TP PROTOCOLE DNS

Exercice 1 :

1. Configuration de Wireshark :
   - Lancez Wireshark et sélectionnez l'interface réseau à surveiller.
   - Configurez un filtre pour ne capturer que le trafic DNS. Entrez dns dans la barre de filtre d'affichage de Wireshark.

2. Capture de Trafic DNS :
   - Démarrez la capture de paquets sur Wireshark.
   - Ouvrez un navigateur web et visitez le site web **newtonformationsnir.fr**
   - Arrêtez la capture après quelques minutes.

3. Analyse des Paquets DNS :
   - Utilisez les capacités de filtrage et d'analyse de Wireshark pour examiner les requêtes et réponses DNS capturées.
   - Identifiez les requêtes DNS (paquets avec le port 53 et le flag "Standard query") et les réponses correspondantes.

4. Points à Examiner :
   - Observez la structure d'une requête DNS, y compris le nom de domaine demandé.
   - Examinez une réponse DNS, notant l'adresse IP renvoyée, le TTL, et d'autres informations.
   - Si possible, capturez des requêtes pour des domaines jamais visités auparavant pour observer la résolution DNS complète.

Exercice 2 : Utilisation de dig

1. Requête de base :
   - Exécuter dig newtonformationsnir.fr pour obtenir une réponse plus détaillée sur le domaine.

2. Traçabilité de la requête :
   - Exécuter dig +trace newtonformationsnir.fr pour voir le chemin complet de résolution DNS, du serveur racine au serveur autoritaire.

3. Afficher un type d'enregistrement spécifique :
   - Exécuter dig newtonformationsnir.fr MX pour voir les enregistrements de serveur de messagerie.

4. Obtenir des informations spécifiques :
   - Exécuter dig newtonformationsnir.fr +noall +answer pour afficher seulement la section de réponse.