

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 hacia 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

The image shows the 'Wireshark - Capture File Properties - lol-arranque.pcapng' window. It displays various details about the capture file, including file information, time, capture settings, interfaces, and statistics.

File

- Name: /home/kike/Documentacion/Informatica/Redes/Wireshark/Traceos/lol-arranque.pcapng
- Length: 3.036 kB
- Hash (SHA256): 2a47cd46f12ff47a22a68ee67c1bab91cf94663ce801cef04cdf35a72b2f4cbb
- Hash (RIPEMD160): 903ae16eb4242a2b5a949d2aaf53a74be30f7ee4
- Hash (SHA1): 3e4ef5544efb6e299176cab158667f14f0bcafc9
- Format: Wireshark/... - pcapng
- Encapsulation: Ethernet

Time

- First packet: 2017-03-30 19:27:53
- Last packet: 2017-03-30 19:29:36
- Elapsed: 00:01:43

Capture

- Hardware: Unknown
- OS: Linux 3.16.0-4-686-pae
- Application: Dumpcap 1.12.1 (Git Rev Unknown from unknown)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
br0	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	6185	6185 (100.0%)	—
Time span, s	103.121	103.121	—
Average pps	60.0	60.0	—
Average packet size, B	457	457	—
Bytes	2827657	2827657 (100.0%)	0
Average bytes/s	27 k	27 k	—
Average bits/s	219 k	219 k	—

Capture file comments

Help Refresh Copy To Clipboard Close Save Comments

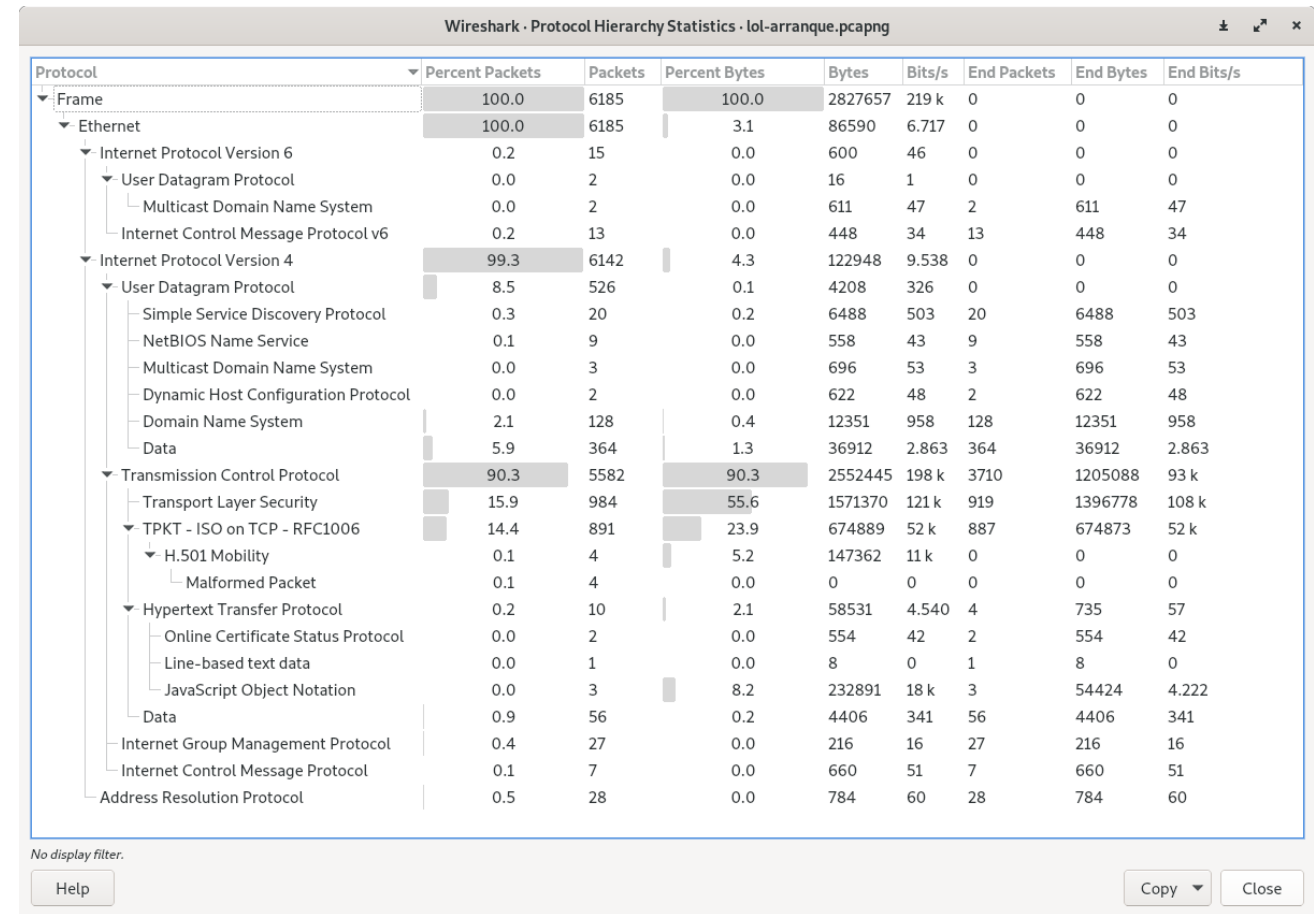
Estadísticas

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



Estadísticas

Protocol Hierarchy

Nos presenta datos estadísticos de los protocolos

- Nombre del protocolo
- **Percent Packets**, porcentaje 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

