

# Troubleshooting VoIP | SIP- & RTP-Analysis with Wireshark

**Benjamin Pfister**

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



- Overview
- Protocol Basics
- Challenges
- Troubleshooting



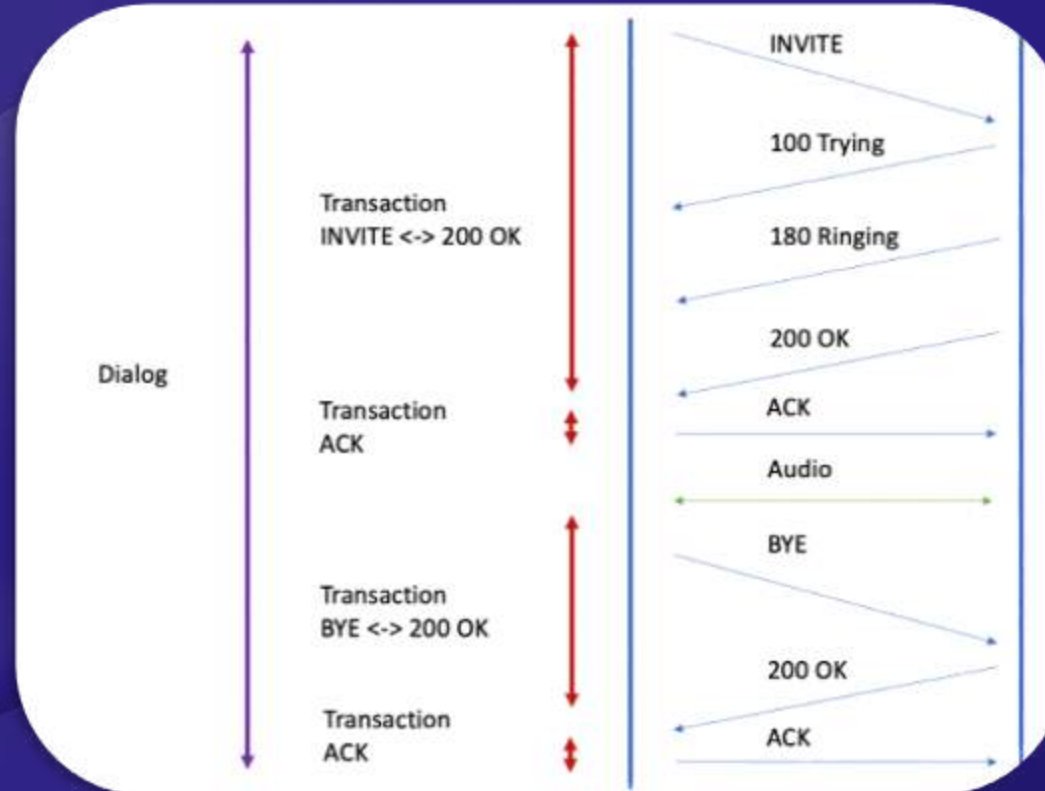
## • VoIP Protocolstack

| OSI-Layer    | Protokoll / Applikation             |
|--------------|-------------------------------------|
| Application  | Voice signaling, Voice transmission |
| Presentation | G.711, G.722, H.263, H.264          |
| Session      | <b>SIP incl. SDP, RTP</b>           |
| 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: elmege_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: elmege_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
  Message Header
    > Via: SIP/2.0/TCP 192.168.178.26:49499;rport=49499;branch=z9hG4bKPjsPReVf0Ru5RCotnVl8t-YGKDHKb1iwho;alias
    > From: "Benjamin Pfister" <sip:23@gw.intern.pfisterit.de>;tag=QCAE7nvHeuGKuKwticvFg14JYR4uWagt
    > To: <sip:08003303762@gw.intern.pfisterit.de>;tag=1EC2957B3B183D109A47312015380500
    Call-ID: 0NhINsgcD0HbrZB1EVpdn5sBUXTMupg.
    [Generated Call-ID: 0NhINsgcD0HbrZB1EVpdn5sBUXTMupg.]
    > 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      | Acknowledgment 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 Response            |
| 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

