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

PROZCENTER
CENTRO DE PROFESIONALES

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”

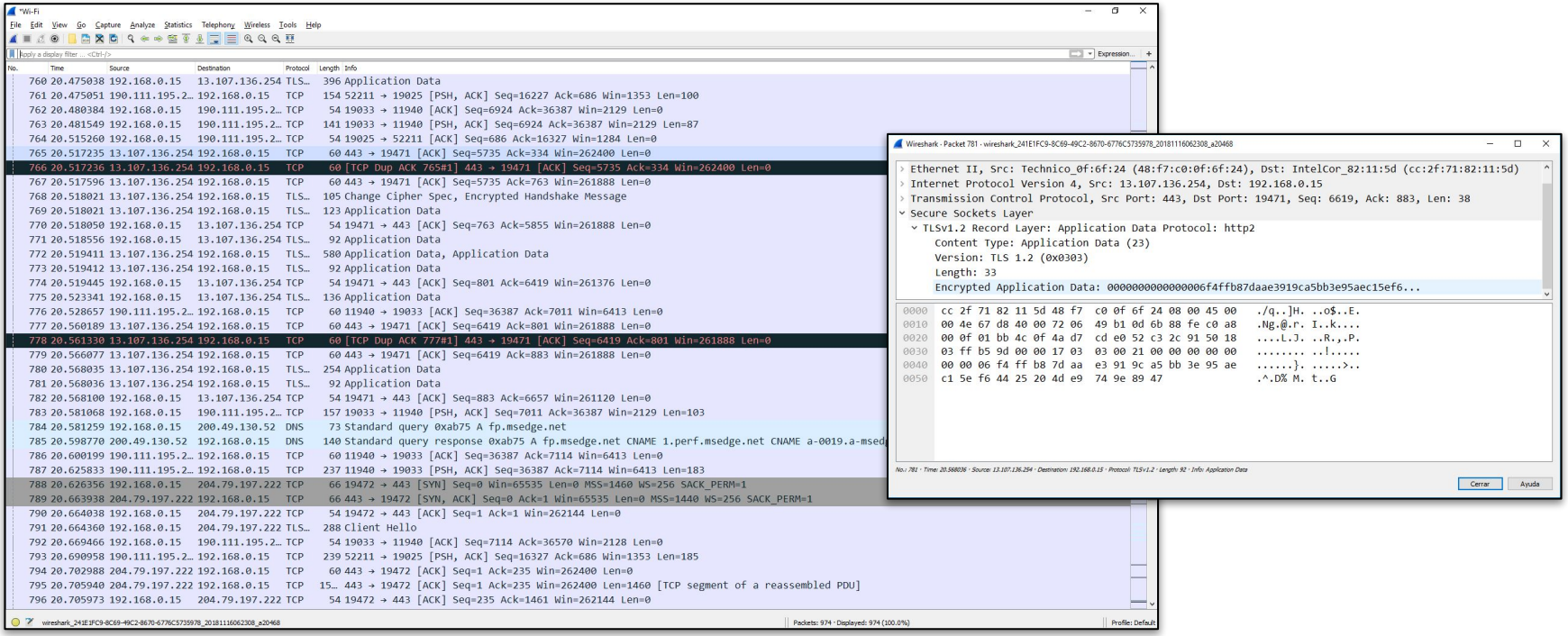
Falso, el problema viene de asociado al protocolo QUIC.

“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:



Comunicación con un sitio Web

- Sitio común HTTP/HTTPs

  1) Consulta DNS
     (UDP 53)

