

Telefonica

WIRESHARK

Voz sobre IP



Voz sobre IP

Protocolo SIP



- Las comunicaciones VoIP consisten principalmente en dos protocolos
 - El protocolo de señalización para la gestión de la llamada
 - El protocolo de transporte para las comunicaciones de voz

- SIP, es un ejemplo de protocolo de señalización, corre sobre UDP en el puerto 5060
- La voz es transportada sobre el protocolo RTP, un protocolo de control RTCP, proporciona información de control y estadística fuera de banda para flujos RTP.

- La voz sobre IP, es muy sensible a:
 - Latencia
 - Jitter, variación en los retrasos
 - Eco
 - Perdida de paquetes
 - Throughput

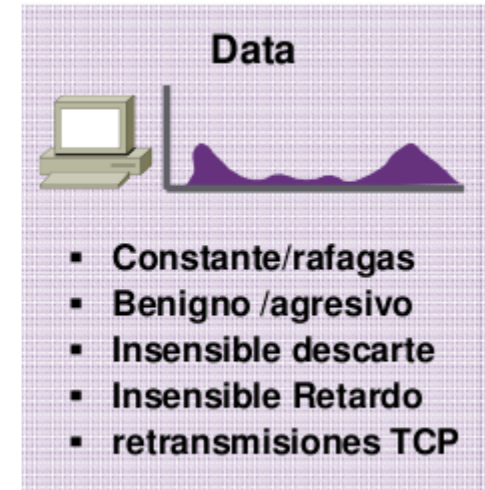
- La latencia total, está determinada por
 - Demoras en los algoritmos de compresión
 - Demoras de procesamiento
 - Demoras de red
- Hasta 100 ms, las demoras son toleradas, mas de 300 ms es imposible comunicarse

- El jitter, es la variación en el retraso, para ello se inserta un buffer de recepción, el cual agrega otro retraso al retraso total.
- El excesivo jitter puede ser causado por congestión en la red, configuraciones de QoS o enlace con poco ancho de banda.

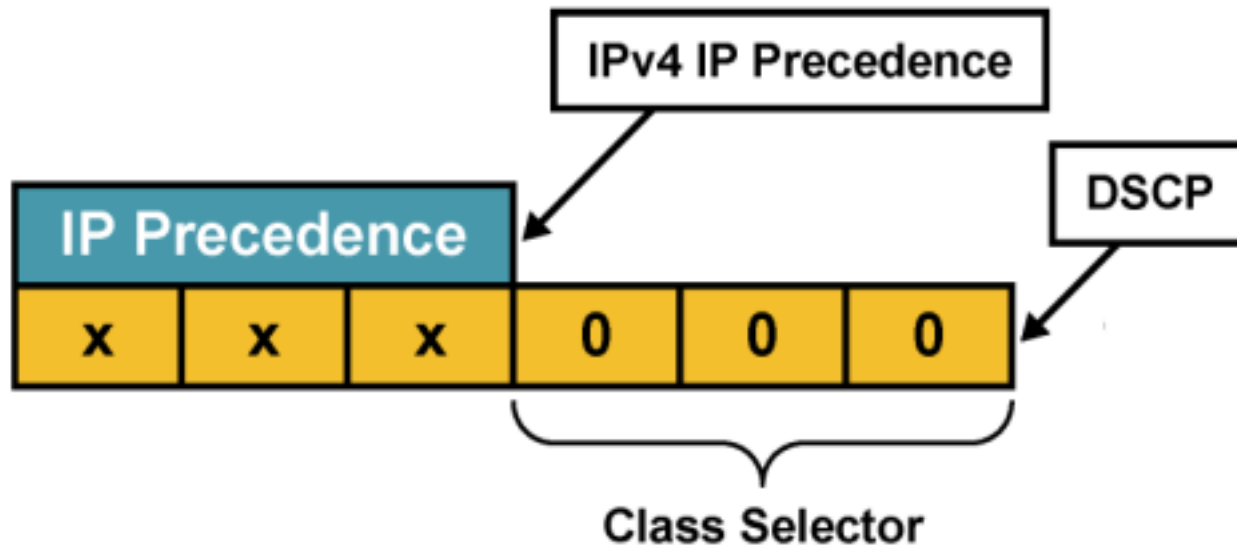
- El eco es debido a una reflexión causada por un desajuste de impedancias.
- No afecta si
 - El tiempo de retardo entre que se habla y se escucha es inferior a 30 ms
 - El nivel de retorno está por debajo de -25 dB
- Se usan canceladores de eco

- Para mejorar el rendimiento de un enlace, se usan técnicas como
 - Supresión de silencios y detección de voz
 - Compresión de cabeceras
- Utilizando priorización, podemos aplicar calidad de servicio.

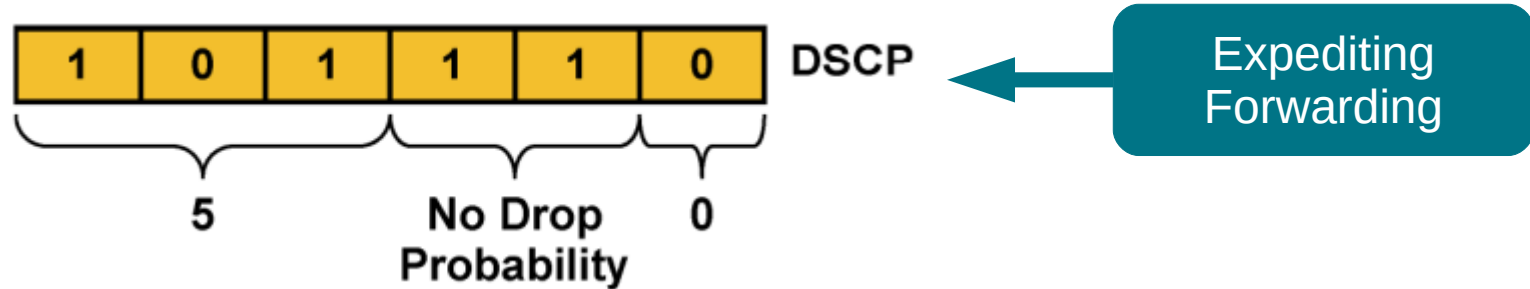
- Perfiles de tráfico



- Cuando hablamos de calidad de servicio, el campo ToS de la cabecera IP se redefine.

