Laboratoire

Capture et analyse de paquets avec Wireshark

## Contexte

Dans ce travail pratique, vous utiliserez Wireshark pour examiner les paquets échangés entre votre ordinateur et internet lorsque vous allez sur la page *www.google.com*. La première partie couvrira l’ouverture de connexion TCP en trois étapes, tandis que la deuxième couvrira la communication UDP avec un serveur DNS pour récupérer l’adresse IP associée au domaine www.google.com.

## Partie I - Préparation de l’environnement

Pour commencer, utilisez la commande ipconfig /all sur l’ordinateur de la salle de laboratoire pour trouver et enregistrer les adresses MAC et IP de la carte réseau et l’adresse IP de la passerelle par défaut et du serveur DNS. Enregistrez ces informations dans le tableau ci-dessous. Elles seront utilisées dans les prochaines sections.**Si vous ne terminez pas le TP durant la première séance, assurez-vous de prendre le même poste à la prochaine.**

| **Adresse IP** |  |
| --- | --- |
| **Adresse MAC** |  |
| **Adresse IP de la passerelle par défaut** |  |
| **Adresse IP du serveur DNS** |  |

Faites une capture d’écran des résultats de votre commande :

*Votre capture d’écran ici*

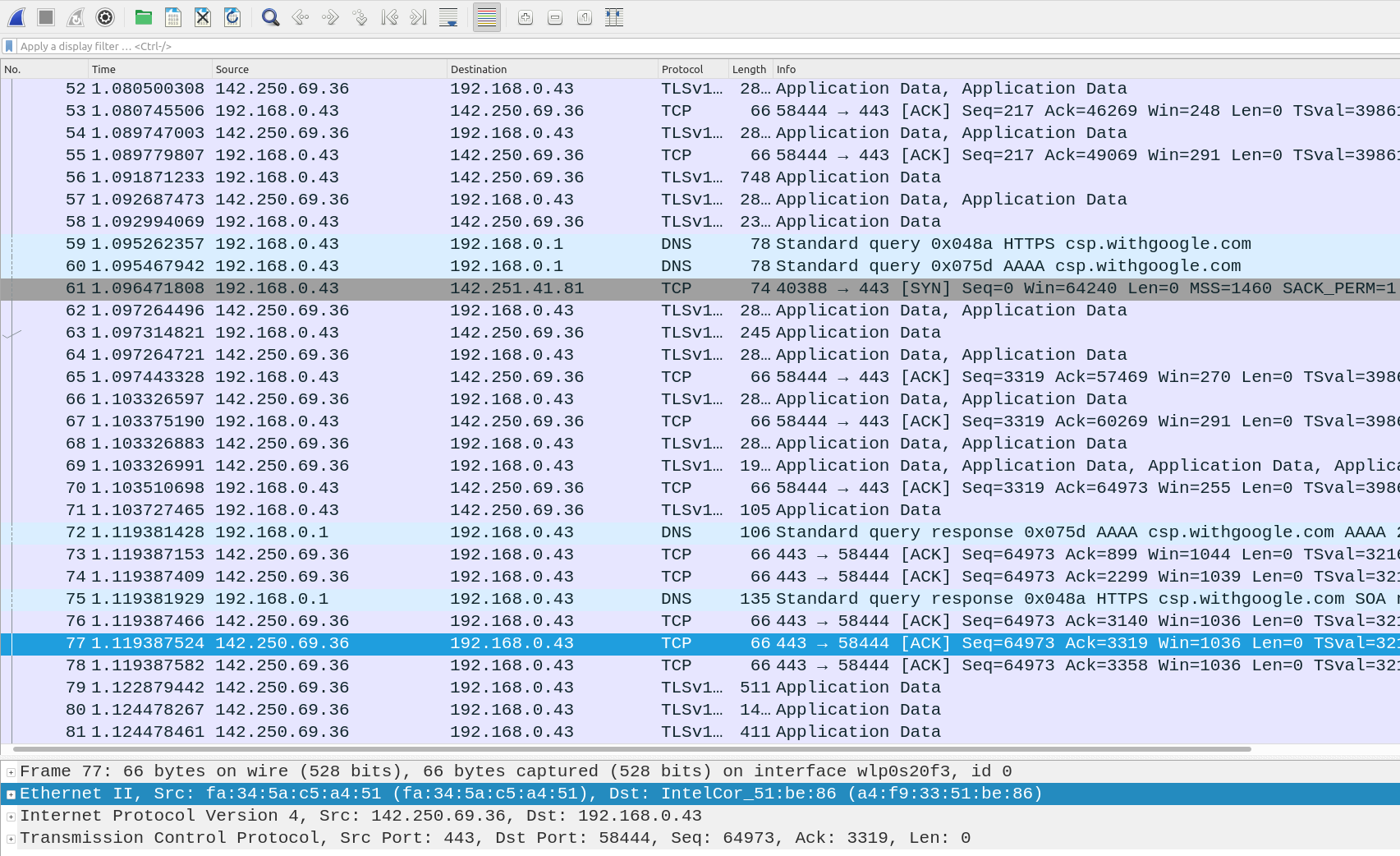
Ensuite, allez sur Wireshark et sélectionnez l’interface associée aux adresses IP et MAC du PC enregistrées ci-haut pour capturer les paquets.