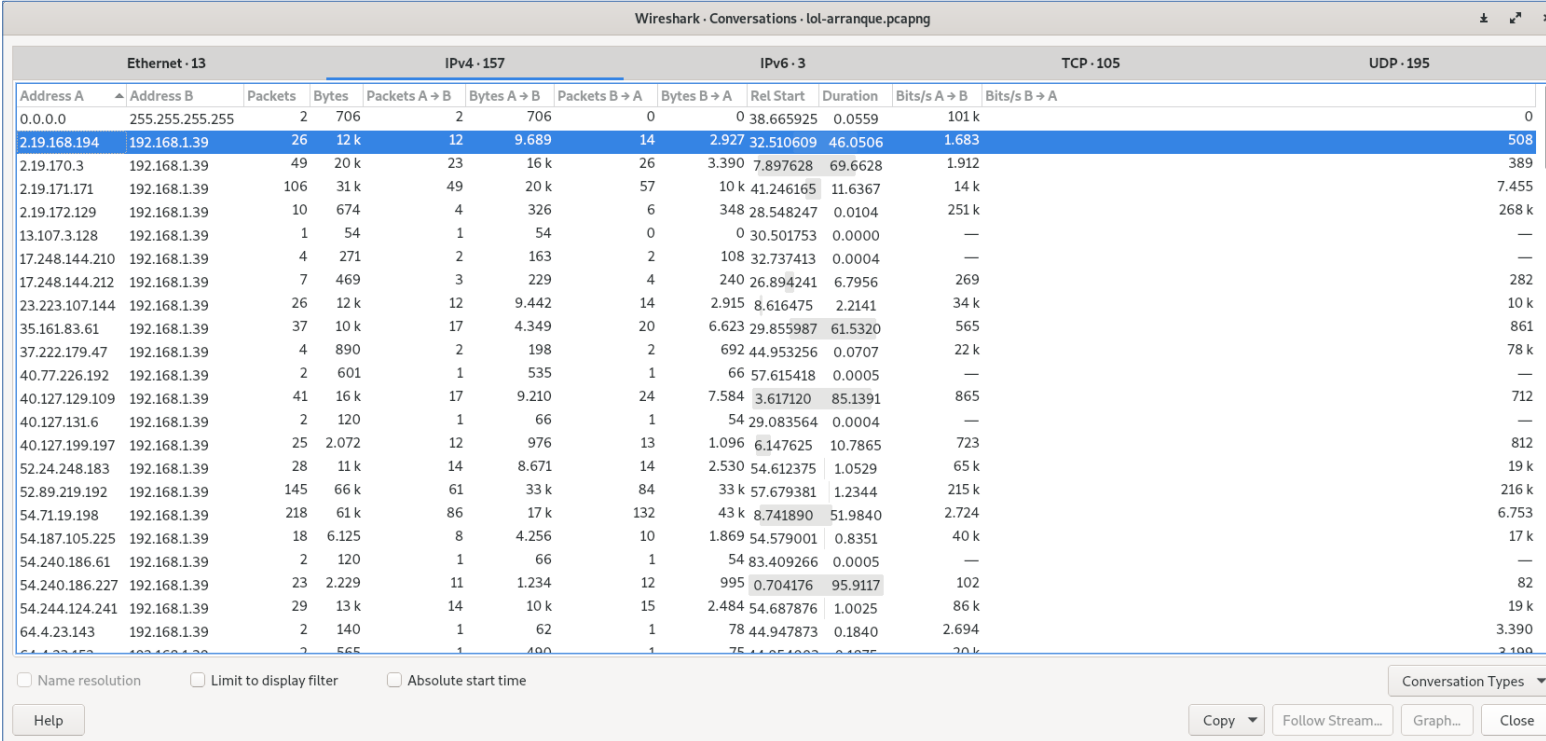
Podemos elegir entre conversaciones

- Ethernet
- IPv4 e IPv6
- TCP
- UDP

Estadísticas

Conversations

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



Wireshark · Conversations · lol-arranque.pcapng

Ethernet · 13		IPv4 · 157				IPv6 · 3				TCP · 105		UDP · 195	
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
0.0.0.0	255.255.255.255	2	706	2	706	0	0	38.665925	0.0559	101 k		0	
219.168.194	192.168.1.39	26	12 k	12	9.689	14	2.927	32.510609	46.0506	1.683		508	
219.170.3	192.168.1.39	49	20 k	23	16 k	26	3.390	7.897628	69.6628	1.912		389	
219.171.171	192.168.1.39	106	31 k	49	20 k	57	10 k	41.246165	11.6367	14 k		7.455	
219.172.129	192.168.1.39	10	674	4	326	6	348	28.548247	0.0104	251 k		268 k	
13.107.3.128	192.168.1.39	1	54	1	54	0	0	30.501753	0.0000	—		—	
17.248.144.210	192.168.1.39	4	271	2	163	2	108	32.737413	0.0004	—		—	
17.248.144.212	192.168.1.39	7	469	3	229	4	240	26.894241	6.7956	269		282	
23.223.107.144	192.168.1.39	26	12 k	12	9.442	14	2.915	8.616475	2.2141	34 k		10 k	
35.161.83.61	192.168.1.39	37	10 k	17	4.349	20	6.623	29.855987	61.5320	565		861	
37.222.179.47	192.168.1.39	4	890	2	198	2	692	44.953256	0.0707	22 k		78 k	
40.77.226.192	192.168.1.39	2	601	1	535	1	66	57.615418	0.0005	—		—	
40.127.129.109	192.168.1.39	41	16 k	17	9.210	24	7.584	3.617120	85.1391	865		712	
40.127.131.6	192.168.1.39	2	120	1	66	1	54	29.083564	0.0004	—		—	
40.127.199.197	192.168.1.39	25	2.072	12	976	13	1.096	6.147625	10.7865	723		812	
52.24.248.183	192.168.1.39	28	11 k	14	8.671	14	2.530	54.612375	1.0529	65 k		19 k	
52.89.219.192	192.168.1.39	145	66 k	61	33 k	84	33 k	57.679381	1.2344	215 k		216 k	
54.71.19.198	192.168.1.39	218	61 k	86	17 k	132	43 k	8.741890	51.9840	2.724		6.753	
54.187.105.225	192.168.1.39	18	6.125	8	4.256	10	1.869	54.579001	0.8351	40 k		17 k	
54.240.186.61	192.168.1.39	2	120	1	66	1	54	83.409266	0.0005	—		—	
54.240.186.227	192.168.1.39	23	2.229	11	1.234	12	995	0.704176	95.9117	102		82	
54.244.124.241	192.168.1.39	29	13 k	14	10 k	15	2.484	54.687876	1.0025	86 k		19 k	
64.4.23.143	192.168.1.39	2	140	1	62	1	78	44.947873	0.1840	2.694		3.390	
64.4.23.143	192.168.1.39	2	140	1	62	1	78	44.947873	0.1840	2.694		3.390	