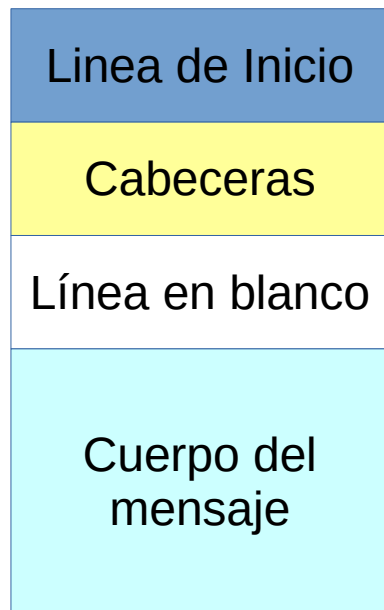


- Los DSCP se dividen en
 - Best Effort (por defecto)
 - Assured Forwarding (reenvío asegurado)
 - Expediting Forwarding (reenvío expedito)



- SIP es un protocolo basado en texto que nos permite
 - Localización del usuario
 - Gestión de la capacidad y disponibilidad del usuario
 - Gestionar los parámetros durante el establecimiento de la llamada
 - Manejar la llamada

- Los mensaje SIP se dividen en:
 - Solicitudes
 - Respuestas



REGISTER, notifica al servidor su dirección IP y su dirección URI

INVITE, invita a un usuario a participar de una sesión

ACK, se ha recibido una respuesta desde un servidor a INVITE

OPTIONS, permite a un usuario interrogar a otro sobre sus capacidades.

BYE, se usa para terminar una sesión

CANCEL, se usa para cancelar una petición previamente enviada

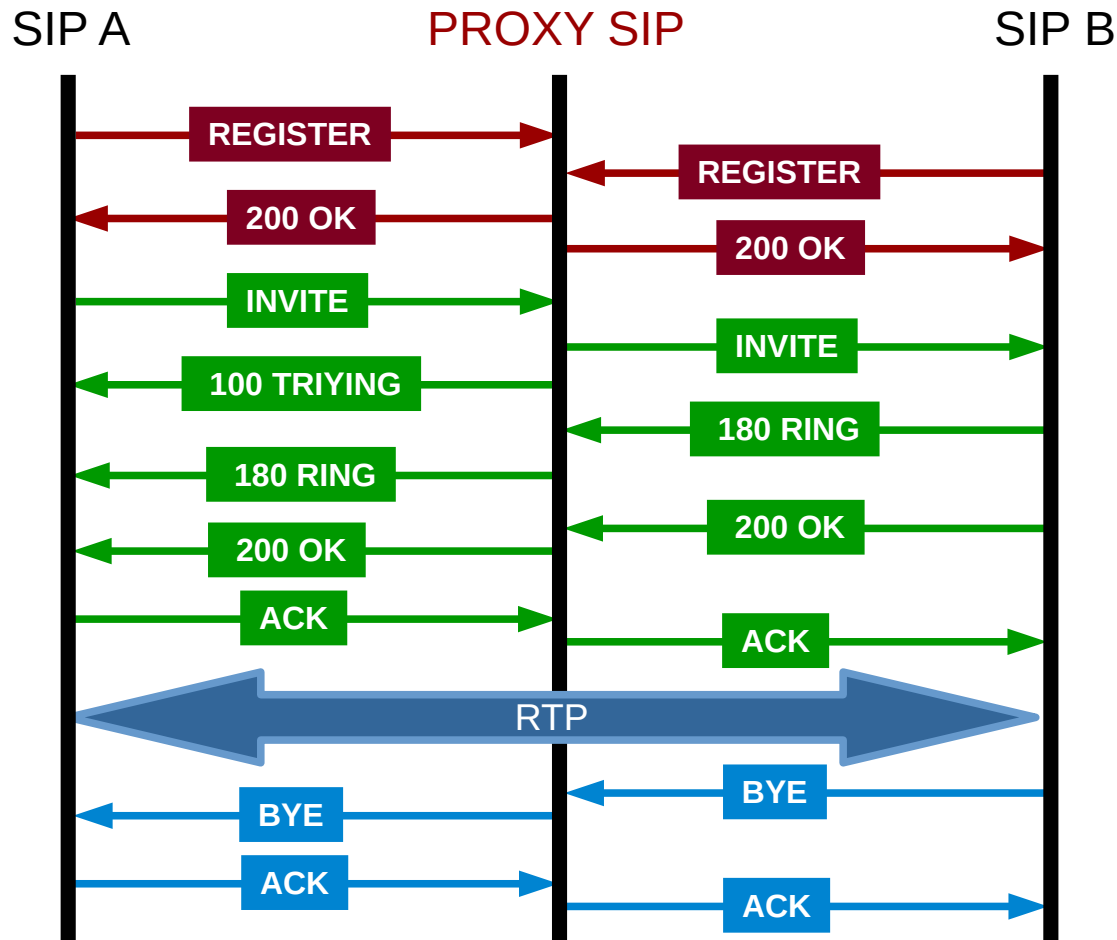
INFO, se usa para enviar información de señalización

UPDATE, permite actualizar características de una sesión

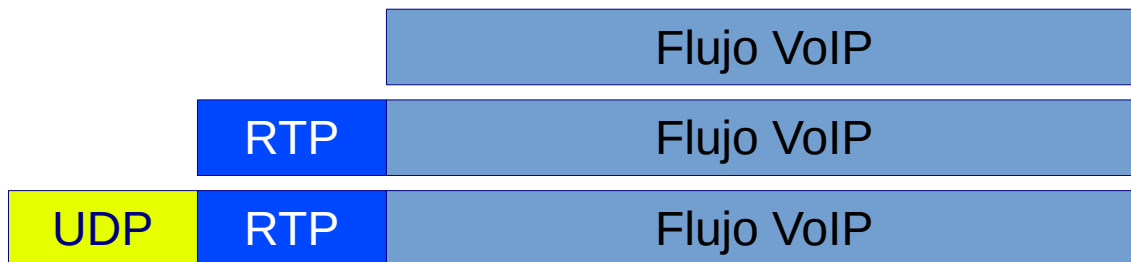
- Hay seis tipos de respuesta
 - 1xx → Provisional
 - 2xx → Aceptación
 - 3xx → Redirección
 - 4xx → Error de petición
 - 5xx → Error de servidor
 - 6xx → Fallos globales

