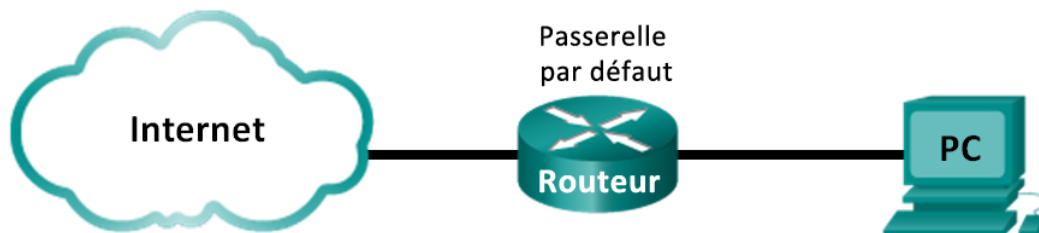


Travaux pratiques – Utilisation de Wireshark pour examiner une capture DNS UDP

Topologie



Objectifs

- 1re partie : Enregistrer les informations de configuration IP d'un ordinateur
- 2e partie : Utiliser Wireshark pour capturer les requêtes et les réponses DNS
- 3e partie : Analyser les paquets DNS ou UDP capturés

Contexte/scénario

Si vous avez déjà utilisé Internet, vous avez utilisé le système de noms de domaine (DNS). DNS est un réseau distribué de serveurs qui traduit les noms de domaine faciles à utiliser comme `www.google.com` en adresse IP. Lorsque vous tapez l'adresse URL d'un site Web dans votre navigateur, votre PC envoie une requête DNS à l'adresse IP du serveur DNS. La requête du serveur DNS de votre ordinateur et la réponse du serveur DNS utilisent le protocole UDP (User Datagram Protocol) comme protocole de couche transport. À la différence du protocole TCP, le protocole UDP est sans connexion et ne nécessite aucune configuration de session. Les requêtes et les réponses DNS sont très petites et ne génèrent pas de surcharge comme le protocole TCP.

Dans le cadre de ces travaux pratiques, vous communiquerez avec un serveur DNS en envoyant une requête DNS à l'aide du protocole de transport UDP. Vous utiliserez Wireshark pour examiner les échanges de requêtes et de réponses DNS avec le serveur de noms.

Remarque : ce TP ne peut être effectué avec Netlab. Ce TP suppose que vous ayez accès à internet.

Ressources requises

1 ordinateur (Windows 7, Vista ou XP, équipé d'un accès à Internet, d'un accès aux invites de commande et de Wireshark)

1re partie : Enregistrer les informations de configuration IP d'un ordinateur

Dans la première partie, vous utiliserez la commande `ipconfig /all` sur votre ordinateur local pour trouver et enregistrer les adresses MAC et IP de la carte d'interface de votre ordinateur, l'adresse IP de la passerelle par défaut spécifiée et l'adresse IP du serveur DNS spécifiée pour l'ordinateur. Enregistrez ces informations dans la table fournie. Elles seront utilisées dans les sections suivantes de ces travaux pratiques avec l'analyse des paquets.

Adresse IP	
Adresse MAC	
Adresse IP de la passerelle par défaut	
Adresse IP du serveur DNS	

2e partie : Utiliser Wireshark pour capturer les requêtes et les réponses DNS

Dans la deuxième partie, vous installerez Wireshark pour capturer les paquets de requête et de réponse DNS pour illustrer l'utilisation du protocole de transport UDP tout en communiquant avec un serveur DNS.

- a. Cliquez sur le bouton **Démarrer** de Windows et accédez au programme Wireshark.

Remarque : si Wireshark n'est pas encore installé, il peut être téléchargé à l'adresse <http://www.wireshark.org/download.html>.