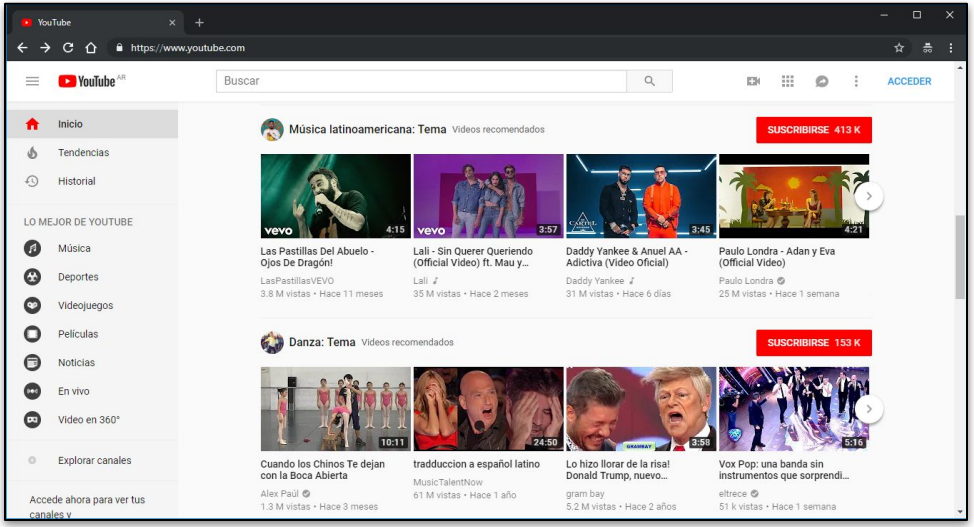
  2) Conexión HTTP/HTTPs
     (TCP 80 o TCP 443)

Comunicación con un sitio Web

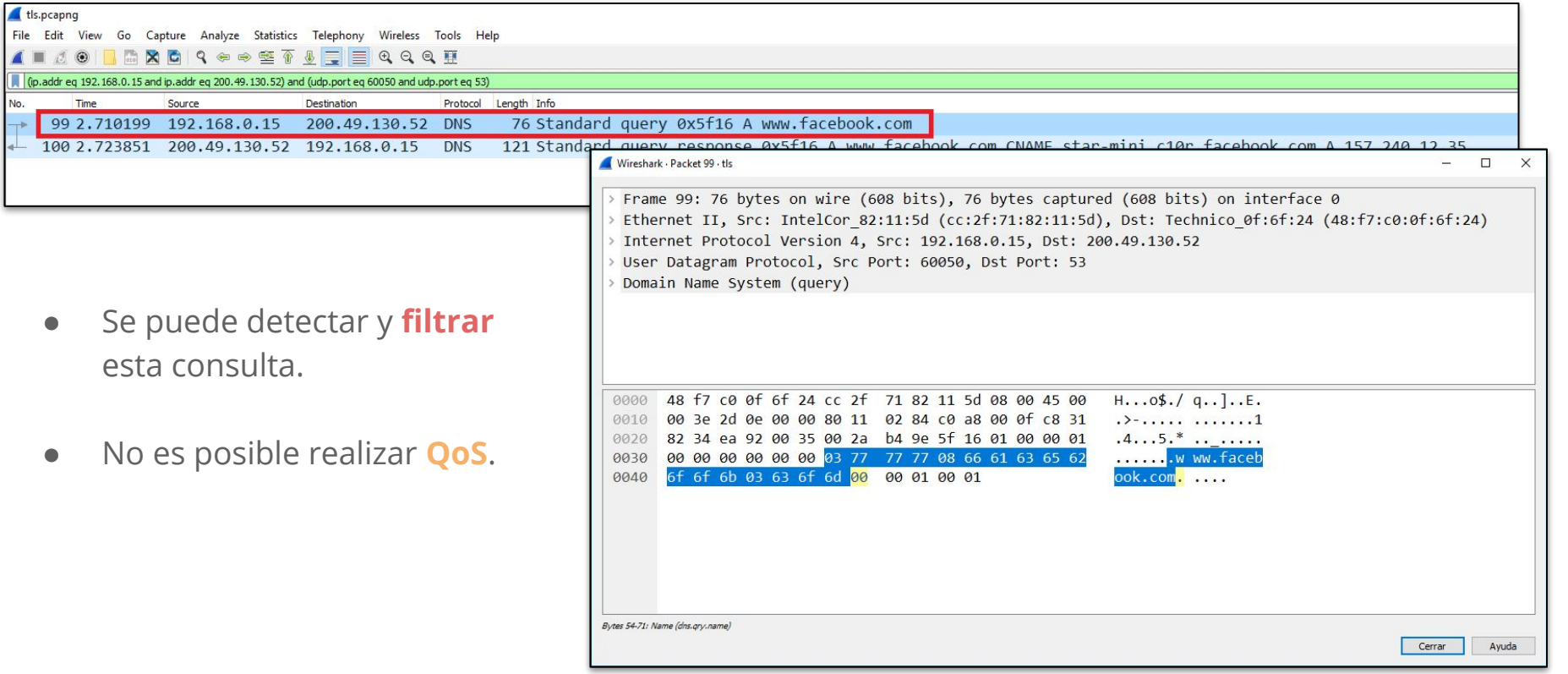
- Sitio de Google Inc. desde Chrome

1) Consulta DNS
(UDP 53)