- Los paquetes SIP contienen un protocolo de descripción de sesión (SDP) que es usado para proporcionar información sobre el flujo de voz en sesiones multimedia.
 - Dueño o iniciador de la sesión
 - Nombre de la sesión (si la hubiera)
 - Información de conexión (IP)
 - Ancho de banda estimado
 - Datos de la media usados por RTP
 - Atributos de sesión (codec ofrecido, generalmente G.711)

- Flujo de una llamada SIP



- RTP es el protocolo utilizado para transportar tráfico en tiempo real
 - Es independiente del protocolo de transporte
 - No reserva recursos en la red
- RTP, va acompañado de un protocolo que asegura el tráfico de control



- La cabecera RTP tiene el siguiente formato

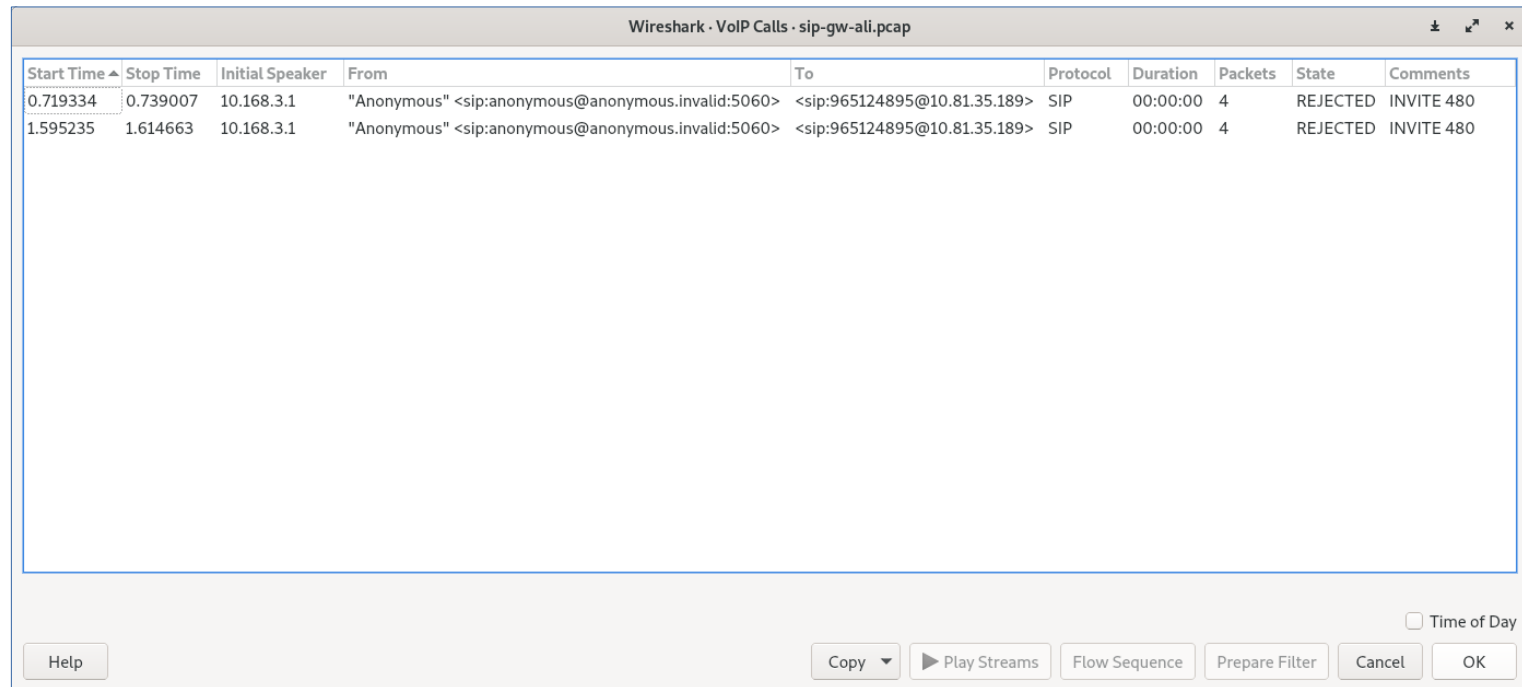


Longitud 32 bits

- RTCP, se encarga del control de los paquetes RTP y el control de la sesión

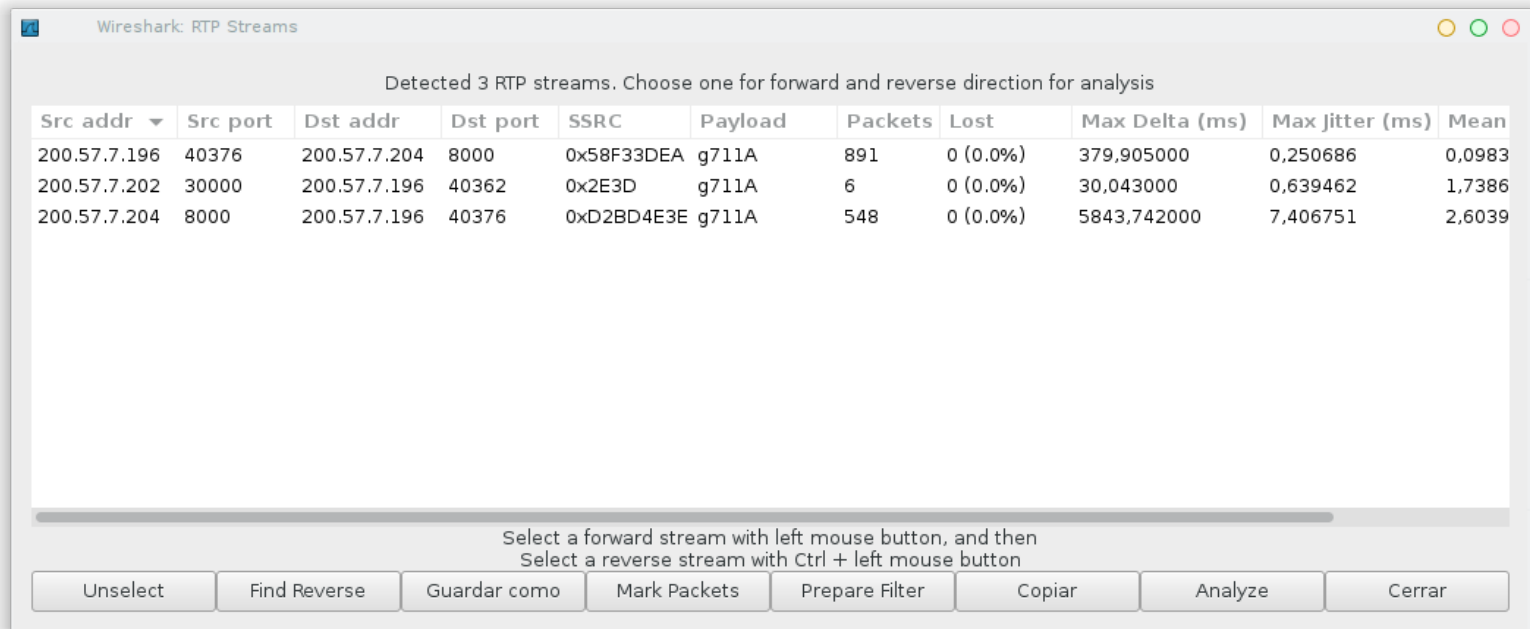
- Desde Wireshark en el menú Telephony nos encontramos con
 - VoIP Calls
 - RTP
 - RTSP
 - Sip Flows
 - Sip Statistics

