SharkFest'25 EUROPE

Troubleshooting VoIP | SIP- & RTP-Analysis with Wireshark

Benjamin Pfister

Troubleshooting VoIP | About Me

- Benjamin Pfister
- Head of Network & Telecommunication
- IT-Consultant / Trainer
- Freelance Author
- Father of BabyShark

Troubleshooting VoIP | Session Content

- Overview
- Protocol Basics
- Challenges
- Troubleshooting

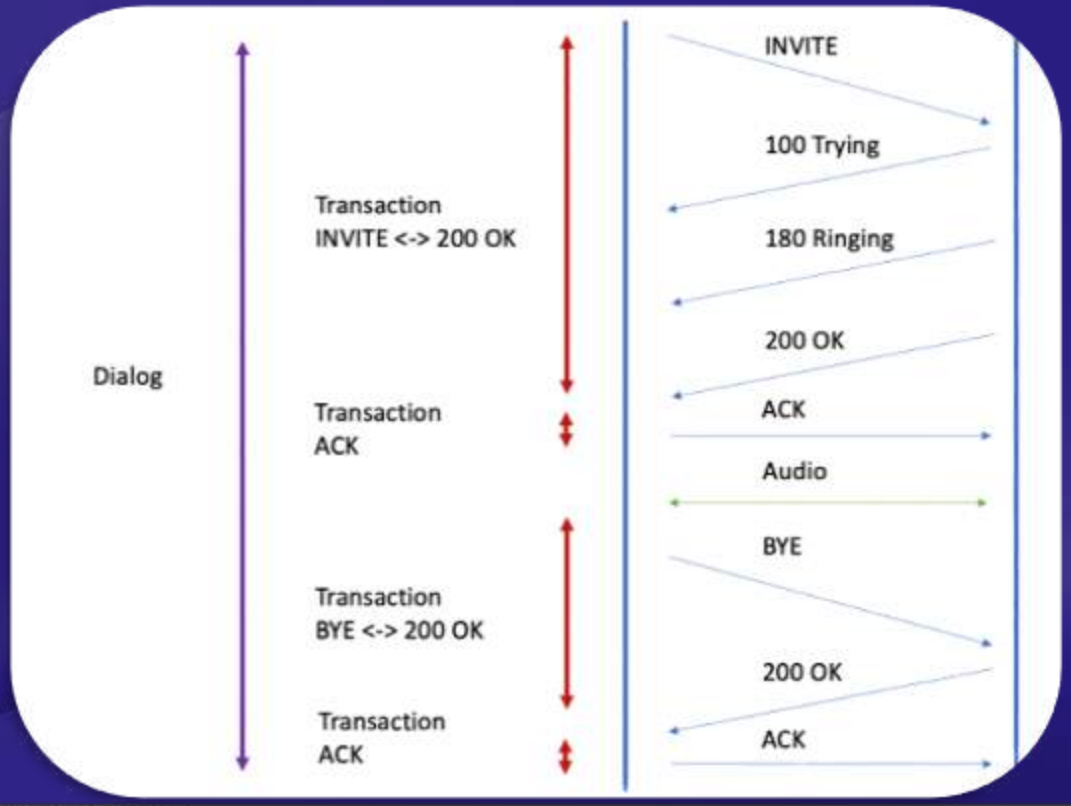
- VoIP Protocolstack

OSI-Layer	Protokoll / Applikation
Application	Voice signaling, Voice transmission
Presentation	G.711, G.722, H.263, H.264
Session	SIP incl. SDP, RTP
Transport	UDP, TCP
Network	IPv4, IPv6
Data Link	Ethernet, PPP
Physical	xDSL, Ethernet

```
> Frame 7: Packet, 1224 bytes on wire (9792 bits), 1224 bytes captured (9792 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:2b:5b (60:3e:5f:36:2b:5b), Dst: elmegt_7a:70:62 (00:09:4f:7a:70:62)
> Internet Protocol Version 4, Src: 192.168.178.26, Dst: 192.168.178.1
> Transmission Control Protocol, Src Port: 49499, Dst Port: 5060, Seq: 1, Ack: 1, Len: 1170
> Session Initiation Protocol (INVITE)
```

```
> Frame 27: Packet, 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface en0, id 0
> Ethernet II, Src: Apple_36:2b:5b (60:3e:5f:36:2b:5b), Dst: elmegt_7a:70:62 (00:09:4f:7a:70:62)
> Internet Protocol Version 4, Src: 192.168.178.26, Dst: 192.168.178.1
> User Datagram Protocol, Src Port: 4002, Dst Port: 10136
> Real-Time Transport Protocol
```

Protocol Basics | SIP-Dialogs und Transactions




```
Session Initiation Protocol (200)
  > Status-Line: SIP/2.0 200 OK
  v Message Header
    > Via: SIP/2.0/TCP 192.168.178.26:49499;rport=49499;branch=z9hG4bKPjsPReVfORu5RCotnVl8t-YGKDHKb1iwho;alias
    > From: "Benjamin Pfister" <sip:23@gw.intern.pfisterit.de>;tag=QCAE7nvHeuGKuKwticvFg14JYR4uWagt
    > To: <sip:08003303762@gw.intern.pfisterit.de>;tag=1EC2957B3B183D109A47312015380500
      Call-ID: 0NhINsgcDOHbrZB1EVpdn5sBUXTMupg.
      [Generated Call-ID: 0NhINsgcDOHbrZB1EVpdn5sBUXTMupg.]
    > CSeq: 17471 INVITE
    > Contact: <sip:08003303762@192.168.178.1:5060;transport=tcp>
```

Protocol Basics | SIP Request Methods

Method	Purpose
INVITE	Initiation or Change
ACK	Acknowledment to a Request
BYE	Terminate Session
CANCEL	Cancels pending request
REGISTER	Location transmission (IP & port) & authentication if necessary
OPTIONS	Availability check & clarification of supported options on Remote station
PRACK	Provisional confirmation

Protocol Basics | SIP Request Methods

Method	Purpose
INFO	Control information during conversation
REFER	Forwarding request to recipient
UPDATE	Call status change

Protokollaufbau | SIP Response Codes

Response	Purpose
1xx	Preliminary status information
2xx	Successful Respsonse
3xx	Forward Information
4xx	Client-side errors
5xx	Server-side errors
6xx	Global errors

