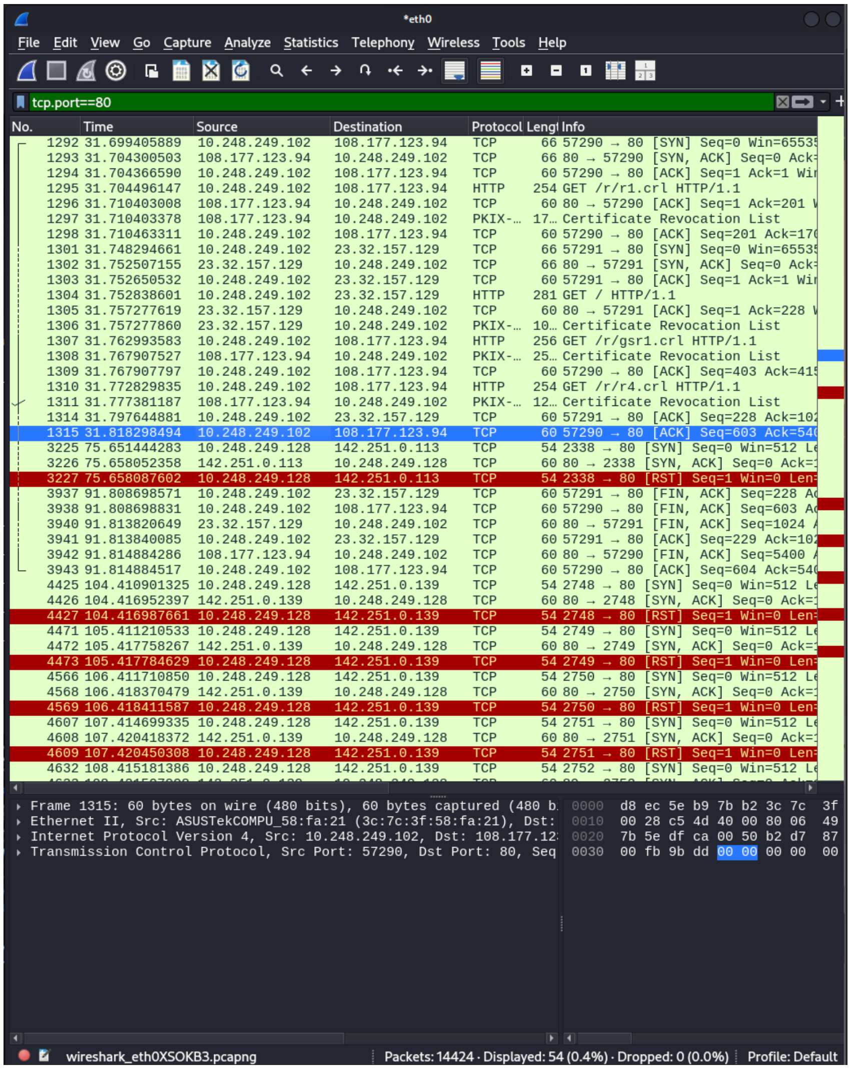
Capturas del tráfico generado con Wireshark durante las pruebas

ICMP



```
icmp
No.  Time             Source          Destination     Protocol Length Info
 639 16.379064733  10.248.249.128  142.251.0.113     ICMP      42 Echo (ping) request  id=
 640 16.385347832  142.251.0.113   10.248.249.128    ICMP      60 Echo (ping) reply    id=
 681 17.381540263  10.248.249.128  142.251.0.113     ICMP      42 Echo (ping) request  id=
 682 17.386601464  142.251.0.113   10.248.249.128    ICMP      60 Echo (ping) reply    id=
 708 18.381736688  10.248.249.128  142.251.0.113     ICMP      42 Echo (ping) request  id=
 709 18.386989132  142.251.0.113   10.248.249.128    ICMP      60 Echo (ping) reply    id=
 736 19.383618331  10.248.249.128  142.251.0.113     ICMP      42 Echo (ping) request  id=
 737 19.389023960  142.251.0.113   10.248.249.128    ICMP      60 Echo (ping) reply    id=
 787 20.383945847  10.248.249.128  142.251.0.113     ICMP      42 Echo (ping) request  id=
 788 20.388943642  142.251.0.113   10.248.249.128    ICMP      60 Echo (ping) reply    id=
```

TCP.PORT==80

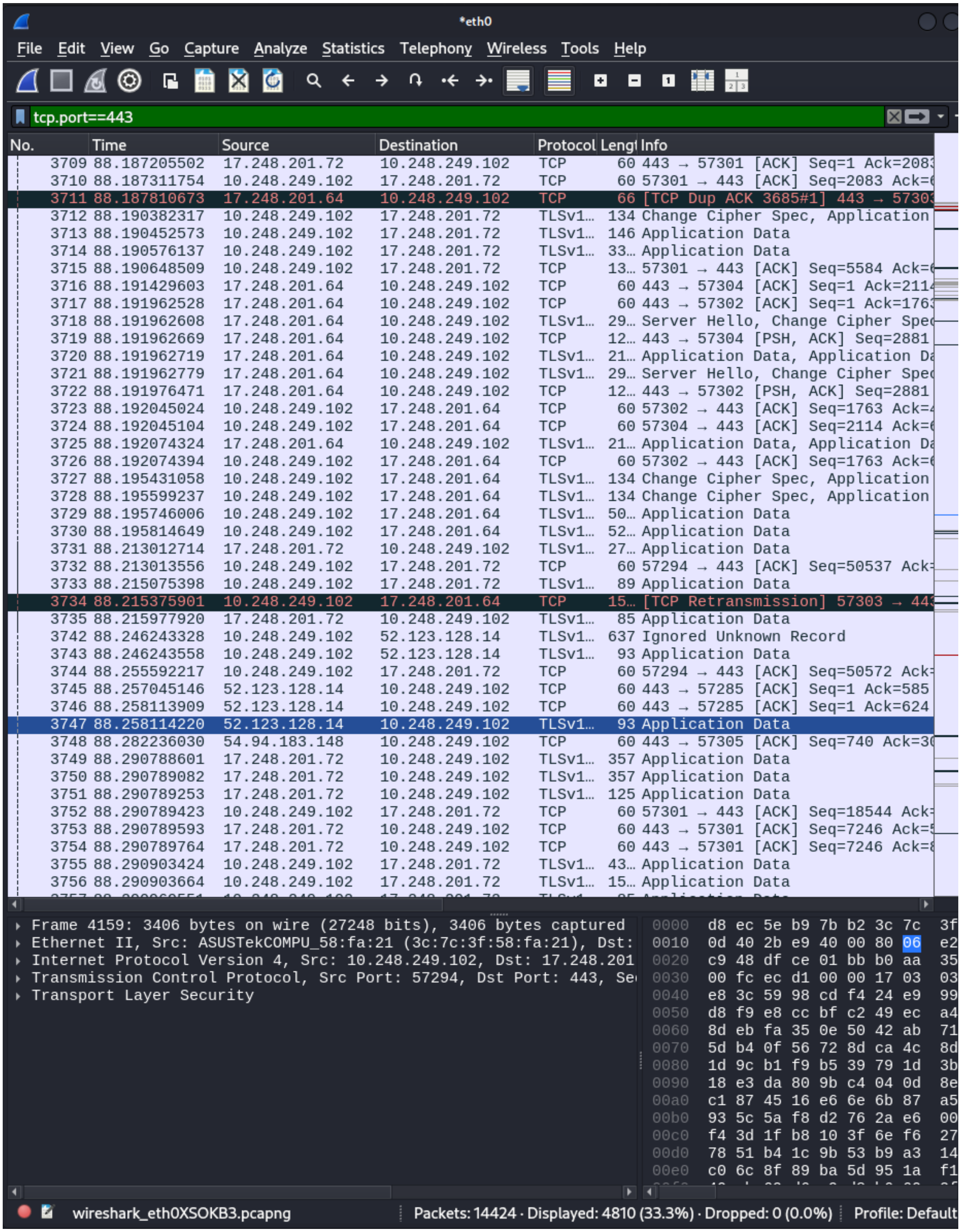


```
tcp.port==80
No.   Time          Source          Destination     Protocol Lengt Info
 1292 31.699405889 10.248.249.102  108.177.123.94  TCP       66 57290 → 80 [SYN] Seq=0 Win=65535
 1293 31.704300503 108.177.123.94  10.248.249.102  TCP       66 80 → 57290 [SYN, ACK] Seq=0 Ack=
 1294 31.704366590 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [ACK] Seq=1 Ack=1 Wir
 1295 31.704496147 10.248.249.102  108.177.123.94  HTTP     254 GET /r/r1.crl HTTP/1.1
 1296 31.710403008 108.177.123.94  10.248.249.102  TCP       60 80 → 57290 [ACK] Seq=1 Ack=201 W
 1297 31.710403378 108.177.123.94  10.248.249.102  PKIX-…   17… Certificate Revocation List
 1298 31.710463311 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [ACK] Seq=201 Ack=170
 1301 31.748294661 10.248.249.102  23.32.157.129   TCP       66 57291 → 80 [SYN] Seq=0 Win=65535
 1302 31.752507155 23.32.157.129   10.248.249.102  TCP       66 80 → 57291 [SYN, ACK] Seq=0 Ack=
 1303 31.752650532 10.248.249.102  23.32.157.129   TCP       60 57291 → 80 [ACK] Seq=1 Ack=1 Wir
 1304 31.752838601 10.248.249.102  23.32.157.129   HTTP     281 GET / HTTP/1.1
 1305 31.757277619 23.32.157.129   10.248.249.102  TCP       60 80 → 57291 [ACK] Seq=1 Ack=228 W
 1306 31.757277860 23.32.157.129   10.248.249.102  PKIX-…   10… Certificate Revocation List
 1307 31.762993583 10.248.249.102  108.177.123.94  HTTP     256 GET /r/gsr1.crl HTTP/1.1
 1308 31.767907527 108.177.123.94  10.248.249.102  PKIX-…   25… Certificate Revocation List
 1309 31.767907797 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [ACK] Seq=403 Ack=415
 1310 31.772829835 10.248.249.102  108.177.123.94  HTTP     254 GET /r/r4.crl HTTP/1.1
 1311 31.777381187 108.177.123.94  10.248.249.102  PKIX-…   12… Certificate Revocation List
 1314 31.797644881 10.248.249.102  23.32.157.129   TCP       60 57291 → 80 [ACK] Seq=228 Ack=102
 1315 31.818298494 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [ACK] Seq=603 Ack=540
 3225 75.651444283 10.248.249.128  142.251.0.113   TCP       54 2338 → 80 [SYN] Seq=0 Win=512 Le
 3226 75.658052358 142.251.0.113   10.248.249.128  TCP       60 80 → 2338 [SYN, ACK] Seq=0 Ack=1
 3227 75.658087602 10.248.249.128  142.251.0.113   TCP       54 2338 → 80 [RST] Seq=1 Win=0 Len=
 3937 91.808698571 10.248.249.102  23.32.157.129   TCP       60 57291 → 80 [FIN, ACK] Seq=228 Ac
 3938 91.808698831 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [FIN, ACK] Seq=603 Ac
 3940 91.813820649 23.32.157.129   10.248.249.102  TCP       60 80 → 57291 [FIN, ACK] Seq=1024 A
 3941 91.813840085 10.248.249.102  23.32.157.129   TCP       60 57291 → 80 [ACK] Seq=229 Ack=102
 3942 91.814884286 108.177.123.94  10.248.249.102  TCP       60 80 → 57290 [FIN, ACK] Seq=5400 A
 3943 91.814884517 10.248.249.102  108.177.123.94  TCP       60 57290 → 80 [ACK] Seq=604 Ack=540
 4425 104.410901325 10.248.249.128 142.251.0.139   TCP       54 2748 → 80 [SYN] Seq=0 Win=512 Le
 4426 104.416952397 142.251.0.139  10.248.249.128  TCP       60 80 → 2748 [SYN, ACK] Seq=0 Ack=1
 4427 104.416987661 10.248.249.128 142.251.0.139   TCP       54 2748 → 80 [RST] Seq=1 Win=0 Len=
 4471 105.411210533 10.248.249.128 142.251.0.139   TCP       54 2749 → 80 [SYN] Seq=0 Win=512 Le
 4472 105.417758267 142.251.0.139  10.248.249.128  TCP       60 80 → 2749 [SYN, ACK] Seq=0 Ack=1
 4473 105.417784629 10.248.249.128 142.251.0.139   TCP       54 2749 → 80 [RST] Seq=1 Win=0 Len=
 4566 106.411710850 10.248.249.128 142.251.0.139   TCP       54 2750 → 80 [SYN] Seq=0 Win=512 Le
 4568 106.418370479 142.251.0.139  10.248.249.128  TCP       60 80 → 2750 [SYN, ACK] Seq=0 Ack=1
 4569 106.418411587 10.248.249.128 142.251.0.139   TCP       54 2750 → 80 [RST] Seq=1 Win=0 Len=
 4607 107.414699335 10.248.249.128 142.251.0.139   TCP       54 2751 → 80 [SYN] Seq=0 Win=512 Le
 4608 107.420418372 142.251.0.139  10.248.249.128  TCP       60 80 → 2751 [SYN, ACK] Seq=0 Ack=1
 4609 107.420450308 10.248.249.128 142.251.0.139   TCP       54 2751 → 80 [RST] Seq=1 Win=0 Len=
 4632 108.415181386 10.248.249.128 142.251.0.139   TCP       54 2752 → 80 [SYN] Seq=0 Win=512 Le

› Frame 1315: 60 bytes on wire (480 bits), 60 bytes captured (480 b    0000  d8 ec 5e b9 7b b2 3c 7c  3f
› Ethernet II, Src: ASUSTekCOMPU_58:fa:21 (3c:7c:3f:58:fa:21), Dst:    0010  00 28 c5 4d 40 00 80 06  49
› Internet Protocol Version 4, Src: 10.248.249.102, Dst: 108.177.12    0020  7b 5e df ca 00 50 b2 d7  87
› Transmission Control Protocol, Src Port: 57290, Dst Port: 80, Seq    0030  00 fb 9b dd 00 00 00 00  00

wireshark_eth0XSOKB3.pcapng    Packets: 14424 · Displayed: 54 (0.4%) · Dropped: 0 (0.0%)    Profile: Default
```

