TP1 : Analyse des protocoles d'interconnexion avec Wireshark

Objectifs :

- Maitriser le modèle en couches protocolaires
- Analyser les entêtes d'encapsulation des messages de la couche application à la couche physique.
- Etablir une analogie entre le Modèle TCP/IP et le Modèle OSI

1. Prérequis :

Pour faire la séquence, vous avez besoin du logiciel wireshark.

Pour l'installer, il faut aller sur le site suivant:
https://www.wireshark.org/download.html

Comme nous allons voir dans le chapitre de la couche réseaux, la commande ping permet de tester la présence sur le réseau d'une machine dont on connait l'adresse IP ou le nom (host Name), Elle permet également d'avoir une idée de la rapidité de communication avec cette machine.

1) Après avoir ouvert l'invité de commande de Windows, lancer dans cette fenêtre la commande :
ping 192.168.1.1 ou ping 192.168.0.1 en fonction de votre box.

Remplacer cette copie d'écran par la copie de votre écran

```
C:\>ping 192.168.0.5

Envoi d'une requête 'Ping'  192.168.0.5 avec 32 octets de données :
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.5 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

3) Tester le commande: ping nomMachine (C'est le nom d'un PC sur le réseau)
La commande ping fonctionne également avec l'adresse internet d'une machine en dehors du réseau.
4) Tester la commande: ping google.fr

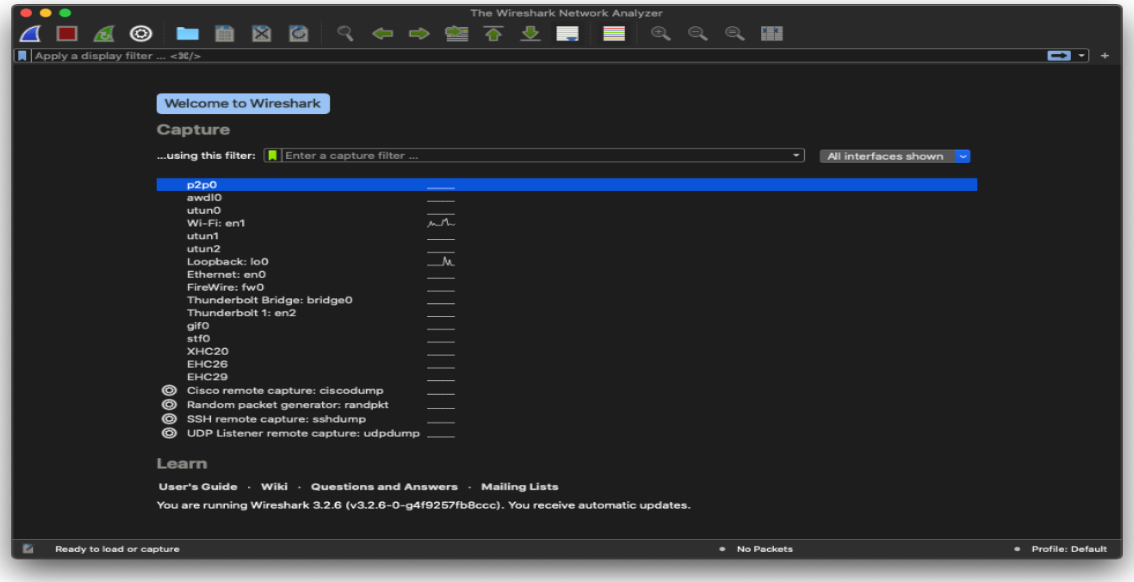
5) Comparer les durées moyennes des ping pour le PC et pour la machine qui héberge le site « google.fr ».

2. Utilisation de Wireshark

Wireshark est un logiciel qui permet d'enregistrer et d'analyser les informations qui circulent le réseau .