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Help

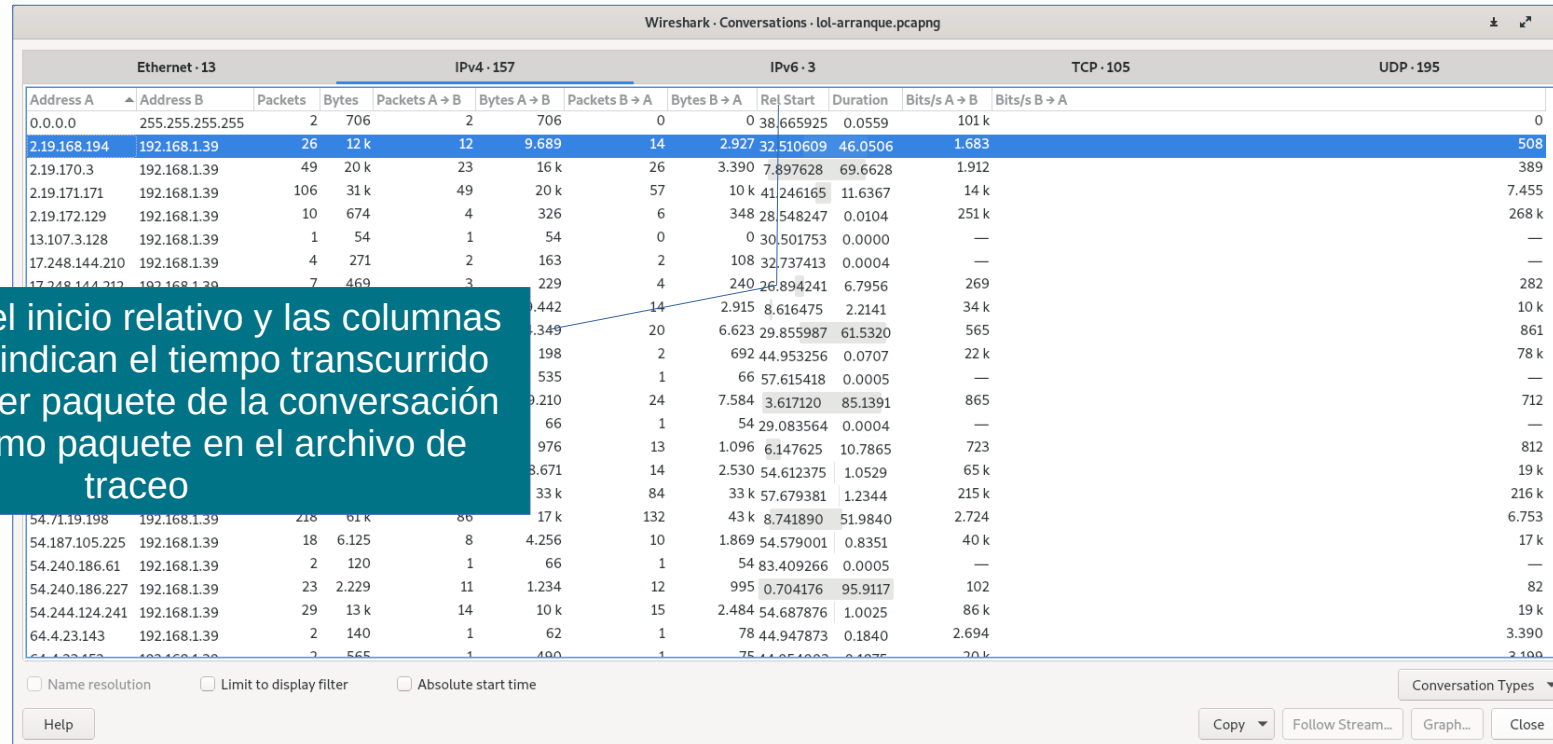
Conversation Types ▾

Copy ▾ Follow Stream... Graph... Close

Estadísticas

Conversations

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



Wireshark · Conversations · lol-arranque.pcapng

Ethernet · 13		IPv4 · 157				IPv6 · 3				TCP · 105		UDP · 195	
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
0.0.0.0	255.255.255.255	2	706	2	706	0	0	38.665925	0.0559	101 k		0	
219.168.194	192.168.1.39	26	12 k	12	9.689	14	2.927	32.510609	46.0506	1.683		508	
219.170.3	192.168.1.39	49	20 k	23	16 k	26	3.390	7.897628	69.6628	1.912		389	
219.171.171	192.168.1.39	106	31 k	49	20 k	57	10 k	41.246165	11.6367	14 k		7.455	
219.172.129	192.168.1.39	10	674	4	326	6	348	28.548247	0.0104	251 k		268 k	
13.107.3.128	192.168.1.39	1	54	1	54	0	0	30.501753	0.0000	—		—	
17.248.144.210	192.168.1.39	4	271	2	163	2	108	32.737413	0.0004	—		—	
17.248.144.212	192.168.1.39	7	469	3	229	4	240	26.894241	6.7956	269		282	
192.168.1.39	192.168.1.39	14	442	14	2.915	8.616475	2.2141	34 k		10 k			
192.168.1.39	192.168.1.39	20	349	20	6.623	29.855987	61.5320	565		861			
192.168.1.39	192.168.1.39	2	198	2	692	44.953256	0.0707	22 k		78 k			
192.168.1.39	192.168.1.39	1	535	1	66	57.615418	0.0005	—		—			
192.168.1.39	192.168.1.39	24	9.210	24	7.584	3.617120	85.1391	865		712			
192.168.1.39	192.168.1.39	1	66	1	54	29.083564	0.0004	—		—			
192.168.1.39	192.168.1.39	13	976	13	1.096	6.147625	10.7865	723		812			
192.168.1.39	192.168.1.39	14	8.671	14	2.530	54.612375	1.0529	65 k		19 k			
192.168.1.39	192.168.1.39	84	33 k	84	33 k	57.679381	1.2344	215 k		216 k			
192.168.1.39	192.168.1.39	132	17 k	132	43 k	8.741890	51.9840	2.724		6.753			
192.168.1.39	192.168.1.39	10	54.187.105.225	10	1.869	54.579001	0.8351	40 k		17 k			
192.168.1.39	192.168.1.39	1	54.240.186.61	1	54	83.409266	0.0005	—		—			
192.168.1.39	192.168.1.39	23	54.240.186.227	23	2.229	0.704176	95.9117	102		82			
192.168.1.39	192.168.1.39	29	54.244.124.241	29	13 k	14	10 k	15	2.484	54.687876	1.0025	86 k	19 k
192.168.1.39	192.168.1.39	2	64.4.23.143	2	140	1	62	1	78	44.947873	0.1840	2.694	3.390
192.168.1.39	192.168.1.39	2	64.1.23.158	2	565	1	480	1	75	11.051803	0.1035	20 k	2.100

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Help

Copy Follow Stream... Graph... Close

Conversation Types

Estadísticas

Conversations

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

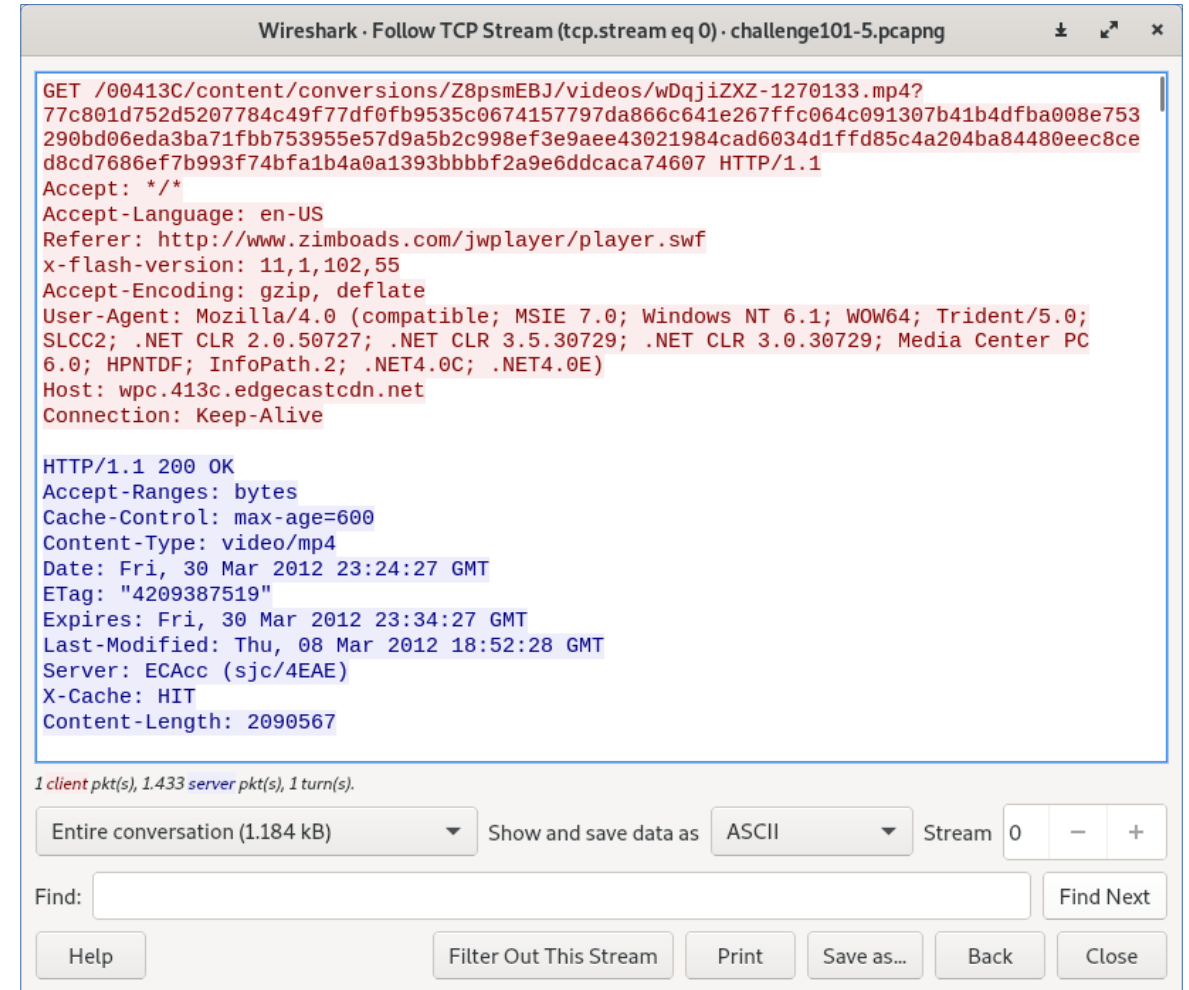
Desde el campo de selección **Display types**, podemos seleccionar que protocolos se van a visualizar