TCP.PORT== 443


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==443

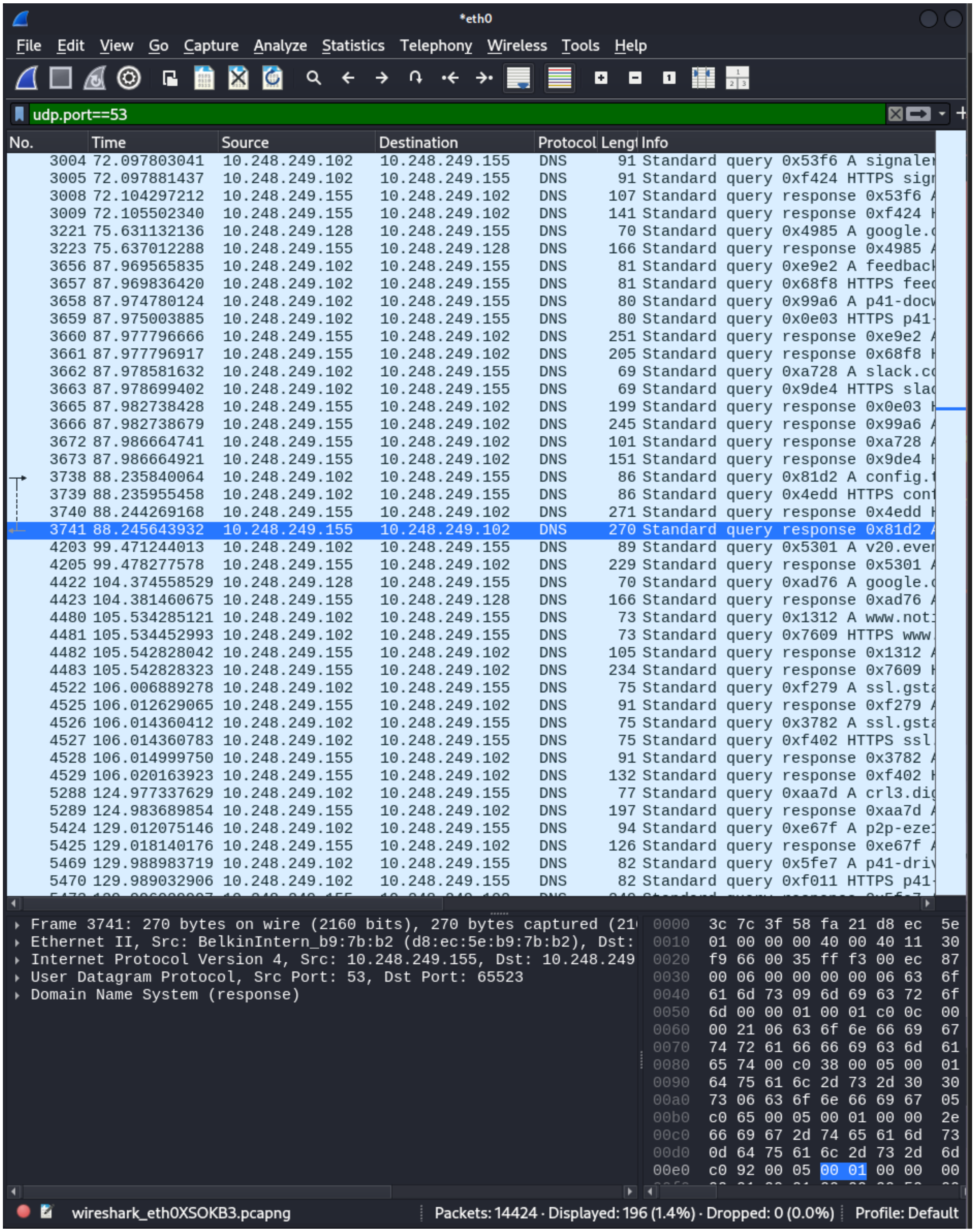
```
No.   Time          Source          Destination     Protocol Lengt Info
 3709 88.187205502  17.248.201.72   10.248.249.102  TCP       60 443 → 57301 [ACK] Seq=1 Ack=208
 3710 88.187311754  10.248.249.102  17.248.201.72   TCP       60 57301 → 443 [ACK] Seq=2083 Ack=
 3711 88.187810673  17.248.201.64   10.248.249.102  TCP       66 [TCP Dup ACK 3685#1] 443 → 5730
 3712 88.190382317  10.248.249.102  17.248.201.72   TLSv1…   134 Change Cipher Spec, Application
 3713 88.190452573  10.248.249.102  17.248.201.72   TLSv1…   146 Application Data
 3714 88.190576137  10.248.249.102  17.248.201.72   TLSv1…   33… Application Data
 3715 88.190648509  10.248.249.102  17.248.201.72   TCP      13… 57301 → 443 [ACK] Seq=5584 Ack=
 3716 88.191429603  17.248.201.64   10.248.249.102  TCP       60 443 → 57304 [ACK] Seq=1 Ack=211
 3717 88.191962528  17.248.201.64   10.248.249.102  TCP       60 443 → 57302 [ACK] Seq=1 Ack=176
 3718 88.191962608  17.248.201.64   10.248.249.102  TLSv1…   29… Server Hello, Change Cipher Spe
 3719 88.191962669  17.248.201.64   10.248.249.102  TCP      12… 443 → 57304 [PSH, ACK] Seq=2881
 3720 88.191962719  17.248.201.64   10.248.249.102  TLSv1…   21… Application Data, Application Da
 3721 88.191962779  17.248.201.64   10.248.249.102  TLSv1…   29… Server Hello, Change Cipher Spe
 3722 88.191976471  17.248.201.64   10.248.249.102  TCP      12… 443 → 57302 [PSH, ACK] Seq=2881
 3723 88.192045024  10.248.249.102  17.248.201.64   TCP       60 57302 → 443 [ACK] Seq=1763 Ack=
 3724 88.192045104  10.248.249.102  17.248.201.64   TCP       60 57304 → 443 [ACK] Seq=2114 Ack=
 3725 88.192074324  17.248.201.64   10.248.249.102  TLSv1…   21… Application Data, Application Da
 3726 88.192074394  10.248.249.102  17.248.201.64   TCP       60 57302 → 443 [ACK] Seq=1763 Ack=
 3727 88.195431058  10.248.249.102  17.248.201.64   TLSv1…   134 Change Cipher Spec, Application
 3728 88.195599237  10.248.249.102  17.248.201.64   TLSv1…   134 Change Cipher Spec, Application
 3729 88.195746006  10.248.249.102  17.248.201.64   TLSv1…   50… Application Data
 3730 88.195814649  10.248.249.102  17.248.201.64   TLSv1…   52… Application Data
 3731 88.213012714  17.248.201.72   10.248.249.102  TLSv1…   27… Application Data
 3732 88.213013556  10.248.249.102  17.248.201.72   TCP       60 57294 → 443 [ACK] Seq=50537 Ack
 3733 88.215075398  10.248.249.102  17.248.201.72   TLSv1…    89 Application Data
 3734 88.215375901  10.248.249.102  17.248.201.64   TCP      15… [TCP Retransmission] 57303 → 44
 3735 88.215977920  17.248.201.72   10.248.249.102  TLSv1…    85 Application Data
 3742 88.246243328  10.248.249.102  52.123.128.14   TLSv1…   637 Ignored Unknown Record
 3743 88.246243558  10.248.249.102  52.123.128.14   TLSv1…    93 Application Data
 3744 88.255592217  10.248.249.102  17.248.201.72   TCP       60 57294 → 443 [ACK] Seq=50572 Ack
 3745 88.257045146  52.123.128.14   10.248.249.102  TCP       60 443 → 57285 [ACK] Seq=1 Ack=585
 3746 88.258113909  52.123.128.14   10.248.249.102  TCP       60 443 → 57285 [ACK] Seq=1 Ack=624
 3747 88.258114220  52.123.128.14   10.248.249.102  TLSv1…    93 Application Data
 3748 88.282236030  54.94.183.148   10.248.249.102  TCP       60 443 → 57305 [ACK] Seq=740 Ack=3
 3749 88.290788601  17.248.201.72   10.248.249.102  TLSv1…   357 Application Data
 3750 88.290789082  17.248.201.72   10.248.249.102  TLSv1…   357 Application Data
 3751 88.290789253  17.248.201.72   10.248.249.102  TLSv1…   125 Application Data
 3752 88.290789423  10.248.249.102  17.248.201.72   TCP       60 57301 → 443 [ACK] Seq=18544 Ack
 3753 88.290789593  17.248.201.72   10.248.249.102  TCP       60 443 → 57301 [ACK] Seq=7246 Ack=
 3754 88.290789764  17.248.201.72   10.248.249.102  TCP       60 443 → 57301 [ACK] Seq=7246 Ack=
 3755 88.290903424  10.248.249.102  17.248.201.72   TLSv1…   43… Application Data
 3756 88.290903664  10.248.249.102  17.248.201.72   TLSv1…   15… Application Data
```

```
▸ Frame 4159: 3406 bytes on wire (27248 bits), 3406 bytes captured
▸ Ethernet II, Src: ASUSTekCOMPU_58:fa:21 (3c:7c:3f:58:fa:21), Dst:
▸ Internet Protocol Version 4, Src: 10.248.249.102, Dst: 17.248.201
▸ Transmission Control Protocol, Src Port: 57294, Dst Port: 443, Se
▸ Transport Layer Security
```

```
0000  d8 ec 5e b9 7b b2 3c 7c  3f
0010  0d 40 2b e9 40 00 80 06  e2
0020  c9 48 df ce 01 bb b0 aa  35
0030  00 fc ec d1 00 00 17 03  03
0040  e8 3c 59 98 cd f4 24 e9  99
0050  d8 f9 e8 cc bf c2 49 ec  a4
0060  8d eb fa 35 0e 50 42 ab  71
0070  5d b4 0f 56 72 8d ca 4c  8d
0080  1d 9c b1 f9 b5 39 79 1d  3b
0090  18 e3 da 80 9b c4 04 0d  8e
00a0  c1 87 45 16 e6 6e 6b 87  a5
00b0  93 5c 5a f8 d2 76 2a e6  00
00c0  f4 3d 1f b8 10 3f 6e f6  27
00d0  78 51 b4 1c 9b 53 b9 a3  14
00e0  c0 6c 8f 89 ba 5d 95 1a  f1
```

wireshark_eth0XSOKB3.pcapng | Packets: 14424 · Displayed: 4810 (33.3%) · Dropped: 0 (0.0%) | Profile: Default

UDP.PORT==53


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port==53
```

```
No.    Time          Source          Destination     Protocol Lengt Info
  3004 72.097803041  10.248.249.102  10.248.249.155  DNS       91 Standard query 0x53f6 A signaler
  3005 72.097881437  10.248.249.102  10.248.249.155  DNS       91 Standard query 0xf424 HTTPS sigr
  3008 72.104297212  10.248.249.155  10.248.249.102  DNS      107 Standard query response 0x53f6 A
  3009 72.105502340  10.248.249.155  10.248.249.102  DNS      141 Standard query response 0xf424 H
  3221 75.631132136  10.248.249.128  10.248.249.155  DNS       70 Standard query 0x4985 A google.c
  3223 75.637012288  10.248.249.155  10.248.249.128  DNS      166 Standard query response 0x4985 A
  3656 87.969565835  10.248.249.102  10.248.249.155  DNS       81 Standard query 0xe9e2 A feedback
  3657 87.969836420  10.248.249.102  10.248.249.155  DNS       81 Standard query 0x68f8 HTTPS feed
  3658 87.974780124  10.248.249.102  10.248.249.155  DNS       80 Standard query 0x99a6 A p41-docw
  3659 87.975003885  10.248.249.102  10.248.249.155  DNS       80 Standard query 0x0e03 HTTPS p41-
  3660 87.977796666  10.248.249.155  10.248.249.102  DNS      251 Standard query response 0xe9e2 A
  3661 87.977796917  10.248.249.155  10.248.249.102  DNS      205 Standard query response 0x68f8 H
  3662 87.978581632  10.248.249.102  10.248.249.155  DNS       69 Standard query 0xa728 A slack.co
  3663 87.978699402  10.248.249.102  10.248.249.155  DNS       69 Standard query 0x9de4 HTTPS slac
  3665 87.982738428  10.248.249.155  10.248.249.102  DNS      199 Standard query response 0x0e03 H
  3666 87.982738679  10.248.249.155  10.248.249.102  DNS      245 Standard query response 0x99a6 A
  3672 87.986664741  10.248.249.155  10.248.249.102  DNS      101 Standard query response 0xa728 A
  3673 87.986664921  10.248.249.155  10.248.249.102  DNS      151 Standard query response 0x9de4 H
  3738 88.235840064  10.248.249.102  10.248.249.155  DNS       86 Standard query 0x81d2 A config.t
  3739 88.235955458  10.248.249.102  10.248.249.155  DNS       86 Standard query 0x4edd HTTPS conf
  3740 88.244269168  10.248.249.155  10.248.249.102  DNS      271 Standard query response 0x4edd H
  3741 88.245643932  10.248.249.155  10.248.249.102  DNS      270 Standard query response 0x81d2 A
  4203 99.471244013  10.248.249.102  10.248.249.155  DNS       89 Standard query 0x5301 A v20.ever
  4205 99.478277578  10.248.249.155  10.248.249.102  DNS      229 Standard query response 0x5301 A
  4422 104.374558529 10.248.249.128  10.248.249.155  DNS       70 Standard query 0xad76 A google.c
  4423 104.381460675 10.248.249.155  10.248.249.128  DNS      166 Standard query response 0xad76 A
  4480 105.534285121 10.248.249.102  10.248.249.155  DNS       73 Standard query 0x1312 A www.noti
  4481 105.534452993 10.248.249.102  10.248.249.155  DNS       73 Standard query 0x7609 HTTPS www.
  4482 105.542828042 10.248.249.155  10.248.249.102  DNS      105 Standard query response 0x1312 A
  4483 105.542828323 10.248.249.155  10.248.249.102  DNS      234 Standard query response 0x7609 H
  4522 106.006889278 10.248.249.102  10.248.249.155  DNS       75 Standard query 0xf279 A ssl.gsta
  4525 106.012629065 10.248.249.155  10.248.249.102  DNS       91 Standard query response 0xf279 A
  4526 106.014360412 10.248.249.102  10.248.249.155  DNS       75 Standard query 0x3782 A ssl.gsta
  4527 106.014360783 10.248.249.102  10.248.249.155  DNS       75 Standard query 0xf402 HTTPS ssl.
  4528 106.014999750 10.248.249.155  10.248.249.102  DNS       91 Standard query response 0x3782 A
  4529 106.020163923 10.248.249.155  10.248.249.102  DNS      132 Standard query response 0xf402 H
  5288 124.977337629 10.248.249.102  10.248.249.155  DNS       77 Standard query 0xaa7d A crl3.dig
  5289 124.983689854 10.248.249.155  10.248.249.102  DNS      197 Standard query response 0xaa7d A
  5424 129.012075146 10.248.249.102  10.248.249.155  DNS       94 Standard query 0xe67f A p2p-eze1
  5425 129.018140176 10.248.249.155  10.248.249.102  DNS      126 Standard query response 0xe67f A
  5469 129.988983719 10.248.249.102  10.248.249.155  DNS       82 Standard query 0x5fe7 A p41-driv
  5470 129.989032906 10.248.249.102  10.248.249.155  DNS       82 Standard query 0xf011 HTTPS p41-
```

