

*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

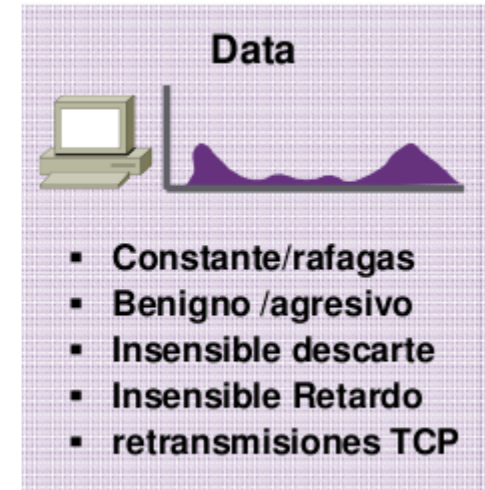
- El jitter, es la variación en el retraso, para ello se inserta un buffer de recepción, el cual agrega otro retraso al retraso total.
- El excesivo jitter puede ser causado por congestión en la red, configuraciones de QoS o enlace con poco ancho de banda.

- 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

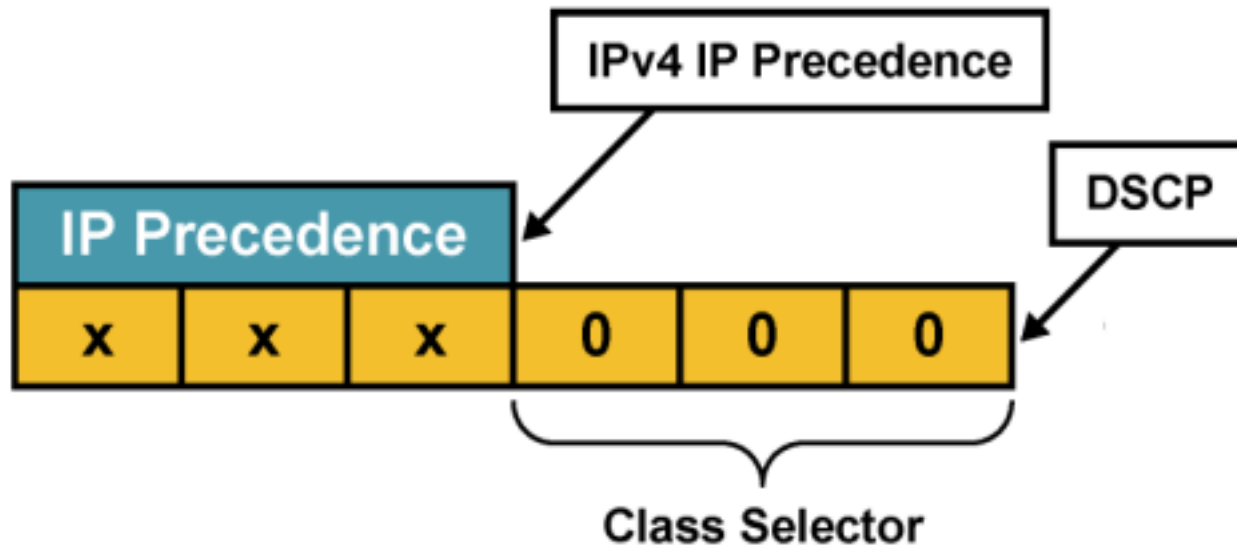


- Para mejorar el rendimiento de un enlace, se usan técnicas como
  - Supresión de silencios y detección de voz
  - Compresión de cabeceras
- Utilizando priorización, podemos aplicar calidad de servicio.

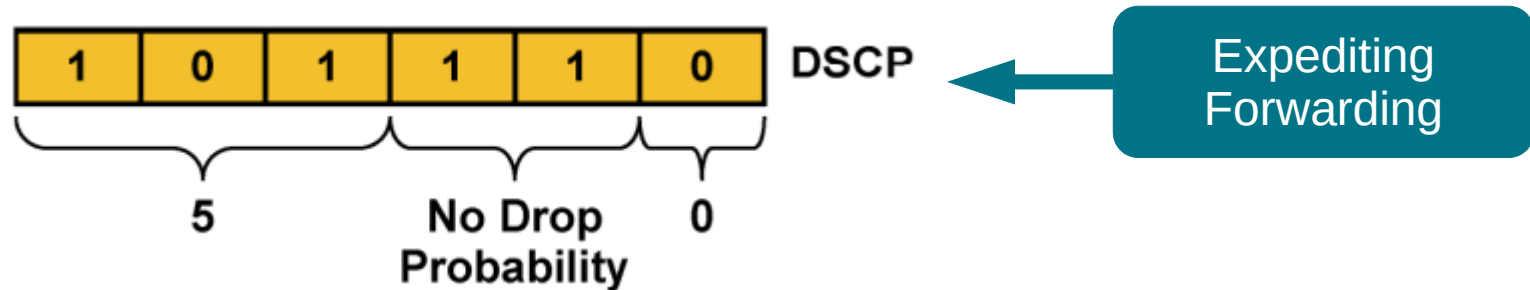
- Perfiles de tráfico



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

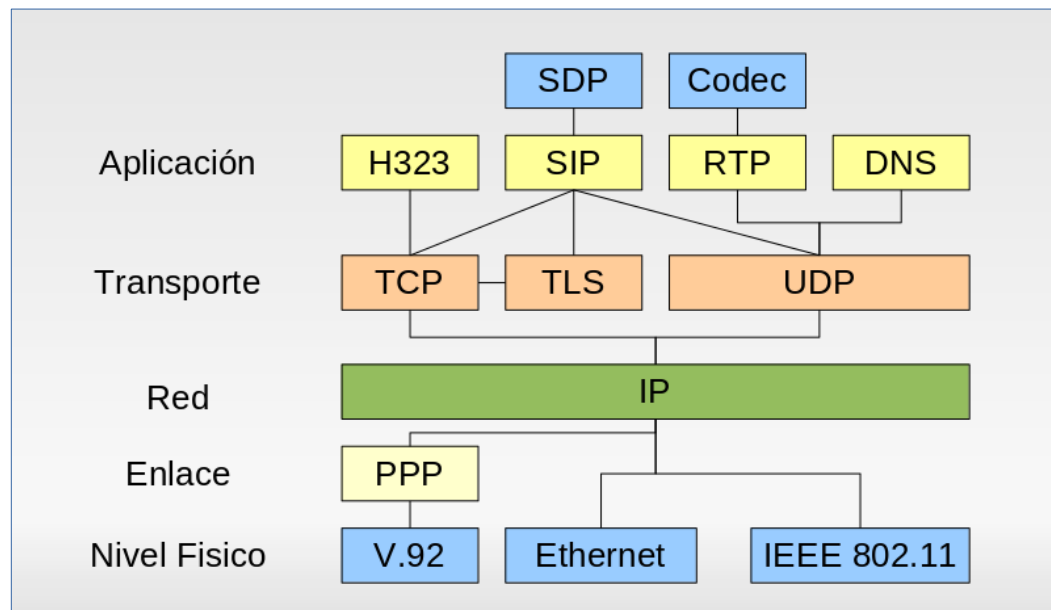


- Los DSCP se dividen en
  - Best Effort (por defecto)
  - Assured Forwarding (reenvío asegurado)
  - Expediting Forwarding (reenvío expedito)