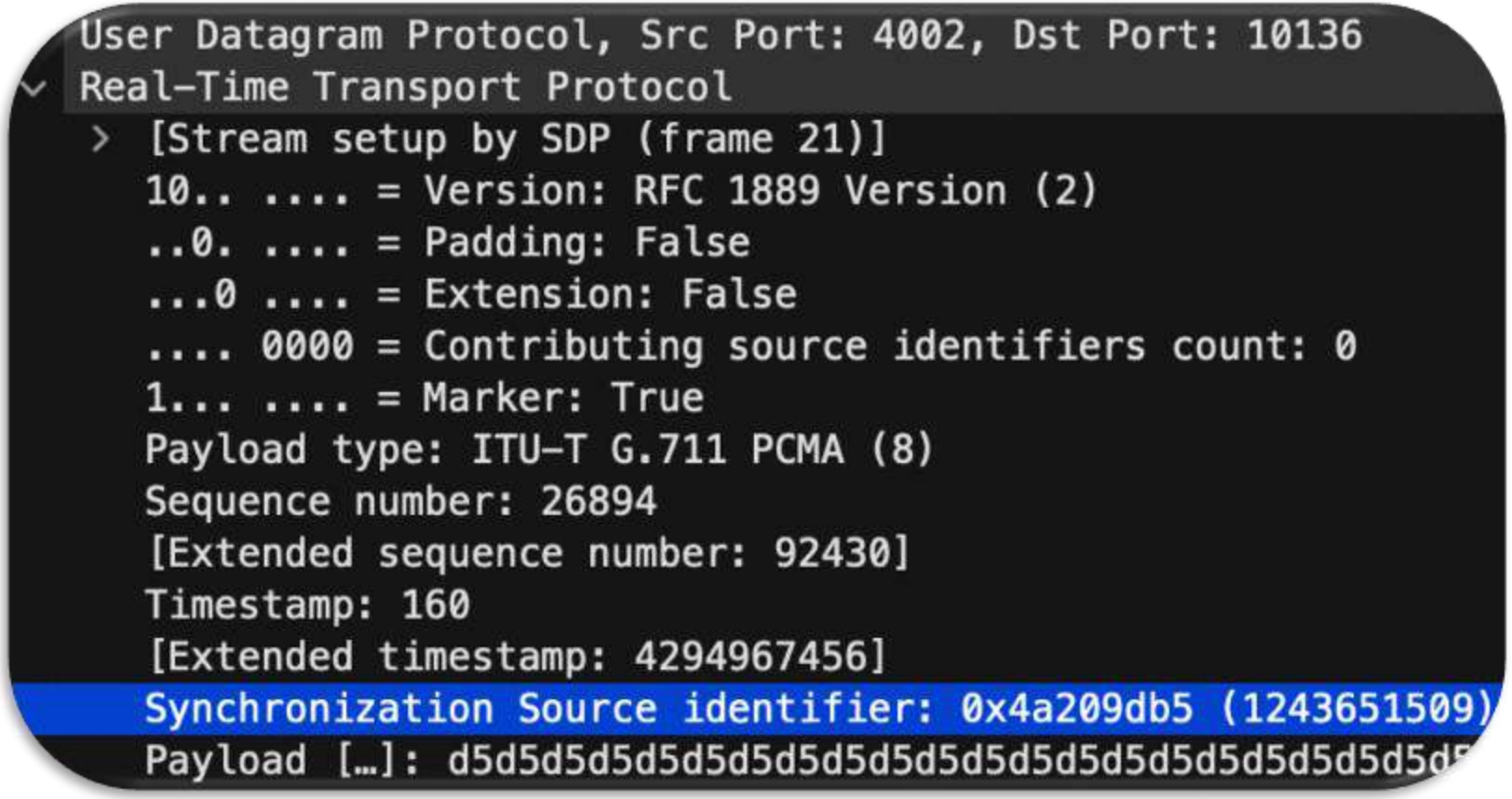
Protokollaufbau | SIP-Antwortcodes


```
Session Initiation Protocol (401)
  > Status-Line: SIP/2.0 401 Unauthorized 11030230348
  v Message Header
    > Via: SIP/2.0/TCP 192.168.4.24:5060;received=80.132.157.249;branch=z9hG4bK655629529
    > To: "VAF SIP Trunk" <sip:+4966239125889@tel.t-online.de>;tag=h7g4Esbg_23c7baae05f3cb1730eb764b914989a8
    > From: "VAF SIP Trunk" <sip:+4966239125889@tel.t-online.de>;tag=437100124
      Call-ID: 3_1827760106@192.168.4.24
      [Generated Call-ID: 3_1827760106@192.168.4.24]
    > CSeq: 1 REGISTER
    > Service-Route: <sip:217.0.21.2:5060;transport=tcp;lr>
    > WWW-Authenticate: Digest realm="tel.t-online.de",nonce="7E019C15DADBE5610000000085C6D515",stale=true,algorithm=MD5,qop="auth"
```

Troubleshooting VoIP | Basic Call

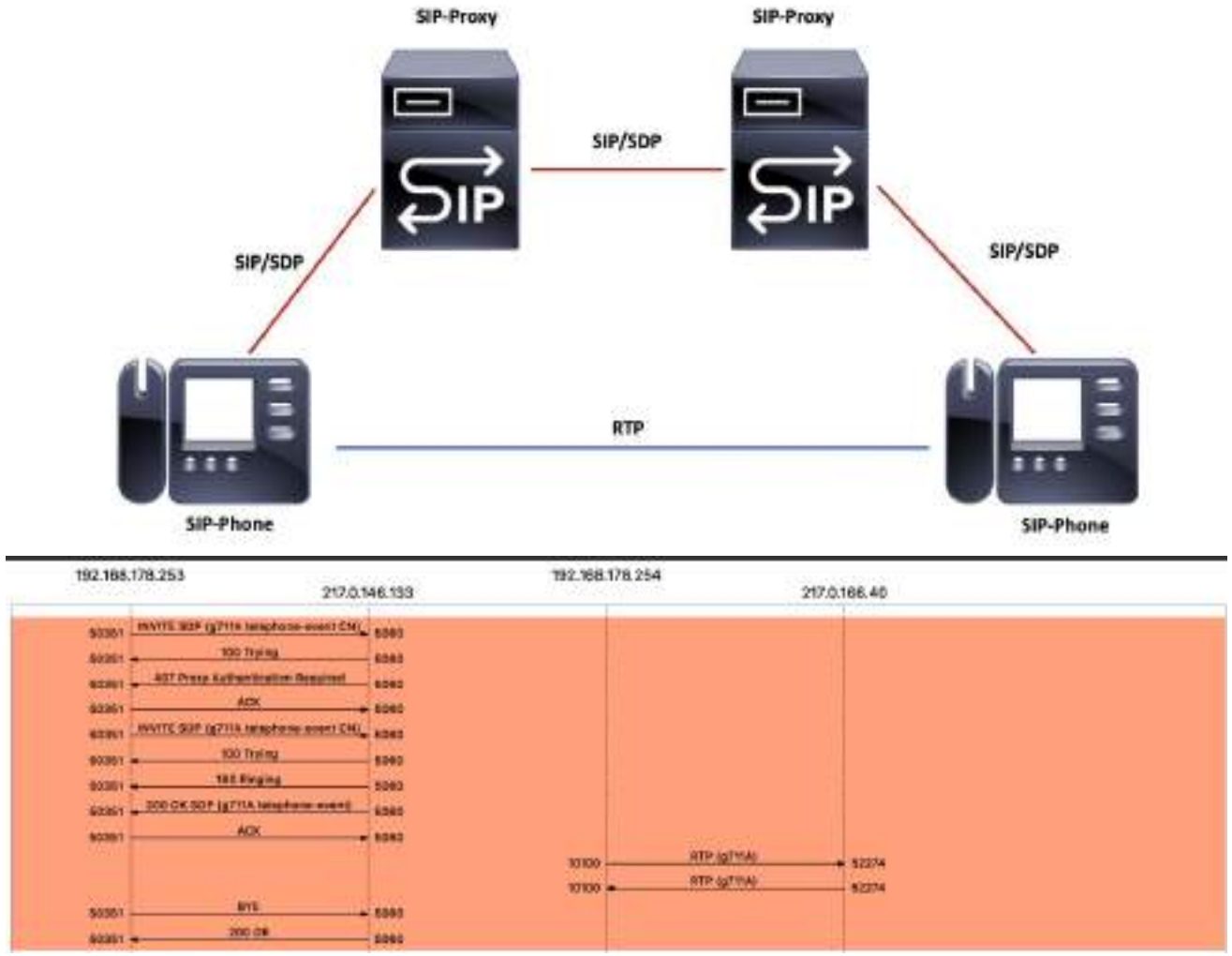
- Basic Call (Softphone <-> PBX)
- Request Methods
- Response Codes
- SIP-Headers
- SDP