```
› Frame 3741: 270 bytes on wire (2160 bits), 270 bytes captured (21
› Ethernet II, Src: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2), Dst:
› Internet Protocol Version 4, Src: 10.248.249.155, Dst: 10.248.249
› User Datagram Protocol, Src Port: 53, Dst Port: 65523
› Domain Name System (response)
```

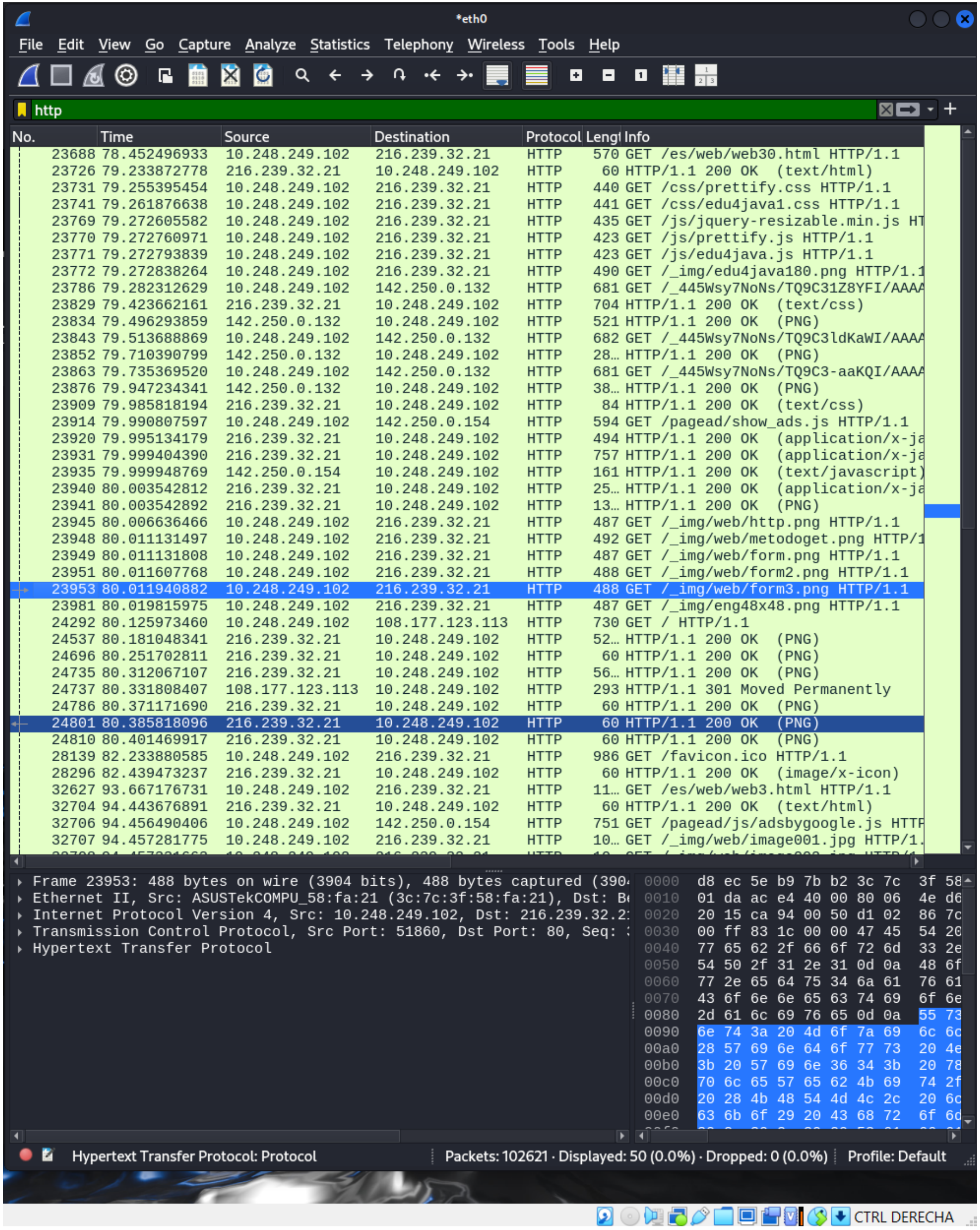
```
0000  3c 7c 3f 58 fa 21 d8 ec  5e
0010  01 00 00 00 40 00 40 11  30
0020  f9 66 00 35 ff f3 00 ec  87
0030  00 06 00 00 00 00 06 63  6f
0040  61 6d 73 09 6d 69 63 72  6f
0050  6d 00 00 01 00 01 c0 0c  00
0060  00 21 06 63 6f 6e 66 69  67
0070  74 72 61 66 66 69 63 6d  61
0080  65 74 00 c0 38 00 05 00  01
0090  64 75 61 6c 2d 73 2d 30  30
00a0  73 06 63 6f 6e 66 69 67  05
00b0  c0 65 00 05 00 01 00 00  2e
00c0  66 69 67 2d 74 65 61 6d  73
00d0  0d 64 75 61 6c 2d 73 2d  6d
00e0  c0 92 00 05 00 01 00 00  00
```

wireshark_eth0XSOKB3.pcapng | Packets: 14424 · Displayed: 196 (1.4%) · Dropped: 0 (0.0%) | Profile: Default

Captura y Análisis de Tráfico con Wireshark Realizar una sesión de captura de tráfico de red durante 10-15 minutos mientras navegas por diferentes sitios web:

a) Acceder a al menos 5 sitios web diferentes (incluir HTTP y HTTPS)
b) Realizar una descarga de archivo pequeño
c) Enviar un correo electrónico o usar una aplicación de mensajería
d) Aplicar los siguientes filtros en Wireshark y documentar los resultados:

- http - Tráfico HTTP


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

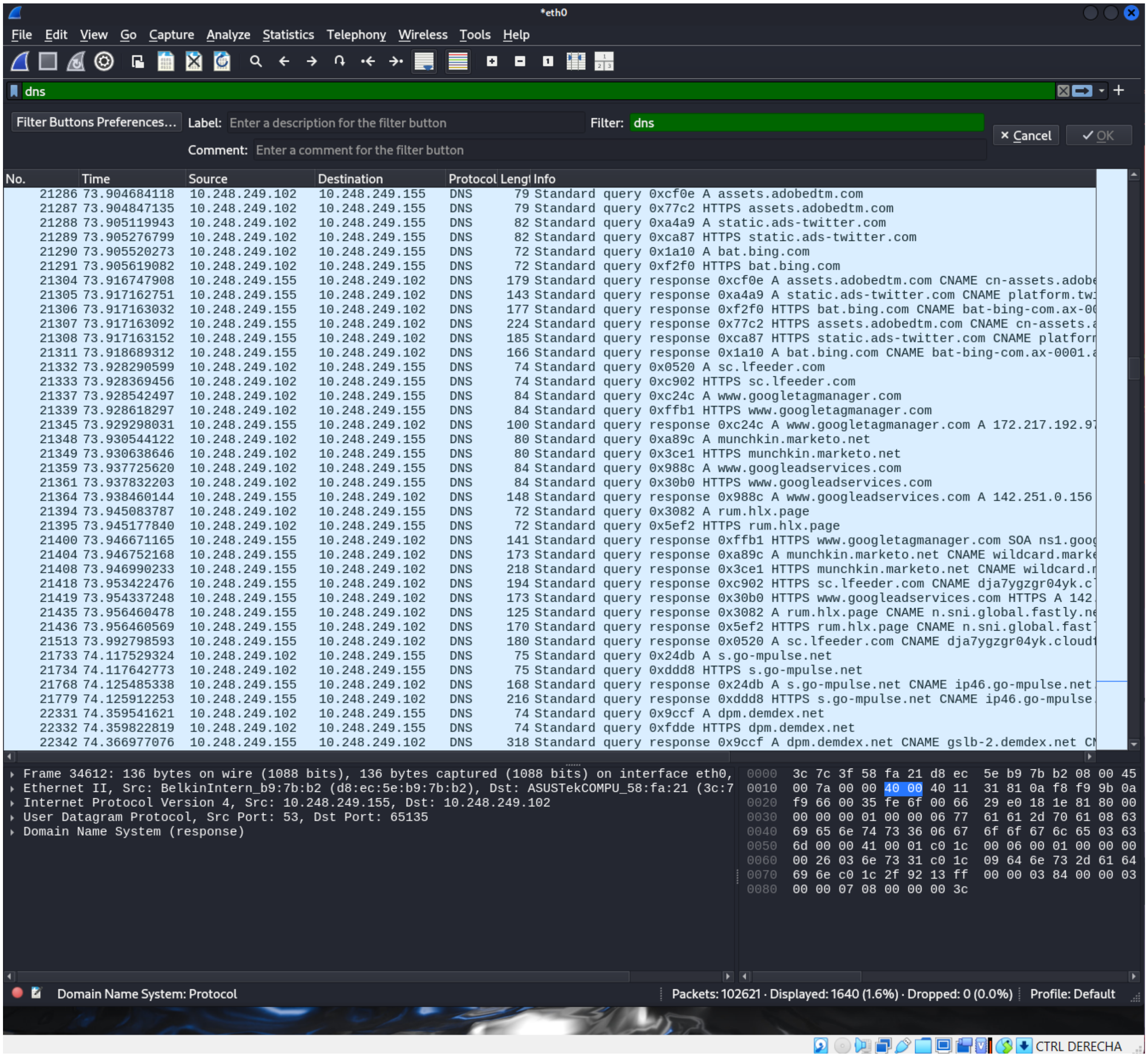
```
No.   Time         Source          Destination     Protocol Lengt Info
23688 78.452496933 10.248.249.102  216.239.32.21   HTTP     570 GET /es/web/web30.html HTTP/1.1
23726 79.233872778 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (text/html)
23731 79.255395454 10.248.249.102  216.239.32.21   HTTP     440 GET /css/prettify.css HTTP/1.1
23741 79.261876638 10.248.249.102  216.239.32.21   HTTP     441 GET /css/edu4java1.css HTTP/1.1
23769 79.272605582 10.248.249.102  216.239.32.21   HTTP     435 GET /js/jquery-resizable.min.js HT
23770 79.272760971 10.248.249.102  216.239.32.21   HTTP     423 GET /js/prettify.js HTTP/1.1
23771 79.272793839 10.248.249.102  216.239.32.21   HTTP     423 GET /js/edu4java.js HTTP/1.1
23772 79.272838264 10.248.249.102  216.239.32.21   HTTP     490 GET /_img/edu4java180.png HTTP/1.1
23786 79.282312629 10.248.249.102  142.250.0.132   HTTP     681 GET /_445Wsy7NoNs/TQ9C31Z8YFI/AAAA
23829 79.423662161 216.239.32.21   10.248.249.102  HTTP     704 HTTP/1.1 200 OK  (text/css)
23834 79.496293859 142.250.0.132   10.248.249.102  HTTP     521 HTTP/1.1 200 OK  (PNG)
23843 79.513688869 10.248.249.102  142.250.0.132   HTTP     682 GET /_445Wsy7NoNs/TQ9C3ldKaWI/AAAA
23852 79.710390799 142.250.0.132   10.248.249.102  HTTP     28… HTTP/1.1 200 OK  (PNG)
23863 79.735369520 10.248.249.102  142.250.0.132   HTTP     681 GET /_445Wsy7NoNs/TQ9C3-aaKQI/AAAA
23876 79.947234341 142.250.0.132   10.248.249.102  HTTP     38… HTTP/1.1 200 OK  (PNG)
23909 79.985818194 216.239.32.21   10.248.249.102  HTTP      84 HTTP/1.1 200 OK  (text/css)
23914 79.990807597 10.248.249.102  142.250.0.154   HTTP     594 GET /pagead/show_ads.js HTTP/1.1
23920 79.995134179 216.239.32.21   10.248.249.102  HTTP     494 HTTP/1.1 200 OK  (application/x-ja
23931 79.999404390 216.239.32.21   10.248.249.102  HTTP     757 HTTP/1.1 200 OK  (application/x-ja
23935 79.999948769 142.250.0.154   10.248.249.102  HTTP     161 HTTP/1.1 200 OK  (text/javascript)
23940 80.003542812 216.239.32.21   10.248.249.102  HTTP     25… HTTP/1.1 200 OK  (application/x-ja
23941 80.003542892 216.239.32.21   10.248.249.102  HTTP     13… HTTP/1.1 200 OK  (PNG)
23945 80.006636466 10.248.249.102  216.239.32.21   HTTP     487 GET /_img/web/http.png HTTP/1.1
23948 80.011131497 10.248.249.102  216.239.32.21   HTTP     492 GET /_img/web/metodoget.png HTTP/1
23949 80.011131808 10.248.249.102  216.239.32.21   HTTP     487 GET /_img/web/form.png HTTP/1.1
23951 80.011607768 10.248.249.102  216.239.32.21   HTTP     488 GET /_img/web/form2.png HTTP/1.1
23953 80.011940882 10.248.249.102  216.239.32.21   HTTP     488 GET /_img/web/form3.png HTTP/1.1
23981 80.019815975 10.248.249.102  216.239.32.21   HTTP     487 GET /_img/eng48x48.png HTTP/1.1
24292 80.125973460 10.248.249.102  108.177.123.113 HTTP     730 GET / HTTP/1.1
24537 80.181048341 216.239.32.21   10.248.249.102  HTTP     52… HTTP/1.1 200 OK  (PNG)
24696 80.251702811 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (PNG)
24735 80.312067107 216.239.32.21   10.248.249.102  HTTP     56… HTTP/1.1 200 OK  (PNG)
24737 80.331808407 108.177.123.113 10.248.249.102  HTTP     293 HTTP/1.1 301 Moved Permanently
24786 80.371171690 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (PNG)
24801 80.385818096 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (PNG)
24810 80.401469917 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (PNG)
28139 82.233880585 10.248.249.102  216.239.32.21   HTTP     986 GET /favicon.ico HTTP/1.1
28296 82.439473237 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (image/x-icon)
32627 93.667176731 10.248.249.102  216.239.32.21   HTTP     11… GET /es/web/web3.html HTTP/1.1
32704 94.443676891 216.239.32.21   10.248.249.102  HTTP      60 HTTP/1.1 200 OK  (text/html)
32706 94.456490406 10.248.249.102  142.250.0.154   HTTP     751 GET /pagead/js/adsbygoogle.js HTTP
32707 94.457281775 10.248.249.102  216.239.32.21   HTTP     10… GET /_img/web/image001.jpg HTTP/1.
```

```
▸ Frame 23953: 488 bytes on wire (3904 bits), 488 bytes captured (3904
▸ Ethernet II, Src: ASUSTekCOMPU_58:fa:21 (3c:7c:3f:58:fa:21), Dst: Be
▸ Internet Protocol Version 4, Src: 10.248.249.102, Dst: 216.239.32.2
▸ Transmission Control Protocol, Src Port: 51860, Dst Port: 80, Seq: 
▸ Hypertext Transfer Protocol
```

```
0000  d8 ec 5e b9 7b b2 3c 7c  3f 58
0010  01 da ac e4 40 00 80 06  4e d6
0020  20 15 ca 94 00 50 d1 02  86 7c
0030  00 ff 83 1c 00 00 47 45  54 20
0040  77 65 62 2f 66 6f 72 6d  33 2e
0050  54 50 2f 31 2e 31 0d 0a  48 6f
0060  77 2e 65 64 75 34 6a 61  76 61
0070  43 6f 6e 6e 65 63 74 69  6f 6e
0080  2d 61 6c 69 76 65 0d 0a  55 73
0090  6e 74 3a 20 4d 6f 7a 69  6c 6c
00a0  28 57 69 6e 64 6f 77 73  20 4e
00b0  3b 20 57 69 6e 36 34 3b  20 78
00c0  70 6c 65 57 65 62 4b 69  74 2f
00d0  20 28 4b 48 54 4d 4c 2c  20 6c
00e0  63 6b 6f 29 20 43 68 72  6f 6d
```

Hypertext Transfer Protocol: Protocol | Packets: 102621 · Displayed: 50 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

- dns - Consultas DNS


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Filter Buttons Preferences...
Label: Enter a description for the filter button
Comment: Enter a comment for the filter button
✕ Cancel
✓ OK
CTRL DERECHA

Filter: dns

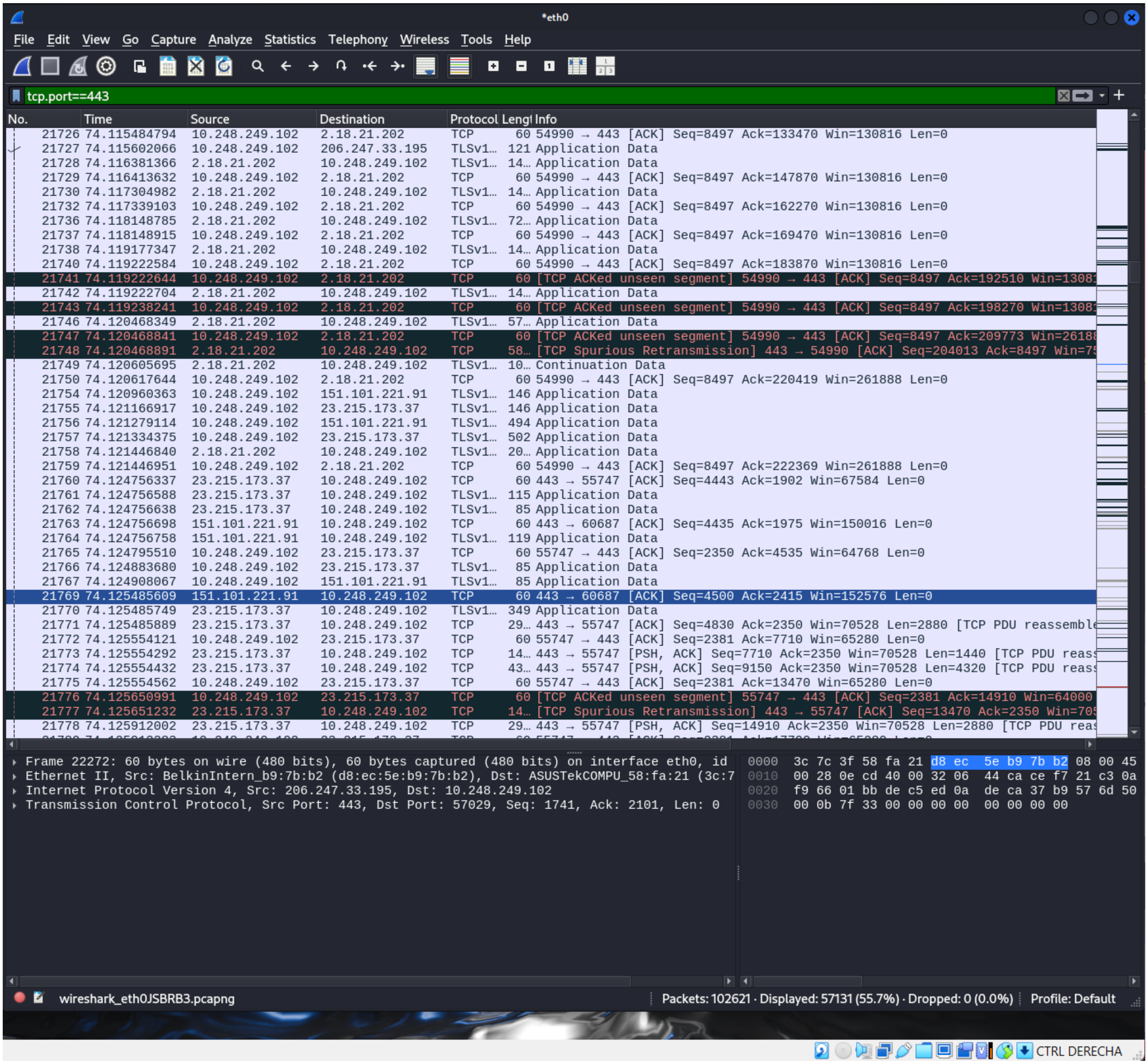
```
No.     Time          Source          Destination     Protocol Lengt Info
  21286 73.904684118  10.248.249.102  10.248.249.155  DNS       79 Standard query 0xcf0e A assets.adobedtm.com
  21287 73.904847135  10.248.249.102  10.248.249.155  DNS       79 Standard query 0x77c2 HTTPS assets.adobedtm.com
  21288 73.905119943  10.248.249.102  10.248.249.155  DNS       82 Standard query 0xa4a9 A static.ads-twitter.com
  21289 73.905276799  10.248.249.102  10.248.249.155  DNS       82 Standard query 0xca87 HTTPS static.ads-twitter.com
  21290 73.905520273  10.248.249.102  10.248.249.155  DNS       72 Standard query 0x1a10 A bat.bing.com
  21291 73.905619082  10.248.249.102  10.248.249.155  DNS       72 Standard query 0xf2f0 HTTPS bat.bing.com
  21304 73.916747908  10.248.249.155  10.248.249.102  DNS      179 Standard query response 0xcf0e A assets.adobedtm.com CNAME cn-assets.adobe
  21305 73.917162751  10.248.249.155  10.248.249.102  DNS      143 Standard query response 0xa4a9 A static.ads-twitter.com CNAME platform.tw
  21306 73.917163032  10.248.249.155  10.248.249.102  DNS      177 Standard query response 0xf2f0 HTTPS bat.bing.com CNAME bat-bing-com.ax-0
  21307 73.917163092  10.248.249.155  10.248.249.102  DNS      224 Standard query response 0x77c2 HTTPS assets.adobedtm.com CNAME cn-assets.a
  21308 73.917163152  10.248.249.155  10.248.249.102  DNS      185 Standard query response 0xca87 HTTPS static.ads-twitter.com CNAME platfor
  21311 73.918689312  10.248.249.155  10.248.249.102  DNS      166 Standard query response 0x1a10 A bat.bing.com CNAME bat-bing-com.ax-0001.
  21332 73.928290599  10.248.249.102  10.248.249.155  DNS       74 Standard query 0x0520 A sc.lfeeder.com
  21333 73.928369456  10.248.249.102  10.248.249.155  DNS       74 Standard query 0xc902 HTTPS sc.lfeeder.com
  21337 73.928542497  10.248.249.102  10.248.249.155  DNS       84 Standard query 0xc24c A www.googletagmanager.com
  21339 73.928618297  10.248.249.102  10.248.249.155  DNS       84 Standard query 0xffb1 HTTPS www.googletagmanager.com
  21345 73.929298031  10.248.249.155  10.248.249.102  DNS      100 Standard query response 0xc24c A www.googletagmanager.com A 172.217.192.9
  21348 73.930544122  10.248.249.102  10.248.249.155  DNS       80 Standard query 0xa89c A munchkin.marketo.net
  21349 73.930638646  10.248.249.102  10.248.249.155  DNS       80 Standard query 0x3ce1 HTTPS munchkin.marketo.net
  21359 73.937725620  10.248.249.102  10.248.249.155  DNS       84 Standard query 0x988c A www.googleadservices.com
  21361 73.937832203  10.248.249.102  10.248.249.155  DNS       84 Standard query 0x30b0 HTTPS www.googleadservices.com
  21364 73.938460144  10.248.249.155  10.248.249.102  DNS      148 Standard query response 0x988c A www.googleadservices.com A 142.251.0.156
  21394 73.945083787  10.248.249.102  10.248.249.155  DNS       72 Standard query 0x3082 A rum.hlx.page
  21395 73.945177840  10.248.249.102  10.248.249.155  DNS       72 Standard query 0x5ef2 HTTPS rum.hlx.page
  21400 73.946671165  10.248.249.155  10.248.249.102  DNS      141 Standard query response 0xffb1 HTTPS www.googletagmanager.com SOA ns1.goog
  21404 73.946752168  10.248.249.155  10.248.249.102  DNS      173 Standard query response 0xa89c A munchkin.marketo.net CNAME wildcard.marke
  21408 73.946990233  10.248.249.155  10.248.249.102  DNS      218 Standard query response 0x3ce1 HTTPS munchkin.marketo.net CNAME wildcard.
  21418 73.953422476  10.248.249.155  10.248.249.102  DNS      194 Standard query response 0xc902 HTTPS sc.lfeeder.com CNAME dja7ygzgr04yk.c
  21419 73.954337248  10.248.249.155  10.248.249.102  DNS      173 Standard query response 0x30b0 HTTPS www.googleadservices.com HTTPS A 142
  21435 73.956460478  10.248.249.155  10.248.249.102  DNS      125 Standard query response 0x3082 A rum.hlx.page CNAME n.sni.global.fastly.ne
  21436 73.956460569  10.248.249.155  10.248.249.102  DNS      170 Standard query response 0x5ef2 HTTPS rum.hlx.page CNAME n.sni.global.fast
  21513 73.992798593  10.248.249.155  10.248.249.102  DNS      180 Standard query response 0x0520 A sc.lfeeder.com CNAME dja7ygzgr04yk.cloud
  21733 74.117529324  10.248.249.102  10.248.249.155  DNS       75 Standard query 0x24db A s.go-mpulse.net
  21734 74.117642773  10.248.249.102  10.248.249.155  DNS       75 Standard query 0xddd8 HTTPS s.go-mpulse.net
  21768 74.125485338  10.248.249.155  10.248.249.102  DNS      168 Standard query response 0x24db A s.go-mpulse.net CNAME ip46.go-mpulse.net
  21779 74.125912253  10.248.249.155  10.248.249.102  DNS      216 Standard query response 0xddd8 HTTPS s.go-mpulse.net CNAME ip46.go-mpulse
  22331 74.359541621  10.248.249.102  10.248.249.155  DNS       74 Standard query 0x9ccf A dpm.demdex.net
  22332 74.359822819  10.248.249.102  10.248.249.155  DNS       74 Standard query 0xfdde HTTPS dpm.demdex.net
  22342 74.366977076  10.248.249.155  10.248.249.102  DNS      318 Standard query response 0x9ccf A dpm.demdex.net CNAME gslb-2.demdex.net C
```