2.1 Capture d'une trame :

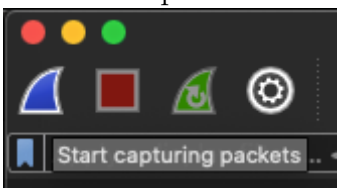
1) Lancer le logiciel Wireshark, la fenêtre suivante apparaît :



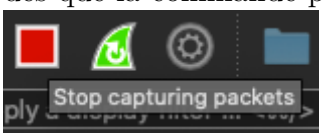
2) Choisir la carte réseau (Ethernet) (c'est celle qui a une activité) :

3) On se propose d'enregistrer les informations circulant pendant l'exécution de la commande:
ping google.fr

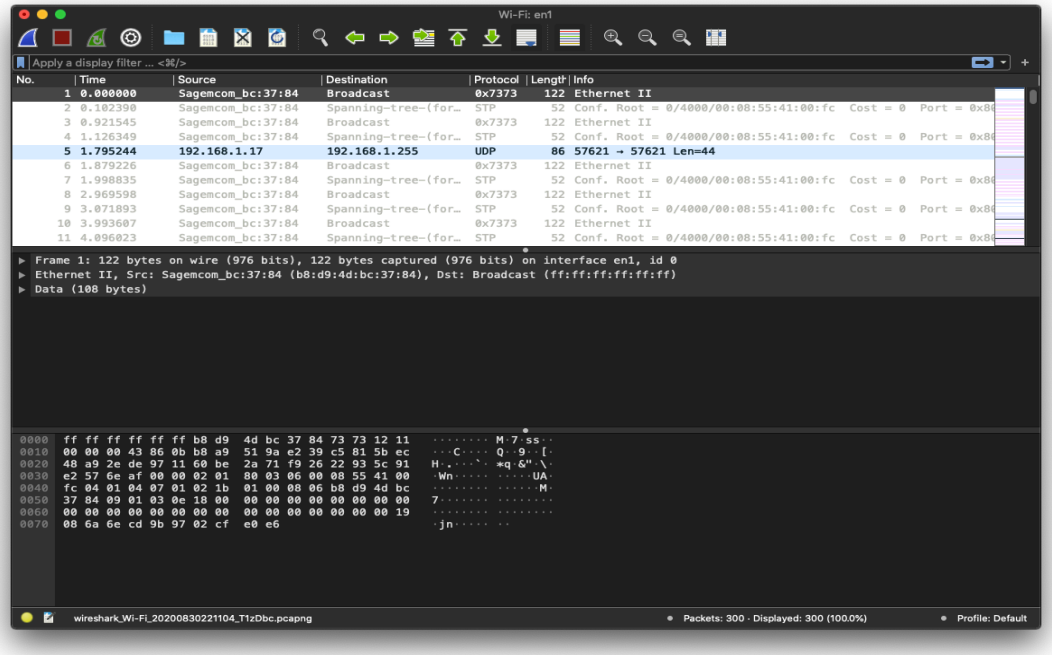
Pour cela il faut:
Ouvrir une fenêtre cmd.exe et écrire la commande ping google.fr sans la valider avec la touche entrée.
ouvrir wireshark
organiser les fenêtres de façon à les voir toutes les deux
lancer la capture dans la fenêtre wireshark en appuyant sur l'icône bleu :



revenir dans la fenêtre cmd.exe et valider la commande avec la touche entrée
retourner dans la fenêtre wireshark et arrêter la capture (en appuyant sur le carré rouge) dès que la commande ping est terminée



Enregistrer la capture dans le dossier Mes documents sous le nom: ping_google.pcap
Observation :
remplacer cette copie partielle d'écran par la copie partielle de votre écran

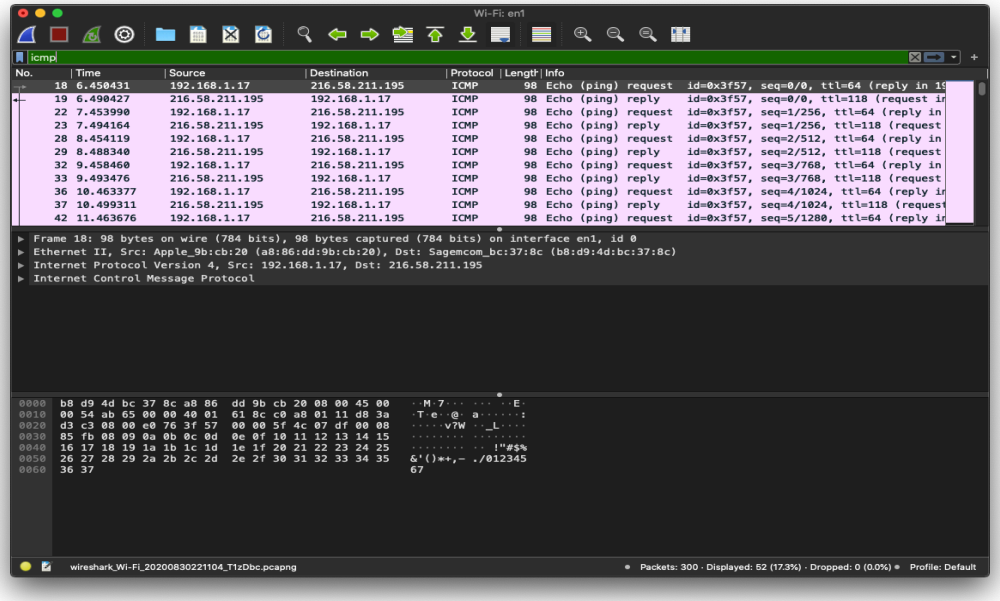


Chaque ligne correspond à un "paquet" d'informations appelé aussi une trame (Frame) ou datagramme. Parmi toutes ces trames certaines n'ont rien à voir avec la commande ping. Seules les trames dont le protocol est ICMP correspondent à l'exécution de cette commande (voir colonne Info).

