GUELLE Mathieu
MARCOULY Hugo
DROUET Eloi

TP : Asterisk Analyse de trames

Sommaire

Mise en place et paramétrage d'un serveur Asterisk

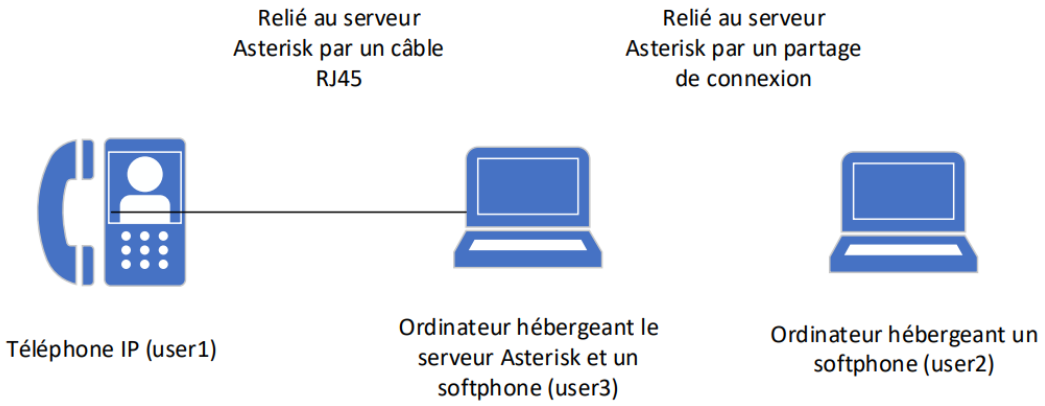
Matériels utilisés :

Pour ce TP nous utiliserons un serveur Linux pour la mise en place du serveur Asterisk. Nous avons donc opté pour **Debian 11** comme distribution. Ce TP est réalisé depuis l'un de nos ordinateurs personnels qui sont sous Windows 10/11, nous devons donc utiliser un outil de virtualisation pour utiliser Debian 11. Pour ce faire, nous avons choisi **Oracle VM VirtualBox**. Enfin, pour ce qui est de la téléphonie, nous avons à notre disposition 1 **téléphone IP physique, un UniFi VOIP UVP-PRO** et 2 softphones installés sur nos ordinateurs personnels. Nous aurons recours à **Linphone** comme logiciel softphone. La connexion à internet est assurée par un partage de connexion sur lequel sont connectés les 2 ordinateurs utilisant Linphone.

Disposition du poste de travail :

Le téléphone IP est alimenté via un câble Ethernet reliant le téléphone à un adaptateur PoE (Power over Ethernet) branché à une prise secteur. D'autre part, le téléphone est relié à l'ordinateur hébergeant le serveur Asterisk via un câble RJ45.

L'un des softphone est sur l'ordinateur hébergeant le serveur Asterisk, l'autre softphone est sur un ordinateur différent mais relié à l'ordinateur hébergeur via une connexion sans fil (partage de connexion).



(Schéma simplifié du poste de travail)

Création des utilisateurs et attributions des adresses IP :

Nous commençons l'installation et la création d'Asterisk. Lors de l'installation notre serveur se voit attribuer l'adresse IP suivante : **192.168.187.12.** Une fois, notre serveur opérationnel, nous passons à la création de nos utilisateurs. Pour cela nous nous rendons dans le fichier "sip.conf" afin de rentrer les informations concernant nos utilisateurs.

```
[user1]                ; Compte SIP
secret=1234            ; Mot de passe
mailbox=100@default    ; Messagerie
type=friend            ;  Tous  les  appels  autorisés  (entrants  et
sortants)
host=dynamic           ; Type d'adresse IP du client
callerid=user1  <100>; Nom et numéro qui s'affiche sur le client
appelé
```

(Syntaxe à utiliser dans le fichier sip.conf)

Nous créons donc 3 utilisateurs nommés “user1”, “user2” et “user3” dans notre fichier de configuration. Nous souhaitons que le “user1” soit joignable en composé le 100. Nous appliquons la même logique pour les autres utilisateurs afin que le “user2” soit joignable au 200 et le “user3” au 300.

Afin de tester la messagerie vocale de chaque utilisateur nous changeons le mot de passe par une suite de chiffres. Afin que ce dernier puisse être rentré depuis un téléphone.

Une fois le paramétrage fini, nous utilisateurs se voient tous attribuer une IP.

