TP 1

1. Présentation du logiciel *Wireshark*

- Démarrez le logiciel Wireskark.
- Ouvrez la trace exemple.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) ?

Dans la session capturée, nous observons que le client (IP : 141.115.64.47) utilise la commande HTTP GET – une méthode standard pour demander une ressource (comme une page web ou un fichier) au serveur. Toutes les requêtes enregistrées dans la trace utilisent justement la méthode GET, y compris celles vers la page principale (/) ainsi que vers des fichiers spécifiques (par exemple, /test.html dans le paquet n°805, Commande: 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*).

Code	Statut	Explication	№ de paquet
200	OK	Réponse réussie, ressource trouvée	№78, №205, №661, №742
204	No Content	Réussite, mais sans contenu	№795 HTTP/1.1 204 No Content
404	Not Found	Ressource non trouvée sur le serveur	№806 HTTP/1.1 404 Not Found

2.3 Consultez le contenu de la première requête HTTP.

La première requête HTTP dans la session capturée est une requête du client vers le site web licinfo.deptinfo.fr. Le domaine du site cible est déterminé à partir de l'en-tête Host dans les en-têtes

HTTP. Dans le paquet n°7 (premier HTTP GET), on trouve la ligne d'en-tête : Host: licinfo.deptinfo.fr, ce qui indique que le client s'adresse bien à une ressource sur ce serveur web. Ainsi, le site cible de la première requête est licinfo.deptinfo.fr, ce qui correspond à l'adresse IP de destination 213.186.33.19 (comme on peut le voir dans la liste des paquets, la source 141.115.64.47 envoie le paquet à cette IP).

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) ?

Le paquet n°7 a une taille totale de 388 octets, qui inclut tous les en-têtes des couches inférieures.

En soustrayant les tailles des en-têtes réseau :

- Ethernet II : 14 octets
- IPv4 : 20 octets
- TCP : 32 octets

388 bytes – (IP Header:20 bytes+ TCP Header: 32 bytes+ Ethernet II: 14 bytes) = 322 bytes

Wireshark indique que la taille totale de la trame n°7 est de 388 octets (ce chiffre inclut à la fois la requête HTTP elle-même et les en-têtes des couches inférieures — Ethernet, IP, TCP). Parmi eux, environ 322 octets correspondent aux données HTTP (le reste étant constitué des en-têtes des protocoles des couches inférieures).

- 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 - C'est la taille exacte du message HTTP complet (en-têtes + corps encodé en chunked), telle qu'interprétée par Wireshark.

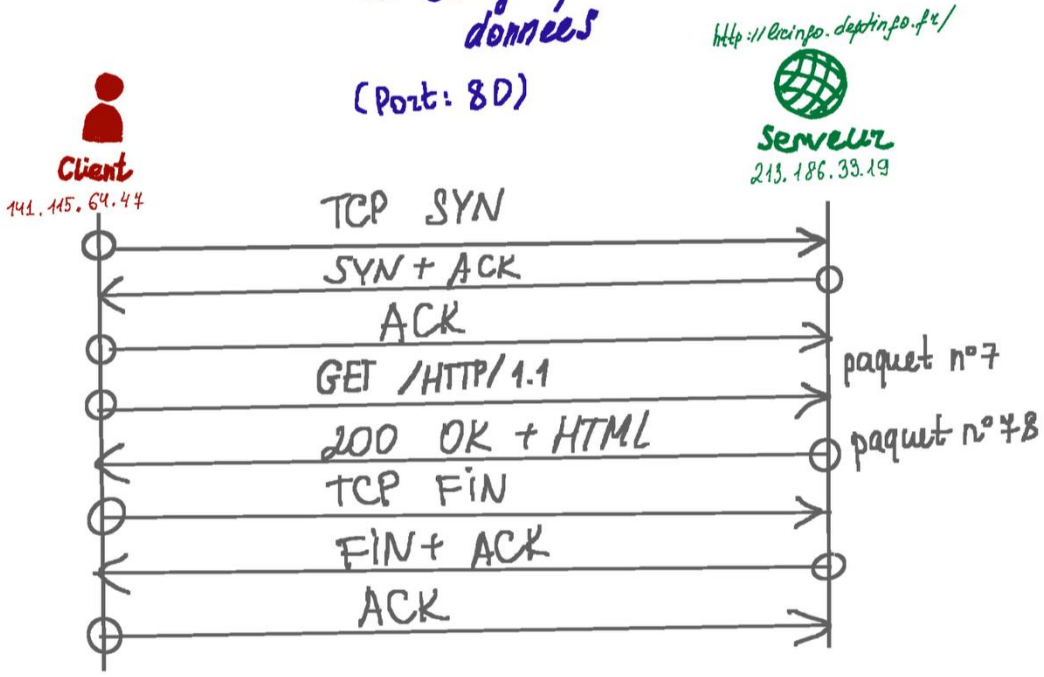
- Que représente le texte décrit en langage HTML ?

