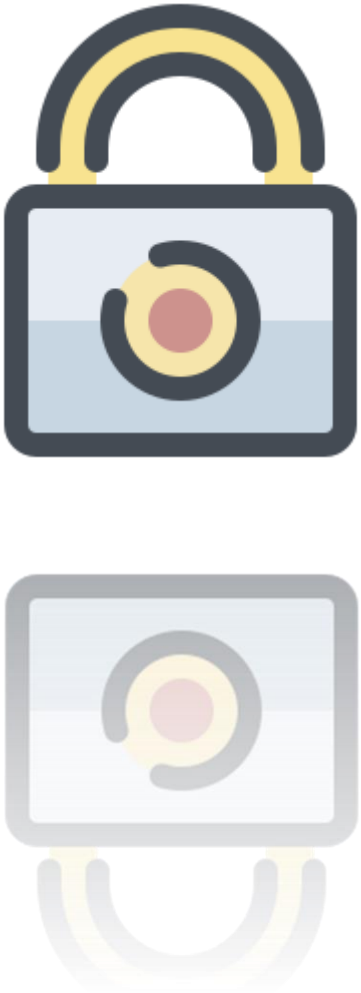
La sécurité des protocoles /Cryptographie



Les protocoles

Les protocoles doivent offrir un **échange sécurisé** et un **chiffrement des données**. On entend par échange sécurisé, une communication qui comprend : - la garantie de **Confidentialité** (l'information n'est pas accessible par un tiers autre que le destinataire) ; - l'**Authenticité** (l'expéditeur est sûr de l'identité du destinataire et inversement) ; - l'**Intégrité** (l'information n'est pas modifiée lors de la communication).
Par la suite le chiffrement des données s'effectue via des **algorithmes**. En effet ces derniers transforment l'information à l'aide de ce qu'on appelle **clefs de cryptage**, où sans ces clefs, une fois cryptée l'information devient ainsi illisible. Il existe ainsi divers types de chiffrement, le **symétrique** et l'**asymétrique**. Le symétrique impose un échange de clef (il est donc impossible d'avoir une communication qui passe en claire sur internet), où au contraire l'asymétrique lui, est efficace si l'on est sur de l'authenticité des pairs.
Il existe une grande variété de protocoles tels que l'HTTPS ou bien le TLS.
Où par exemple l'http étant un protocole d'échange web sur un réseau (internet & intranet).

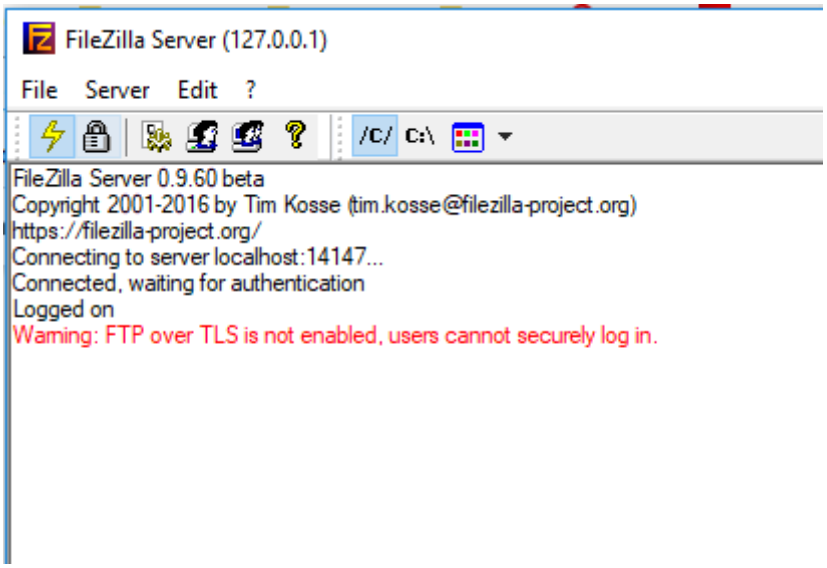
L’importance de crypter

> En effet, sans ces protocoles, les données lors de communication peuvent donc être interprétées par un tiers. Voici donc ci-dessous un exemple, d’une des manières où sans protocoles les données sont détournées. (De la création du serveur au piratage des données)

