Utilizando Layer7

Para Filter y QoS

PROZCENTER
CENTRO DE PROFESIONALES

Sobre nosotros

Cursos oficiales

Dictamos entrenamientos oficiales en modalidad presencial y virtual de las marcas MikroTik, Ubiquiti, LigoWave y redes TCP/IP.

Ver catálogo

Consultoría

Contamos con un grupo de consultores profesionales con conocimiento y experiencia en las áreas de redes de datos y TI.

Más información

Soporte

A través de nuestro Centro de Soporte, alineamos los recursos necesarios para ofrecer asistencia a redes ISP y empresariales.

Consultar planes

Objetivo de esta presentación

- Poder detectar y marcar tráfico en base al contenido de alguno de los paquetes de una conexión.
- Aplicar reglas de **Filter**.
- Aplicar políticas de **QoS**.
- En esta presentación se darán ejemplos con sitios web.

Agenda

- **Introducción**
- **Comunicación con un sitio web**
  - Comunicación DNS
  - Comunicación HTTP
  - Comunicación HTTPs
  - Comunicación QUIC
- **Layer7 en acción**
  - Detección con Layer7
  - Ejemplos con Filter y QoS
- **Consideraciones especiales**
  - Compatibilidad con IPv6
  - DNS gestionado

Tipo de comunicaciones

PROZCENTER
CENTRO DE PROFESIONALES

Introducción

Algunos mitos y verdades:

“Layer7 no funciona con tráfico HTTPs”

Cierto, aunque de todos modos algo puede hacerse.

“Layer7 no funciona con servicios de Google”

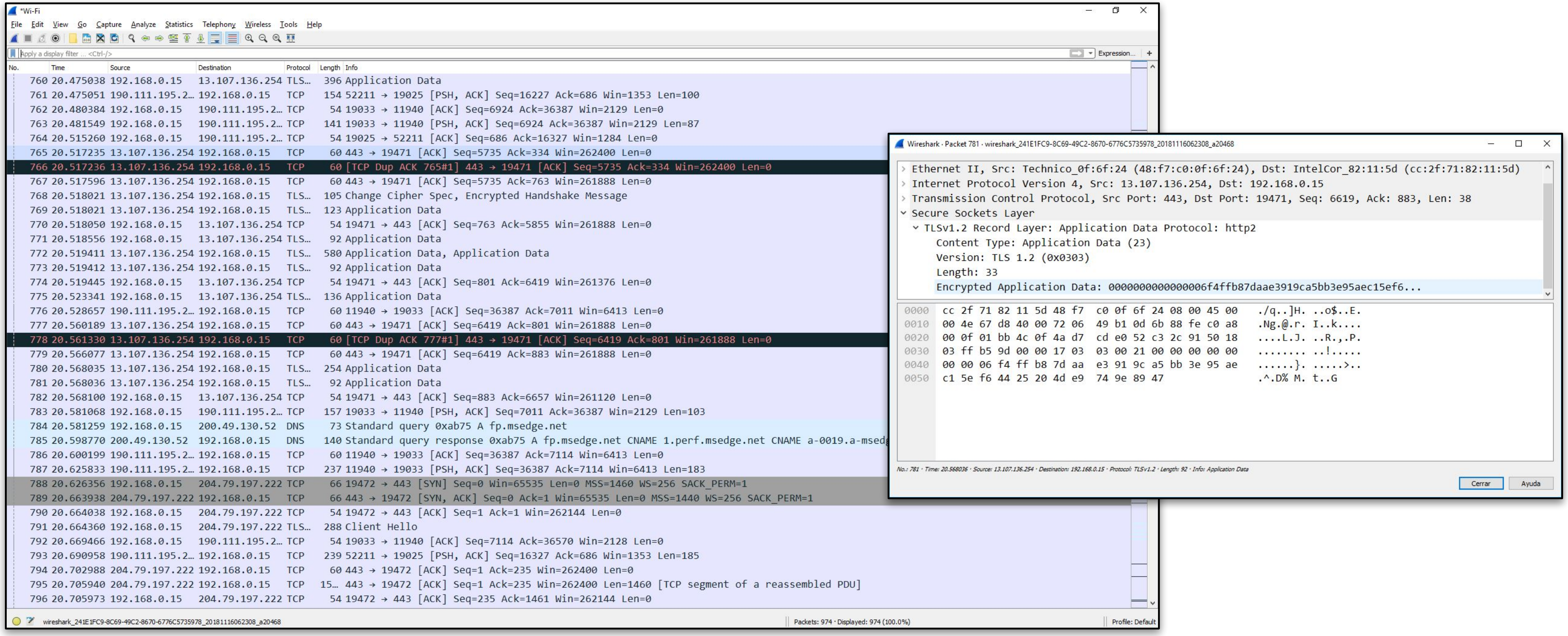
Falso, el problema viene de asociado al protocolo QUIC.

“Layer7 me carga mucho el CPU”

Cierto, pero bien configurado podemos evitar el problema.