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

Estadísticas

Conversations

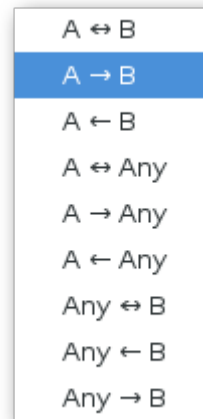
Desde la pestaña TCP, si seleccionamos una conversación, se activará el botón **Follow Stream**, que extrae el flujo de datos establecido en una sesión TCP



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

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

Estadísticas

Estadísticas IP

Nos ofrece varias estadísticas sobre el tráfico IP

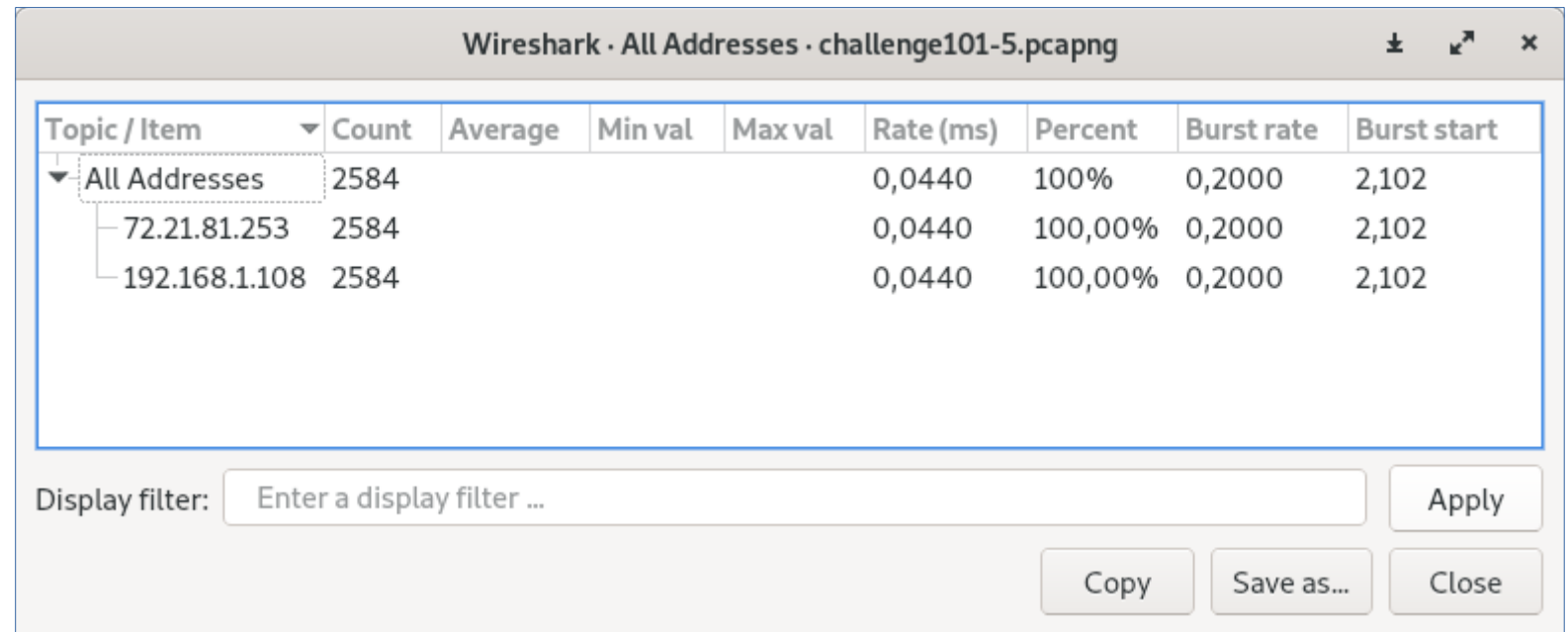
- All addresses, se visualizan todas las estadísticas de paquetes
- Destination and ports, mostrará todas las direcciones IP destino al cual son enviados y sobre qué protocolos.
- IP protocol types
- Source and destination addresses

Estadísticas

Estadísticas IP

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

- Texto plano
- Archivos csv
- Archivos YAML

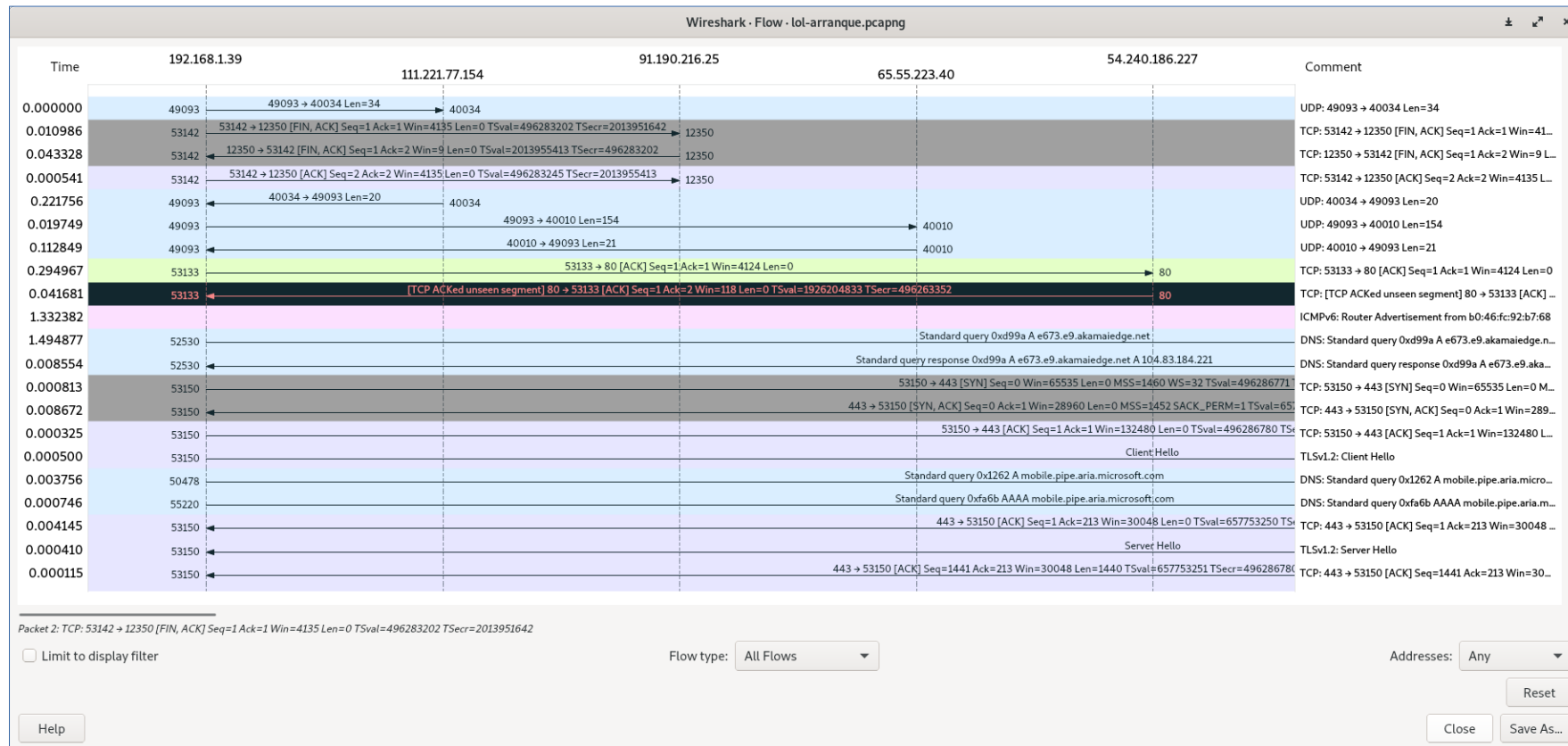
The image shows a screenshot of the 'Wireshark · All Addresses · challenge101-5.pcapng' window. It displays a table of IP address statistics. The table has columns for 'Topic / Item', 'Count', 'Average', 'Min val', 'Max val', 'Rate (ms)', 'Percent', 'Burst rate', and 'Burst start'. The data is organized into a tree structure under 'All Addresses', showing two sub-items: '72.21.81.253' and '192.168.1.108', each with a count of 2584. Below the table, there is a 'Display filter' input field and buttons for 'Apply', 'Copy', 'Save as...', and 'Close'.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ All Addresses	2584				0,0440	100%	0,2000	2,102
72.21.81.253	2584				0,0440	100,00%	0,2000	2,102
192.168.1.108	2584				0,0440	100,00%	0,2000	2,102

