AGFEO

Wiki: Netzwerkanalysen mit AGFEO und Wireshark

AGFEO Wiki: Netzwerkanalysen mit Wireshark

Stand 22.01.2026LB

Alle Angaben ohne Gewähr!

Inhalt:

Vorwort
Die hier gezeigten Möglichkeiten eines Netzwerkmitschnitts zeichnen ausschließlich alle Datenpakete auf, die am Netzwerk-Interface der Anlage anliegen. Im Unterschied zu einem heute nicht mehr gebräuchlichen Netzwerk-*Hub*, stellt ein Netzwerk-*Switch* an den jeweiligen Switch-Ports ausschließlich Datenpakete zur Verfügung, die von diesem angefordert oder für diesen bestimmt sind. Soll demnach der komplette Netzwerk-Traffic mitgeschnitten werden, so ist *auf* dem Switch bzw. über einen sog. *Monitorport* (Mirror) mitzuschneiden.

> Wichtiger Hinweis:
> Für eine spätere Analyse von VoIP-Problemen durch AGFEO ist allein die Aufzeichnung direkt durch und mit dem AGFEO Kommunikationssystem wie nachfolgend gezeigt entscheidend!

Der Mitschnitt erfolgt somit sinnvollerweise direkt auf der Anlage:
Telefon.....ES/HV.....ROUTER/FIREWALL.....Provider

HyperFonie Cloud-Telefonanlage
Wird eine HyperFonie Cloud Telefonanlage verwendet, so sind dabei verschiedene Themen zu berücksichtigen:

- Ein Netzwerkmitschnitt schneidet nur die Daten der Telefonanlage mit
- Sollen Probleme eines lokalen Netzwerkgerätes analysiert werden, sind geeignete lokale Netzwerkmitschnittmassnahmen anzuwenden
- Jeglicher gerätebezogene Datenverkehr mit der HyperFonie Cloud-Telefonanlage ist durchgängig verschlüsselt

Datenschutz beachten!
Ein Netzwerkmitschnitt schneidet mitunter personenbezogene Daten (Gespräche, etc.) mit und ermöglicht somit u.a. das (spätere) Mithören von Verbindungen. Daher sind die jeweiligen

gesetzlichen Vorgaben und Pflichten, insbesondere zum Datenschutz und der Mitbestimmung etc. zu beachten!

Einstieg in den Umgang mit Netzwerkmitschnitten

Zur Auswertung von Netzwerkmitschnitten wird ein externes Software-Tool benötigt, genannt „*Wireshark*". Es ist ein kostenloses, äußerst leistungsstarkes PC-Tool.

Weitere Informationen dazu und Download unter www.wireshark.org.

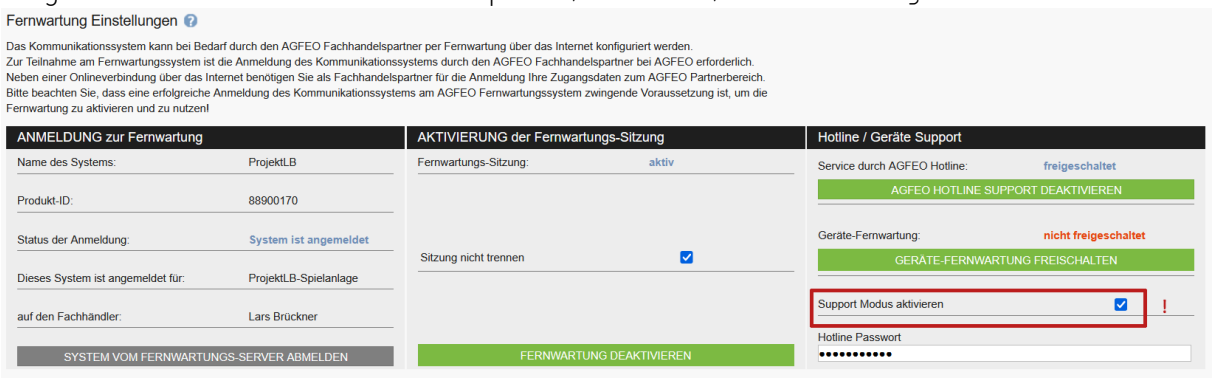
Externe Web-Seitenempfehlung:
Im Internet finden sich zahlreiche weitere Informationen zur Analyse und Aufbau von VoIP-Verbindungen mittels des Session-Initiation Protokolls. Als hervorragenden Einstieg möchten wir auf eine (amerikanische) Webseite verweisen, die sehr detailliert und mit verständlichen Beispielen die einzelnen Themen einer SIP Verbindung erklärt.

> Andrew Prokop – "How to be a SIP Rock Star"
> s.a. https://andrewjprokop.wordpress.com/2014/08/04/come-together-a-collection-of-articles-designed-to-make-you-a-sip-rock-star/

Unterschied Logging / Netzwerkmitschnitt

Ein Netzwerkmitschnitt zeichnet allein die Netzwerkdaten „vor" der Anlage auf, nicht jedoch den Programmablauf innerhalb der System-Firmware der Kommunikationssysteme. Für eine spätere, vollständige technische Analyse durch AGFEO ist es ergänzend notwendig die *Protokoll-Tiefe* der Anlagen zu erhöhen, so dass zusätzlich zum Netzwerkmitschnitt auch die Programmablaufroutinen des Kommunikationssystems aufgezeichnet werden.

Dazu ist der sog. `Support-Modus` zu aktivieren, der somit für erweiterte Log-Ausschriften sorgt. Die Funktion ist über den Menüpunkt `/Service/Fernwartung` erreichbar.



Wie wird ein Netzwerkmitschnitt erstellt?

Fall 1: Erstellung mit dem AGFEO Werkzeug

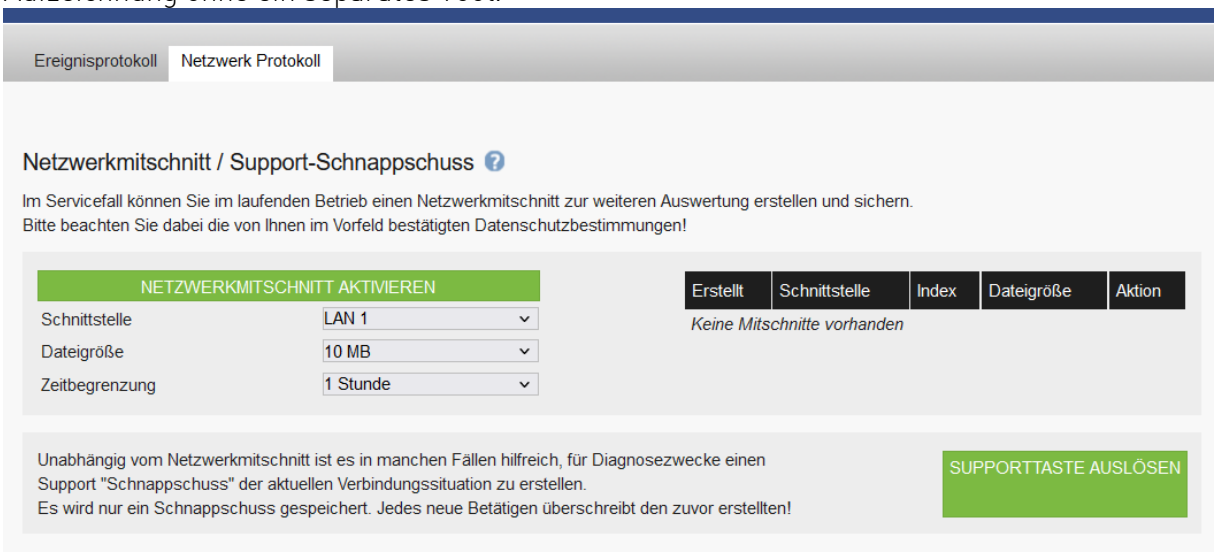
Das AGFEO Werkzeug kann über den AGFEO Partnerbereich geladen werden. Es steht für MS

Windows zur Verfügung und benötigt keine Installation. Die lancfg.exe kann direkt gestartet werden.

Vorteil: Möglichkeit des Live-Mitschnitts
(Direktes streamen zu einem installierten Wireshark)
Unabhängig der Speichergröße der Anlage (=größere Aufzeichnungsdauer)
Nachteil: Werkzeug muss im lokalen Netzwerk gestartet werden

Zum Aufrufen der Netzwerkaufzeichnungsoption ist die zuvor über eine Suche im AGFEO Werkzeug gefundene Anlage erst zu markieren und anschließend das *Ampelsymbol* anzuklicken. Im nachfolgenden Dialog ist dann der „Start" Button auszuwählen.

Fall 2: Erstellung über die TK-Anlagenkonfiguration
Jedes moderne AGFEO Kommunikationssystem bietet über die Webkonfiguration im Menüpunkt `/Service/Protokolle/Netzwerkmitschnitt` die Möglichkeit zur Aufzeichnung ohne ein separates Tool.



Vorteil: Nutzung auch ohne vor Ort Einsatz über die AGFEO Fernwartung möglich!

Nachteil: Kleinerer Zeitraum des Mitschnitts auf Grund begrenztem Speicher der Anlage.