- Para ver como fueron las llamadas capturadas
- Telephony → VoIP Calls

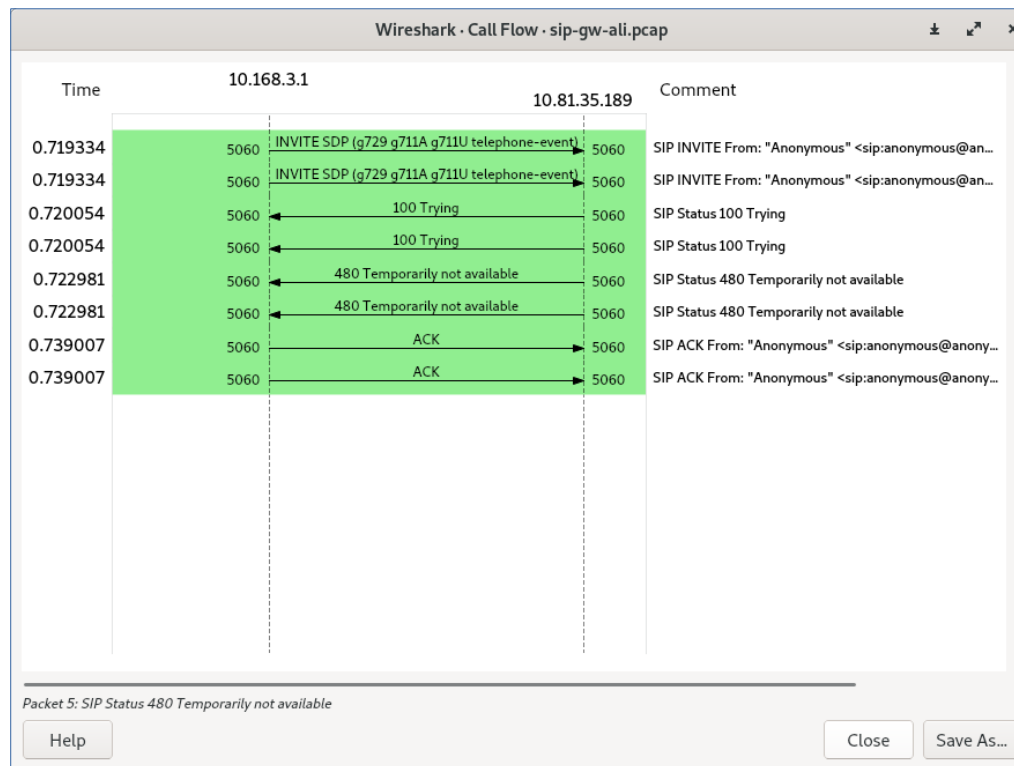


Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.719334	0.739007	10.168.3.1	"Anonymous" <sip:anonymous@anonymous.invalid:5060>	<sip:965124895@10.81.35.189>	SIP	00:00:00	4	REJECTED	INVITE 480
1.595235	1.614663	10.168.3.1	"Anonymous" <sip:anonymous@anonymous.invalid:5060>	<sip:965124895@10.81.35.189>	SIP	00:00:00	4	REJECTED	INVITE 480