- b. Sélectionnez une interface pour Wireshark afin de capturer des paquets. Utilisez **Interface List** pour choisir l'interface associée aux adresses IP et MAC (Media Access Control) du PC enregistrées dans la première partie.
- c. Après avoir sélectionné l'interface souhaitée, cliquez sur **Démarrer** pour capturer les paquets.
- d. Ouvrez un navigateur Web et tapez **www.google.com**. Appuyez sur Entrée pour continuer.
- e. Cliquez sur **Stop (Arrêter)** pour arrêter la capture Wireshark lorsque la page d'accueil de Google s'affiche.

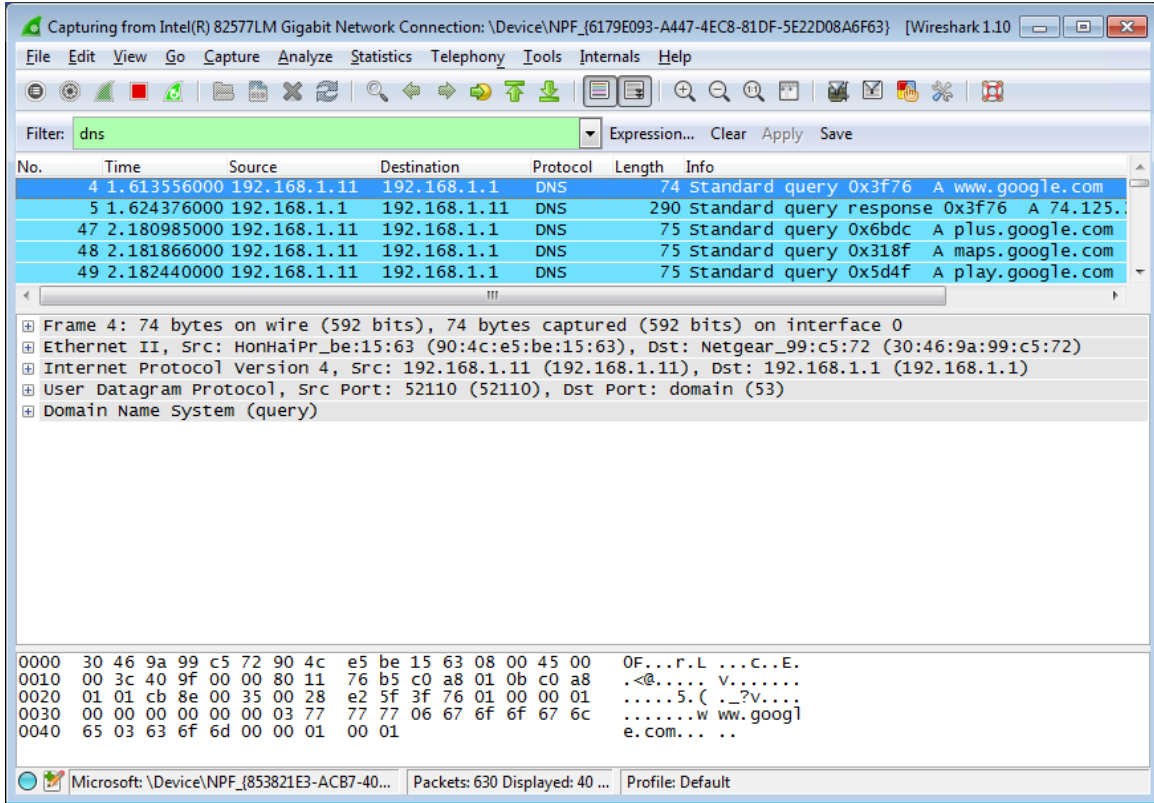
3e partie : Analyser les paquets DNS ou UDP capturés

Dans la troisième partie, vous examinerez les paquets UDP qui ont été générés lors de la communication avec un serveur DNS des adresses IP pour **www.google.com**.

Étape 1 : Filtrez les paquets DNS.

- a. Dans la fenêtre principale de Wireshark, tapez **dns** dans la zone de saisie de la barre d'outils **Filter** (Filtre). Cliquez sur **Apply (Appliquer)** ou appuyez sur Entrée.