Utilisation d'un filtre (Filter) pour ne conserver à l'écran que les trames ICMP.

4) Taper icmp dans la fenêtre et cliquer sur apply :

observation: remplacer cette copie d'écran par la copie de votre écran

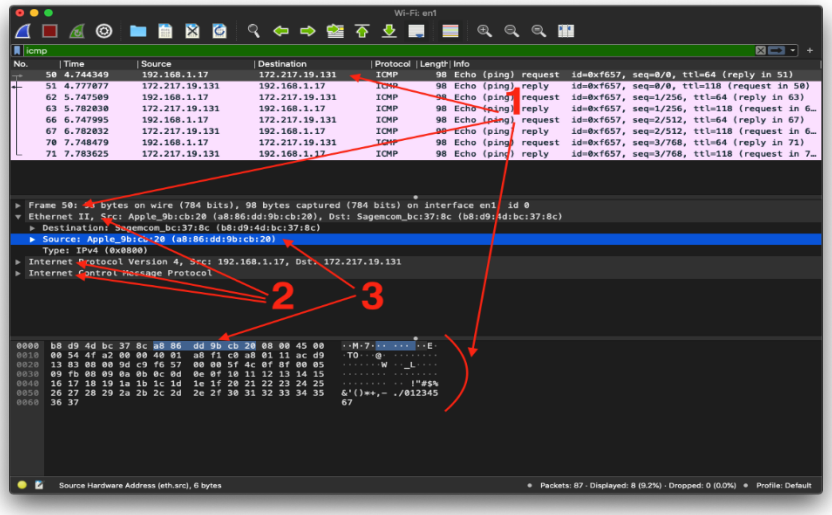


Il ne reste que 8 trames correspondant à une alternance de requêtes (request) et de réponses (reply).

Les requêtes circulent du PC (source) dont l'adresse IP est: .....

au PC (destination) dont l'adresse IP est: .....

2.2 Analyse d'une trame :



Dans l'exemple ci-dessus :

1 – Sur les différentes trames enregistrées, la trame n°50 est sélectionnée, on peut voir les différentes couches qu'elle contient sur la fenêtre du milieu et le détail de la trame en hexadécimal sur la fenêtre du bas.

2 – Cette trame comporte 3 couches : la couche Ethernet, la couche Internet Protocol et la couche Internet Control Message Protocol.

3 – La couche Ethernet de cette trame est détaillée et comporte elle-même 3 champs : le champ Destination, le champ Source et le champ Type. Ici, le champs source est sélectionné, et l'on peut le voir dans la partie hexadécimale.

3. La couche Ethernet

3.1 la structure

1) A partir de la capture réalisée précédemment appliquer un filtre icmp et sélectionner la couche Ethernet de la deuxième trame (ping reply). Compléter alors le tableau suivant:

deuxième trame (ping reply). Compléter alors le tableau suivant :

Contenu			
Champs	Adresse MAC destination	Adresse MAC source	Type*

*Le champ Type définit la couche suivante : 08 00 = couche IP ; 08 06 = couche arp.

2) Observer les autres trames : elles commencent toute par une couche de type Ethernet.

3.2 Rôle

La couche Ethernet permet aux trames de circuler sur le réseau.
Supposons que les machines d'un réseau soient reliées par un hub. Si une machine envoie une trame, celle-ci arrive à toutes les autres machines. Le champ "Adresse MAC destination" de la couche Ethernet permet aux machines réceptrices de savoir si la trame leur est destinée.
