ExoLab : Etude des couches du modèle OSI

a) Installer le logiciel « Wireshark » sur votre PC.

b) Lancez une capture de trames sur votre carte réseau.

c) Utilisez votre navigateur pour générer du trafic sur votre interface réseau. Vous devez voir apparaitre les trames capturées, dans le cas contraire sélectionnez une autre interface réseau.

d) Quelles données voyez-vous apparaitre dans la fenêtre du haut ?
On observe les trames capturées : n° trame, heure de la capture, ip source, ip destination, protocole, longueur trame, descriptif

e) Donner des exemples de protocoles capturés.
TCP, IP, ARP, http, UDP, DNS, TLS, DHCP, …

f) Sélectionnez et analyser quelques trames capturées. Toutes les couches du modèle OSI sont-elles représentées dans la fenêtre du milieu ? Expliquez.
Certaines trames ne contiennent pas toutes les couches du modèle osi.
Exemple : trame échangées pour établir une session TCP, …

g) Choisissez une trame dans laquelle le protocole HTTP est présent (il faut pour cela que vous génériez du trafic avec votre navigateur). Sélectionnez ensuite dans la fenêtre du milieu les différents protocoles présents dans cette trame (Ethernet, IP, TCP, HTTP).

h) Quels sont les 2 types d'échanges entre le client et le serveur web ?

- La requête http du client vers le serveur
- La réponse du serveur web (page en html et css) vers le client web

i) Comment sont encapsulées les données HTTP pour, finalement, constituer une trame circulant sur le réseau ?

j) Lancer une nouvelle capture, ouvrir CMD et effectuer un ping vers le serveur google.com.

k) Effectuer un filtre sur le protocole ICMP. Quels sont les 2 types d'échanges effectués avec le protocole ICMP ? Quelle est l'adresse IP du serveur google.com ? Est-ce une adresse publique ou privée ?
Il y a 2 trames échangées :

- La requête « ECHO » de l'émetteur
- La réponse « REPLAY » du destinataire

Google.com a une adresse IP publique.
Remarque : ICMP est un protocole de la couche 3 OSI.

l) Lancer une nouvelle capture, ouvrir CMD et taper la commande : ***nslookup*** ac-limoges.fr

```
C:\Users\emile>nslookup ac-limoges.fr
Serveur :   dc1-0870019y.0870019y.lan
Address:  10.187.88.5

Réponse ne faisant pas autorité :
Nom :    ac-limoges.fr
Address:  185.75.143.93
```

Nslookup permet de tester le fonctionnement du service DNS en demandant la résolution d'un nom de domaine en adresse IP.
Ici, notre serveur DNS 10.187.88.5 nous a renvoyé l'adresse 185.75.143.93 correspondant au nom ac-limoges.fr.
Remarque : le serveur DNS 10.187.88.5 n'est pas autoritaire sur le domaine ac-limoges.fr. C'est un résolveur qui effectue la recherche auprès des serveurs DNS d'internet.

m) Quelle est l'adresse IP du serveur ac-limoges.fr ?
L'adresse IP du serveur ac-limoges.fr est 185.75.143.93.

n) Quelle est l'adresse du serveur qui a envoyé le résultat ?
L'adresse du serveur qui a envoyé le résultat est 10.187.88.5.

o) Effectuer un filtre sur le protocole DNS.

- Que contient la requête DNS ?

```
> Frame 94: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{26B17168-
> Ethernet II, Src: Fortinet_d1:34:2e (e0:23:ff:d1:34:2e), Dst: AzureWav_81:f7:0f (14:13:33:81:f7:0f)
> Internet Protocol Version 4, Src: 10.187.88.5, Dst: 10.187.35.113
> User Datagram Protocol, Src Port: 53, Dst Port: 58066
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ac-limoges.Fr: type A, class IN
        Name: ac-limoges.Fr
        [Name Length: 13]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  > Answers
    [Request In: 93]
    [Time: 0.006078000 seconds]
```

- Que contient la réponse DNS ?