Troubleshooting VoIP | Basic Call

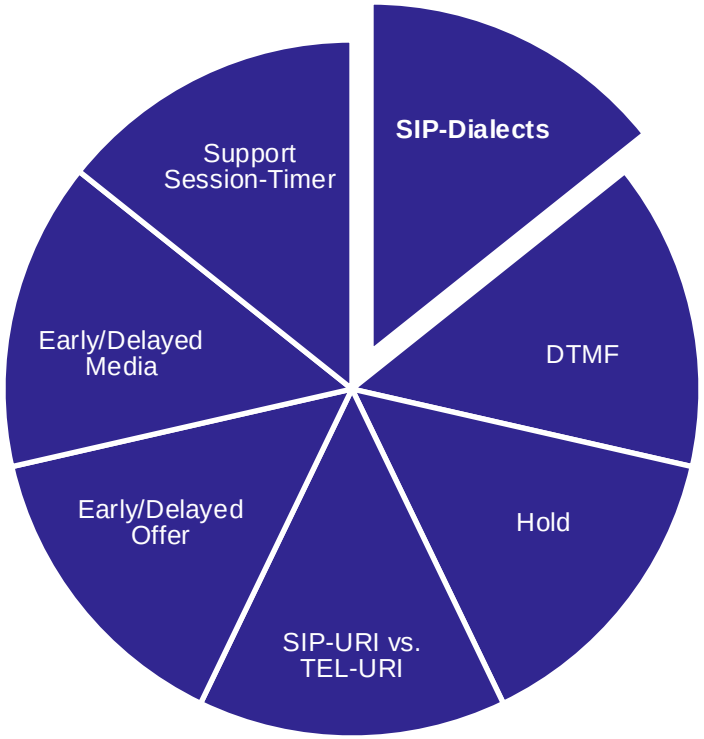


Troubleshooting VoIP | Challenges

- Transport SIP: UDP, TCP or TCP & TLS
- Two (Three) Streams: SIP & RTP (RTCP)
- Firewalling: dynamic negotiation of RTP-Ports
- RTP-Portrange configurable



Troubleshooting VoIP | Challenges




```
> Real-Time Transport Protocol
v RFC 2833 RTP Event
    Event ID: DTMF Eight 8 (8)
    1... .... = End of Event: True
    .1.. .... = Reserved: True
    ..00 0001 = Volume: 1
    Event Duration: 8458
```

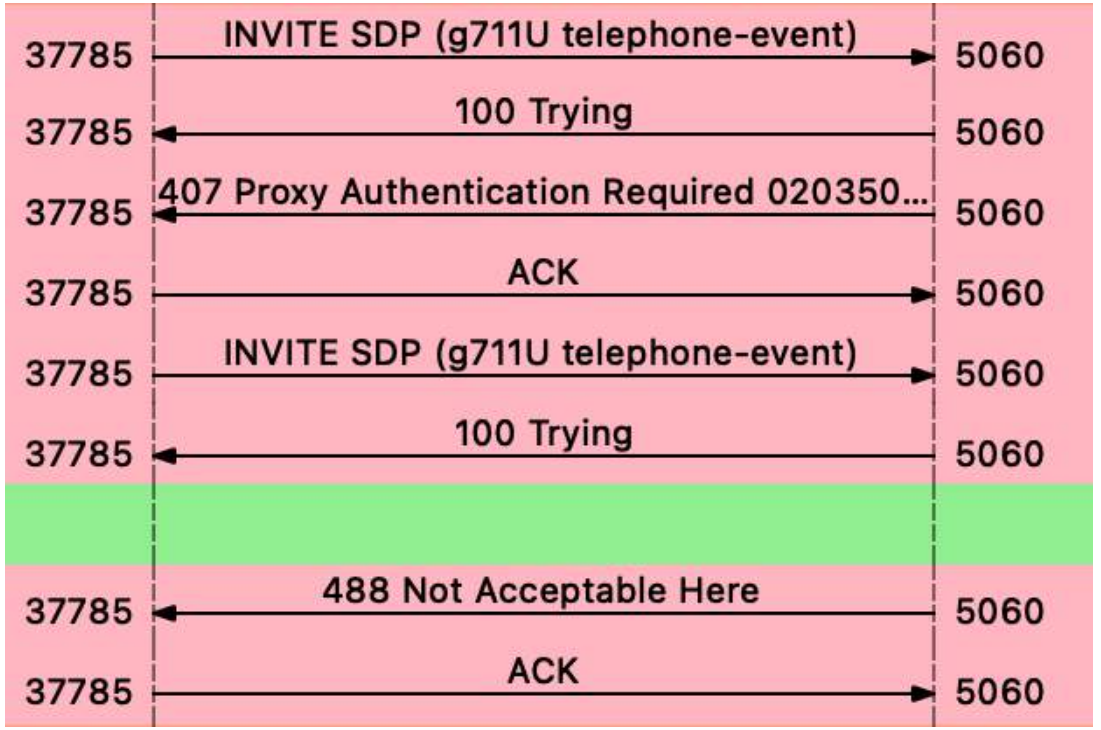
```
v Message Body
    Signal=2\r\n
    Duration=86\r\n
```

```
> Reason: Q.850;cause=102;text="Recovery on timer expiry"
```

```
Require: timer
Server: (innovaphone IP0011/14r1 sr5 [14.1.0534/136386/600])
Supported: 100rel,replaces,privacy,timer,from-change,histinfo,
P-Preferred-Identity: <sip:004966239159807@192.168.178.253>
Session-Expires: 1800;refresher=uac
```