Wie betrachtet man einen Netzwerkmitschnitt?
Die Datei-Endung für Netzwerkmitschnitte lautet im Normalfall .pcap oder .pcapng: Der Mitschnitt über die Anlagenkonfiguration ab FW 4.0a liefert dagegen die Dateiendungen pcap0 bzw. pcap1:

Empfehlung:
pcap* umbenennen zu pcap oder diese durch die Anlage indizierten Dateiendungen über die Mittel des verwendeten Betriebssystems ebenfalls mit der Wireshark-Anwendung verknüpfen

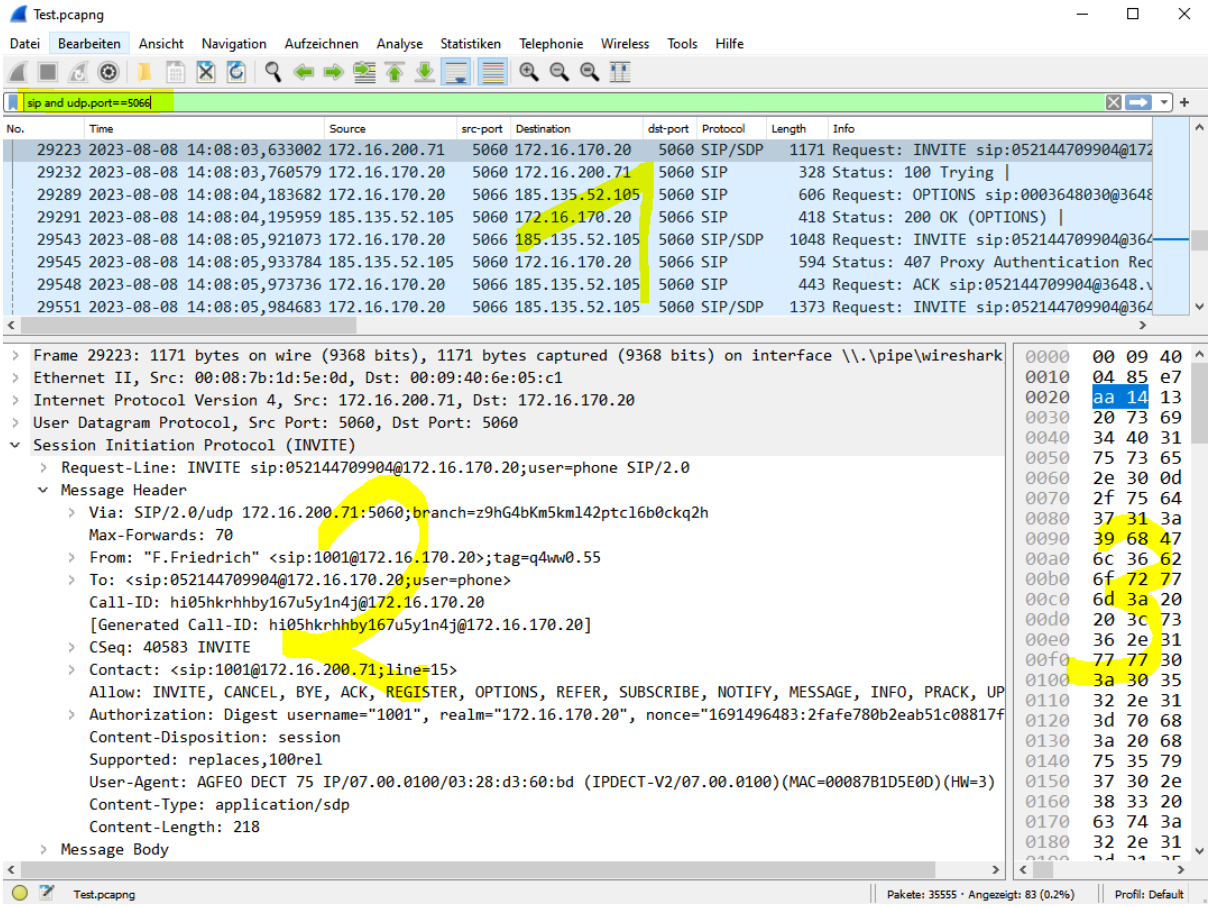
Entsprechende Mitschnitt-Dateien können dann im Nachgang über das Programm `Wireshark` (s.o.) geöffnet und analysiert werden.

Wurde im AGFEO Werkzeug vor dem Start der Aufzeichnung die Option "*direkt zu Wireshark streamen*" aktiviert wird ein lokal installiertes Wireshark-Programm gestartet, was dann ermöglicht die Aufzeichnung „live" zu analysieren.

Analyse eines Mitschnittes

Vorbereitungen und Filter

Wireshark – Arbeitsoberfläche – Aufteilung



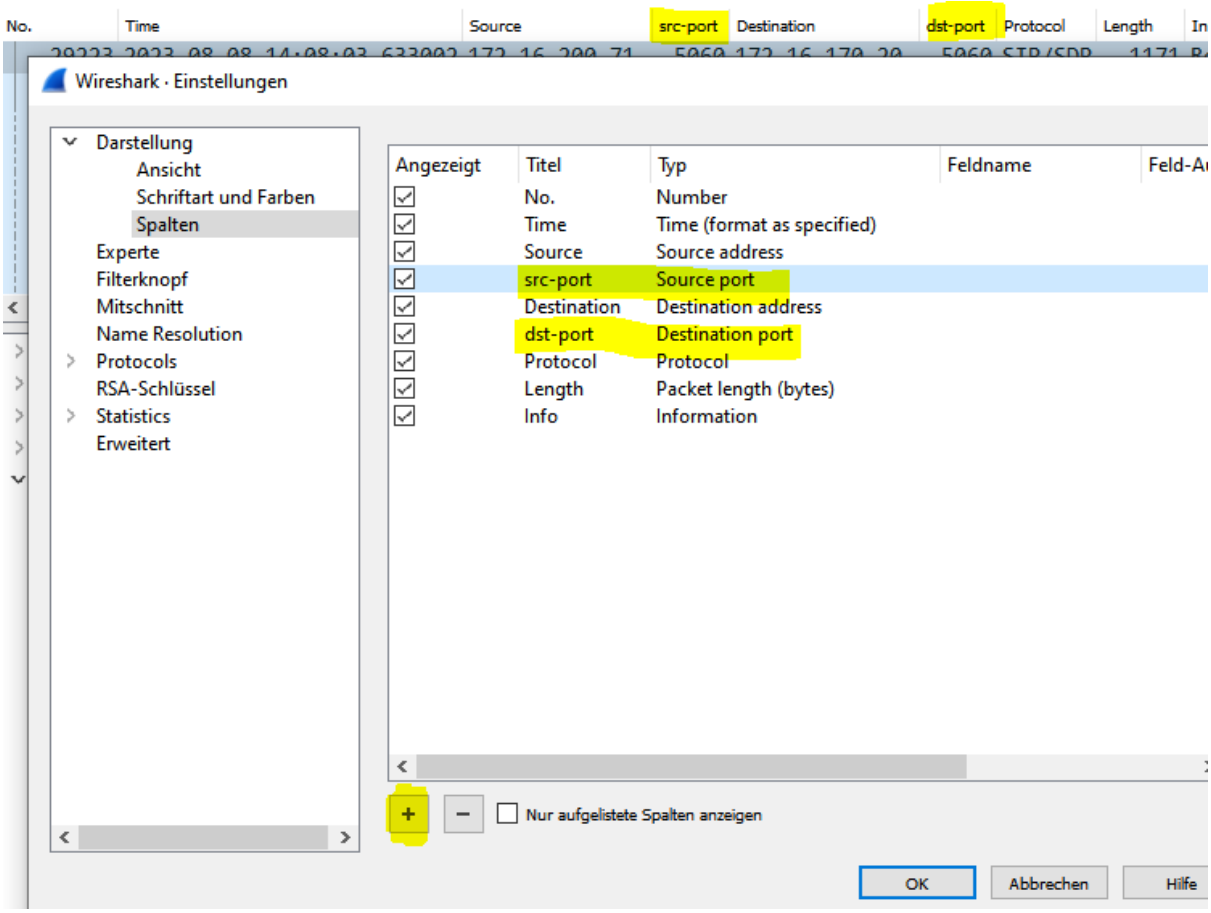
Fensteransichten
1 -> Liste mit allen Paketen entsprechend dem gesetzten Filter
2 -> Paket-Details
3 -> Paket-Hex-Dump

Oberhalb dieser Fensteransichten befindet sich eine Filter-Zeile (im obigen Screenshot gelb markiert und grün unterlegt). Durch Eingabe von Ausdrücken in diesem frei editierbaren Feld können die in den Fenstern jeweils dargestellten Pakete auf das Wesentliche bzw. hinsichtlich der Filtereingabe reduziert werden.

Zusätzliche Src-/Dst-Port-Spalten erstellen
…. macht es sehr viel übersichtlicher…:
Netzwerkkommunikation erfolgt anhand von IP-Adressen (=Hostangabe) und Ports (=Dienst). Um eine bessere VoIP Analyse in Wireshark zu ermöglichen, sollte zusätzlich noch die Angabe des jeweiligen Ports eingeblendet werden.

Dazu im Wireshark die *rechte* Maustaste auf die *Spaltentitel*-Zeile klicken und dann über das erscheinende Kontextmenu die *Spalteneigenschaft* auswählen. Danach dann über das *Plus*-Zeichen zunächst 2 neue `Spalten hinzufügen`. Danach diese jeweils markieren und dort durch Doppelklick auf das *Typ*-Feld dann `Source Port` = *Quellport* des Pakets und `Destination Port`= *Zielport* des Paketes ergänzen (hinterher ggf. an die richtige Spaltenstelle verschieben).

Angezeigt wird dann auch noch der jeweilige Host-Port.



Hinweis:
Auf diese Art und Weise lässt sich auch die genaue Uhrzeit des Aufzeichnungs-Zeitpunktes jedes einzelnen Pakets einblenden. Besonders interessant, wenn die Kunden einen konkreten Zeitbezug des Problems benennen können.

Filter
Durch Filter werden die Datenanzeige auf das Wesentliche reduziert. Diese können z.B. über das Filter-Feld (s.o.) eingegeben werden.