Estadísticas

Flow Graph

Nos ofrece una ventana con el tráfico en modo gráfico



Estadísticas

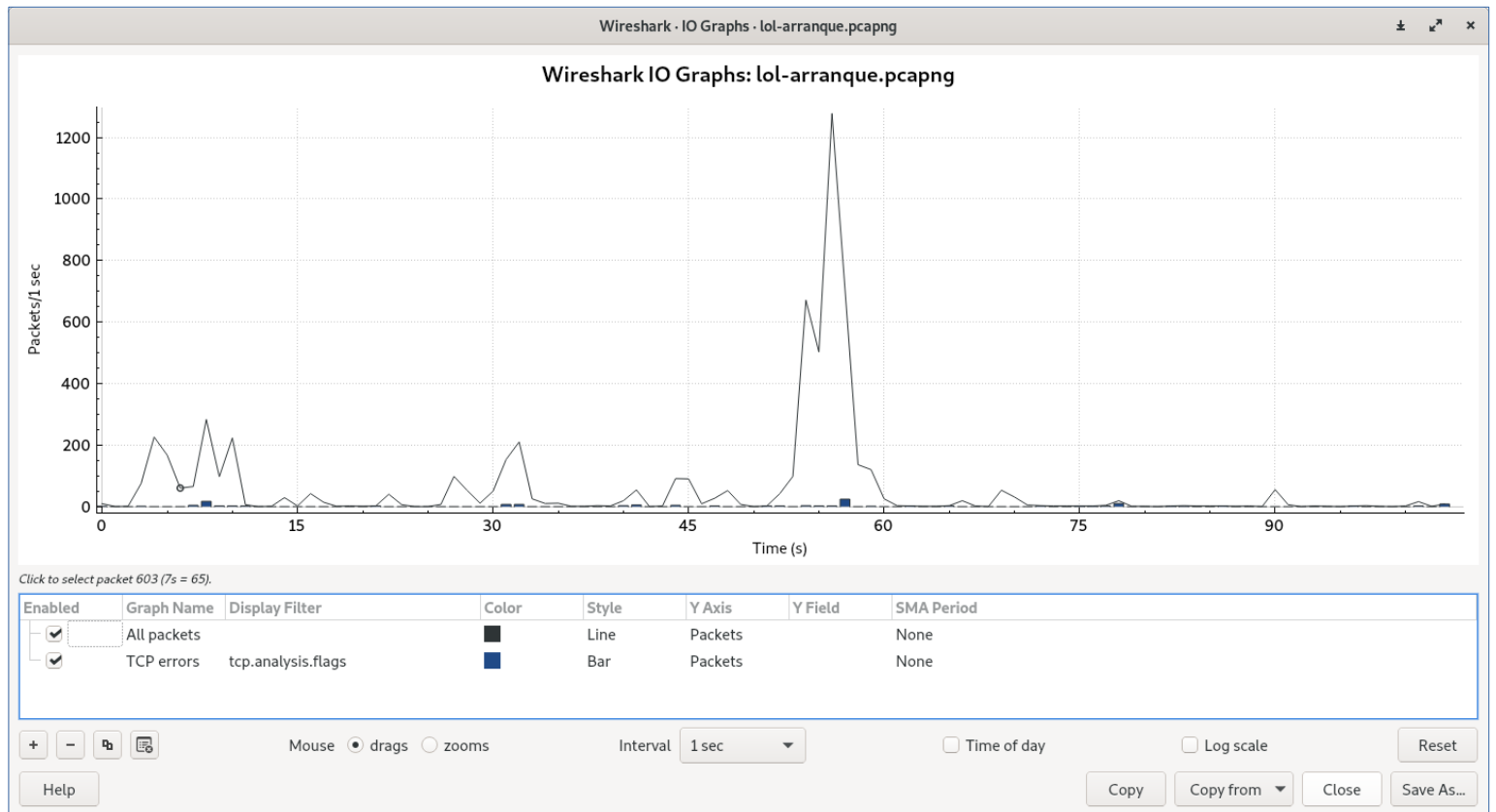
Laboratorio 3

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 queremos 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