### 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>

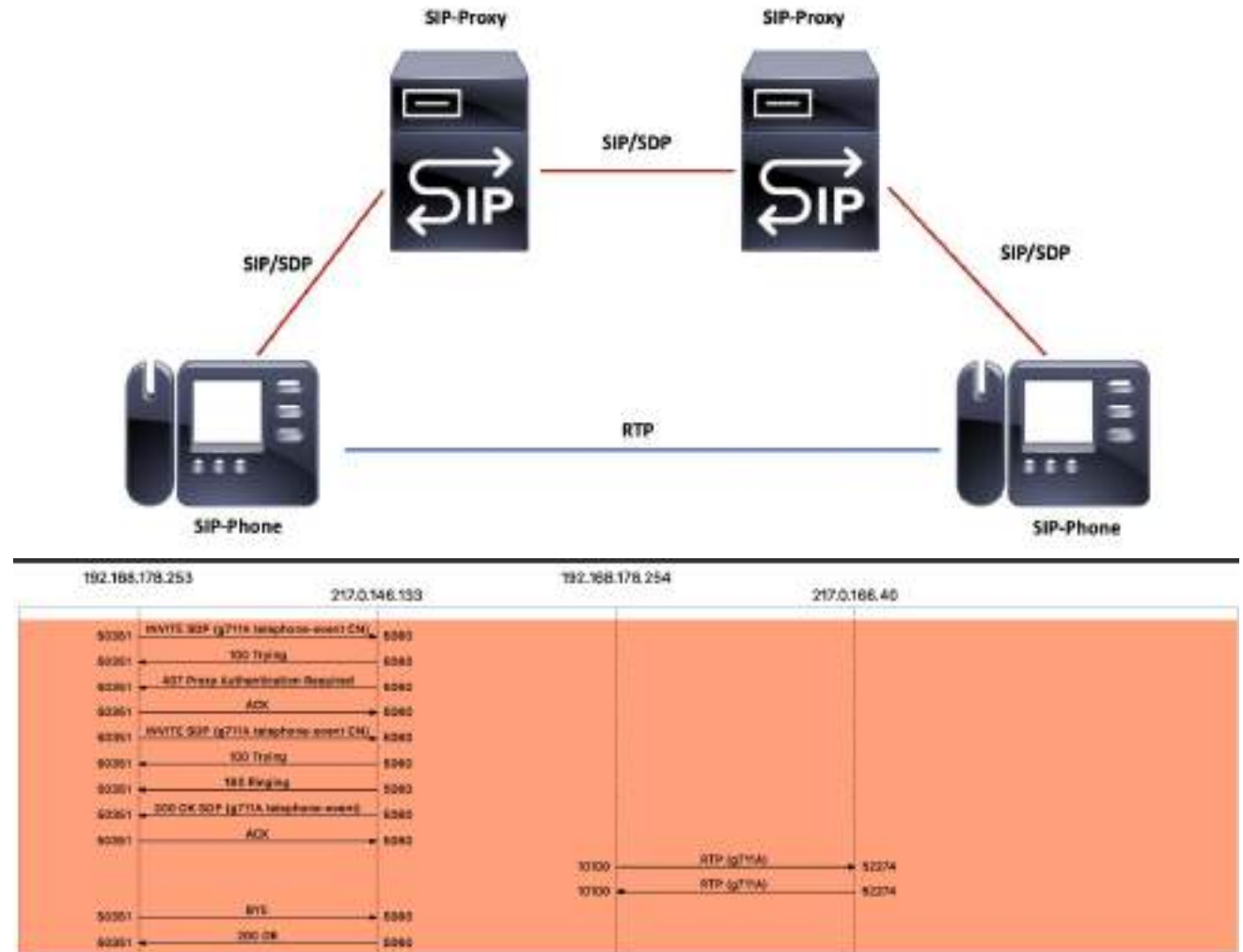
> WWW-Authenticate: Digest realm="tel.t-online.de",nonce="7E019C15DADBE5610000000085C6D515",stale=true,algorithm=MD5,qop="auth"

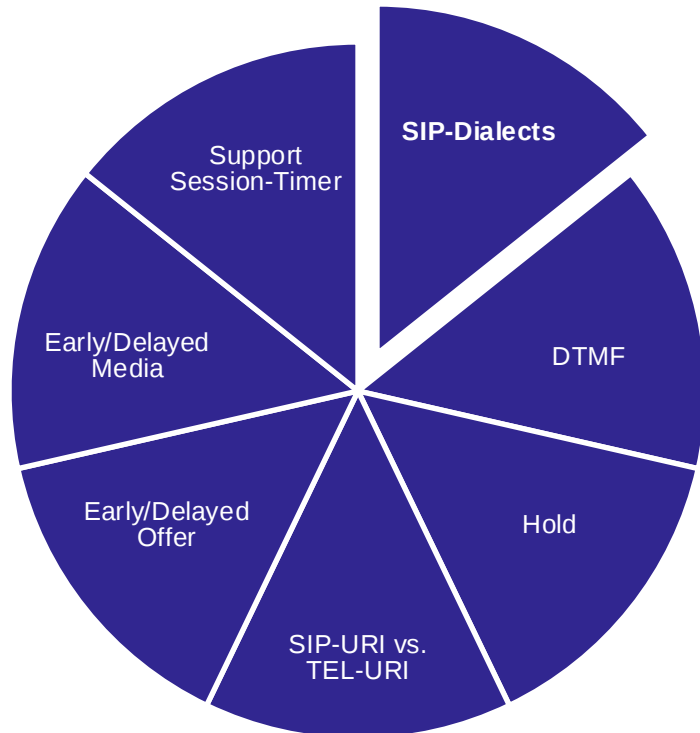
- Basic Call (Softphone <-> PBX)
- Request Methods
- Response Codes
- SIP-Headers
- SDP

```
User Datagram Protocol, Src Port: 4002, Dst Port: 10136
Real-Time Transport Protocol
> [Stream setup by SDP (frame 21)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  1... .... = Marker: True
  Payload type: ITU-T G.711 PCMA (8)
  Sequence number: 26894
  [Extended sequence number: 92430]
  Timestamp: 160
  [Extended timestamp: 4294967456]
  Synchronization Source identifier: 0x4a209db5 (1243651509)
  Payload [...]: d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5d5
```