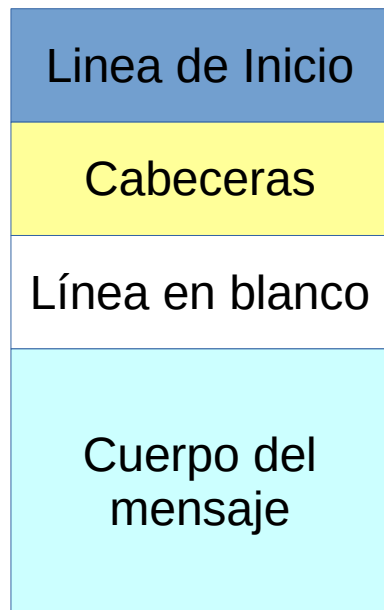


- SIP es un protocolo basado en texto que nos permite
  - Localización del usuario
  - Gestión de la capacidad y disponibilidad del usuario
  - Gestionar los parámetros durante el establecimiento de la llamada
  - Puede establecer, modificar y finalizar, sesiones multimedia

- SIP, debe usarse junto a otros protocolos, para proporcionar servicios completos, de forma que construye una arquitectura multimedia



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



### MÉTODOS

**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

- La solicitud SIP, contiene un nombre de método, un URI de solicitud y la versión del protocolo

Request-Line: INVITE sip:16543@192.168.10.11 SIP/2.0



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

Status-Line: SIP/2.0 100 Trying

- Campos de cabecera, consta de un nombre de campo, seguido de dos puntos y el valor del campo

```
▼ Message Header
  ▶ Via: SIP/2.0/UDP 192.168.5.10:5060;rport;branch=z9hG4bK8c66661
  ▶ From: "John Haller"<sip:201@192.168.5.11>;tag=45dda1fd
  ▶ To: "Auto Attendant"<sip:0@192.168.5.11>;tag=cdac5f5f0b
  - Call-ID: 673b0437-dc3f99dd-699f99a7-92fd8066@192.168.5.10
  - [Generated Call-ID: 673b0437-dc3f99dd-699f99a7-92fd8066@192.168.5.10]
  ▶ CSeq: 33155 INVITE
  - User-Agent: MSFTRP 2.0
  - Content-Length: 0
```

- 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)

- El protocolo SDP, viene en el cuerpo del mensaje

```
▼ Message Body
  ▼ Session Description Protocol
    - Session Description Protocol Version (v): 0
    ▶ Owner/Creator, Session Id (o): ipr1E680EB66B 4684162 4684162 IN IP4 192.168.5.10
    - Session Name (s): -
    ▶ Connection Information (c): IN IP4 192.168.5.10
    ▶ Time Description, active time (t): 0 0
    ▶ Media Description, name and address (m): audio 8000 RTP/AVP 18 0 8 101
    ▶ Media Attribute (a): rtpmap:18 G729/8000
    ▶ Media Attribute (a): rtpmap:0 PCMU/8000
    ▶ Media Attribute (a): rtpmap:8 PCMA/8000
    ▶ Media Attribute (a): rtpmap:101 telephone-event/8000
    ▶ Media Attribute (a):ptime:20
    ▶ Media Attribute (a):fmtp:101 0-16
    - [Generated Call-ID: f49fa0af-e84c7379-6649d13e-60bbc1c9@192.168.5.10]
```

- Si un usuario desea iniciar una conversación, debe consultar a un servidor proxy, la localización de ese usuario, que previamente se ha de registrar.

- El registro, implica enviar una solicitud REGISTER a un servidor (UAS)

### ▼ Session Initiation Protocol (REGISTER)

▶ Request-Line: REGISTER sip:porcelanosan1 SIP/2.0

#### ▼ Message Header

▶ Via: SIP/2.0/UDP 10.3.12.2:5060;branch=z9hG4bK8b1a45bc55f625d8d71b1a8f39cd4fa;rport

▶ From: "166501" <sip:166501@porcelanosan1>;tag=3393978879

▶ To: "166501" <sip:166501@porcelanosan1>

— Call-ID: 1637712510@10\_3\_12\_2

— [Generated Call-ID: 1637712510@10\_3\_12\_2]

▶ CSeq: 702 REGISTER

▶ Contact: <sip:166501@10.3.12.2:5060>

— Max-Forwards: 70

— User-Agent: C530 IP/42.231.00.000.000

— Expires: 1800

— Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO, SUBSCRIBE, NOTIFY, REFER

— Content-Length: 0

- El método SIP OPTIONS, permite consultar, tanto a un usuario como a un proxy, sus capacidades

```
▼ Session Initiation Protocol (OPTIONS)
  ▼ Request-Line: OPTIONS sip:192.168.5.2:5060 SIP/2.0
    |
    |─ Method: OPTIONS
    |
    |─ Request-URI: sip:192.168.5.2:5060
    |
    |─ [Resent Packet: False]
    |
  ▼ Message Header
    |
    |─ Via: SIP/2.0/UDP 213.0.49.3:5060;branch=z9hG4bK4ro3th203on56tv6c5f0
    |
    |─ Call-ID: df8e64f9707fc07294c3c62ebbae7795000qth0400@213.0.49.3
    |
    |─ [Generated Call-ID: df8e64f9707fc07294c3c62ebbae7795000qth0400@213.0.49.3]
    |
    |─ To: sip:ping@SA1461487001-2
    |
    |─ From: <sip:ping@213.0.49.3>;tag=e7920f70e332ea7c50fffd619761fedc000qth0
    |
    |─ Max-Forwards: 70
    |
    |─ CSeq: 56611 OPTIONS
    |
    |─ Route: <sip:192.168.5.2:5060;lr>
```

