Análisis de Tráfico con Wireshark y Control con Layer7

Ing. Antonio Xavier Omiste Nava

TERACOM-Bolivia

2016

Presentación-TERACOM

- Empresa dedicada al Rubro de TELECOM y Networking.
- Amplia Gama de Soluciones, VoIP, Networking, Wireless, Wan Optimization, Análisis Espectral, construcción de Network Management Systems
- Expertos con 10+ Años de experiencia en el rubro,
- Certificados MTCNA,MTCTCE,MTCRE,MTCINE.

¿Por qué tengo que analizar mi Tráfico?

- El internet ya no es lo que era:
  - El nuevo modelo apuesta por Tener CDNs a nivel Global
    - Esto causa que el viejo modelo de filtros bloqueando IPs sea inútil
    - Los QoS por servicio (Youtube, Facebook, etc) a nivel capa 3 y 4 se vuelven cada vez mas generales y difíciles de controlar.
  - Cada operador busca tener su propio CDN o Cache dentro de su red:
    - Causando que múltiples servicios sean direccionando a una sola IP
    - No haya división de servicios por IPs.
    - Hace cuestionarte si realmente vale la pena bloquear por IP.

¿Que es un CDN?

- Content Delivery Network
- Contiene copias de datos locales para ser redistribuidos de manera local o regional
- Las ventajas que provee:
  - Dan a los usuarios una mayor calidad de conexión y al servicio una mayor capacidad para aumentar usuarios.
  - Disminuye tiempo de entrega y respuesta de la información al usuario
  - MAYOR RENTABILIDAD AL ISP, ya que el contenido no sale de la nube de datos del Proveedor y no viaja hacia otras regiones.
  - Problemas en filtros y creación de QoS para el usuario final ☺.

¿Qué puedo hacer?

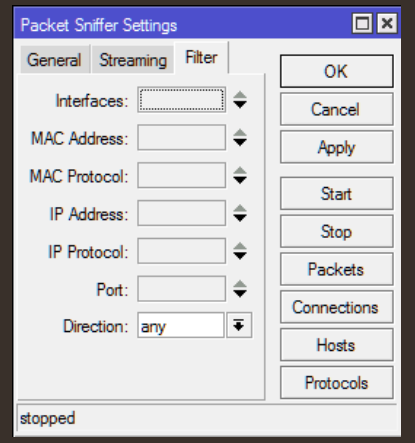
- Adaptarme al nuevo esquema
  - Dejar de vivir en la capa 1,2,3 del modelo OSI es un muy buen primer paso ☺.
  - Empezar a explorar las Capas 4,5,6,7,8… Si 8, salir a relacionarte con los usuarios es muy bueno (Ingeniería Social), conocer lo que hacen.
  - Si no se puede con la capa 8, Pues solo queda Analizar (Sniffear) el trafico del usuario.
  - Atacar por otros lados: Dominios, Extensiones de archivos, tipos de respuesta, tipos de consulta, o una mezcla de todo lo anterior
  - Layer7.