Troubleshooting VoIP | Challenges

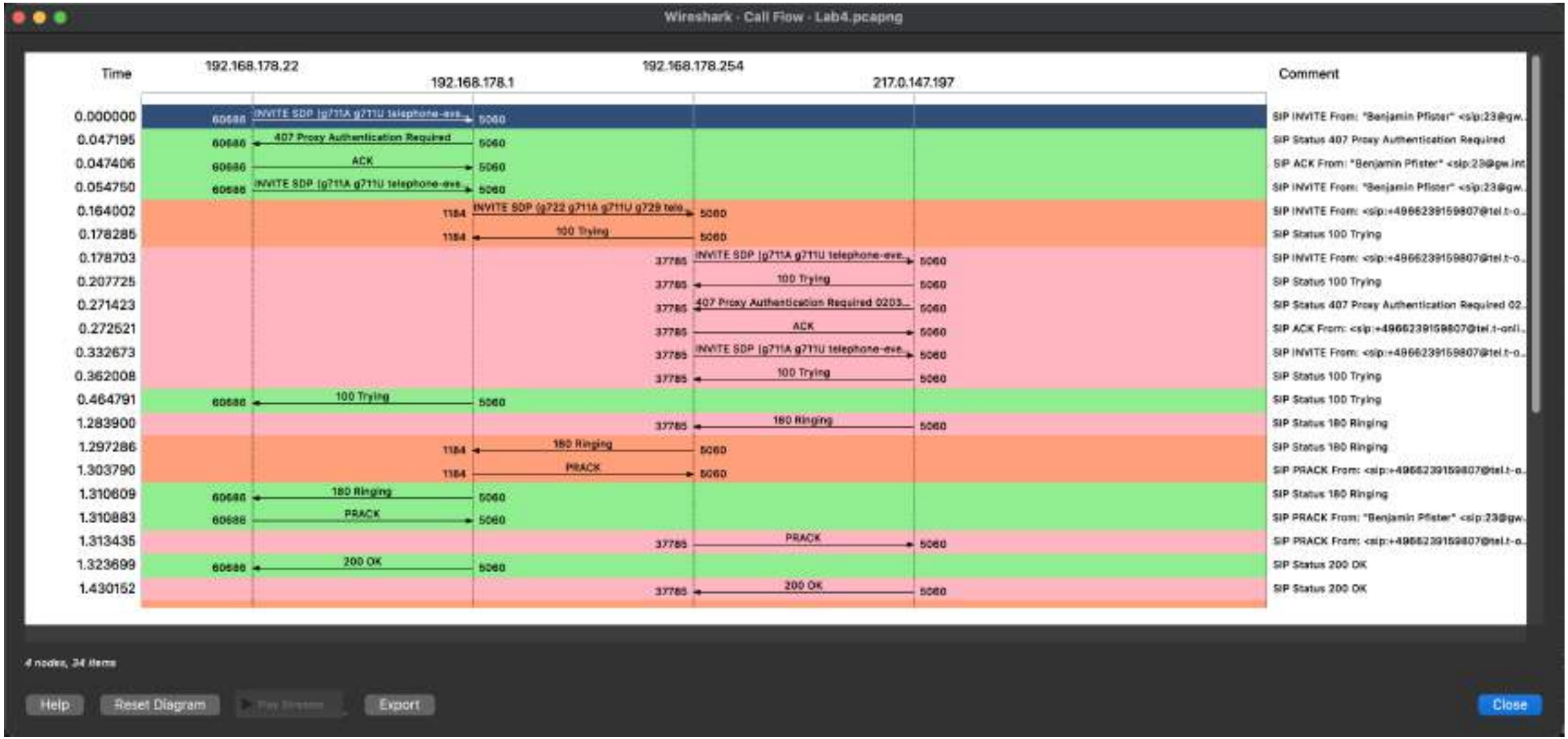
- **RTP**
- Packetloss, Jitter & Delay
- Codecs
- Framing time
- NAT
- SRTP key exchange



Capture-Challenges

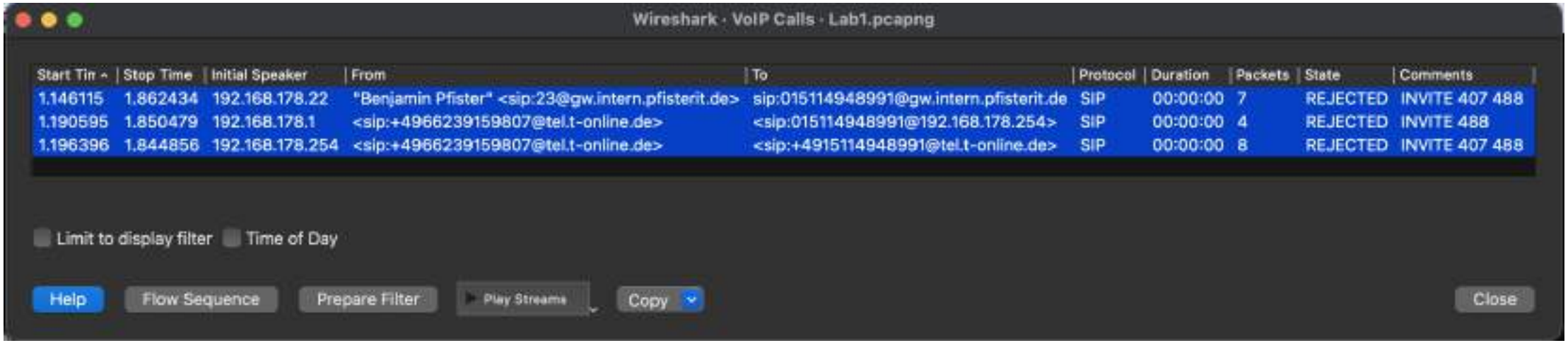
- PBX only signaling
- Different Call-Legs / SBCs
- Dynamic RTP-Ports
- High Packet rates
- SIP-TLS Encryption
- Sometimes no capture on devices