Beispiele für Filterausdrücke

```
sip
ip.addr==192.168.x.x
rtp
udp.port==5066
classicstun
stun
dns
sip.Call-ID== ..
```

Filterausdrücke sind logisch kombinierbar:

```
and / or / not
```

bzw. `&& / || / !`

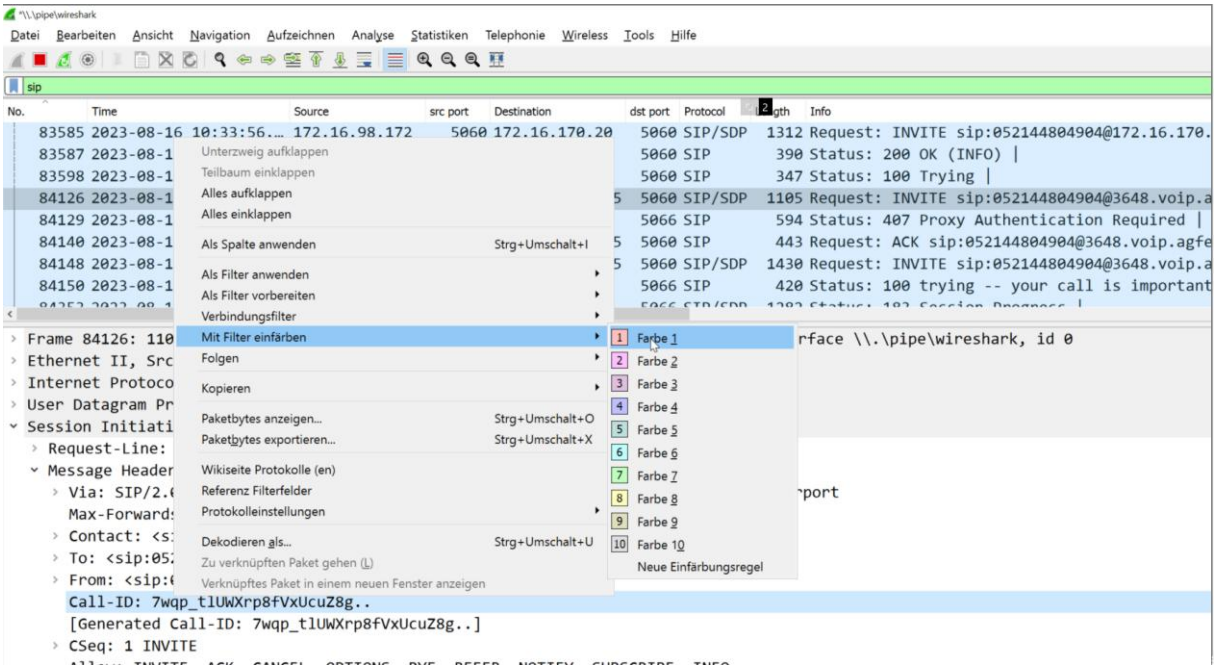
Beispiel 1 einer Filterkombination: `(sip and udp.port==5066) || rtp`
Hierdurch werden alle SIP-Pakete des SIP-Kontos mit dem lokalen SIP-Port 5066, aber auch alle RTP-Sprach-Pakete angezeigt.

Beispiel 2 einer Filterkombination: `sip and !sip.CSeq.method==OPTIONS`
AGFEO TK-Systeme senden alle 30 Sekunden ein SIP Options Paket. Durch die Häufigkeit dieser Meldungen wird die Durchsicht des Netzwerkmitschnitts im Wireshark zunächst recht unübersichtlich. Mit diesem Filter werden nur noch alle anderen SIP Meldungen aufgelistet.

TIPP 1:
Filter können manuell in der Filterzeile angegeben werden oder über die *rechte Maustaste* auf einen Parameter z. B. im *SIP-Message - Header*, z. B. *Call-ID*:
`Als Filter auswählen bzw. vorbereiten` -> Das "Ausgewählte"

TIPP 2:
Die Call-ID fasst alle SIP-Nachrichten zusammen, die zu einem bestimmten Ruf (Call) gehören!

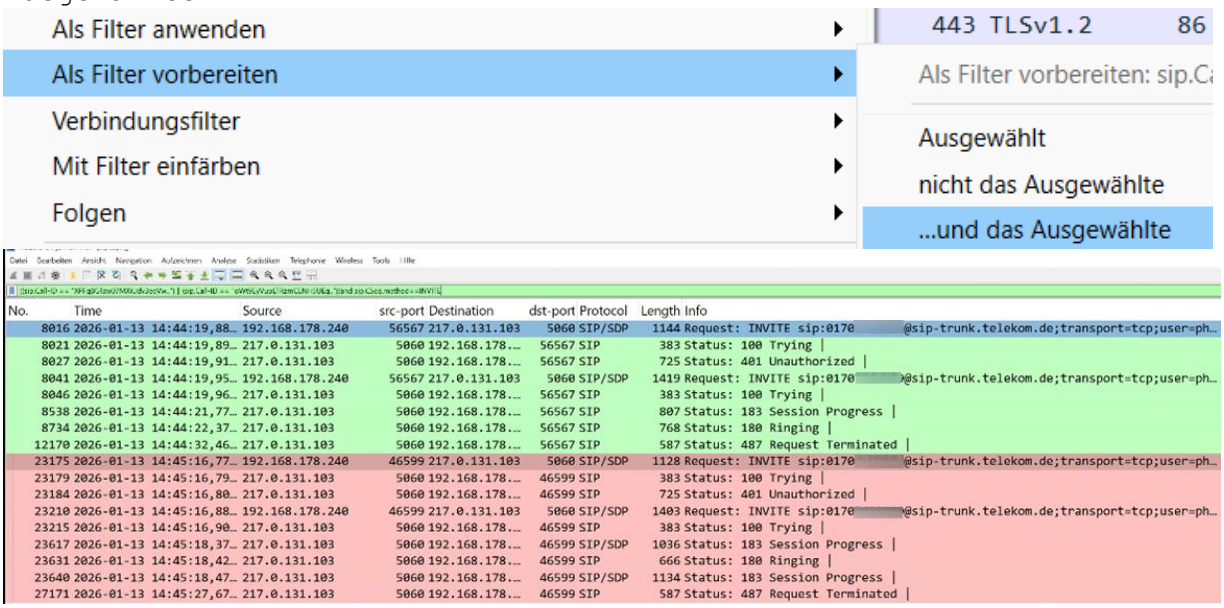
TIPP 3: Will man alle SIP-Nachrichten des bestimmten Rufes "einfärben", dann geht das ebenfalls über die rechte Maustaste auf die Call-ID und anschließend -> "Mit Filter einfärben"



TIPP 4: Vergleichen von Verbindungen

Wireshark bietet Möglichkeiten verschiedene Filter intelligent zu verknüpfen, so dass man z.B. leicht einen Gutfall mit einem Schlechtfall vergleichen kann.

Dazu wieder die Call-ID der verschiedenen INVITES verwenden. Jedoch beim ersten Mal nur die Funktion `als Filter vorbereiten` auswählen und dann erst beim zweiten INVITE Paket die Funktion `als Filter anwenden` mit der dortigen Unterfunktion …`und das Ausgewählte` nutzen.

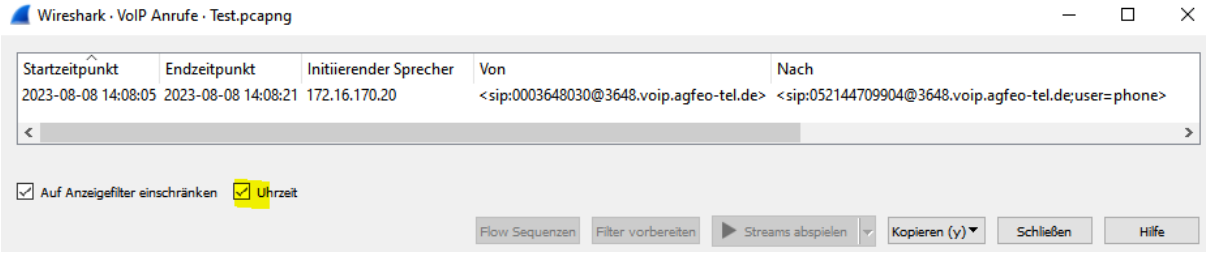


Wireshark filtert dann auf die beiden CallIDs und stellt somit diese beiden übersichtlich dar. Wenn man nun noch beide CallIDs farbig über die Filterfunktion `Mit Filter einfärben` unterschiedlich einfärbt, kann man beide Verbindungen sehr gut vergleichen.

Erster Überblick

`Menü -> Telefonie -> Voip Anrufe`

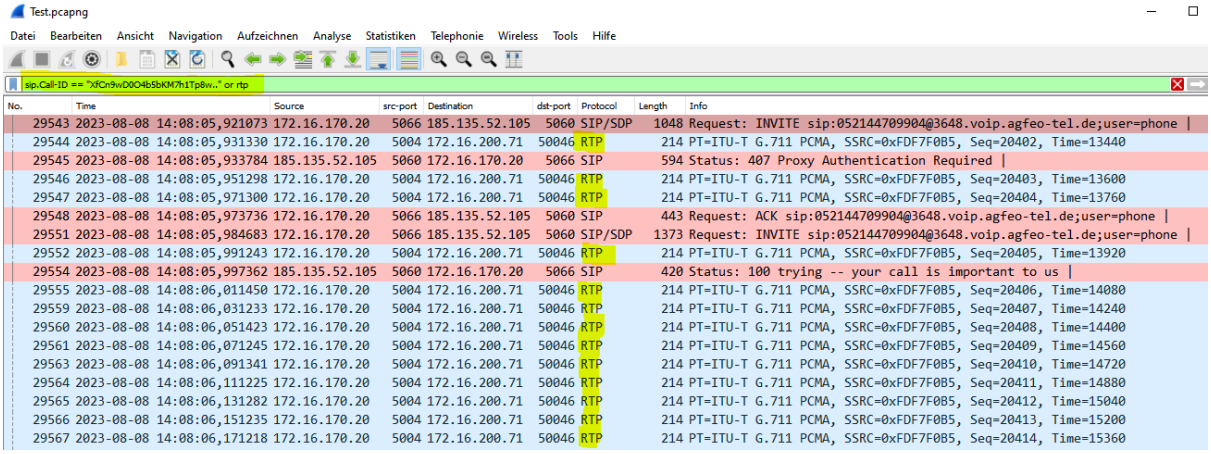
Zeigt eine Auflistung aller im Mitschnitt enthaltenen vollständigen SIP Anrufe.



Auftrennung in SIP und RTP

Bei einem VoIP-Anruf werden die Signalisierungsdaten (verglb. ISDN D-Kanal) von den eigentlichen Sprachdaten (verglb. ISDN B-Kanal) durch die Nutzung unterschiedlicher Protokolle getrennt!

Signalisierung: `SIP`
Sprache: `RTP`



Der Screenshot zeigt aus dem Mitschnitt mittels FILTER-Funktion separierte SIP- und RTP-Daten an. Alle Einträge, die zu einem bestimmten Ruf gehören, sind wie zuvor beschrieben rot eingefärbt!