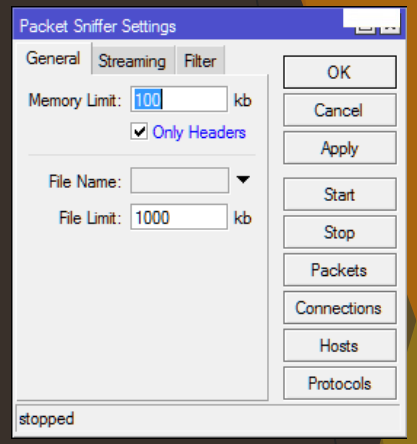
Análisis de Trafico con Mikrotik

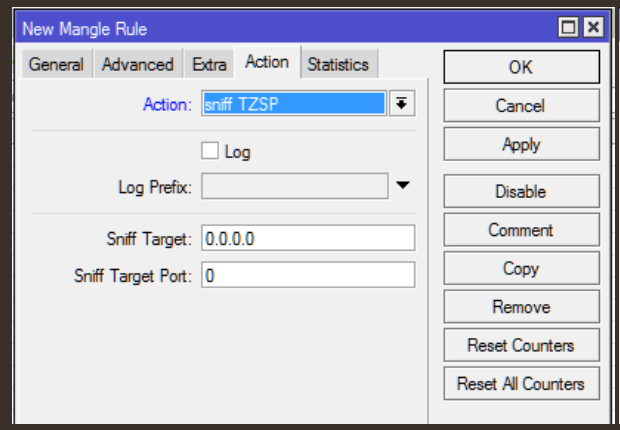
- Mikrotik en su calidad de router posee las siguientes ventajas a nivel de análisis de trafico:
  - Aprovecha al máximo el uso y compatibilidad con wireshark
  - Permite hacer streaming de análisis en tiempo real hacia un monitor (Wireshark)
  - Permite el uso de Guardado de captura de trafico en un archivo, como un pcap.
  - Permite realizar un análisis mas a fondo paquetes tomando en cuenta en un esquema de Firewall o mangle

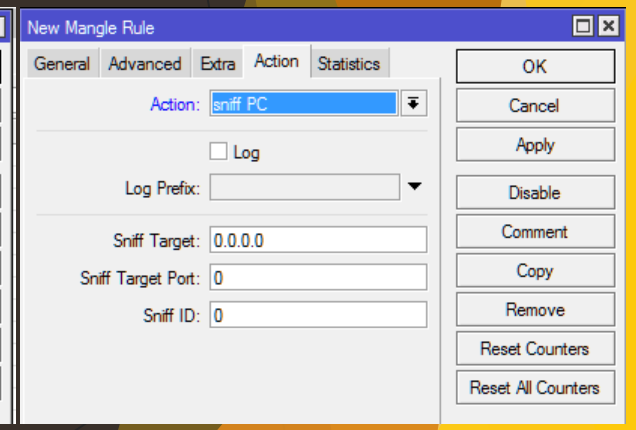
Análisis de trafico – Funciones Mikrotik

- Mikrotik como analizador de Tráfico
  - Principales Funciones:
    - Tools – Packet Sniffer: Filtro Básico, Análisis por defecto, Función de guardado en disco (Único)
    - Mangle – Sniff – TZSP: Filtro Avanzado, Stream por TZSP, compatibilidad con orden de Mangles.
    - Mangle – Sniff-PC: Filtro Avanzado, Stream por TZSP, Separacion por ID de sniffing, funciona con CALEA.









Análisis de Trafico-streaming-Wireshark

- Una vez enviado el análisis de trafico (mangle/Sniff-TZSP o /tools/Packet Sniffer):
  - Se procede a usar wireshark con filtros udp.port == 37008 (O el puerto que se use si es por mangle)

udp.port == 37008

No.	Time	Source	Destination	Protocol	Leng	Info
23…	406.…	192.168.88.1	192.168.88.200	DNS	176	Standard query response 0xd9e5 A web.whatsapp.com
23…	408.…	192.168.88.200	192.168.88.1	DNS	122	Standard query 0x8db1 A www.tera.com.bo
23…	408.…	192.168.88.200	192.168.88.1	DNS	122	Standard query 0x8db1 A www.tera.com.bo
23…	408.…	192.168.1.2	8.8.4.4	DNS	122	Standard query 0xeb5e A www.tera.com.bo
23…	408.…	8.8.4.4	192.168.1.2	DNS	152	Standard query response 0xeb5e A www.tera.com.bo

Análisis de Trafico-Wireshark

- Dentro de la segunda Fila tenemos que tomar en cuenta que esta separado por dos análisis uno encapsulado en TZSP y el otro directamente conectado al servidor:

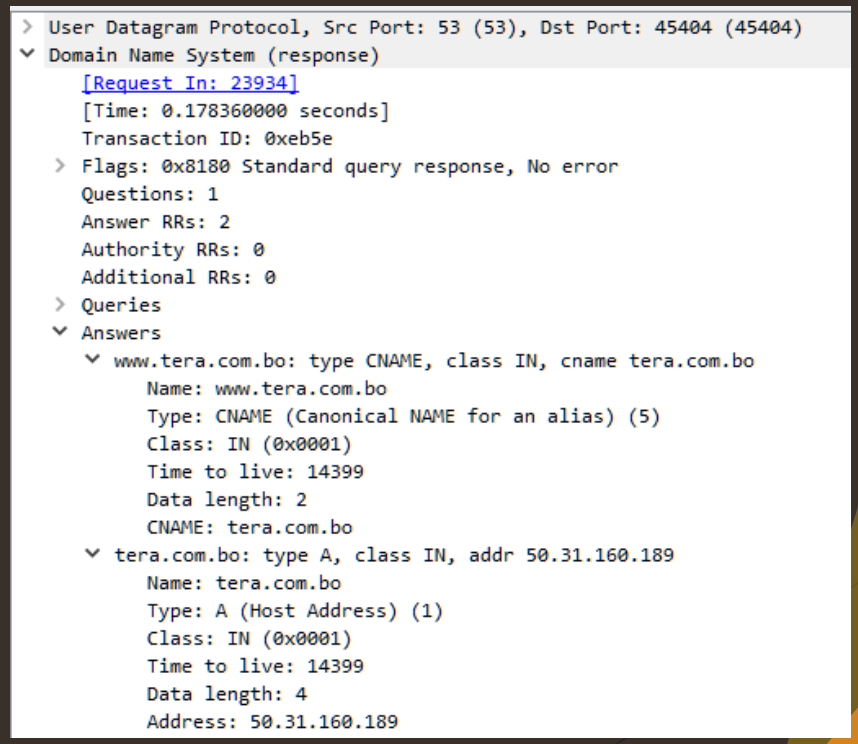
```
> Frame 23944: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0
> Ethernet II, Src: Routerbo_ed:43:9b (4c:5e:0c:ed:43:9b), Dst: Lifetron_05:bc:45 (00:0f:60:05:bc:45)
> Internet Protocol Version 4, Src: 192.168.88.1, Dst: 192.168.88.200
> User Datagram Protocol, Src Port: 57018 (57018), Dst Port: 37008 (37008)
> TZSP: Ethernet
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 8.8.4.4, Dst: 192.168.1.2
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 45404 (45404)
> Domain Name System (response)
```