Détenteur de l’adresse	Adresse IP	Numéro associé
Serveur	192.168.187.12	
user1	192.168.187.10	100
user2	192.168.187.87	200
user3	192.168.187.51	300

(Tableau récapitulatif de l’attribution des adresses IP)

A titre d'information, le “user1” se trouve sur le téléphone IP physique alors que les “user2” et “user3” sont sur le softphone, Linphone.

Etablissement des règles de routage :

Afin de terminer le paramétrage et de permettre l’appel entre nos différents utilisateurs, nous procédons à la création de règle de routage simple dans le fichier “extensions.conf”.

```
[local]
exten => 100,1,Dial(SIP/user1,8)
exten => 100,3,Dial(SIP/user2,8)

exten => 200,1,Dial(SIP/user2,8)
;exten => 200,2,System(/usr/bin/aplay /var/msg/standard/test.wav)
exten => 200,2,VoiceMail(200)
exten => 200,n,Hangup()

exten => 300,1,Dial(SIP/user3,8)
exten => 300,2,VoiceMail(300)
exten => 300,n,Hangup()

        ; Appeler user1 et user2
exten => 11,1,Dial(SIP/user1&SIP/user2,10)
exten => 11,n,Hangup()

        ; Consulter la boite vocale
exten => 99,1,VoiceMailMain()
exten => 99,n,Hangup()

        ; Accéder au menu principale
exten => 50,1,goto(Menu,s,1)
exten => 50,n,Hangup()

[Menu]
exten => s,1,Background(/var/msg/standard)      ; Lire le message proposant le menu
exten => s,2,WaitExten(2)                       ; Attendre le choix au clavier pendant 2 secondes
exten => s,3,Goto(Menu,s,1)             ; Retourner au début du menu

exten => 1,1,SayNumber(1)                       ; Prononcer « 1 »
exten => 1,2,Goto(local,100,1)          ; Faire l'action 100 du contexte local appel user1

exten => 2,1,SayNumber(2)                       ; Prononcer « 2 »
exten => 2,2,Goto(local,200,1)          ; Faire l'action 200 du contexte local appel user2

exten => 3,1,SayNumber(3)                       ; Prononcer « 3 »
exten => 3,2,Goto(local,300,1)          ; Faire l'action 300 du contexte local appel user3

exten => 4,1,SayNumber(4)                       ; Prononcer « 4 »
exten => 4,2,Hangup                             ; Raccrocher

exten => 5,1,SayNumber(5)                       ; Prononcer « 5 »
exten => 5,2,Goto(secretariat,s,1)              ; Aller au sous-menu secretariat

exten => 6,1,SayNumber(6)                       ; Prononcer « 6 »
exten => 6,2,Goto(comptabilite,s,1)             ; Aller au sous-menu comptabilite
```

(Règles de routages mis en place dans notre extensions.conf)

Dans le domaine local, nous avons mis les règles de routage demandées tout au long du TP.

```
exten => 100,1,Dial(SIP/user1,8)

exten => 100,3,Dial(SIP/user2,8)
```

La première ligne permet de joindre le user1 en tapant 100. L'appel sonnera pendant 8 secondes. En cas de non réponse au bout de 8 sec, l'appel sera transféré au user2.

```
exten => 200,1,Dial(SIP/user2,8)

exten => 200,2,System(/usr/bin/aplay /var/msg/standard/test.wav)

exten => 200,VoiceMail(200)
```

La deuxième ligne permet de jouer un message enregistré en cas d'absence ou de non réponse de la part du user2.

Récolte des trames

Objectifs du TP :

Le but final de ce TP est de capturer les trames qui sont échangées lors d'un appel en VoIP entre deux utilisateurs. Une fois, les trames capturées nous allons devoir les analyser afin de récupérer et d'écouter la conversation entre les deux utilisateurs. Nous devons en particulier repérer les échanges effectués lors des différentes phases d'une communication VoIP :