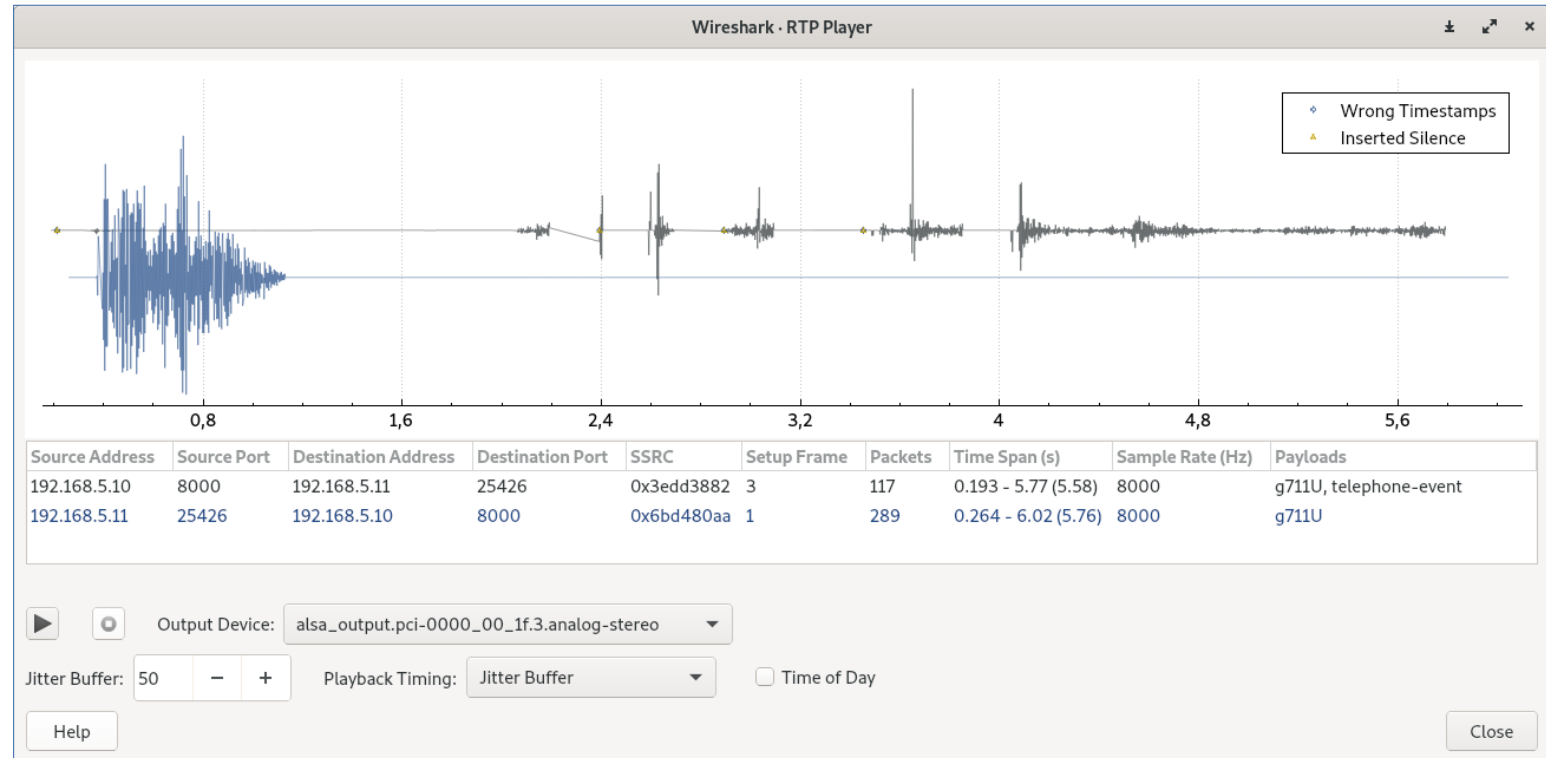
- Si queremos ver información sobre los flujos capturados
- RTP → Show all stream



- Seleccionando una llamada y pulsando “Flow”, vemos la sesión SIP.

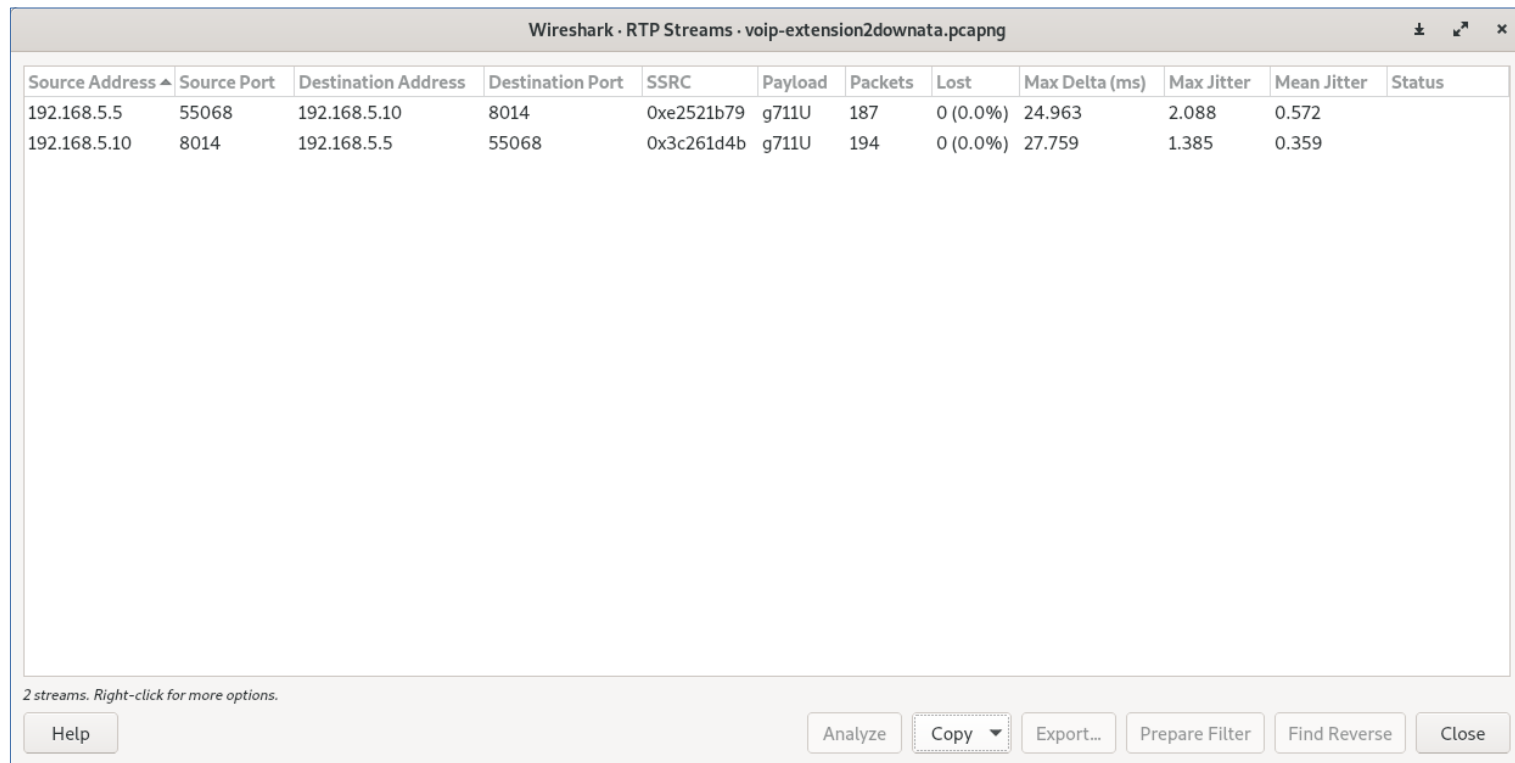


- Seleccionando un flujo, podemos escuchar la conversación, siempre que dispongamos del codec adecuado.