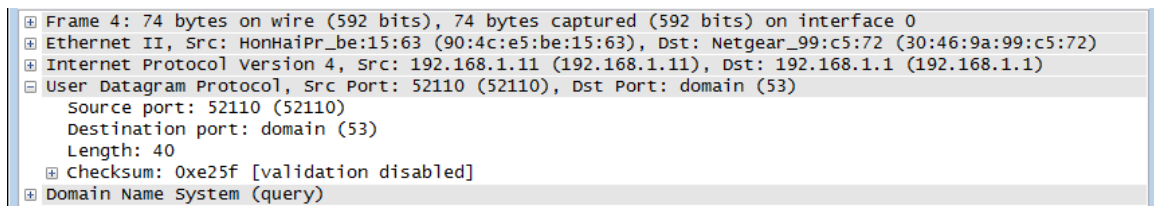
Remarque : si vous ne voyez aucun résultat après l'application du filtre DNS, fermez le navigateur web et dans la fenêtre d'invite de commandes, tapez **ipconfig /flushdns** pour supprimer tous les résultats DNS précédents. Redémarrez la capture Wireshark et répétez les instructions des sections b à e de la deuxième partie. Si cela ne résout pas le problème, dans la fenêtre d'invite de commandes, vous pouvez taper **nslookup www.google.com** au lieu d'utiliser le navigateur Web.



- b. Dans le volet de la liste des paquets (section supérieure) de la fenêtre principale, localisez le paquet qui inclut « standard query » et « A www.google.com ». Voir la trame 4 comme exemple.

Étape 2 : Examinez le segment UDP au moyen d'une requête DNS.

Examinez le segment UDP à l'aide d'une requête DNS pour www.google.com telle que capturée par Wireshark. Dans cet exemple, la trame 4 de capture Wireshark dans le volet de la liste des paquets est sélectionnée pour l'analyse. Les protocoles dans cette requête apparaissent dans le volet de détails des paquets (section centrale) de la fenêtre principale. Les entrées de protocole sont mises en surbrillance en gris.



- a. Dans le volet de détails des paquets, la trame 4 possède 74 octets de données sur le câble comme indiqué à la première ligne. C'est le nombre d'octets nécessaires pour envoyer une requête DNS à un serveur de noms demandant les adresses IP de www.google.com.
- b. La ligne Ethernet II affiche les adresses MAC source et de destination. L'adresse MAC provient de votre PC local, car c'est lui qui a émis la requête DNS. L'adresse MAC de destination provient de la passerelle par défaut, car c'est le dernier arrêt avant la sortie de cette requête du réseau local.

L'adresse MAC source est-elle identique à celle enregistrée dans la première partie pour le PC local ?

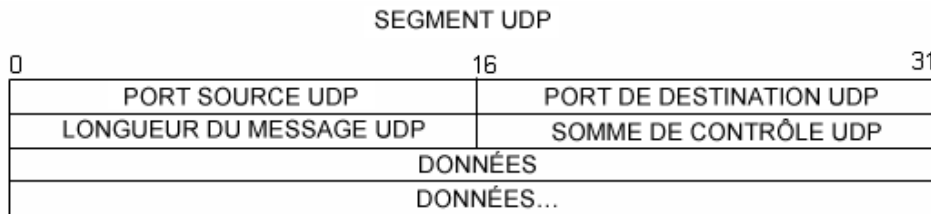
- c. Sur la ligne Internet Protocol Version 4, la capture Wireshark de paquets IP indique que l'adresse IP source de cette requête DNS est 192.168.1.11 et l'adresse IP de destination est 192.168.1.1. Dans cet exemple, l'adresse de destination est la passerelle par défaut. Le routeur est la passerelle par défaut sur ce réseau.

Pouvez-vous associer les adresses MAC et IP pour les périphériques source et de destination ?