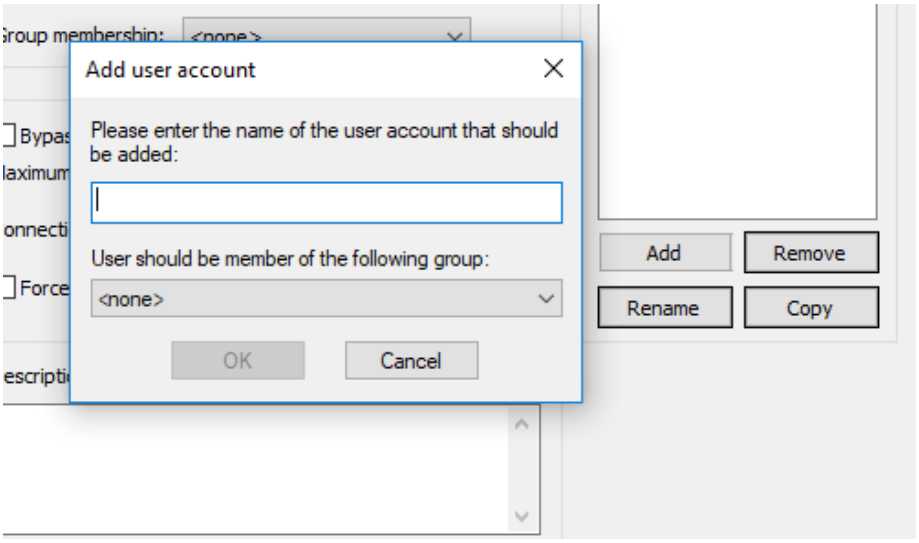
“Man in the Middle”