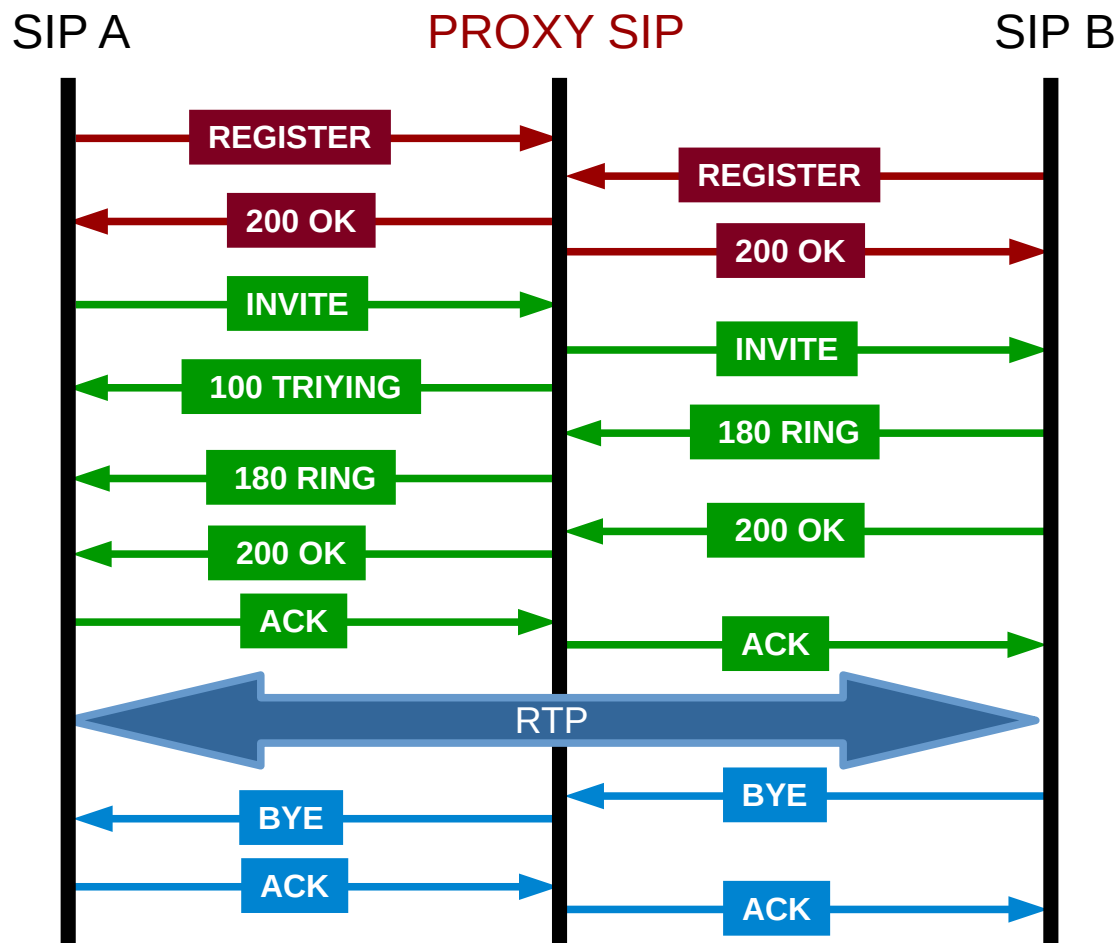
- Cuando un usuario desea iniciar una sesión, formula un INVITE, para establecer dicha sesión

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:964158170@10.81.33.236;transport=UDP SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 10.88.200.7:5060;branch=z9hG4bK2osaej1040722o7ovlj0sb12g0ml1.1
    To: "Teresa Mayayo" <sip:964158170@10.81.33.236;user=phone>;tag=4cd4bfa87f34196576a3203bc02e60b0
    From: <sip:977702507@10.88.200.7;user=phone>;tag=f6f18fd51f2e3eea70d9723aee4f08fa
    Call-ID: 370c82a25cfbba9550fdb4e867eb257b@10.81.33.236
    [Generated Call-ID: 370c82a25cfbba9550fdb4e867eb257b@10.81.33.236]
    CSeq: 1094738027 INVITE
    Max-Forwards: 67
    Content-Length: 319
    Contact: <sip:10.88.200.7:5060;transport=udp>
    Content-Type: application/sdp
    Allow: INVITE, ACK, BYE, CANCEL
    Supported: timer
    P-Asserted-Identity: <sip:977702507@10.250.64.22>
    Accept-Language: en;q=0.0
    Date: Thu, 25 Oct 2018 08:08:47 GMT
    P-Charging-Vector: icid-value=3f2fa03702ec2dff10d3b6ac8023ee5c;orig-voi=c010.f02.ims.telefonica.net
    Session-Expires: 900;refresher=uas
    Min-SE: 180
  Message Body
```



- Durante la sesión, se pueden modificar parámetros de la misma, se hace con una solicitud RE-INVITE
- Para terminar una sesión, se usa la solicitud BYE

- Flujo de una llamada SIP



- SIP, proporciona un mecanismo de autenticación, basado en desafíos (Digest) y sin estado
- Es muy similar a HTTP Authenticate, y usa un código de respuesta 401, cuando el usuario no está autorizado
- En la cabecera, irán los campos.
  - Authorization
  - Proxy-Authorization

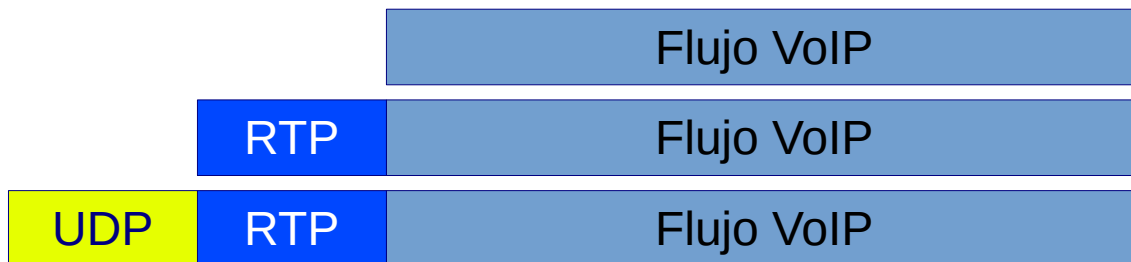
## • Autenticación Digest