2) Conexión QUIC
(UDP 80 o UDP 443)

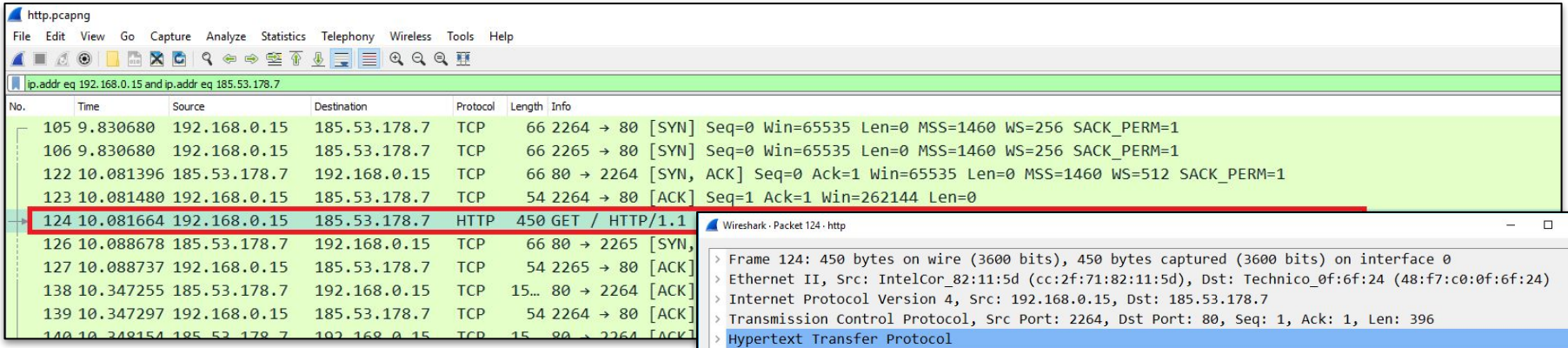


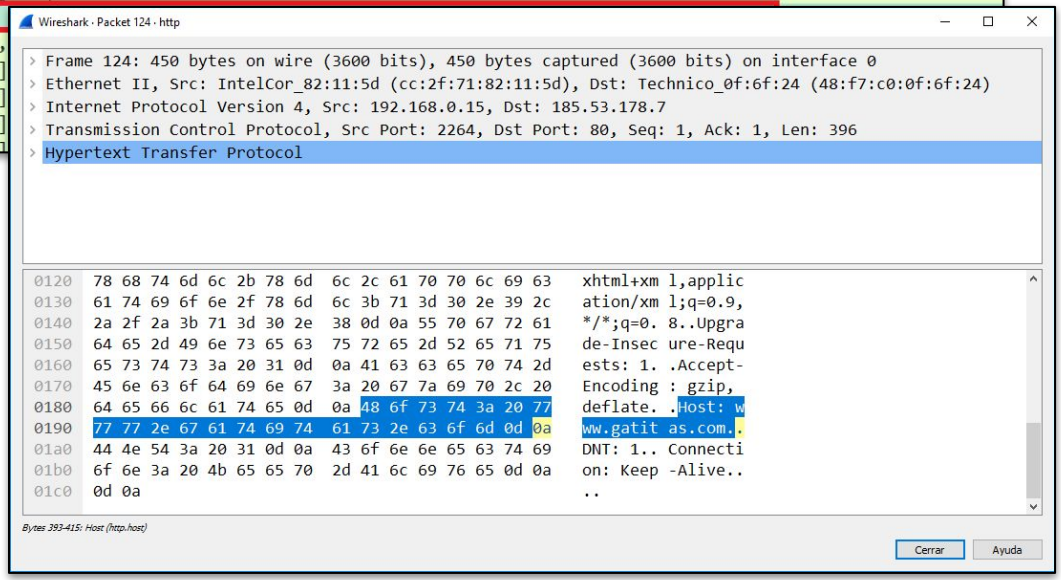
Comunicación DNS



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

Comunicación HTTP

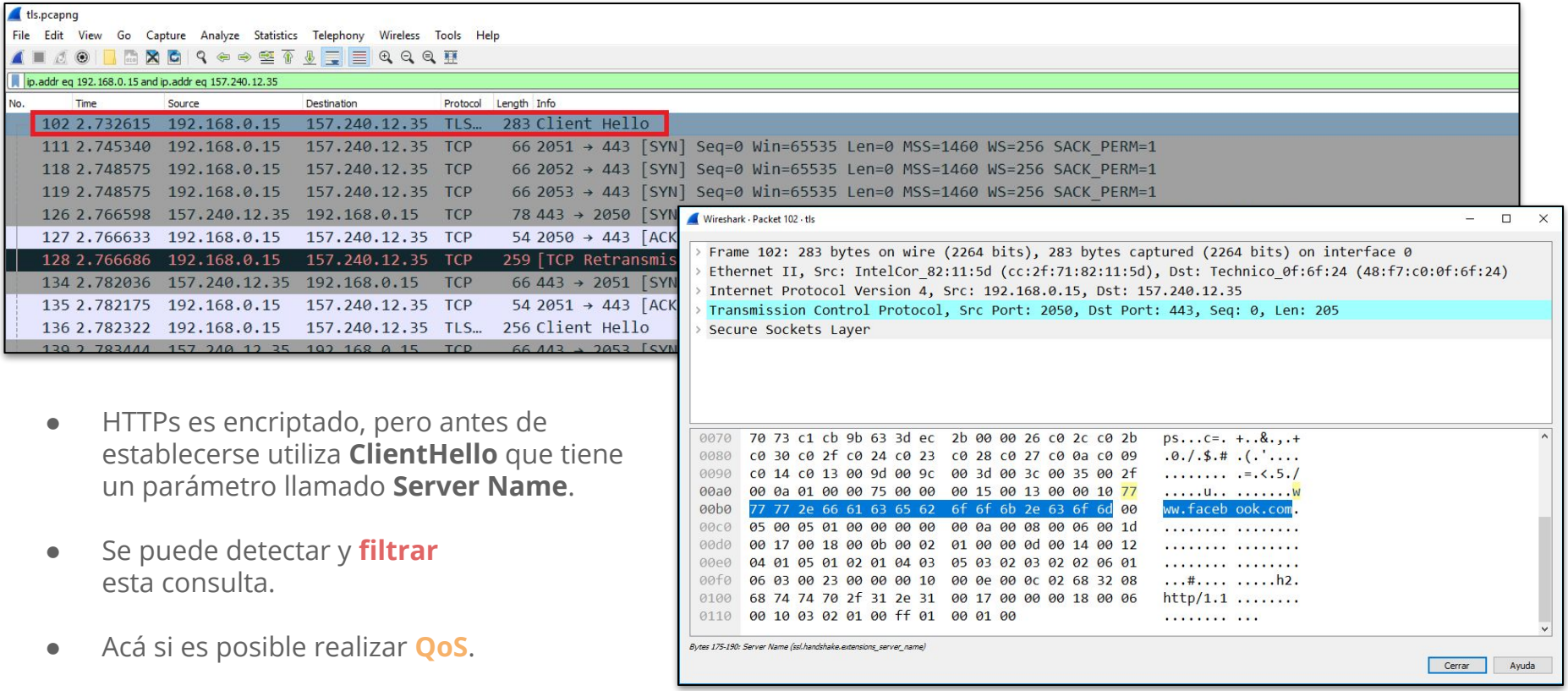




- Se puede detectar y **filtrar** esta consulta.