Troubleshooting VoIP | Challenges

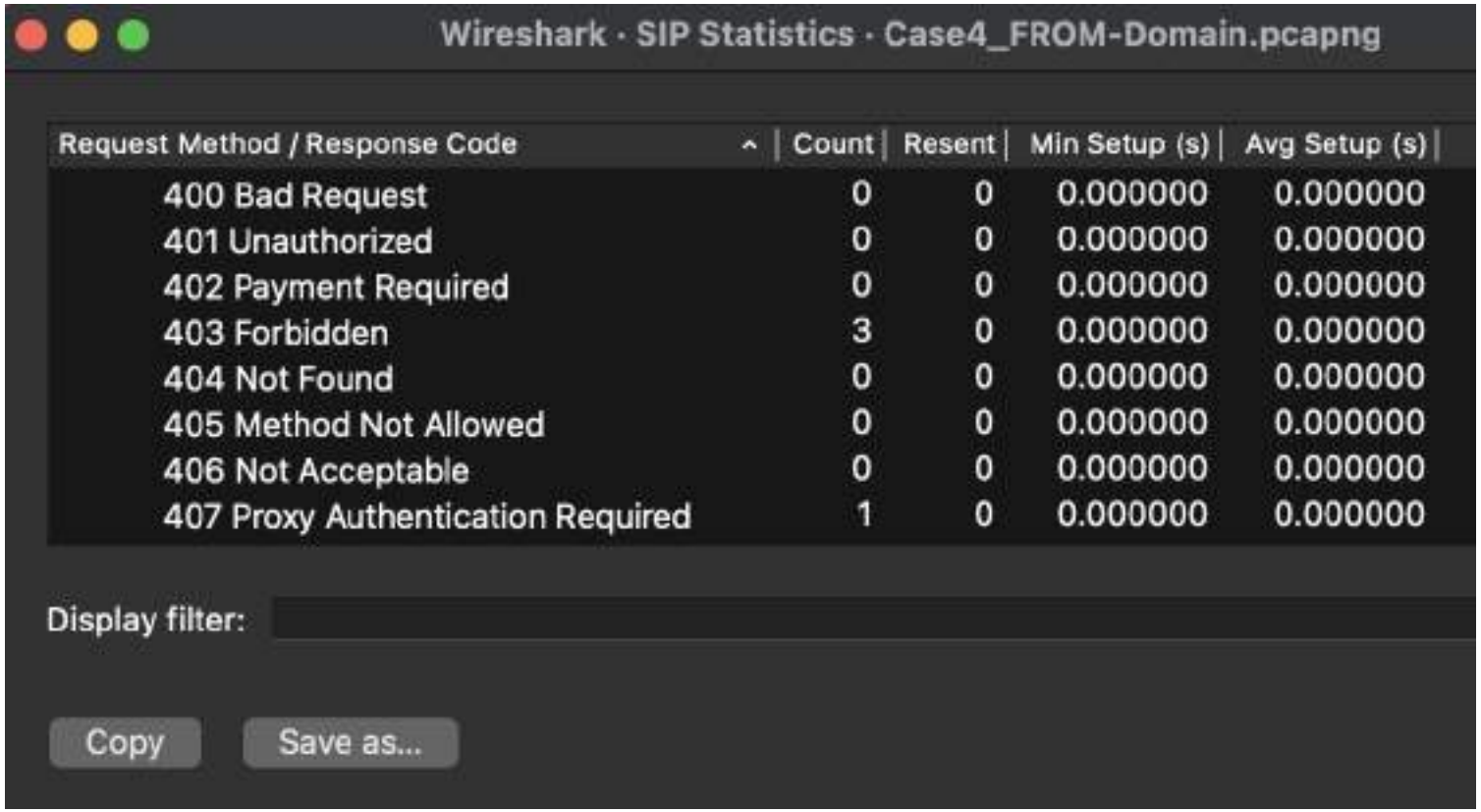


Analysis Options SIP

- Call Listing
- SIP Flows



SIP Statistics



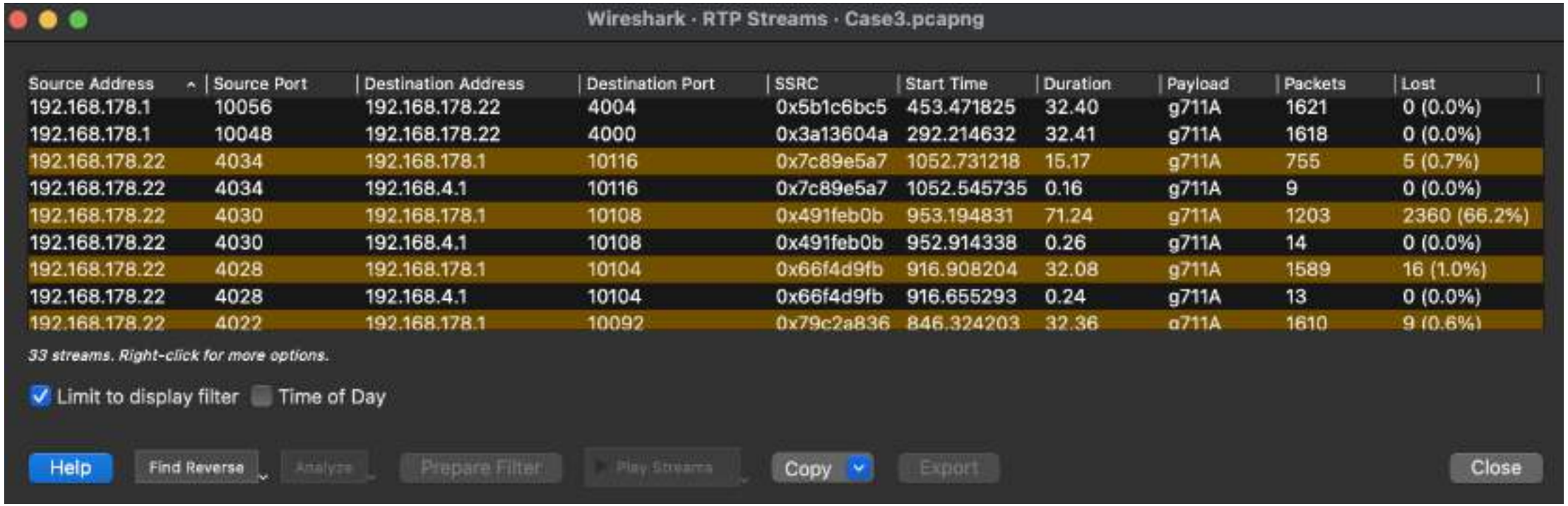
Display-Filter SIP & SDP

Display-Filter	Description
sip	Session Initiation Protocol
sip.Method == "INVITE“	Filter specific Request Method
sip.from.user == “xxxxx“	Filter specific source number
sip.to.user == „xxxxx“	Filter specific destination number
sip.Call-ID == "xxxxx@192.0.2.1"	Filter SIP messages on specific call on a leg
sip.call_id_generated == „xxxxx“	Filter SIP & RTP messages on specific call on a leg
sdp	Packets with SDP
sdp.connection_info == "IN IP4 192.0.2.1“	Packets with 192.0.2.1 in C-Line in SDP
sdp.media contains "RTP/SAVP"	Packets with SRTP/SDES Key Exchange