Server-Pirate-Client

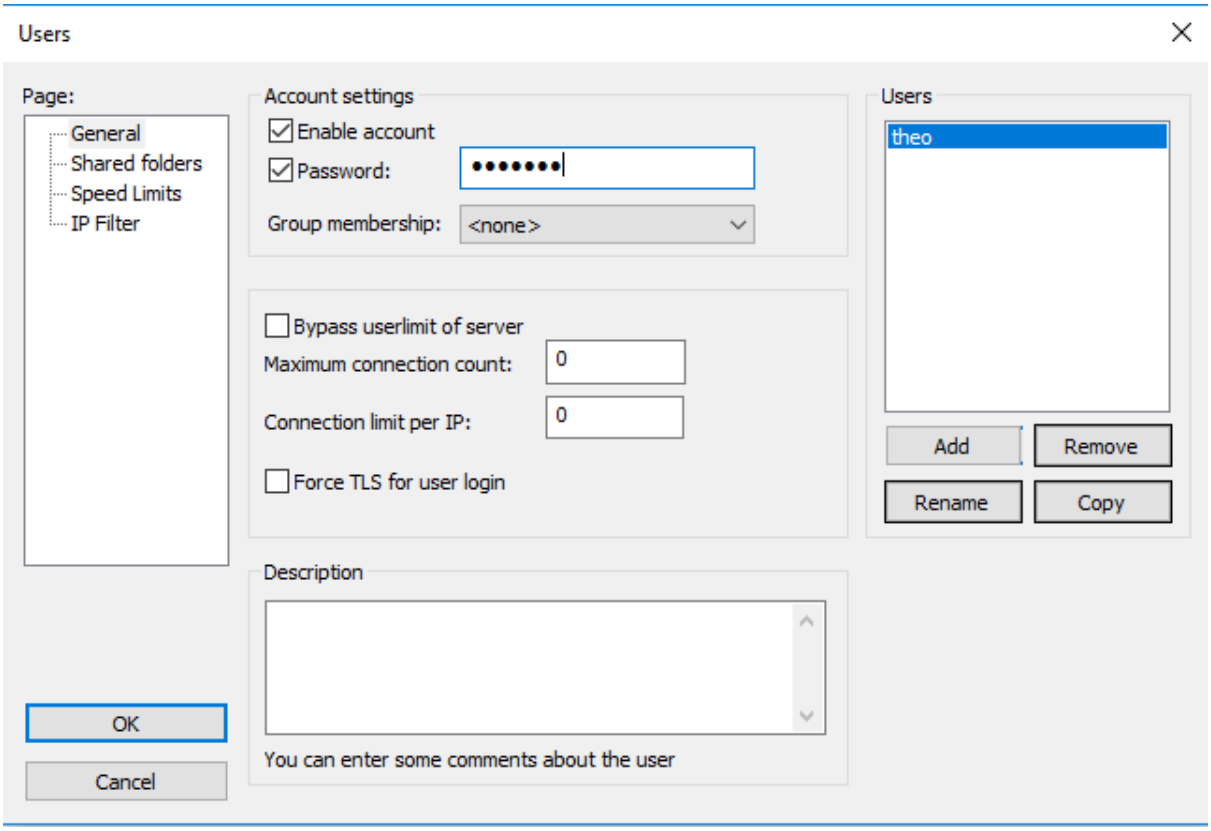
Etape 1 : Ouverture du FTP serveur



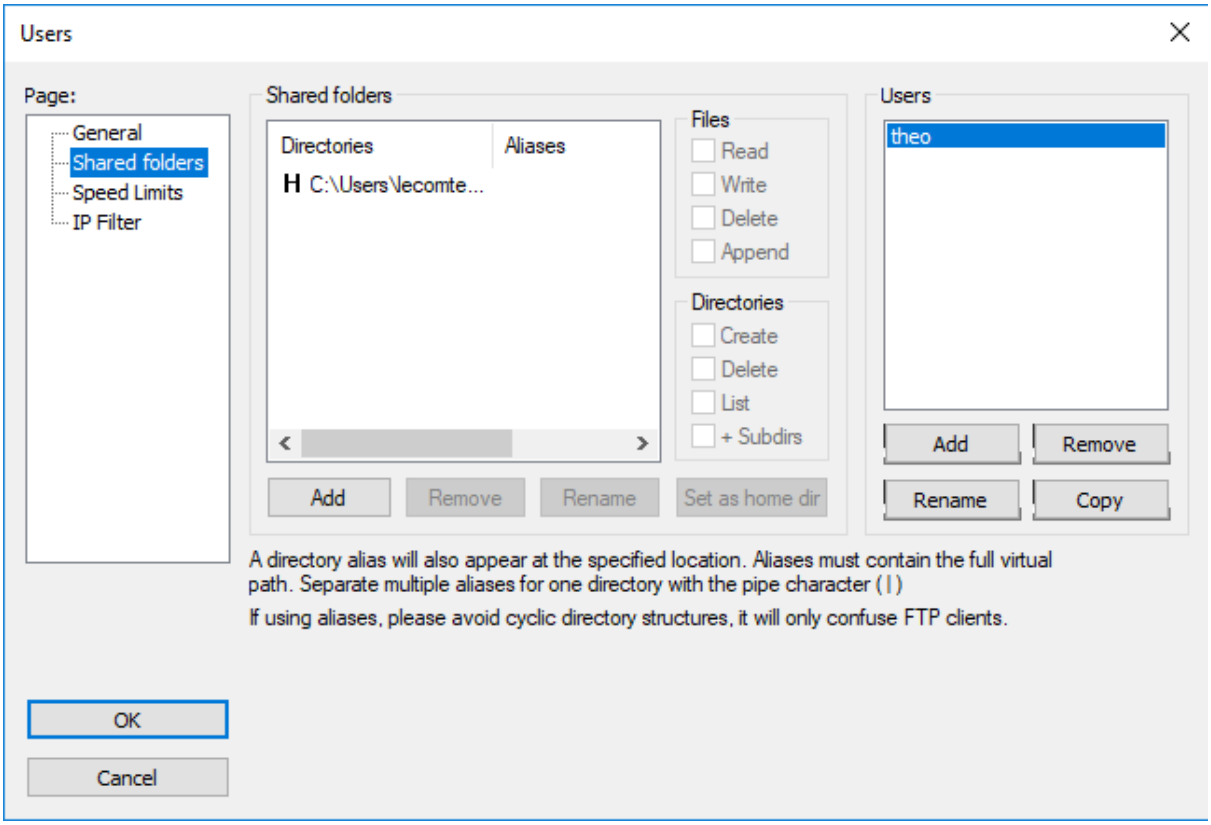