```
› Frame 34612: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface eth0,
› Ethernet II, Src: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2), Dst: ASUSTekCOMPU_58:fa:21 (3c:7
› Internet Protocol Version 4, Src: 10.248.249.155, Dst: 10.248.249.102
› User Datagram Protocol, Src Port: 53, Dst Port: 65135
› Domain Name System (response)
```

```
0000  3c 7c 3f 58 fa 21 d8 ec  5e b9 7b b2 08 00 45
0010  00 7a 00 00 40 00 40 11  31 81 0a f8 f9 9b 0a
0020  f9 66 00 35 fe 6f 00 66  29 e0 18 1e 81 80 00
0030  00 00 00 01 00 00 06 77  61 61 2d 70 61 08 63
0040  69 65 6e 74 73 36 06 67  6f 6f 67 6c 65 03 63
0050  6d 00 00 41 00 01 c0 1c  00 06 00 01 00 00 00
0060  00 26 03 6e 73 31 c0 1c  09 64 6e 73 2d 61 64
0070  69 6e c0 1c 2f 92 13 ff  00 00 03 84 00 00 03
0080  00 00 07 08 00 00 00 3c
```

Domain Name System: Protocol | Packets: 102621 · Displayed: 1640 (1.6%) · Dropped: 0 (0.0%) | Profile: Default

- tcp.port == 443 - Tráfico HTTPS


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==443
```

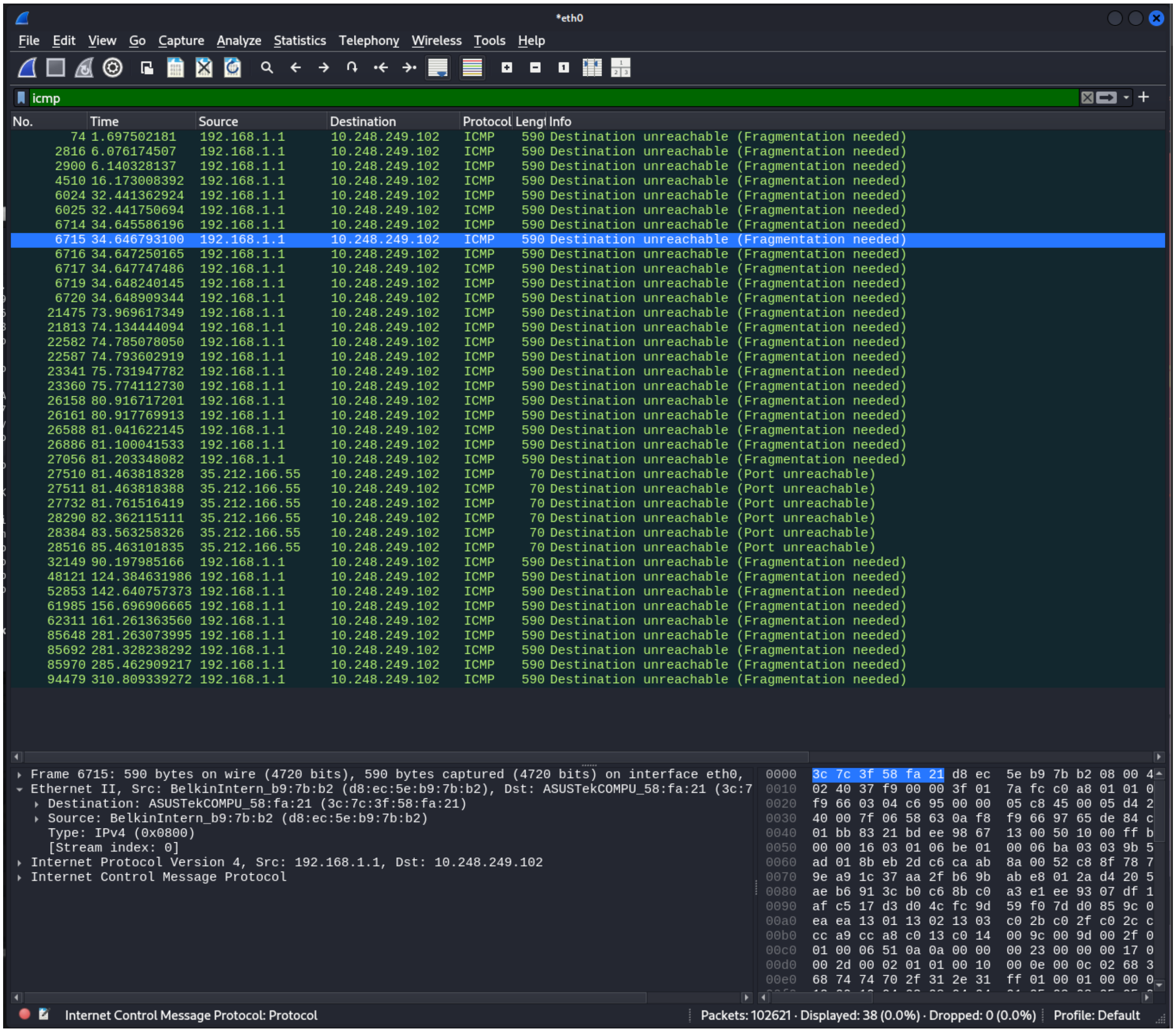
```
No.   Time            Source          Destination     Protocol Lengt Info
21726 74.115484794 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=133470 Win=130816 Len=0
21727 74.115602066 10.248.249.102  206.247.33.195  TLSv1…    121 Application Data
21728 74.116381366 2.18.21.202     10.248.249.102  TLSv1…    14… Application Data
21729 74.116413632 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=147870 Win=130816 Len=0
21730 74.117304982 2.18.21.202     10.248.249.102  TLSv1…    14… Application Data
21732 74.117339103 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=162270 Win=130816 Len=0
21736 74.118148785 2.18.21.202     10.248.249.102  TLSv1…    72… Application Data
21737 74.118148915 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=169470 Win=130816 Len=0
21738 74.119177347 2.18.21.202     10.248.249.102  TLSv1…    14… Application Data
21740 74.119222584 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=183870 Win=130816 Len=0
21741 74.119222644 10.248.249.102  2.18.21.202     TCP        60 [TCP ACKed unseen segment] 54990 → 443 [ACK] Seq=8497 Ack=192510 Win=1308
21742 74.119222704 2.18.21.202     10.248.249.102  TLSv1…    14… Application Data
21743 74.119238241 10.248.249.102  2.18.21.202     TCP        60 [TCP ACKed unseen segment] 54990 → 443 [ACK] Seq=8497 Ack=198270 Win=1308
21746 74.120468349 2.18.21.202     10.248.249.102  TLSv1…    57… Application Data
21747 74.120468841 10.248.249.102  2.18.21.202     TCP        60 [TCP ACKed unseen segment] 54990 → 443 [ACK] Seq=8497 Ack=209773 Win=2618
21748 74.120468891 2.18.21.202     10.248.249.102  TCP       58… [TCP Spurious Retransmission] 443 → 54990 [ACK] Seq=204013 Ack=8497 Win=7
21749 74.120605695 2.18.21.202     10.248.249.102  TLSv1…    10… Continuation Data
21750 74.120617644 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=220419 Win=261888 Len=0
21754 74.120960363 10.248.249.102  151.101.221.91  TLSv1…    146 Application Data
21755 74.121166917 10.248.249.102  23.215.173.37   TLSv1…    146 Application Data
21756 74.121279114 10.248.249.102  151.101.221.91  TLSv1…    494 Application Data
21757 74.121334375 10.248.249.102  23.215.173.37   TLSv1…    502 Application Data
21758 74.121446840 2.18.21.202     10.248.249.102  TLSv1…    20… Application Data
21759 74.121446951 10.248.249.102  2.18.21.202     TCP        60 54990 → 443 [ACK] Seq=8497 Ack=222369 Win=261888 Len=0
21760 74.124756337 23.215.173.37   10.248.249.102  TCP        60 443 → 55747 [ACK] Seq=4443 Ack=1902 Win=67584 Len=0
21761 74.124756588 23.215.173.37   10.248.249.102  TLSv1…    115 Application Data
21762 74.124756638 23.215.173.37   10.248.249.102  TLSv1…     85 Application Data
21763 74.124756698 151.101.221.91  10.248.249.102  TCP        60 443 → 60687 [ACK] Seq=4435 Ack=1975 Win=150016 Len=0
21764 74.124756758 151.101.221.91  10.248.249.102  TLSv1…    119 Application Data
21765 74.124795510 10.248.249.102  23.215.173.37   TCP        60 55747 → 443 [ACK] Seq=2350 Ack=4535 Win=64768 Len=0
21766 74.124883680 10.248.249.102  23.215.173.37   TLSv1…     85 Application Data
21767 74.124908067 10.248.249.102  151.101.221.91  TLSv1…     85 Application Data
21769 74.125485609 151.101.221.91  10.248.249.102  TCP        60 443 → 60687 [ACK] Seq=4500 Ack=2415 Win=152576 Len=0
21770 74.125485749 23.215.173.37   10.248.249.102  TLSv1…    349 Application Data
21771 74.125485889 23.215.173.37   10.248.249.102  TCP       29… 443 → 55747 [ACK] Seq=4830 Ack=2350 Win=70528 Len=2880 [TCP PDU reassemble
21772 74.125554121 10.248.249.102  23.215.173.37   TCP        60 55747 → 443 [ACK] Seq=2381 Ack=7710 Win=65280 Len=0
21773 74.125554292 23.215.173.37   10.248.249.102  TCP       14… 443 → 55747 [PSH, ACK] Seq=7710 Ack=2350 Win=70528 Len=1440 [TCP PDU reas
21774 74.125554432 23.215.173.37   10.248.249.102  TCP       43… 443 → 55747 [PSH, ACK] Seq=9150 Ack=2350 Win=70528 Len=4320 [TCP PDU reas
21775 74.125554562 10.248.249.102  23.215.173.37   TCP        60 55747 → 443 [ACK] Seq=2381 Ack=13470 Win=65280 Len=0
21776 74.125650991 10.248.249.102  23.215.173.37   TCP        60 [TCP ACKed unseen segment] 55747 → 443 [ACK] Seq=2381 Ack=14910 Win=64000
21777 74.125651232 23.215.173.37   10.248.249.102  TCP       14… [TCP Spurious Retransmission] 443 → 55747 [ACK] Seq=13470 Ack=2350 Win=70
21778 74.125912002 23.215.173.37   10.248.249.102  TCP       29… 443 → 55747 [PSH, ACK] Seq=14910 Ack=2350 Win=70528 Len=2880 [TCP PDU reas
```

```
› Frame 22272: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id
› Ethernet II, Src: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2), Dst: ASUSTekCOMPU_58:fa:21 (3c:7
› Internet Protocol Version 4, Src: 206.247.33.195, Dst: 10.248.249.102
› Transmission Control Protocol, Src Port: 443, Dst Port: 57029, Seq: 1741, Ack: 2101, Len: 0
```

```
0000  3c 7c 3f 58 fa 21 d8 ec  5e b9 7b b2 08 00 45
0010  00 28 0e cd 40 00 32 06  44 ca ce f7 21 c3 0a
0020  f9 66 01 bb de c5 ed 0a  de ca 37 b9 57 6d 50
0030  00 0b 7f 33 00 00 00 00  00 00 00 00
```

wireshark_eth0JSBRB3.pcapng | Packets: 102621 · Displayed: 57131 (55.7%) · Dropped: 0 (0.0%) | Profile: Default

- icmp - Tráfico ICMP



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
```

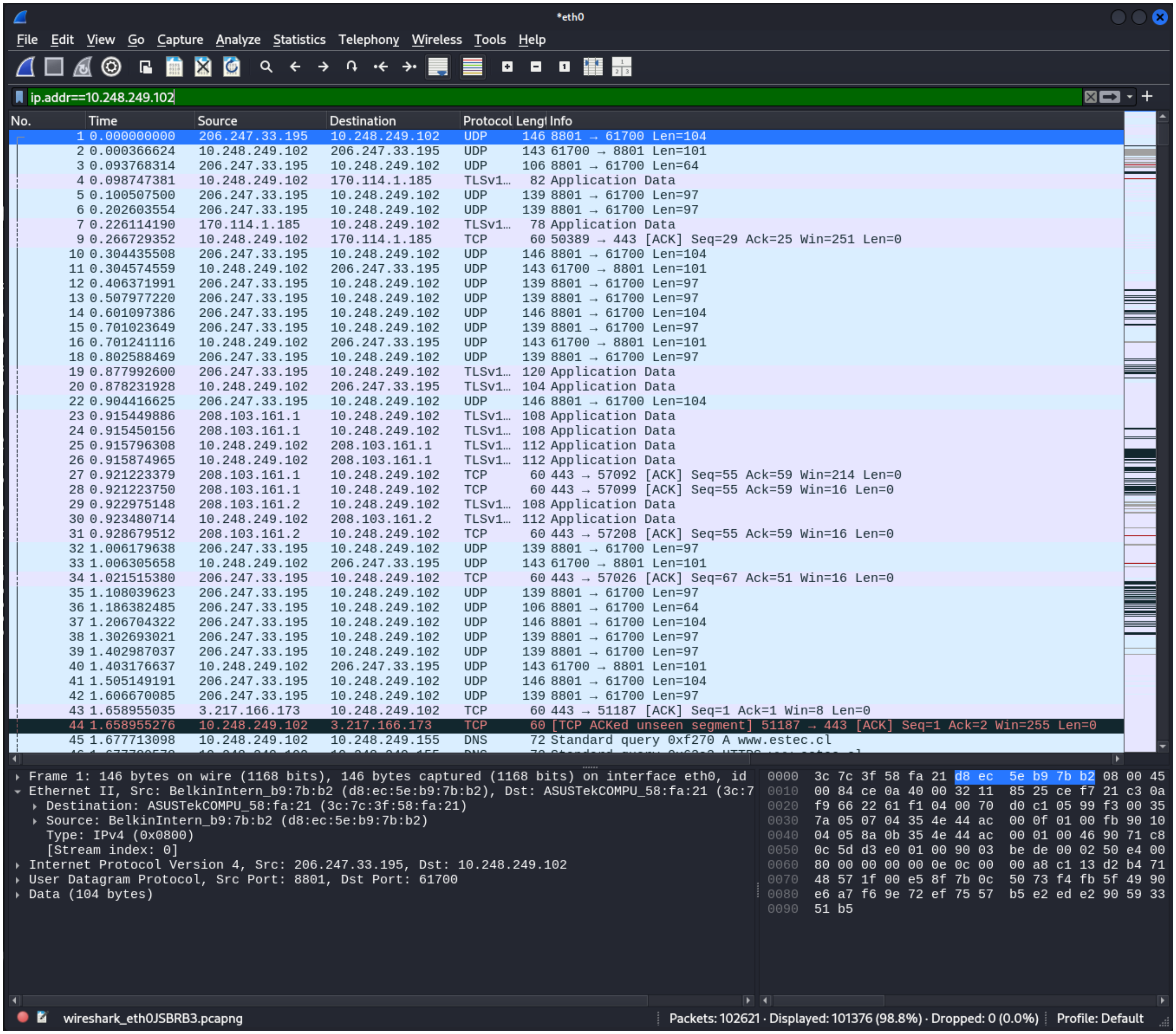
```
No.        Time          Source          Destination      Protocol Lengt Info
      74 1.697502181   192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    2816 6.076174507   192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    2900 6.140328137   192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    4510 16.173008392  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6024 32.441362924  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6025 32.441750694  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6714 34.645586196  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6715 34.646793100  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6716 34.647250165  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6717 34.647747486  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6719 34.648240145  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
    6720 34.648909344  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   21475 73.969617349  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   21813 74.134444094  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   22582 74.785078050  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   22587 74.793602919  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   23341 75.731947782  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   23360 75.774112730  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   26158 80.916717201  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   26161 80.917769913  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   26588 81.041622145  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   26886 81.100041533  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   27056 81.203348082  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   27510 81.463818328  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   27511 81.463818388  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   27732 81.761516419  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   28290 82.362115111  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   28384 83.563258326  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   28516 85.463101835  35.212.166.55   10.248.249.102   ICMP      70 Destination unreachable (Port unreachable)
   32149 90.197985166  192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   48121 124.384631986 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   52853 142.640757373 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   61985 156.696906665 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   62311 161.261363560 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   85648 281.263073995 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   85692 281.328238292 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   85970 285.462909217 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
   94479 310.809339272 192.168.1.1     10.248.249.102   ICMP     590 Destination unreachable (Fragmentation needed)
```

```
› Frame 6715: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0,
⌄ Ethernet II, Src: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2), Dst: ASUSTekCOMPU_58:fa:21 (3c:7
  › Destination: ASUSTekCOMPU_58:fa:21 (3c:7c:3f:58:fa:21)
  › Source: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2)
    Type: IPv4 (0x0800)
    [Stream index: 0]
› Internet Protocol Version 4, Src: 192.168.1.1, Dst: 10.248.249.102
› Internet Control Message Protocol
```

```
0000  3c 7c 3f 58 fa 21 d8 ec  5e b9 7b b2 08 00 4
0010  02 40 37 f9 00 00 3f 01  7a fc c0 a8 01 01 0
0020  f9 66 03 04 c6 95 00 00  05 c8 45 00 05 d4 2
0030  40 00 7f 06 58 63 0a f8  f9 66 97 65 de 84 c
0040  01 bb 83 21 bd ee 98 67  13 00 50 10 00 ff b
0050  00 00 16 03 01 06 be 01  00 06 ba 03 03 9b 5
0060  ad 01 8b eb 2d c6 ca ab  8a 00 52 c8 8f 78 7
0070  9e a9 1c 37 aa 2f b6 9b  ab e8 01 2a d4 20 5
0080  ae b6 91 3c b0 c6 8b c0  a3 e1 ee 93 07 df 1
0090  af c5 17 d3 d0 4c fc 9d  59 f0 7d d0 85 9c 0
00a0  ea ea 13 01 13 02 13 03  c0 2b c0 2f c0 2c c
00b0  cc a9 cc a8 c0 13 c0 14  00 9c 00 9d 00 2f 0
00c0  01 00 06 51 0a 0a 00 00  00 23 00 00 00 17 0
00d0  00 2d 00 02 01 01 00 10  00 0e 00 0c 02 68 3
00e0  68 74 74 70 2f 31 2e 31  ff 01 00 01 00 00 0
```

Internet Control Message Protocol: Protocol | Packets: 102621 · Displayed: 38 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

- ip.addr == [10.248.249.102] - Todo el tráfico de tu máquina



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==10.248.249.102
```