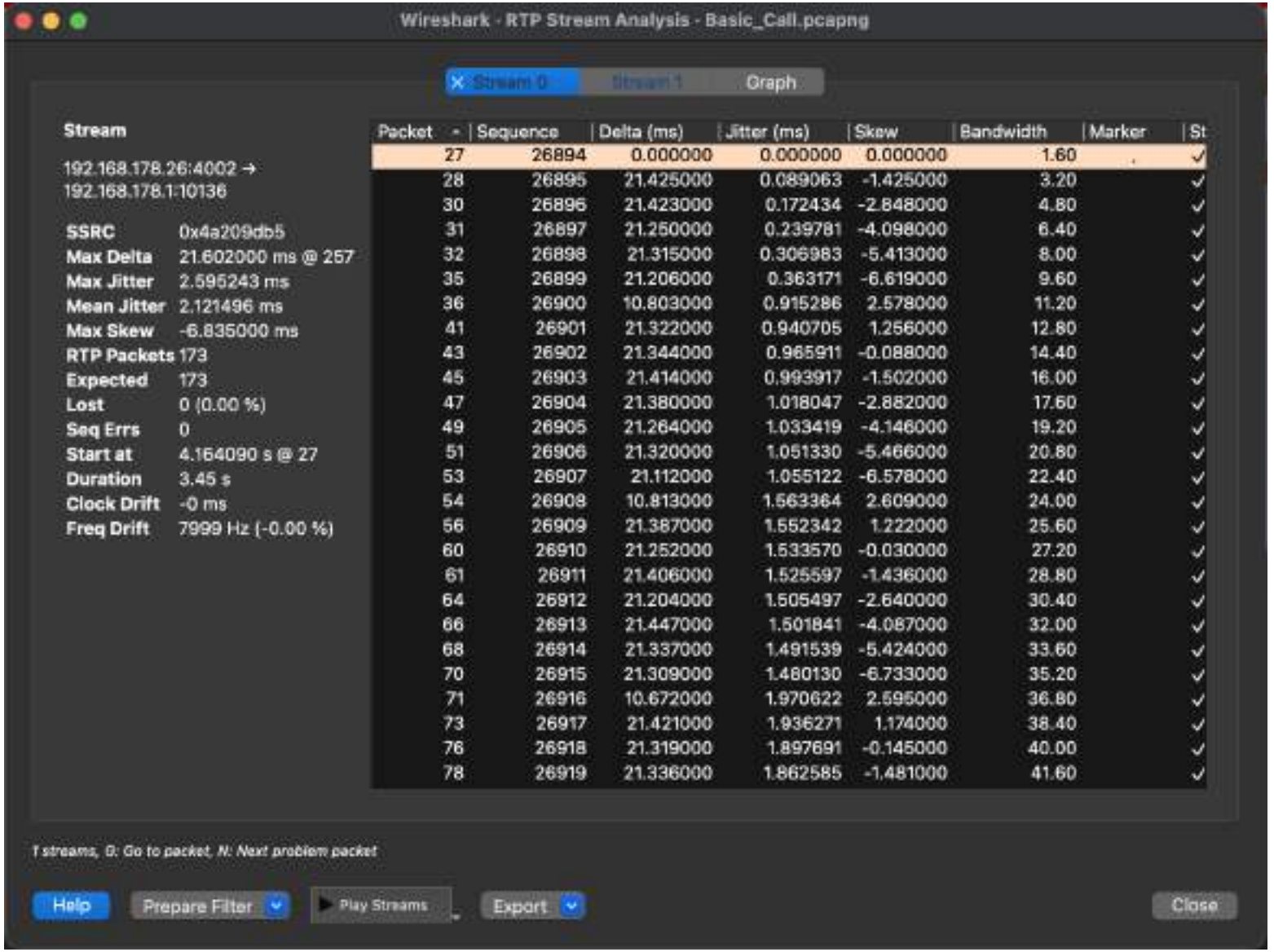
Filter-Button

- Status-Code Buttons
- SIP oder RTP
- Call-ID Generated
- Failed Handshake on TCP
- SDP