Análisis de la interfaz Server Wireshark

Análisis de la interfaz Seleccionada en Mikrotik

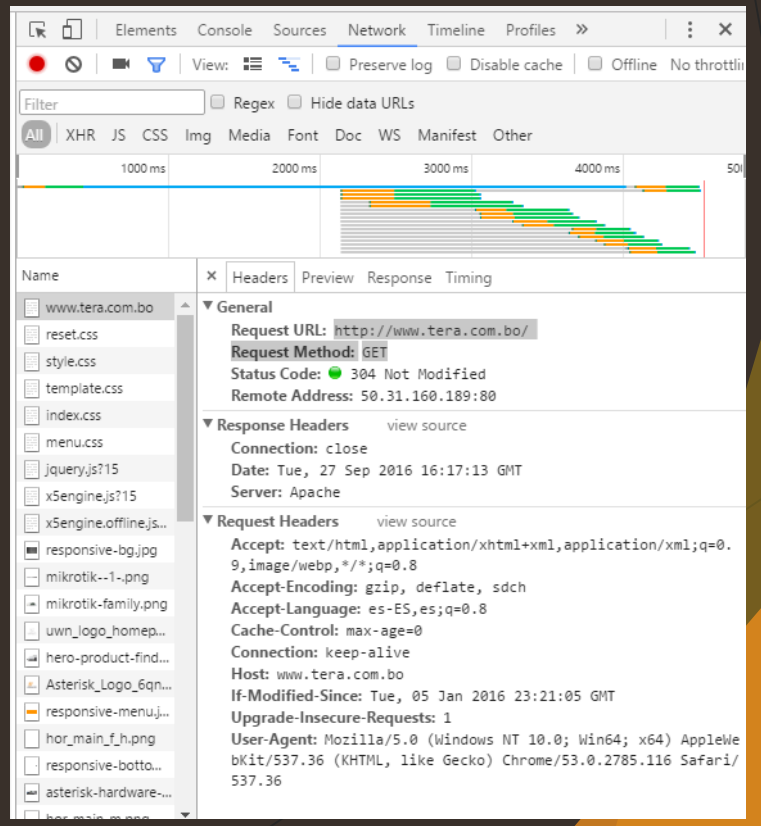
Análisis de Trafico-Wireshark

- De la segunda Fila podemos rescatar lo siguiente
  - Tomando en cuenta que inspeccionamos un paquete DNS podemos observar:
    - La respuesta al query de DNS:
      - Query: www.tera.com.bo
      - Primer Tipo de Registro:CNAME
      - TTL:14399
      - Segunda Consulta (Resolucion del CNAME)
        - Tipo de Registro A
        - TTL:14399
        - Direccion: 50.31.160.189



Análisis de tráfico a nivel web

- Para comprobar el anterior análisis realizamos un análisis a nivel WEB (F12 Herramientas de desarollador) y observamos que podemos capturar:
  - Observamos que la petición inicial del navegador es la de consultar esta dirección www.tera.com.bo
  - Lo cual provoca que el servicio DNS sea consultado.
  - Es decir que a nivel HTTP se trabaja por Nombre de dominio.
  - Relacionando ambas capturas, concluimos que la palabra clave en esta problemática es: www.tera.com.bo