# 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





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

> Real-Time Transport Protocol

✓ 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

✓ Message Body

Signal=2\r\n

Duration=86\r\n

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

RTP

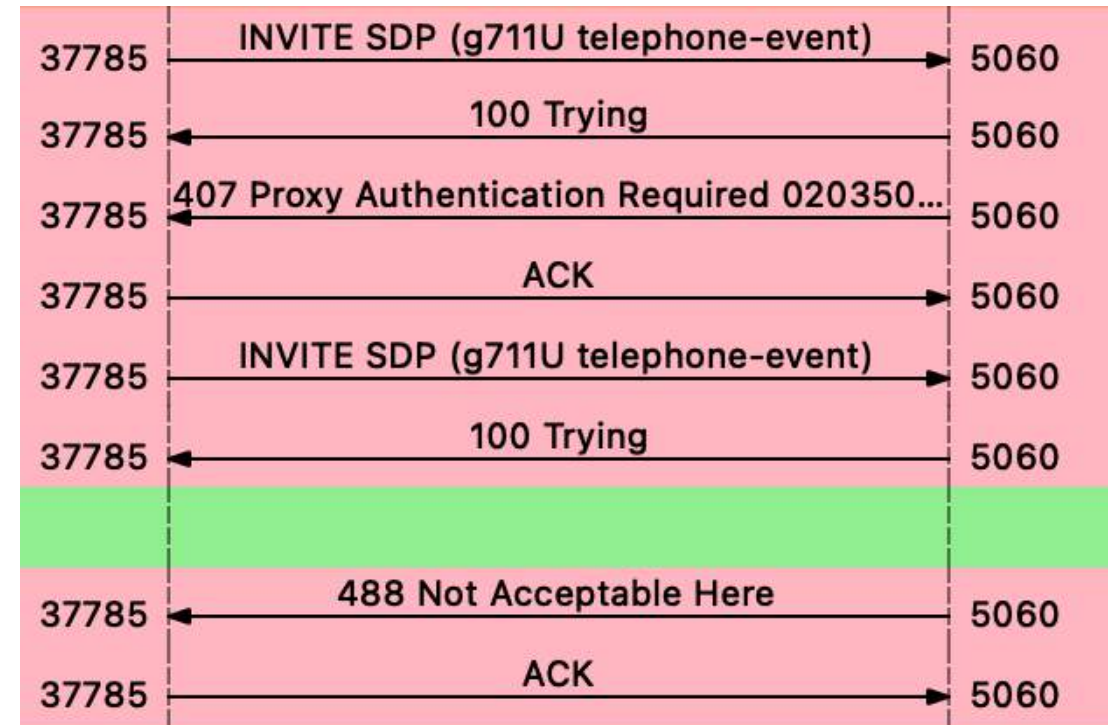
Packetloss, Jitter & Delay

Codecs

Framing time

NAT

SRTP key exchange



## Capture- Challenges

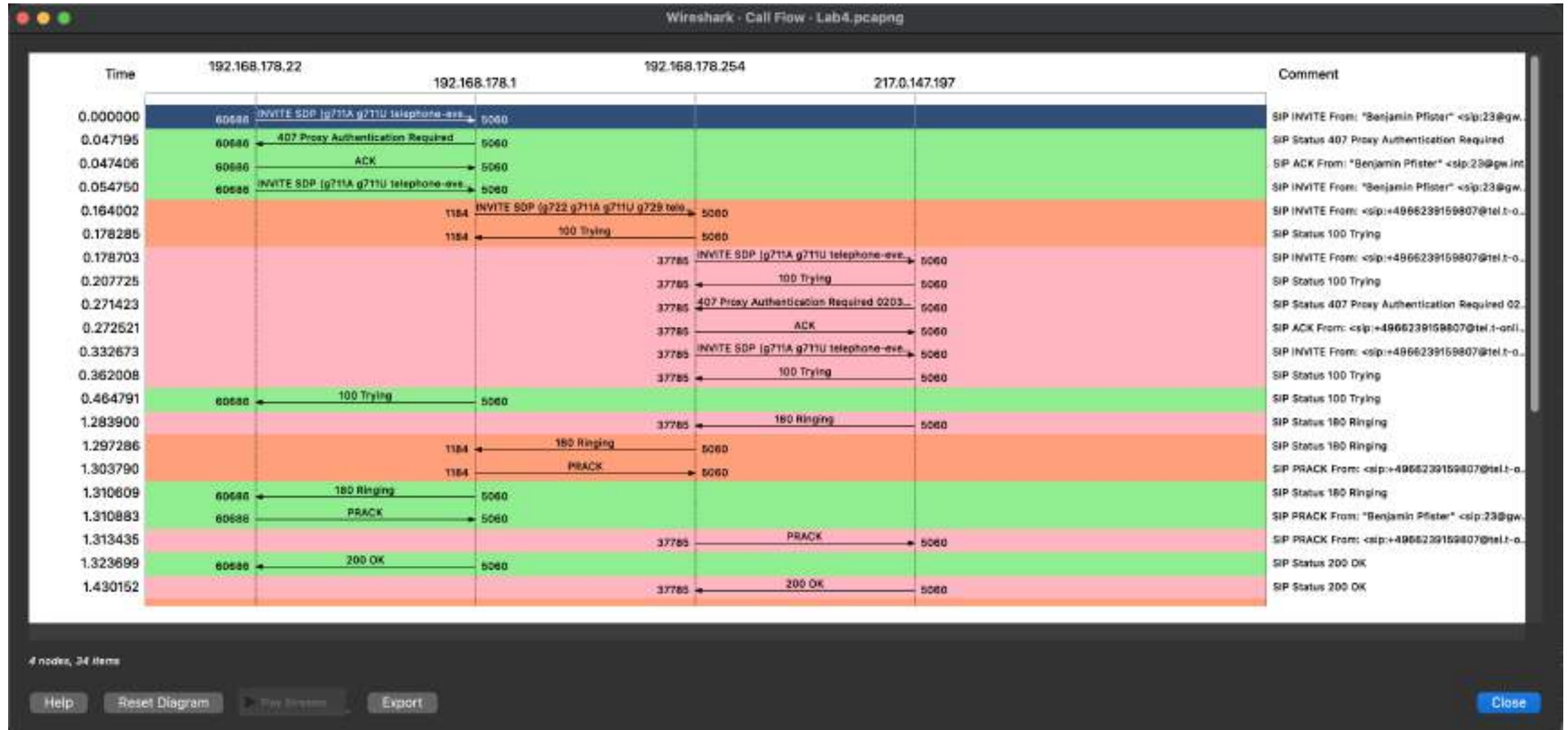
- PBX only signaling
- Different Call-Legs / SBCs
- Dynamic RTP-Ports
- High Packet rates
- SIP-TLS Encryption
- Sometimes no capture on devices