Supposons maintenant que les machines d'un réseau soient reliées par un switch. Si une machine envoie une trame, celle-ci arrive au switch. Le champ "Adresse MAC destination" de la couche Ethernet permet au switch de savoir à qui la trame est destinée. Ainsi dans tous les cas la trame arrive à son destinataire.

4. La couche Internet Protocol (IP)

4.1 La structure

1) A partir de la capture réalisée précédemment, appliquer un filtre icmp et sélectionner la couche IP de la deuxième trame. Compléter alors le tableau suivant :

Contenu										
Champs	Version	Differenjtiel services field	Length	identification		flags		Time to live	Protocol	

Contenu										
Champs	Checksum		IP source				IP destination			

Signification des principaux champs :
V: Version (1 quartet) il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4)
H: Header lenght (1 quartet), c'est le nombre de groupes de 4 octets constituant la couche IP (nota : la valeur par défaut est 5, soit 5*4octets=20octets).
Serv: Type de service (1 octet)
Lenght: Longueur totale (2 octets), indique la taille totale de la trame en octets (sans la couche Ethernet). La taille de ce champ étant de 2 octets, la taille totale d'une trame ne peut pas dépasser 65536 octets.
Identification (2 octets)
Offset (2 octets)
Time : Durée de vie (1 octet) appelée aussi TTL, pour Time To Live. Ce champ indique le nombre maximal de routeurs à travers lesquels la trame peut passer. Ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit la trame. Cela évite l'encombrement du réseau.
Protocole (1 octet) : ce champ, permet de savoir quel est le protocole de la couche suivante. exemples ICMP : 0x01 TCP : 0x06 UDP: 0x11
Checksum : Somme de contrôle de l'en-tête,(2 octets) : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de la trame.
Adresse IP source (4 octets) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre
Adresse IP destination (4 octets) : adresse IP du destinataire du message.

4.2 Rôle

La couche IP permet à une machine de dialoguer avec une autre machine qui n'est pas sur le même réseau.

Si une machine A envoie une trame à une machine B n'appartenant pas au même réseau, A envoie la trame à la passerelle, qui fait partie du réseau de A (Adresse MAC destination= passerelle) mais dans la couche IP l'adresse est l'IP de la machine B.

5. Le protocole ICMP (Internet Control Message Protocol)

5.1 La structure

A partir de la capture réalisée précédemment, appliquer un filtre icmp et sélectionner la couche ICMP de la première trame (ping request).

1) Compléter le tableau en indiquant les noms et les nombres d'octets des 6 champs constituant cette couche :

Nom du champ	Type	Code				
Nombre d'octet	1					

2) Observer les différentes trames et en déduire le rôle du champ Type :

3) Observer les différentes trames et en déduire le rôle du champ Séquence number

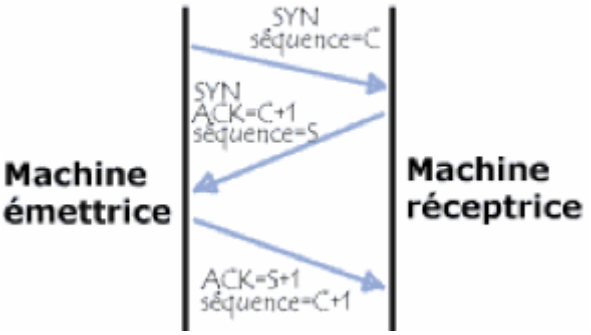
6. La couche TCP

6.1 Le fonctionnement

La couche TCP permet de communiquer en mode connecté, c'est-à-dire avec des accusés de réception permettant à chaque machine de savoir si l'information qu'elle a envoyées a bien été reçue et de faire transiter sur la même ligne plusieurs conversations "simultanément". Ceci est possible grâce au concept de ports (ou sockets): un port est un nombre différent associé à chaque machine et valable pendant une "conversation".

Établissement d'une connexion
Le processus de communication, qui se fait grâce à une émission de données et d'un accusé de réception, est basé sur un numéro d'ordre (Sequence number ou Acknowledgement number), il faut que les machines émettrices et réceptrices (client et serveur) connaissent le numéro d'ordre initial de l'autre machine.

