UTILISATION DE WIRESHARK POUR AFFICHER DES UNITÉS DE DONNÉES DE PROTOCOLE ET METTRE EN EVIDENCE LES COUCHES DU MODELE OSI

OBJECTIFS

```
* Expliquer l'objectif d'un analyseur de protocoles (Wireshark).
* Exécuter une capture de base des unités de données de protocole (PDU) à l'aide de Wireshark.
* Exécuter une analyse de base des PDU sur un trafic de données réseau simple.
* Se familiariser aux fonctionnalités et options de Wireshark telles que la capture des PDU et le
filtrage   de l'affichage.
* Identifier les couches du modèles OSI à l'aide d'une analyse de trame.
```

COURS DE REFERENCE ASSOCIE

RAPPEL SUR LES MODELES OSI ET TCP/IP

ET HOP ! C'EST PARTI !

1 – lancer l'émulateur RINN.

2 – S'assurer que la MV Ubuntu-Server communique bien avec l'Internet par les commandes suivantes :

```
$  ping   -c 4   8.8.8.8
```

Le ping doit répondre.

Entrez la commande :

```
$ host 8.8.8.8
```

Quel est le rôle de la commande « host » ? A quoi correspond l'adresse 8.8.8.8 ?

Vérifiez que l'on trouve un résultat similaire avec les commandes « dig » et « nslookup » Si le ping ne répond pas, tentez d'obtenir automatiquement une configuration réseau en interrogeant un éventuel serveur DHCP :

```
# dhclient
```

CAPTURE !

3 – lancer Wireshark.

4 – lancer une capture de trames en choisissant la bonne interface réseau.

4 – faire un ping de 4 coups sur « www.free.fr »

5 – stopper la capture.

ANALYSE DES TRAMES DNS

6 – filtrer les trames relatives au protocole DNS. A quoi correspond le protocole DNS ?

7 – sélectionner la première trame de la liste.

8 – Faites apparaître de manière claire les couches 2, 3 et 4 de la trame sélectionnée.

Quel nom est donné par Wireshark à la couche 2 ? A la couche 3 ? A la couche 4 ?

9 – Quelle est la longueur en octets de la trame sélectionnée ?

10 – A quel type d'adresses fait référence la couche 2 ?

11 – De combien de champs est composée une adresse de couche 2 ? Quel est le nom du constructeur des cartes Ethernet concernées par la trame sélectionnée ? Quelle est la longueur exprimée en bits d'une adresse couche 2 ?

12 - A quel type d'adresses fait référence la couche 3 ?

13 – Quelle est la longueur exprimée en bits d'une adresse couche 3 ? Retrouvez l'équivalent hexadécimal de l'adresse source couche 3 de la trame sélectionnée.

14 - A quel type d'adresses fait référence la couche 4 ? Réfléchissez bien ! )

15 – Quel est le numéro du port source référencé dans la couche 4 ? Quel est le numéro du port destination référencé dans la couche 4 ? Existe-t-il un port « bien connu » de vous ?

16 – Au final, à quoi sert exactement cette trame ?

ANALYSE DES TRAMES ICMP

17 – filtrer les trames relatives au protocole ICMP. A quoi correspond le protocole ICMP ?

18 – sélectionner la première trame de la liste.

19 – Faites apparaître de manière claire les couches 2, 3 de la trame sélectionnée.

20 – Peut-on visualiser la couche 4 ? Justifiez !

21 – Quel est le type du message ICMP véhiculé par la trame sélectionnée ? A quoi correspond ce type ?

22 – sélectionner la deuxième trame de la liste.

23 - Quel est le type du message ICMP véhiculé par la trame sélectionnée ? A quoi correspond ce type ?