Etape 2 : Création du compte



Etape 3 : Adressage du mot de passe

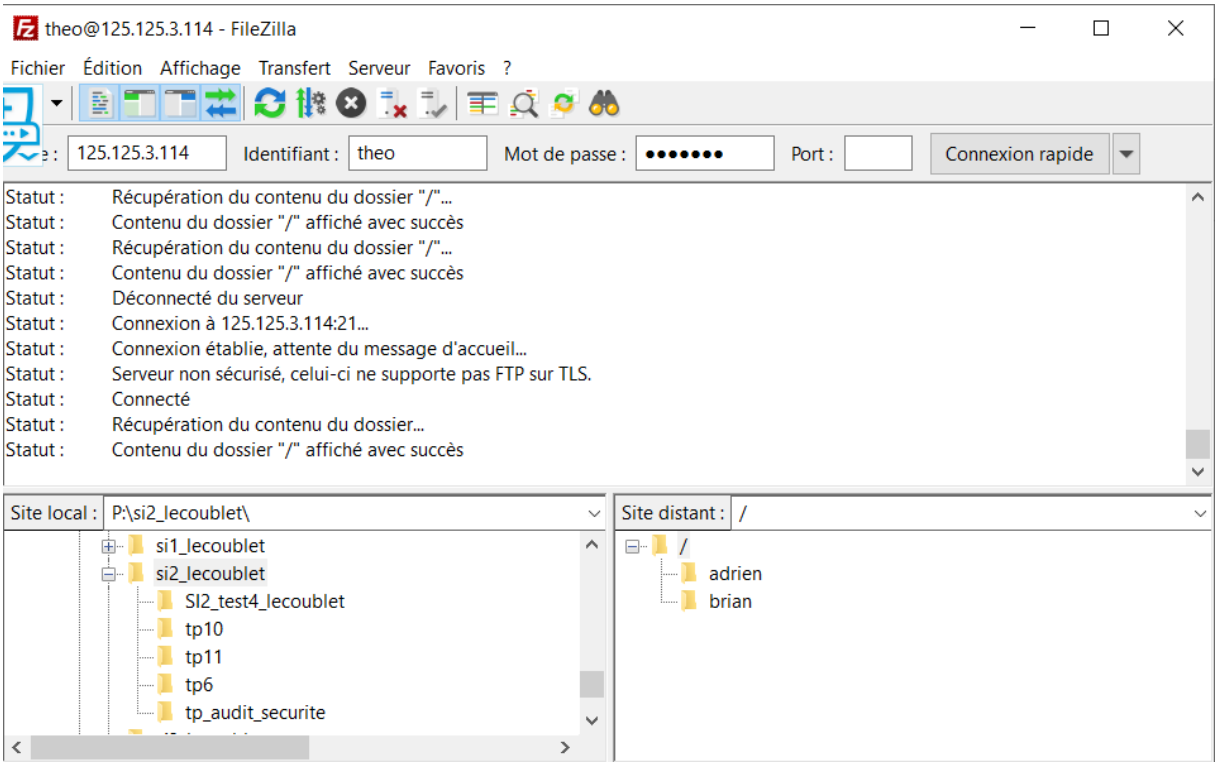


Etape 4 : Don des droits d'accès aux