Neben den SIP-Nachrichten dieser Verbindung erkennt Wireshark die zugehörigen Sprachpakete, die NICHT als SIP-Pakete, sondern als sog. *RTP-Pakete* übertragen werden! Damit es während der Übertragung von RTP Daten nicht zu unnötigen Verzögerungen und Overhead kommt, werden diese idR. stets mittels *UDP* und damit *verbindungslos* und nicht zusätzlich abgesichert übertragen. Dies ist zwar Voraussetzung für eine möglichst zügige Übertragung, führt aber mitunter zu einer gestörten Gesprächsqualität (s.u.).

Analyse von AGFEO IP Systemtelefonen

AGFEO IP-Systemtelefone nutzen nicht SIP, sondern ASIP als proprietäres Protokoll. Hierbei wird zur Sprachübertragung ebenfalls das RTP-Protokoll (stets über den UDP Port 5896) und zur Signalisierung stets der TCP-Port 5904 verwendet. Mit entsprechenden Filtern auf die IP

und/oder Port und anschließender Umkodierung der UDP Portpakete auf RTP lassen sich die Sprachdaten auch anhören und ebenfalls über Wireshark analysieren.

Der Filter lautet demnach:
tcp.port==5904 or udp.port==5896

Mit diesem Filter sieht man somit die die Signalisierung (TCP) und die Sprechwege (UDP) von AGFEO IP-Systemtelefonen der ST4x IP und ST5x IP Serie. Um RTP-Analysen der Sprachpakete vorzunehmen, sind zunächst die UDP-Rahmen über Kontextmenü ("rechte Maustaste) als RTP zu dekodieren.

DNS und SIP – häufige Ursache für Registrierungs- und Gesprächsprobleme
SIP-Kommunikation ist in hohem Maß von einer korrekt funktionierenden DNS-Auflösung abhängig. Kann ein SIP-Server nicht oder nur unzuverlässig aufgelöst werden, ist weder eine erfolgreiche Registrierung noch ein stabiler Gesprächsaufbau möglich.

Zur Analyse von DNS-Vorgängen in Wireshark kann folgender Filter verwendet werden

dns

Damit lassen sich sowohl DNS-Anfragen (request) als auch die zugehörigen Antworten (response) übersichtlich darstellen.

DNS A-Records vs. DNS SRV-Records
DNS A-Records
Ein A-Record liefert eine direkte konkrete IP-Adresse zu einem Hostnamen.
Bei SIP bedeutet dies, dass das Endgerät immer genau diesen einen Server anspricht.

DNS SRV-Records
DNS SRV-Records werden von vielen SIP-Providern genutzt, um:
- Mehrere SIP-Server bereitzustellen
- Zur Lastverteilung
- Erhöhung der Ausfallsicherheit

Ein SRV-Record enthält zusätzlich:
- Priorität
- Gewichtung (Weight)
- Mehrere Zielhosts und jeweiligen Port

Das Endgerät entscheidet dann anhand dieser Angaben, welcher Server der DNS SRV-Response zuerst angesprochen wird. Ggf. erfolgt im Nachgang dann ein DNS A-Record Request, sofern der zu verwendene Zielhost nicht als IP-Adresse übermittelt wurde.

Praxisprobleme mit DNS SRV
In der Praxis treten mit DNS SRV häufig Probleme auf, insbesondere wenn Provider:
- einen Server mit höchster Priorität ausliefern, der jedoch nicht erreichbar oder fehlerhaft ist

- mehrere Server mit derselben (höchsten) Priorität aber unterschiedlicher Gewichtung liefern und dann nicht damit zurecht kommen, wenn die Server entsprechend ihrer Gewichtung verwendet werden
- während einer laufenden Verbindung erneut DNS-Abfragen durchführen und dabei auf einen anderen Server wechseln

Letzteres kann dazu führen, dass:
- RTP-Ströme abbrechen
- Gespräche unerwartet beendet werden
- Sprachverbindungen einseitig ausfallen

Solche Effekte sind im Wireshark gut erkennbar, wenn DNS-Antworten zeitlich mit Gesprächsabbrüchen oder Neuaufbauten zusammenfallen.

DNS NAPTR-Records im SIP-Umfeld
DNS NAPTR-Records werden von dem SIP Stack eines AGFEO Kommunikationssystems immer dann genutzt, um festzulegen, welches Transportprotokoll (z. B. UDP, TCP, TLS) und welcher SIP-Dienst verwendet werden soll, wenn nicht vor vornherein eine gesicherte (TCP) oder verschlüsselte (TLS) SIP-Verbindung genutzt werden soll. NAPTR-Records werden dabei häufig vor DNS SRV-Records abgefragt.

Ist ein NAPTR-Record vorhanden, entscheidet er darüber, ob und welche SRV-Abfragen anschließend erfolgen. Fehlerhafte oder unvollständige NAPTR-Einträge können daher dazu führen, dass trotz vorhandener und funktionierender SRV- oder A-Records keine SIP-Registrierung zustande kommt.

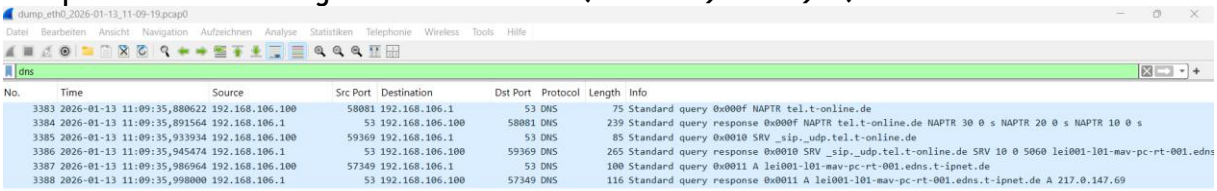
Zur Analyse von NAPTR-Abfragen in Wireshark kann ebenfalls der Filter

dns

verwendet werden. Bleiben nach einer DNS-Antwort weitere SRV- oder A-Abfragen aus, kann dies auf ein Problem in der NAPTR-Auflösung hindeuten.

Hinweis:
Nicht alle SIP-Provider nutzen NAPTR-Records. In vielen Umgebungen erfolgt die SIP-Auflösung direkt über SRV- oder A-Records.

Beispiel: DNS-Auflösung eines SIP-Servers (NAPTR → SRV → A)



Der dargestellte Wireshark-Mitschnitt zeigt eine vollständige DNS-Auflösungskette, wie sie bei vielen SIP-Providern üblich ist. Gefiltert wurde auf *dns*, sodass ausschließlich DNS-Anfragen und -Antworten sichtbar sind.

1. Zunächst erfolgt von der Telefonanlage (192.168.106.100) eine *DNS-NAPTR*-Abfrage auf die Domain des SIP-Providers (tel.t-online.de).

2. Anscheinend ist der Router 192.168.106.1 dort als DNS Server eingetragen. In seiner Antwort liefert der DNS-Server mehrere NAPTR-Einträge mit unterschiedlichen Prioritäten. Diese legen fest, welche Art der weiteren Auflösung verwendet wird und welche SIP-Dienste grundsätzlich zur Verfügung stehen.
3. Im nächsten Schritt folgt von der TK-Anlage eine *DNS-SRV*-Abfrage (_sip._udp.tel.t-online.de).
4. Der DNS-Server antwortet mit einem konkreten SIP-Servernamen (lei001-101-mav-pc-rt-001.edns.t-ipnet.de) sowie dem zugehörigen Port (5060).
5. Hierzu wird dann ein DNS A Request erzeugt, der dann 217.0.147.69 als konkrete IP Adresse des am höchst gewichtetsten und priorisiertesten Servers ausliefert.

Abschließend wird also für den durch SRV ermittelten Hostnamen eine DNS-A-Abfrage durchgeführt. Erst diese liefert die konkrete IP-Adresse des SIP-Servers, über die anschließend die SIP-Registrierung und der Gesprächsaufbau erfolgen. Anhand der erhaltenen SRV-Informationen entscheidet also die TK-Anlage bzw. SIP-Endgerät, welcher SIP-Server bevorzugt angesprochen wird.

Wichtiger Praxis-Hinweis
An diesem Ablauf lässt sich gut erkennen, dass SIP idR. nicht direkt mit einer IP-Adresse startet, sondern mehrere DNS-Schritte durchläuft. Fehler oder Inkonsistenzen in NAPTR- oder SRV-Antworten können daher dazu führen, dass:

- keine SIP-Registrierung zustande kommt
- ein nicht erreichbarer SIP-Server bevorzugt ausgewählt wird
- bei erneuten DNS-Abfragen während des Betriebs ein Serverwechsel erfolgt

Solche Situationen können im laufenden Betrieb zu Gesprächsabbrüchen oder einseitiger Sprachübertragung führen und sind im Wireshark anhand zeitlich zusammenfallender DNS- und SIP-Ereignisse gut nachvollziehbar.

Bei unerklärlichen SIP-Registrierungsproblemen oder Gesprächsabbrüchen sollte daher stets vorab geprüft werden:

- ob der DNS Server angesprochen werden kann
- ob DNS-Antworten überhaupt erfolgen
- ob A- oder SRV-Records verwendet werden
- welche Server mit welcher Priorität ausgeliefert werden
- ob DNS-Auflösungen während laufender Gespräche stattfinden

⇨ Gerade bei SIP-Problemen gilt:
Nicht erreichbare oder falsch priorisierte DNS-Ziele führen zu denselben Symptomen wie Netzwerk- oder Provider-Störungen.

Praxis: REGISTER

Wozu Registrieren?
-> Registrierung, um Gespräche empfangen zu können
-> SIP-Konto wird beim Provider daraufhin als AKTIV betrachtet.