```
▼ Session Initiation Protocol (401)
  ▼ Status-Line: SIP/2.0 401 Unauthorized
    ├── Status-Code: 401
    ├── [Resent Packet: False]
    ├── \[Request Frame: 314\]
    └── [Response Time (ms): 636]
  ▼ Message Header
    ├── ▶ Via: SIP/2.0/UDP 172.17.69.4:2054;branch=z9hG4bK-1774C674;rport
    ├── ▼ From: <sip:5801@10.17.1.93>;tag=2522882856
    │   ├── ▶ SIP from address: sip:5801@10.17.1.93
    │   └── SIP from tag: 2522882856
    ├── ▼ To: <sip:5801@10.17.1.93>;tag=1202256324
    │   ├── ▶ SIP to address: sip:5801@10.17.1.93
    │   └── SIP to tag: 1202256324
    ├── Date: Mon, 29 Jan 2018 11:28:36 GMT
    ├── Call-ID: 85fad34e00000001b5ae00013e1d2d64
    ├── [Generated Call-ID: 85fad34e00000001b5ae00013e1d2d64]
    ├── ▶ CSeq: 1000 REGISTER
    ├── ▼ WWW-Authenticate: Digest realm="ccmsipline", nonce="zvMekdf6Ee9dIGgh5N2z39pFr9ttSm/z", algorithm=MD5
    │   ├── Authentication Scheme: Digest
    │   ├── Realm: "ccmsipline"
    │   ├── Nonce Value: "zvMekdf6Ee9dIGgh5N2z39pFr9ttSm/z"
    │   └── Algorithm: MD5
    └── Content-Length: 0
```

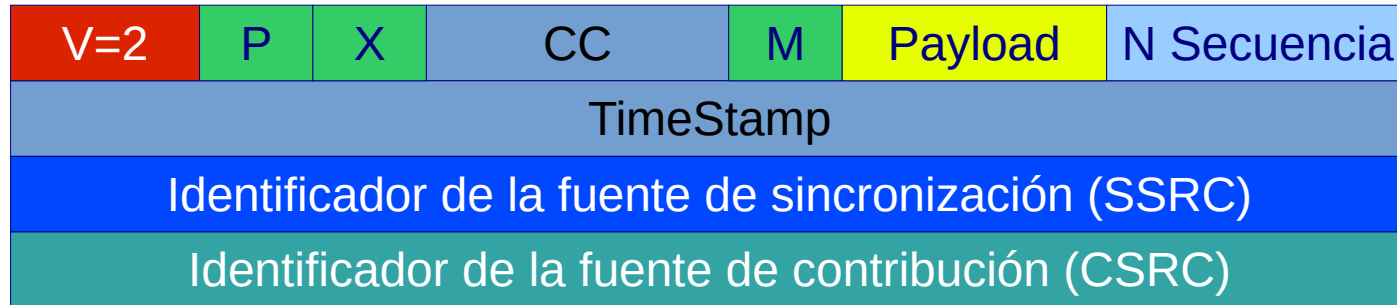
## • Autenticación Digest

Time	172.17.69.4	10.17.1.93	Comment
0.000000	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)
0.499789	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)
0.134596	2054	Status: 100 Trying	SIP: Status: 100 Trying
0.000870	2054	Status: 401 Unauthorized	SIP: Status: 401 Unauthorized
0.000008	2054	Status: 401 Unauthorized	SIP: Status: 401 Unauthorized
0.000920	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)
0.024583	2054	Status: 100 Trying	SIP: Status: 100 Trying
0.034748	2054	Status: 404 Not Found	SIP: Status: 404 Not Found
9.984671	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)
0.499624	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)
0.031078	2054	Status: 100 Trying	SIP: Status: 100 Trying
0.053241	2054	Status: 404 Not Found	SIP: Status: 404 Not Found
0.018365	2054	Status: 404 Not Found	SIP: Status: 404 Not Found
19.977673	2054	Request: REGISTER sip:10.17.1.93...	SIP: Request: REGISTER sip:10.17.1.93 (1 binding)

- 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

- La función principal de RTP, es implementar números de secuencia para reanudar la información de voz o vídeo, permite
  - Identificar el tipo de información transmitida
  - Agregar marcadores temporales y números de secuencia
  - Controlar la llegada de los paquetes a destino



- RTP no proporciona calidad de servicio, pero detecta:
  - Perdida de paquetes
  - Retardo variable en el transporte (Jitter)
  - Llegada de paquetes fuera de secuencia
  - Enrutamiento asimétrico

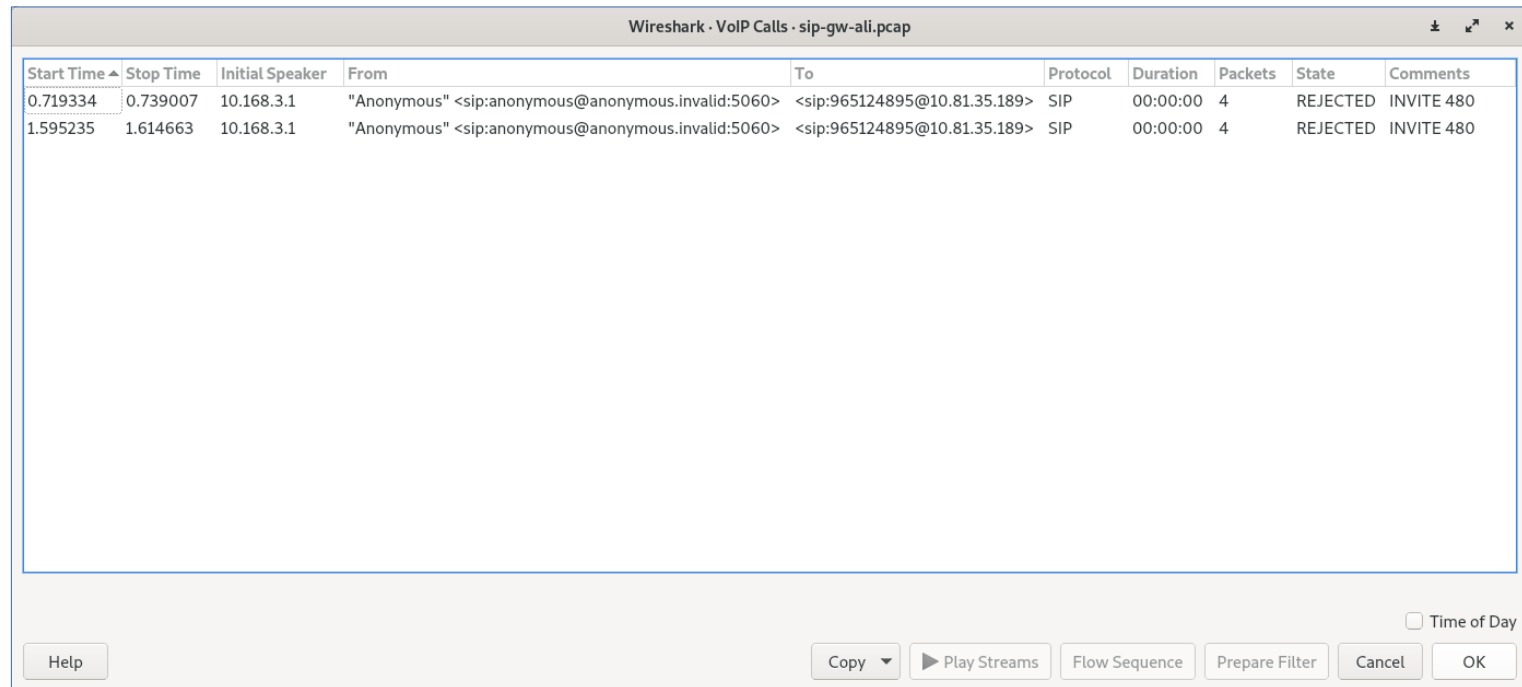
- Mensaje RTP