Comunicación con un sitio Web

- Para conocer cómo funcionan estas comunicaciones utilizamos Wireshark:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source          Destination     Protocol Length Info
 760 20.475038 192.168.0.15    13.107.136.254  TLS…      396 Application Data
 761 20.475051 190.111.195.2…  192.168.0.15    TCP       154 52211 → 19025 [PSH, ACK] Seq=16227 Ack=686 Win=1353 Len=100
 762 20.480384 192.168.0.15    190.111.195.2…  TCP        54 19033 → 11940 [ACK] Seq=6924 Ack=36387 Win=2129 Len=0
 763 20.481549 192.168.0.15    190.111.195.2…  TCP       141 19033 → 11940 [PSH, ACK] Seq=6924 Ack=36387 Win=2129 Len=87
 764 20.515260 192.168.0.15    190.111.195.2…  TCP        54 19025 → 52211 [ACK] Seq=686 Ack=16327 Win=1284 Len=0
 765 20.517235 13.107.136.254  192.168.0.15    TCP        60 443 → 19471 [ACK] Seq=5735 Ack=334 Win=262400 Len=0
 766 20.517236 13.107.136.254  192.168.0.15    TCP        60 [TCP Dup ACK 765#1] 443 → 19471 [ACK] Seq=5735 Ack=334 Win=262400 Len=0
 767 20.517596 13.107.136.254  192.168.0.15    TCP        60 443 → 19471 [ACK] Seq=5735 Ack=763 Win=261888 Len=0
 768 20.518021 13.107.136.254  192.168.0.15    TLS…      105 Change Cipher Spec, Encrypted Handshake Message
 769 20.518021 13.107.136.254  192.168.0.15    TLS…      123 Application Data
 770 20.518050 192.168.0.15    13.107.136.254  TCP        54 19471 → 443 [ACK] Seq=763 Ack=5855 Win=261888 Len=0
 771 20.518556 192.168.0.15    13.107.136.254  TLS…       92 Application Data
 772 20.519411 13.107.136.254  192.168.0.15    TLS…      580 Application Data, Application Data
 773 20.519412 13.107.136.254  192.168.0.15    TLS…       92 Application Data
 774 20.519445 192.168.0.15    13.107.136.254  TCP        54 19471 → 443 [ACK] Seq=801 Ack=6419 Win=261376 Len=0
 775 20.523341 192.168.0.15    13.107.136.254  TLS…      136 Application Data
 776 20.528657 190.111.195.2…  192.168.0.15    TCP        60 11940 → 19033 [ACK] Seq=36387 Ack=7011 Win=6413 Len=0
 777 20.560189 13.107.136.254  192.168.0.15    TCP        60 443 → 19471 [ACK] Seq=6419 Ack=801 Win=261888 Len=0
 778 20.561330 13.107.136.254  192.168.0.15    TCP        60 [TCP Dup ACK 777#1] 443 → 19471 [ACK] Seq=6419 Ack=801 Win=261888 Len=0
 779 20.566077 13.107.136.254  192.168.0.15    TCP        60 443 → 19471 [ACK] Seq=6419 Ack=883 Win=261888 Len=0
 780 20.568035 13.107.136.254  192.168.0.15    TLS…      254 Application Data
 781 20.568036 13.107.136.254  192.168.0.15    TLS…       92 Application Data
 782 20.568100 192.168.0.15    13.107.136.254  TCP        54 19471 → 443 [ACK] Seq=883 Ack=6657 Win=261120 Len=0
 783 20.581068 192.168.0.15    190.111.195.2…  TCP       157 19033 → 11940 [PSH, ACK] Seq=7011 Ack=36387 Win=2129 Len=103
 784 20.581259 192.168.0.15    200.49.130.52   DNS        73 Standard query 0xab75 A fp.msedge.net
 785 20.598770 200.49.130.52   192.168.0.15    DNS       140 Standard query response 0xab75 A fp.msedge.net CNAME 1.perf.msedge.net CNAME a-0019.a-msedg
 786 20.600199 190.111.195.2…  192.168.0.15    TCP        60 11940 → 19033 [ACK] Seq=36387 Ack=7114 Win=6413 Len=0
 787 20.625833 190.111.195.2…  192.168.0.15    TCP       237 11940 → 19033 [PSH, ACK] Seq=36387 Ack=7114 Win=6413 Len=183
 788 20.626356 192.168.0.15    204.79.197.222  TCP        66 19472 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 789 20.663938 204.79.197.222  192.168.0.15    TCP        66 443 → 19472 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
 790 20.664038 192.168.0.15    204.79.197.222  TCP        54 19472 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 791 20.664360 192.168.0.15    204.79.197.222  TLS…      288 Client Hello
 792 20.669466 192.168.0.15    190.111.195.2…  TCP        54 19033 → 11940 [ACK] Seq=7114 Ack=36570 Win=2128 Len=0
 793 20.690958 190.111.195.2…  192.168.0.15    TCP       239 52211 → 19025 [PSH, ACK] Seq=16327 Ack=686 Win=1353 Len=185
 794 20.702988 204.79.197.222  192.168.0.15    TCP        60 443 → 19472 [ACK] Seq=1 Ack=235 Win=262400 Len=0
 795 20.705940 204.79.197.222  192.168.0.15    TCP       15… 443 → 19472 [ACK] Seq=1 Ack=235 Win=262400 Len=1460 [TCP segment of a reassembled PDU]
 796 20.705973 192.168.0.15    204.79.197.222  TCP        54 19472 → 443 [ACK] Seq=235 Ack=1461 Win=262144 Len=0
```

wireshark_241E1FC9-8C69-49C2-8670-6776C5735978_20181116062308_a20468 | Packets: 974 · Displayed: 974 (100.0%) | Profile: Default

Wireshark · Packet 781 · wireshark_241E1FC9-8C69-49C2-8670-6776C5735978_20181116062308_a20468

```
> Ethernet II, Src: Technico_0f:6f:24 (48:f7:c0:0f:6f:24), Dst: IntelCor_82:11:5d (cc:2f:71:82:11:5d)
> Internet Protocol Version 4, Src: 13.107.136.254, Dst: 192.168.0.15
> Transmission Control Protocol, Src Port: 443, Dst Port: 19471, Seq: 6619, Ack: 883, Len: 38
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Application Data Protocol: http2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 33
      Encrypted Application Data: 0000000000000006f4ffb87daae3919ca5bb3e95aec15ef6...
```

