Telefonica

WIRESHARK

Estadísticas

Trabajando con paquetes capturados

Estadísticas

Estadísticas

Introducción

Uno de los puntos fuertes de Wireshark, es la herramienta Estadísticas

Las estadísticas, nos proporcionan datos sobre la red, quien habla con quien, el tamaño de los paquetes, etc... en definitiva, información sobre el comportamiento de la red.

Estadísticas

Introducción

Nos encontramos con estadísticas específicas de un protocolo y estadísticas generales

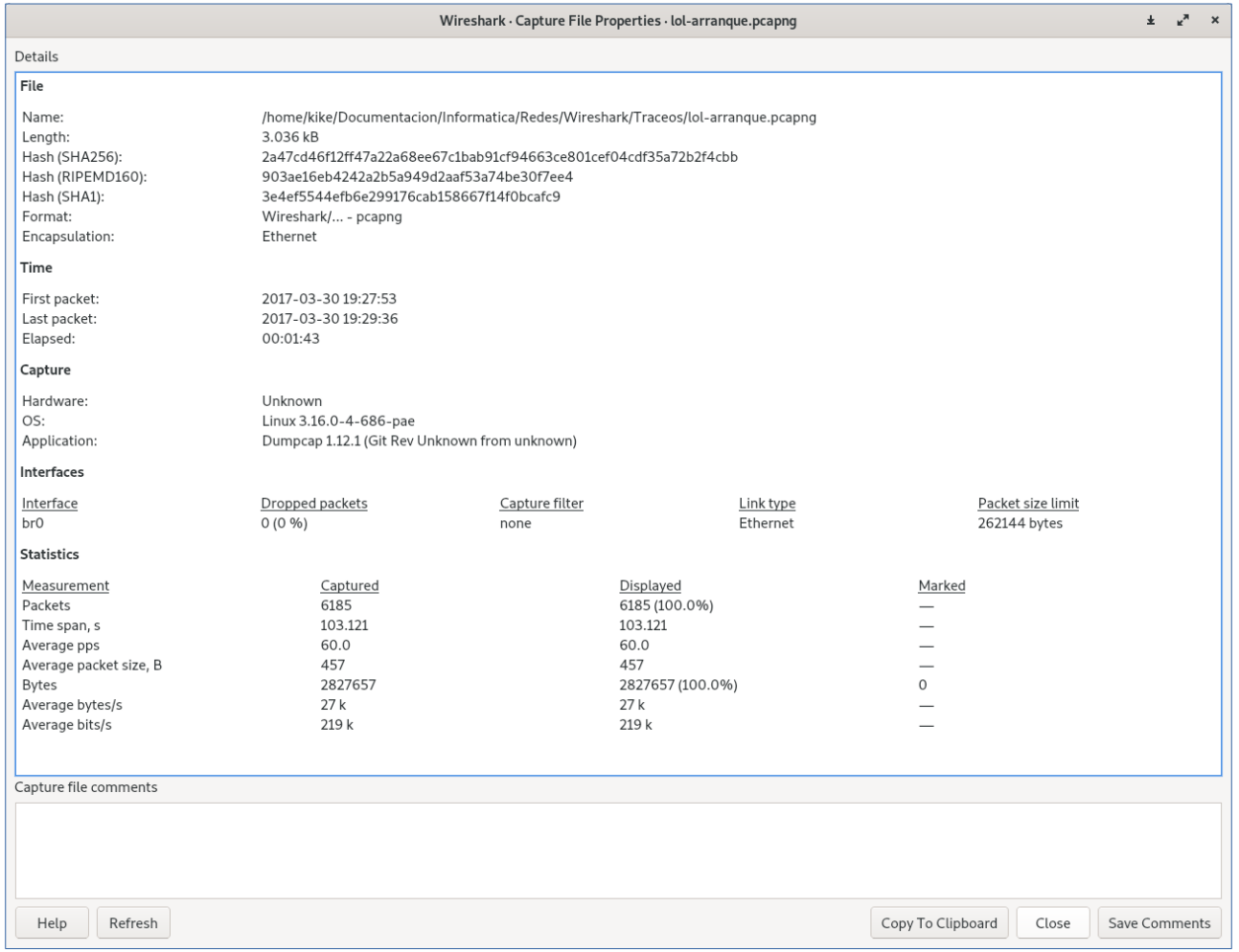
- **Capture File properties**, propiedades sobre el archivo de captura
- **Protocol Hierarchy**, jerarquía de protocolos
- **Conversations**, tráfico entre direcciones IP
- **Endpoints**, tráfico acia y desde una dirección IP
- **I/O Graphs**, gráficos sobre el número de paquetes respecto al tiempo

Estadísticas

Capture file properties

Nos proporciona datos estadísticos del archivo de captura

- Nombre del archivo, formato, hash, tamaño
- Fecha y hora del primer y último paquete
- Sistema operativo de la máquina dónde se realizó la captura
- Estadísticas de paquetes capturados



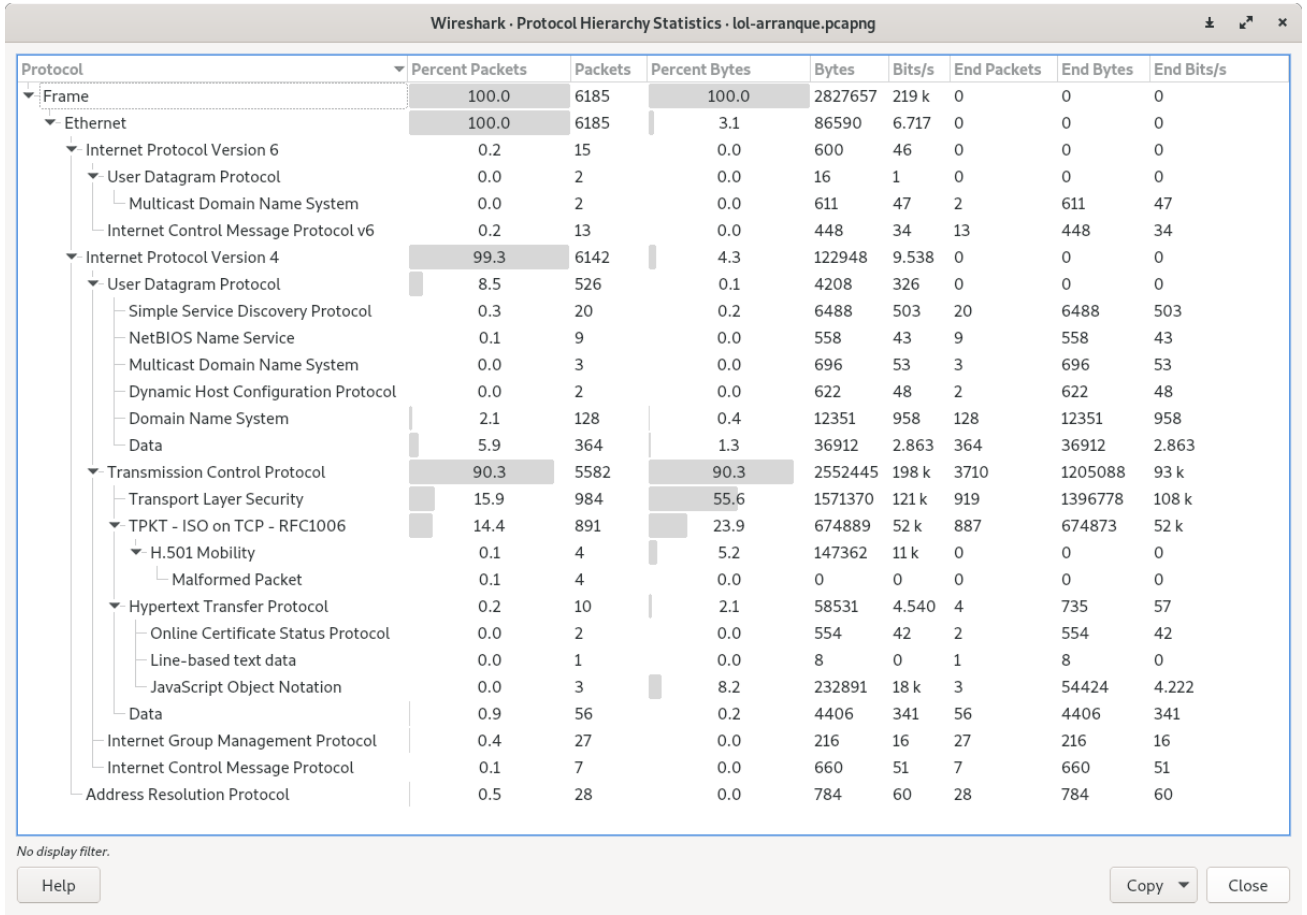
Estadísticas

Protocol Hierarchy

Si queremos conocer el tipo de tráfico que corre a través de la red, se presenta como un árbol

Cada fila contiene los valores estadísticos de los protocolos.