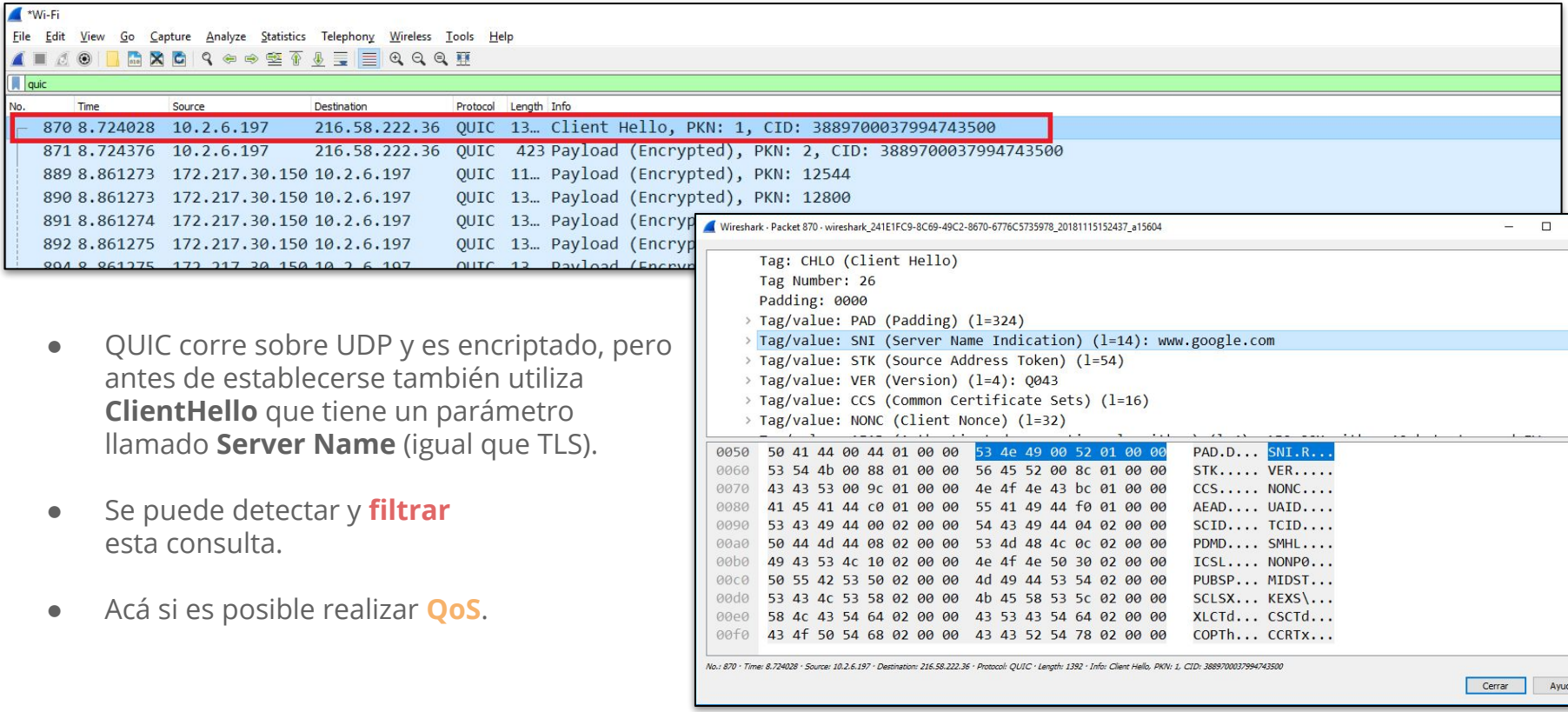
- Acá si es posible realizar **QoS**.