```
▼ Real-Time Transport Protocol
  ▶ [Stream setup by SDP (frame 3)]
    - 10.. .... = Version: RFC 1889 Version (2)
    - ..0. .... = Padding: False
    - ...0 .... = Extension: False
    - .... 0000 = Contributing source identifiers count: 0
    - 0... .... = Marker: False
    - Payload type: ITU-T G.711 PCMU (0)
    - Sequence number: 166
    - [Extended sequence number: 65702]
    - Timestamp: 3460791139
    - Synchronization Source identifier: 0x3edd3882 (1054685314)
    - Payload: ffffffffffffffffffffffffffffffffffffffffffffffff...
```

- 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



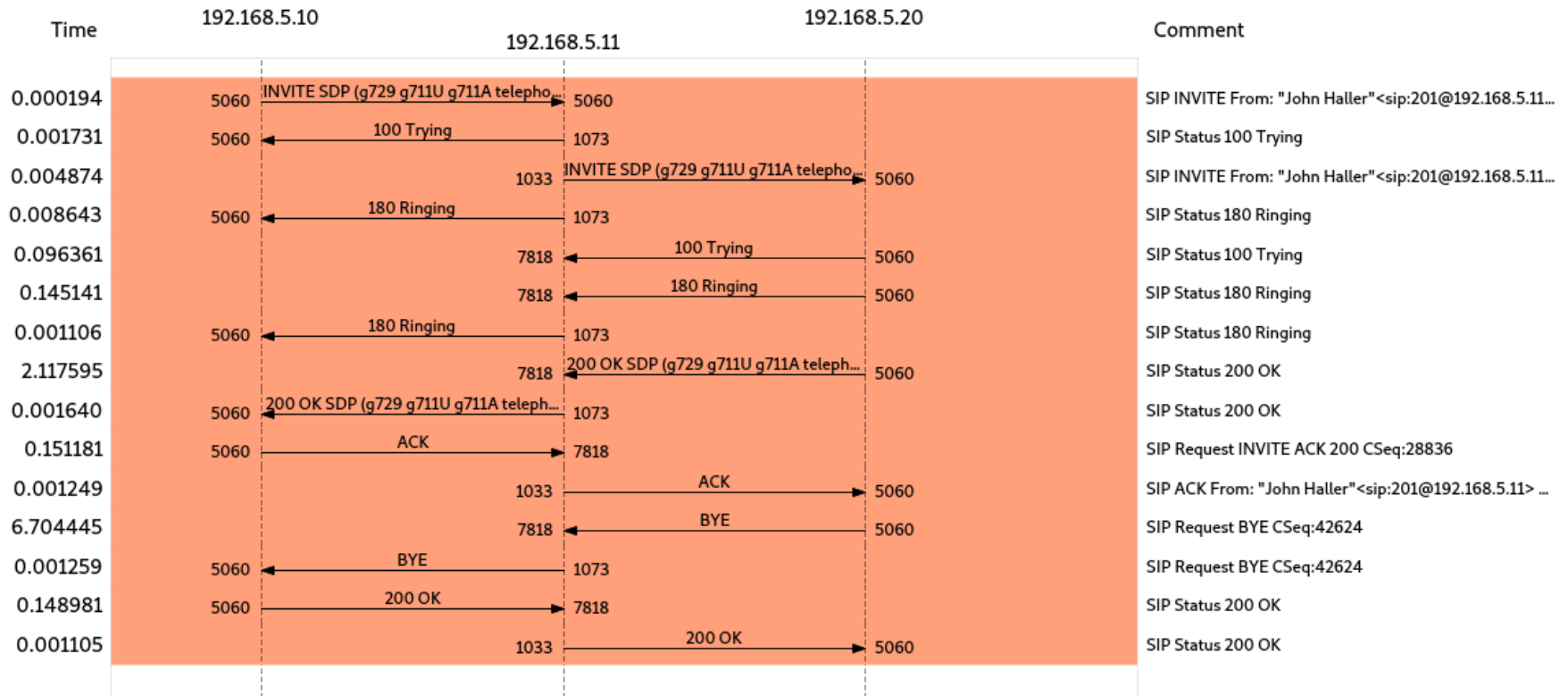
Wireshark · VoIP Calls · sip-gw-ali.pcap

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

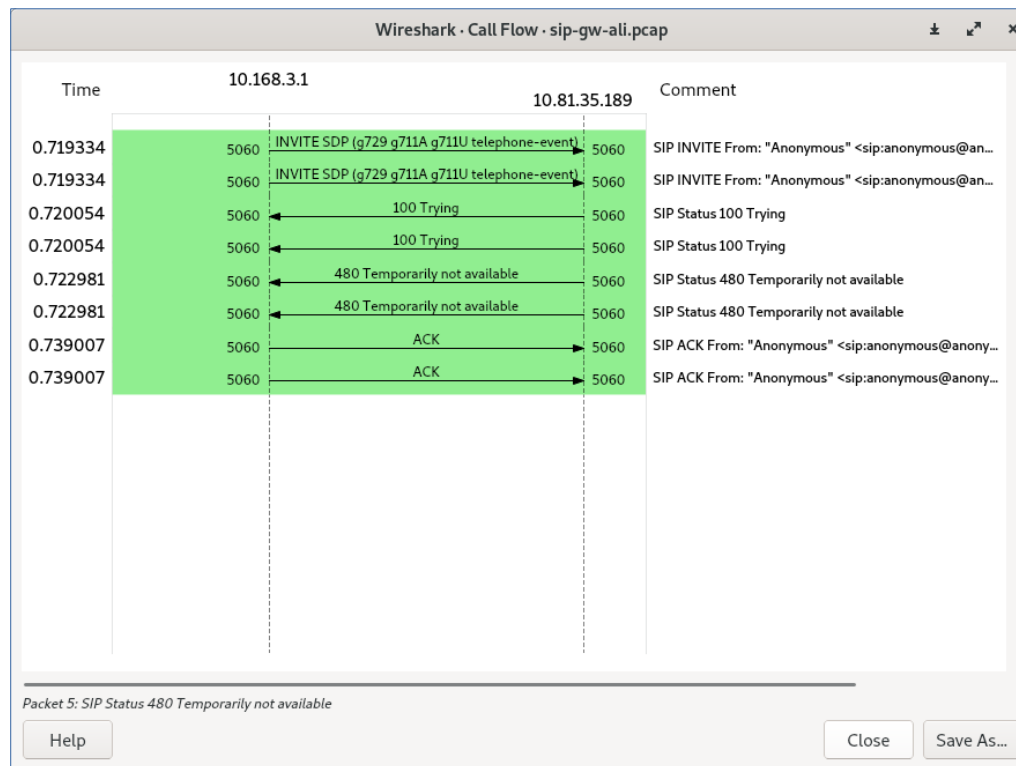
Help Copy Play Streams Flow Sequence Prepare Filter Cancel OK

☐ Time of Day

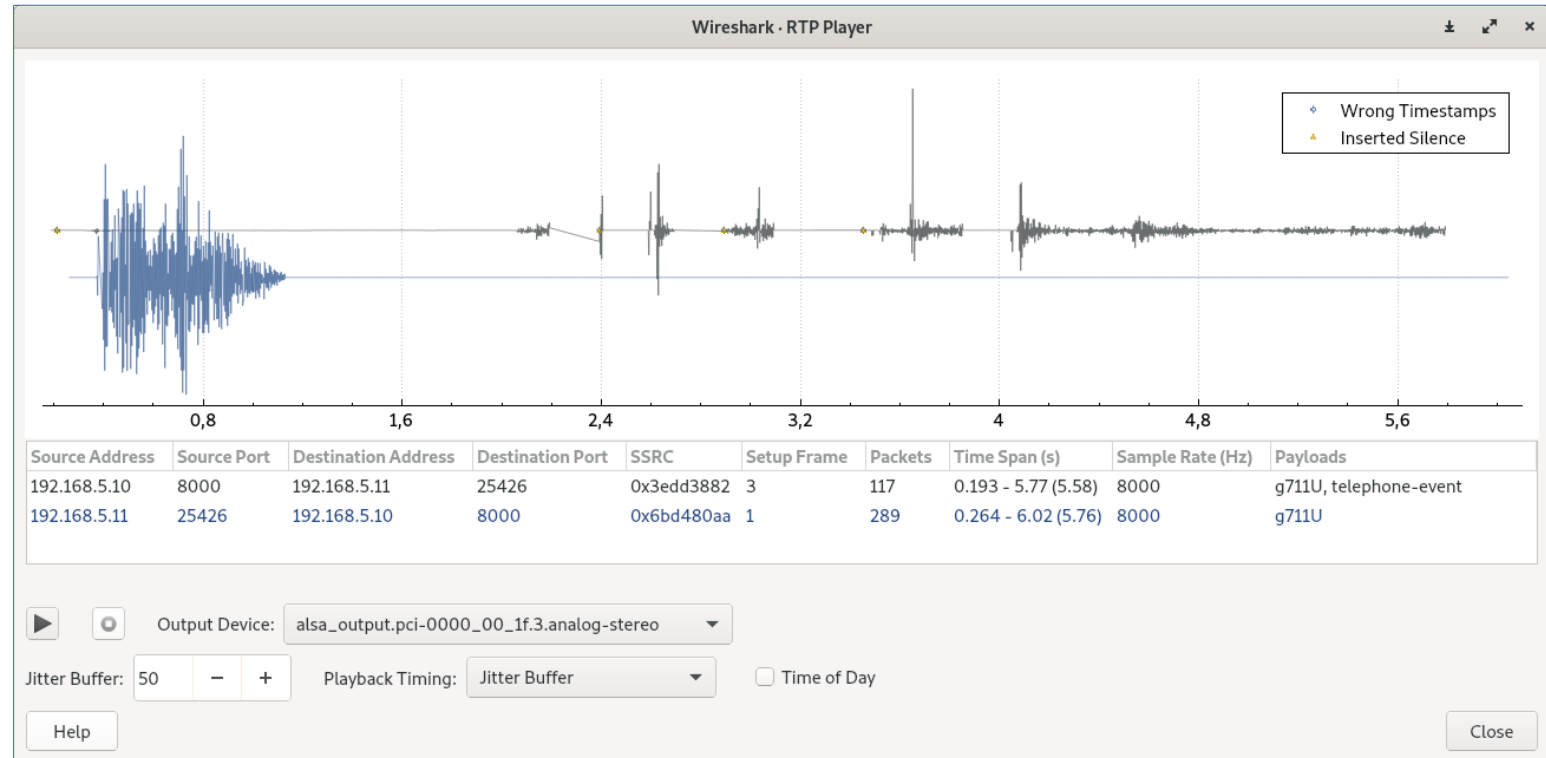
- Seleccionando una llamada y pulsando “Flow”, vemos la sesión SIP.



- Resultado de cuando no puede progresar una llamada



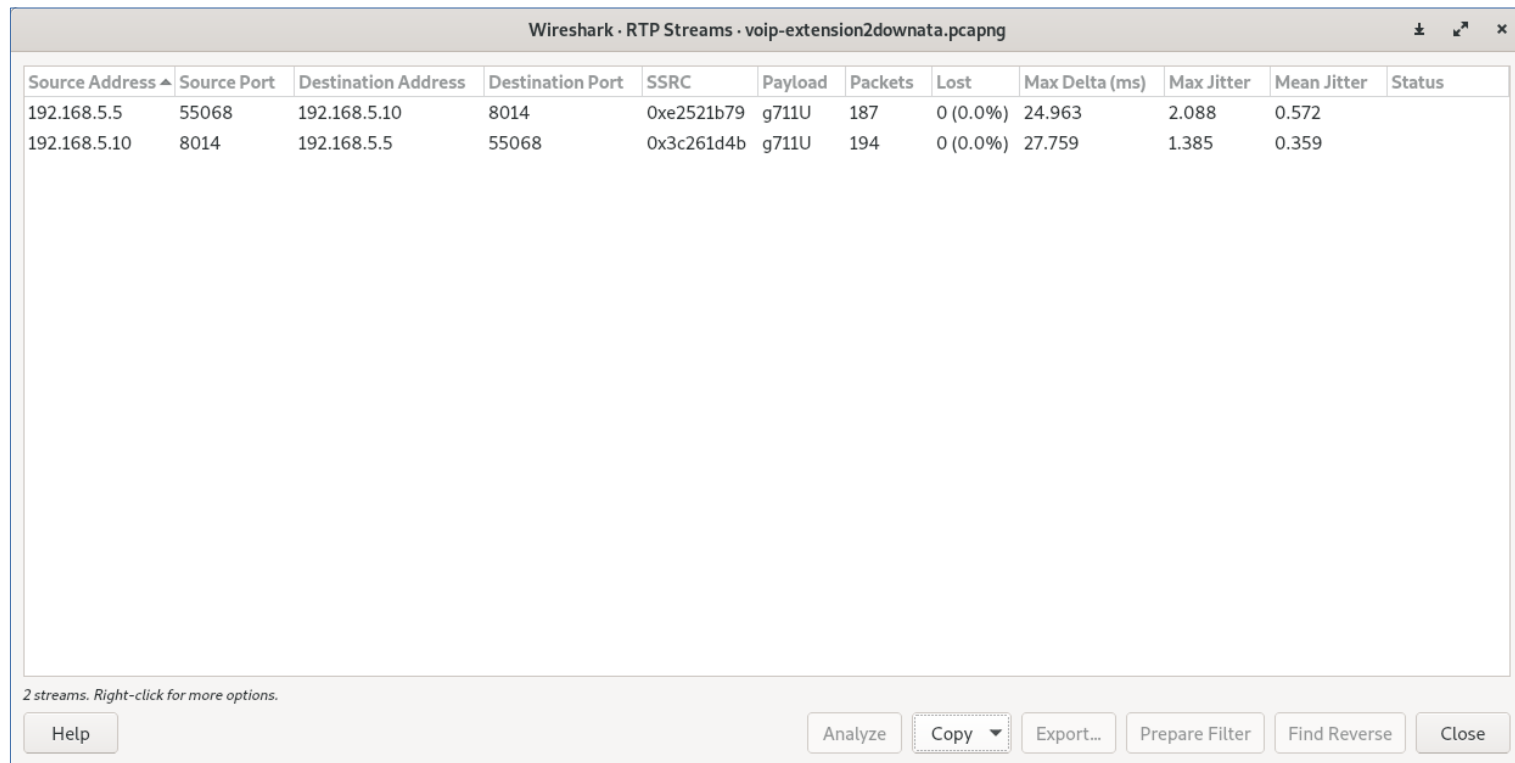
- Seleccionando un flujo, podemos escuchar la conversación, siempre que dispongamos del codec adecuado.





- 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