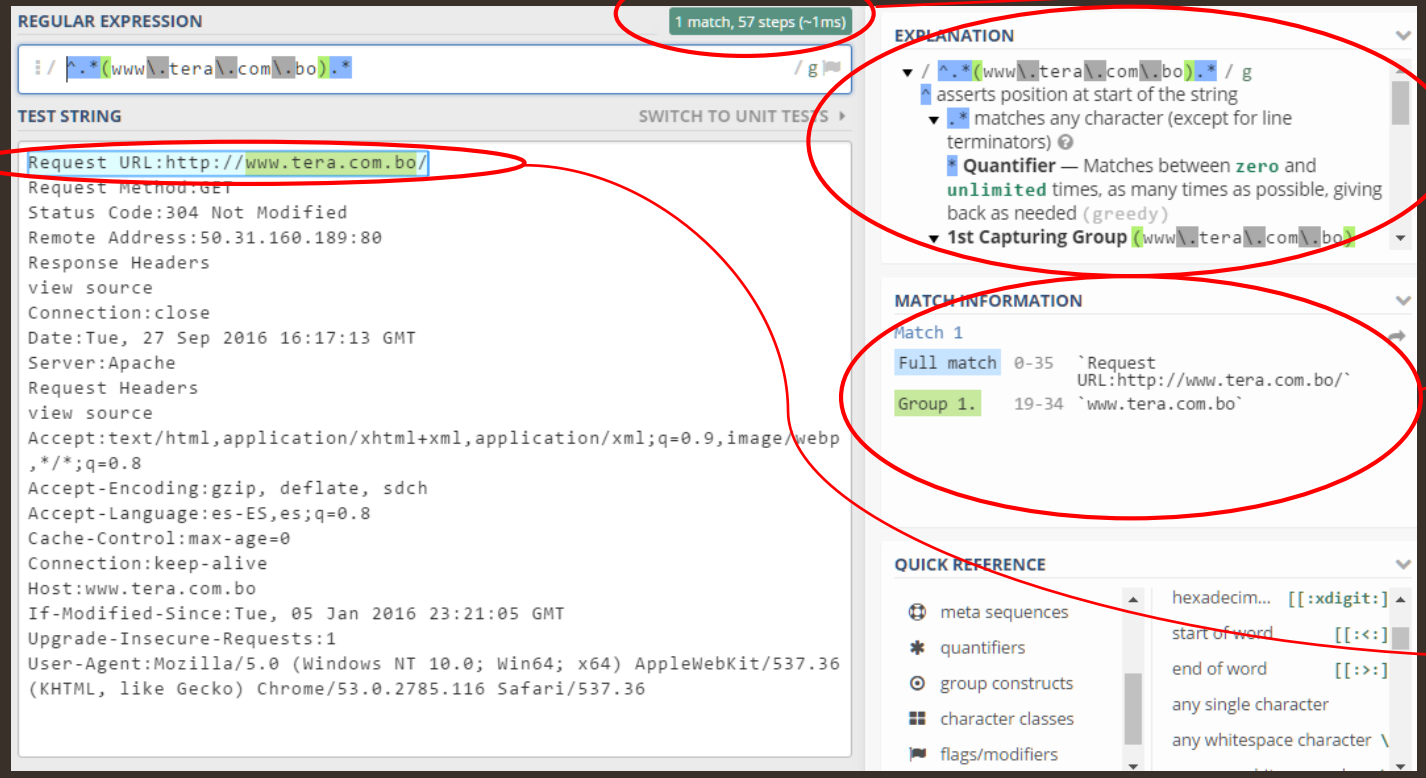


Layer 7

- Como su nombre lo dice se basa en la capa 7 del modelo OSI y los protocolos que están dentro de esa capa
- En layer7 de Mikrotik trabajamos con expresiones regulares
- Dichas expresiones regulares sirven como matchers para capturar un determinado string o cadena dentro de un paquete o en este caso cabecera:
  - Una buena fuente de practica y de prueba es regex101.com
  - Todo lo que capturamos en Wireshark puede ser usado para el regexp
  - Se tiene que tomar en consideración que dependiendo el tipo de matchers usado puede llegar a consumir todo el CPU del RB y dejarlo inoperativo (Hasta que se quite el layer 7 aplicado).

Layer7 - Regexp

- Usando los datos que ya poseemos y nuestra palabra clave procedemos a realizar el Regexp:



Tiempo de resolución

Matchers usados y su explicación

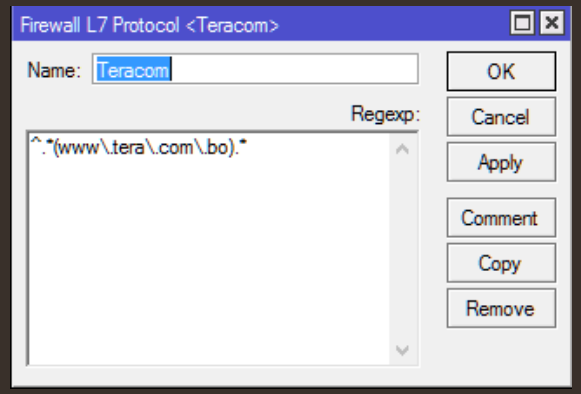
Donde se encontró Nro Linea

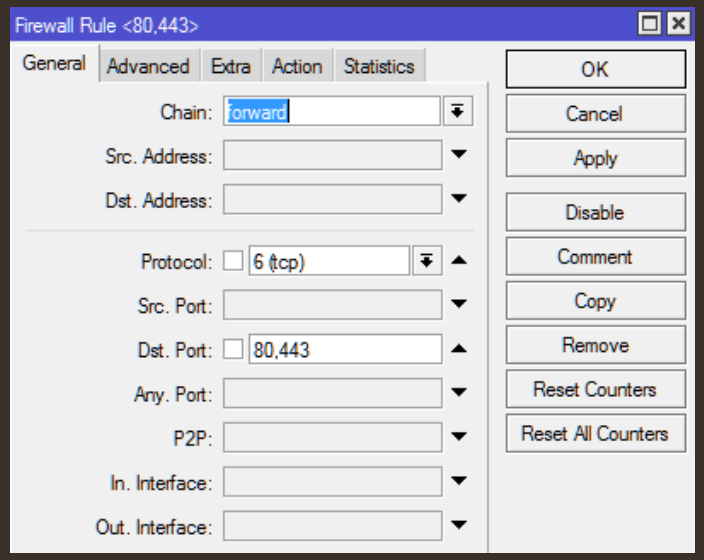
Resaltado de los Matchs

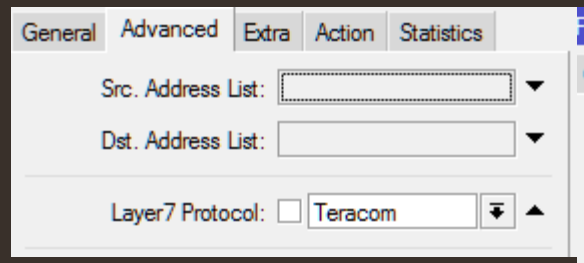
Cabe destacar que el servicio que usamos (regex101.com) nos permite hacer un test de captura, y a su vez el tiempo de resolución en analizarlo y encontrado (Muy importante para determinar el consumo de CPU)

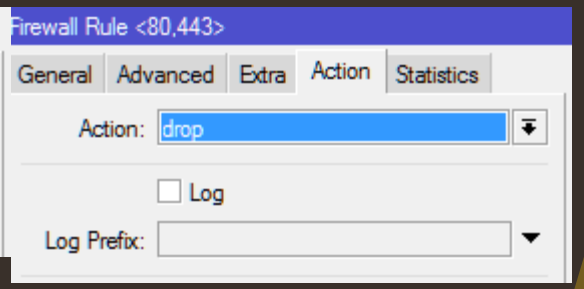
Layer 7 - Mikrotik

- Y finalmente En Mikrotik Firewall Layer7
- Imaginándonos que queremos bloquear
  Realizamos un filtrado en Ip Firewall Filters