fichiers/dossiers à l'utilisateur

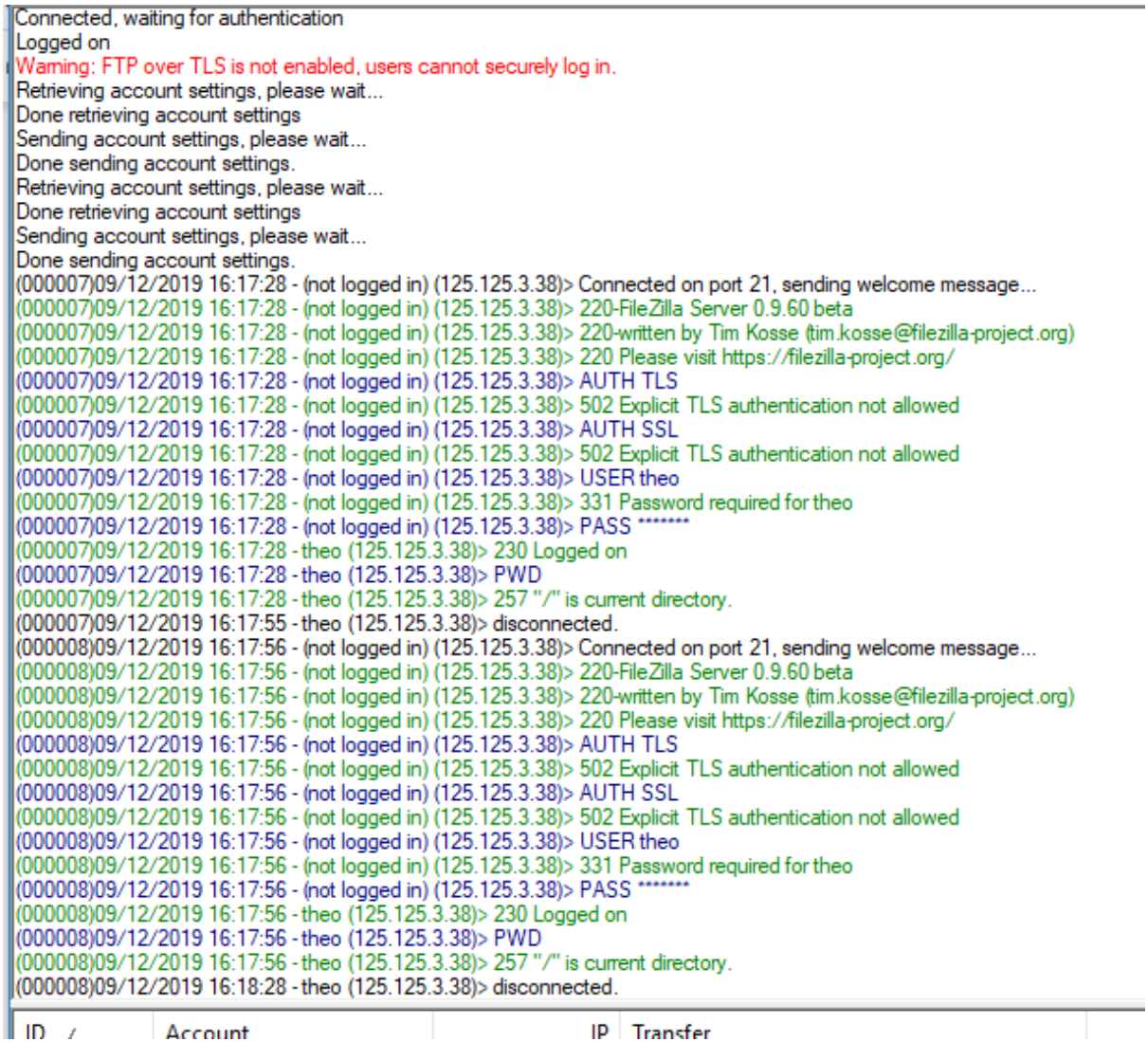


Etape 5 : Connexion entre le Client et le Serveur

Vue client :