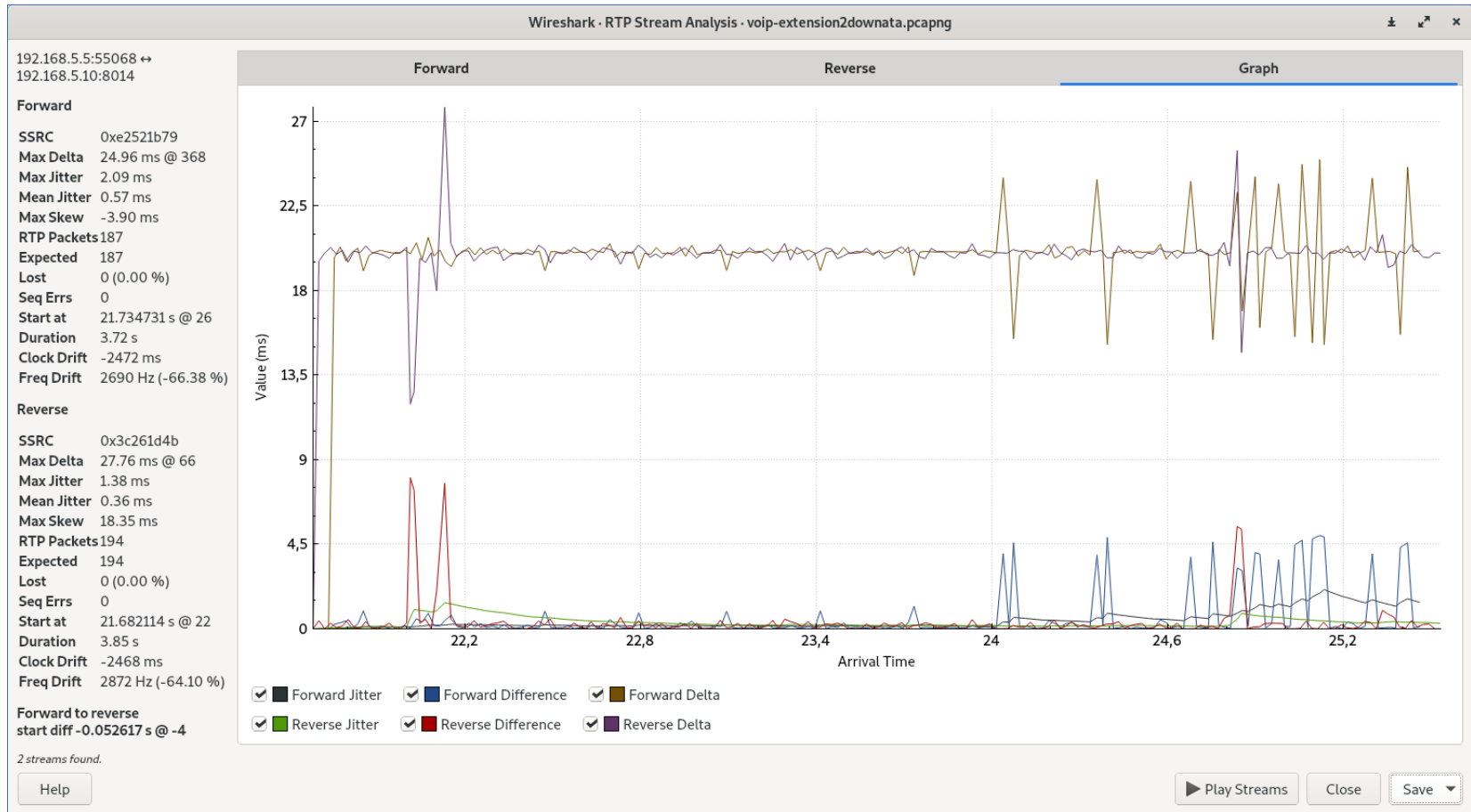
2 streams found.

Help

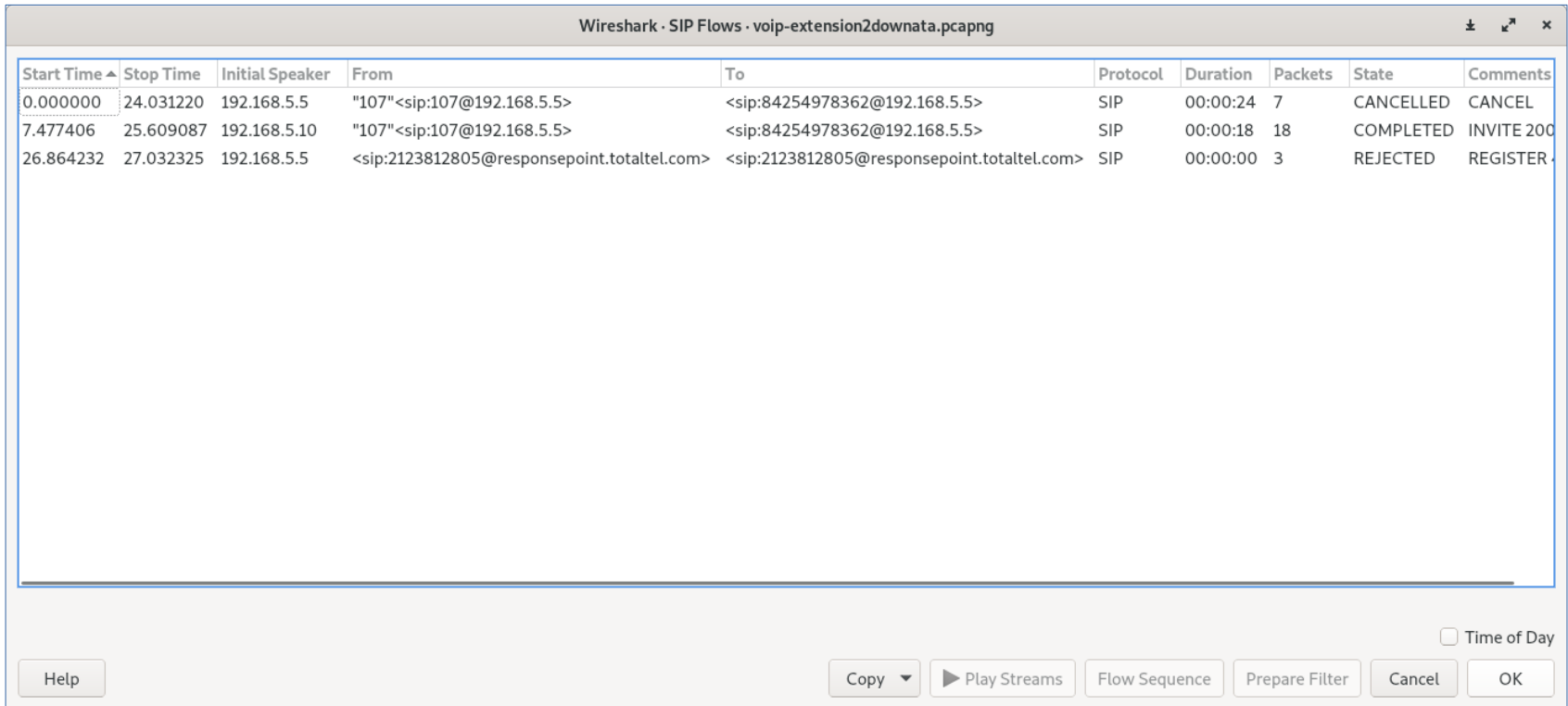
Play Streams Close Save

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

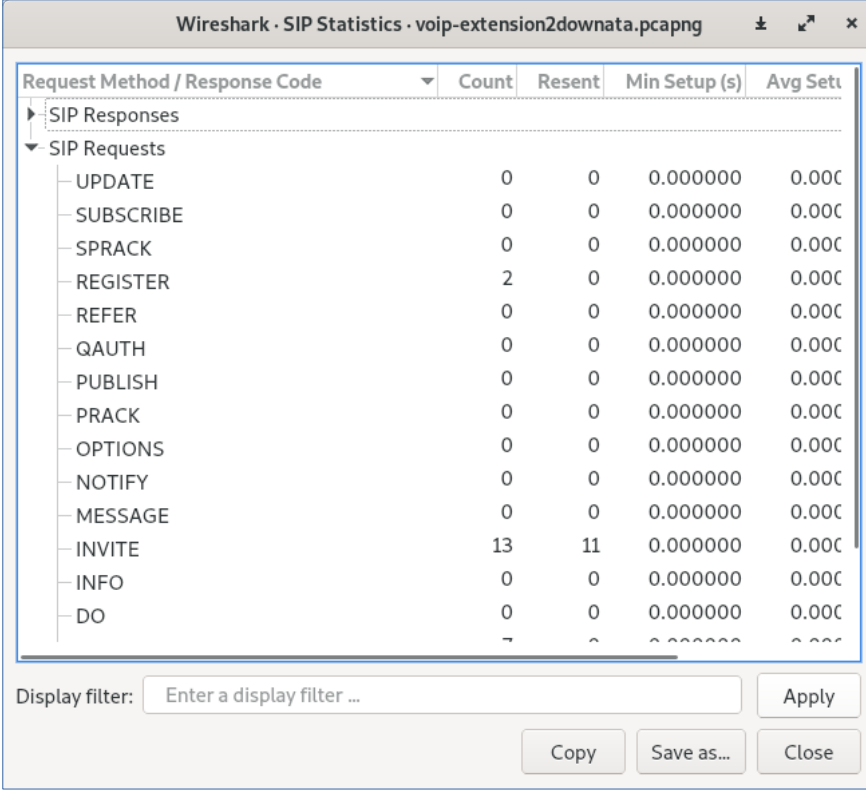


Wireshark · SIP Flows · voip-extension2downata.pcapng

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**



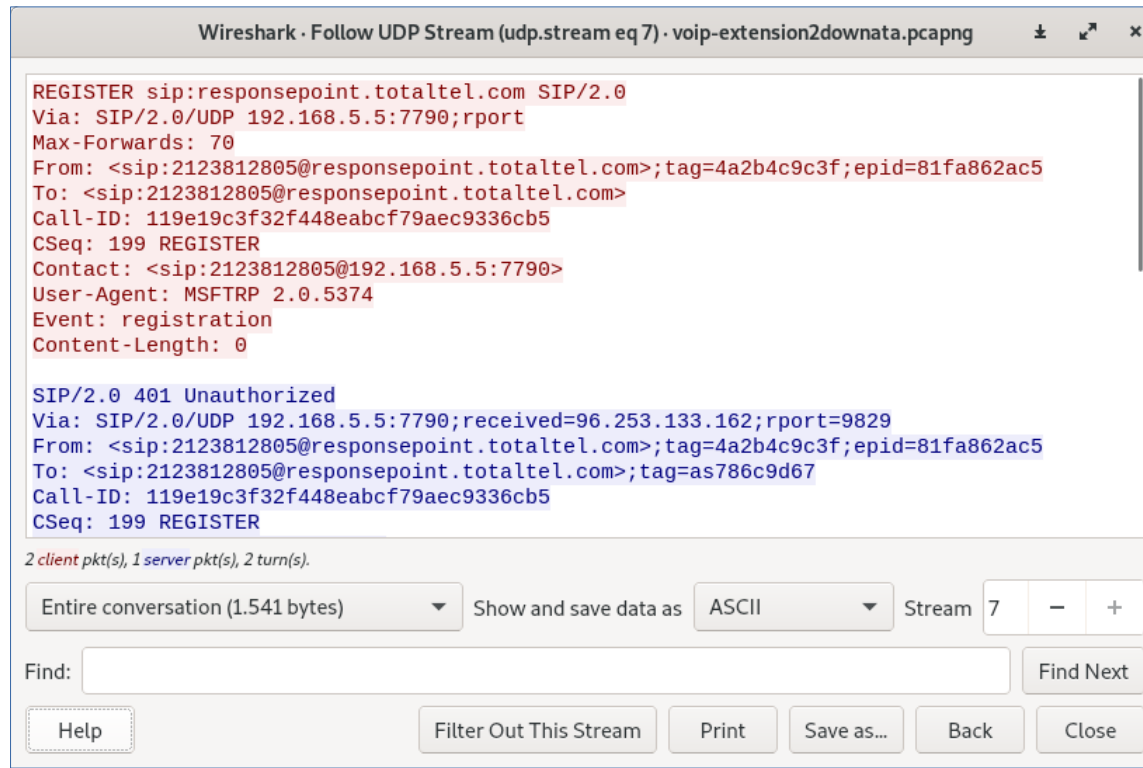
Wireshark · SIP Statistics · voip-extension2downata.pcapng

Request Method / Response Code	Count	Resent	Min Setup (s)	Avg Setu
SIP Responses				
SIP Requests				
UPDATE	0	0	0.000000	0.000
SUBSCRIBE	0	0	0.000000	0.000
SPRACK	0	0	0.000000	0.000
REGISTER	2	0	0.000000	0.000
REFER	0	0	0.000000	0.000
QAUTH	0	0	0.000000	0.000
PUBLISH	0	0	0.000000	0.000
PRACK	0	0	0.000000	0.000
OPTIONS	0	0	0.000000	0.000
NOTIFY	0	0	0.000000	0.000
MESSAGE	0	0	0.000000	0.000
INVITE	13	11	0.000000	0.000
INFO	0	0	0.000000	0.000
DO	0	0	0.000000	0.000

Display filter:



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



# Voz IP

## Laboratorio 1

Ver el mecanismo de una llamada VoIP y las estadísticas sobre dicha llamada.

Ver qué filtros podemos utilizar para buscar mensaje de llamada y códigos de error

Qué le pasa al segundo archivo

# 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** 