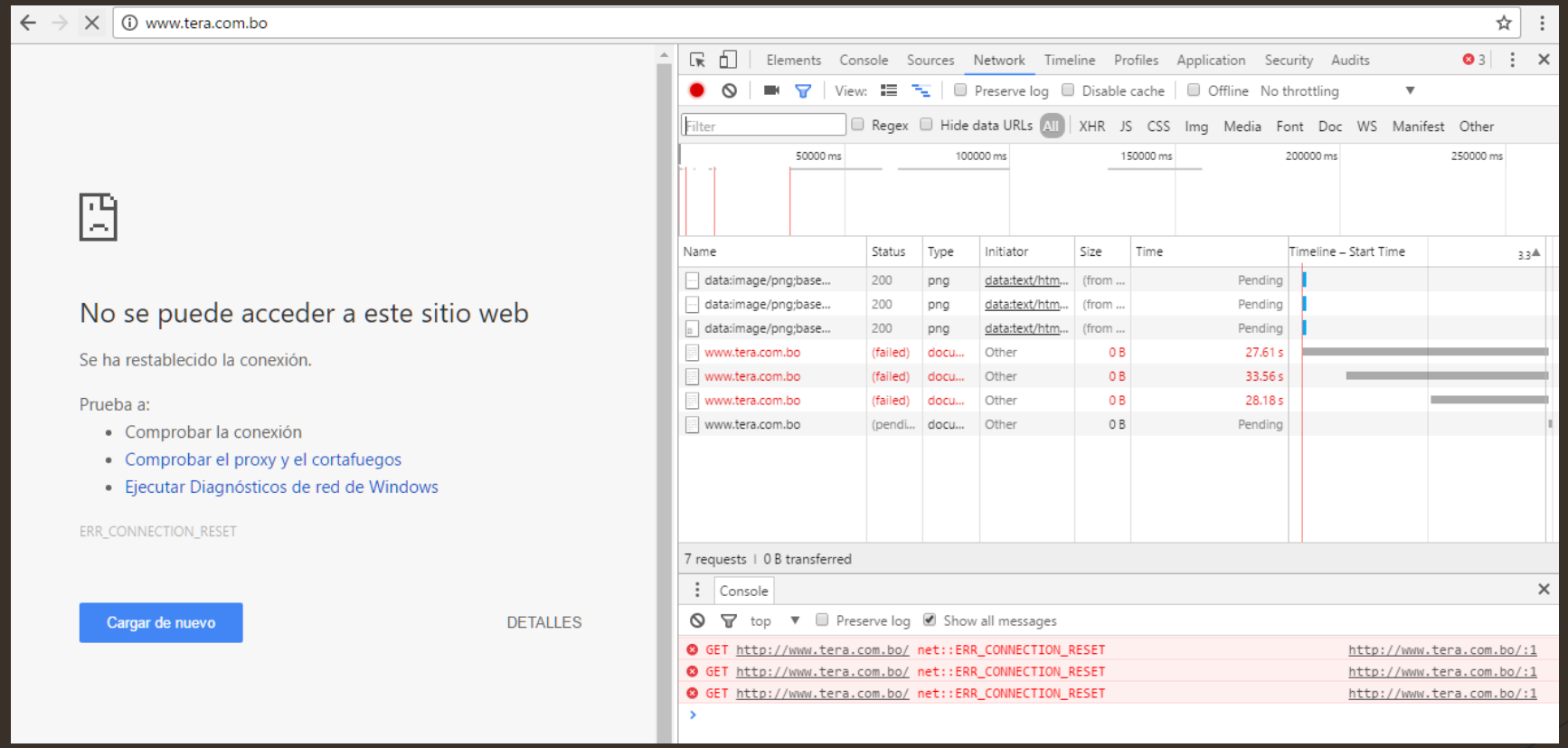








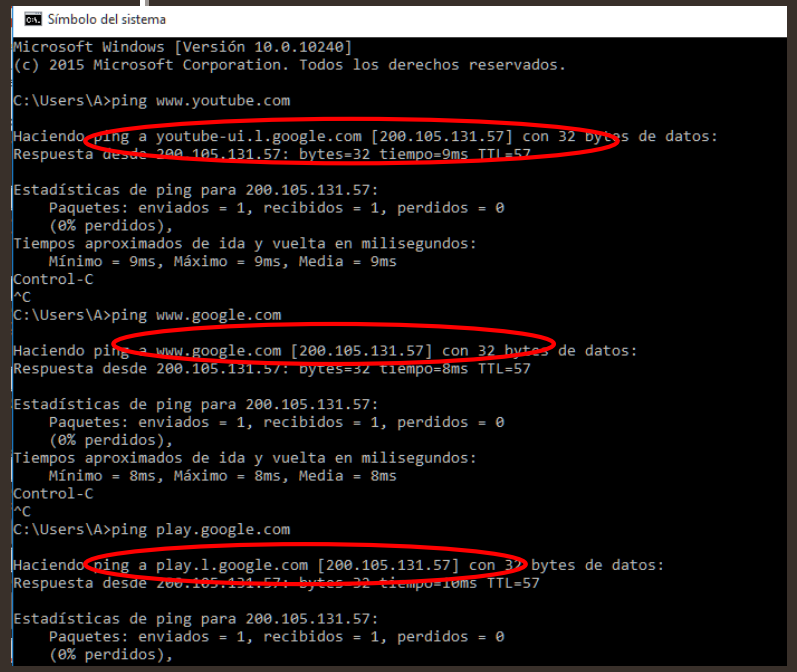
Layer7 Resultado



Soluciones Alternas….

- No es mas fácil hacer un Filtrado a través de address list, no se si te enteraste pero ahora mikrotik te deja meter dominios en el address list.
  - Si es verdad que Mikrotik desde la versión 6.36 deja hacer address list con dominios, pero….

- Cada operador busca tener su propio CDN o Cache dentro de su red:
  - Causando que múltiples servicios sean direccionando a una sola IP



Layer7- Mejores cosas que hacer con el

- Hasta ahora se vio algo básico, con lo que se puede hacer con Layer7, solo para abrir el apetito, Otros ejemplos de lo que se puede realizar con layer7 son:
  - Bloqueo o QoS de Youtube, sin afectar servicios de Gmail, Google.com, etc
  - Bloqueo o QoS de contenido especifico de Facebook, Ej.: Bloqueo de solo videos de Facebook,
  - Bloqueo o QoS de extensiones de archivos.
  - Bloqueo de contenido HTTPs.
  - Bloqueo a nivel capa7 ☺, a usar la imaginacion.

Layer7

- Vamos a proceder con una DEMO de algo mas especifico y complejo con layer 7:

DEMO