Si se configura un filtro de visualización, sólo aparecen los protocolos que cumplan la regla de filtrado



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	6185	100.0	2827657	219 k	0	0	0
Ethernet	100.0	6185	3.1	86590	6.717	0	0	0
Internet Protocol Version 6	0.2	15	0.0	600	46	0	0	0
User Datagram Protocol	0.0	2	0.0	16	1	0	0	0
Multicast Domain Name System	0.0	2	0.0	611	47	2	611	47
Internet Control Message Protocol v6	0.2	13	0.0	448	34	13	448	34
Internet Protocol Version 4	99.3	6142	4.3	122948	9.538	0	0	0
User Datagram Protocol	8.5	526	0.1	4208	326	0	0	0
Simple Service Discovery Protocol	0.3	20	0.2	6488	503	20	6488	503
NetBIOS Name Service	0.1	9	0.0	558	43	9	558	43
Multicast Domain Name System	0.0	3	0.0	696	53	3	696	53
Dynamic Host Configuration Protocol	0.0	2	0.0	622	48	2	622	48
Domain Name System	2.1	128	0.4	12351	958	128	12351	958
Data	5.9	364	1.3	36912	2.863	364	36912	2.863
Transmission Control Protocol	90.3	5582	90.3	2552445	198 k	3710	1205088	93 k
Transport Layer Security	15.9	984	55.6	1571370	121 k	919	1396778	108 k
TPKT - ISO on TCP - RFC1006	14.4	891	23.9	674889	52 k	887	674873	52 k
H.501 Mobility	0.1	4	5.2	147362	11 k	0	0	0
Malformed Packet	0.1	4	0.0	0	0	0	0	0
Hypertext Transfer Protocol	0.2	10	2.1	58531	4.540	4	735	57
Online Certificate Status Protocol	0.0	2	0.0	554	42	2	554	42
Line-based text data	0.0	1	0.0	8	0	1	8	0
JavaScript Object Notation	0.0	3	8.2	232891	18 k	3	54424	4.222
Data	0.9	56	0.2	4406	341	56	4406	341
Internet Group Management Protocol	0.4	27	0.0	216	16	27	216	16
Internet Control Message Protocol	0.1	7	0.0	660	51	7	660	51
Address Resolution Protocol	0.5	28	0.0	784	60	28	784	60

Estadísticas

Protocol Hierarchy

Nos presenta datos estadísticos de los protocolos

- Nombre del protocolo
- **Percent Packets**, orcentaje de paquetes que corresponden con el protocolo
- **Packets**, número de paquetes de ese protocolo
- **Percent Bytes**, porcentaje del número de bytes
- **Bytes**, número de bytes del protocolo
- **Bits/s**, especifica el ancho de banda de ese protocolo en relación con el tiempo de captura

Estadísticas

Protocol Hierarchy

Cuando expandimos una sección, los paquetes que dependen de él, son la suma del total de la sección

Wireshark, no asocia el tráfico TCP como aplicación y habrá muchos paquetes que no formen parte de una aplicación. Sin embargo, si sumamos los valores de UDP, estos deben ser muy parecidos o muy cercanos al valor global de UDP

Con el botón derecho del ratón, podemos aplicar un filtro o construir una regla de coloreado para ese protocolo o aplicación

Estadísticas

Laboratorio 1

Tráfico sospechoso

- Detectar aplicaciones o tráfico sospechoso
- Filtrarlo para examinar mejor, buscar nombres de usuario, servidor, etc...