```
0000  cc 2f 71 82 11 5d 48 f7  c0 0f 6f 24 08 00 45 00   ./q..]H. ..o$..E.
0010  00 4e 67 d8 40 00 72 06  49 b1 0d 6b 88 fe c0 a8   .Ng.@.r. I..k....
0020  00 0f 01 bb 4c 0f 4a d7  cd e0 52 c3 2c 91 50 18   ....L.J. ..R.,.P.
0030  03 ff b5 9d 00 00 17 03  03 00 21 00 00 00 00 00   ........ ..!.....
0040  00 00 06 f4 ff b8 7d aa  e3 91 9c a5 bb 3e 95 ae   ......}. .....>..
0050  c1 5e f6 44 25 20 4d e9  74 9e 89 47               .^.D% M. t..G
```

No.: 781 · Time: 20.568036 · Source: 13.107.136.254 · Destination: 192.168.0.15 · Protocol: TLSv1.2 · Length: 92 · Info: Application Data

Comunicación con un sitio Web

- Sitio común HTTP/HTTPs

  1) Consulta DNS
     (UDP 53)

  2) Conexión HTTP/HTTPs
     (TCP 80 o TCP 443)

Facebook - Inicia sesión o regístr

https://www.facebook.com

facebook

Correo electrónico o teléfono

Contraseña

Iniciar sesión

¿Olvidaste tu cuenta?

Facebook te ayuda a comunicarte y compartir con las personas que forman parte de tu vida.

Abre una cuenta

Es gratis y lo será siempre.

Nombre

Apellido

Número de celular o correo electrónico

Contraseña nueva

Fecha de nacimiento

15 nov 1993

¿Por qué tengo que indicar mi fecha de nacimiento?

Mujer Hombre

Al hacer clic en "Registrarte", aceptas nuestras Condiciones, la Política de datos y la Política de cookies. Es posible que te enviemos notificaciones por SMS, que puedes desactivar cuando quieras.

Registrarte

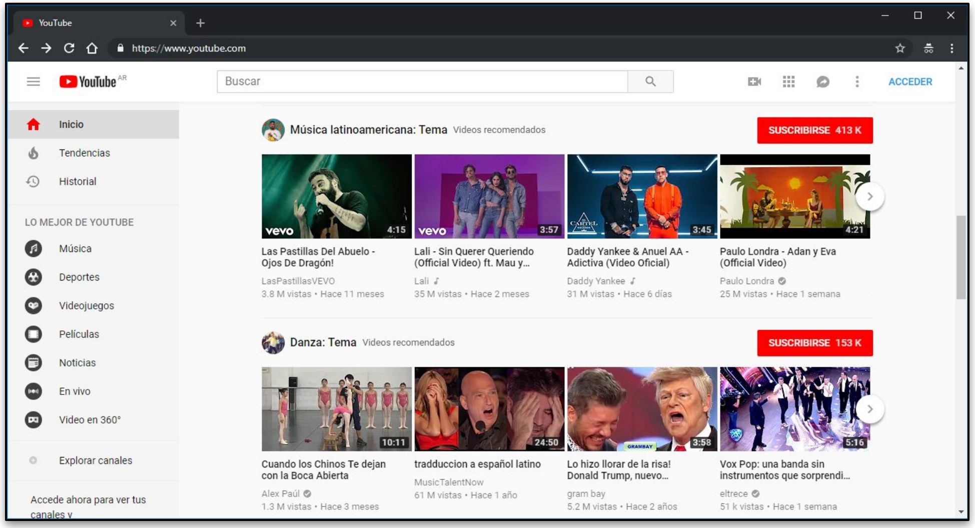
Crea una página para un personaje público, un grupo de música

Comunicación con un sitio Web

- Sitio de Google Inc. desde Chrome

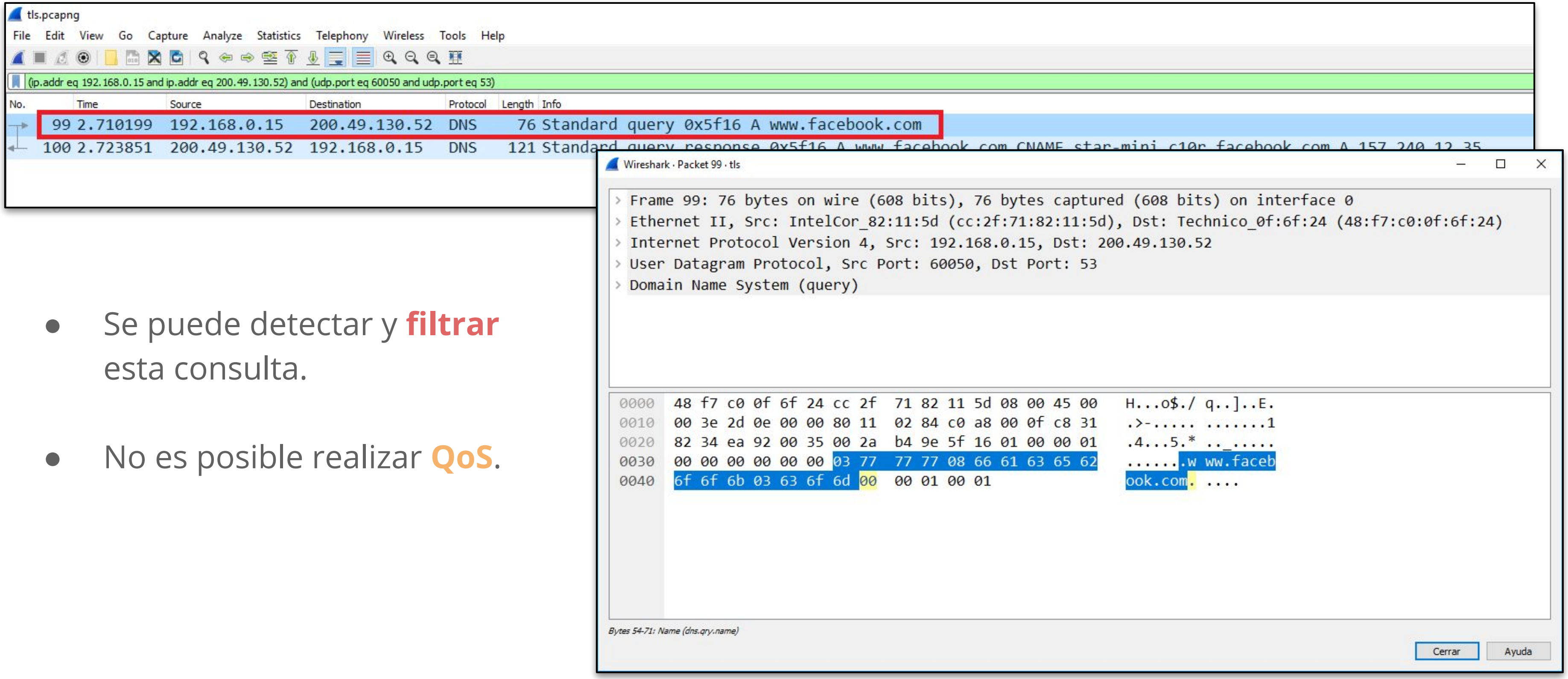
  1) Consulta DNS
  (UDP 53)

  2) Conexión QUIC
  (UDP 80 o UDP 443)


YouTube
https://www.youtube.com
YouTube AR
Buscar
ACCEDER
Inicio
Tendencias
Historial
LO MEJOR DE YOUTUBE
Música
Deportes
Videojuegos
Películas
Noticias
En vivo
Video en 360°
Explorar canales
Accede ahora para ver tus canales y
Música latinoamericana: Tema Videos recomendados
SUSCRIBIRSE 413 K
Las Pastillas Del Abuelo - Ojos De Dragón!
LasPastillasVEVO
3.8 M vistas • Hace 11 meses
Lali - Sin Querer Queriendo (Official Video) ft. Mau y...
Lali
35 M vistas • Hace 2 meses
Daddy Yankee & Anuel AA - Adictiva (Video Oficial)
Daddy Yankee
31 M vistas • Hace 6 días
Paulo Londra - Adan y Eva (Official Video)
Paulo Londra
25 M vistas • Hace 1 semana
Danza: Tema Videos recomendados
SUSCRIBIRSE 153 K
Cuando los Chinos Te dejan con la Boca Abierta
Alex Paúl
1.3 M vistas • Hace 3 meses
tradduccion a español latino
MusicTalentNow
61 M vistas • Hace 1 año
Lo hizo llorar de la risa! Donald Trump, nuevo...
gram bay
5.2 M vistas • Hace 2 años
Vox Pop: una banda sin instrumentos que sorprendi...
eltrece
51 k vistas • Hace 1 semana

PROZCENTER
CENTRO DE PROFESIONALES

Comunicación DNS


tls.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 99 · tls
Cerrar
Ayuda

```
(ip.addr eq 192.168.0.15 and ip.addr eq 200.49.130.52) and (udp.port eq 60050 and udp.port eq 53)