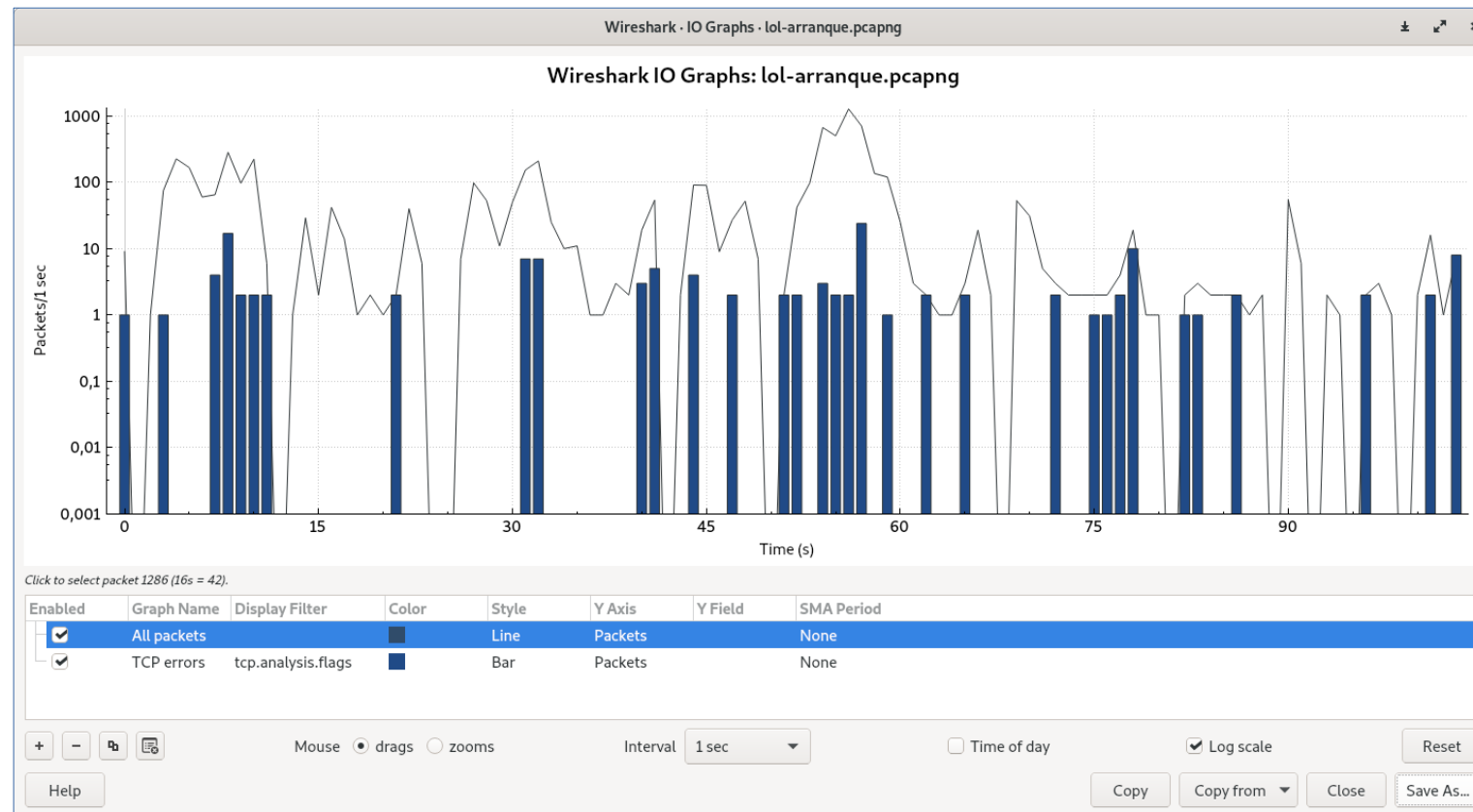
Cuando se hace un gráfico de aplicaciones basadas en TCP, asegúrese de aplicar el filtro en el puerto, en lugar de en el nombre de la aplicación

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

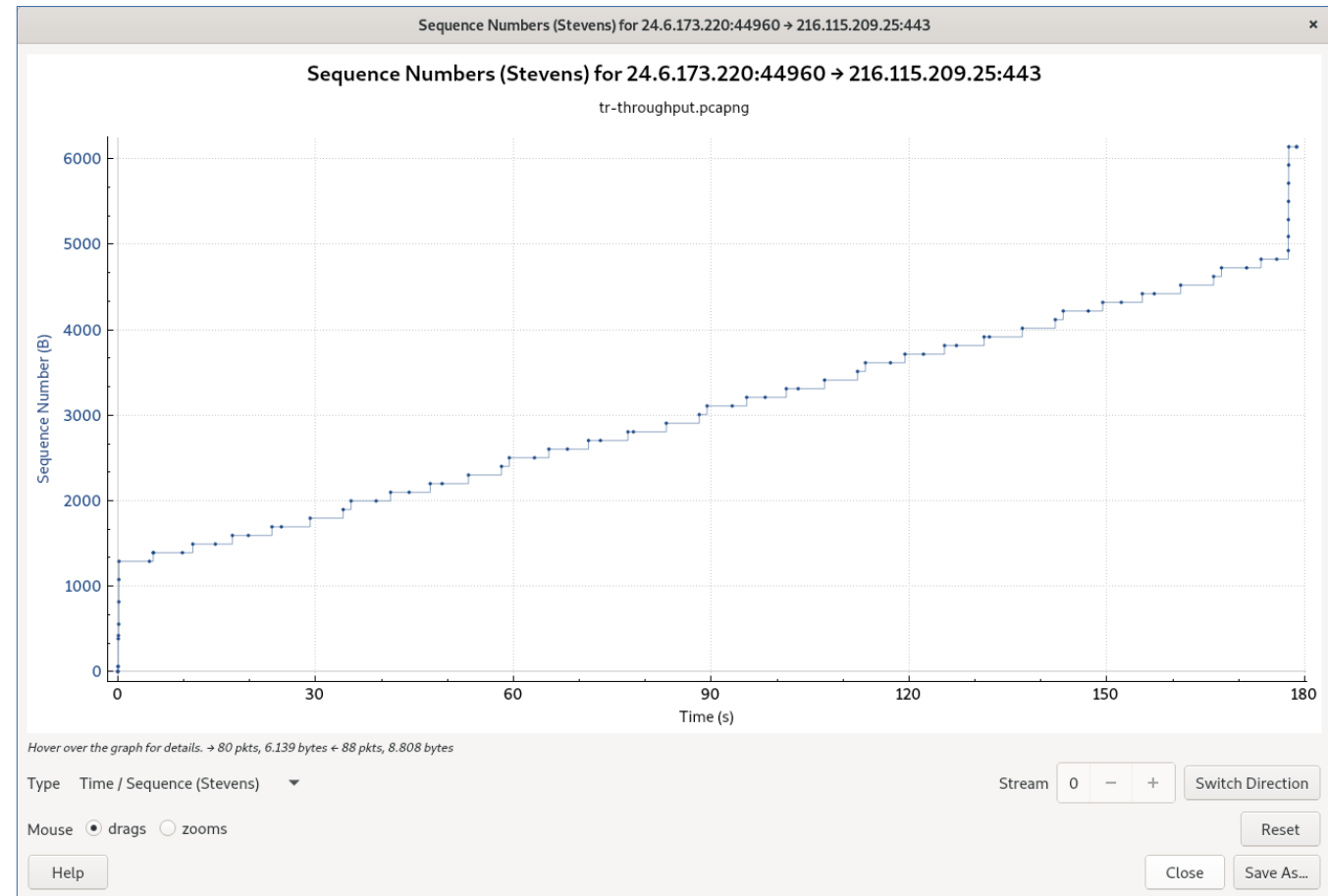
Una de las herramientas que nos permite profundizar en el comportamiento de las aplicaciones, es el gráfico de flujo TCP, **TCP Stream Graph** (Time Sequence Graph)

