Analyse d'un échange FTP

Objectifs :

Capturer une trame échangée entre 2 ordinateurs à l'aide d'un outil approprié.
Isoler les entêtes à l'intérieur de cette trame.
Analyser ces entêtes ainsi que le champ données.

Installation du logiciel de capture :

Le logiciel d'analyse doit être utilisé en tant qu'administrateur pour avoir accès à la carte réseau. Il faut donc l'installer sur la station virtuelle :
(Stock_samba\ressources\Logiciels\WireShark)

Capture de la trame :

Lancer un client **FTP** et saisir les coordonnées de connexion sur le compte perso **SRV-BPSEN** mais ne pas lancer la connexion.
Lance ce logiciel **WireShark**.
Cliquer sur Interfaces list puis cliquer sur start en face de la carte réseau de l'ordinateur.
Lancer la connexion dans le client FTP puis arrêter la capture (quatrième icône en haut en partant de la gauche).
Retrouver la trame correspondant à cette connexion.
La sélectionner et l'enregistrer.

Analyse :
Couche **réseau** (modèle **TCP/IP**):
- **A**dresse **MAC** et le nom du fabricant de la carte réseau du destinataire.
- **A**dresse **MAC** et le nom du fabricant de la carte réseau de l'expéditeur.
- **T**ype de protocole.

Entête **IP** :
- **V**ersion.
- **L**a longueur de l'entête.
- **L**ongueur totale.
- **P**rotocole.
- **A**dresse **IP** de l'expéditeur.
- **A**dresse **IP** du destinataire.

Entête **TCP** :
- **P**ort source.
- **P**ort destination.
- **L**ongueur totale.

Données :
- **N**om d'utilisateur.
- **M**ot de passe.

Vérification :

Il doit y avoir concordance entre la valeur des paramètres relevée dans le logiciel d'analyse et la valeur réelle de ceux-ci. Par ex on peut vérifier la valeur d'une adresse **MAC** avec la commande **ARP**.

Rédiger un compte rendu détaillant la vérification de la concordance de chacun des paramètres ci-dessus.