No.  Time      Source         Destination    Protocol  Length Info
 99 2.710199  192.168.0.15   200.49.130.52  DNS        76 Standard query 0x5f16 A www.facebook.com
100 2.723851  200.49.130.52  192.168.0.15   DNS       121 Standard query response 0x5f16 A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.12.35
```

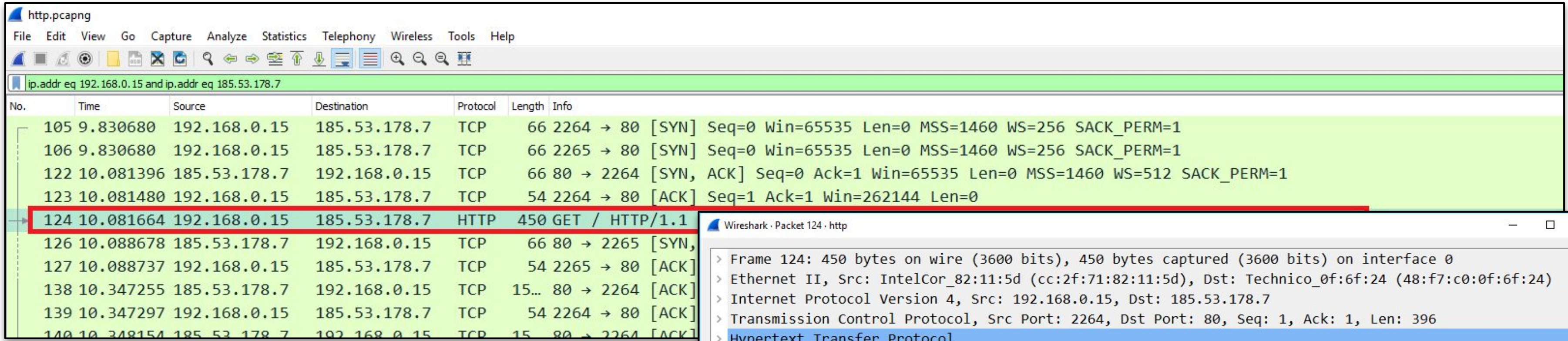
```
> Frame 99: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
> Ethernet II, Src: IntelCor_82:11:5d (cc:2f:71:82:11:5d), Dst: Technico_0f:6f:24 (48:f7:c0:0f:6f:24)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 200.49.130.52
> User Datagram Protocol, Src Port: 60050, Dst Port: 53
> Domain Name System (query)

0000  48 f7 c0 0f 6f 24 cc 2f  71 82 11 5d 08 00 45 00   H...o$./ q..]..E.
0010  00 3e 2d 0e 00 00 80 11  02 84 c0 a8 00 0f c8 31   .>-..... .......1
0020  82 34 ea 92 00 35 00 2a  b4 9e 5f 16 01 00 00 01   .4...5.* .._.....
0030  00 00 00 00 00 00 03 77  77 77 08 66 61 63 65 62   .......w ww.faceb
0040  6f 6f 6b 03 63 6f 6d 00  00 01 00 01               ook.com. ....

Bytes 54-71: Name (dns.qry.name)
```

- Se puede detectar y **filtrar** esta consulta.
- No es posible realizar **QoS**.

Comunicación HTTP

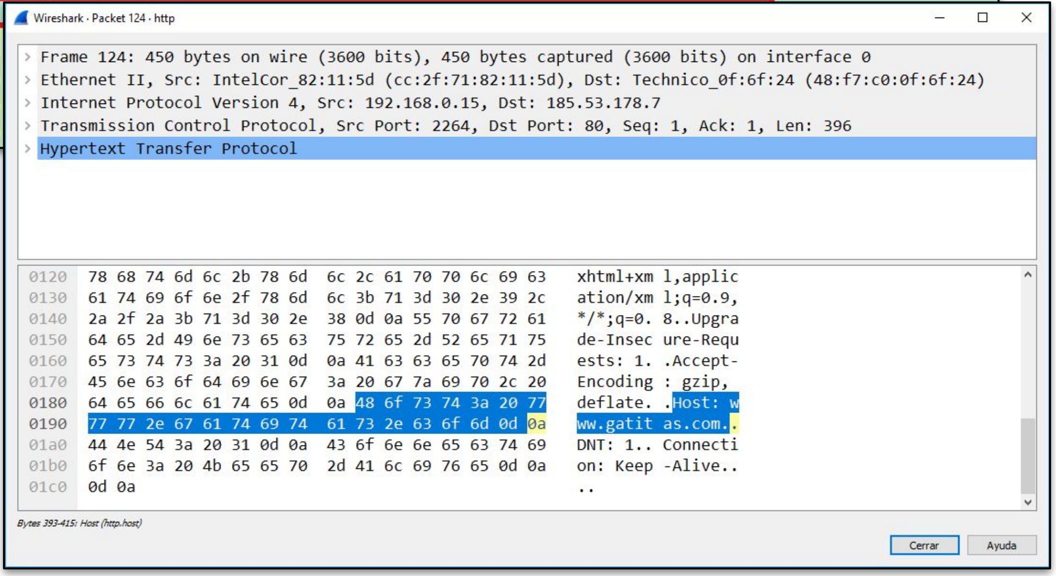


http.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr eq 192.168.0.15 and ip.addr eq 185.53.178.7

No.  Time      Source        Destination   Protocol Length Info
 105 9.830680  192.168.0.15  185.53.178.7  TCP      66 2264 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 106 9.830680  192.168.0.15  185.53.178.7  TCP      66 2265 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 122 10.081396 185.53.178.7  192.168.0.15  TCP      66 80 → 2264 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=512 SACK_PERM=1
 123 10.081480 192.168.0.15  185.53.178.7  TCP      54 2264 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 124 10.081664 192.168.0.15  185.53.178.7  HTTP    450 GET / HTTP/1.1
 126 10.088678 185.53.178.7  192.168.0.15  TCP      66 80 → 2265 [SYN,
 127 10.088737 192.168.0.15  185.53.178.7  TCP      54 2265 → 80 [ACK]
 138 10.347255 185.53.178.7  192.168.0.15  TCP     15… 80 → 2264 [ACK]
 139 10.347297 192.168.0.15  185.53.178.7  TCP      54 2264 → 80 [ACK]
 140 10.348154 185.53.178.7  192.168.0.15  TCP     15… 80 → 2264 [ACK]
```