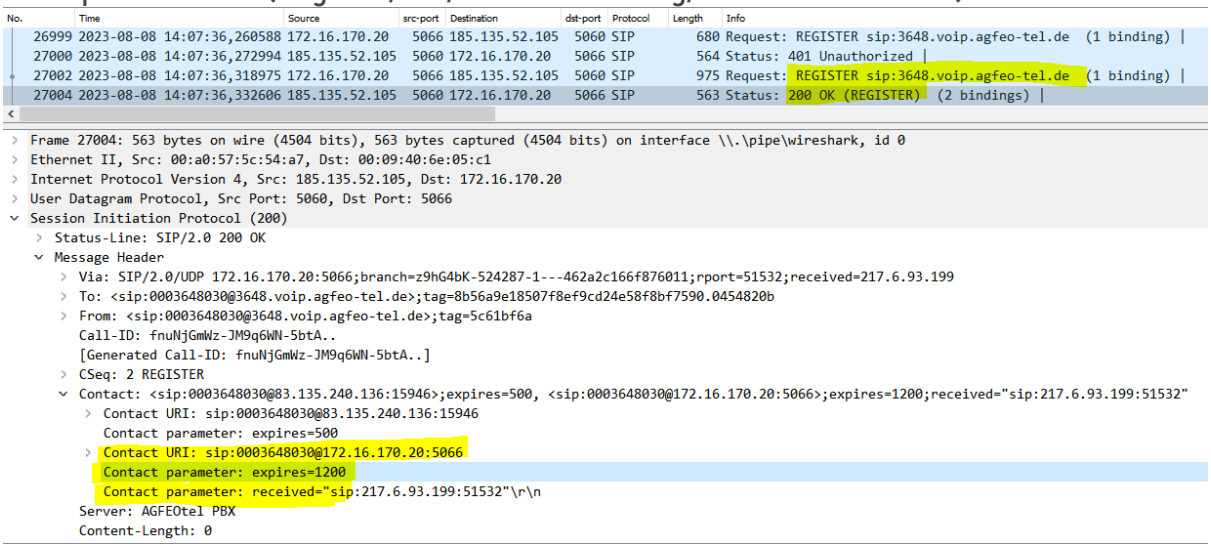
Wo der Provider beim ankommenden Ruf das INVITE hinschicken soll, wird ihm über die IP-Adresse im `Contact` Parameter mitgeteilt.

Gültigkeit einer Registration
Die Registrierung muss aufrechterhalten werden! -> `expire`-Parameter. So lange ist die Registrierung beim Provider gültig! Innerhalb dieser Zeit muss eine Re-Registrierung erfolgen.

Regelmäßige Neu-Registrationen vor Ablauf der Gültigkeit notwendig!
Innerhalb dieses Zeitraums besteht zwischen SIP Server/Registrar und SIP-Client/Endgerät KEINE Verbindung.

➔ Jede Instanz „glaubt" in dieser Zeit somit nur, dass die andere Seite noch da / aktiv ist!

Prinzipieller Ablauf (Register/401/Authentifizierung/Contact-Parameter)



1. REGISTER (ohne Authentifizierung)
   Das Endgerät meldet sich beim Provider und teilt mit, unter welcher Adresse es erreichbar ist.

2. 401 Unauthorized (mit Senden eines NONCE-Wertes)
   Der Provider fordert die Authentifizierung an und übermittelt dazu einen einmalig gültigen NONCE-Wert.

3. REGISTER (mit Authentifizierung und NONCE)
   Das Endgerät verwendet genau den im vorherigen 401 übermittelten NONCE-Wert, um daraus zusammen mit *Benutzername* und *Kennwort* die Authentifizierungsdaten zu

berechnen. Die berechneten Zugangsdaten werden dabei nicht im Klartext, sondern als Hashwert im Authorization-Header des REGISTER übertragen. Der NONCE selbst wird nicht verändert, sondern ausschließlich zur Berechnung dieser Antwort verwendet.

4. Contact-Parameter
   Enthält IP-Adresse und Port, unter denen das Endgerät Anrufe empfangen kann.

5. 200 OK
   Die Registrierung ist erfolgreich abgeschlossen und für die angegebene Zeit gültig.

Typischer Fehlerfall: Endlosschleife REGISTER / 401
Tritt im Mitschnitt eine fortlaufende Abfolge von REGISTER und 401 Unauthorized auf, wurde die Authentifizierung nicht erfolgreich abgeschlossen. Häufige Ursachen sind:

- falscher Benutzername (führt meistens zu Fehler 404)
- falsches Kennwort (führt meistens zu Fehler 403)
- Zeitabweichungen zwischen Endgerät und Provider
- Manipulation der SIP-Nachrichten durch Firewall oder SIP-ALG
- abgelaufener oder vom Endgerät nicht korrekt übernommener NONCE)

⇨ Solange keine erfolgreiche Authentifizierung erfolgt, bestätigt der Provider die Registrierung nicht mit 200 OK und das SIP-Konto gilt als nicht erreichbar.
⇨ Typisch für 401 - Wiederholung: Das aufgrund des Authorisierungsheaders längere INVITE nach einem 401 wird von Router mit fehlerhafter MTU-Ermittlung geblockt

TIPP: Erst de-registrieren, dann aufzeichnen!
==> In vielen Fällen ist es sinnvoll in einem Netzwerkmitschnitt auch die SIP-Registration aufzuzeichnen, da der anschliessende SIP-Datenverkehr mitunter Bezug dazu nimmt. Bei Problemen mit dem SIP Amt daher sinvollerweise vor Start der Aufzeichnung das externe SIP Konto deaktivieren, nun den Netzwerkmitschnitt starten und erst danach das SIP Konto wieder aktivieren. Bei Analysen zu SIP Geräten dann ähnlich verfahren.

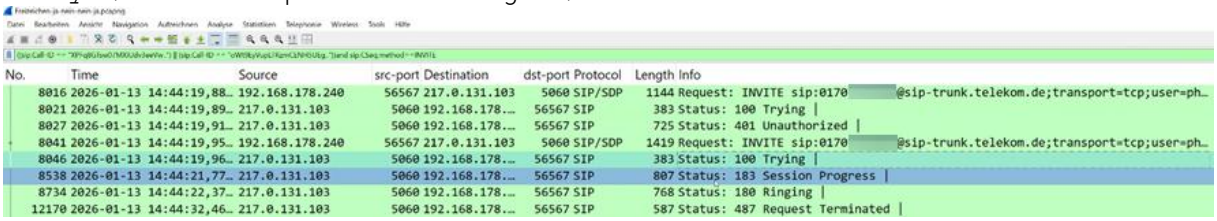
Anmerkungen zu STUN-Server/RPORT
Wird ein STUN-Server oder RPORT verwendet, wird im `Contact` Parameter die *externe* IP-Adresse eingetragen. Ohne STUN/RPORT kann im Contact Parameter dagegen nur die *lokale* IP-Adresse eingetragen werden. Von extern wären diese lokalen Adressdaten allerdings nicht erreichbar!

Bei den meisten Providern ist es deshalb gängige Praxis, dass sie in diesem Fall die IP-Adresse und den Port verwenden, von wo aus das REGISTER zum Provider gesendet wurde. Solche Provider benötigen dann KEINEN STUN-Server-Eintrag bzw. RPORT-Mechanismus.

Bei Providern, die keinen STUN-Server-Eintrag und keinen RPORT-Mechanismus benötigen, stehen im SDP (s. u. "Aushandlung der Sprechverbindung" weiter unten) die LOKALEN Adressdaten (IP-Adresse und Port). Die Provider fangen hierbei dann erst mit dem Senden von RTP-Daten an, wenn diese welche zuvor von der TK-Anlage empfangen. Vorher wissen die Provider nicht, wohin die Pakete gesendet werden sollen.

Praxis: Verbindungsaufbau

Der Verbindungsaufbau folgt einem bestimmten Ablauf. Dabei werden bestimmte SIP-Nachrichten verwendet. Die Reihenfolge kann dabei mitunter jedoch unterschiedlich sein, wie auch je nach Provider bestimmte SIP Meldungen manchmal gar nicht verwendet werden. Jedoch beginnt ein Verbindungsaufbau an sich immer mit einem `INVITE`. Die Gegenseite beantwortet diese Verbindungs-Einladung wie beim Register-Vorgang idR. mit einer Ablehnung (`401 Unauthorized`) und sendet dabei einen erneuten `NONCE`-Wert. Im Anschluss wird dann ein neues `INVITE` inkl. auf Basis des neuen `NONCE`-Werts passend angepassten Credentials erzeugt. Dieses wird dann entsprechend zugestellt. In der Folge kann die Gegenseite dann SIP 100er Meldungen wie zB. ein `100 Trying`, `180 Ringing` und/oder auch ein `183 Session Progress` senden. Diese können, müssen aber nicht per `ACK` bestätigt werden (abhängig vom PRACK-/100rel Verfahren). Bei Annahme der Verbindung kommt es dann idR. zu einem `200 OK`. Wird jedoch vorher aufgelegt, so kommt es mitunter zu einem `487 Request Terminated`. Wird das Gespräch beendet, so gibt es ein `Bye` (meist ohne spezielle Code-Angabe).