Estadísticas

Conversations

Una conversación de red, es el tráfico entre dos puntos finales específicos

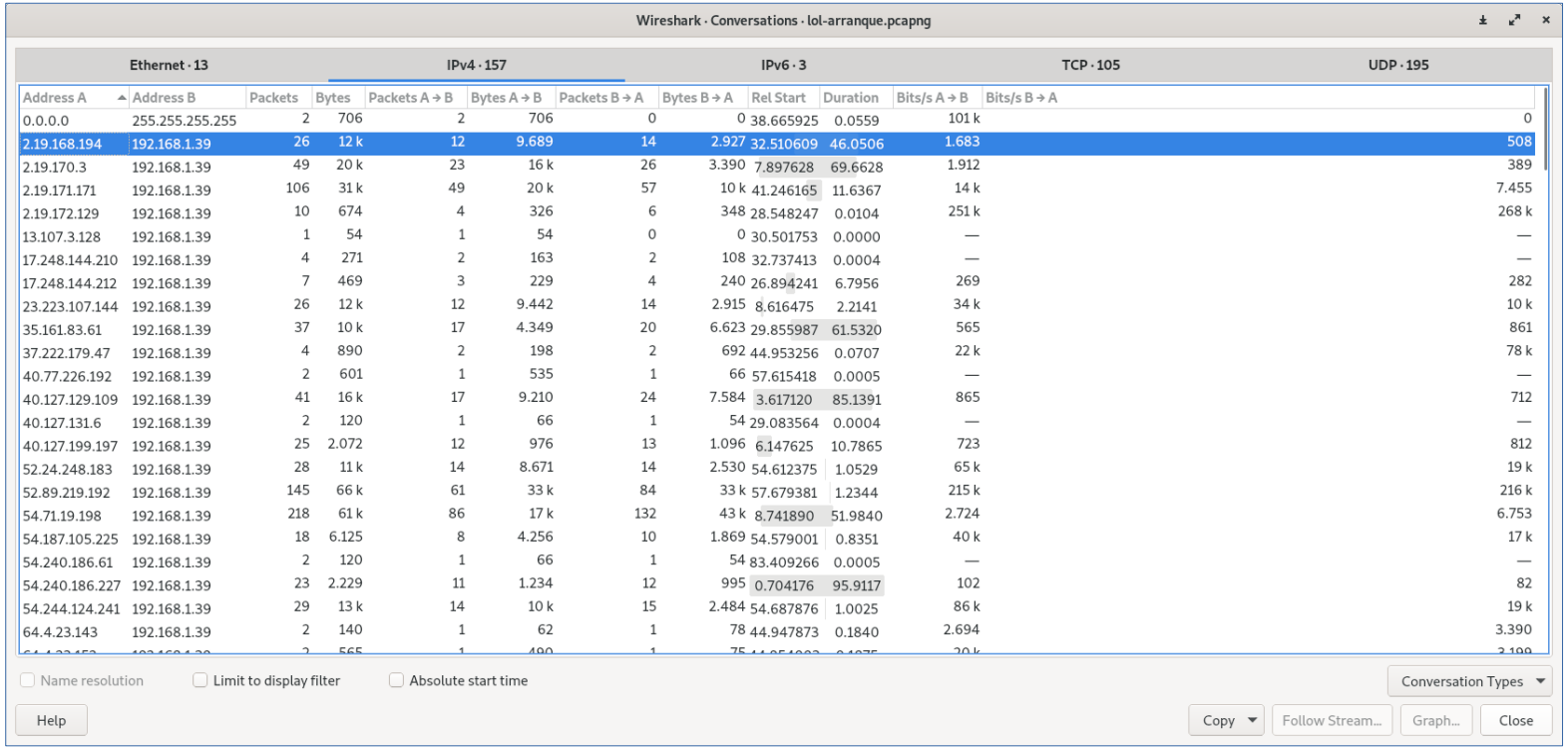
Podemos elegir entre conversaciones

- Ethernet
- IPv4 e IPv6
- TCP
- UDP

Estadísticas

Conversations

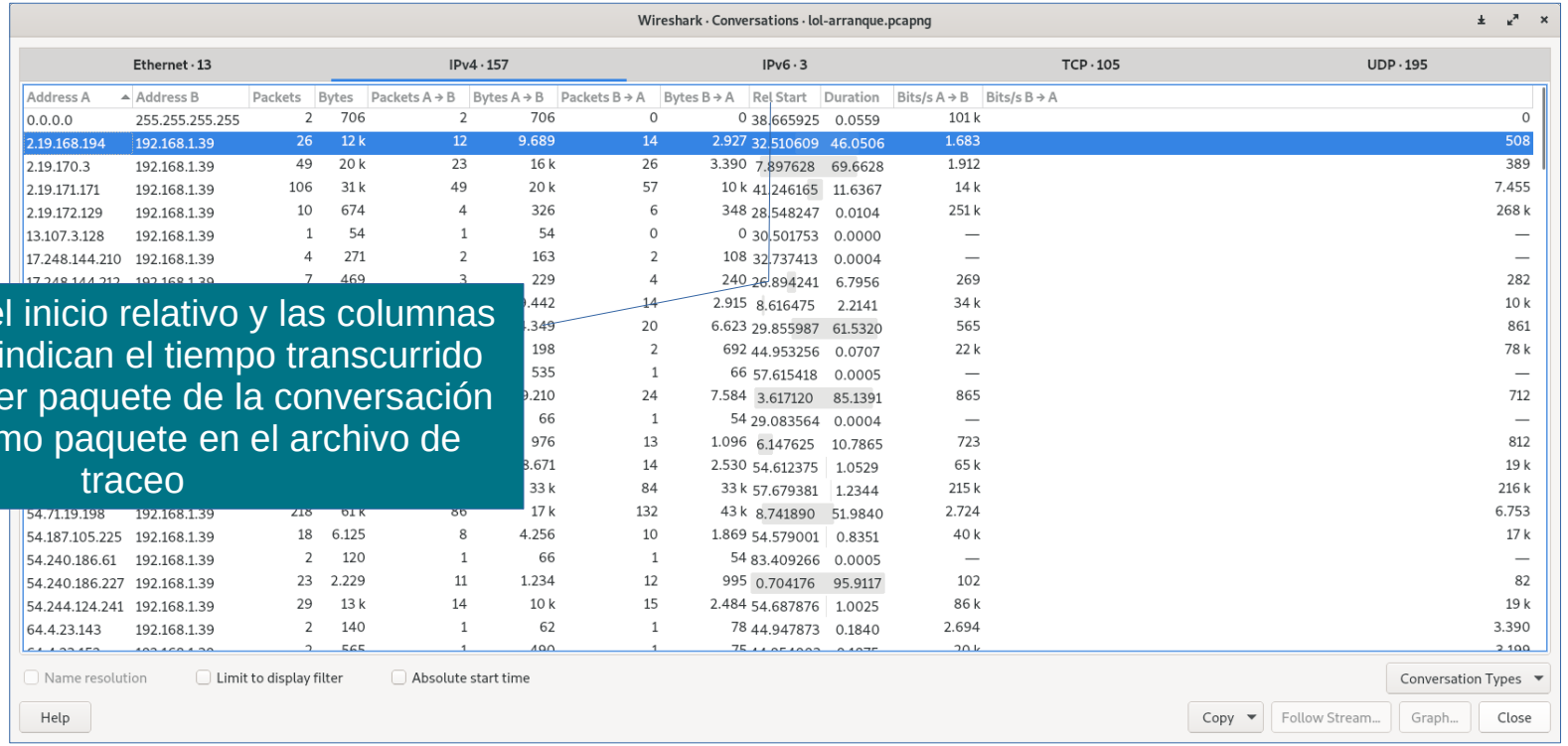
Se presenta una ventana con todas las conversaciones capturadas, clasificadas por protocolos



Estadísticas

Conversations

Se presenta una ventana con todas las conversaciones capturadas, clasificadas por protocolos



Rel Start, es el inicio relativo y las columnas de duración, indican el tiempo transcurrido desde el primer paquete de la conversación hasta el último paquete en el archivo de traceo

Estadísticas

Conversations

Se pueden limitar las conversaciones con un filtro de visualización marcando la casilla **Limit to display**

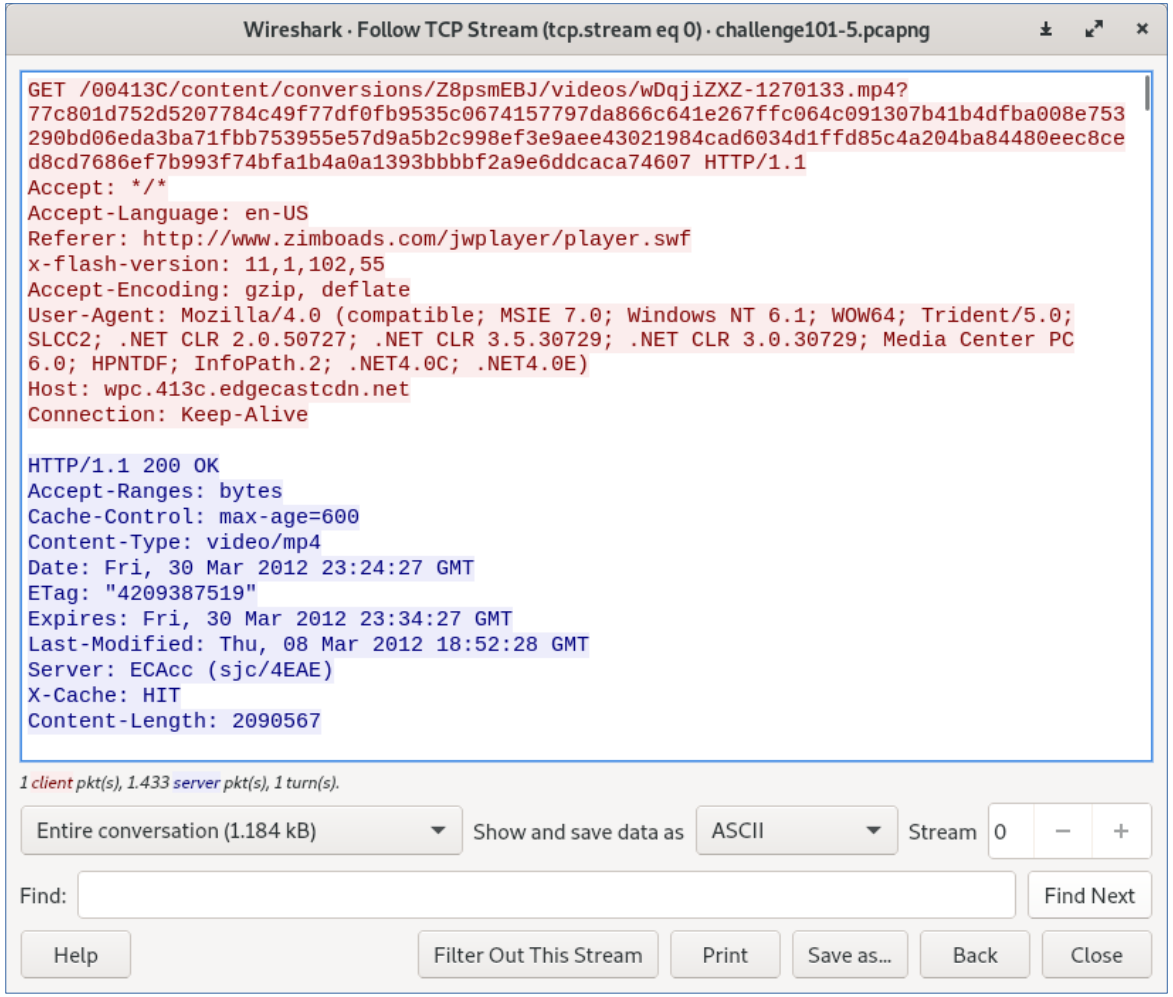
Desde el campo de selección **Display types**, podemos seleccionar que protocolos se van a visualizar