Comunicación HTTPs



- 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

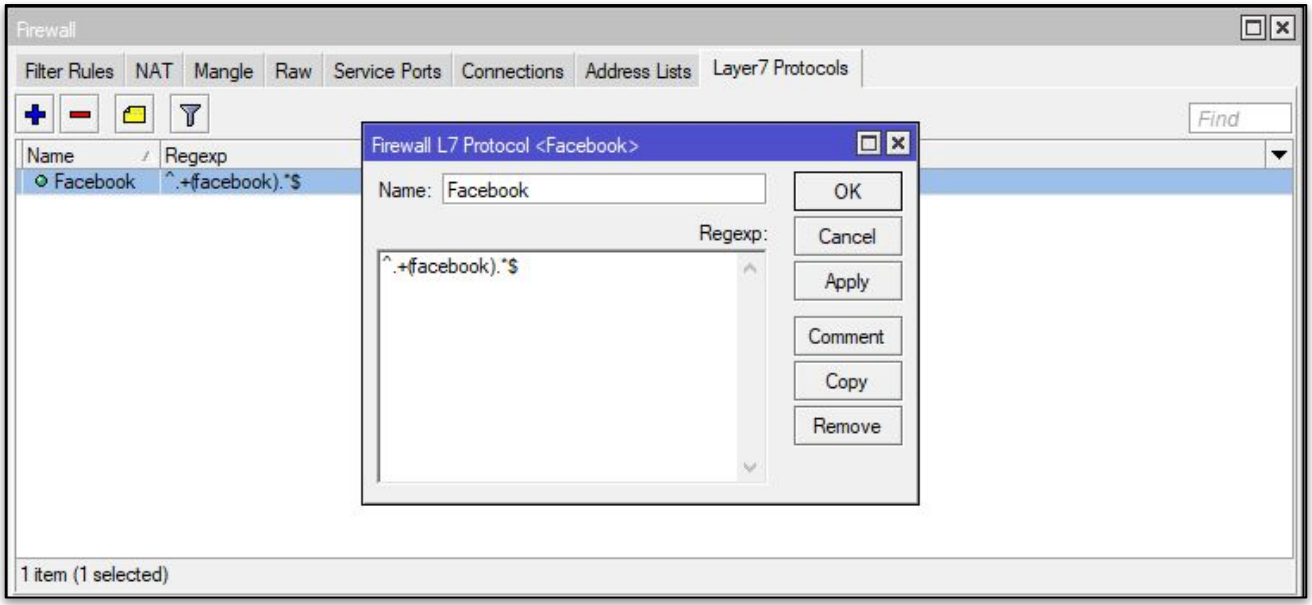


- QUIC corre sobre UDP y es encriptado, pero antes de establecerse también utiliza **ClientHello** que tiene un parámetro llamado **Server Name** (igual que TLS).
- Se puede detectar y **filtrar** esta consulta.
- Acá si es posible realizar **QoS**.