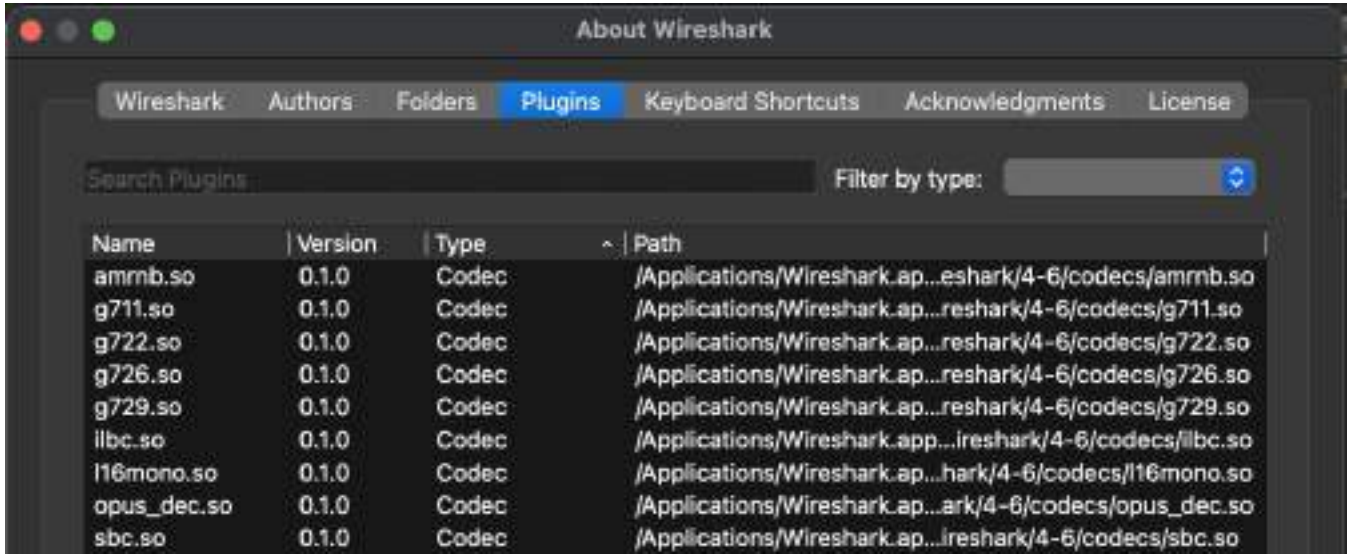
Troubleshooting VoIP | RTP-Analysis



Troubleshooting VoIP | RTP-Analysis



Troubleshooting VoIP | RTP-Analysis

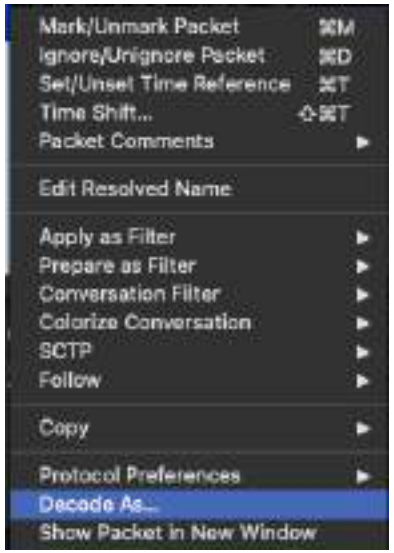


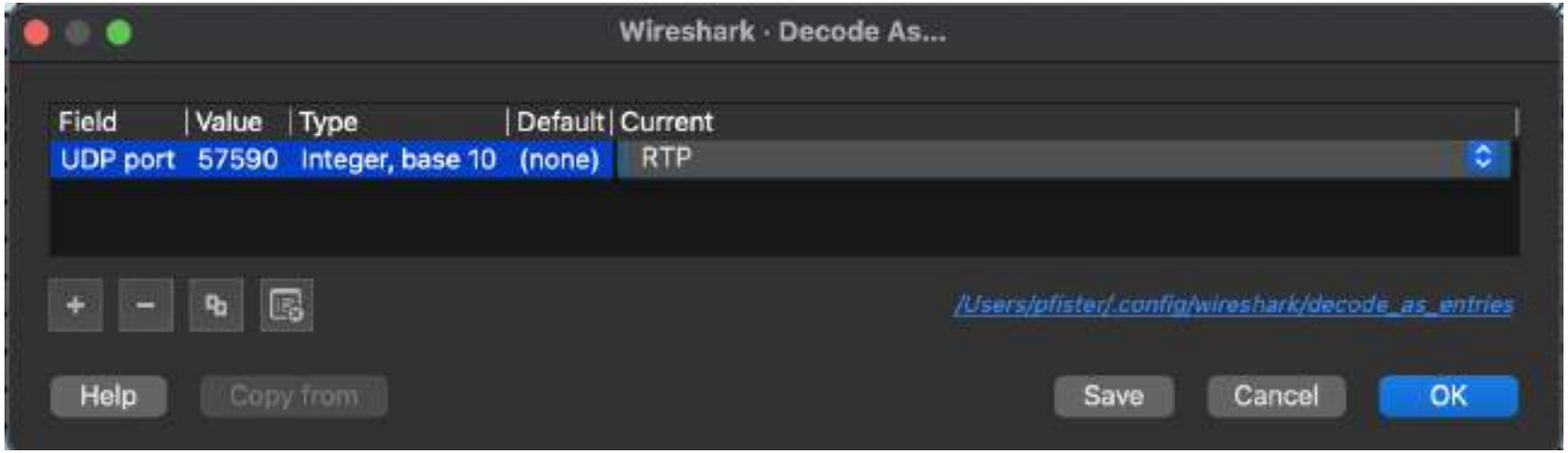
- # Display-Filter RTP

Display-Filter	Description
rtp	Real-Time Transport Protocol
rtp.ssrc == 0x0f51d0da	Filter specific RTP stream
rtp.p_type == 8	Filter payload type
srtp.enc_payload	SRTP packets
rtp.setup-method == "DTLS-SRTP“	SRTP packets negotiated via DTLS-SRTP
rtpevent	RFC2833 & RFC4733


authenticated
encrypted
RTP-Header
Payload
Hash

Troubleshooting VoIP | SRTP-Analysis





Troubleshooting VoIP | SRTP-Analysis

1672	32.834816	0.010119	192.168.178.22	192.168.178.28	UDP	176	50004 → 50002 Len=134
1673	32.860177	0.025361	192.168.178.22	192.168.178.28	UDP	181	50004 → 50002 Len=139
1674	32.880485	0.020308	192.168.178.22	192.168.178.28	UDP	172	50004 → 50002 Len=130
1675	32.886491	0.006006	192.168.178.28	192.168.178.22	UDP	112	50002 → 50004 Len=70
1676	32.886503	0.000012	192.168.178.28	192.168.178.22	UDP	121	50002 → 50004 Len=79
1677	32.886504	0.000001	192.168.178.28	192.168.178.22	UDP	115	50002 → 50004 Len=73
1678	32.887839	0.001335	192.168.178.28	192.168.178.22	UDP	116	50002 → 50004 Len=74
1679	32.887851	0.000012	192.168.178.28	192.168.178.22	UDP	111	50002 → 50004 Len=69