La resolución de nombre, se realizará si se selecciona en la ventana y si está activa para la capa de protocolo específica

Estadísticas

Conversations

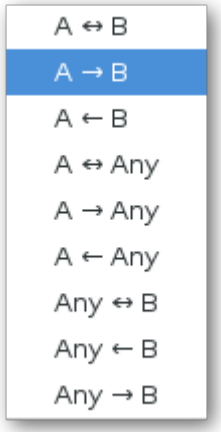
Desde la pestaña TCP, si seleccionamos una conversación, se activará el botón **Follow Stream**, que extrae el flujo de datos establecido en una sesión TCP



Estadísticas

Conversations

También podemos aplicar un filtro, seleccionando con el botón derecho **Apply as filter**, pudiendo seleccionar la dirección en la que estamos interesados para filtrar



Estadísticas

Conversations

Para determinar porqué un enlace está saturado, hay que buscar qué conversación está ocupando mas ancho de banda ordenando la columna bytes de mayor a menor

Busque elementos con muchas conexiones abiertas

Busque puertos que no conoce

Estadísticas

Endpoint

Muestra el tráfico de los elementos finales, ofreciendo estadísticas de ese host concreto

Podemos utilizar esta ventana para ver la actividad de una máquina en particular

Estadísticas

Laboratorio 2

Conversación más activa

- ¿Cuantas máquinas hay?
- ¿Qué está haciendo el usuario?

Estadísticas

Estadísticas IP

Nos ofrece varias estadísticas sobre el tráfico IP

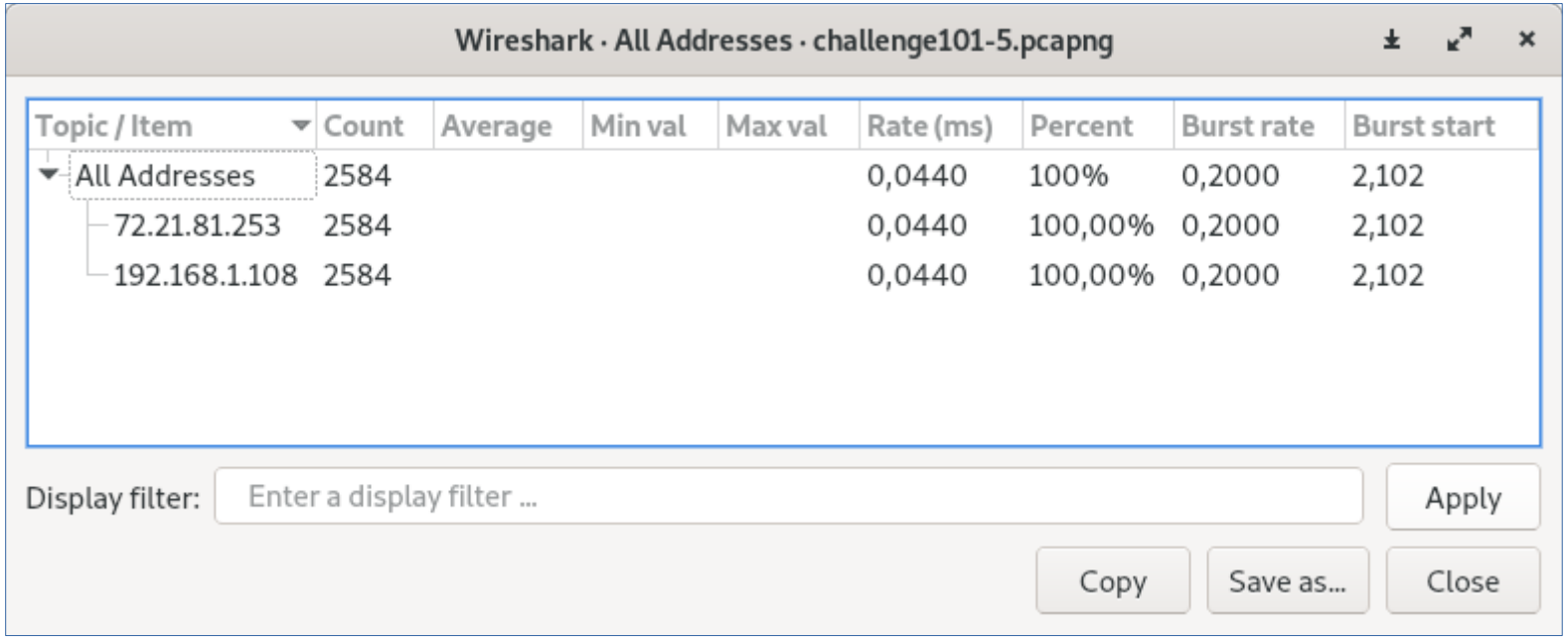
- All addresses, se visualizan todas las estadísticas de paquetes
- Destination and ports, mostrará todas las direcciones IP destino al cual son enviados y sobre qué protocolos.
- IP protocol types
- Source and destination addresses

Estadísticas

Estadísticas IP

Todos los resultados estadísticos, se pueden exportar a varios formatos de archivo

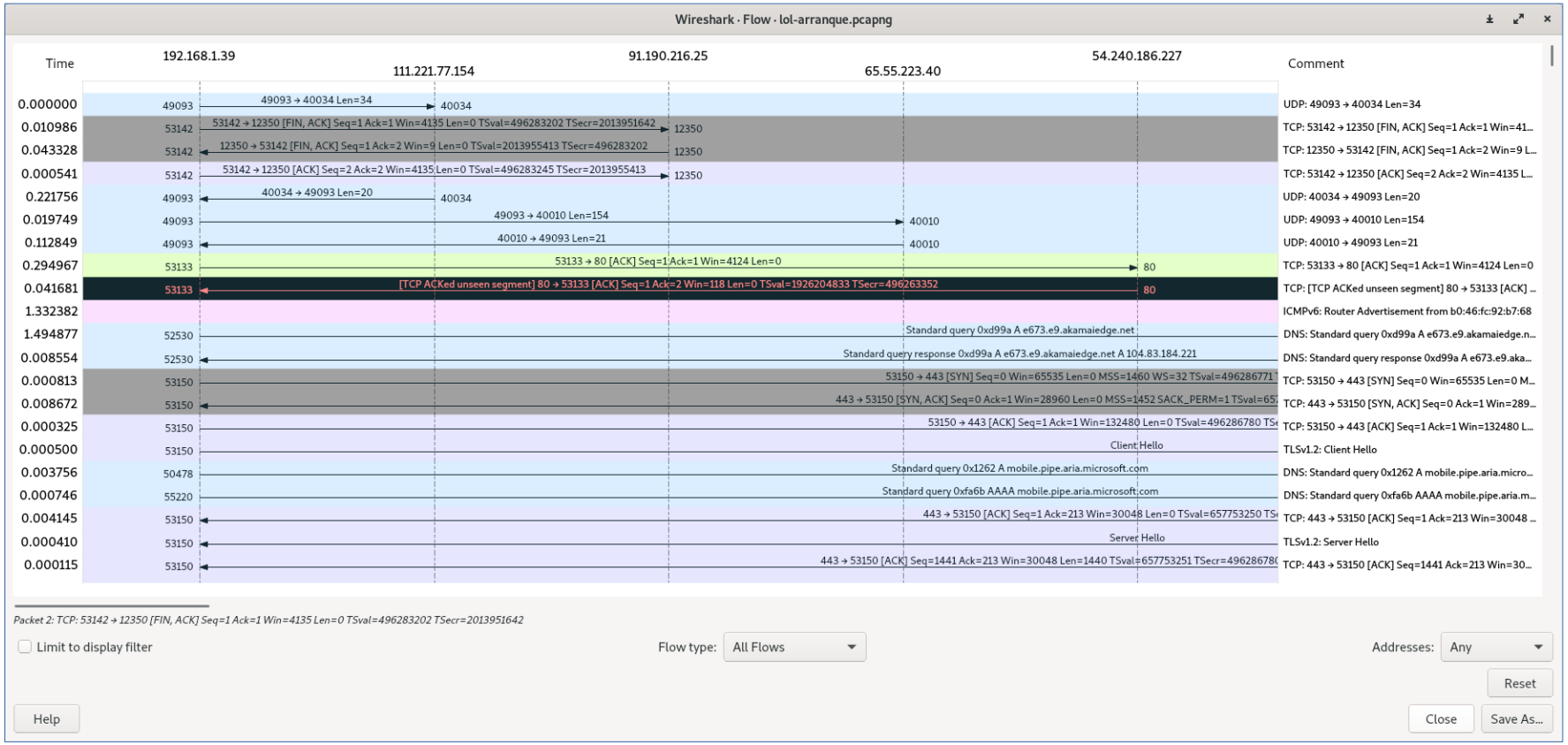
- Texto plano
- Archivos csv
- Archivos YAML