L'établissement de la connexion entre deux applications se fait souvent selon le schéma suivant :



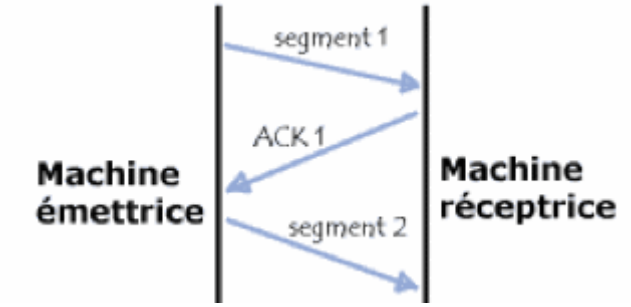
Les deux machines doivent donc synchroniser leurs séquences grâce à un mécanisme communément appelé three ways handshake (poignée de main en trois temps).

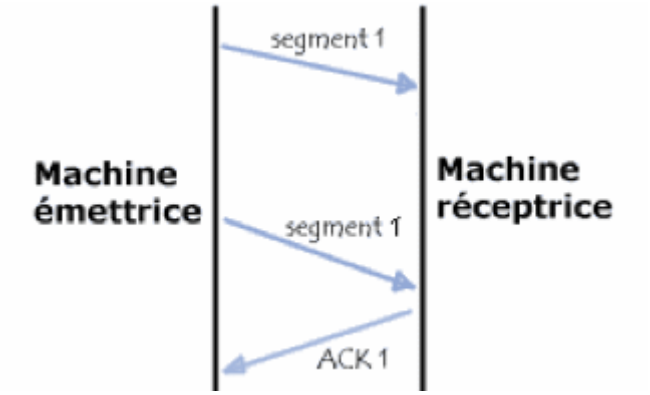
Ce dialogue permet d'initier la communication, il se déroule en trois temps, comme sa dénomination l'indique :

Dans un premier temps la machine émettrice (le client) transmet une trame dont le drapeau SYN est à 1 (pour signaler qu'il s'agit d' une trame de synchronisation), avec un numéro de séquence C
Dans un second temps la machine réceptrice (le serveur) reçoit la trame initiale provenant du client, puis lui envoie un accusé de réception, c'est-à-dire une trame dont le drapeau ACK est à 1 et le drapeau SYN est à 1 (car il s'agit là encore d'une synchronisation). Ce segment contient un numéro de séquence S et un numéro d'accusé de réception C+1,
Enfin, le client transmet au serveur un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est à 1, dont le drapeau SYN est à zéro (il ne s'agit plus d' une trame de synchronisation). Son numéro de séquence est C+1 et son numéro d'accusé de réception est S+1.
Suite à cette séquence comportant trois échanges les deux machines sont synchronisées et la communication peut commencer!

Lors de l'émission d'une trame, un numéro d'accusé de réception et un numéro de séquence sont associés. A réception de cette trame , la machine réceptrice va retourner une trame dont le drapeau ACK est à 1 (afin de signaler qu'il s'agit d'un accusé de réception) accompagné d'un numéro de séquence égal au numéro d' accusé de réception précédent et d'un nouveau numéro d' accusé de réception,

De plus, grâce à une minuterie déclenchée dès l'émission d' une trame au niveau de la machine émettrice, la trame est réexpédié dès que le temps imparti est écoulé, car dans ce cas la machine émettrice considère que la trame est perdu...



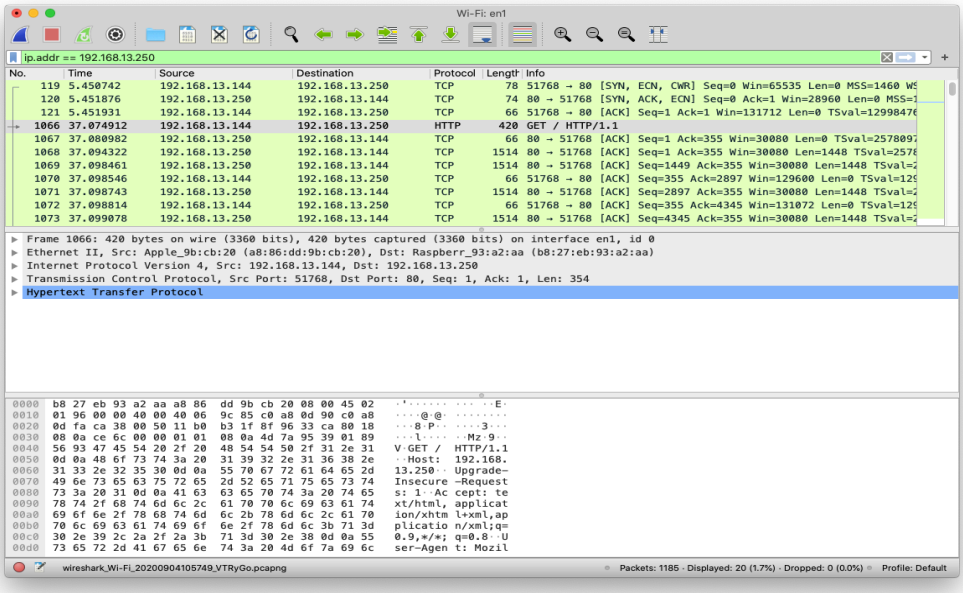


Toutefois, si la trame n'est pas perdue et qu'elle arrive tout de même à destination, la machine réceptrice saura grâce au numéro d'ordre qu'il s'agit d'un doublon et ne conservera que la dernière trame arrivée à destination...