Layer7 en acción

Ejemplo con Filter - Detección con Layer7

```
/ip firewall layer7-protocol
add 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.

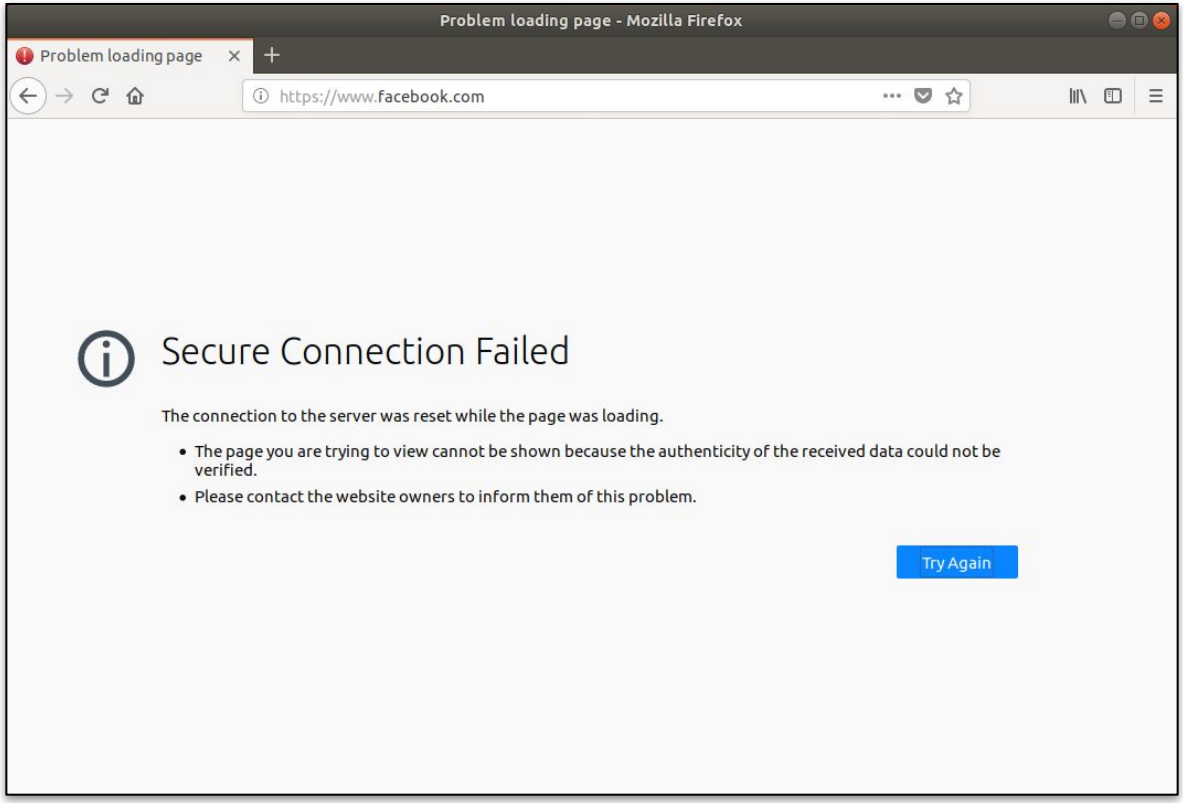
Ejemplo con Filter (QUIC)

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

Registro Layer7.

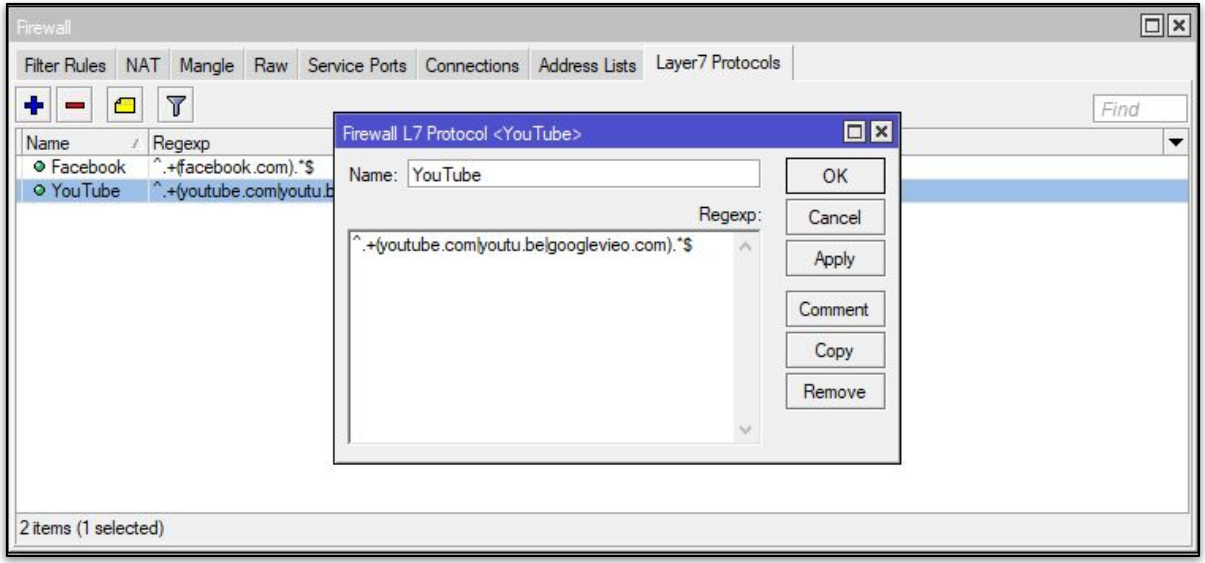
Rechazo casi instantáneo.

Ejemplo con Filter (HTTP/HTTPs/QUIC)



Ejemplo con QoS - Detección con Layer7