Estadísticas

Flow Graph

Nos ofrece una ventana con el tráfico en modo gráfico



Estadísticas

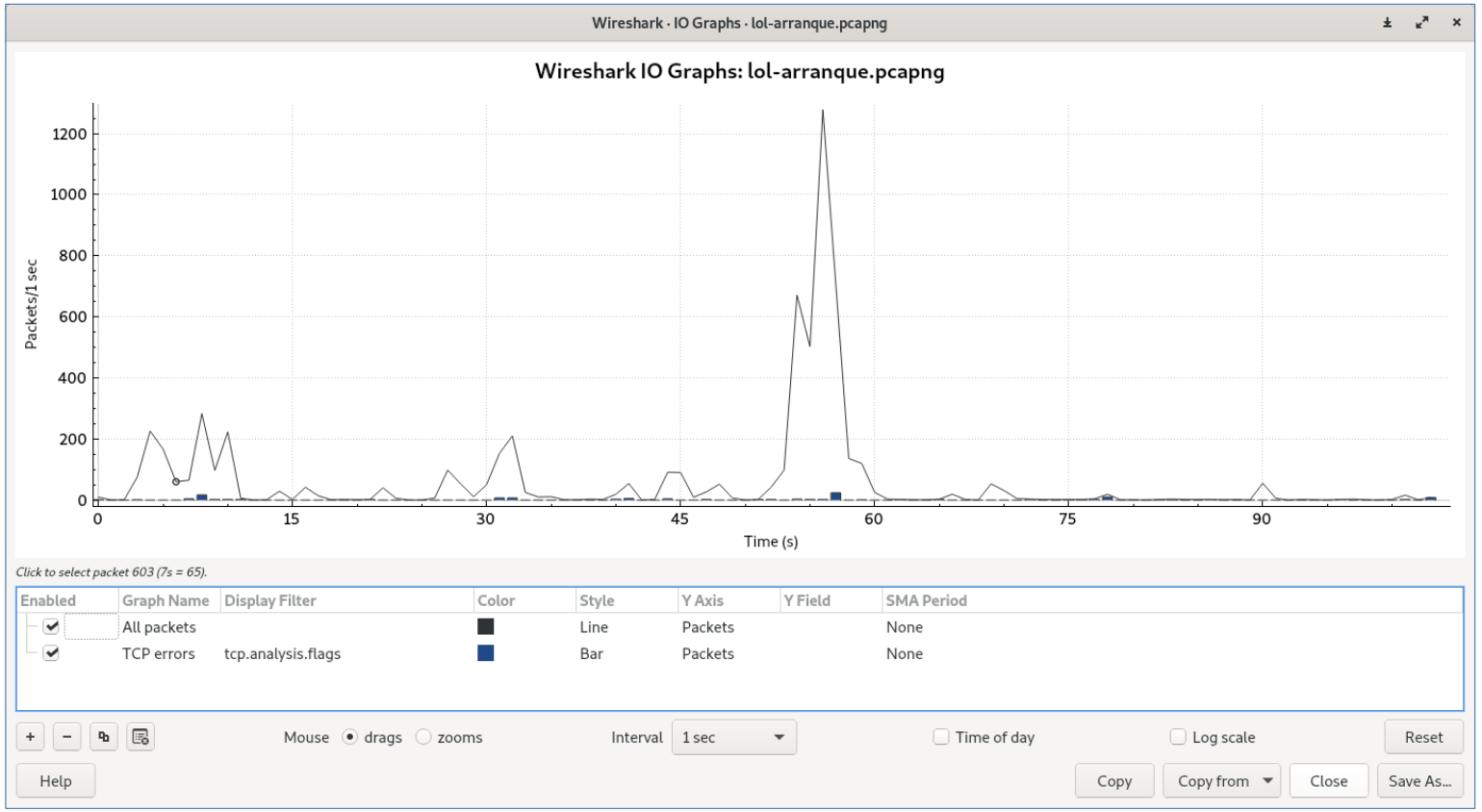
Laboratorio 3

Hacer un estudio desde la perspectiva de Flow Graph, filtrar por aplicación y vuelve a ver el flujo de datos

Estadísticas

Estadísticas IO-Graph

Un gráfico, nos permite analizar el flujo de una aplicación o host y compararlo con ciertos eventos o comportamientos



Estadísticas

Estadísticas IO-Graph

El eje X, corresponde al tiempo, el eje Y, puede contener un filtro y

- Paquetes
- Bytes
- Operaciones estadísticas
  - Suma (SUM), resúmen de parámetros en el intervalo
  - Conteos (COUNT FRAME y COUNT FIELD), cuenta lo encontrado en tramas y campos filtrados
  - Valores máximos, mínimos y medias (MAX, MIN y AVG)
  - Tiempos de respuesta (LOAD), se utiliza para gráficos de tiempo de respuesta

Estadísticas

Estadísticas IO-Graph

Podemos elegir varios tipos de gráficas

- Barras
- Linea
- Puntos
- Cuadrados
- Impulsos

Podemos añadir otros gráficos para comprarar, y elegir en Display filter, los paquetes que queramos elegir en el estudio

Estadísticas

Estadísticas IO-Graph

Si el archivo que queremos estudiar, tiene varias conversaciones, debemos utilizar un filtro para ver la conversación deseada

