TP : Etude du protocole TCP

L'objectif de ce TP est d'étudier les différentes phases du protocole TCP et d'analyser le contenu de l'entête TCP.

Nous avons choisis le protocole HTTP , un protocole au niveau de la couche application, qui utilise tcp comme protocole de transport.

Le protocole HTTP se déroule en deux étapes. La première étape consiste à envoyer une requête contenant le nom de la page Web demandée de la part du client. En deuxième étape, le serveur va traiter la requête et il va renvoyer la page demandée.

Une capture Wireshark d'un échange HTTP est déjà réalisée. Cette capture comporte un échange HTTP entre un client et un serveur HTTP. Cet échange génère un flux tcp.

Pour le déroulement du TP suivez les étapes suivantes :

1. Ouvrir la capture **tp_tcp.pcap en utilisant wireshark**
2. **Utiliser le filtre http pour visualiser que l'échange HTTP (couche application)**
    a. Quelle est l'adresse du client et l'adresse du serveur :

    b. Que représente la première ligne

    c. Que représente la deuxième ligne

3. **Pour visualiser que les segments tcp générés par le client et le serveur utiliser le filtre tcp au niveau wireshark.**
   Par la suite vous allez identifier la phase de l'ouverture, la phase d'échange de données et la phase de la fermeture.
4. Identification de segments de l'ouverture de la connexion :

    a. Quel est le port utilisé par le client ?

    b. Quel est le port utilisé par le serveur ? De quel service s'agit-il ?

    c. Donner le numéro de séquence initiale du client et du serveur ?

    d. Donner la signification des paramètres (MSS et WIN) ? Expliquer la valeur de ces paramètres du coté client et serveur ?

    e. Compléter le diagramme suivant en montrant les échanges de la phase de l'ouverture de la connexion :

Source destination	Seq	ack	Flag
Client serveur			
Serveur client			
Client serveur			

5. Identification de la phase de transfert de données.
    a. Quelle est le rôle du premier segment de cette phase ? quelle est l'information véhiculée dans ce segment ?

    b. Interpréter la valeur des flags SYN et PSH dans ce premier segment ?

    c. Quel est le nombre de segments ainsi que la taille de données dans chaque segment envoyé par le serveur (justifier la taille de chaque segment) ?

    d. Interpréter les options de l'envoi du dernier segment en particulier?

    e. Déduire la taille de la page transférée ?

6. Identification de la phase de la fermeture de la connexion
    a. Qui a demandé la fermeture de la connexion ?

    b. Compléter le diagramme suivant en montrant les échanges de la fermeture de la connexion :

Source destination	Seq	ack	Flag
Serveur client			
Client serveur			
Client serveur			
Serveur client			

7. Confirmer les résultats des questions précédentes avec Wireshark
   Utiliser le menu **statistics flow graph** (choisir les paquets TCP uniquement)

8. Au niveau de Wireshark, utiliser le filtre http . Compléter le diagramme suivant en montrant les échanges effectués au niveau http ? Expliquer ces échanges (faire le lien avec TCP)