Capture filter for selected interfaces:

 ip host 192.0.2.1 and port 5060 || portrange 16384-32767

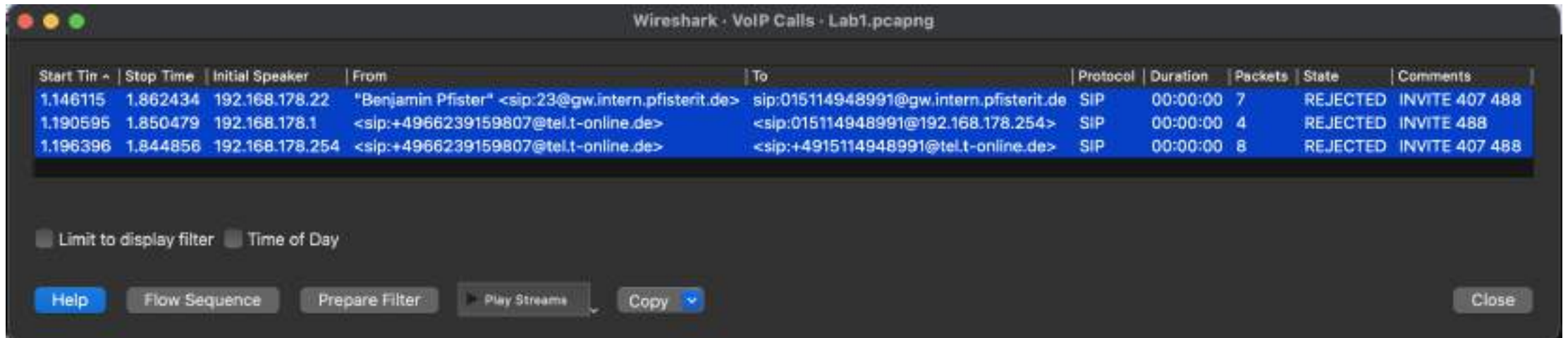


# Troubleshooting VoIP | Challenges



## Analysis Options SIP

- Call Listing
- SIP Flows



Wireshark - VoIP Calls - Lab1.pcapng

| Start Time | Stop Time | Initial Speaker | From                                               | To                                      | Protocol | Duration | Packets | State    | Comments       |
|------------|-----------|-----------------|----------------------------------------------------|-----------------------------------------|----------|----------|---------|----------|----------------|
| 1.146115   | 1.862434  | 192.168.178.22  | "Benjamin Pfister" <sip:23@gw.intern.pfisterit.de> | sip:015114948991@gw.intern.pfisterit.de | SIP      | 00:00:00 | 7       | REJECTED | INVITE 407 488 |
| 1.190595   | 1.850479  | 192.168.178.1   | <sip:+4966239159807@tel.t-online.de>               | <sip:015114948991@192.168.178.254>      | SIP      | 00:00:00 | 4       | REJECTED | INVITE 488     |
| 1.196396   | 1.844856  | 192.168.178.254 | <sip:+4966239159807@tel.t-online.de>               | <sip:+4915114948991@tel.t-online.de>    | SIP      | 00:00:00 | 8       | REJECTED | INVITE 407 488 |

☐ Limit to display filter ☐ Time of Day

Help Flow Sequence Prepare Filter Play Streams Copy Close

## SIP Statistics

Wireshark · SIP Statistics · Case4\_FROM-Domain.pcapng

| Request Method / Response Code    | Count | Resent | Min Setup (s) | Avg Setup (s) |
|-----------------------------------|-------|--------|---------------|---------------|
| 400 Bad Request                   | 0     | 0      | 0.000000      | 0.000000      |
| 401 Unauthorized                  | 0     | 0      | 0.000000      | 0.000000      |
| 402 Payment Required              | 0     | 0      | 0.000000      | 0.000000      |
| 403 Forbidden                     | 3     | 0      | 0.000000      | 0.000000      |
| 404 Not Found                     | 0     | 0      | 0.000000      | 0.000000      |
| 405 Method Not Allowed            | 0     | 0      | 0.000000      | 0.000000      |
| 406 Not Acceptable                | 0     | 0      | 0.000000      | 0.000000      |
| 407 Proxy Authentication Required | 1     | 0      | 0.000000      | 0.000000      |

Display filter:

Copy Save as...