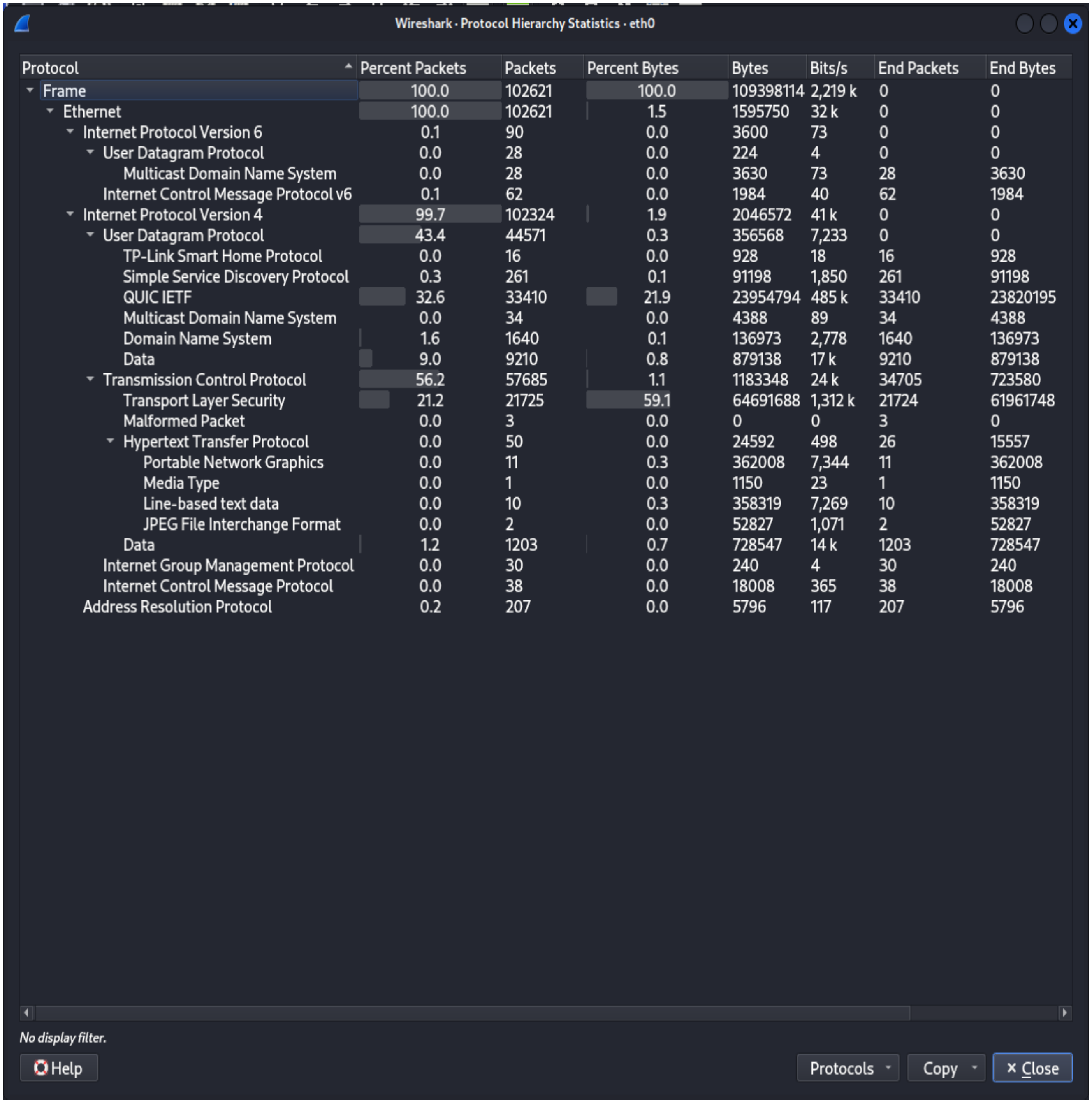
```
No.   Time        Source          Destination     Protocol Lengt Info
    1 0.000000000 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
    2 0.000366624 10.248.249.102  206.247.33.195  UDP      143 61700 → 8801 Len=101
    3 0.093768314 206.247.33.195  10.248.249.102  UDP      106 8801 → 61700 Len=64
    4 0.098747381 10.248.249.102  170.114.1.185   TLSv1…    82 Application Data
    5 0.100507500 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
    6 0.202603554 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
    7 0.226114190 170.114.1.185   10.248.249.102  TLSv1…    78 Application Data
    9 0.266729352 10.248.249.102  170.114.1.185   TCP       60 50389 → 443 [ACK] Seq=29 Ack=25 Win=251 Len=0
   10 0.304435508 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
   11 0.304574559 10.248.249.102  206.247.33.195  UDP      143 61700 → 8801 Len=101
   12 0.406371991 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   13 0.507977220 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   14 0.601097386 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
   15 0.701023649 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   16 0.701241116 10.248.249.102  206.247.33.195  UDP      143 61700 → 8801 Len=101
   18 0.802588469 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   19 0.877992600 206.247.33.195  10.248.249.102  TLSv1…   120 Application Data
   20 0.878231928 10.248.249.102  206.247.33.195  TLSv1…   104 Application Data
   22 0.904416625 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
   23 0.915449886 208.103.161.1   10.248.249.102  TLSv1…   108 Application Data
   24 0.915450156 208.103.161.1   10.248.249.102  TLSv1…   108 Application Data
   25 0.915796308 10.248.249.102  208.103.161.1   TLSv1…   112 Application Data
   26 0.915874965 10.248.249.102  208.103.161.1   TLSv1…   112 Application Data
   27 0.921223379 208.103.161.1   10.248.249.102  TCP       60 443 → 57092 [ACK] Seq=55 Ack=59 Win=214 Len=0
   28 0.921223750 208.103.161.1   10.248.249.102  TCP       60 443 → 57099 [ACK] Seq=55 Ack=59 Win=16 Len=0
   29 0.922975148 208.103.161.2   10.248.249.102  TLSv1…   108 Application Data
   30 0.923480714 10.248.249.102  208.103.161.2   TLSv1…   112 Application Data
   31 0.928679512 208.103.161.2   10.248.249.102  TCP       60 443 → 57208 [ACK] Seq=55 Ack=59 Win=16 Len=0
   32 1.006179638 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   33 1.006305658 10.248.249.102  206.247.33.195  UDP      143 61700 → 8801 Len=101
   34 1.021515380 206.247.33.195  10.248.249.102  TCP       60 443 → 57026 [ACK] Seq=67 Ack=51 Win=16 Len=0
   35 1.108039623 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   36 1.186382485 206.247.33.195  10.248.249.102  UDP      106 8801 → 61700 Len=64
   37 1.206704322 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
   38 1.302693021 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   39 1.402987037 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   40 1.403176637 10.248.249.102  206.247.33.195  UDP      143 61700 → 8801 Len=101
   41 1.505149191 206.247.33.195  10.248.249.102  UDP      146 8801 → 61700 Len=104
   42 1.606670085 206.247.33.195  10.248.249.102  UDP      139 8801 → 61700 Len=97
   43 1.658955035 3.217.166.173   10.248.249.102  TCP       60 443 → 51187 [ACK] Seq=1 Ack=1 Win=8 Len=0
   44 1.658955276 10.248.249.102  3.217.166.173   TCP       60 [TCP ACKed unseen segment] 51187 → 443 [ACK] Seq=1 Ack=2 Win=255 Len=0
   45 1.677713098 10.248.249.102  10.248.249.155  DNS       72 Standard query 0xf270 A www.estec.cl
```

```
› Frame 1: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface eth0, id
⌄ Ethernet II, Src: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2), Dst: ASUSTekCOMPU_58:fa:21 (3c:7
  › Destination: ASUSTekCOMPU_58:fa:21 (3c:7c:3f:58:fa:21)
  › Source: BelkinIntern_b9:7b:b2 (d8:ec:5e:b9:7b:b2)
    Type: IPv4 (0x0800)
    [Stream index: 0]
› Internet Protocol Version 4, Src: 206.247.33.195, Dst: 10.248.249.102
› User Datagram Protocol, Src Port: 8801, Dst Port: 61700
› Data (104 bytes)
```

```
0000  3c 7c 3f 58 fa 21 d8 ec  5e b9 7b b2 08 00 45
0010  00 84 ce 0a 40 00 32 11  85 25 ce f7 21 c3 0a
0020  f9 66 22 61 f1 04 00 70  d0 c1 05 99 f3 00 35
0030  7a 05 07 04 35 4e 44 ac  00 0f 01 00 fb 90 10
0040  04 05 8a 0b 35 4e 44 ac  00 01 00 46 90 71 c8
0050  0c 5d d3 e0 01 00 90 03  be de 00 02 50 e4 00
0060  80 00 00 00 00 0e 0c 00  00 a8 c1 13 d2 b4 71
0070  48 57 1f 00 e5 8f 7b 0c  50 73 f4 fb 5f 49 90
0080  e6 a7 f6 9e 72 ef 75 57  b5 e2 ed e2 90 59 33
0090  51 b5
```

wireshark_eth0JSBRB3.pcapng | Packets: 102621 · Displayed: 101376 (98.8%) · Dropped: 0 (0.0%) | Profile: Default

- e) Identificar y explicar:
  - Protocolos más utilizados

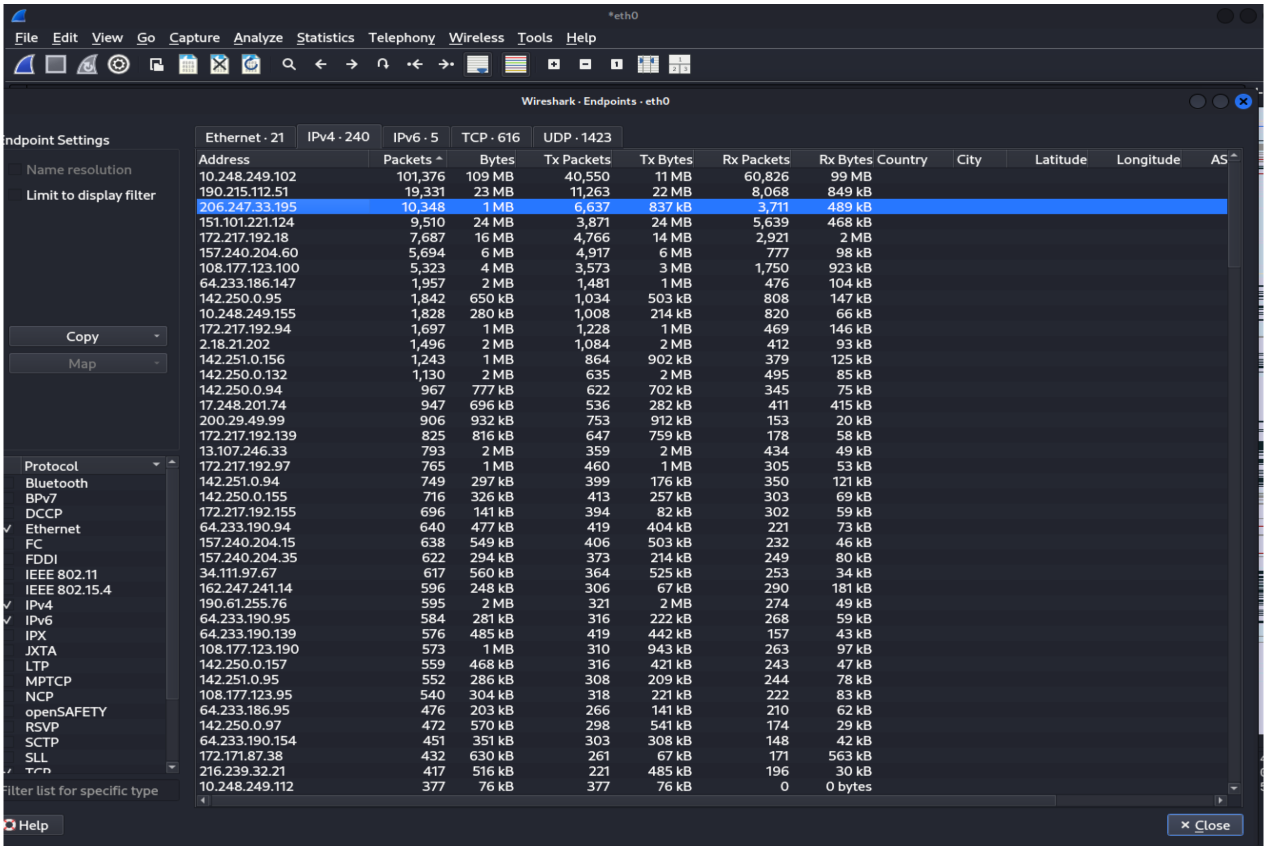


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Frame	100.0	102621	100.0	109398114	2,219 k	0	0
Ethernet	100.0	102621	1.5	1595750	32 k	0	0
Internet Protocol Version 6	0.1	90	0.0	3600	73	0	0
User Datagram Protocol	0.0	28	0.0	224	4	0	0
Multicast Domain Name System	0.0	28	0.0	3630	73	28	3630
Internet Control Message Protocol v6	0.1	62	0.0	1984	40	62	1984
Internet Protocol Version 4	99.7	102324	1.9	2046572	41 k	0	0
User Datagram Protocol	43.4	44571	0.3	356568	7,233	0	0
TP-Link Smart Home Protocol	0.0	16	0.0	928	18	16	928
Simple Service Discovery Protocol	0.3	261	0.1	91198	1,850	261	91198
QUIC IETF	32.6	33410	21.9	23954794	485 k	33410	23820195
Multicast Domain Name System	0.0	34	0.0	4388	89	34	4388
Domain Name System	1.6	1640	0.1	136973	2,778	1640	136973
Data	9.0	9210	0.8	879138	17 k	9210	879138
Transmission Control Protocol	56.2	57685	1.1	1183348	24 k	34705	723580
Transport Layer Security	21.2	21725	59.1	64691688	1,312 k	21724	61961748
Malformed Packet	0.0	3	0.0	0	0	3	0
Hypertext Transfer Protocol	0.0	50	0.0	24592	498	26	15557
Portable Network Graphics	0.0	11	0.3	362008	7,344	11	362008
Media Type	0.0	1	0.0	1150	23	1	1150
Line-based text data	0.0	10	0.3	358319	7,269	10	358319
JPEG File Interchange Format	0.0	2	0.0	52827	1,071	2	52827
Data	1.2	1203	0.7	728547	14 k	1203	728547
Internet Group Management Protocol	0.0	30	0.0	240	4	30	240
Internet Control Message Protocol	0.0	38	0.0	18008	365	38	18008
Address Resolution Protocol	0.2	207	0.0	5796	117	207	5796

No display filter.

- **TCP 56% el cual incluye TLS que representa el 21.2% del tráfico.**
- **UDP 43.4%**

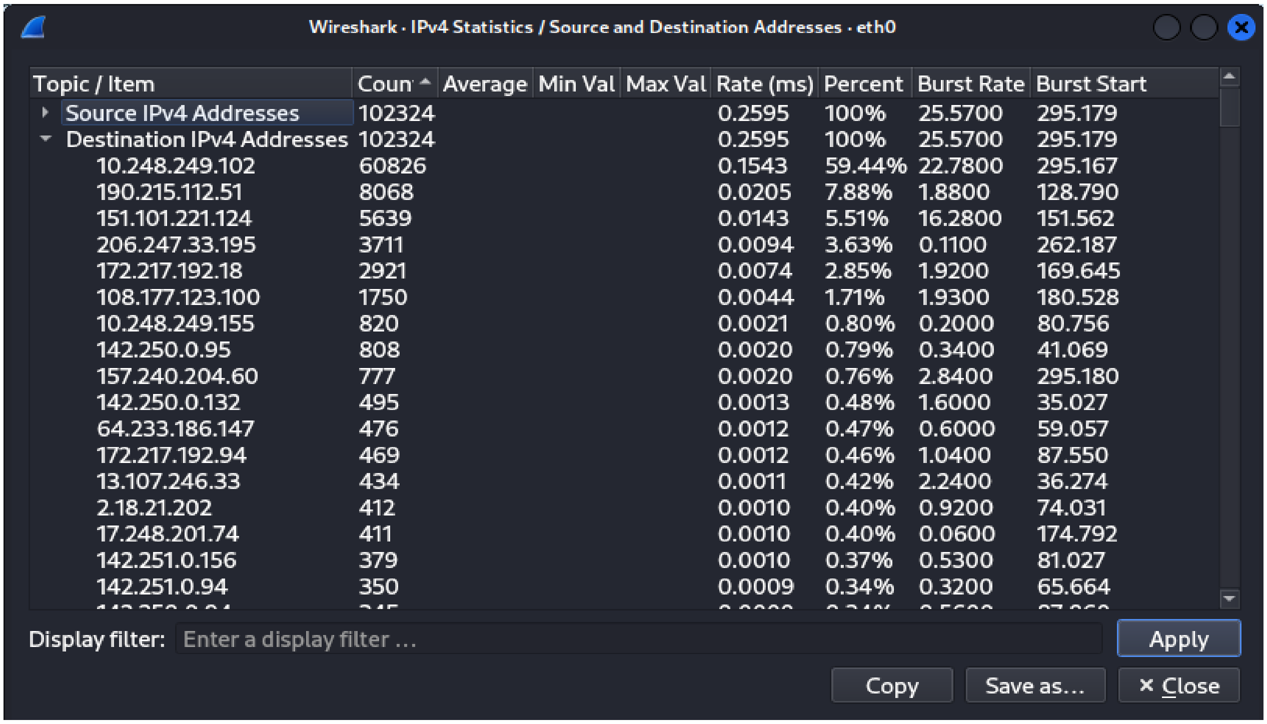
- Direcciones IP de destino más frecuentes