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



Ejemplo con QoS

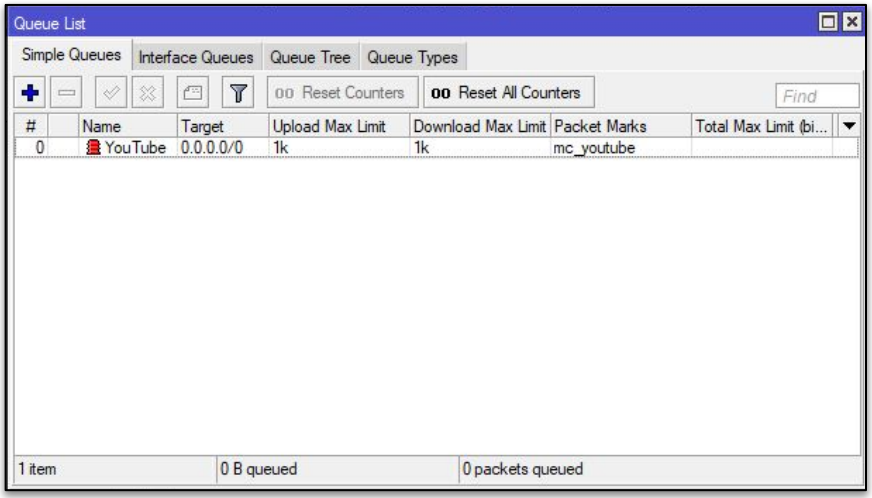
```
/ip firewall mangle
add comment="Marcar conexiones de YouTube" \
chain=forward \
connection-mark=no-mark \
layer7-protocol=YouTube \
action=mark-connection \
new-connection-mark=mc_youtube \
passthrough=yes
```

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
```



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