## Display-Filter SIP & SDP

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



## Filter-Button

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

# Troubleshooting VoIP | RTP-Analysis

Wireshark · RTP Streams · Case3.pcapng

| Source Address | Source Port | Destination Address | Destination Port | SSRC       | Start Time  | Duration | Payload | Packets | Lost         |
|----------------|-------------|---------------------|------------------|------------|-------------|----------|---------|---------|--------------|
| 192.168.178.1  | 10056       | 192.168.178.22      | 4004             | 0x5b1c6bc5 | 453.471825  | 32.40    | g711A   | 1621    | 0 (0.0%)     |
| 192.168.178.1  | 10048       | 192.168.178.22      | 4000             | 0x3a13604a | 292.214632  | 32.41    | g711A   | 1618    | 0 (0.0%)     |
| 192.168.178.22 | 4034        | 192.168.178.1       | 10116            | 0x7c89e5a7 | 1052.731218 | 15.17    | g711A   | 755     | 5 (0.7%)     |
| 192.168.178.22 | 4034        | 192.168.4.1         | 10116            | 0x7c89e5a7 | 1052.545735 | 0.16     | g711A   | 9       | 0 (0.0%)     |
| 192.168.178.22 | 4030        | 192.168.178.1       | 10108            | 0x491feb0b | 953.194831  | 71.24    | g711A   | 1203    | 2360 (66.2%) |
| 192.168.178.22 | 4030        | 192.168.4.1         | 10108            | 0x491feb0b | 952.914338  | 0.26     | g711A   | 14      | 0 (0.0%)     |
| 192.168.178.22 | 4028        | 192.168.178.1       | 10104            | 0x66f4d9fb | 916.908204  | 32.08    | g711A   | 1589    | 16 (1.0%)    |
| 192.168.178.22 | 4028        | 192.168.4.1         | 10104            | 0x66f4d9fb | 916.655293  | 0.24     | g711A   | 13      | 0 (0.0%)     |
| 192.168.178.22 | 4022        | 192.168.178.1       | 10092            | 0x79c2a836 | 846.324203  | 32.36    | g711A   | 1610    | 9 (0.6%)     |

33 streams. Right-click for more options.

☒ Limit to display filter ☐ Time of Day

Help Find Reverse Analyze Prepare Filter Play Streams Copy Export Close

# Troubleshooting VoIP | RTP-Analysis

Wireshark - RTP Stream Analysis - Basic\_Call.pcapng

X Stream 0 Stream 1 Graph

| Stream                                       | Packet | Sequence | Delta (ms) | Jitter (ms) | Skew      | Bandwidth | Marker | St |
|----------------------------------------------|--------|----------|------------|-------------|-----------|-----------|--------|----|
| 192.168.178.26:4002 →<br>192.168.178.1:10136 | 27     | 26894    | 0.000000   | 0.000000    | 0.000000  | 1.60      |        | ✓  |
|                                              | 28     | 26895    | 21.425000  | 0.089063    | -1.425000 | 3.20      |        | ✓  |
|                                              | 30     | 26896    | 21.423000  | 0.172434    | -2.848000 | 4.80      |        | ✓  |
| SSRC 0x4a209db5                              | 31     | 26897    | 21.250000  | 0.239781    | -4.098000 | 6.40      |        | ✓  |
| Max Delta 21.602000 ms @ 257                 | 32     | 26898    | 21.315000  | 0.306983    | -5.413000 | 8.00      |        | ✓  |
| Max Jitter 2.595243 ms                       | 35     | 26899    | 21.206000  | 0.363171    | -6.619000 | 9.60      |        | ✓  |
| Mean Jitter 2.121496 ms                      | 36     | 26900    | 10.803000  | 0.915286    | 2.578000  | 11.20     |        | ✓  |
| Max Skew -6.835000 ms                        | 41     | 26901    | 21.322000  | 0.940705    | 1.256000  | 12.80     |        | ✓  |
| RTP Packets 173                              | 43     | 26902    | 21.344000  | 0.985911    | -0.088000 | 14.40     |        | ✓  |
| Expected 173                                 | 45     | 26903    | 21.414000  | 0.993917    | -1.502000 | 16.00     |        | ✓  |
| Lost 0 (0.00 %)                              | 47     | 26904    | 21.380000  | 1.018047    | -2.882000 | 17.60     |        | ✓  |
| Seq Errs 0                                   | 49     | 26905    | 21.264000  | 1.033419    | -4.146000 | 19.20     |        | ✓  |
| Start at 4.164090 s @ 27                     | 51     | 26906    | 21.320000  | 1.051330    | -5.466000 | 20.80     |        | ✓  |
| Duration 3.45 s                              | 53     | 26907    | 21.112000  | 1.055122    | -6.578000 | 22.40     |        | ✓  |
| Clock Drift -0 ms                            | 54     | 26908    | 10.813000  | 1.563364    | 2.609000  | 24.00     |        | ✓  |
| Freq Drift 7999 Hz (-0.00 %)                 | 56     | 26909    | 21.387000  | 1.552342    | 1.222000  | 25.60     |        | ✓  |
|                                              | 60     | 26910    | 21.252000  | 1.533570    | -0.030000 | 27.20     |        | ✓  |
|                                              | 61     | 26911    | 21.406000  | 1.525597    | -1.436000 | 28.80     |        | ✓  |
|                                              | 64     | 26912    | 21.204000  | 1.505497    | -2.640000 | 30.40     |        | ✓  |
|                                              | 66     | 26913    | 21.447000  | 1.501841    | -4.087000 | 32.00     |        | ✓  |
|                                              | 68     | 26914    | 21.337000  | 1.491539    | -5.424000 | 33.60     |        | ✓  |
|                                              | 70     | 26915    | 21.309000  | 1.480130    | -6.733000 | 35.20     |        | ✓  |
|                                              | 71     | 26916    | 10.672000  | 1.970622    | 2.595000  | 36.80     |        | ✓  |
|                                              | 73     | 26917    | 21.421000  | 1.936271    | 1.174000  | 38.40     |        | ✓  |
|                                              | 76     | 26918    | 21.319000  | 1.897691    | -0.145000 | 40.00     |        | ✓  |
|                                              | 78     | 26919    | 21.336000  | 1.862585    | -1.481000 | 41.60     |        | ✓  |