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · eth0
ndpoint Settings
Name resolution
Limit to display filter
Copy
Map
Protocol
Filter list for specific type
Help
× Close

Bluetooth
BPv7
DCCP
✓ Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
✓ IPv4
✓ IPv6
IPX
JXTA
LTP
MPTCP
NCP
openSAFETY
RSVP
SCTP
SLL
✓ TCP

Ethernet · 21 | IPv4 · 240 | IPv6 · 5 | TCP · 616 | UDP · 1423

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS
10.248.249.102	101,376	109 MB	40,550	11 MB	60,826	99 MB					
190.215.112.51	19,331	23 MB	11,263	22 MB	8,068	849 kB					
206.247.33.195	10,348	1 MB	6,637	837 kB	3,711	489 kB					
151.101.221.124	9,510	24 MB	3,871	24 MB	5,639	468 kB					
172.217.192.18	7,687	16 MB	4,766	14 MB	2,921	2 MB					
157.240.204.60	5,694	6 MB	4,917	6 MB	777	98 kB					
108.177.123.100	5,323	4 MB	3,573	3 MB	1,750	923 kB					
64.233.186.147	1,957	2 MB	1,481	1 MB	476	104 kB					
142.250.0.95	1,842	650 kB	1,034	503 kB	808	147 kB					
10.248.249.155	1,828	280 kB	1,008	214 kB	820	66 kB					
172.217.192.94	1,697	1 MB	1,228	1 MB	469	146 kB					
2.18.21.202	1,496	2 MB	1,084	2 MB	412	93 kB					
142.251.0.156	1,243	1 MB	864	902 kB	379	125 kB					
142.250.0.132	1,130	2 MB	635	2 MB	495	85 kB					
142.250.0.94	967	777 kB	622	702 kB	345	75 kB					
17.248.201.74	947	696 kB	536	282 kB	411	415 kB					
200.29.49.99	906	932 kB	753	912 kB	153	20 kB					
172.217.192.139	825	816 kB	647	759 kB	178	58 kB					
13.107.246.33	793	2 MB	359	2 MB	434	49 kB					
172.217.192.97	765	1 MB	460	1 MB	305	53 kB					
142.251.0.94	749	297 kB	399	176 kB	350	121 kB					
142.250.0.155	716	326 kB	413	257 kB	303	69 kB					
172.217.192.155	696	141 kB	394	82 kB	302	59 kB					
64.233.190.94	640	477 kB	419	404 kB	221	73 kB					
157.240.204.15	638	549 kB	406	503 kB	232	46 kB					
157.240.204.35	622	294 kB	373	214 kB	249	80 kB					
34.111.97.67	617	560 kB	364	525 kB	253	34 kB					
162.247.241.14	596	248 kB	306	67 kB	290	181 kB					
190.61.255.76	595	2 MB	321	2 MB	274	49 kB					
64.233.190.95	584	281 kB	316	222 kB	268	59 kB					
64.233.190.139	576	485 kB	419	442 kB	157	43 kB					
108.177.123.190	573	1 MB	310	943 kB	263	97 kB					
142.250.0.157	559	468 kB	316	421 kB	243	47 kB					
142.251.0.95	552	286 kB	308	209 kB	244	78 kB					
108.177.123.95	540	304 kB	318	221 kB	222	83 kB					
64.233.186.95	476	203 kB	266	141 kB	210	62 kB					
142.250.0.97	472	570 kB	298	541 kB	174	29 kB					
64.233.190.154	451	351 kB	303	308 kB	148	42 kB					
172.171.87.38	432	630 kB	261	67 kB	171	563 kB					
216.239.32.21	417	516 kB	221	485 kB	196	30 kB					
10.248.249.112	377	76 kB	377	76 kB	0	0 bytes					

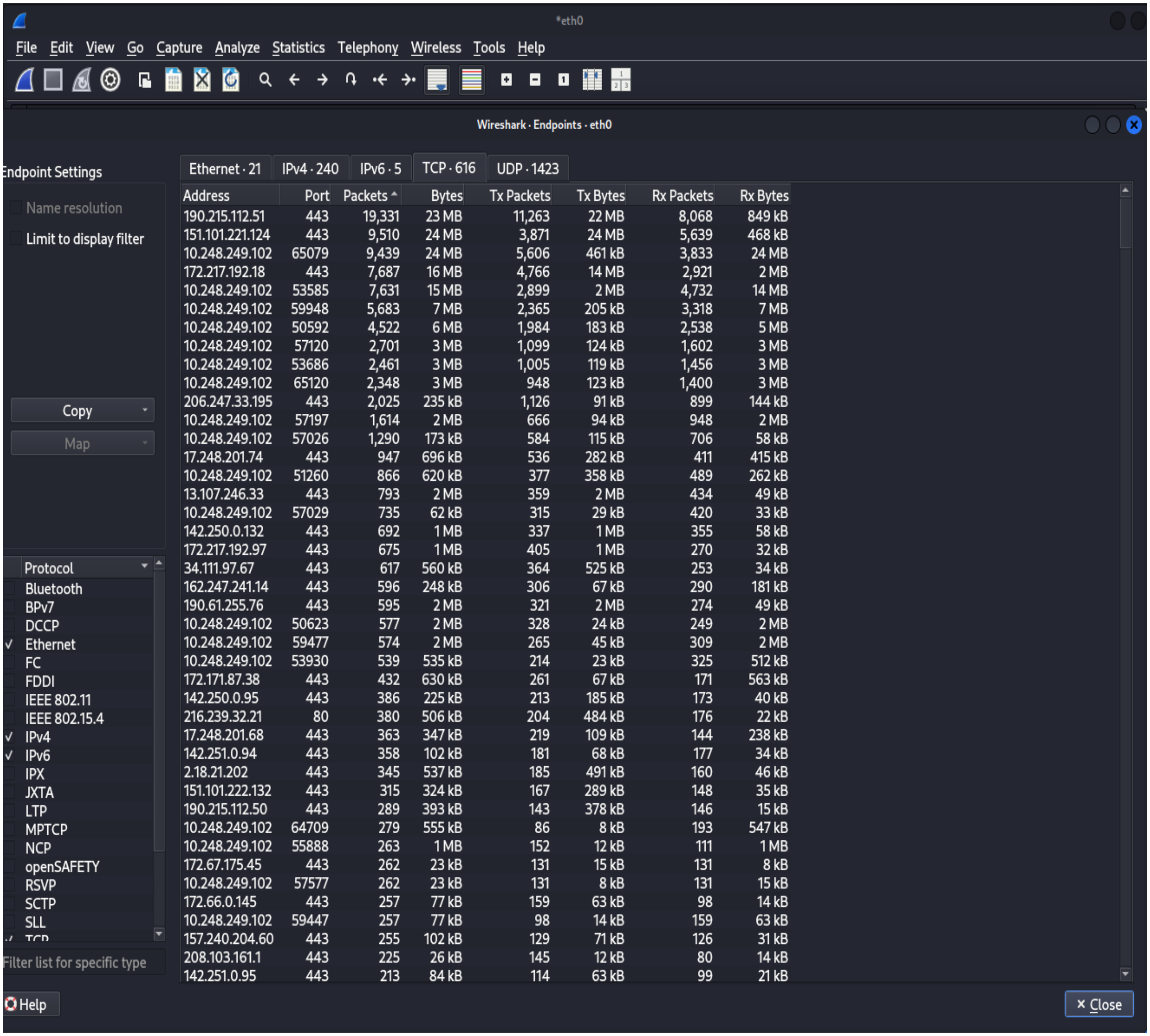

Wireshark · IPv4 Statistics / Source and Destination Addresses · eth0
Apply
Copy
Save as…
× Close

Topic / Item	Coun	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	102324				0.2595	100%	25.5700	295.179
Destination IPv4 Addresses	102324				0.2595	100%	25.5700	295.179
10.248.249.102	60826				0.1543	59.44%	22.7800	295.167
190.215.112.51	8068				0.0205	7.88%	1.8800	128.790
151.101.221.124	5639				0.0143	5.51%	16.2800	151.562
206.247.33.195	3711				0.0094	3.63%	0.1100	262.187
172.217.192.18	2921				0.0074	2.85%	1.9200	169.645
108.177.123.100	1750				0.0044	1.71%	1.9300	180.528
10.248.249.155	820				0.0021	0.80%	0.2000	80.756
142.250.0.95	808				0.0020	0.79%	0.3400	41.069
157.240.204.60	777				0.0020	0.76%	2.8400	295.180
142.250.0.132	495				0.0013	0.48%	1.6000	35.027
64.233.186.147	476				0.0012	0.47%	0.6000	59.057
172.217.192.94	469				0.0012	0.46%	1.0400	87.550
13.107.246.33	434				0.0011	0.42%	2.2400	36.274
2.18.21.202	412				0.0010	0.40%	0.9200	74.031
17.248.201.74	411				0.0010	0.40%	0.0600	174.792
142.251.0.156	379				0.0010	0.37%	0.5300	81.027
142.251.0.94	350				0.0009	0.34%	0.3200	65.664

Display filter: Enter a display filter …

- Puertos más utilizados

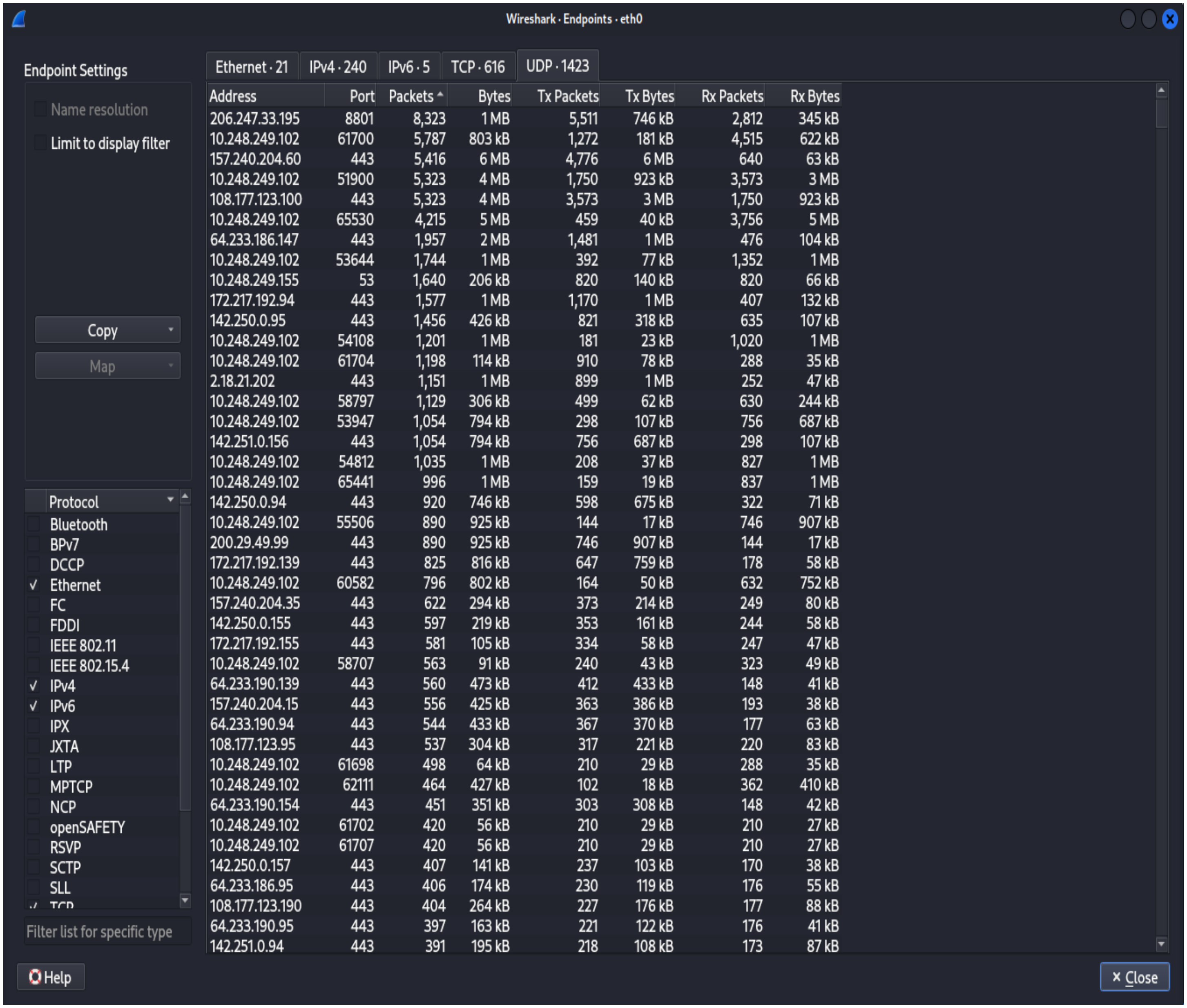
Puertos TCP



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
190.215.112.51	443	19,331	23 MB	11,263	22 MB	8,068	849 kB
151.101.221.124	443	9,510	24 MB	3,871	24 MB	5,639	468 kB
10.248.249.102	65079	9,439	24 MB	5,606	461 kB	3,833	24 MB
172.217.192.18	443	7,687	16 MB	4,766	14 MB	2,921	2 MB
10.248.249.102	53585	7,631	15 MB	2,899	2 MB	4,732	14 MB
10.248.249.102	59948	5,683	7 MB	2,365	205 kB	3,318	7 MB
10.248.249.102	50592	4,522	6 MB	1,984	183 kB	2,538	5 MB
10.248.249.102	57120	2,701	3 MB	1,099	124 kB	1,602	3 MB
10.248.249.102	53686	2,461	3 MB	1,005	119 kB	1,456	3 MB
10.248.249.102	65120	2,348	3 MB	948	123 kB	1,400	3 MB
206.247.33.195	443	2,025	235 kB	1,126	91 kB	899	144 kB
10.248.249.102	57197	1,614	2 MB	666	94 kB	948	2 MB
10.248.249.102	57026	1,290	173 kB	584	115 kB	706	58 kB
17.248.201.74	443	947	696 kB	536	282 kB	411	415 kB
10.248.249.102	51260	866	620 kB	377	358 kB	489	262 kB
13.107.246.33	443	793	2 MB	359	2 MB	434	49 kB
10.248.249.102	57029	735	62 kB	315	29 kB	420	33 kB
142.250.0.132	443	692	1 MB	337	1 MB	355	58 kB
172.217.192.97	443	675	1 MB	405	1 MB	270	32 kB
34.111.97.67	443	617	560 kB	364	525 kB	253	34 kB
162.247.241.14	443	596	248 kB	306	67 kB	290	181 kB
190.61.255.76	443	595	2 MB	321	2 MB	274	49 kB
10.248.249.102	50623	577	2 MB	328	24 kB	249	2 MB
10.248.249.102	59477	574	2 MB	265	45 kB	309	2 MB
10.248.249.102	53930	539	535 kB	214	23 kB	325	512 kB
172.171.87.38	443	432	630 kB	261	67 kB	171	563 kB
142.250.0.95	443	386	225 kB	213	185 kB	173	40 kB
216.239.32.21	80	380	506 kB	204	484 kB	176	22 kB
17.248.201.68	443	363	347 kB	219	109 kB	144	238 kB
142.251.0.94	443	358	102 kB	181	68 kB	177	34 kB
2.18.21.202	443	345	537 kB	185	491 kB	160	46 kB
151.101.222.132	443	315	324 kB	167	289 kB	148	35 kB
190.215.112.50	443	289	393 kB	143	378 kB	146	15 kB
10.248.249.102	64709	279	555 kB	86	8 kB	193	547 kB
10.248.249.102	55888	263	1 MB	152	12 kB	111	1 MB
172.67.175.45	443	262	23 kB	131	15 kB	131	8 kB
10.248.249.102	57577	262	23 kB	131	8 kB	131	15 kB
172.66.0.145	443	257	77 kB	159	63 kB	98	14 kB
10.248.249.102	59447	257	77 kB	98	14 kB	159	63 kB
157.240.204.60	443	255	102 kB	129	71 kB	126	31 kB
208.103.161.1	443	225	26 kB	145	12 kB	80	14 kB
142.251.0.95	443	213	84 kB	114	63 kB	99	21 kB

- 443
- 65079
- 53585
- 59948

Puertos UDP



Endpoint Settings

□ Name resolution

□ Limit to display filter

Protocol

- □ Bluetooth
- □ BPv7
- □ DCCP
- ✓ Ethernet
- □ FC
- □ FDDI
- □ IEEE 802.11
- □ IEEE 802.15.4
- ✓ IPv4
- ✓ IPv6
- □ IPX
- □ JXTA
- □ LTP
- □ MPTCP
- □ NCP
- □ openSAFETY
- □ RSVP
- □ SCTP
- □ SLL
- ✓ TCP

