Laboratoire 2 : Le protocole DNS (corrigé)

2. Utilisation de DNS avant une requête HTTP

a. Localisez les paquets DNS requête et réponse. Quel est le protocole de la couche transport utilisé, TCP ou UDP?

Réponse: UDP.

b. À Quelle adresse IP la requête DNS est envoyée? Utilisez la commande ipconfig pour déterminer l'adresse IP du serveur DNS local. Est-ce que les deux adresses IP sont les mêmes?

Réponse : Adresse IP du serveur DNS local. Les mêmes adresses.

c. Examinez la requête DNS. Quel est le "type" de cette requête? Est-ce que cette requête contient des réponses?

Réponse : Type A. Ne contient pas de réponses.

```
Questions: 1
Answer RRs: 0
▾ Queries
  ▾ www.ietf.org: type A, class IN
      Name: www.ietf.org
```

d. Examinez la réponse DNS. Combien de réponses sont fournies? Quel est le contenu de chaque réponse?

Réponse : 2 réponses de type=A avec nom de domaine et adresse IP.

```
▾ Answers
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 214
      Data length: 4
      Address: 104.20.1.85
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 214
      Data length: 4
      Address: 104.20.0.85
```

e. Cette page web contient des images. Avant de télécharger chaque image, est ce que votre poste de travail a envoyé d'autres requêtes DNS?

Réponse : Non. L'adresse IP de ietf.org est stockée dans le cache.

3. Utilisation de DNS avec nslookup

f. Quelle est le port de destination de la requête DNS? Quelle est le port source de la réponse DNS?

Réponse : Port 53. Port 53.

g. À quelle adresse IP la requête DNS est-elle envoyée? Est-ce l'adresse IP de votre serveur DNS local?

Réponse : Adresse IP du serveur DNS local. Oui.

h. Examinez une des requêtes DNS résultat de la commande nslookup. Quel est le "type" de la requête? Est-ce que la requête contient des réponses?

Réponse : Type A. Ne contient pas de réponses.

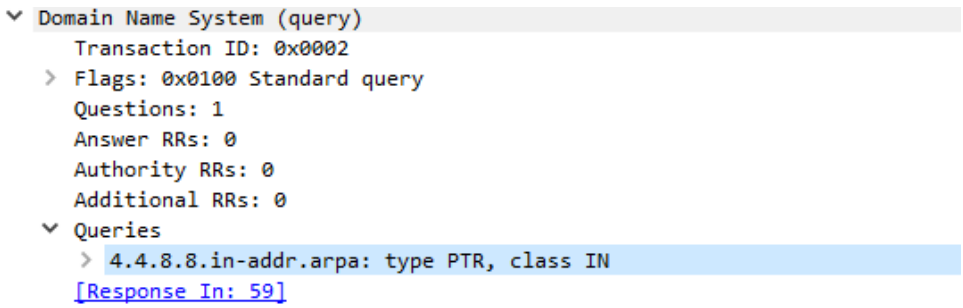
i. Examinez la réponse DNS de la requête de la question h. Combien y-a-t-il de réponses? Que contient chaque réponse? Inscrivez les trois ou quatre premières lignes de la réponse.

Réponse : Une réponse avec le nom du serveur, type d'adresse et l'adresse IP.

4. Requête DNS inversée (reverse DNS lookup)

j. Examinez la requête DNS résultat de la commande nslookup. Quel est le "type" de la requête? Quel est le nom de domaine contenu dans la question formulée par la requête?

Réponse : Requête de type=PTR. Le nom de domaine est 4.4.8.8.in-addr.arp.



k. Examinez la réponse DNS de la requête de la question j. Combien y-a-t-il de réponses? Que contient chaque réponse? À quoi correspond?

Réponse : Une seule réponse. La réponse contient le nom de domaine du serveur DNS de google: dns.google.

```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  > Queries
  v Answers
    v 4.4.8.8.in-addr.arpa: type PTR, class IN, dns.google
          Name: 4.4.8.8.in-addr.arpa
          Type: PTR (domain name PoinTeR) (12)
          Class: IN (0x0001)
          Time to live: 3871
          Data length: 12
          Domain Name: dns.google
  > Authoritative nameservers
  > Additional records
    [Request In: 58]
    [Time: 0.024756000 seconds]
```

l. 8.8.4.4 correspond à l'adresse IP du serveur DNS de google. Donnez la commande qui permet d'utiliser ce serveur pour faire la résolution DNS à la place de votre serveur DNS local par défaut.