Wireshark · Packet 124 · http

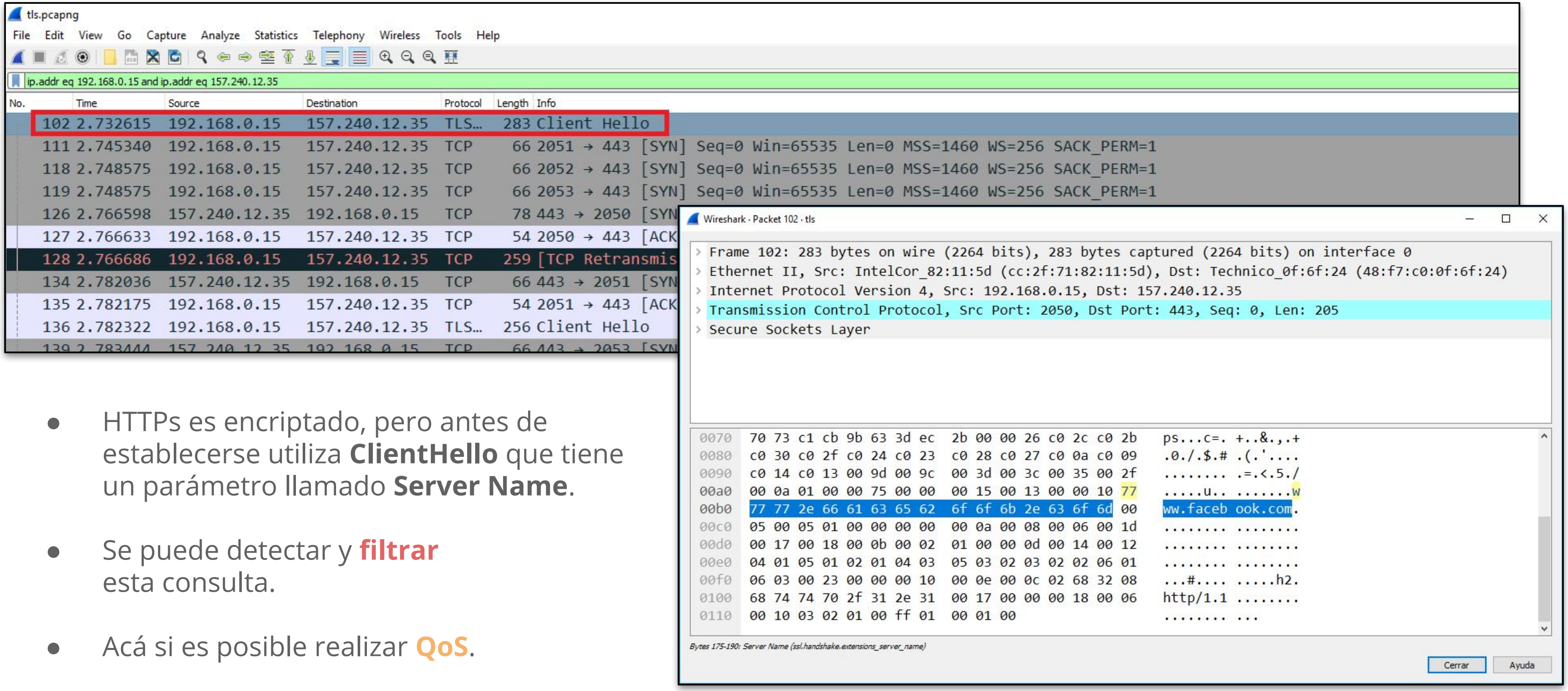
```
> Frame 124: 450 bytes on wire (3600 bits), 450 bytes captured (3600 bits) on interface 0
> Ethernet II, Src: IntelCor_82:11:5d (cc:2f:71:82:11:5d), Dst: Technico_0f:6f:24 (48:f7:c0:0f:6f:24)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 185.53.178.7
> Transmission Control Protocol, Src Port: 2264, Dst Port: 80, Seq: 1, Ack: 1, Len: 396
> Hypertext Transfer Protocol

0120  78 68 74 6d 6c 2b 78 6d  6c 2c 61 70 70 6c 69 63   xhtml+xm l,applic
0130  61 74 69 6f 6e 2f 78 6d  6c 3b 71 3d 30 2e 39 2c   ation/xm l;q=0.9,
0140  2a 2f 2a 3b 71 3d 30 2e  38 0d 0a 55 70 67 72 61   */*;q=0. 8..Upgra
0150  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
0160  65 73 74 73 3a 20 31 0d  0a 41 63 63 65 70 74 2d   ests: 1. .Accept-
0170  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 20   Encoding : gzip,
0180  64 65 66 6c 61 74 65 0d  0a 48 6f 73 74 3a 20 77   deflate. .Host: w
0190  77 77 2e 67 61 74 69 74  61 73 2e 63 6f 6d 0d 0a   ww.gatit as.com..
01a0  44 4e 54 3a 20 31 0d 0a  43 6f 6e 6e 65 63 74 69   DNT: 1.. Connecti
01b0  6f 6e 3a 20 4b 65 65 70  2d 41 6c 69 76 65 0d 0a   on: Keep -Alive..
01c0  0d 0a                                              ..

Bytes 393-415: Host (http.host)
```

- Se puede detectar y **filtrar** esta consulta.
- Acá si es posible realizar **QoS**.

Comunicación HTTPs


tls.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 102 · tls
Cerrar
Ayuda

```
ip.addr eq 192.168.0.15 and ip.addr eq 157.240.12.35

No.  Time      Source          Destination     Protocol Length Info
 102 2.732615  192.168.0.15    157.240.12.35   TLS…     283 Client Hello
 111 2.745340  192.168.0.15    157.240.12.35   TCP       66 2051 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 118 2.748575  192.168.0.15    157.240.12.35   TCP       66 2052 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 119 2.748575  192.168.0.15    157.240.12.35   TCP       66 2053 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 126 2.766598  157.240.12.35   192.168.0.15    TCP       78 443 → 2050 [SYN
 127 2.766633  192.168.0.15    157.240.12.35   TCP       54 2050 → 443 [ACK
 128 2.766686  192.168.0.15    157.240.12.35   TCP      259 [TCP Retransmis
 134 2.782036  157.240.12.35   192.168.0.15    TCP       66 443 → 2051 [SYN
 135 2.782175  192.168.0.15    157.240.12.35   TCP       54 2051 → 443 [ACK
 136 2.782322  192.168.0.15    157.240.12.35   TLS…     256 Client Hello
 139 2.783444  157.240.12.35   192.168.0.15    TCP       66 443 → 2053 [SYN
```