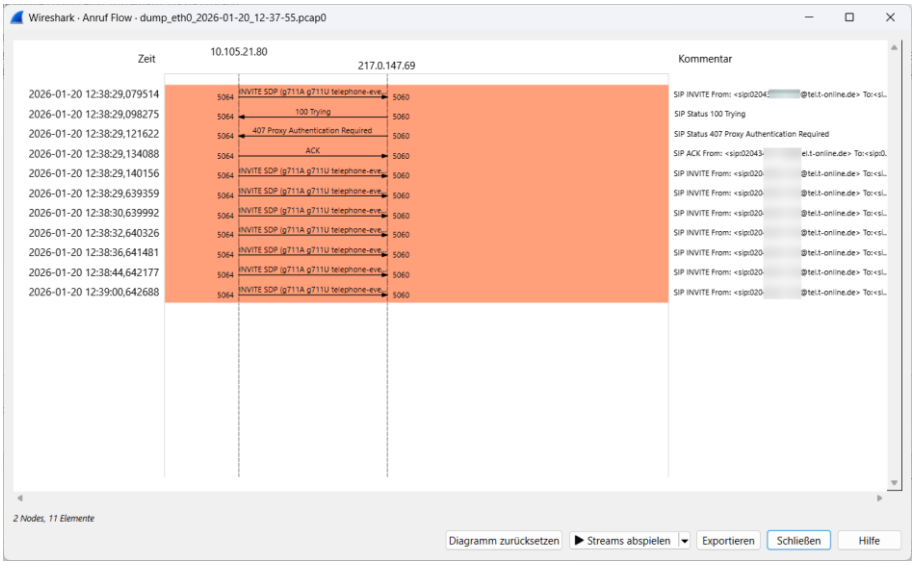
No.	Time	Source	src-port	Destination	dst-port	Protocol	Length	Info
8016	2026-01-13 14:44:19,88…	192.168.178.240	56567	217.0.131.103	5060	SIP/SDP	1144	Request: INVITE sip:0170 [redacted] @sip-trunk.telekom.de;transport=tcp;user=ph…
8021	2026-01-13 14:44:19,89…	217.0.131.103	5060	192.168.178.…	56567	SIP	383	Status: 100 Trying |
8027	2026-01-13 14:44:19,91…	217.0.131.103	5060	192.168.178.…	56567	SIP	725	Status: 401 Unauthorized |
8041	2026-01-13 14:44:19,95…	192.168.178.240	56567	217.0.131.103	5060	SIP/SDP	1419	Request: INVITE sip:0170 [redacted] @sip-trunk.telekom.de;transport=tcp;user=ph…
8046	2026-01-13 14:44:19,96…	217.0.131.103	5060	192.168.178.…	56567	SIP	383	Status: 100 Trying |
8538	2026-01-13 14:44:21,77…	217.0.131.103	5060	192.168.178.…	56567	SIP	807	Status: 183 Session Progress |
8734	2026-01-13 14:44:22,37…	217.0.131.103	5060	192.168.178.…	56567	SIP	768	Status: 180 Ringing |
12170	2026-01-13 14:44:32,46…	217.0.131.103	5060	192.168.178.…	56567	SIP	587	Status: 487 Request Terminated |

Entscheidend für die spätere Sprachverbindung ist dann hierbei die Übermittlung von RTP-Kommunikationsparametern im sog. Session Description Protocoll (SDP).

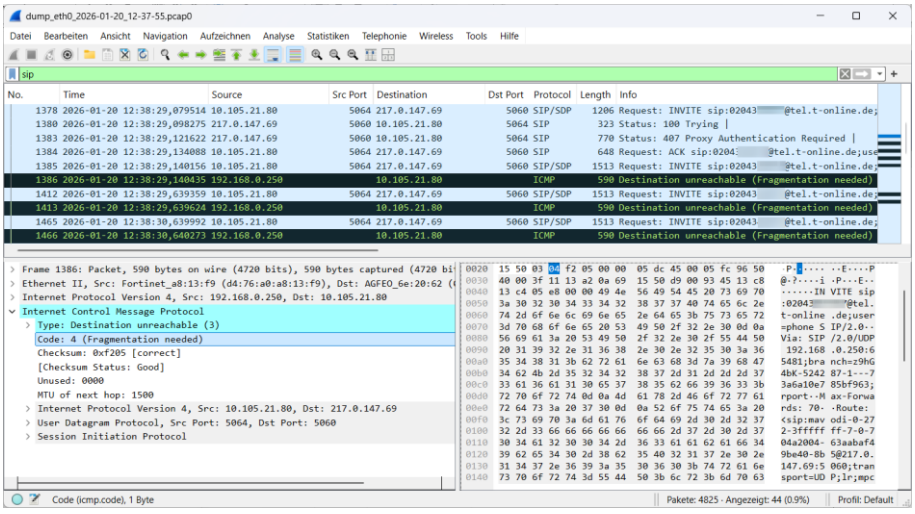
Typischer Fehlerfall: Endlosschleife INVITE
Tritt im Mitschnitt eine fortlaufende Anzeige des Verbindungsaufbaus (SIP INVITE-Nachrichten) auf, so ist der Datenaustausch mit und zum Provider gestört. Dies kann vielfältige Ursachen haben. So z.B. ein mangelhaftes DNS Ergebniss, falsches Routing, Blockaden durch Firewall-Systeme oder auch komplexere Ursachen wie eine fehlerhafte oder fehlende Fragmentierung.

Das nachstehende Bild zeigt die Analyse der Abläufe auf SIP Protokollebene. Die TK-Anlage kommuniziert initial auch mit dem Provider. Nach Aufnahme des NONCE durch die initiale Provider-Ablehnung (407) versucht die Anlage dann erneut den Provider passend zu kontaktieren. Da kein Datenaustausch vorgenommen werden kann, werden dazu zahlreiche weitere Versuche [vergeblich] vorgenommen.

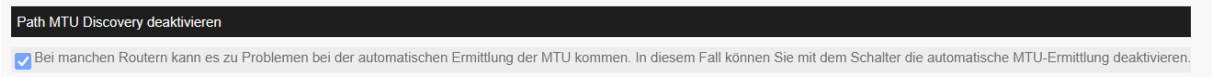
Es gilt nun also nicht nur die SIP Kommunikation, sondern bereits den vorgelagerten Verbindungsaufbau umfassend zu analysieren.



Erst die weitere Analyse des Datenverbindungsaufbaus zeigt dann die Ursache in einer mangelhaften Fragmentierung des Netzwerks (Meldung in schwarzen Zeilen: „`Destination unreachable, Fragmentation needed`“). Die von der Anlage versendeten SIP Daten verlassen somit schon nicht das lokale Netzwerk und erreichen den Provider gar nicht.



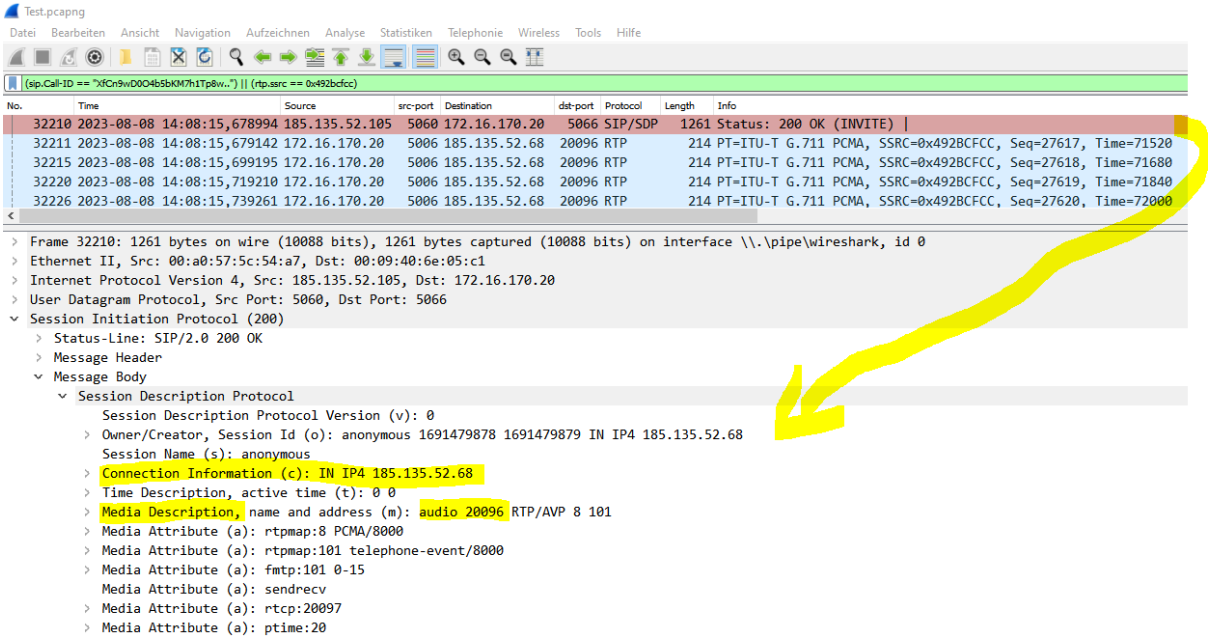
TIPP:
AGFEO TK-Systeme verfügen über eine Möglichkeit das Verhalten bzgl. einer Fragemtierung beeinflussen zu können. Dazu kann in solchen Fällen im Menüpunkt /Hardware/Netzwerkeinstellungen die dortige Checkbox `Path MTU Discovery deaktivieren` mal testweise aktiviert werden. In Abhängigkeit der verwendeten Netzwerkkomponenten funktioniert dann danach ggf. der Aufbau der Datenverbindung. Ansonsten sind weitere Analysen auf Seite der Kundenkomponenten notwendig.



Aushandlung der Sprechverbindung
Die Übermittlung erfolgt im *Message Body* der SIP-Nachricht
-> `Session Description Protocoll` (`SDP`) z.B. im INVITE, 183 Session Progress

und/oder 200OK. Hierüber werden die aufzubauenden konkreten Multimediadatenströme definiert. Es dient also dazu die Kommunikationsparameter des RTP Streams genauer zu definieren und legt dabei z.B. die möglichen Parameter der RTP-Sprachdaten fest. Beide Geräte müssen hierzu dann entsprechend kompatibel sein.

Das AGFEO Kommunikationssystem teilt dem Provider im INVITE die *IP-Adresse* und den *Port* mit, wo der Provider die RTP-Pakete hinsenden soll. Umgekehrt teilt der Provider spätestens im 200OK mit, wo das TK-System die RTP-Daten hinsenden müssen. Die SDP Daten finden sich im `Message Body` eines solchen SIP Paketes.



Der Wert der `Connection Information` gibt somit dem Gegenüber die *„Sende-die-Pakete-hierhin-IP-Adresse"* mit (Beispiel: 185.135.52.68), während der dabei dann anzusprechende Port in der `Media Description` als `audio` angegeben ist (Beispiel: 20096).

Die `Media Attributes (a=)` beschreiben die technischen Eigenschaften der in der Media Description angegebenen Payload-Typen. Dabei wird festgelegt, welche Codecs bzw. Zusatzfunktionen sich hinter den dort genannten Nummern verbergen.

Im gezeigten Beispiel bedeutet dies:

Payload-Typ 8 → PCMA (G.711 A-law), 8000 Hz
Payload-Typ 101 → telephone-event, 8000 Hz (DTMF-Signale)

⇨ Erst durch die Media Attributes ist somit eindeutig definiert, wie die übertragenen RTP-Sprachpakete zu interpretieren sind.