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.

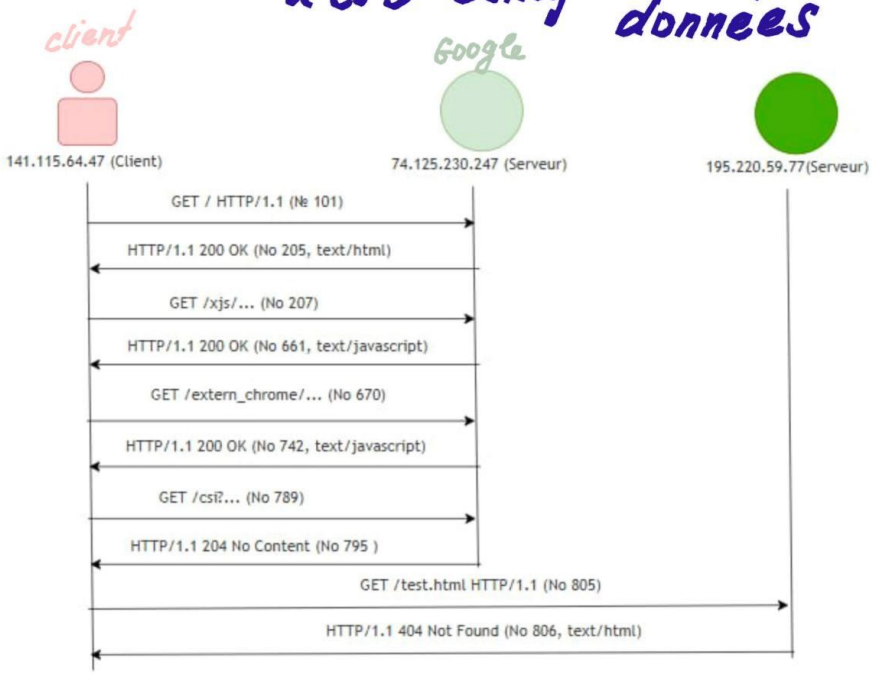
Diagramme de séquence

1er échange de données



---

2 et 3 échanges de données



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.

- 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)

Paquet n°7 dans notre capture correspond au premier requête HTTP (GET) envoyée par le client au serveur. Voici une présentation plus concise de sa structure, par couches et par tailles :

Niveau 2 (liaison) : Ethernet II. Le cadre Ethernet II inclut un en-tête de 14 octets, contenant :

- L'adresse MAC de destination (6 octets)
- L'adresse MAC source (6 octets)
- Le champ EtherType (2 octets), qui vaut ici 0x0800 (IPv4)

Niveau 3 (réseau) : IPv4. Sitôt l'en-tête Ethernet, on trouve l'en-tête IP (20 octets en l'absence d'options). Dans le paquet n°7 :

- IP source : 141.115.64.47
- IP destination : 213.186.33.19
- Protocole (Protocol) = 6 (TCP)

Niveau 4 (transport) : TCP. Le segment TCP suit l'en-tête IP. Sa taille minimale est 20 octets, mais des options l'allongent souvent. Ici, après établissement de la session HTTP, l'en-tête TCP mesure 32 octets, en raison d'options telles que Timestamps et SACK Permitted (habituellement +12 octets).