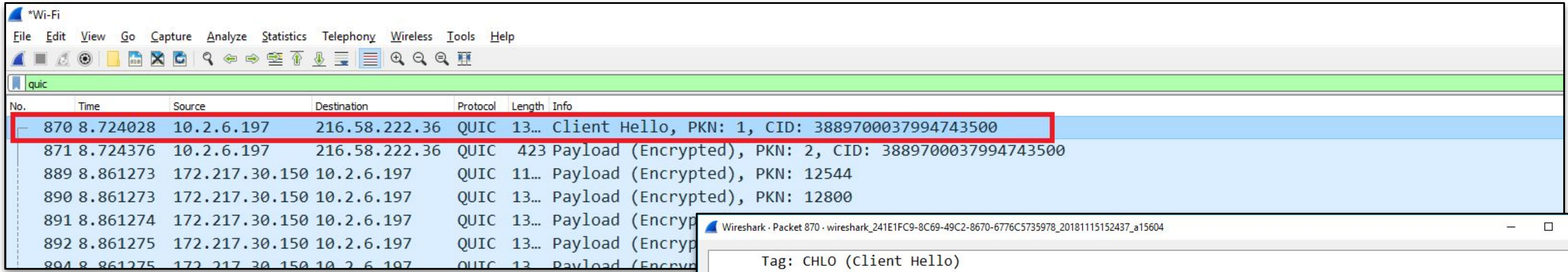
```
> Frame 102: 283 bytes on wire (2264 bits), 283 bytes captured (2264 bits) on interface 0
> Ethernet II, Src: IntelCor_82:11:5d (cc:2f:71:82:11:5d), Dst: Technico_0f:6f:24 (48:f7:c0:0f:6f:24)
> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 157.240.12.35
> Transmission Control Protocol, Src Port: 2050, Dst Port: 443, Seq: 0, Len: 205
> Secure Sockets Layer
```

```
0070  70 73 c1 cb 9b 63 3d ec  2b 00 00 26 c0 2c c0 2b   ps...c=. +..&.,.+
0080  c0 30 c0 2f c0 24 c0 23  c0 28 c0 27 c0 0a c0 09   .0./.$.# .(.'....
0090  c0 14 c0 13 00 9d 00 9c  00 3d 00 3c 00 35 00 2f   ........ .=.<.5./
00a0  00 0a 01 00 00 75 00 00  00 15 00 13 00 00 10 77   .....u.. .......w
00b0  77 77 2e 66 61 63 65 62  6f 6f 6b 2e 63 6f 6d 00   ww.faceb ook.com.
00c0  05 00 05 01 00 00 00 00  00 0a 00 08 00 06 00 1d   ........ ........
00d0  00 17 00 18 00 0b 00 02  01 00 00 0d 00 14 00 12   ........ ........
00e0  04 01 05 01 02 01 04 03  05 03 02 03 02 02 06 01   ........ ........
00f0  06 03 00 23 00 00 00 10  00 0e 00 0c 02 68 32 08   ...#.... .....h2.
0100  68 74 74 70 2f 31 2e 31  00 17 00 00 00 18 00 06   http/1.1 ........
0110  00 10 03 02 01 00 ff 01  00 01 00                  ........ ...
```

Bytes 175-190: Server Name (ssl.handshake.extensions_server_name)

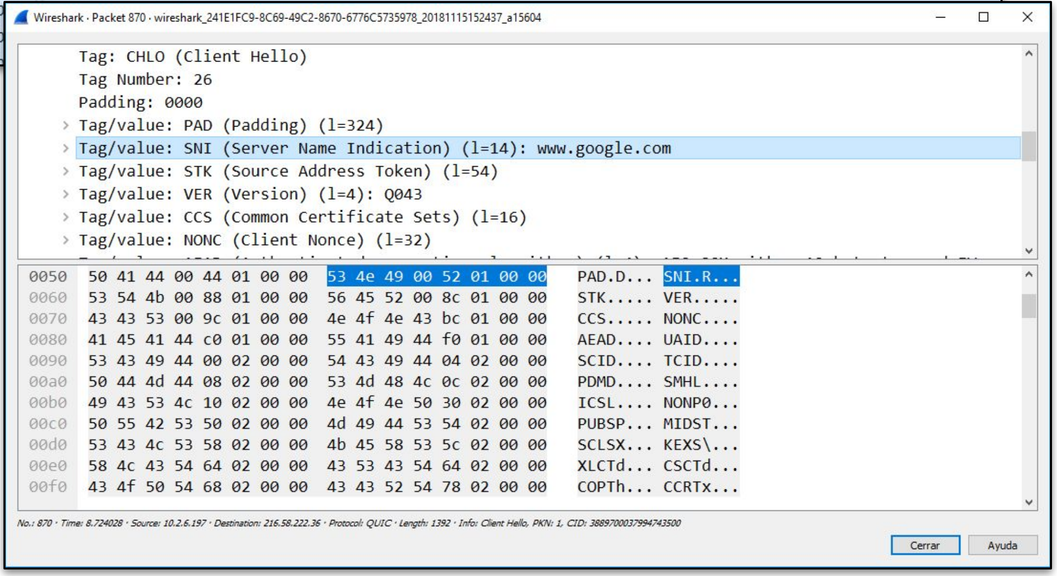
- HTTPs es encriptado, pero antes de establecerse utiliza **ClientHello** que tiene un parámetro llamado **Server Name**.
- Se puede detectar y **filtrar** esta consulta.
- Acá si es posible realizar **QoS**.

Comunicación QUIC



```
quic

No.  Time      Source         Destination    Protocol Length Info
 870 8.724028  10.2.6.197     216.58.222.36  QUIC     13…    Client Hello, PKN: 1, CID: 3889700037994743500
 871 8.724376  10.2.6.197     216.58.222.36  QUIC     423    Payload (Encrypted), PKN: 2, CID: 3889700037994743500
 889 8.861273  172.217.30.150 10.2.6.197     QUIC     11…    Payload (Encrypted), PKN: 12544
 890 8.861273  172.217.30.150 10.2.6.197     QUIC     13…    Payload (Encrypted), PKN: 12800
 891 8.861274  172.217.30.150 10.2.6.197     QUIC     13…    Payload (Encryp
 892 8.861275  172.217.30.150 10.2.6.197     QUIC     13…    Payload (Encryp
 894 8.861275  172.217.30.150 10.2.6.197     QUIC     13…    Payload (Encryp
```



Wireshark · Packet 870 · wireshark_241E1FC9-8C69-49C2-8670-6776C5735978_20181115152437_a15604

```
    Tag: CHLO (Client Hello)
    Tag Number: 26
    Padding: 0000
  > Tag/value: PAD (Padding) (l=324)
  > Tag/value: SNI (Server Name Indication) (l=14): www.google.com
  > Tag/value: STK (Source Address Token) (l=54)
  > Tag/value: VER (Version) (l=4): Q043
  > Tag/value: CCS (Common Certificate Sets) (l=16)
  > Tag/value: NONC (Client Nonce) (l=32)
```

```
0050  50 41 44 00 44 01 00 00  53 4e 49 00 52 01 00 00   PAD.D... SNI.R...
0060  53 54 4b 00 88 01 00 00  56 45 52 00 8c 01 00 00   STK..... VER.....
0070  43 43 53 00 9c 01 00 00  4e 4f 4e 43 bc 01 00 00   CCS..... NONC....
0080  41 45 41 44 c0 01 00 00  55 41 49 44 f0 01 00 00   AEAD.... UAID....
0090  53 43 49 44 00 02 00 00  54 43 49 44 04 02 00 00   SCID.... TCID....
00a0  50 44 4d 44 08 02 00 00  53 4d 48 4c 0c 02 00 00   PDMD.... SMHL....
00b0  49 43 53 4c 10 02 00 00  4e 4f 4e 50 30 02 00 00   ICSL.... NONP0...
00c0  50 55 42 53 50 02 00 00  4d 49 44 53 54 02 00 00   PUBSP... MIDST...
00d0  53 43 4c 53 58 02 00 00  4b 45 58 53 5c 02 00 00   SCLSX... KEXS\...
00e0  58 4c 43 54 64 02 00 00  43 53 43 54 64 02 00 00   XLCTd... CSCTd...
00f0  43 4f 50 54 68 02 00 00  43 43 52 54 78 02 00 00   COPTh... CCRTx...
```

