## ****TP 1****

### ****1. Présentation du logiciel *Wireshark*****

- Démarrez le logiciel Wireskark.  
- Ouvrez la trace [exemple.pcap](http://moodle.univ-tlse3.fr/file.php/1071/captures-reseau/trace_http.pcap) et familiarisez vous avec l'interface utilisateur en identifiant les différentes parties exposées précédemment.

### ****2. Concept de Protocole****

2.1 Rappelez ce qu'est un "protocole".

Un protocole est un ensemble de règles définissant la manière dont les données sont échangées entre des entités d’un réseau. Il spécifie le format, l’ordre des messages échangés, ainsi que les actions à entreprendre en cas d’erreurs ou de conditions particulières.

2.2 Quelle est la commande HTTP (opération protocolaire) utilisée par le client pour demander au serveur une ressource (un fichier) ?

GET /test.html HTTP/1.1

Quels sont les types de réponse HTTP qui sont mises en évidence dans cette capture ? Donnez leur code de retour (*Status Code*).

HTTP/1.1 404 Not Found

2.3 Consultez le contenu de la première requête HTTP.

7 1.530092 141.115.64.47 213.186.33.19 HTTP 388 GET / HTTP/1.1   
- Quelle est la taille (en octets) de cette requête HTTP (uniquement la partie HTTP) ?

388 bytes – (IP Header:20 bytes+ TCP Header: 32 bytes+ Ethernet II: 14 bytes) = 322 bytes  
- Quel est le site web consulté ?

Host: licinfo.deptinfo.fr

[Full request URI: http://licinfo.deptinfo.fr/]

**2.4** Observez le contenu de la réponse du serveur.  
- Quelle est la taille (en octets) de la réponse HTTP (message HTTP incluant les données) ?

*448* bytes

- Que représente le texte décrit en langage HTML ?

Il s’agit du contenu de la page web renvoyée par le serveur (le fichier HTML)

2.5 Reconstituez la totalité des échanges HTTP dans un diagramme de séquence.  
Vous préciserez l'émetteur, le récepteur et le type de message HTTP.

### ****3. Concepts de Couche et d'Encapsulation****

3.1 Rappelez une définition du concept de "couche".

Une couche est un niveau de l’architecture réseau (OSI ou TCP/IP) qui fournit des services à la couche supérieure en s’appuyant sur les services de la couche inférieure. Chaque couche s’occupe d’un certain type de fonctions (ex. transport fiable, routage IP, adressage physique, etc.) et communique via des interfaces bien définies.

3.2 Sur la capture de la section précédente, observez les différents niveaux d'encapsulation de la trame numéro 7 dans la zone packet details.

Frame 7: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits)

*(Frame 7, Frame (frame), 388 byte(s).)*

Ethernet II, Src: HewlettP\_21:2d:eb (00:24:81:21:2d:eb), Dst: JuniperN\_98:51:81 (78:19:f7:98:51:81)

*(Frame 7, Ethernet (eth), 14 byte(s))*

MAC Destination: JuniperN\_98:51:81 (78:19:f7:98:51:81)

MAC Source: HewlettP\_21:2d:eb (00:24:81:21:2d:eb)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 141.115.64.47, Dst: 213.186.33.19

*(Frame 7, Internet Protocol Version 4 (ip), 20 byte(s).)*

Adresse source, Adresse de destination, etc.

Transmission Control Protocol, Src Port: 54258, Dst Port: 80, Seq: 1, Ack: 1, Len: 322

*(Frame 7, Transmission Control Protocol (tcp), 32 byte(s).)*

*Sequence Number, Options (12 bytes), Source Port: 54258, Destination Port: 80, etc.*

Hypertext Transfer Protocol

*(Frame 7, Hypertext Transfer Protocol (http), 322 byte(s).)*

- Reconstituez la structure complète de cette trame qui est transmise sur le réseau. Vous préciserez les en-têtes des différentes couches (sans donner le détail des champs) ainsi que leur taille en octets.  
- Vérifiez que la somme totale des en-têtes corresponde bien à la taille totale des données capturées.  
- Positionnez les différentes couches par rapport au modèle OSI (sachant qu'il n'existe pas explicitement de couches session et présentation dans le modèle TCP/IP)

3.3 Même question avec les trames numéro 96 et 797 (pensez avant à retirer le filtre http)

### ****4. Concept de Point d'Accès aux Services****

4.1 L'identifiant du point d'accès au service de la couche transport (T-SAP) est un numéro de *port*. Repérez ce numéro dans l'en-tête de la PDU transport.

- Quel est le numéro de port pour l'entité HTTP de la machine d'adresse 74.125.230.247 ?  
- Même question pour la machine d'adresse 141.115.64.47 communicant avec l'entité HTTP de 74.125.230.247.

4.2 A partir d'un quelconque message HTTP de la trace, trouvez les autres identifiants des points d'accès aux services des couches réseau et liaison (i.e. les identifiants permettant l'acheminement des unités de données entre les couches Transport-Réseau et Réseau-Liaison).