Réponse : La commande est "nslookup – 8.8.4.4".

m. Lancez la commande de la question l. et analyser le comportement de votre client DNS. (Vous pouvez utiliser Wireshark pour avoir une idée plus claire sur ce qui se passe.)

Réponse : L'adresse IP destination de la première requête est l'adresse IP du serveur DNS de google.

```
C:\Users\Cirine Chaieb>nslookup - 8.8.4.4
Serveur par dÚfaut :   dns.google
Address:  8.8.4.4

> www.google.ca
Serveur :   dns.google
Address:  8.8.4.4
```

dns

No.	Time	Source	Destination	Protocol	Length	Info
…	10.547…	192.168.0…	8.8.4.4	DNS	73	Standard query 0x0002 A www.google.ca
…	10.646…	8.8.4.4	192.168.0…	DNS	89	Standard query response 0x0002 A www.google.ca A 172.217.10.…

5. Requête DNS itérative

n. Avant d'analyser les paquets capturés par Wireshark, donnez une première explication de la dernière réponse obtenue par nslookup. En d'autres termes, pourquoi on n'arrive pas à obtenir l'adresse IP de www.cbc.ca?

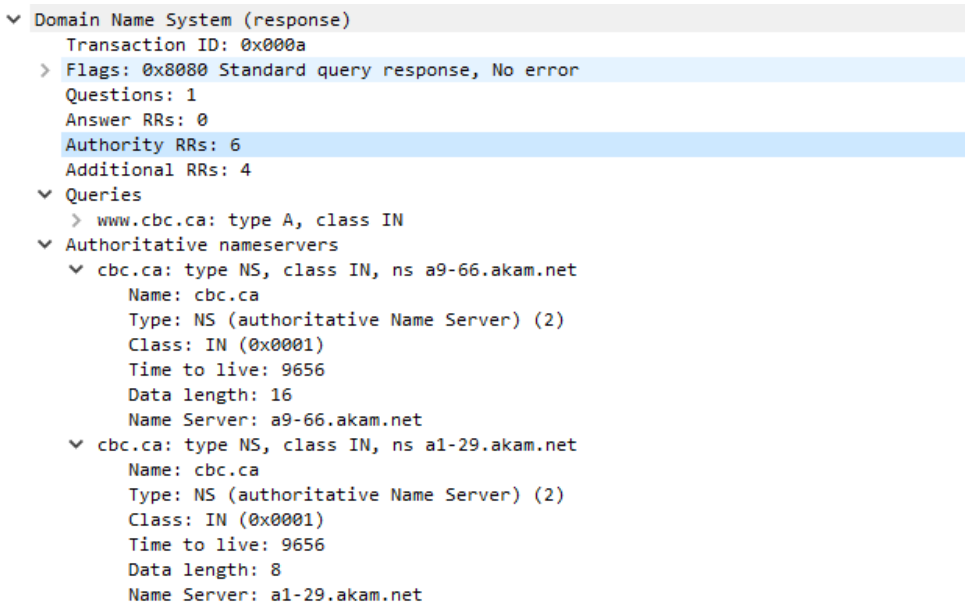
Réponse: Dû à l'utilisation de la commande "set norecurse" .

o. Dans Wireshark, examinez la requête DNS résultat de la commande nslookup. Quel est le "type" de la requête?

Réponse: Type A.

p. Examinez la réponse DNS de la requête de la question o. Combien y-a-t-il de réponses? À quoi sert le contenu des "Authority RRs"?

Réponse: Aucune réponse. "Authority RRs" liste les serveurs qui font autorité.



q. Quel est l'effet de la commande set norecurse sur le comportement du client DNS?

Réponse: La commande "set norecurse" oblige le client DNS à envoyer des requêtes récursives, au lieu des requêtes itératives. Par conséquent, si le serveur local ne possède pas la correspondance demandée, il va retourner les adresses d'autres serveurs.

r. Utilisez le contenu des "Authority RRs" pour lancez une commande nslookup qui permet d'obtenir l'adresse IP de www.cbc.ca.

Réponse: La commande est "server [adresse IP d'un serveur appartenant à la liste authoritative nameservers]". Elle permet d'interroger directement le serveur faisant autorité sur le nom de domaine www.cbc.ca