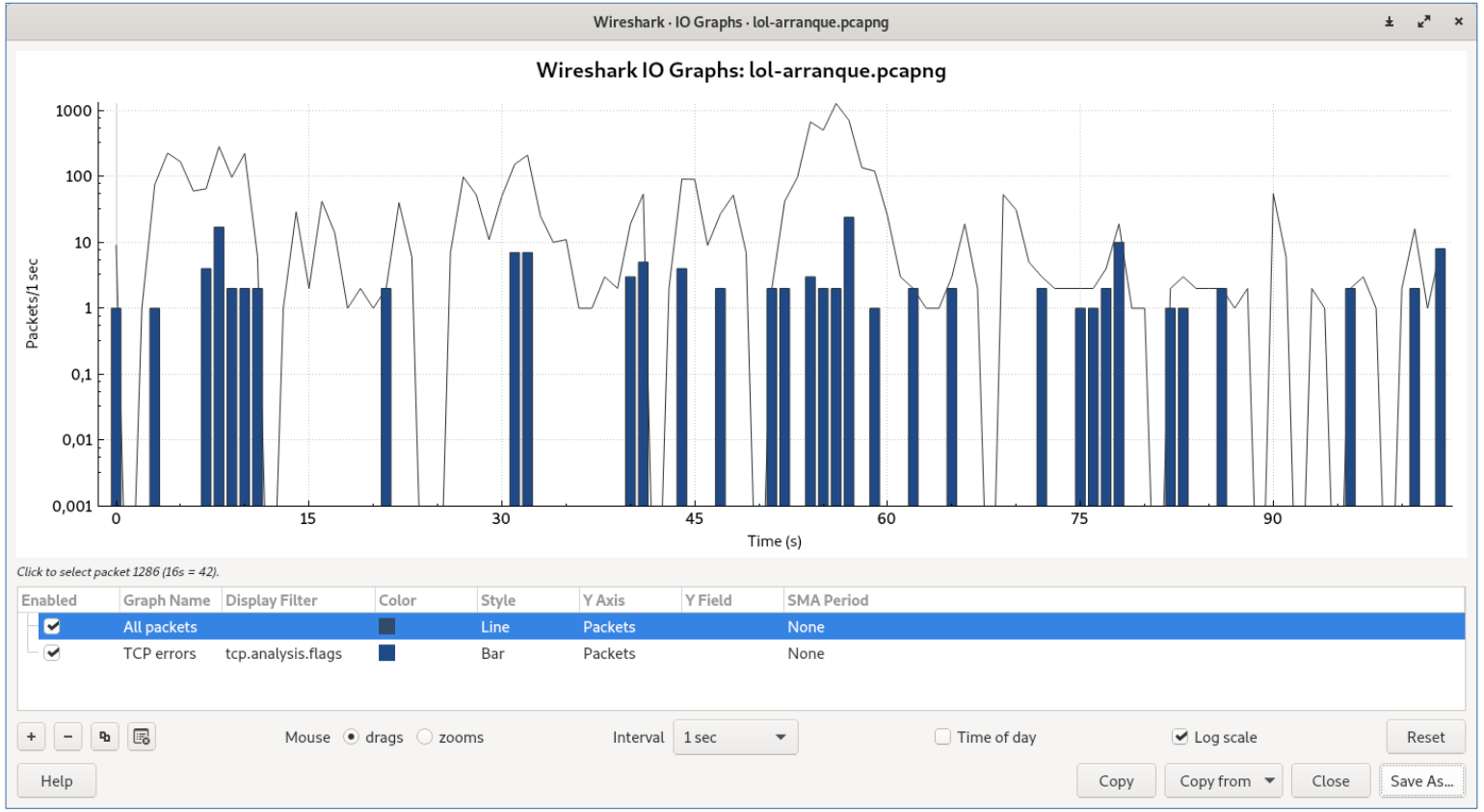
Cuando se hace un gráfico de aplicaciones basadas en TCP, asegurese de aplicar el filtro en el puerto, en lugar de en el nombre de la aplicación

Con Time of Day, ajustamos el tiempo en valor absoluto

Estadísticas

Estadísticas IO-Graph

Con Log scale, vemos el gráfico, como una escala logarítmica



Estadísticas

Laboratorio 4

Estudio de bajo rendimiento

- Crear un gráfico IO para comprobar el momento en que cae el rendimiento
- Ver la lista del paquete en el momento que aparece el problema
- ¿Cuál es la causa del problema?

Estadísticas

Laboratorio 5

Errores TCP

- Errores que afectan al rendimiento
- Mirar la evolución de los numeros de secuencia

Estadísticas

TCP Stream Graph

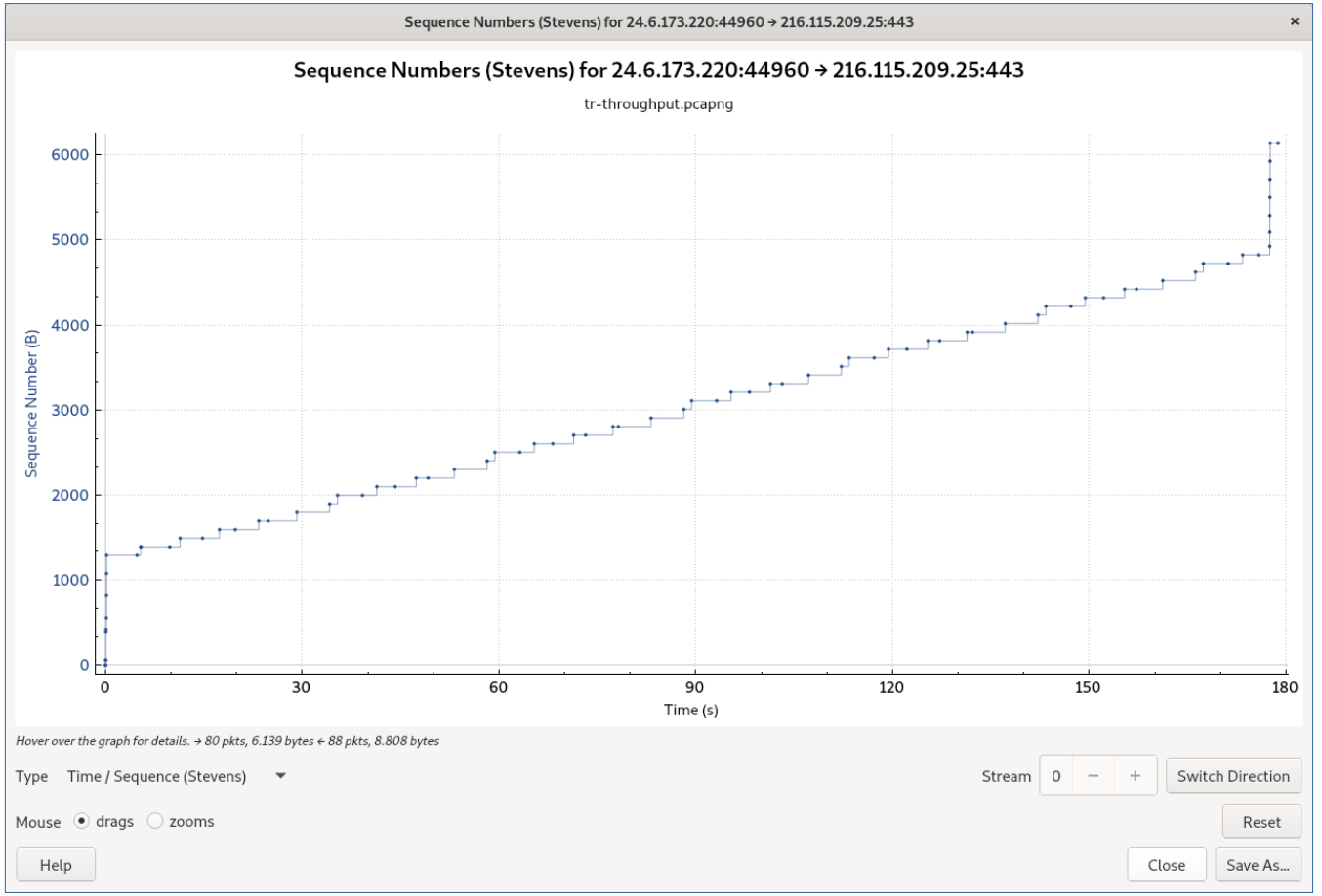
Una de las herramientas que nos permite profundizar en el comportamiento de las aplicaciones, es el gráfico de flujo TCP, **TCP Stream Graph** (Time Secuence Graph)

En todos los tipos de gráficos, nos aparece la dirección de la conversación IP (origen → destino) y un botón **Switch Direction**, para ver el sentido contrario de la conversación