Fragestellung: Wer erzeugt das Freizeichen - ?!
Wenn die Gegenseite auf eine INVITE Anfrage auch eine Session Description (SDP) in einer Antwort (z.B. im 183 Session Progress) mitsendet, so sind die Rahmenparameter für die eigentliche Sprachverbindung übermittelt. In diesem Fall schaltet die Telefonanlage auf den

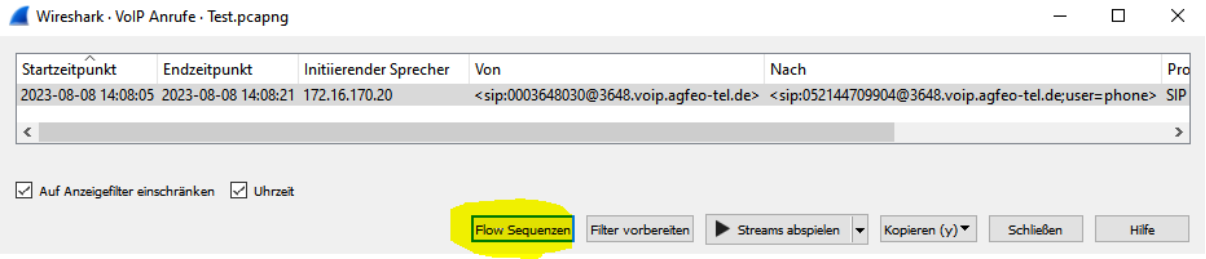
RTP-Datenstrom der Gegenseite um. Daher wird dann das Freizeichen von der Gegenseite übermittelt.

Fehlen in den Antworten der Gegenseite noch die SDP-Informationen, erzeugt dagegen die Telefonanlage das Freizeichen.

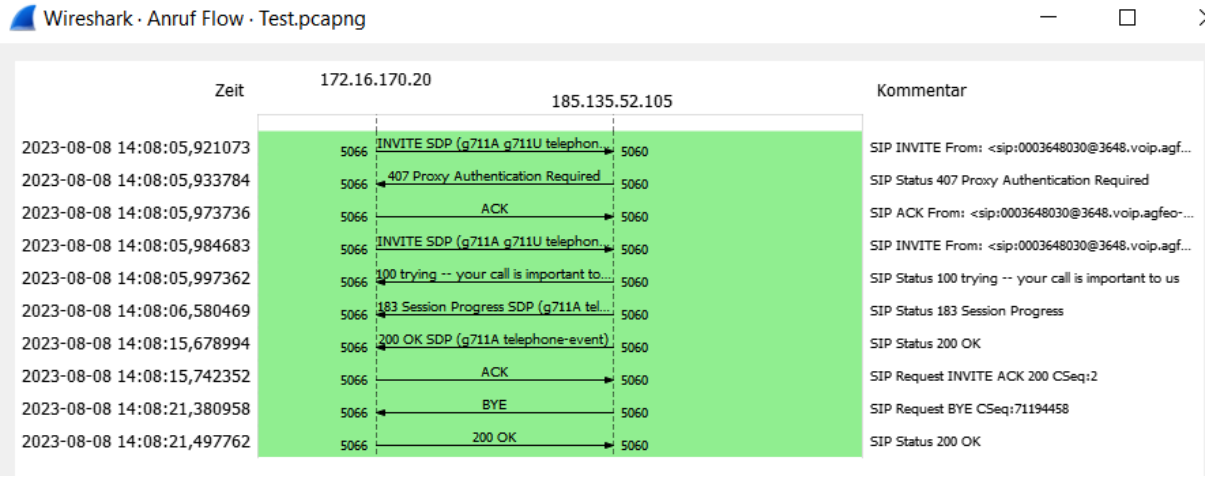
Praxis: Ruf nach Extern

Übersicht über alle aufgezeichneten Rufe -> `Menü: VOIP-Anrufe`

Ruf markieren -> `Flow Sequenzen:`



Das *Flussdiagramm* liefert nun eine bildliche Darstellung der jeweiligen Verbindung:

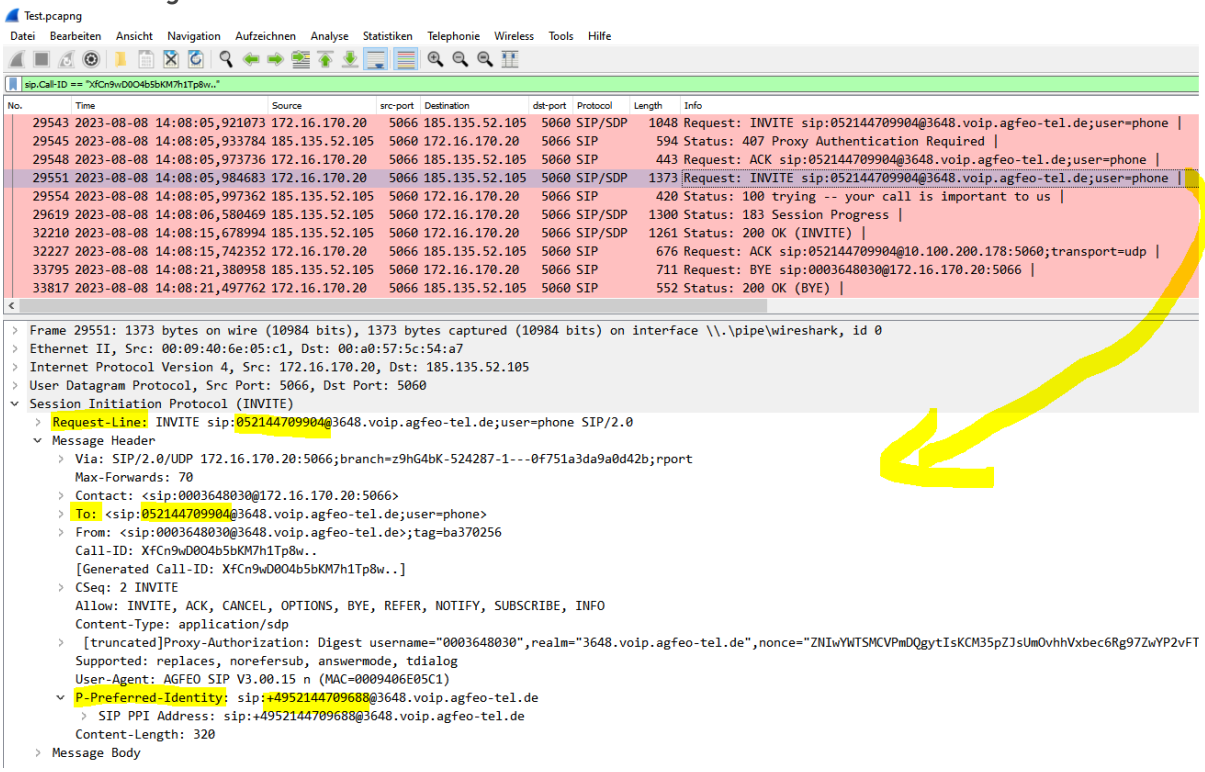


VoIP Anrufe - unter Umständen gibt es hier 2 Verbindungen für 1 Ruf.
In dem Menü /Telefonie/VoIP-Anrufe können für ein und denselben Ruf mitunter weitere Einträge erscheinen. Und zwar abhängig vom Typ des Endgerätes und dem Verbindungsziel.

Fall 1: SIP-Telefon (AGFEO-Softphone, DECT IP, T17 SIP etc.)
Es werden idR. 2 Verbindungen angezeigt -> Eine Verbindung vom SIP-Telefon zum TK Sytem (SIP-intern) und eine zusätzliche Verbindung von der Anlage zum Provider (SIP-extern)

Fall 2: AGFEO System-Telefon: (kein SIP, eigenes Protokoll)
Nur 1 dargestellte Verbindung - Verbindung vom IP-Systemtelefon zum TK-System wird nicht angezeigt - lediglich die Verbindung vom TK-System zum Provider (SIP-extern) ist sichtbar, da ein AGFEO IP-Systemtelefon nicht mittels SIP arbeitet. Selbstverständlich wird auch dann nur eine Verbindung von Wireshark erkannt, wenn es sich um ein klassisches Endgerät (Up0, a/b, ISDN) handelt.

Übermittlung der Rufnummern



Beispiel:
Abgehender Ruf - A (052144709688) ruft B (052144709904),
d. h.: A = *Anrufer* / B = *Angerufener*

A-Nummer kann je nach Provider z. B. in folgenden Parametern stehen:

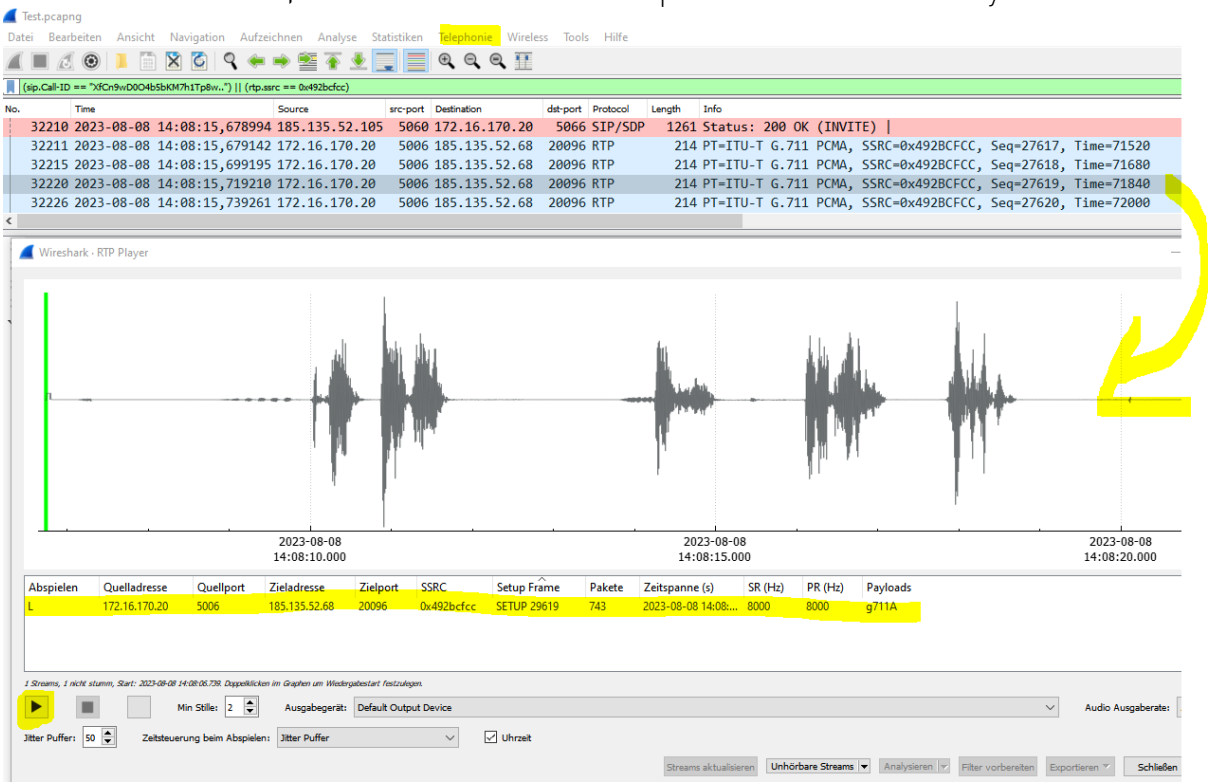
`P-Preferred-Identity` oder
`P-Asserted-Identity` oder
`From – Parameter`