No.: 870 · Time: 8.724028 · Source: 10.2.6.197 · Destination: 216.58.222.36 · Protocol: QUIC · Length: 1392 · Info: Client Hello, PKN: 1, CID: 3889700037994743500

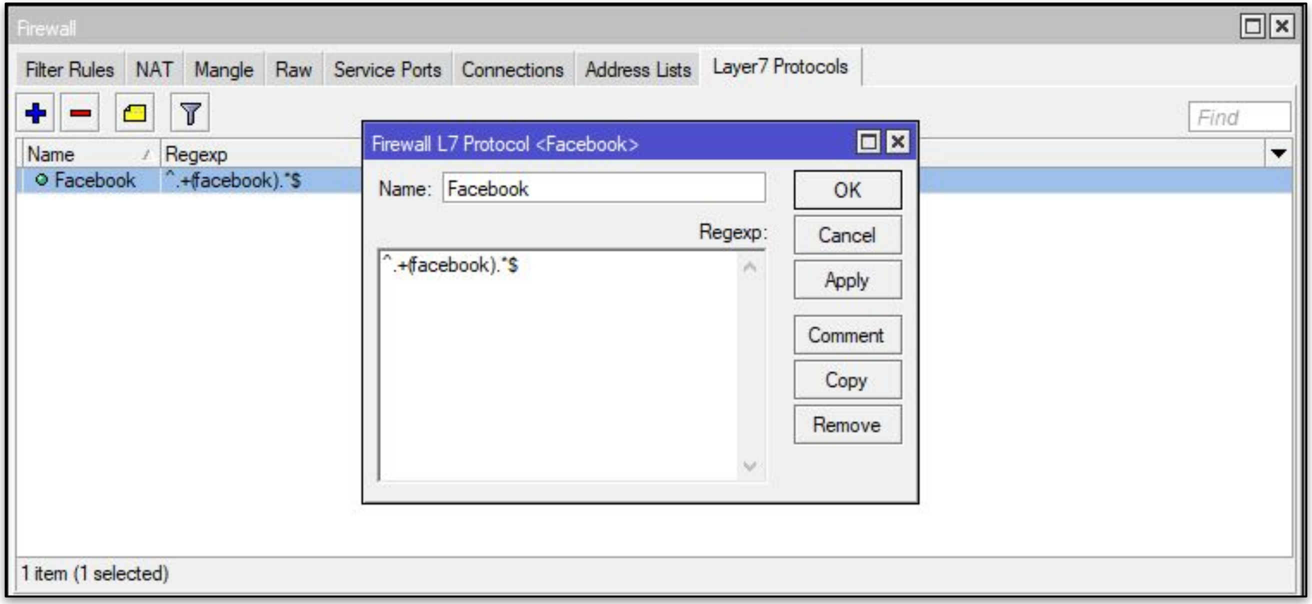
- QUIC corre sobre UDP y es encriptado, pero antes de establecerse también utiliza **ClientHello** que tiene un parámetro llamado **Server Name** (igual que TLS).
- Se puede detectar y **filtrar** esta consulta.
- Acá si es posible realizar **QoS**.

Layer7 en acción

PROZCENTER
CENTRO DE PROFESIONALES

Ejemplo con Filter - Detección con Layer7

```
/ip firewall layer7-protocol
add name=Facebook regexp="^.+(facebook).*\$"
```



Name	Regexp
Facebook	^.+(facebook).*$

1 item (1 selected)

Firewall L7 Protocol <Facebook>

Name: Facebook

Regexp:

```
^.+(facebook).*$
```

Ejemplo con Filter (HTTP/HTTPs)

```
/ip firewall filter
add comment="Analisis TCP" \
chain=forward \
protocol=tcp \
dst-port=80,443 \
connection-bytes=0-100000 \
action=jump jump-target=analisis_layer7
```

Acotar la regla a conexiones TCP 80 y 443.

Conexiones de hasta 100k de transferencia.

Salto a otra cadena.

Ejemplo con Filter (HTTP/HTTPs)

```
/ip firewall filter
add comment="Bloquear Facebook" \
chain=analisis_layer7 \
protocol=tcp \
layer7-protocol=Facebook  \
action=reject reject-with=tcp-reset
```

Registro Layer7.

Rechazo instantáneo.

Ejemplo con Filter (QUIC)

```
/ip firewall filter
add comment="Analisis UDP" \
chain=forward \
protocol=udp \
dst-port=80,443 \
connection-bytes=0-100000 \
action=jump jump-target=analisis_layer7
```

QUIC funciona en UDP.

Acotar la regla a conexiones UDP 80 y 443.

Salto a otra cadena.

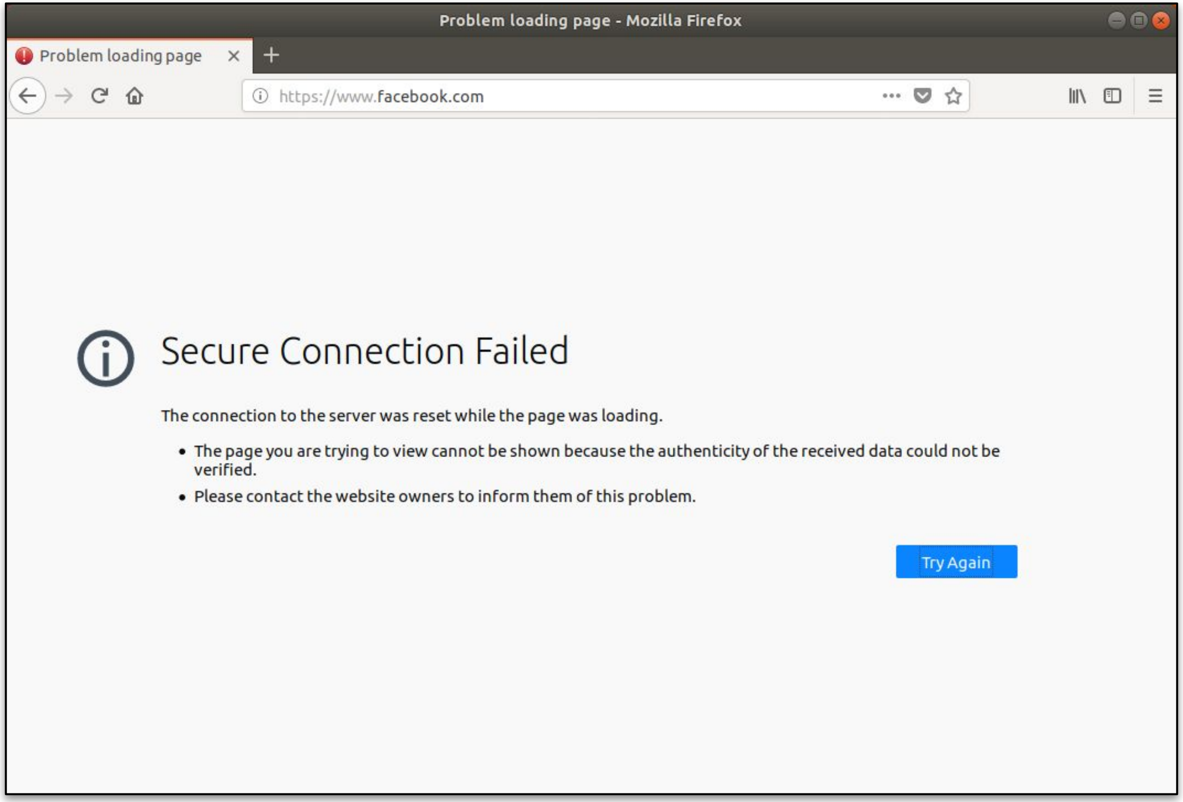
Ejemplo con Filter (QUIC)

```
/ip firewall filter
add comment="Bloquear YouTube" \
chain=analisis_layer7 \
layer7-protocol=YouTube  \
action=reject reject-with=icmp-admin-prohibited
```