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

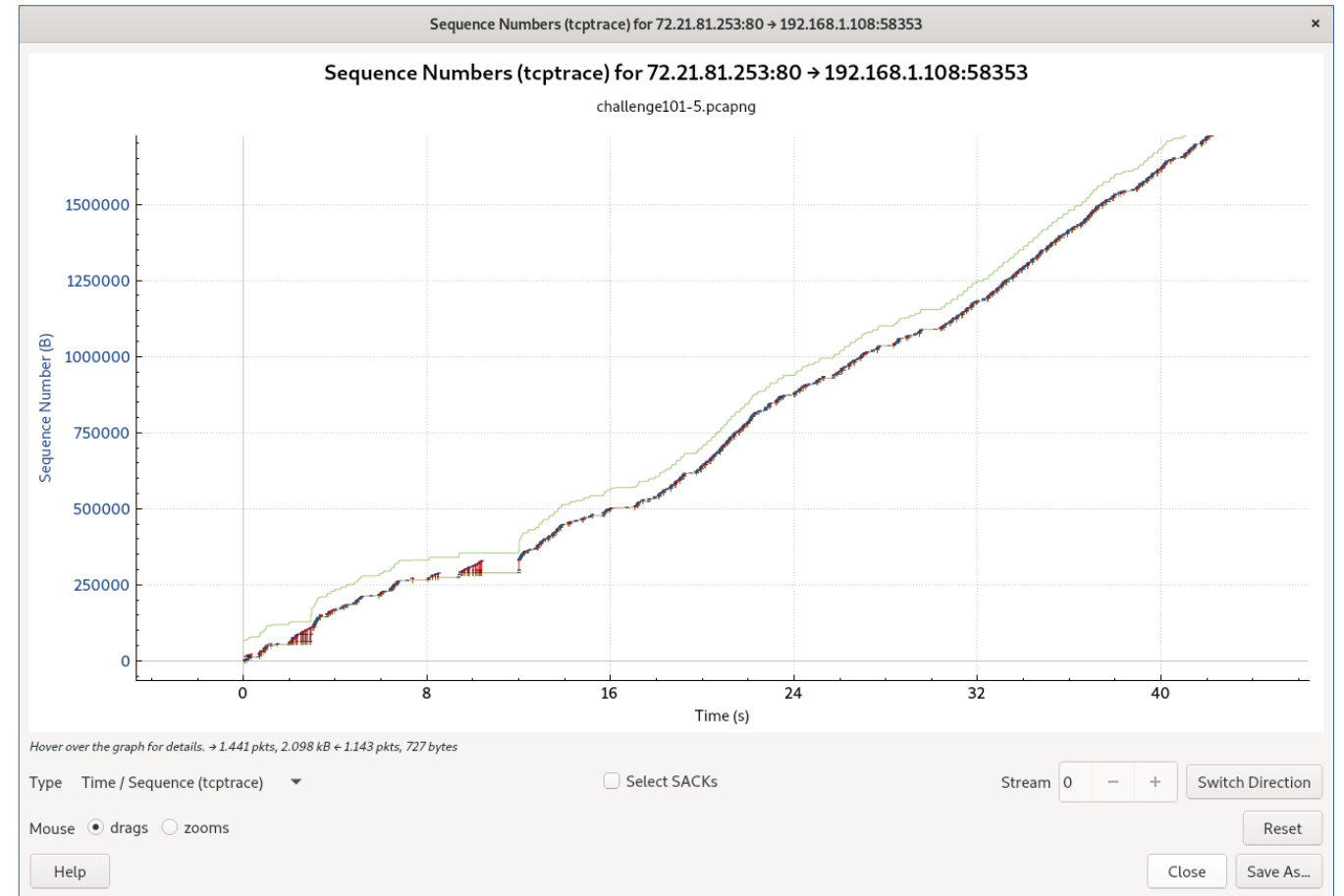
Muestra un gráfico con el número de secuencia a lo largo del tiempo, es decir, vemos el avance de la transferencia de bytes en el tiempo