Über das entsprechende *AGFEO-Providertemplate* werden die passenden Felder für alle unterstützten Provider automatisch gesetzt.

B-Nummer steht ebenfalls je nach Provider in folgenden Parametern
z. B. in der `Request-Line` bzw. im
`To - Parameter`

Sprachpakete anhören

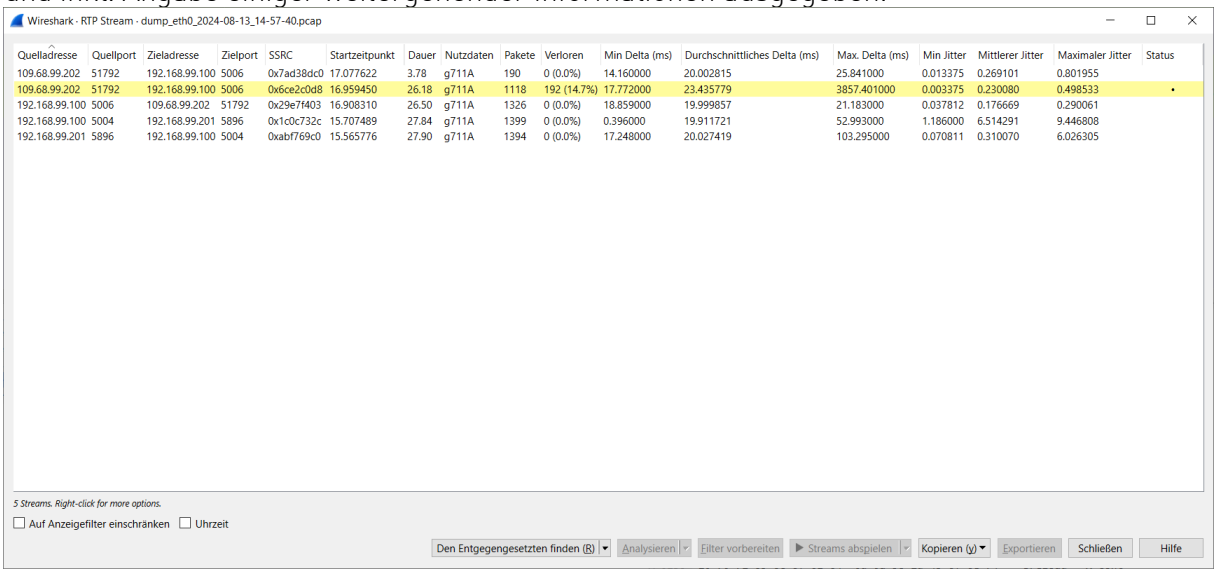
RTP-Paket markieren, anschließend: Menü -> Telephonie -> RTP -> RTP Player



Die Sprachaufzeichnung kann mit dem "`Play`"-Button angehört werden.

Sprachpakete analysieren

Wireshark verfügt über eine sehr mächtige Funktion zur Analyse der RTP Sprachpakete. Dazu das `Menü -> Telephonie -> RTP -> RTP Analyse` aufrufen. Im Nachgang werden alle von Wireshark ermittelten RTP Streams der aktuell geladenen Aufzeichnung zeilenweise und inkl. Angabe einiger weitergehender Informationen ausgegeben.



Bereits aus dieser Ansicht können zur Bewertung der Gesprächsqualität wichtige Angaben ermitteln werden.

Nutzdaten - Angaben zum verwendeten Audiocodec (z.B. G.711a)
Verloren - Angaben zu nicht angekommenen Paketen (niedrig)

Delta - Angabe zum Zeitraum zwischen einzelnen Paketen (gleichmäßig)
Jitter - Laufzeitschwankungen (niedrig)

Im Idealfall kommt es zu keinen oder nur wenigen Paketverlusten, das durchschnittliche Delta liegt um die 20ms ohne aber große Ausreißer nach oben (max. Delta) und der Jitter ist möglichst niedrig (z.B. < 10ms).

!

Wird bereits vom Programm selbst ein problematischer Stream erkannt, so wird dieser gelb markiert. Im oberen Bild ist somit der zweite RTP-Stream als *problematisch* einzustufen! Bei näherer Betrachtung ist zu erkennen, dass bei diesem knapp 15% aller Pakete verloren gegangen sind und mit knapp 4000ms auch zu einem sehr großen Delta von fast 4 Sekunden gekommen ist.

⇨ Die Sprachübertragung war hierbei somit stark eingeschränkt, obwohl die Jitter-Werte durchaus unproblematisch scheinen. Die Gesprächsqualität wird hierbei demnach unbrauchbar gewesen sein.

Typische Fehlerbilder & erste Interpretation

Die Auswertung von RTP-Streams liefert zahlreiche Messwerte. Entscheidend ist jedoch nicht allein der Wert selbst, sondern dessen Einordnung im praktischen Umfeld. Die folgenden Beispiele zeigen typische Fehlerbilder und deren häufigste Ursachen.

Hoher Paketverlust (Packet Loss)
Ein erhöhter Anteil verlorener RTP-Pakete führt zu Aussetzern, abgehackter Sprache oder komplett fehlenden Sprachanteilen. In der Praxis sind hierfür meist Netzwerkprobleme verantwortlich, z. B. eine überlastete Internetanbindung, fehlende Priorisierung von VoIP-Daten (QoS) oder instabile WLAN-Verbindungen.

Große Max-Delta-Werte
Ein stark erhöhter Max-Delta-Wert deutet darauf hin, dass Sprachpakete zeitweise sehr verzögert ankommen. Ursache sind häufig Paketstaus (Buffering) in Routern, Firewalls oder VPN-Tunneln. Auch kurzzeitige Netzüberlastungen können zu solchen Ausreißern führen.

Geringer Jitter bei dennoch schlechter Sprachqualität
Ein niedriger Jitter-Wert allein garantiert keine gute Sprachqualität. Treten gleichzeitig Paketverluste auf, kann die Sprachübertragung trotz gleichmäßiger Paketlaufzeiten unbrauchbar sein. In solchen Fällen ist der Paketverlust das dominierende Problem – nicht die Laufzeitschwankung.

Typische Fehlerbilder – Messwerte und mögliche Ursachen

Nachstehend ein paar typische Problembeispiele und Ursachen von Sprachproblemen. Ohne jeglichen Anspruch auf Vollständigkeit.

Hinweis zur Interpretation
Die Tabelle dient als erste Orientierung. Eine eindeutige Ursachenbestimmung erfordert stets die Betrachtung des gesamten Netzwerkkontextes (Endgerät, LAN, WAN, Provider-Strecke).

Beobachtung im Wireshark	Typische Messwerte	Erste Interpretation / mögliche Ursache
Abgehackte Sprache, Aussetzer	Erhöhter Packet Loss (≥ 1–2 %)	Netzwerkprobleme, Überlastung der Internetanbindung, fehlendes QoS oder instabile WLAN- bzw. VPN-Verbindung
Kurze Gesprächsunterbrechungen	Hoher Max Delta (deutlich > 20 ms)	Paketstau (Buffering) in Routern, Firewalls oder VPN-Tunneln
Verzögerte Sprache, unnatürlicher Gesprächsfluss	Erhöhte Laufzeiten / große Delta-Ausreißer	Netzüberlastung, zusätzliche Latenzen durch Routing oder VPN
Schlechte Sprachqualität trotz scheinbar stabiler Werte	Niedriger Jitter, aber vorhandener Packet Loss	Paketverluste dominieren die Sprachqualität, nicht die Laufzeitschwankung
Einseitige Sprachprobleme	Unvollständige RTP-Streams	NAT-, Firewall- oder Port-Weiterleitungsprobleme auf der RTP-Strecke
Schwankende Qualität im Tagesverlauf	Unterschiedliche Werte je nach Zeitpunkt	Lastabhängige Probleme im LAN, WAN oder beim Provider

! Die Analyse zeigt in vielen Fällen klar, dass die Ursache von Qualitätsproblemen außerhalb des AGFEO Kommunikationssystems liegt, typischerweise im lokalen Netzwerk oder auf der Provider-Strecke.

Hinweis bei aktiver Verschlüsselung:
Keine sichtbaren SIP-Pakete -> die Übermittlung erfolgt über verschlüsselte Pakete; Sprachpakete sind normale RTP-Pakete, der Inhalt der RTP-Pakete ist jedoch ebenfalls verschlüsselt.

Ohne Weiteres können die Mitschnittdaten solcher verschlüsselten Verbindungen daher dann nicht vollständig im Wireshark analysiert werden!

⇨ Die AGFEO HyperFonie Cloud-Telefonanlage nutzt für die Kommunikation mit den Endgeräten stets eine Vollverschlüsselung der Signalisierungs- (SIP/ASIP) und Sprachdaten (RTP)!

EIGENE NOTIZEN: