UTILISATION AVANCEE DE WIRESHARK

PC - Windows / LINUX
Configuration avancée
Tutoriel **WIRESHARK** – WINDOWS / LINUX
1 avril 2025

David GOÏTRÉ

Table des matières

Introduction

Wireshark possède plusieurs fonctions avancées pour scanner, analyser et détecter les anomalies sur un trafic normal, mais aussi sur un trafic multimédia, le SIP.

1. Prérequis

On a besoin de différents matériels et logiciels pour la capture d'un trafic réseau

- Un PC client sous Windows ou Linux
- Le logiciel Wireshark installé
- Les droits Administrateur
- Connaître le modèle O.S.I
- Connaître les différents protocoles réseau

2. Les outils de statistiques

Ces outils permettent plusieurs affichages détaillés en fonction des paramètres choisis tel que le type de protocole, l'adresse IP, etc...

La hiérarchie des protocoles

Cet outil affiche une vue d'ensemble de tous les protocoles utilisés dans la capture. Il montre une dissection par couche OSI des données affichées.

a) Conversations

Si on utilise une application ou protocole de la suite TCP/IP, on doit trouver quatre onglets actifs pour les conversations Ethernet, IP, TCP ou UDP. Une **conversation** représente le trafic entre deux hôtes.

b) Points de terminaisons

Les points de terminaisons (Endpoints) fournissent des statistiques sur les données reçues et transmisses par hôte. Le nombre après le protocole dans l'onglet.

c) Graphique I/O

Des graphiques basiques peuvent être obtenus dans la section **IO Graphs**. Plusieurs graphiques en fonction du filtre d'affichage peuvent être ajoutés dans la même fenêtre.

d) Graphique des Flux

Des graphiques qui fournissent une analyse séquentielle de connexions par rapport au **type de flux** sélectionner dans la liste.

e) HTTP (Hypertext Transfer Protocol) est un protocole de communication client-serveur utilisé pour transférer des fichiers HTML. Un client HTTP, la plupart du temps un navigateur internet, envoie un fichier de requête HTTP à un serveur web avec le champ bien connu **URL** pour localiser le fichier. Le serveur web va répondre avec une **réponse HTTP** et fournit au client la page web désirée.

Trois sous-sections sont disponibles sous HTTP :

- **Répartition de charge** (Load Distribution) : Affiche la charge
- **Compteur de paquets** (Packet Counter) : Affiche les requêtes et réponses HTTP.
- **Requêtes** (Requests) : Affiche les fichiers consultés sur le serveur web.

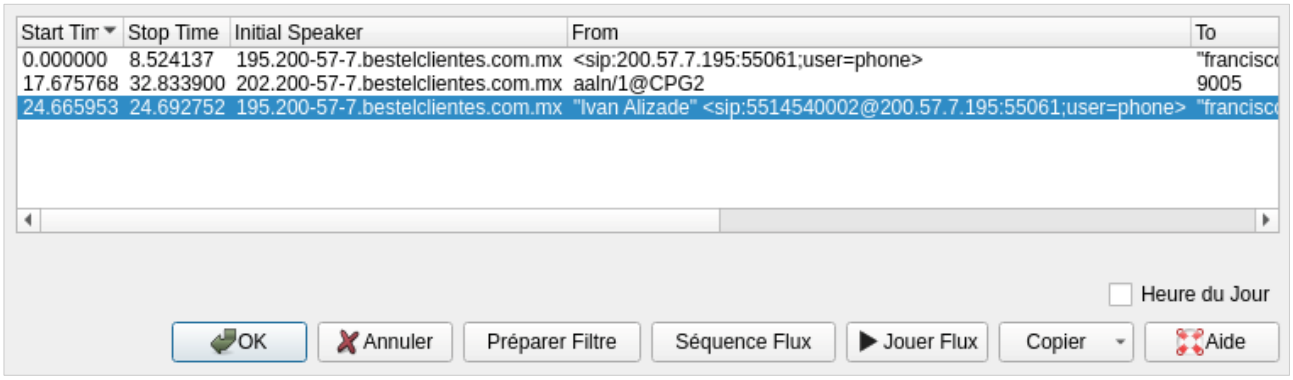
3. Les outils de téléphonie

Wireshark fournit une large gamme de statistiques de réseau liées à la téléphonie. Ces statistiques vont des **protocoles de signalisation** spécifiques à l'analyse de **Signalisation** et **flux multimédia**. Si le flux multimédia est codé dans un codage compatible, il peut même être joué.

Les Appels VoIP affiche une liste de tous les appels VoIP détectés dans les appels capturés Trafic. Il détecte les appels par leur signalisation et affiche les flux RTP associés. Les protocoles VoIP actuellement pris en charge sont :

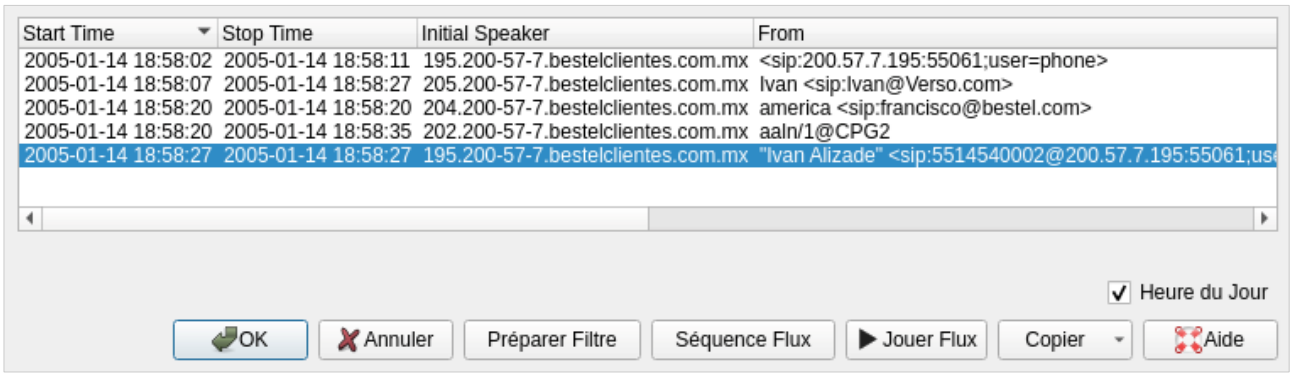
- H.323, IAX32, ISUP, MGCP, SIP, SKINNY, UNISTIM

a) Sélectionner le menu **Téléphonie/Appels VoIP** ou **Téléphonie/SIP Flux**
b) Sélectionner une ligne, puis cliquer sur le bouton **Jouer Flux**



Le protocole RTP (Real Time Transport Protocol), fait référence au protocole de transport en temps réel, qui est un protocole réseau utilisé pour diffuser de l'audio et de la vidéo via des réseaux IP. Comme son nom l'indique, RTP est conçu pour faire face au trafic en temps réel comme l'audio et la vidéo.

a) Sélectionner le menu **Téléphonie/RTP/Flux RTP**
b) Sélectionner un ou plusieurs paquets
c) Cliquer sur le bouton **Analyse**

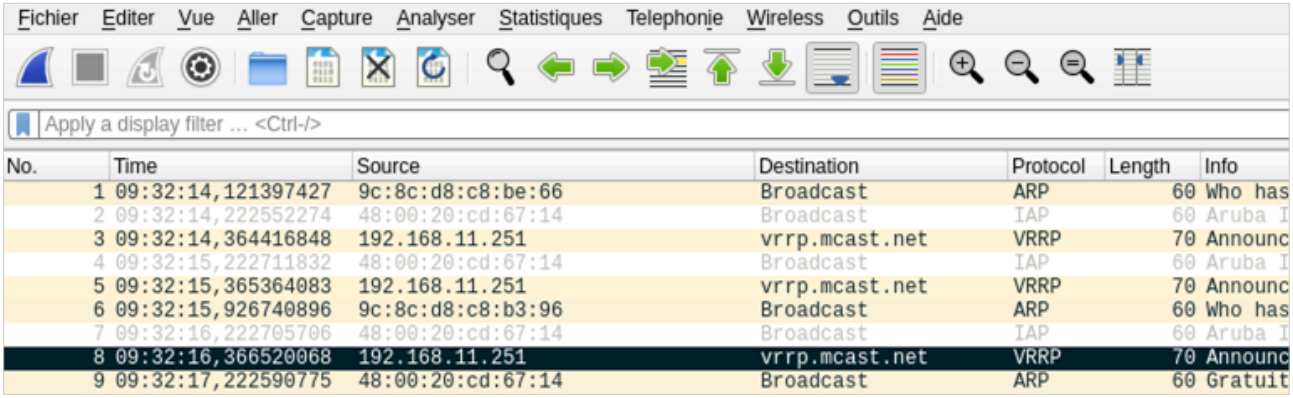


Le protocole SIP Statistics
La fenêtre Statistiques SIP affiche les transactions SIP capturées. Elle est divisée en réponses SIP et requêtes SIP. Dans cette fenêtre, l'utilisateur peut filtrer, copier ou enregistrer les statistiques dans un fichier.

4. Marquage d'un ou plusieurs paquets

Grâce au marquage de paquets, on va pouvoir retrouver facilement certains paquets dans une capture réseau. Utile pour estampiller les paquets qui nous intéressent vraiment, le marquage de paquets s'effectue dans la liste des paquets de la capture réseau.

a) Faire un clic droit sur le paquet à marquer
b) Cliquer sur le menu **Marquer/Démarquer le(s) paquet(s)**
c) Le paquet est surligner en noir avec une écriture blanche



d) Afficher uniquement les paquets marqués

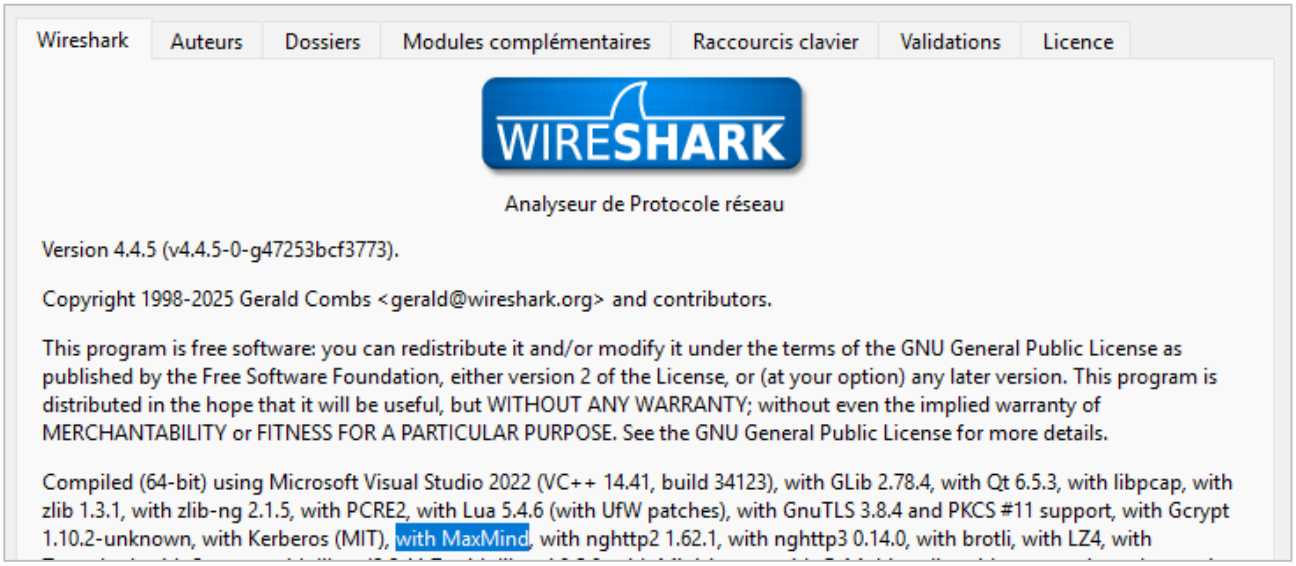
Filtre d'affichage	**Exemple**
Sur les paquets marqués	frame.marked==1

5a. La géolocalisation d'adresses IP

Cette fonctionnalité va permettre d'afficher des informations sur les adresses IP publiques **via les bases de données MaxMind GeoLite2**, afin de connaître l'origine ou la destination d'un flux dans **Wireshark**. Voici les informations que l'on pourra obtenir :

- ASN : le numéro Autonomous System
- Le Pays
- La ville

Pour utiliser les **bases de données MaxMind**, il faut vérifier la version de **Wireshark compatible** avec cette fonctionnalité. Elle est disponible depuis la **version 2.6**.



a) Sélectionner le menu **Aide/A Propos de Wireshark** pour vérifier la compatibilité
b) Télécharger les fichiers Gzip : GeoLite2 ASN, GeoLite2 City, GeoLite2 Country

5b. Intégration des bases de données

L'intégration des bases de données dans **Wireshark** est très simple. Il faut spécifier le dossier où sont stockés les fichiers.

a) Sélectionner le menu **Editer/Préférences...**
b) Dans la section, cliquer sur **Name Resolution**
c) Descendre jusqu'à la section **Maxmind database directories**
d) Cliquer sur le bouton **Edit...**
e) Dans la nouvelle fenêtre, cliquer sur le **bouton +**
f) Cliquer sur le bouton **Parcourir...** pour spécifier le dossier
g) Cliquer sur le bouton **OK**

5c. Utilisation de la fonctionnalité GeoIP

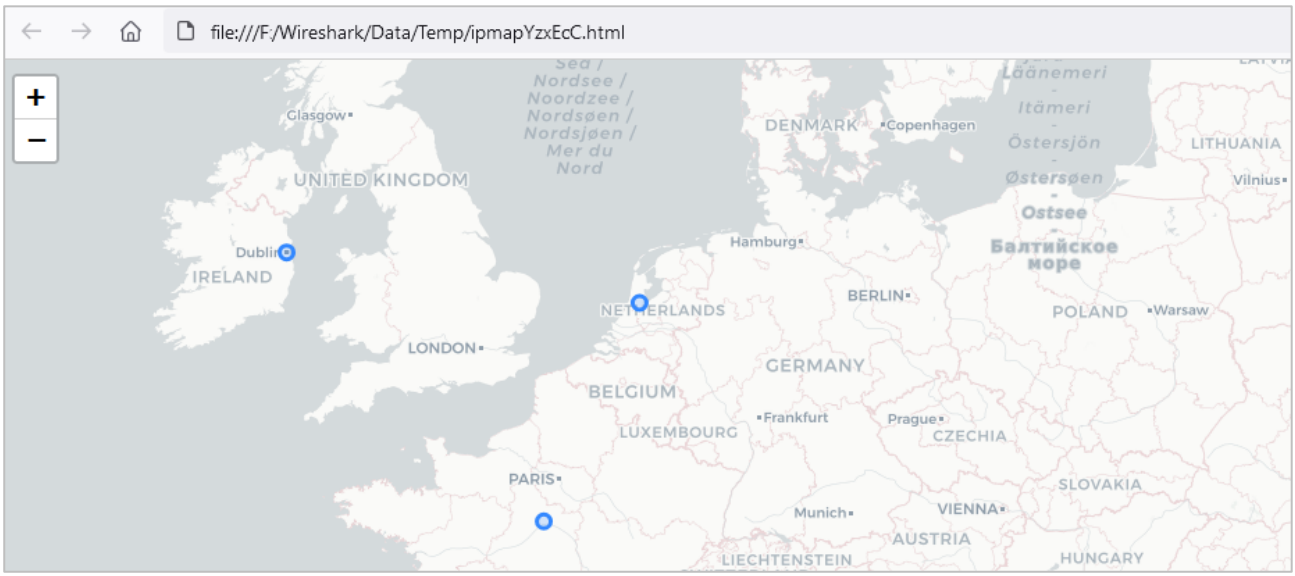
Les filtres de capture permettent comme le nom l'indique de filtrer les flux de capture en entrée afin de voir seulement le trafic qui nous intéressent, pour ensuite l'analyser plus facilement, car la capture sera épurée.

a) Sélectionner le menu **Statistiques/Points de terminaisons**
b) Sélectionner l'**onglet IPv4**, on constate l'apparition de quatre nouvelles colonnes

- Country : localise le pays d'une adresse IP
- City : localise la ville d'une adresse IP
- AS : Permet de spécifier dans quelle AS se trouve une adresse IP
- AS Organisation : permet de spécifier à quelle entreprise appartient cette IP

5d. La carte de GeoIP

Dans la fenêtre des **points de terminaisons**, on peut afficher une mappemonde avec toutes les IP par localisation. Le navigateur s'ouvrira avec la carte basée sur **OpenStreetMap**, et on voit le **nombre d'adresses IP par localisation**.
a) Cliquer sur le bouton **Map**
b) Cliquer sur le bouton **Ouvrir dans un navigateur**



5e. Les filtres d'affichage par GeoIP

Il est possible de filtrer une trace réseau via les **informations de GeoIP**, voici les filtres intéressants à garder précieusement.

Filtres d'affichage	Exemples
Sur pays en source ou destination	ip.geoip.country == "United States"
Sur pays en source	ip.geoip.src_country == "United States"
Sur pays en destination	ip.geoip.dst_country == "United States"
Sur le code d'un pays source ou dest	ip.geoip.country_iso == "US"
Sur une organisation	ip.geoip.org == "GOOGLE"

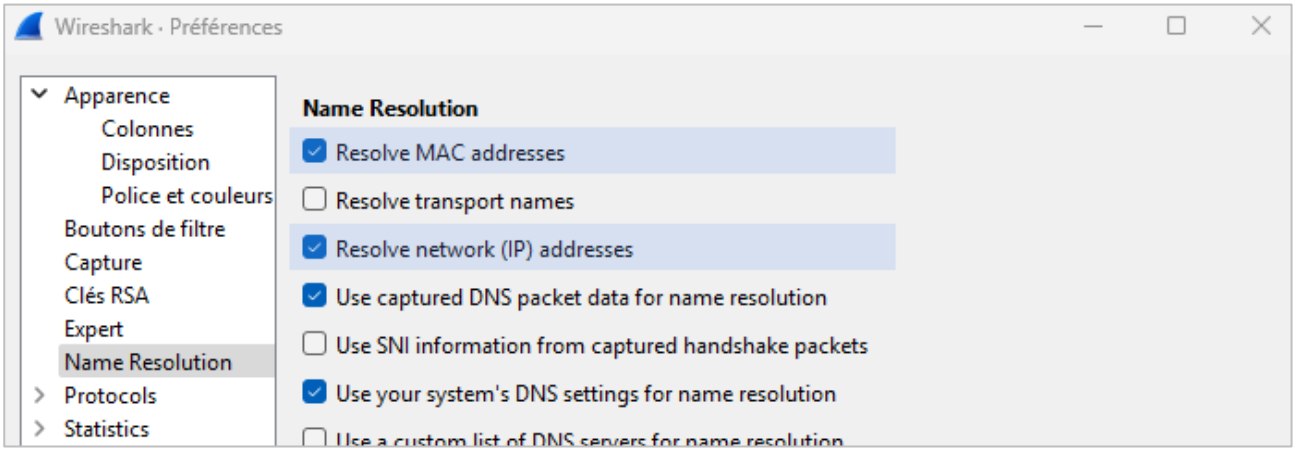
6a. La résolution de noms

Pour rappel, la résolution de nom permet de trouver l'adresse IP associée à un nom de domaine. C'est plus facile de travailler avec les noms même si les machines se réfèrent à l'adresse IP. Plus généralement, la résolution de nom permet de convertir certaines valeurs numériques dans un format plus compréhensible.
La résolution de nom Ethernet dans **Wireshark** permet de résoudre la partie **OUI** (Organizationally Unique Identifier) d'une adresse MAC.

Wireshark s'appuie le fichier **les blocs d'adresses MAC** pour effectuer sa résolution de nom Ethernet.
Pour afficher ces blocs d'adresses MAC, sélectionner le menu **Outils/Blocs d'adresses MAC**
Pour personnaliser cette liste, télécharger le fichier manuf et le placer dans le **dossier de Wireshark**.

6b. Activation de la résolution de nom Ethernet

a) Cliquer sur le menu **Editer/Préférences**
b) Dans la section, cliquer sur **Name Resolution**
c) Cocher la case **Resolve MAC adresses**



d) Cocher la case **Resolve network (IP) addresses** pour afficher les noms à la place des @IP

6c. Activation de la résolution de nom IP

L'activation de la résolution de nom IP se situe au même endroit que pour la partie Ethernet, à savoir dans le menu **Editer** puis **Préférences**. On va configurer la résolution de nom IP en cochant les lignes suivantes :

- Requêtes DNS de la capt... : **Use captured DNS packet data for address resolution**
- Paramètres DNS de l'hôte : **Use an external network name resolver**
- Résolution de nom IP : **Resolve network(IP) addresses**

Cette fois-ci encore, la modification est prise en compte directement par Wireshark. Il suffit de regarder la liste des paquets, on verra le nom des sites internet apparaître au lieu des adresses IP.

7. Annexes

Liste de contenu à consulter

- Fichier exemples de capture : https://wiki.wireshark.org/samplecaptures
- Les protocoles VoIP : https://sip.goffinet.org/wireshark/hiérarchie-de-protocoles
- Protocole RTP : https://www.wireshark.org/docs/wsug_html_chunked/ChTelRTP.html

8. Conclusion

Wireshark permet une analyse poussée avec ses statistiques et la téléphonie. De plus la fonctionnalité de **Géolocalisation IP** peut être utile dans le cadre d'une tentative de cyberattaque afin d'identifier de quel pays provient cette tentative, dans le cadre d'une analyse post mortem.

Grâce à la fonctionnalité **GeoIP**, on dispose d'informations supplémentaires très pratique pour analyser des paquets, et surtout précieuses dans le cadre d'analyses liées à un incident de cybersécurité.