Estadísticas

TCP Stream Graph Steven

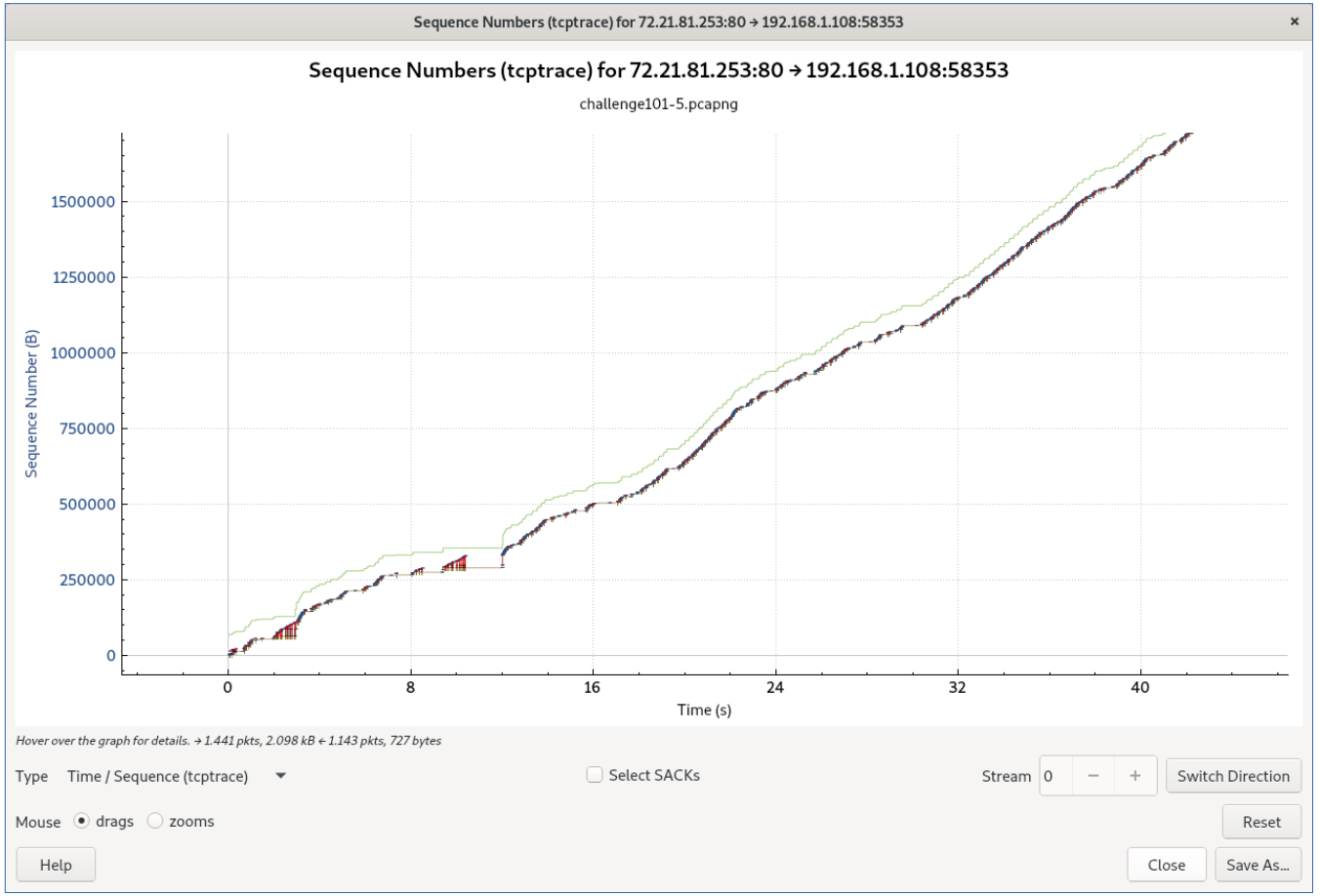
Muestra un gráfico con el número de secuencia a lo largo del tiempo, es decir, vemos el avance de la transferencia de bytes en el tiempo



Estadísticas

TCP Stream Graph Steven

Estos gráficos, además del número de secuencia / segundo, también recibe información sobre los ACKs que se enviaron, retransmisiones, tamaño de ventana y más detalles que permiten analizar los problemas de conexión

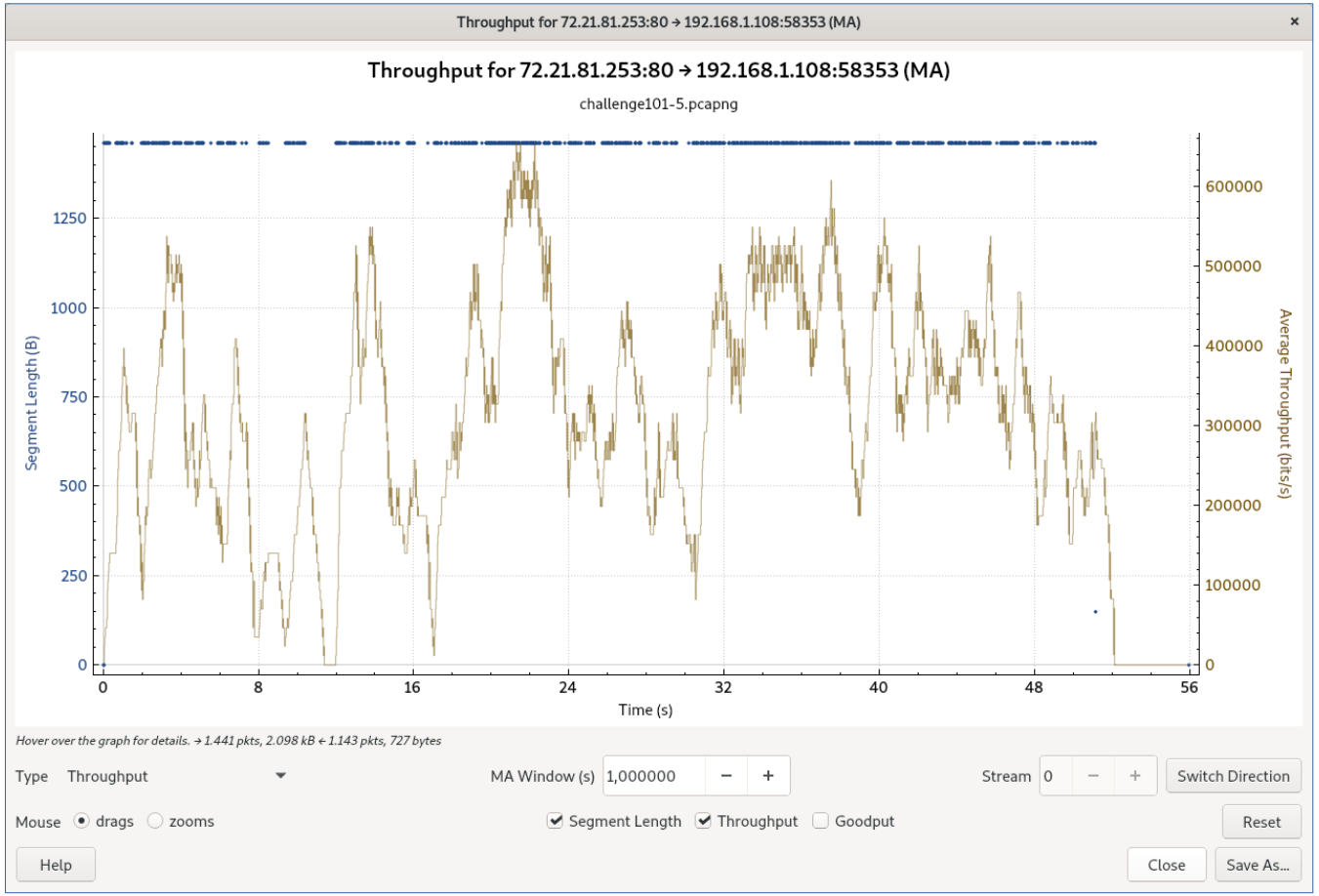


Estadísticas

TCP Stream Graph Throughput

Nos permite ver el rendimiento de una conexión y verificar su inestabilidad.