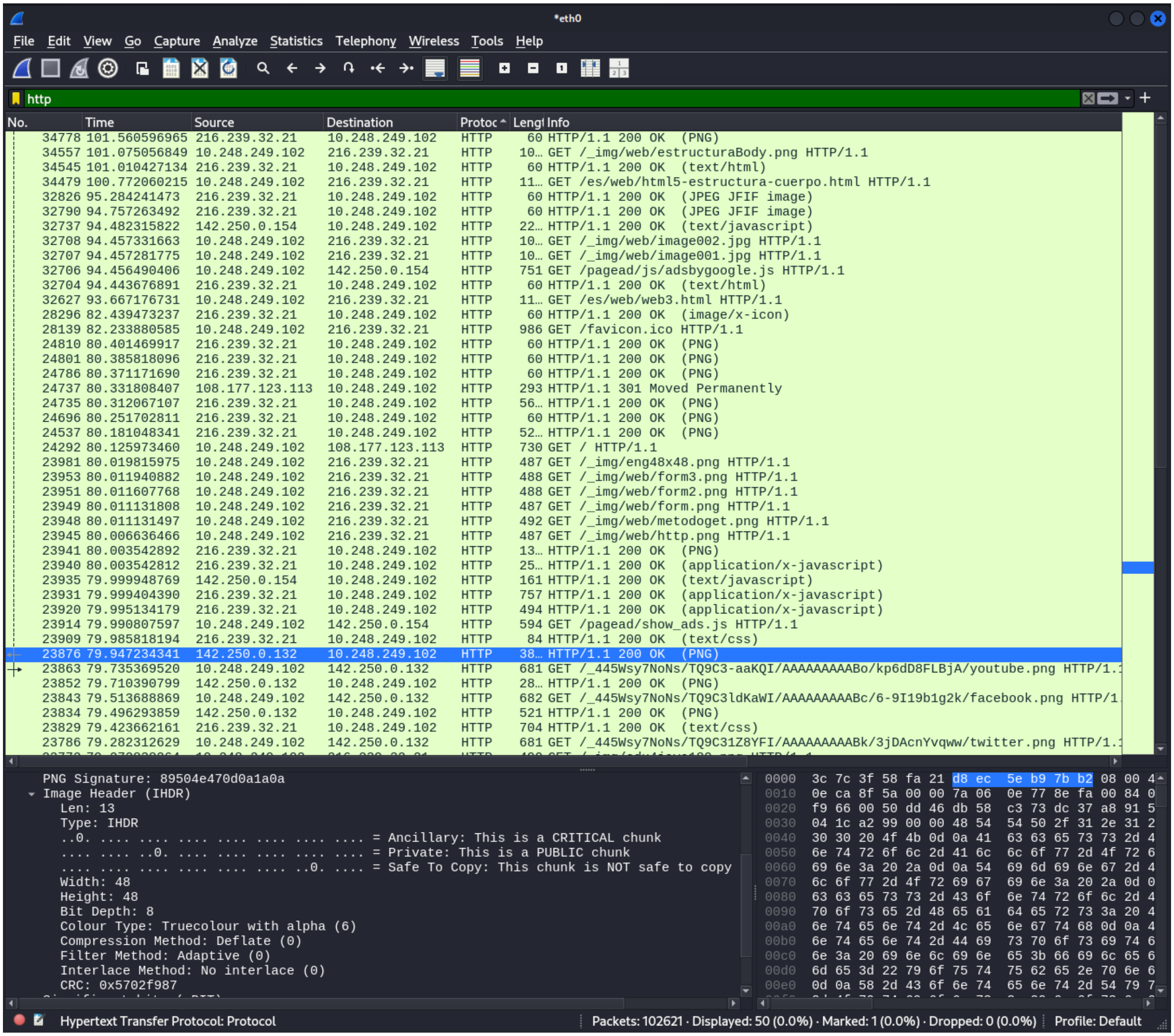
Filter list for specific type

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
206.247.33.195	8801	8,323	1 MB	5,511	746 kB	2,812	345 kB
10.248.249.102	61700	5,787	803 kB	1,272	181 kB	4,515	622 kB
157.240.204.60	443	5,416	6 MB	4,776	6 MB	640	63 kB
10.248.249.102	51900	5,323	4 MB	1,750	923 kB	3,573	3 MB
108.177.123.100	443	5,323	4 MB	3,573	3 MB	1,750	923 kB
10.248.249.102	65530	4,215	5 MB	459	40 kB	3,756	5 MB
64.233.186.147	443	1,957	2 MB	1,481	1 MB	476	104 kB
10.248.249.102	53644	1,744	1 MB	392	77 kB	1,352	1 MB
10.248.249.155	53	1,640	206 kB	820	140 kB	820	66 kB
172.217.192.94	443	1,577	1 MB	1,170	1 MB	407	132 kB
142.250.0.95	443	1,456	426 kB	821	318 kB	635	107 kB
10.248.249.102	54108	1,201	1 MB	181	23 kB	1,020	1 MB
10.248.249.102	61704	1,198	114 kB	910	78 kB	288	35 kB
2.18.21.202	443	1,151	1 MB	899	1 MB	252	47 kB
10.248.249.102	58797	1,129	306 kB	499	62 kB	630	244 kB
10.248.249.102	53947	1,054	794 kB	298	107 kB	756	687 kB
142.251.0.156	443	1,054	794 kB	756	687 kB	298	107 kB
10.248.249.102	54812	1,035	1 MB	208	37 kB	827	1 MB
10.248.249.102	65441	996	1 MB	159	19 kB	837	1 MB
142.250.0.94	443	920	746 kB	598	675 kB	322	71 kB
10.248.249.102	55506	890	925 kB	144	17 kB	746	907 kB
200.29.49.99	443	890	925 kB	746	907 kB	144	17 kB
172.217.192.139	443	825	816 kB	647	759 kB	178	58 kB
10.248.249.102	60582	796	802 kB	164	50 kB	632	752 kB
157.240.204.35	443	622	294 kB	373	214 kB	249	80 kB
142.250.0.155	443	597	219 kB	353	161 kB	244	58 kB
172.217.192.155	443	581	105 kB	334	58 kB	247	47 kB
10.248.249.102	58707	563	91 kB	240	43 kB	323	49 kB
64.233.190.139	443	560	473 kB	412	433 kB	148	41 kB
157.240.204.15	443	556	425 kB	363	386 kB	193	38 kB
64.233.190.94	443	544	433 kB	367	370 kB	177	63 kB
108.177.123.95	443	537	304 kB	317	221 kB	220	83 kB
10.248.249.102	61698	498	64 kB	210	29 kB	288	35 kB
10.248.249.102	62111	464	427 kB	102	18 kB	362	410 kB
64.233.190.154	443	451	351 kB	303	308 kB	148	42 kB
10.248.249.102	61702	420	56 kB	210	29 kB	210	27 kB
10.248.249.102	61707	420	56 kB	210	29 kB	210	27 kB
142.250.0.157	443	407	141 kB	237	103 kB	170	38 kB
64.233.186.95	443	406	174 kB	230	119 kB	176	55 kB
108.177.123.190	443	404	264 kB	227	176 kB	177	88 kB
64.233.190.95	443	397	163 kB	221	122 kB	176	41 kB
142.251.0.94	443	391	195 kB	218	108 kB	173	87 kB

- 8801
- 61700
- 443
- 51900

- Posibles vulnerabilidades observadas (tráfico no cifrado, etc.)

Tendría que revisar a detalle el tráfico generado para determinar si hay vulnerabilidades mayores, a simple vista en el tráfico http se logran identificar los nombres de algunos archivos y sus posibles rutas los cuales no se encuentran cifrados.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.        Time          Source           Destination      Protoc Lengt Info
    34778 101.560596965 216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (PNG)
    34557 101.075056849 10.248.249.102   216.239.32.21    HTTP    10… GET /_img/web/estructuraBody.png HTTP/1.1
    34545 101.010427134 216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (text/html)
    34479 100.772060215 10.248.249.102   216.239.32.21    HTTP    11… GET /es/web/html5-estructura-cuerpo.html HTTP/1.1
    32826 95.284241473  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (JPEG JFIF image)
    32790 94.757263492  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (JPEG JFIF image)
    32737 94.482315822  142.250.0.154    10.248.249.102   HTTP    22… HTTP/1.1 200 OK  (text/javascript)
    32708 94.457331663  10.248.249.102   216.239.32.21    HTTP    10… GET /_img/web/image002.jpg HTTP/1.1
    32707 94.457281775  10.248.249.102   216.239.32.21    HTTP    10… GET /_img/web/image001.jpg HTTP/1.1
    32706 94.456490406  10.248.249.102   142.250.0.154    HTTP    751 GET /pagead/js/adsbygoogle.js HTTP/1.1
    32704 94.443676891  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (text/html)
    32627 93.667176731  10.248.249.102   216.239.32.21    HTTP    11… GET /es/web/web3.html HTTP/1.1
    28296 82.439473237  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (image/x-icon)
    28139 82.233880585  10.248.249.102   216.239.32.21    HTTP    986 GET /favicon.ico HTTP/1.1
    24810 80.401469917  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (PNG)
    24801 80.385818096  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (PNG)
    24786 80.371171690  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (PNG)
    24737 80.331808407  108.177.123.113  10.248.249.102   HTTP    293 HTTP/1.1 301 Moved Permanently
    24735 80.312067107  216.239.32.21    10.248.249.102   HTTP    56… HTTP/1.1 200 OK  (PNG)
    24696 80.251702811  216.239.32.21    10.248.249.102   HTTP     60 HTTP/1.1 200 OK  (PNG)
    24537 80.181048341  216.239.32.21    10.248.249.102   HTTP    52… HTTP/1.1 200 OK  (PNG)
    24292 80.125973460  10.248.249.102   108.177.123.113  HTTP    730 GET / HTTP/1.1
    23981 80.019815975  10.248.249.102   216.239.32.21    HTTP    487 GET /_img/eng48x48.png HTTP/1.1
    23953 80.011940882  10.248.249.102   216.239.32.21    HTTP    488 GET /_img/web/form3.png HTTP/1.1
    23951 80.011607768  10.248.249.102   216.239.32.21    HTTP    488 GET /_img/web/form2.png HTTP/1.1
    23949 80.011131808  10.248.249.102   216.239.32.21    HTTP    487 GET /_img/web/form.png HTTP/1.1
    23948 80.011131497  10.248.249.102   216.239.32.21    HTTP    492 GET /_img/web/metodoget.png HTTP/1.1
    23945 80.006636466  10.248.249.102   216.239.32.21    HTTP    487 GET /_img/web/http.png HTTP/1.1
    23941 80.003542892  216.239.32.21    10.248.249.102   HTTP    13… HTTP/1.1 200 OK  (PNG)
    23940 80.003542812  216.239.32.21    10.248.249.102   HTTP    25… HTTP/1.1 200 OK  (application/x-javascript)
    23935 79.999948769  142.250.0.154    10.248.249.102   HTTP    161 HTTP/1.1 200 OK  (text/javascript)
    23931 79.999404390  216.239.32.21    10.248.249.102   HTTP    757 HTTP/1.1 200 OK  (application/x-javascript)
    23920 79.995134179  216.239.32.21    10.248.249.102   HTTP    494 HTTP/1.1 200 OK  (application/x-javascript)
    23914 79.990807597  10.248.249.102   142.250.0.154    HTTP    594 GET /pagead/show_ads.js HTTP/1.1
    23909 79.985818194  216.239.32.21    10.248.249.102   HTTP     84 HTTP/1.1 200 OK  (text/css)
    23876 79.947234341  142.250.0.132    10.248.249.102   HTTP    38… HTTP/1.1 200 OK  (PNG)
    23863 79.735369520  10.248.249.102   142.250.0.132    HTTP    681 GET /_445Wsy7NoNs/TQ9C3-aaKQI/AAAAAAAAABo/kp6dD8FLBjA/youtube.png HTTP/1.1
    23852 79.710390799  142.250.0.132    10.248.249.102   HTTP    28… HTTP/1.1 200 OK  (PNG)
    23843 79.513688869  10.248.249.102   142.250.0.132    HTTP    682 GET /_445Wsy7NoNs/TQ9C3ldKaWI/AAAAAAAAABc/6-9I19b1g2k/facebook.png HTTP/1
    23834 79.496293859  142.250.0.132    10.248.249.102   HTTP    521 HTTP/1.1 200 OK  (PNG)
    23829 79.423662161  216.239.32.21    10.248.249.102   HTTP    704 HTTP/1.1 200 OK  (text/css)
    23786 79.282312629  10.248.249.102   142.250.0.132    HTTP    681 GET /_445Wsy7NoNs/TQ9C31Z8YFI/AAAAAAAAABk/3jDAcnYvqww/twitter.png HTTP/1.1
```

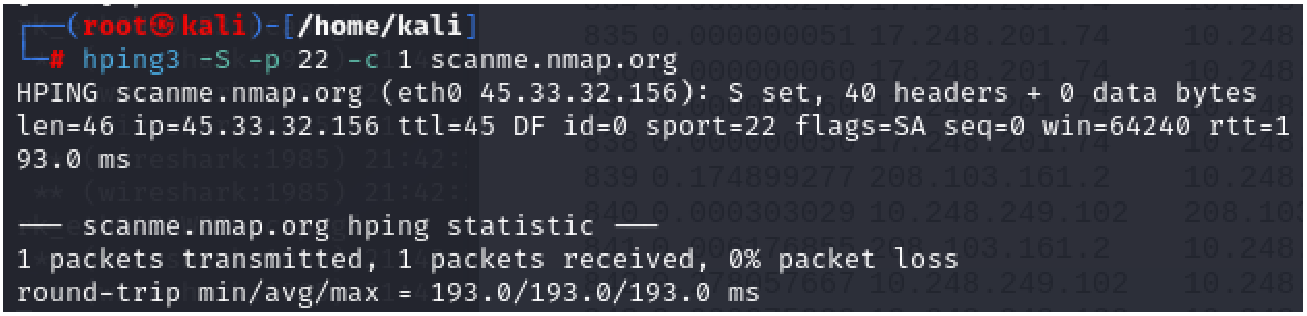
```
    PNG Signature: 89504e470d0a1a0a
  ▾ Image Header (IHDR)
      Len: 13
      Type: IHDR
      ..0. .... .... .... .... .... .... .... = Ancillary: This is a CRITICAL chunk
      .... .... ..0. .... .... .... .... .... = Private: This is a PUBLIC chunk
      .... .... .... .... .... .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy
      Width: 48
      Height: 48
      Bit Depth: 8
      Colour Type: Truecolour with alpha (6)
      Compression Method: Deflate (0)
      Filter Method: Adaptive (0)
      Interlace Method: No interlace (0)
      CRC: 0x5702f987
```

```
0000  3c 7c 3f 58 fa 21 d8 ec  5e b9 7b b2 08 00 4
0010  0e ca 8f 5a 00 00 7a 06  0e 77 8e fa 00 84 0
0020  f9 66 00 50 dd 46 db 58  c3 73 dc 37 a8 91 5
0030  04 1c a2 99 00 00 48 54  54 50 2f 31 2e 31 2
0040  30 30 20 4f 4b 0d 0a 41  63 63 65 73 73 2d 4
0050  6e 74 72 6f 6c 2d 41 6c  6c 6f 77 2d 4f 72 6
0060  69 6e 3a 20 2a 0d 0a 54  69 6d 69 6e 67 2d 4
0070  6c 6f 77 2d 4f 72 69 67  69 6e 3a 20 2a 0d 0
0080  63 63 65 73 73 2d 43 6f  6e 74 72 6f 6c 2d 4
0090  70 6f 73 65 2d 48 65 61  64 65 72 73 3a 20 4
00a0  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 0d 0a 4
00b0  6e 74 65 6e 74 2d 44 69  73 70 6f 73 69 74 6
00c0  6e 3a 20 69 6e 6c 69 6e  65 3b 66 69 6c 65 6
00d0  6d 65 3d 22 79 6f 75 74  75 62 65 2e 70 6e 6
00e0  0d 0a 58 2d 43 6f 6e 74  65 6e 74 2d 54 79 7
```

Hypertext Transfer Protocol: Protocol | Packets: 102621 · Displayed: 50 (0.0%) · Marked: 1 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

Análisis de Conectividad y Respuesta de Red Utilizando tanto hping3 como Wireshark:

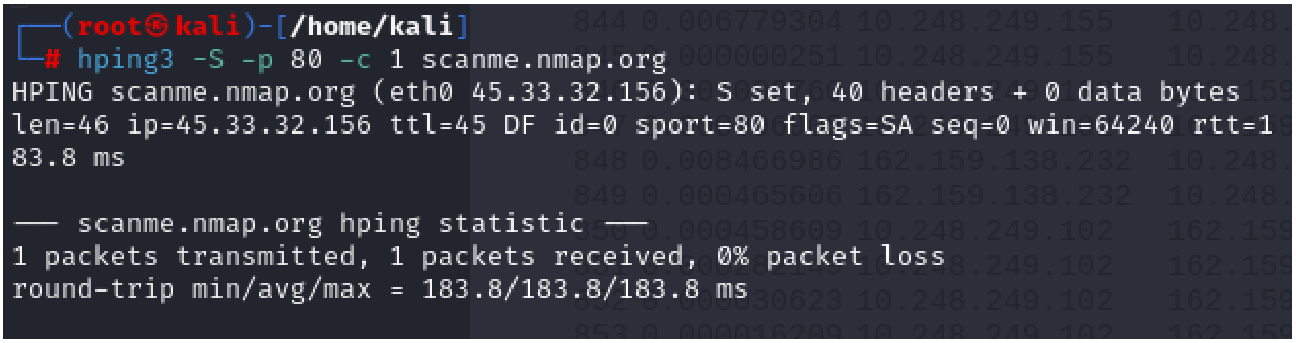
- a) Realizar un análisis de conectividad a diferentes puertos de un servidor remoto:
    - Puerto 22 (SSH)



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 22 -c 1 scanme.nmap.org
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=45 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=1
93.0 ms

--- scanme.nmap.org hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 193.0/193.0/193.0 ms
```

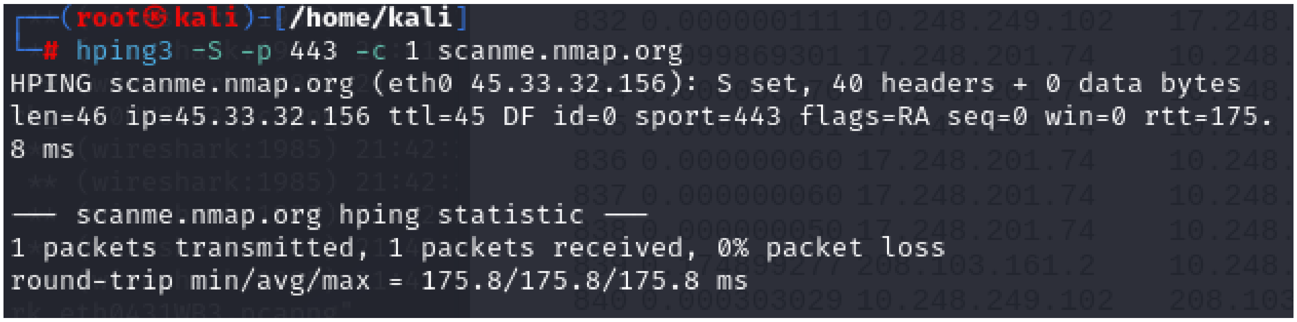
- Puerto 80 (HTTP)



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 80 -c 1 scanme.nmap.org
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=45 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=1
83.8 ms