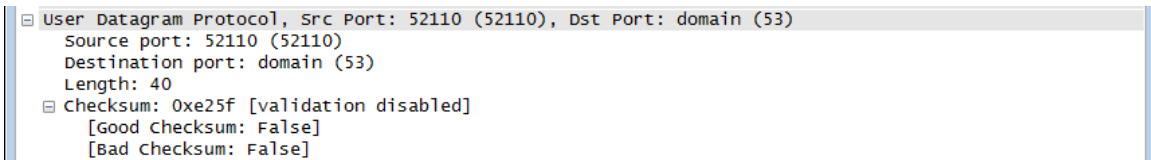
Périphérique	Adresse IP	Adresse MAC
PC local		
Passerelle par défaut		

L'en-tête et le paquet IP encapsulent le segment UDP. Le segment UDP contient la requête DNS comme données.

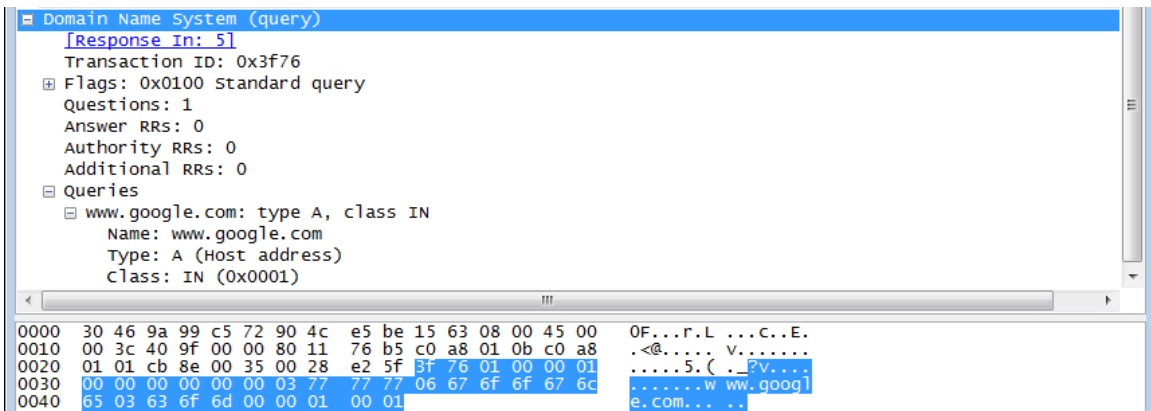
- d. Un en-tête UDP comporte uniquement quatre champs : source port (port source), destination port (port de destination), length (longueur) et checksum (somme de contrôle). Chaque champ de l'en-tête UDP ne dispose que de 16 bits comme indiqué ci-dessous.



Développez le protocole UDP (User Datagram Protocol) dans le volet de détails des paquets en cliquant sur le signe plus (+). Notez qu'il n'existe que quatre champs. Le numéro du port source dans cet exemple est 52110. Le port source a été généré aléatoirement par le PC local au moyen des numéros de port qui ne sont pas réservés. Le port de destination est le 53. Le port 53 est un port réservé destiné à une utilisation avec DNS. Les serveurs DNS écoutent sur le port 53 les requêtes DNS provenant des clients.



Dans cet exemple, la longueur de ce segment UDP est de 40 octets. Sur 40 octets, 8 sont utilisés pour l'en-tête. Les 32 autres octets sont utilisés par les données de requête DNS. Les 32 octets de données de requête DNS sont mis en surbrillance dans l'illustration suivante du volet d'octets des paquets (section inférieure) de la fenêtre principale de Wireshark.



La somme de contrôle est utilisée pour déterminer l'intégrité du paquet une fois qu'il a transité par Internet.

L'en-tête UDP surcharge peu le réseau parce que le protocole UDP n'a pas de champs associés à l'échange en trois étapes du protocole TCP. Tous les problèmes de fiabilité liés au transfert des données doivent être gérés par la couche application.