f streams, G: Go to packet, N: Next problem packet

Help Prepare Filter Play Streams Export Close

# Troubleshooting VoIP | RTP-Analysis

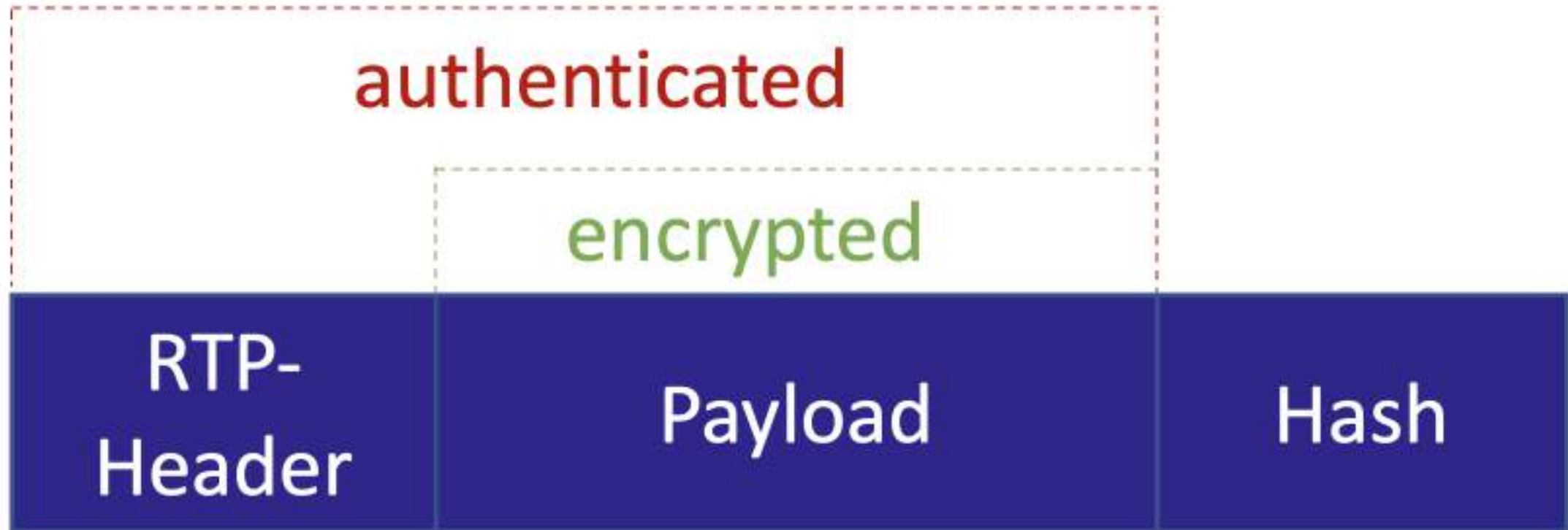


The About Wireshark window displays the Plugins tab. The search bar is empty, and the filter by type is set to 'All'. The following table lists the installed plugins:

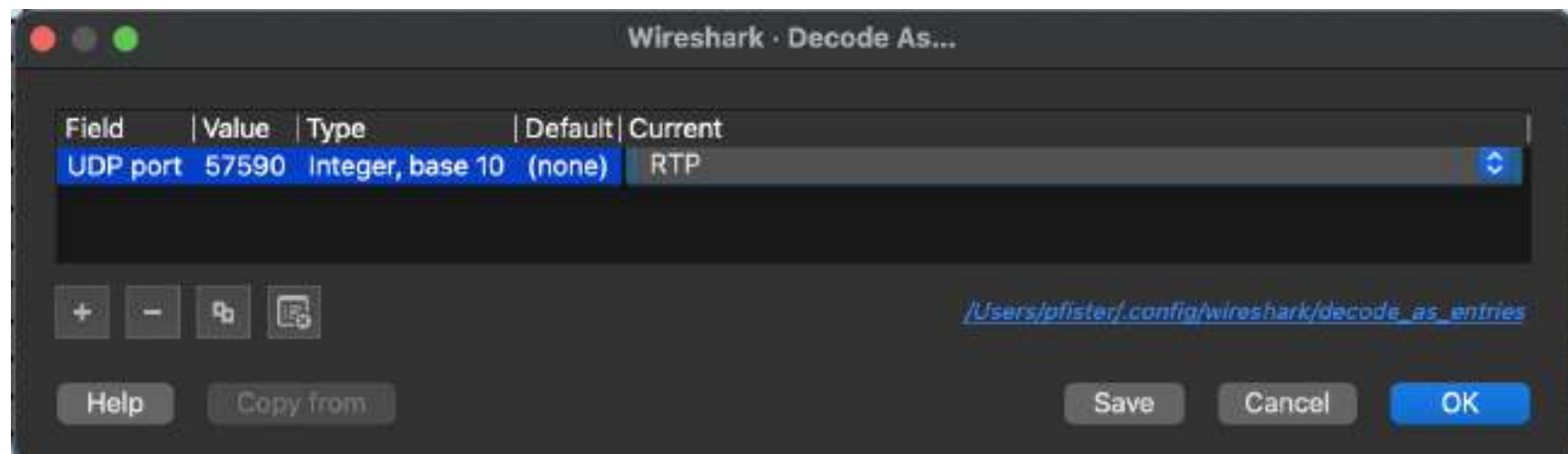
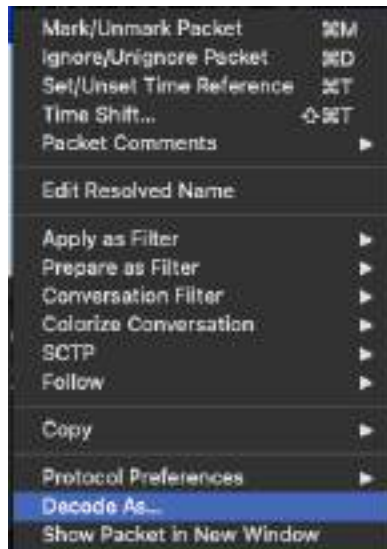
| Name        | Version | Type  | Path                                                    |
|-------------|---------|-------|---------------------------------------------------------|
| amrnb.so    | 0.1.0   | Codec | /Applications/Wireshark.ap...eshark/4-6/codecs/amrnb.so |
| g711.so     | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/g711.so |
| g722.so     | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/g722.so |
| g726.so     | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/g726.so |
| g729.so     | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/g729.so |
| ilbc.so     | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/ilbc.so |
| l16mono.so  | 0.1.0   | Codec | /Applications/Wireshark.ap...hark/4-6/codecs/l16mono.so |
| opus_dec.so | 0.1.0   | Codec | /Applications/Wireshark.ap...ark/4-6/codecs/opus_dec.so |
| sbc.so      | 0.1.0   | Codec | /Applications/Wireshark.ap...reshark/4-6/codecs/sbc.so  |

- **Display-Filter RTP**

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



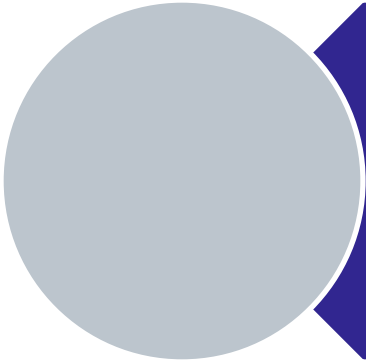
# Troubleshooting VoIP | SRTP-Analysis



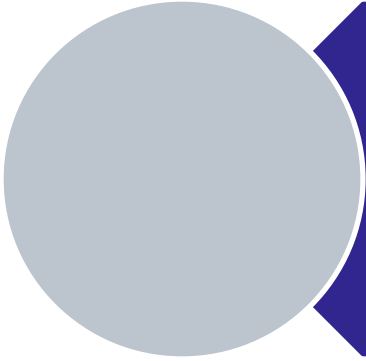
# Troubleshooting VoIP | SRTP-Analysis

|      |           |          |                |                |     |     |               |         |
|------|-----------|----------|----------------|----------------|-----|-----|---------------|---------|
| 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