- Podemos construir un filtro, seleccionando la conversación y pulsado el botón **Prepare Filter**

- Con **RTP Stream**, podemos ver estadísticas sobre los parámetros de la media



Wireshark · RTP Streams · voip-extension2downata.pcapng

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
192.168.5.5	55068	192.168.5.10	8014	0xe2521b79	g711U	187	0 (0.0%)	24.963	2.088	0.572	
192.168.5.10	8014	192.168.5.5	55068	0x3c261d4b	g711U	194	0 (0.0%)	27.759	1.385	0.359	

2 streams. Right-click for more options.

Help Analyze Copy Export... Prepare Filter Find Reverse Close

- Analizando un flujo, obtenemos estadísticas, para ambos sentidos
 - Paquete
 - Numero de secuencias RTP
 - Delta time
 - Jitter
 - Skew
 - Consumo de ancho de banda
 - Status

Voz sobre IP

Wireshark

1.1

Wireshark · RTP Stream Analysis · voip-extension2downata.pcapng

192.168.5.5:55068 ↔
192.168.5.10:8014

Forward

SSRC 0xe2521b79
Max Delta 24.96 ms @ 368
Max Jitter 2.09 ms
Mean Jitter 0.57 ms
Max Skew -3.90 ms
RTP Packets 187
Expected 187
Lost 0 (0.00 %)
Seq Errs 0
Start at 21.734731 s @ 26
Duration 3.72 s
Clock Drift -2472 ms
Freq Drift 2690 Hz (-66.38 %)

Reverse

SSRC 0x3c261d4b
Max Delta 27.76 ms @ 66
Max Jitter 1.38 ms
Mean Jitter 0.36 ms
Max Skew 18.35 ms
RTP Packets 194
Expected 194
Lost 0 (0.00 %)
Seq Errs 0
Start at 21.682114 s @ 22
Duration 3.85 s
Clock Drift -2468 ms
Freq Drift 2872 Hz (-64.10 %)

Forward to reverse
start diff -0.052617 s @ -4

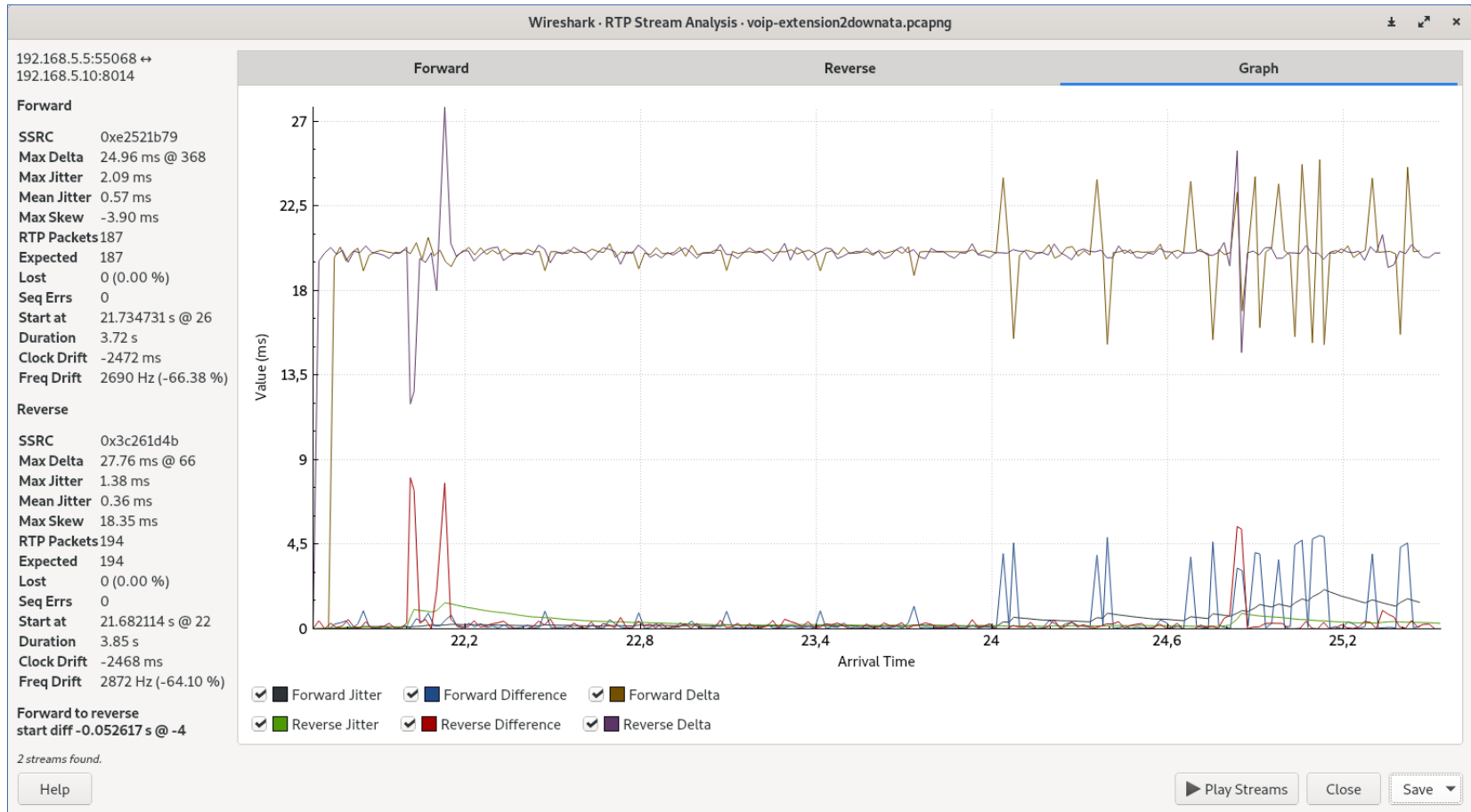
2 streams found.