Notez les résultats de Wireshark dans la table ci-dessous :

Taille de trame	
Adresse MAC source	
Adresse MAC de destination	
Adresse IP source	
Adresse IP de destination	
Port source	
Port de destination	

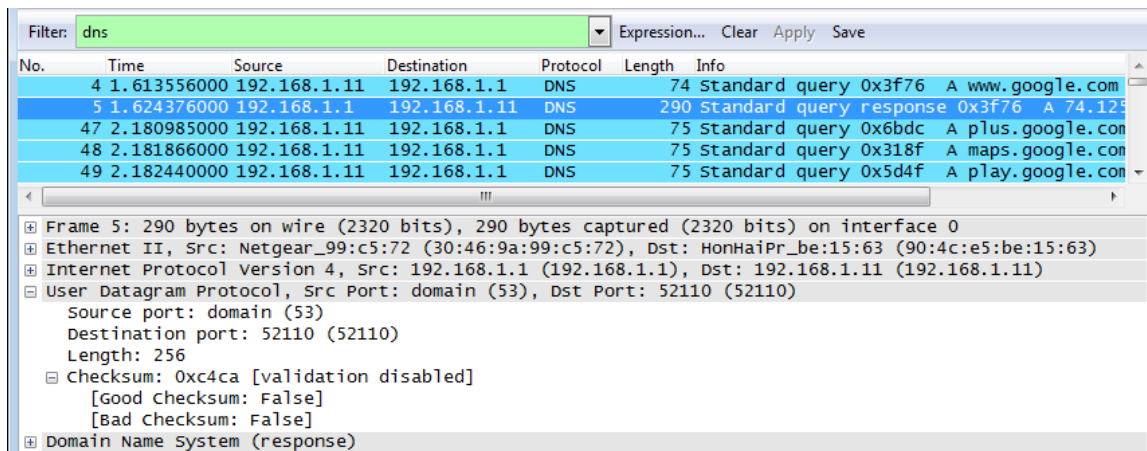
L'adresse IP source est-elle identique à l'adresse IP du PC local enregistrée dans la première partie ?

L'adresse IP de destination est-elle identique à la passerelle par défaut notée dans la première partie ?

Étape 3 : Examinez le protocole UDP au moyen des réponses DNS.

Dans cette étape, vous examinerez le paquet de réponse DNS et vérifierez que le paquet de réponse DNS utilise aussi le protocole UDP.

- a. Dans cet exemple, la trame 5 est le paquet de réponse DNS correspondant. Notez que le nombre d'octets sur le câble correspond à 290 octets. Il s'agit d'un paquet plus gros par rapport au paquet de requête DNS.



- b. Dans la trame Ethernet II pour la réponse DNS, de quel périphérique provient l'adresse MAC source et à quel périphérique correspond l'adresse MAC de destination ?

- c. Notez les adresses IP source et de destination du paquet IP. Quelle est l'adresse IP de destination ? Quelle est l'adresse IP source ?