enregistrement d'un utilisateur SIP

émission d'un appel

conversation

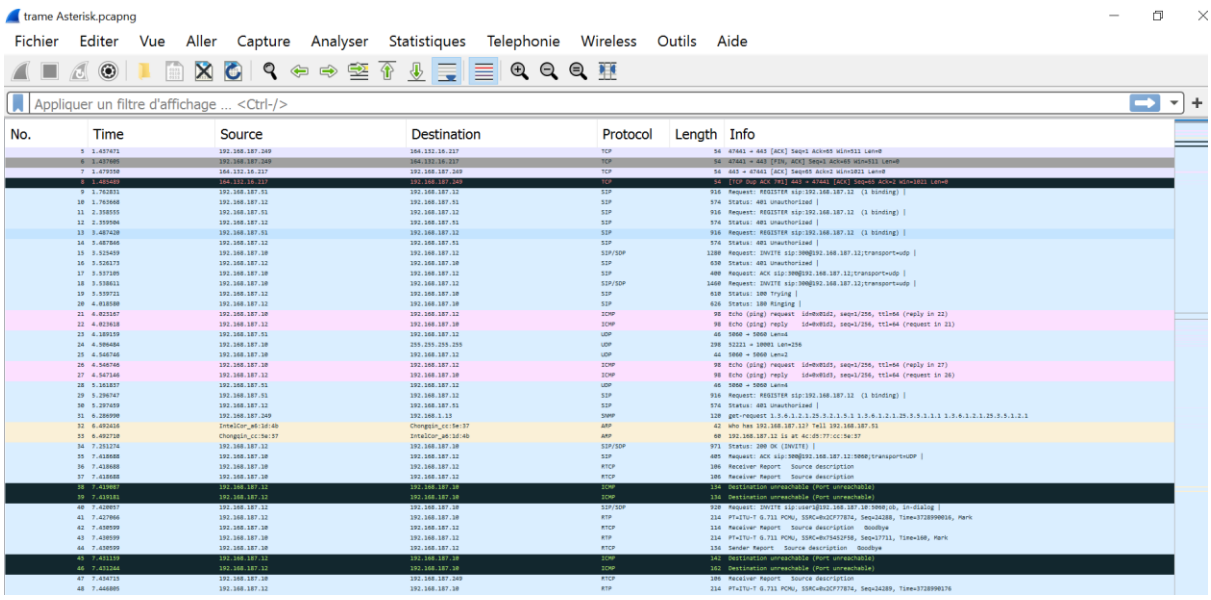
fin d'un appel

Matériels utilisés :

La communication se fera entre le téléphone IP physique (user1) et le softphone (ici, user3). Pour capturer les trames de l'appel, nous utiliserons un analyseur de paquets (ici, Wireshark). Enfin pour écouter la conversation que nous allons capter de manière audible, nous exporterons l'enregistrement vers un logiciel d'édition de son (ici, Audacity).

Déroulement de l'appel et de la capture de paquets :

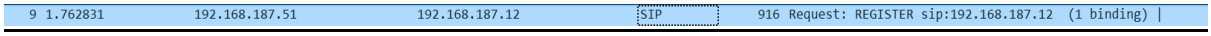
Nous lançons la capture de paquet sur Wireshark, la communication entre "user1" et "user3" commence quelques secondes après. La communication entre les deux utilisateurs durent un peu plus de 1 minute. La capture de paquet est arrêtée quelques secondes après la fin de la communication.



(Trames collectées par Whireshark durant l'appel entre les 2 utilisateurs)

Analyse des trames collectées

Enregistrement d'un utilisateur SIP :



Dans cette trame, le chiffre **9** correspond au numéro de la trame en question dans notre capture de paquets.

Le nombre **1.762831** correspond au time code (ou horodatage) de la trame en question.

192.168.187.51 correspond à l'adresse IP de l'hôte qui envoie la trame (source de la trame). La trame est donc envoyée par notre "user3".

192.168.187.12 correspond à l'adresse IP du destinataire de la trame.

Dans notre cas, on peut en déduire que cette trame vient de "user3" est s'adresse à notre serveur Asterisk.

SIP (Session Initiation Protocol) est le protocole utilisé, ce dernier est un protocole de communication VoIP.

916 est la longueur de la trame capturée en octets.

Request: REGISTER sip:192.168.187.12 (1 binding) cette partie comporte les informations spécifiques à cette trame.

Le "**Request: REGISTER sip:192.168.187.12 (1 binding)**" nous indique que cette trame est une requête du "user3" afin de s'enregistrer auprès du serveur SIP dont l'adresse IP est 192.168.187.12 soit notre serveur Asterisk.

Emission d'un appel :

(Trame déclenchant l'appel)

Comme pour la trame précédente, **15** est le numéro de la trame et **3.525459** l'horodatage de la trame.

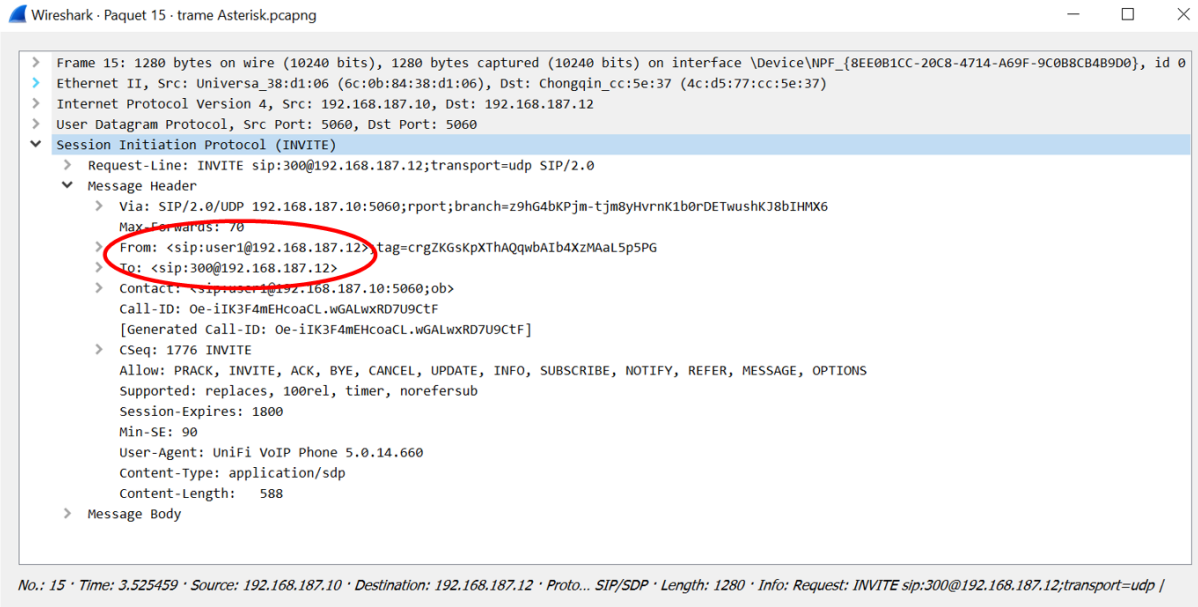
Cette trame part du "user1" (possédant l'adresse **192.168.187.10**) et est à destination du serveur Asterisk(**192.168.187.12**).

Les protocoles sont **SIP**(Session Initiation Protocol)**/ SDP**(Session Description Protocol), 2 protocoles de communications.

Request: INVITE sip:300@192.168.187.12;transport=udp, cette partie nous informe qu'il s'agit d'une invitation à une session VoIP pour le "user3".

Cette trame est donc celle qui déclenche l'appel du "user1" vers le "user3".

Nous pouvons le vérifier en allant dans les détails de la trame (en faisant un double clique sur la trame en question)



(Détail de la trame n°15, on remarque le destinataire "To" et l'émetteur "From")

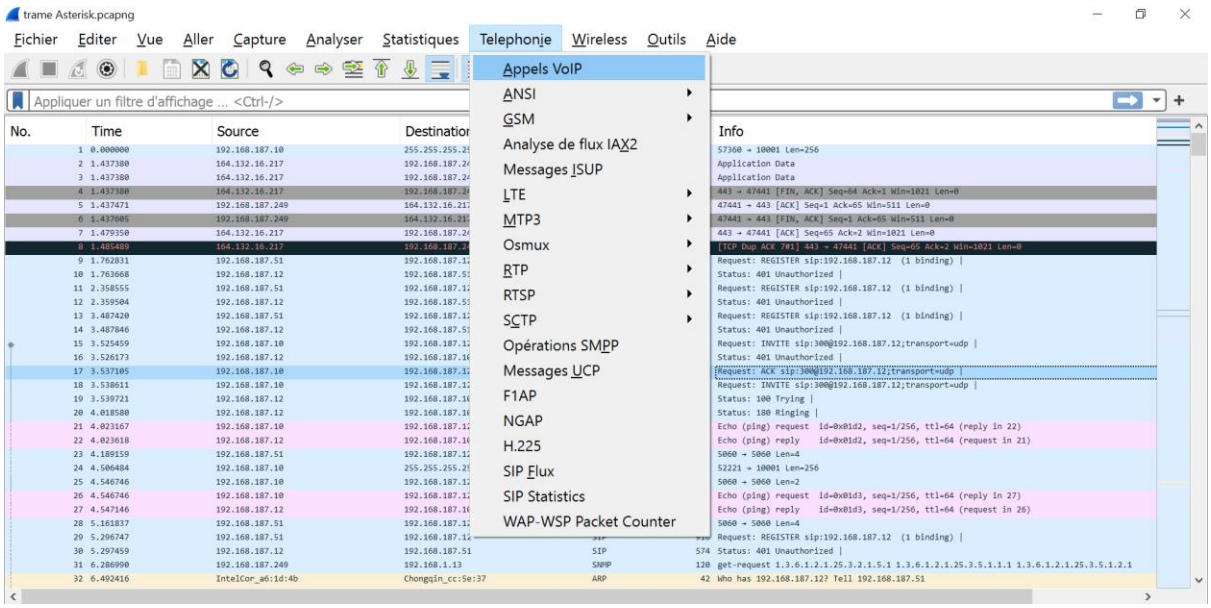
19	3.539721	192.168.187.12	192.168.187.10	SIP	610 Status: 100 Trying |
20	4.018580	192.168.187.12	192.168.187.10	SIP	626 Status: 180 Ringing |

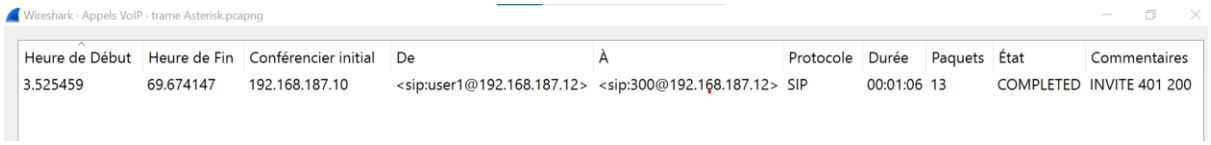
Ces deux trames montrent que l'appel à bien été déclenché. Le statut « Trying » de la trame n°19 est une réponse provisoire qui indique que le serveur Asterisk a reçu la demande d'appel et qu'elle est en cours de traitement. De plus, cela signifie que la communication entre le user1 et le user3 est en cours d'établissement.

Le statut « Ringing » de la trame n°20, nous informe que l'appel est en cours et que le téléphone du destinataire (ici, user3) est en train de sonner.

<u>Transcription vocale de la conversation :</u>

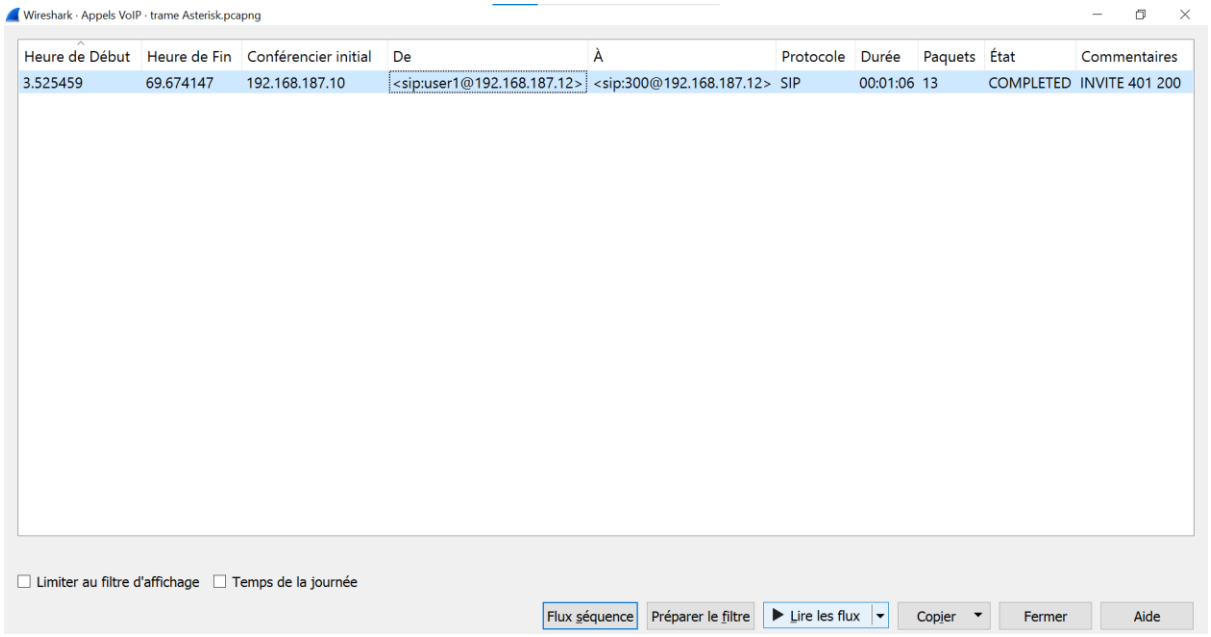
Une fois toutes les trames de l'appel VoIP, en allant dans "Telephonie > AppelsVoIP" nous retrouvons toutes les informations sur la communication enregistrée.



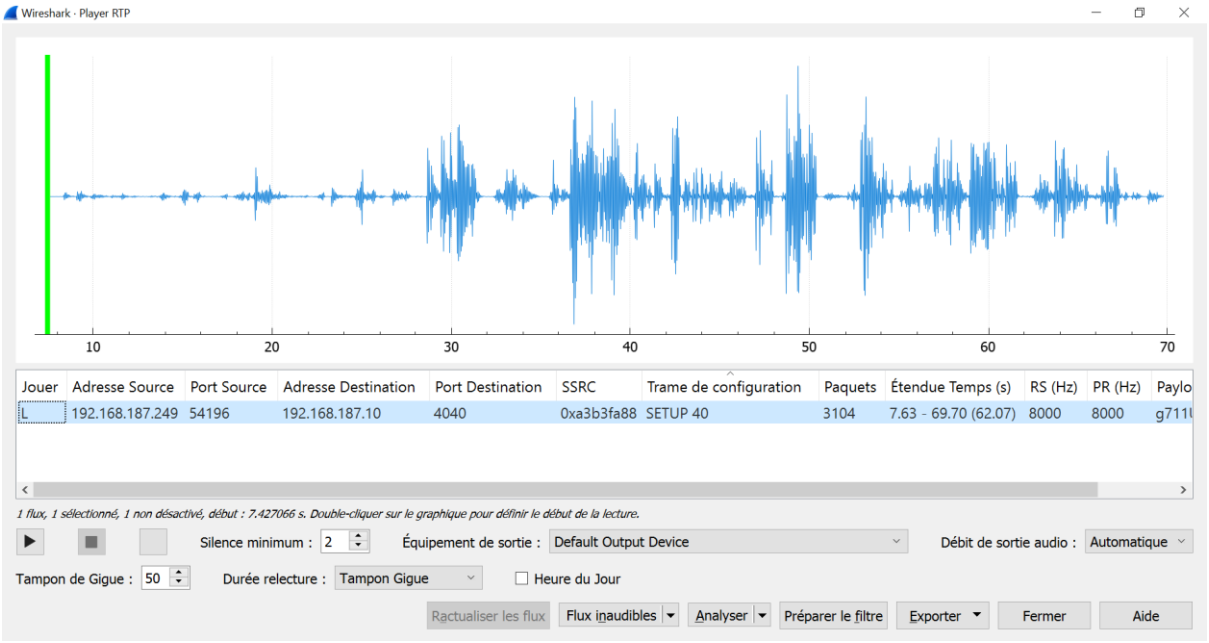


(Synthèse de l'appel)

On remarque que l'appel venait du "user1" et qu'il a composé le 300 pour contacter le destinataire, il a donc contacté le "user3". L'appel a commencé à 3,53 sec et s'est fini à 69,67 sec, la conversation entre le "user1" et le "user3" 1 min et 6 sec. Comme indiqué dans la section "Durée".



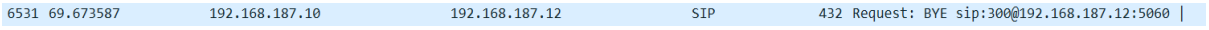
En sélectionnant l'appel capté en cliquant sur "Lire les flux", nous obtenons enfin la transcription vocale de l'appel. Il nous est donc possible d'écouter ou de réécouter la conversation en entier.



(Enregistrement audio capté grâce à Wireshark)

Une fois l'enregistrement obtenu, nous pouvons l'exporter en fichier .wav afin qu'il soit ouvert avec Audacity pour une meilleure qualité d'écoute.

Détection de la fin d'un appel :



(Trame déclenchant la fin de l'appel)

Comme pour les trames précédentes, **6531** est le numéro de la trame et **69,673587** l'horodatage de la trame.

Cette trame part du "user1" (possédant l'adresse **192.168.187.10**) et est à destination du serveur Asterisk(**192.168.187.12**).

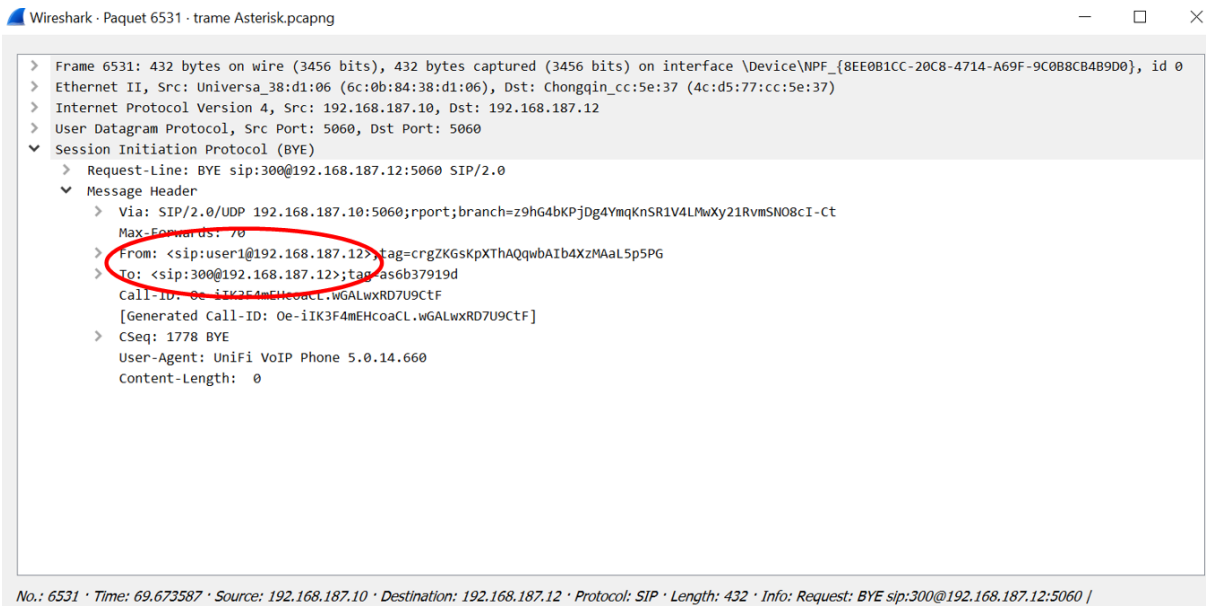
Le protocole est **SIP**(Session Initiation Protocol), un protocole de communication.

La taille de la trame est de **432** octets.

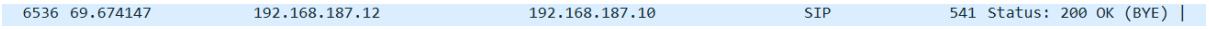
Request: BYE sip:300@192.168.187.12:5060, cette partie nous informe qu'il s'agit d'une requête BYE. Il s'agit d'une demande de fin de session. Lorsqu'un utilisateur envoie un message BYE, cela signifie qu'il souhaite mettre fin à la session VoIP en cours.

Cette trame est donc celle qui déclenche la fin de l'appel du "user1" vers le "user3".

Nous pouvons le vérifier en allant dans les détails de la trame (en faisant un double clique sur la trame en question)



(Détails de la trame n° 6531)



(Trame mettant fin à l'appel)

Comme pour les trames précédentes, **6536** est le numéro de la trame et **69,674147** l'horodatage de la trame.

Cette trame part du serveur Asterisk (possédant l'adresse **192.168.187.12**) et est à destination du "user1"(**192.168.187.10**).

Le protocole est **SIP**(Session Initiation Protocol), un protocole de communication.

La taille de la trame est de **541** octets.

Status: 200 OK (BYE), cette partie nous informe qu'il s'agit d'une réponse SIP avec le code de statut "200 OK", ce qui signifie que la requête BYE précédente a été traitée avec succès. Cette réponse indique que le serveur ou le destinataire a accepté la demande BYE et a pris les mesures nécessaires pour mettre fin à l'appel VoIP.

Cette trame est donc celle qui met fin à l'appel.