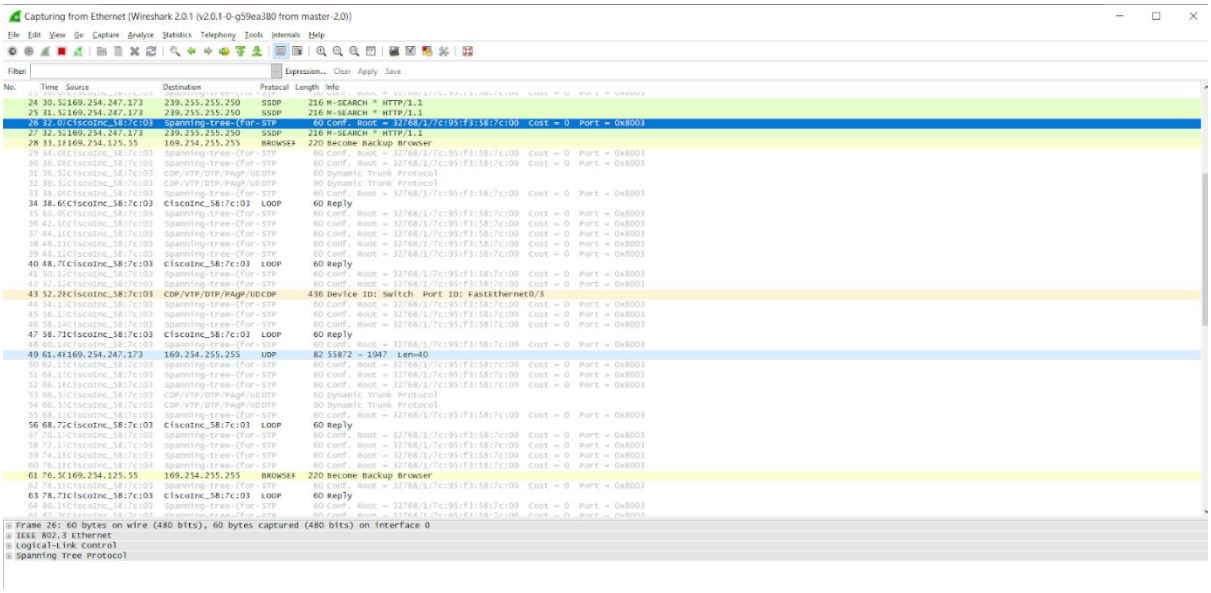


Vue serveur :

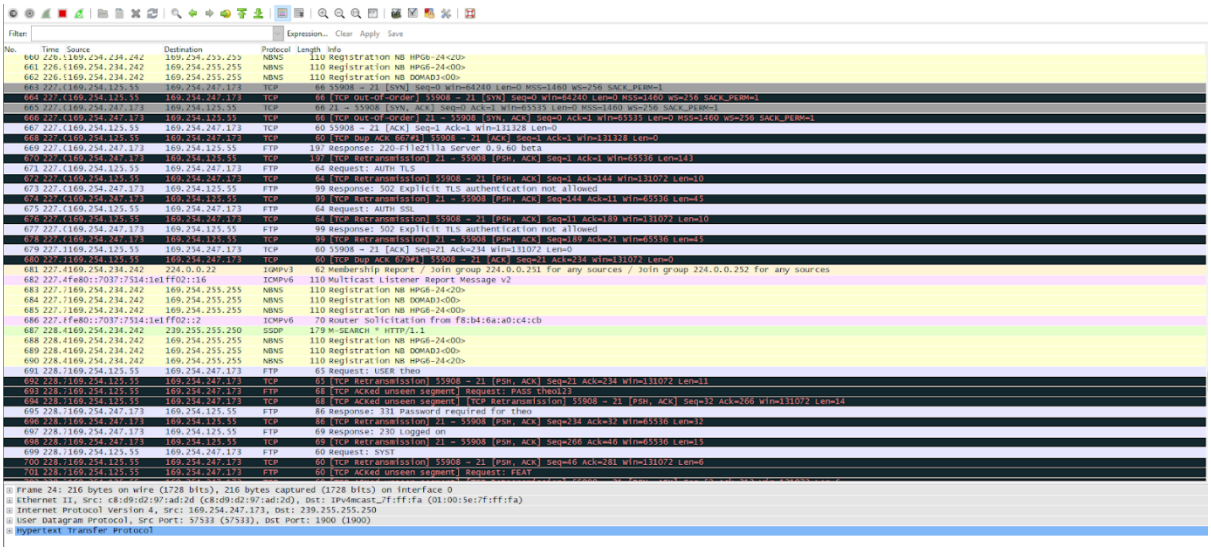


Etape 6 : Connexion du pirate en parallèle de l'**Etape 5** / Interception du pirate

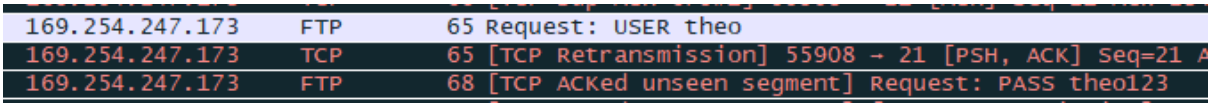
Le pirate s'est connecté au réseau :



Il intercepte les paquets durant la connexion du client au serveur :



Plus précisément ceci :



Ainsi il a sa disposition les informations suivante sous cette forme :