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

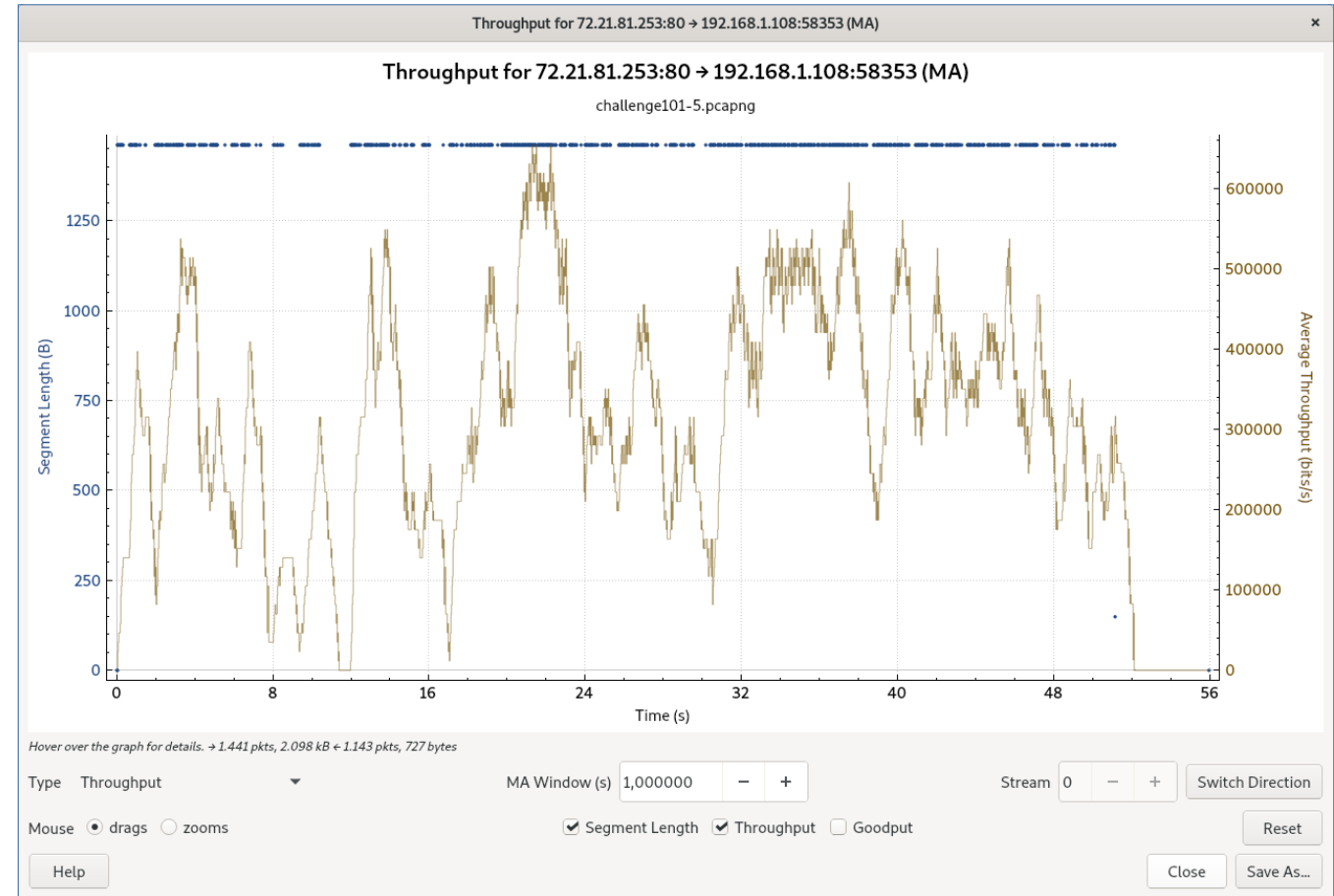


Estadísticas

TCP Stream Graph Throughput

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

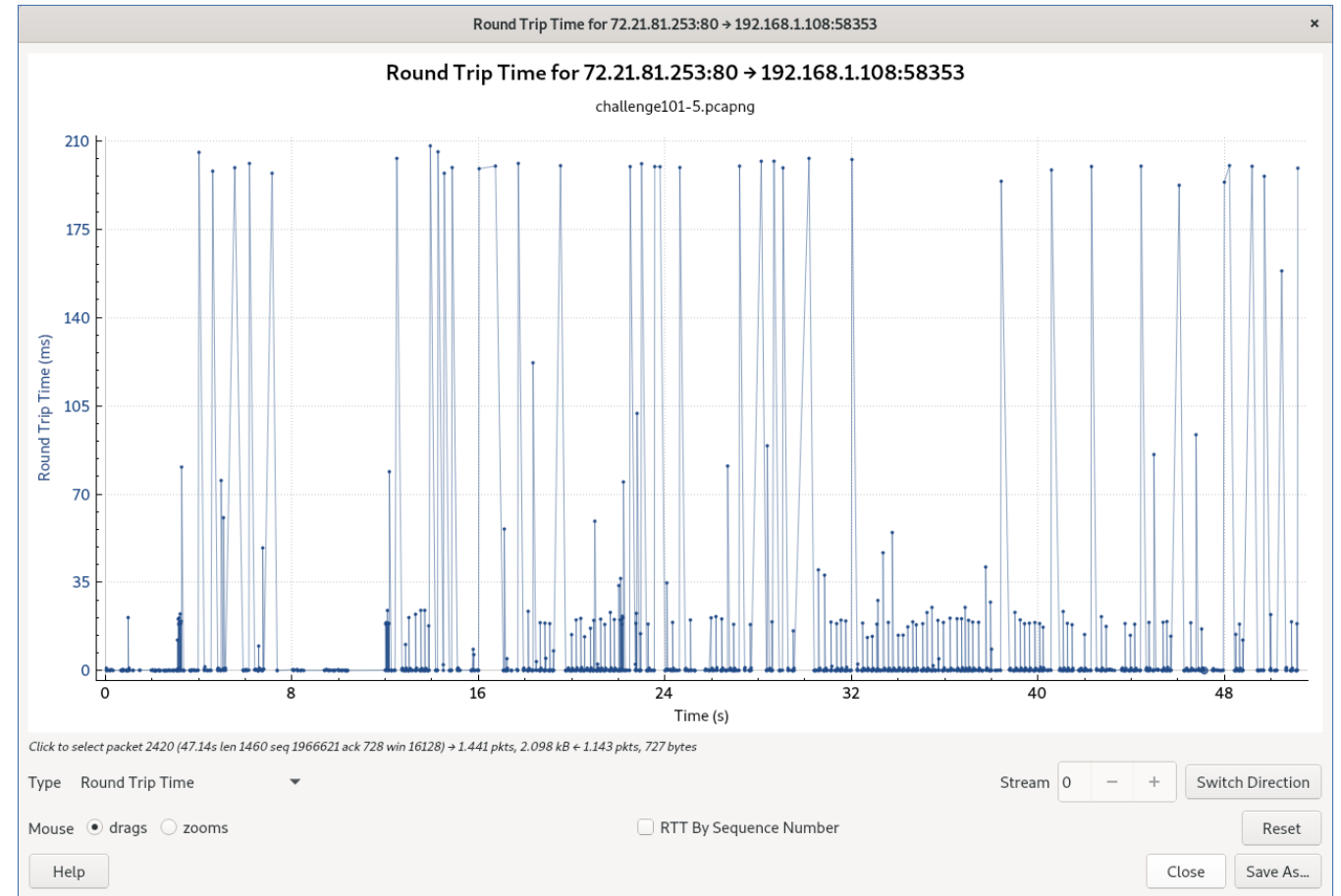
Podemos elegir ver, la relación del tamaño del paquete con respecto al rendimiento



Estadísticas

TCP Stream Graph Round Trip Time

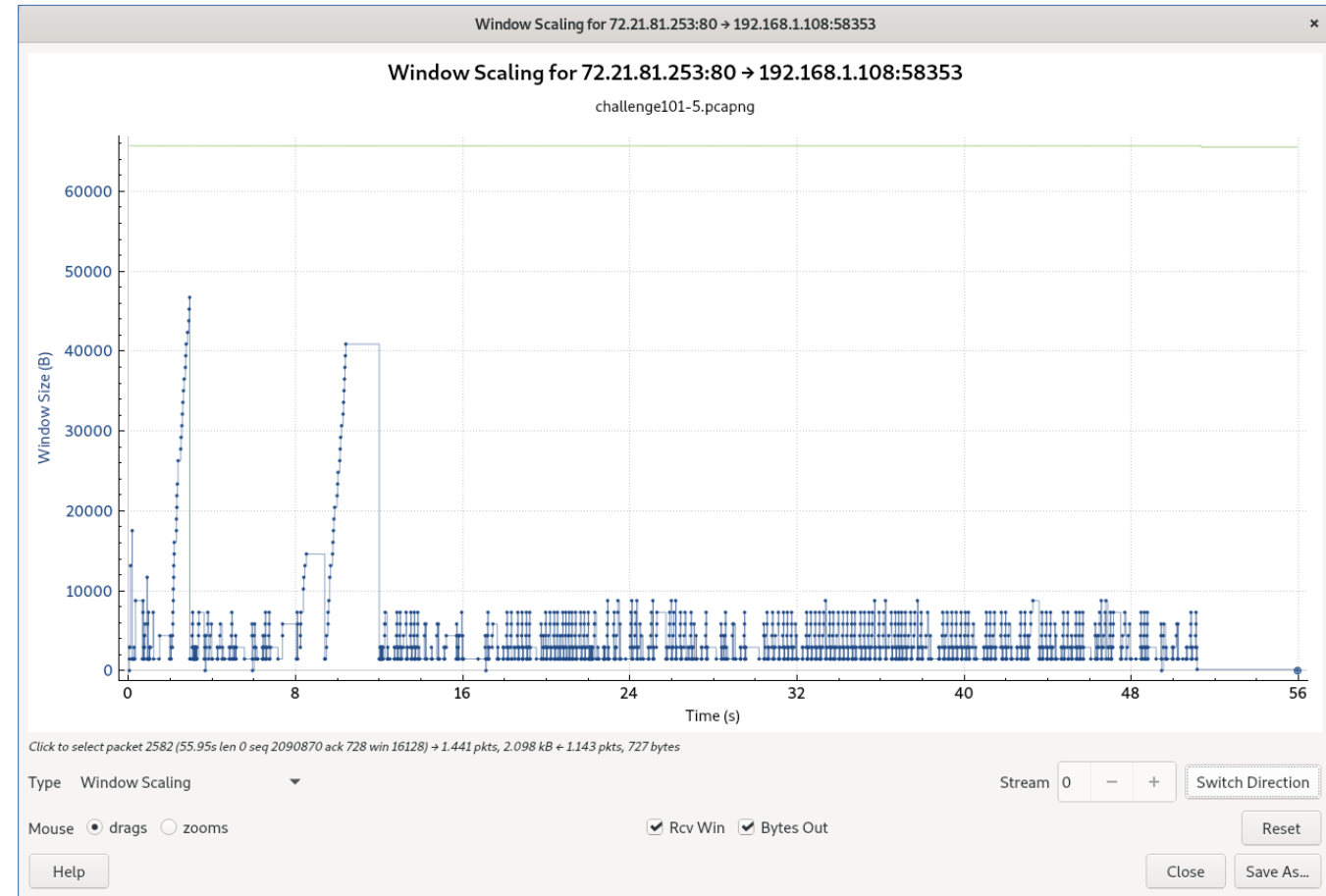
El gráfico, representa los números de secuencia TCP frente al tiempo que llevó reconocerlos



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