- Port source : 54258 (port éphémère côté client)
- Port destination : 80 (HTTP)
- Numéros de séquence et d'acquittement, drapeaux (PSH/ACK), taille de fenêtre, somme de contrôle et options TCP.

Niveau 7 (application) : HTTP.

Couche (OSI)	Protocole	Taille (octets)	Contenu principal
Liaison (2)	Ethernet II	14	MAC source/dest, EtherType=0x0800
Réseau (3)	IPv4	20	IP source, IP dest, Protocol=6, TTL, checksum
Transport (4)	TCP	32	Ports (54258→80), séquence/ACK, drapeaux, options
Application (7)	HTTP (GET)	322	Requête GET / HTTP/1.1 et en-têtes HTTP
Total	Cadre Ethernet	388	Ensemble du paquet encapsulant les données HTTP

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

Paquet n°96 : il s'agit d'une requête DNS (protocole DNS sur UDP). Le client cherche à résoudre un nom de domaine (ici www.google.fr), afin d'obtenir une adresse IP correspondante.

Ethernet II (couche liaison)

14 octets d'en-tête Ethernet : adresses MAC source/destination, champ EtherType = 0x0800 (IPv4).

IPv4 (couche réseau)

20 octets d'en-tête IP : adresse source 141.115.64.47 (client), adresse destination 141.115.4.41 (serveur DNS), champ Protocol = 17 (UDP), pas de fragmentation.

UDP (couche transport)

8 octets d'en-tête : port source (éphémère côté client), port destination 53 (DNS), longueur (taille totale de la datagramme), somme de contrôle.

DNS (couche application)

31 octets de données DNS : requête de type A pour www.google.fr, avec l'ID de la requête, flags (0x0100) et section Question (pas de réponses dans ce paquet).

En additionnant ces champs (14 + 20 + 8 + 31), on obtient 73 octets pour le cadre Ethernet complet. Tout de suite après la requête (paquet n°96) se trouve la réponse DNS (paquet n°97), plus volumineuse (251 octets) car elle inclut les enregistrements d'adresses renvoyés par le serveur DNS.

Paquet n°797 : il s'agit d'un paquet ARP (Address Resolution Protocol). ARP ne passe pas par IP, mais directement sur Ethernet pour associer une adresse MAC à une adresse IP dans le même segment réseau.

Ethernet II (couche liaison)

14 octets d'en-tête Ethernet : champ EtherType = 0x0806 (ARP). L'adresse MAC de destination peut être le broadcast (ff:ff:ff:ff:ff:ff) si c'est une requête ARP, ou une MAC spécifique si c'est une réponse.

ARP (« couche 2.5 »)

28 octets de données ARP : type matériel (Ethernet), type protocole (0x0800 = IPv4), longueur d'adresse matérielle (6) et protocole (4), code d'opération (1 = request, 2 = reply), adresses MAC/IP source et destination.

Padding

Pour atteindre la taille minimale d'un cadre Ethernet (64 octets avec FCS, 60 octets sans FCS), on ajoute 18 octets de remplissage.

Le paquet total fait donc 60 octets : 14 (Ethernet) + 28 (ARP) + 18 (padding). ARP étant en dehors du flux IP, on le place souvent "entre" la couche liaison (2) et la couche réseau (3).

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.

Port serveur HTTP (T-SAP) sur 74.125.230.247 : 80

Port client sur 141.115.64.47 : un port: 54258

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).

Pour la couche Réseau (N-SAP) :
Les adresses IP (source/destination) sont 141.115.64.47 et 74.125.230.247.

Le champ Protocol de l’en-tête IP = 6 (TCP).

Pour la couche Liaison (L-SAP) :
Adresses MAC source et destination (par ex. 00:24:81:21:2d:eb → 78:19:f7:98:51:81)
Le champ EtherType = 0x0800 .