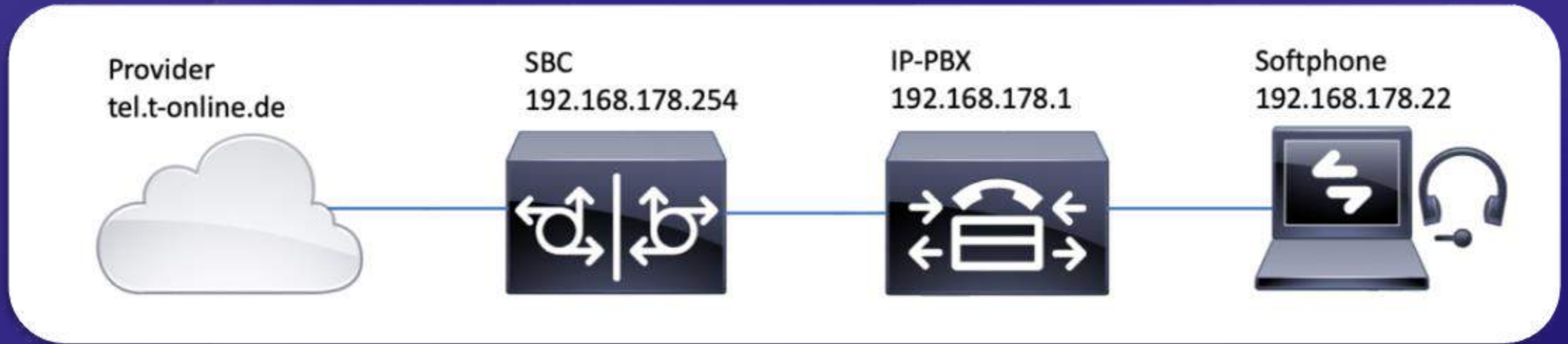


## Case 1

- 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



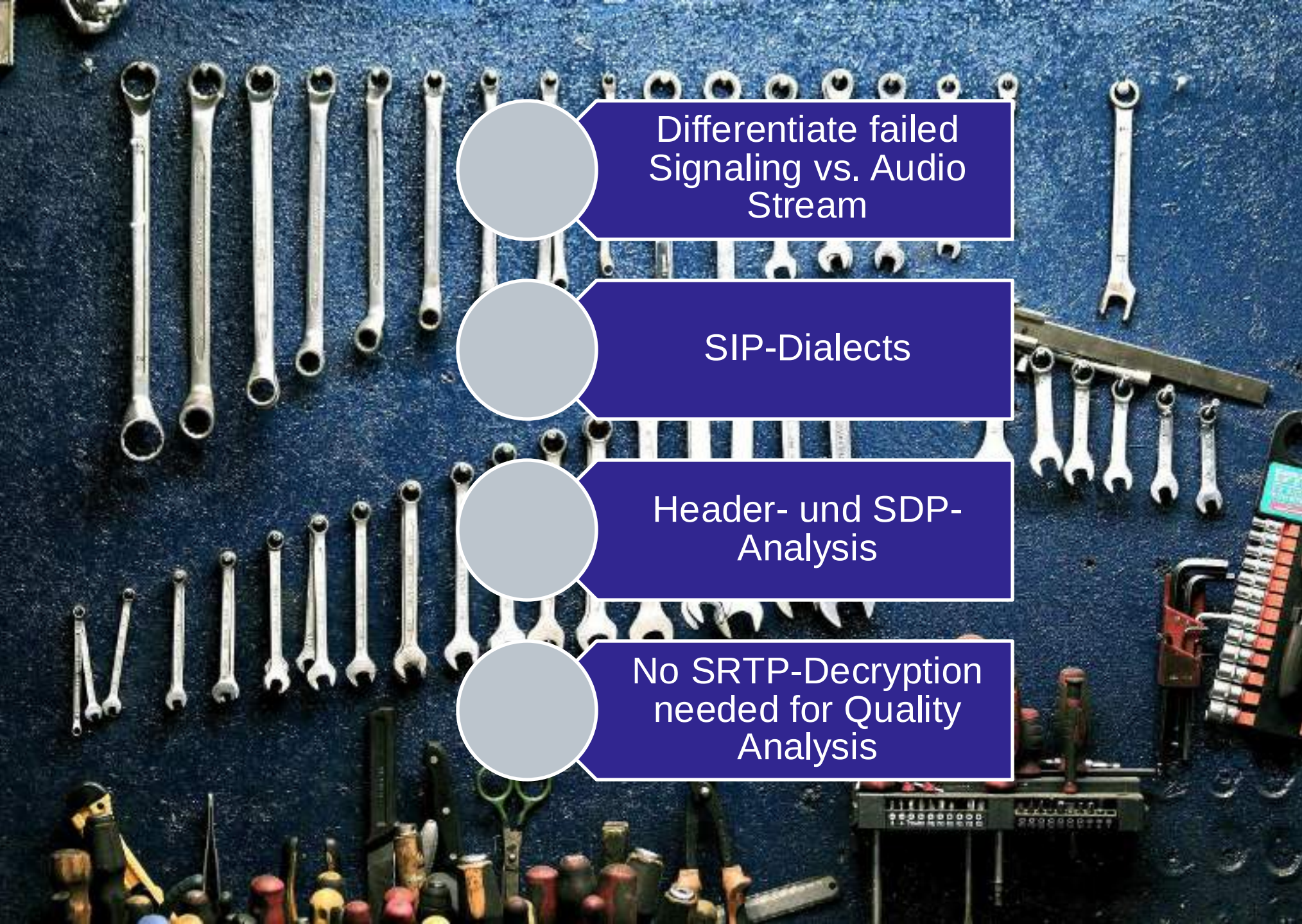
## Case 4

No outgoing  
Calls to  
External

Internal  
okay

Topology  
from Case  
1

# Lessons Learned



Differentiate failed  
Signaling vs. Audio  
Stream

SIP-Dialects

Header- und SDP-  
Analysis

No SRTP-Decryption  
needed for Quality  
Analysis

# Thanks

[linkedin.com/in/benjamin-pfister-90136b298](https://www.linkedin.com/in/benjamin-pfister-90136b298)



#sf25eu

# Sources

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