--- scanme.nmap.org hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 183.8/183.8/183.8 ms
```

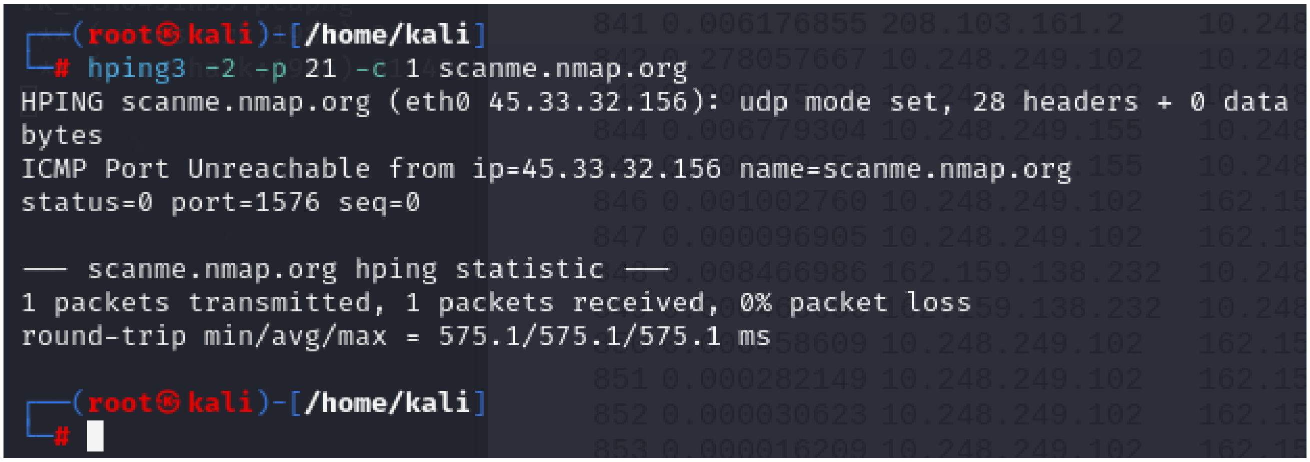
- Puerto 443 (HTTPS)



```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -S -p 443 -c 1 scanme.nmap.org
HPING scanme.nmap.org (eth0 45.33.32.156): S set, 40 headers + 0 data bytes
len=46 ip=45.33.32.156 ttl=45 DF id=0 sport=443 flags=RA seq=0 win=0 rtt=175.
8 ms

--- scanme.nmap.org hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 175.8/175.8/175.8 ms
```

- ○ Puerto 21 (FTP)



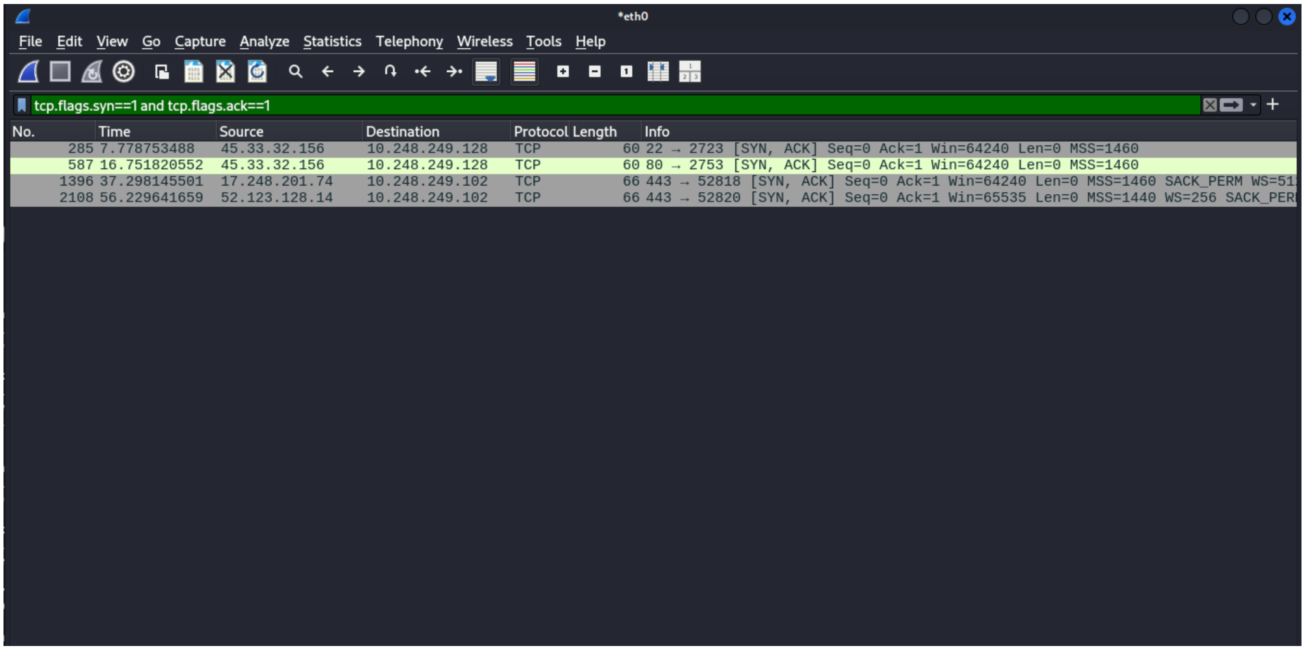
```
┌──(root㉿kali)-[/home/kali]
└─# hping3 -2 -p 21 -c 1 scanme.nmap.org
HPING scanme.nmap.org (eth0 45.33.32.156): udp mode set, 28 headers + 0 data
bytes
ICMP Port Unreachable from ip=45.33.32.156 name=scanme.nmap.org
status=0 port=1576 seq=0

--- scanme.nmap.org hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 575.1/575.1/575.1 ms

┌──(root㉿kali)-[/home/kali]
└─# 
```

- b) Documentar qué puertos están abiertos, cerrados o filtrados

Abiertos



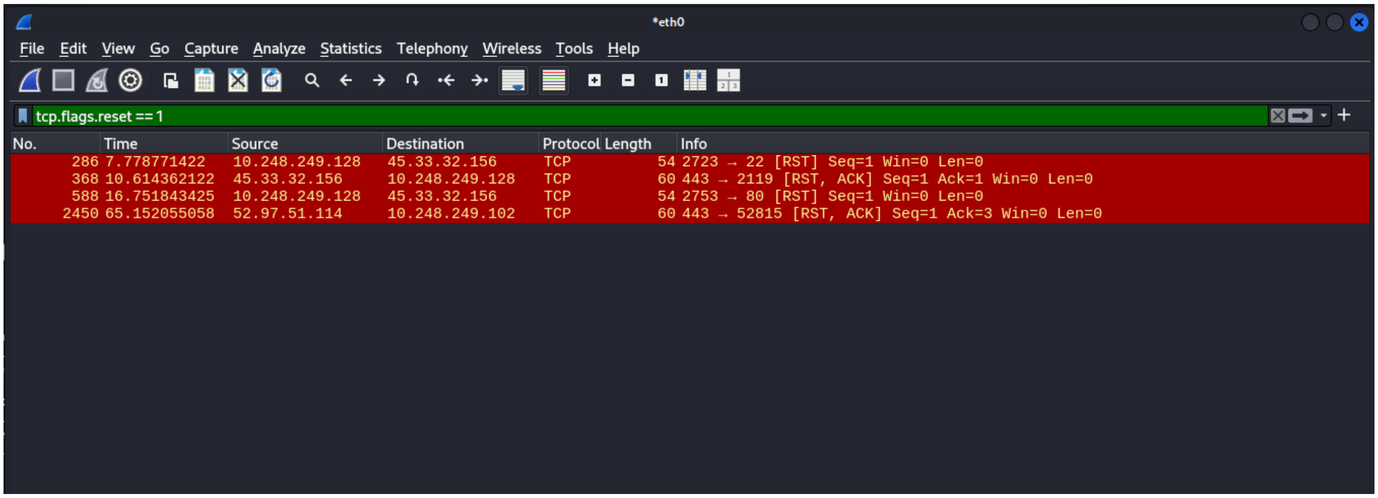
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn==1 and tcp.flags.ack==1

No.	Time	Source	Destination	Protocol	Length	Info
285	7.778753488	45.33.32.156	10.248.249.128	TCP	60	22 → 2723 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
587	16.751820552	45.33.32.156	10.248.249.128	TCP	60	80 → 2753 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1396	37.298145501	17.248.201.74	10.248.249.102	TCP	66	443 → 52818 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=51
2108	56.229641659	52.123.128.14	10.248.249.102	TCP	66	443 → 52820 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PER

- **22**
- **80**
- **443**

Cerrados

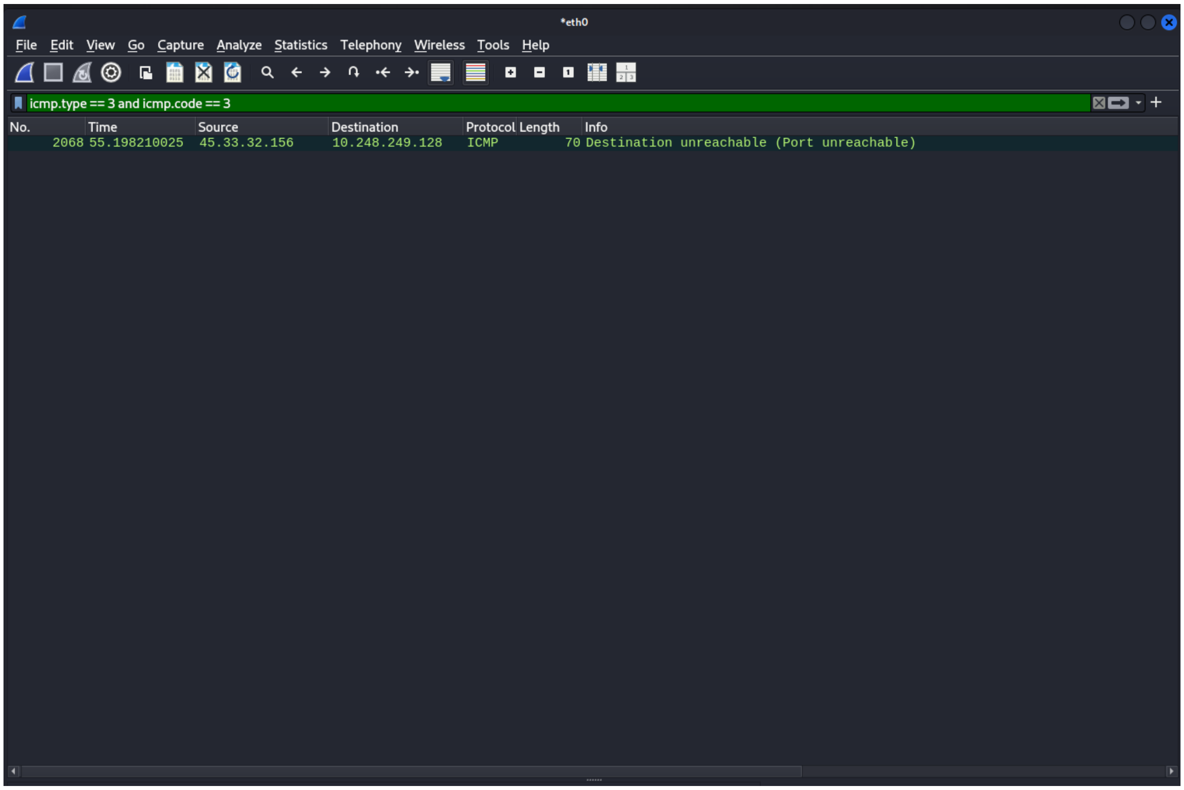

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.reset == 1

```
No.     Time         Source          Destination     Protocol Length Info
    286 7.778771422  10.248.249.128  45.33.32.156    TCP          54 2723 → 22 [RST] Seq=1 Win=0 Len=0
    368 10.614362122 45.33.32.156    10.248.249.128  TCP          60 443 → 2119 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    588 16.751843425 10.248.249.128  45.33.32.156    TCP          54 2753 → 80 [RST] Seq=1 Win=0 Len=0
   2450 65.152055058 52.97.51.114    10.248.249.102  TCP          60 443 → 52815 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0
```

- 22
- 2119
- 80

Puerto UDP

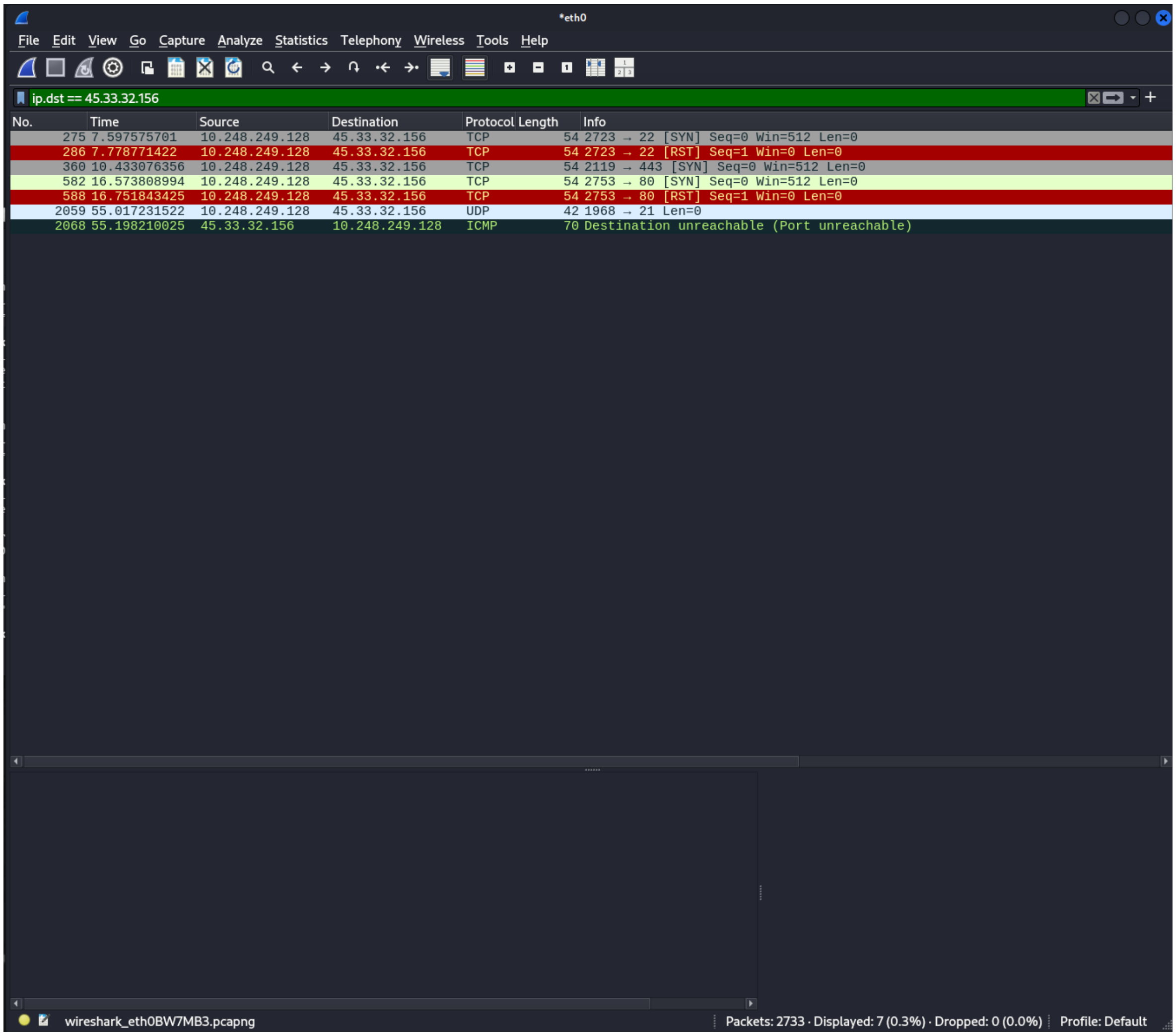

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp.type == 3 and icmp.code == 3

```
No.     Time         Source          Destination     Protocol Length Info
   2068 55.198210025 45.33.32.156    10.248.249.128  ICMP         70 Destination unreachable (Port unreachable)
```

No hay respuesta porque el protocolo UDP no necesita respuesta del host para transmitir datos

Filtrados


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 45.33.32.156

```
No.     Time         Source          Destination     Protocol Length Info
    275 7.597575701  10.248.249.128  45.33.32.156    TCP          54 2723 → 22 [SYN] Seq=0 Win=512 Len=0
    286 7.778771422  10.248.249.128  45.33.32.156    TCP          54 2723 → 22 [RST] Seq=1 Win=0 Len=0
    360 10.433076356 10.248.249.128  45.33.32.156    TCP          54 2119 → 443 [SYN] Seq=0 Win=512 Len=0
    582 16.573808994 10.248.249.128  45.33.32.156    TCP          54 2753 → 80 [SYN] Seq=0 Win=512 Len=0
    588 16.751843425 10.248.249.128  45.33.32.156    TCP          54 2753 → 80 [RST] Seq=1 Win=0 Len=0
   2059 55.017231522 10.248.249.128  45.33.32.156    UDP          42 1968 → 21 Len=0
   2068 55.198210025 45.33.32.156    10.248.249.128  ICMP         70 Destination unreachable (Port unreachable)
```

wireshark_eth0BW7MB3.pcapng | Packets: 2733 · Displayed: 7 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

- c) Analizar los tiempos de respuesta y patrones de conectividad

Puerto 22: Tiempo de respuesta promedio 193.0 ms

Puerto 80: Tiempo de respuesta promedio 183.8 ms

Puerto 443: Tiempo de respuesta promedio 175.8 ms

Puerto 21: Tiempo de respuesta promedio 575.1 ms

Recomendaciones:

De acuerdo a los hallazgos obtenidos en las pruebas se pueden indicar las siguientes recomendaciones:

- Implementar reglas para asegurar el acceso solo a sitios HTTPS para asegurar que toda la comunicación se encuentre cifrada, con esto se puede mitigar fuga de información a través de la red.
- Revisar periódicamente servidores para mantener puertos en desuso cerrados.
- Aplicar hardening al equipamiento de red.

Conclusiones:

Este análisis demostró que aunque la red es funcional, presenta vulnerabilidades en cuanto a la transmisión de datos en Texto plano (sitios http). El uso de herramientas de seguridad como hping3 y wireshark es fundamental para identificar los riesgos a los que se expone la red y documentarlos para implementar medidas que faciliten la mitigación de las vulnerabilidades.

Este informe resalta la importancia de realizar configuraciones en los servicios u equipos que permitan proteger la red de amenazas externas.