Registro Layer7.

Rechazo casi instantáneo.

Ejemplo con Filter (HTTP/HTTPs/QUIC)



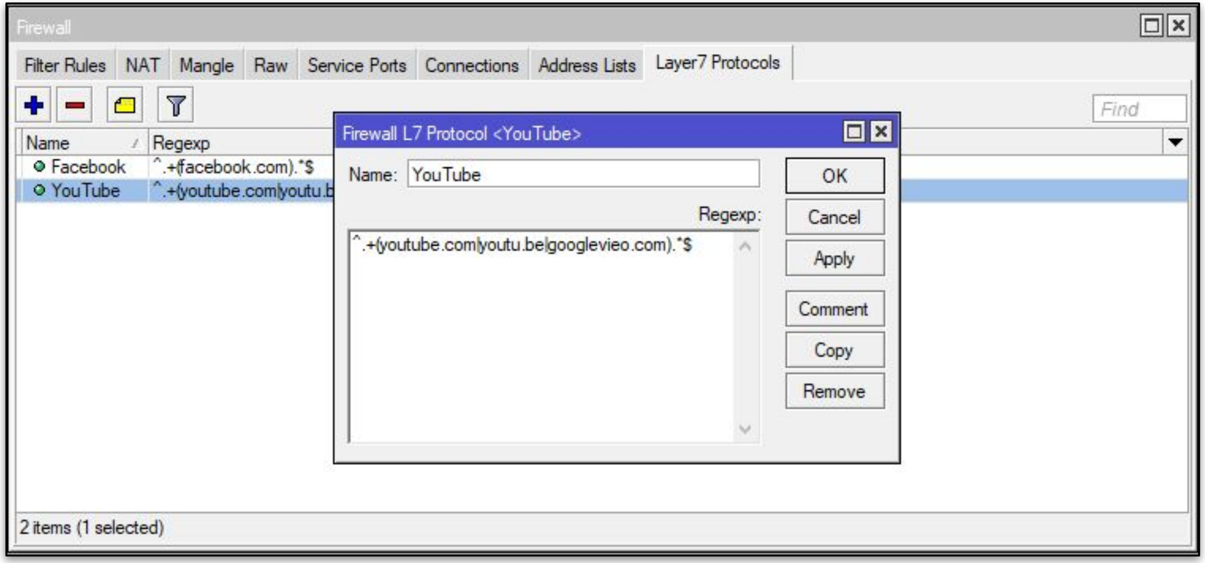
Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Ejemplo con QoS - Detección con Layer7

```
/ip firewall layer7-protocol
add name=YouTube \
regexp="^.+(youtube.com|youtu.be|googlevideo.com).*\$"
```



Name	Regexp
Facebook	^.+(facebook.com).*$
YouTube	^.+(youtube.com|youtu.b

Name: YouTube

Regexp:

```
^.+(youtube.com|youtu.be|googlevieo.com).*$
```

2 items (1 selected)

Ejemplo con QoS

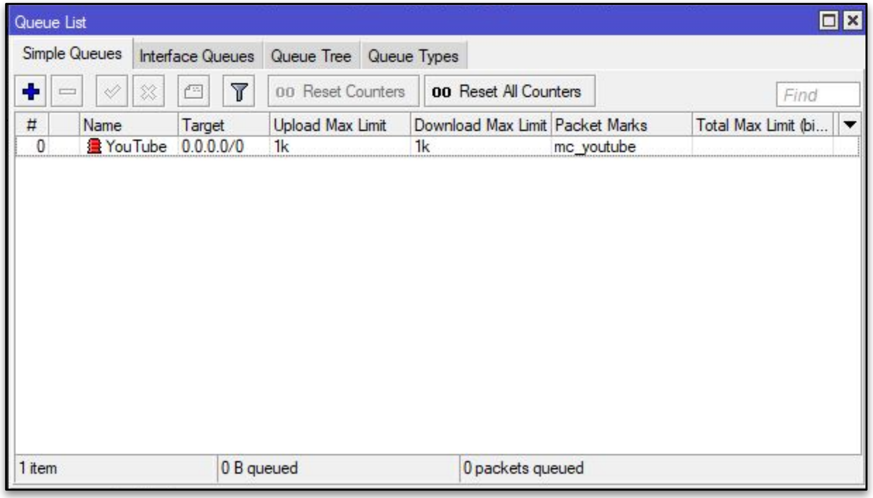
```
/ip firewall mangle
add comment="Marcar conexiones de YouTube" \
chain=forward \
connection-mark=no-mark \
layer7-protocol=YouTube \
action=mark-connection \
new-connection-mark=mc_youtube \
passthrough=yes
```

Ejemplo con QoS

```
/ip firewall mangle
add comment="Marcar paquetes de YouTube" \
chain=forward \
connection-mark=mc_youtube \
action=mark-packet \
new-packet-mark=mc_youtube \
passthrough=no
```

Ejemplo con QoS

```
/queue simple
add name="No Vas A Ver YouTube, No"  \
target="" \
packet-marks=mc_youtube \
max-limit=1k/1k
```



#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bi...
0	YouTube	0.0.0.0/0	1k	1k	mc_youtube	

```
1 item    0 B queued    0 packets queued
```

Consideraciones especiales

PROZCENTER
CENTRO DE PROFESIONALES

Consideraciones especiales

- Para QoS por sitio web, de momento esta es la única técnica que se puede utilizar sobre cierto patrón de tráfico*.

- Para filtrado, esta técnica es poco escalable y es recomendable utilizar un **DNS gestionado**.

- En IPv6 aún no está disponible el comparador Layer7, pero puede utilizarse el comparador ***content***.

¿Preguntas?

Utilizando Layer7 para Filter y QoS

PROZCENTER
CENTRO DE PROFESIONALES