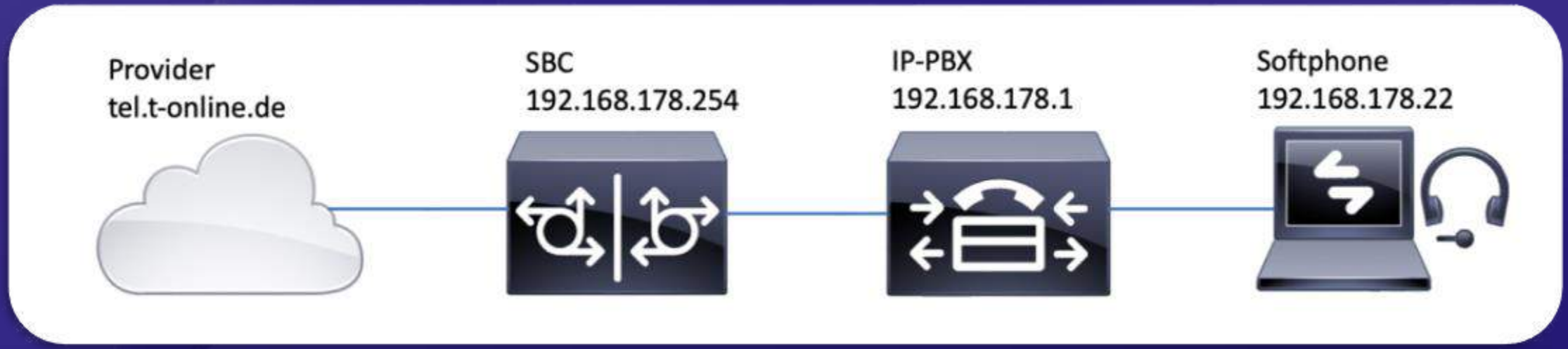
1672	32.834816	0.010119	192.168.178.22	192.168.178.28	RTP	176	PT=DynamicRTP-Type-108, SSRC=0x3FD5, Seq=20515, Time=513119563
1673	32.860177	0.025361	192.168.178.22	192.168.178.28	RTP	181	PT=DynamicRTP-Type-108, SSRC=0x3FD5, Seq=20516, Time=513120523
1674	32.880485	0.020308	192.168.178.22	192.168.178.28	RTP	172	PT=DynamicRTP-Type-108, SSRC=0x3FD5, Seq=20517, Time=513121483
1675	32.886491	0.006006	192.168.178.28	192.168.178.22	RTP	112	PT=DynamicRTP-Type-108, SSRC=0xA0E4, Seq=7717, Time=23624619
1676	32.886503	0.000012	192.168.178.28	192.168.178.22	RTP	121	PT=DynamicRTP-Type-108, SSRC=0xA0E4, Seq=7718, Time=23625579
1677	32.886504	0.000001	192.168.178.28	192.168.178.22	RTP	115	PT=DynamicRTP-Type-108, SSRC=0xA0E4, Seq=7719, Time=23626539
1678	32.887839	0.001335	192.168.178.28	192.168.178.22	RTP	116	PT=DynamicRTP-Type-108, SSRC=0xA0E4, Seq=7720, Time=23627499
1679	32.887851	0.000012	192.168.178.28	192.168.178.22	RTP	111	PT=DynamicRTP-Type-108, SSRC=0xA0E4, Seq=7721, Time=23628459

- Real errors recreated in the lab
- Procedure & Root-Cause

Case 1

- No outgoing calls
- Only to External
- Incoming working
- Working for years before

Case 2- No outgoing calls



Case 3

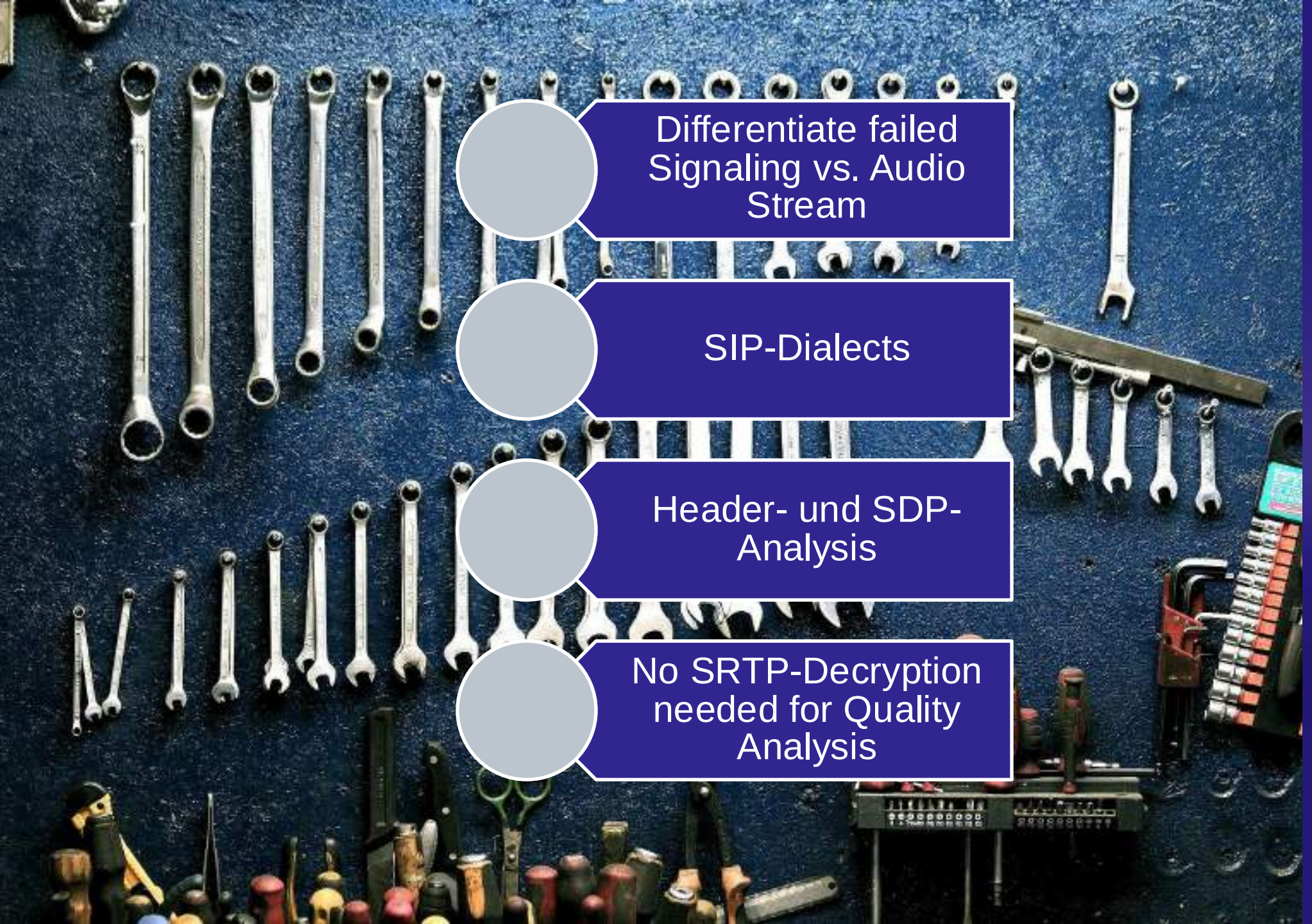
- Initial delayed incoming Audio
- Sometimes no Audio
- Outgoing Call
- RTP not captured

Case 4

No outgoing Calls to External

Internal okay

Topology from Case 1



- Differentiate failed Signaling vs. Audio Stream
- SIP-Dialects
- Header- und SDP-Analysis
- No SRTP-Decryption needed for Quality Analysis

Lessons Learned

Thanks

linkedin.com/in/benjamin-pfister-90136b298

Sources

https://unsplash.com
https://pixabay.com/de
https://www.pexels.com
https://ideogram.ai