Help

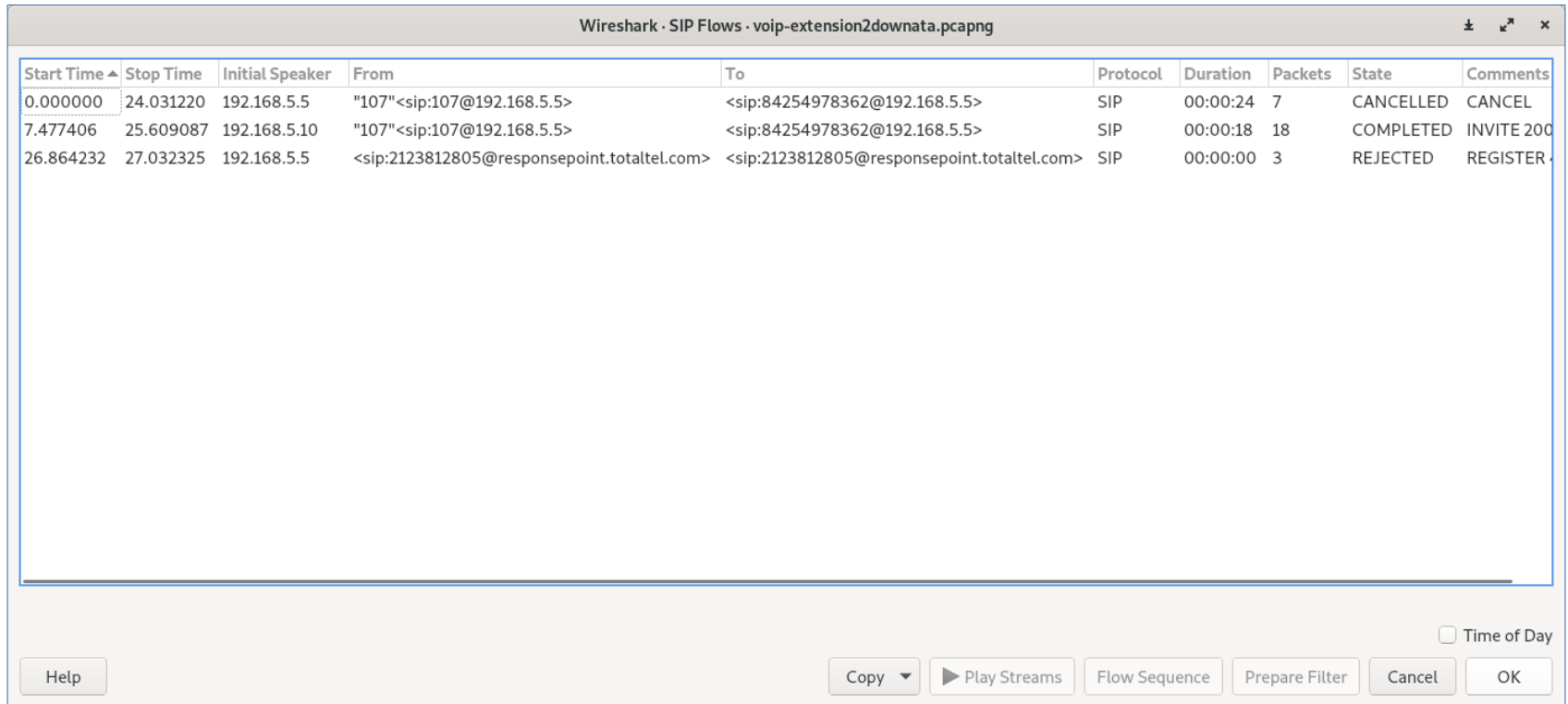
Play Streams Close Save

Forward				Reverse				Graph
Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status	
26	63	0.00	0.00	0.00	1.60		✓	
28	64	19.75	0.02	0.25	3.20		✓	
30	65	20.31	0.03	-0.07	4.80		✓	
32	66	19.58	0.06	0.35	6.40		✓	
34	67	20.03	0.06	0.33	8.00		✓	
36	68	20.25	0.07	0.07	9.60		✓	
38	69	19.05	0.12	1.03	11.20		✓	
40	70	19.88	0.12	1.14	12.80		✓	
42	71	20.05	0.12	1.10	14.40		✓	
44	72	20.14	0.12	0.95	16.00		✓	
46	73	20.06	0.12	0.90	17.60		✓	
48	74	20.00	0.11	0.90	19.20		✓	
50	75	19.97	0.10	0.93	20.80		✓	
52	76	20.18	0.11	0.75	22.40		✓	
55	77	19.96	0.10	0.79	24.00		✓	
57	78	20.54	0.13	0.25	25.60		✓	
59	79	19.65	0.15	0.60	27.20		✓	
61	80	20.83	0.19	-0.22	28.80		✓	
63	81	19.83	0.19	-0.05	30.40		✓	
65	82	20.15	0.18	-0.21	32.00		✓	
67	83	19.53	0.20	0.27	33.60		✓	
69	84	19.27	0.24	1.00	35.20		✓	
71	85	19.88	0.23	1.11	36.80		✓	
73	86	20.06	0.22	1.05	38.40		✓	
75	87	20.29	0.22	0.76	40.00		✓	
77	88	19.90	0.22	0.86	41.60		✓	

- También, obtenemos un gráfico donde podemos ver, en ambos sentidos
 - Jitter
 - skew
 - Delta time
- Podemos exportar
 - Valores estadísticos
 - Audio
 - Gráfico