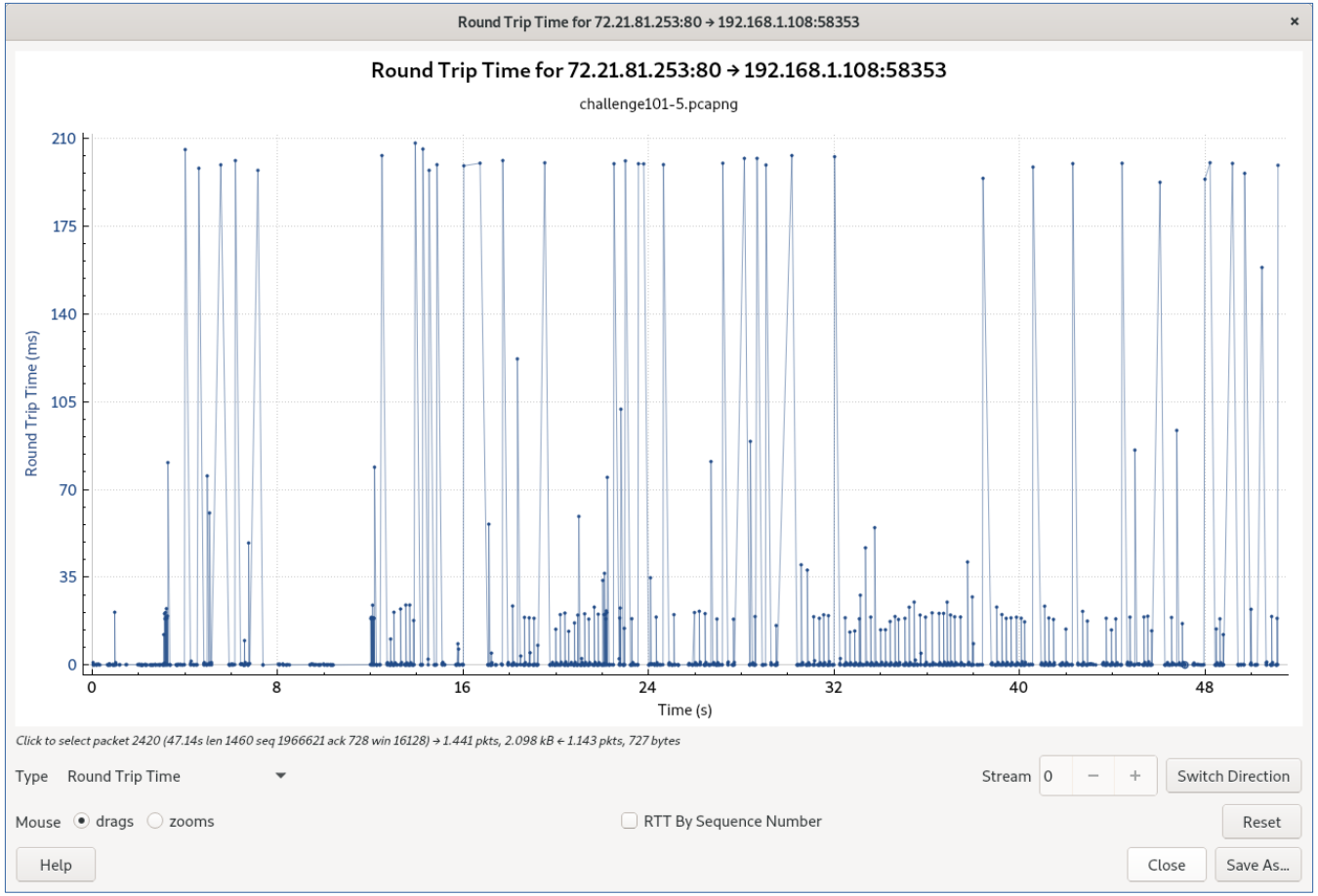
Podemos elegir ver, la relación del tamaño del paquete con respecto al rendimiento



Estadísticas

TCP Stream Graph Round Trip Time

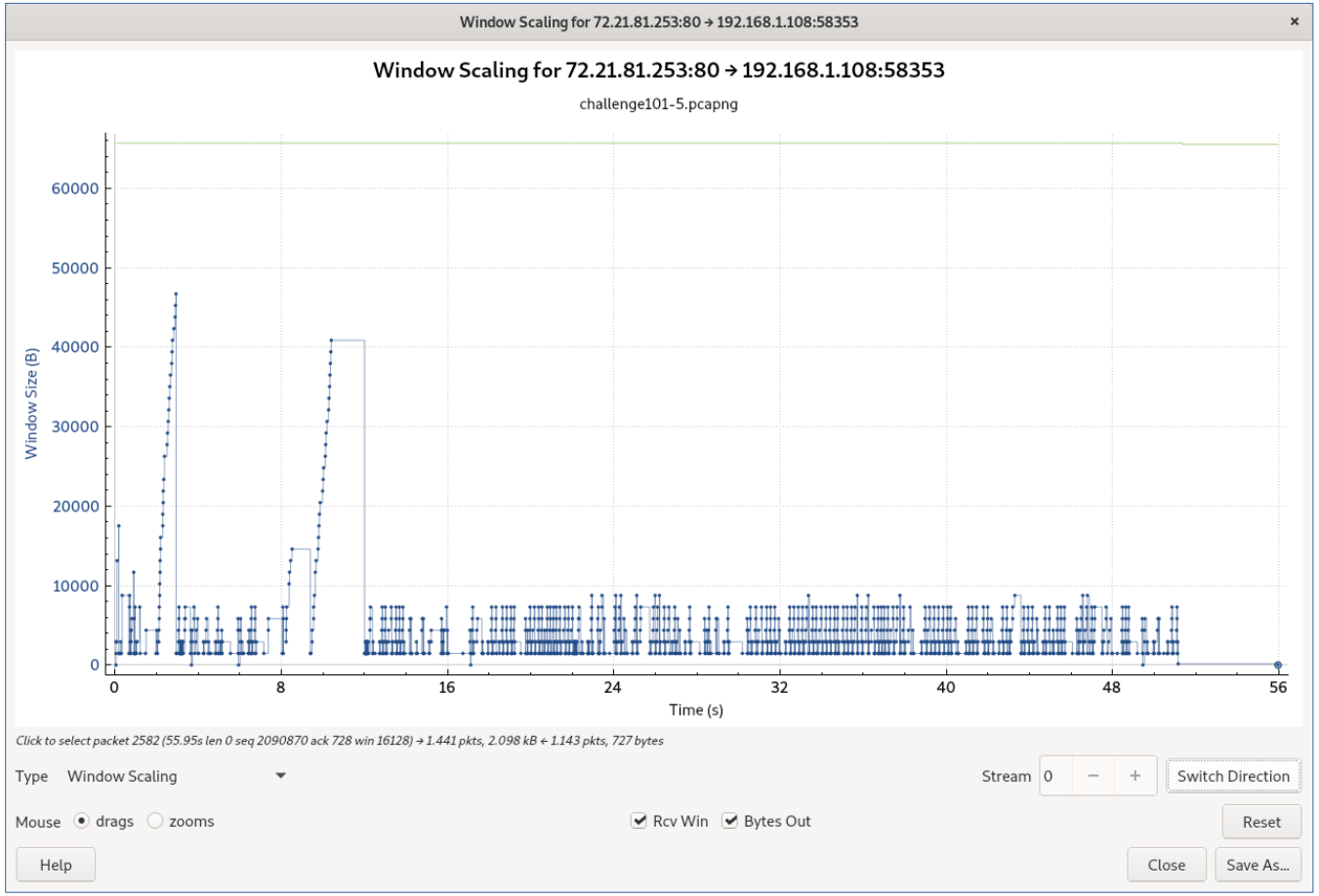
El gráfico, representa los números de secuencia TCP frente al tiempo que llevó reconocerlos



Estadísticas

TCP Stream Graph Window Scaling

Nos permite ver el tamaño de la ventana publicada por el lado del receptor, que es una indicación de la incapacidad del receptor para procesar datos



Estadísticas

Laboratorio 6

Archivo HTTP con problemas

- Mirar qué tipo de problemas tiene y analizar con gráfico
- Ver la evolución del tráfico enviado
- Mirar la relación con el tamaño de la ventana y RTT
- Exportar gráficos representativos a archivo.png


Telefónica