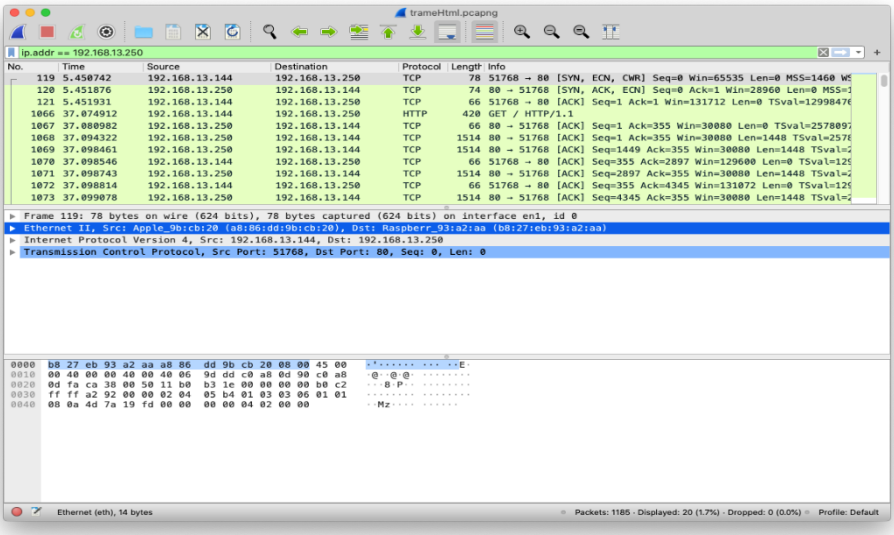
6.2 Observation des trames:

Nous allons à présent visualiser les informations circulant sur le câble Ethernet et correspondant aux échanges entre client et serveur lors de la visualisation de la page HTML du site web edoctorat.usmba.ac.ma hébergée par le serveur Apache situé dans le 196.200.146.55

a. Ouvrir un navigateur web (par exemple Chrome)
b. Ouvrir Wireshark et configurer la capture avec le filtre: ip.addr == 196.200.146.55
c. Lancer la capture dans la fenêtre wireshark
d. Saisir edoctorat.usmba.ac.ma dans votre navigateur et appuyer la touche Entrée
e. Arrêter la capture dans la fenêtre wireshark dés que la page HTML apparaît et sauvegarder dans le dossier Mes documents sous le nom
f. Remplacer cette copie partielle d'écran par la copie partielle de votre écran



g. Relever le contenu complet de la première trame (repérable par l'information [SYN] dans la colonne Info). Remplacer cette copie partielle d'écran par la copie partielle de votre écran



h. Repérer sur la trame précédente les différentes couches

i. A partir de la capture réalisée précédemment, sélectionner la couche TCP (Transmission Control Protocol) de la première trame (repérable par l'information [SYN] dans la colonne Info). Compléter alors le tableau suivant en hexadécimal sauf pour l'octet flag à convertir en binaire:

t flag à convertir en binaire:

Contenu													
champ	Source port		Dest. port		Sequence number				Acknowledgement number				H. len	flag

Le client: je veux communiquer sur le port (……..)H, (port HTML par défaut sur lequel le serveur écoute) il faudra me répondre sur le port (……..)H. mon numéro de séquence est (……..)H

j. même travail pour la deuxième trame (repérable par l'information [SYN ,ACK] dans la colonne Info).