- Con **SIP Flow**, obtenemos listado de todos los flujos, completados o no

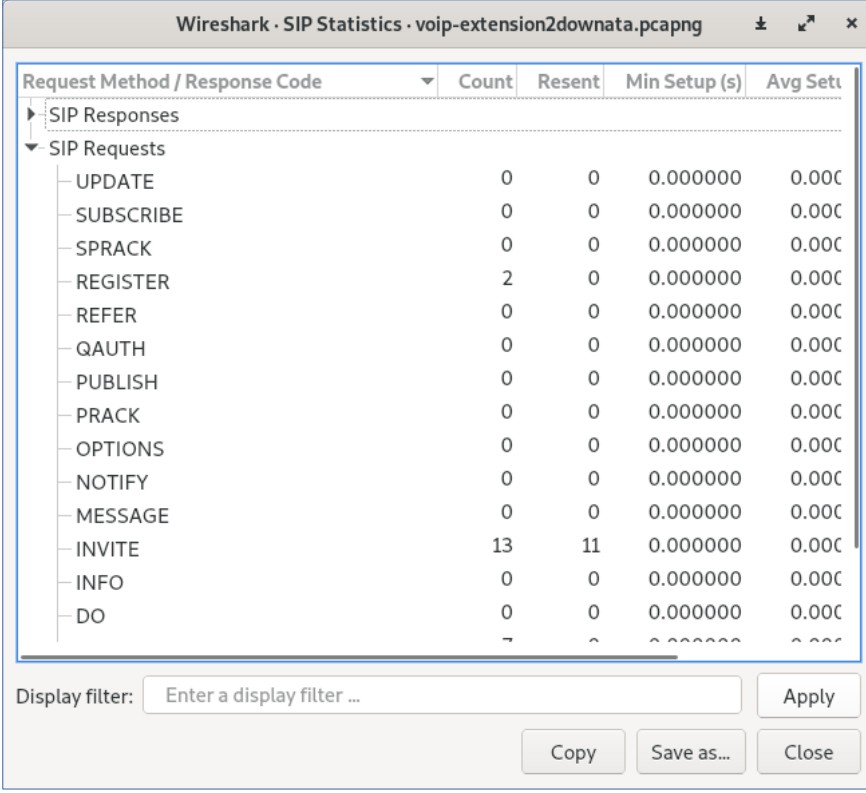


Wireshark · SIP Flows · voip-extension2downata.pcapng

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.000000	24.031220	192.168.5.5	"107"<sip:107@192.168.5.5>	<sip:84254978362@192.168.5.5>	SIP	00:00:24	7	CANCELLED	CANCEL
7.477406	25.609087	192.168.5.10	"107"<sip:107@192.168.5.5>	<sip:84254978362@192.168.5.5>	SIP	00:00:18	18	COMPLETED	INVITE 200
26.864232	27.032325	192.168.5.5	<sip:2123812805@responsepoint.totaltel.com>	<sip:2123812805@responsepoint.totaltel.com>	SIP	00:00:00	3	REJECTED	REGISTER

Help Copy Play Streams Flow Sequence Prepare Filter Cancel OK ☐ Time of Day

- Podemos obtener estadísticas de los mensaje con **SIP Statistics**

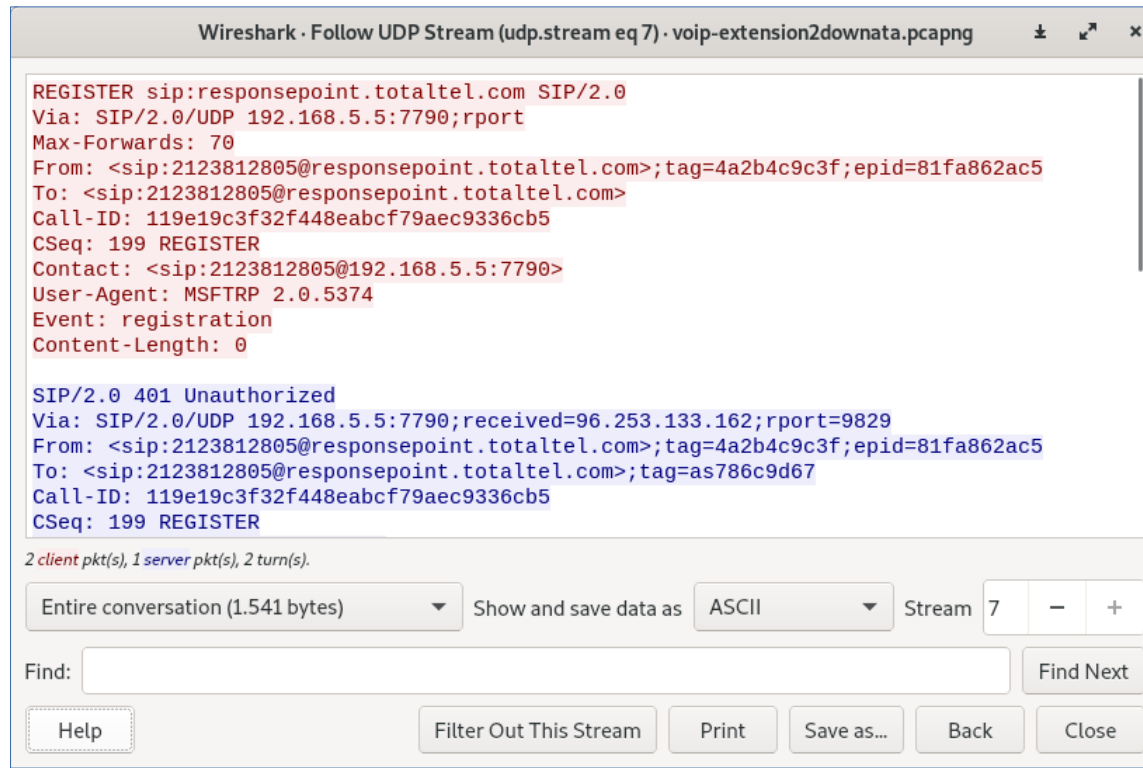


Wireshark · SIP Statistics · voip-extension2downata.pcapng

Request Method / Response Code	Count	Resent	Min Setup (s)	Avg Setu
SIP Responses				
SIP Requests				
UPDATE	0	0	0.000000	0.000000
SUBSCRIBE	0	0	0.000000	0.000000
SPRACK	0	0	0.000000	0.000000
REGISTER	2	0	0.000000	0.000000
REFER	0	0	0.000000	0.000000
QAUTH	0	0	0.000000	0.000000
PUBLISH	0	0	0.000000	0.000000
PRACK	0	0	0.000000	0.000000
OPTIONS	0	0	0.000000	0.000000
NOTIFY	0	0	0.000000	0.000000
MESSAGE	0	0	0.000000	0.000000
INVITE	13	11	0.000000	0.000000
INFO	0	0	0.000000	0.000000
DO	0	0	0.000000	0.000000

Display filter:

- También podemos ver toda la sesión SIP desde **Analyze → Flow UDP Stream**



Voz IP

Laboratorio 1

Archivo: **DNS lento**

- Analizar el contenido del archivo y observar los posibles errores en el servicio DNS.

Archivo: **DNS error de servidor**

- Observar la respuesta cuando se presenta un error

Voz IP

Laboratorio 1

Crear un perfil específico para el análisis de tráfico VoIP

- Reglas de coloreado
- Detección de errores de señalización.
- Añadir una columna para diferenciar la calidad de servicio
- Establecer una columna para el Timestamp

Telefónica

BE MORE 