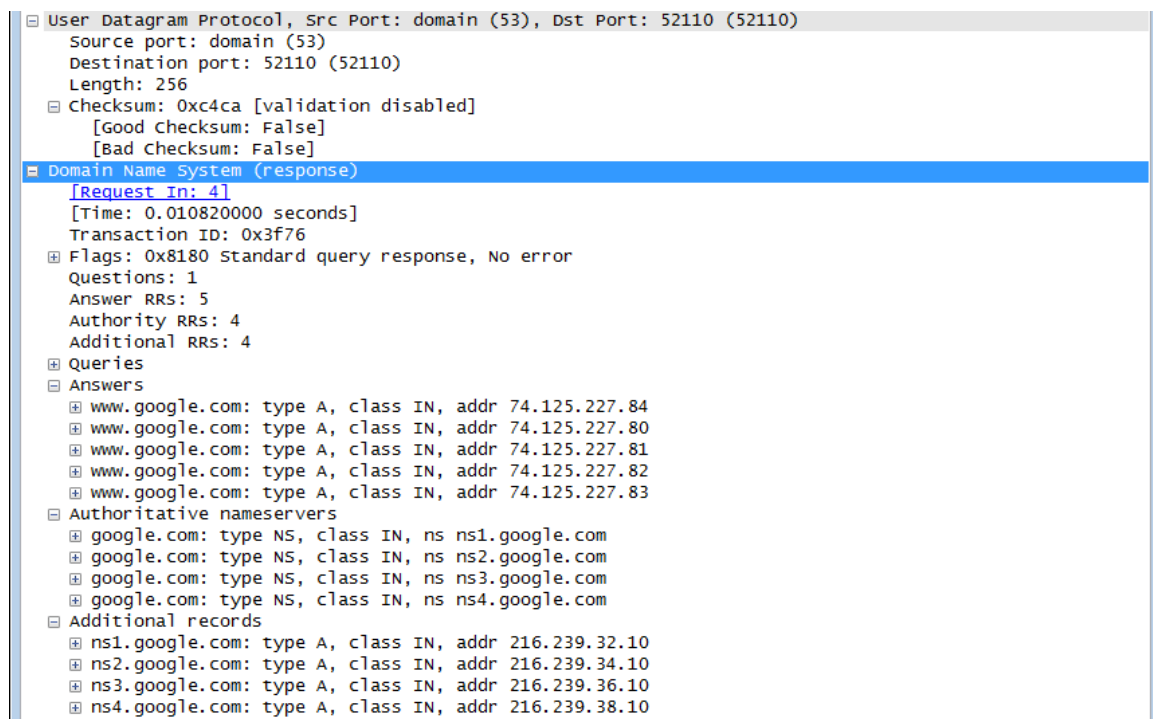
Adresse IP de destination : _____ Adresse IP source : _____

Qu'est-il arrivé aux rôles de la source et de la destination pour l'hôte local et la passerelle par défaut ?

- d. Dans le segment UDP, le rôle des numéros de port a également été inversé. Le numéro du port de destination est 52110. Le numéro de port 52110 est le même port que celui qui a été généré par le PC local lorsque la requête DNS a été envoyée au serveur DNS. Votre PC local attend une réponse DNS sur ce port.

Le numéro du port source est 53. Le serveur DNS attend une requête DNS sur le port 53, puis envoie une réponse DNS avec le numéro de port source 53 à l'émetteur de la requête DNS.

Lorsque la réponse DNS est développée, examinez les adresses IP résolues pour `www.google.com` dans la section **Answers (Réponses)**.



```

User Datagram Protocol, Src Port: domain (53), Dst Port: 52110 (52110)
  Source port: domain (53)
  Destination port: 52110 (52110)
  Length: 256
  Checksum: 0xc4ca [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  Domain Name System (response)
    [Request In: 4]
    [Time: 0.010820000 seconds]
    Transaction ID: 0x3f76
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 4
    Additional RRs: 4
    Queries
    Answers
      www.google.com: type A, class IN, addr 74.125.227.84
      www.google.com: type A, class IN, addr 74.125.227.80
      www.google.com: type A, class IN, addr 74.125.227.81
      www.google.com: type A, class IN, addr 74.125.227.82
      www.google.com: type A, class IN, addr 74.125.227.83
    Authoritative nameservers
      google.com: type NS, class IN, ns ns1.google.com
      google.com: type NS, class IN, ns ns2.google.com
      google.com: type NS, class IN, ns ns3.google.com
      google.com: type NS, class IN, ns ns4.google.com
    Additional records
      ns1.google.com: type A, class IN, addr 216.239.32.10
      ns2.google.com: type A, class IN, addr 216.239.34.10
      ns3.google.com: type A, class IN, addr 216.239.36.10
      ns4.google.com: type A, class IN, addr 216.239.38.10

```

Remarques générales

Quels sont les avantages de l'utilisation du protocole UDP par rapport au protocole TCP comme protocole de transport sur un serveur DNS ?