contenu													
champ	Source port		Dest. port		Sequence number				Acknowledgement number				H. len	flag

H. len

flag

le serveur: bien reçu votre n° de séquence, si j'ajoute 1 cela donne(.....)H . Mon numéro de séquence est (.....)H

k. troisième trame (repérable par l'information [ACK] dans la colonne Info).

contenu														
champ	Source port		Dest. port		Sequence number				Acknowledgement number				H. len	flag

Le client: bien reçu votre n° de séquence, si j'ajoute 1 cela donne(.....)H .

l. quatrième trame (GET / HTTP/1.1).

-

contenu														
champ	Source port		Dest. port		Sequence number				Acknowledgement number				H. len	flag

Le client: voici mon message (voir couches suivante de cette trame), son n° d' accusé de réception est (.....)H .

m. cinquième trame (HTTP/1.1 200 OK).

-

contenu														
champ	Source port		Dest. port		Sequence number				Acknowledgement number				H. len	flag

Le serveur: j'ai bien reçu votre message n°(.....)16 voici ma réponse (voir couches suivante de cette trame) son n° d' accusé de réception est (.....)16 .

7. La couche HTTP

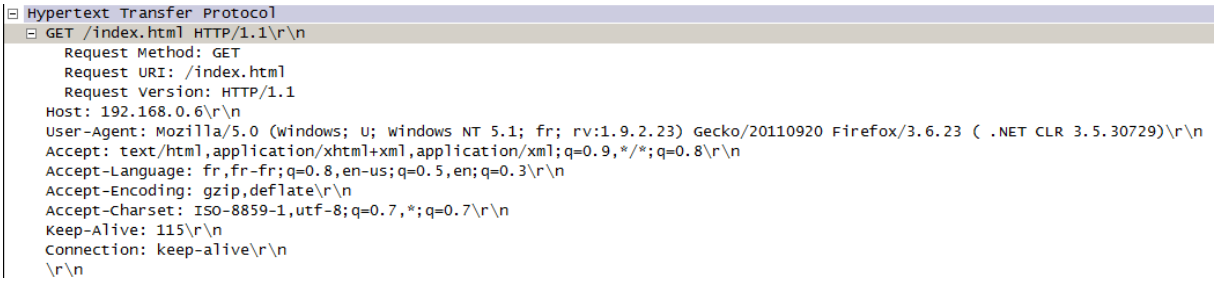
7.1 Observation des trames

a. Combien de couche comporte la trame "GET /index.html HTTP/1.1"

b. Quelle est la machine qui a émis cette trame et quel est le statu (client ou serveur) de cette machine?

c. A partir de la capture réalisée précédemment sélectionner la couche HTTP (Hypertext Transferl Protocol) de la trame "GET /index.html HTTP/1.1"

d. Remplacer cette copie partielle d'écran par la copie partielle de votre écran



Remarque: la couche http est un texte codé en ASCII, les "\r\n" correspondes aux octets 0d(Carriage Return) et 0a (Line Feed).

e. Combien de lignes cette couche http comporte elle?
La couche étudiée est un demande émise par une machine ayant un statut de client. On l'appelle une requête http.

7.2 structure d'une requête http:

- ligne de requête:

	Method	Request URI*	HTTP-version
exemple:	GET	/exemple1.html	HTTP1.1

*Uniform Resource Identifier

- lignes suivantes: (facultatives): ces lignes fournissent des informations sur le client HTML :

Exemples:

User-Agent	indique le client HTML utilisé
Accept-Language	indique que langue doit être utilisée pour la réponse

Accept	indique le type de donnée à utiliser pour la réponse

7.3 structure d'une réponse http:

- ligne de réponse:

Compléter le tableau dans le cas d'une réponse à la requête.

Reponse version	Status-Code	Reponse-Phrase
.		

- lignes suivantes: (facultatives): ces lignes fournissent des informations fournies par le serveur HTML :

exemples:

Server	indique le serveur HTML utilisé
Date	indique que date de la réponse
Keep-Alive	indique la durée pendant laquelle le serveur restif actif en cas de nom réponse du client

- Ligne : indiquer dans votre cas ces lignes :

gne : indiquer dans votre cas ces lignes :

Server	
Date	
Keep-Alive	