Après avoir sélectionné l’interface, cliquez sur Démarrer pour commencer à capturer les paquets. Ensuite, ouvrez un navigateur Web et rendez-vous à l’adresse www.google.com. Réduisez la fenêtre Google et retournez dans Wireshark. Appuyez sur Stop (Arrêter) pour arrêter la capture Wireshark.

## Partie II - Examiner une connexion TCP en trois étapes (/6)

Dans Wireshark, localisez les colonnes **Source**, **Destination**, et **Protocol**.

Recherchez le premier paquet de la connexion en trois étapes. Dans l’exemple ci-dessous il s’agit de la trame 61 :



*2.1. Quelle est l’adresse IP du serveur Web de Google dans le cas ci-dessus?* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

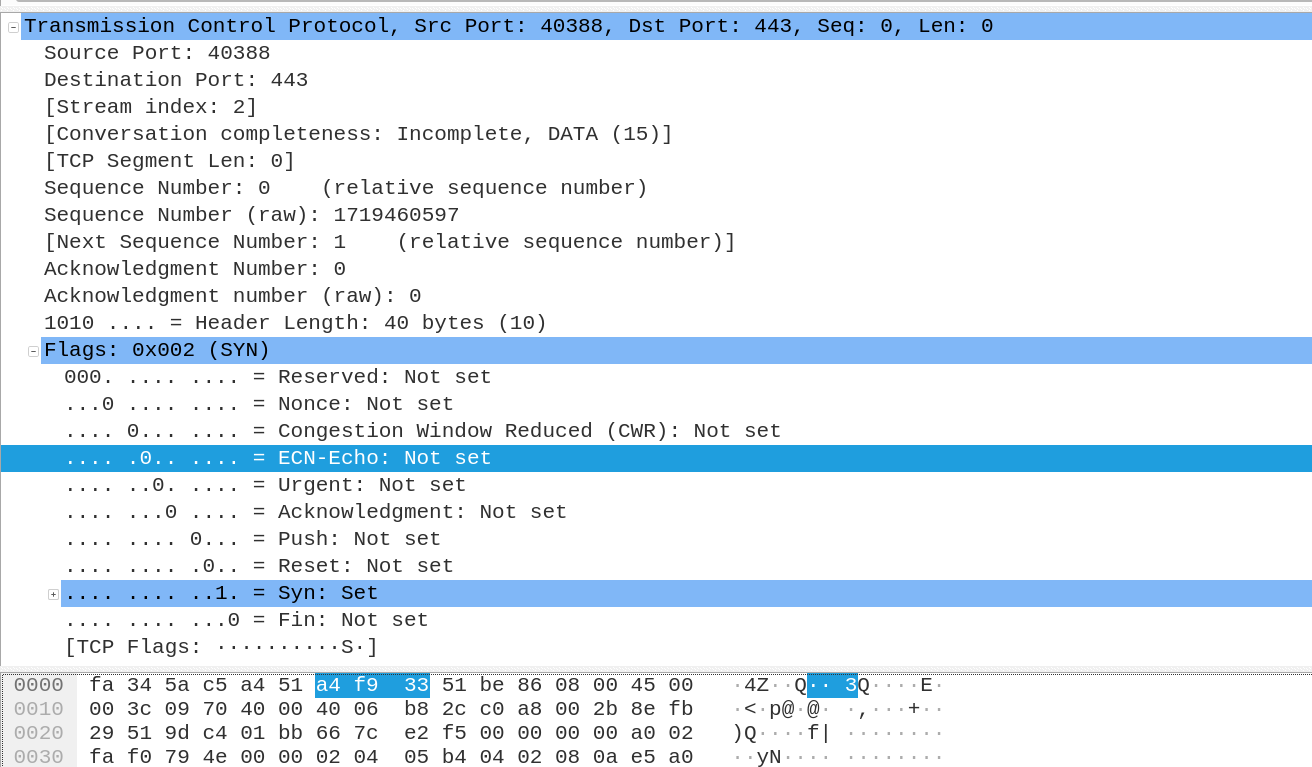
Si vous avez de nombreux paquets qui ne sont pas liés à la connexion TCP, il peut être nécessaire d’utiliser la fonction de filtre de Wireshark. Saisissez **tcp** dans la zone de saisie du filtre dans Wireshark et appuyez sur Entrée.

Dans notre exemple, la trame 61 correspond au début de la connexion en trois étapes entre l’ordinateur et le serveur Web de Google. Dans le volet de la liste des paquets (section supérieure de la fenêtre principale), sélectionnez la trame correspondante. Cette action met en surbrillance la ligne et affiche les informations décodées de ce paquet dans les deux volets inférieurs.

Cliquez sur l’icône **+** à gauche du protocole TCP (Transmission Control Protocol) dans le volet de détails des paquets pour développer l’affichage des informations TCP.

Cliquez sur l’icône **+** à gauche des bits de contrôle.

Examinez les ports source et de destination ainsi que les bit de contrôles définis.



Faites une capture d’écran de vos résultats :

*Votre capture d’écran ici*

*2.2. Quel est le numéro du port source TCP ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*2.3. Comment classifieriez-vous le port source ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

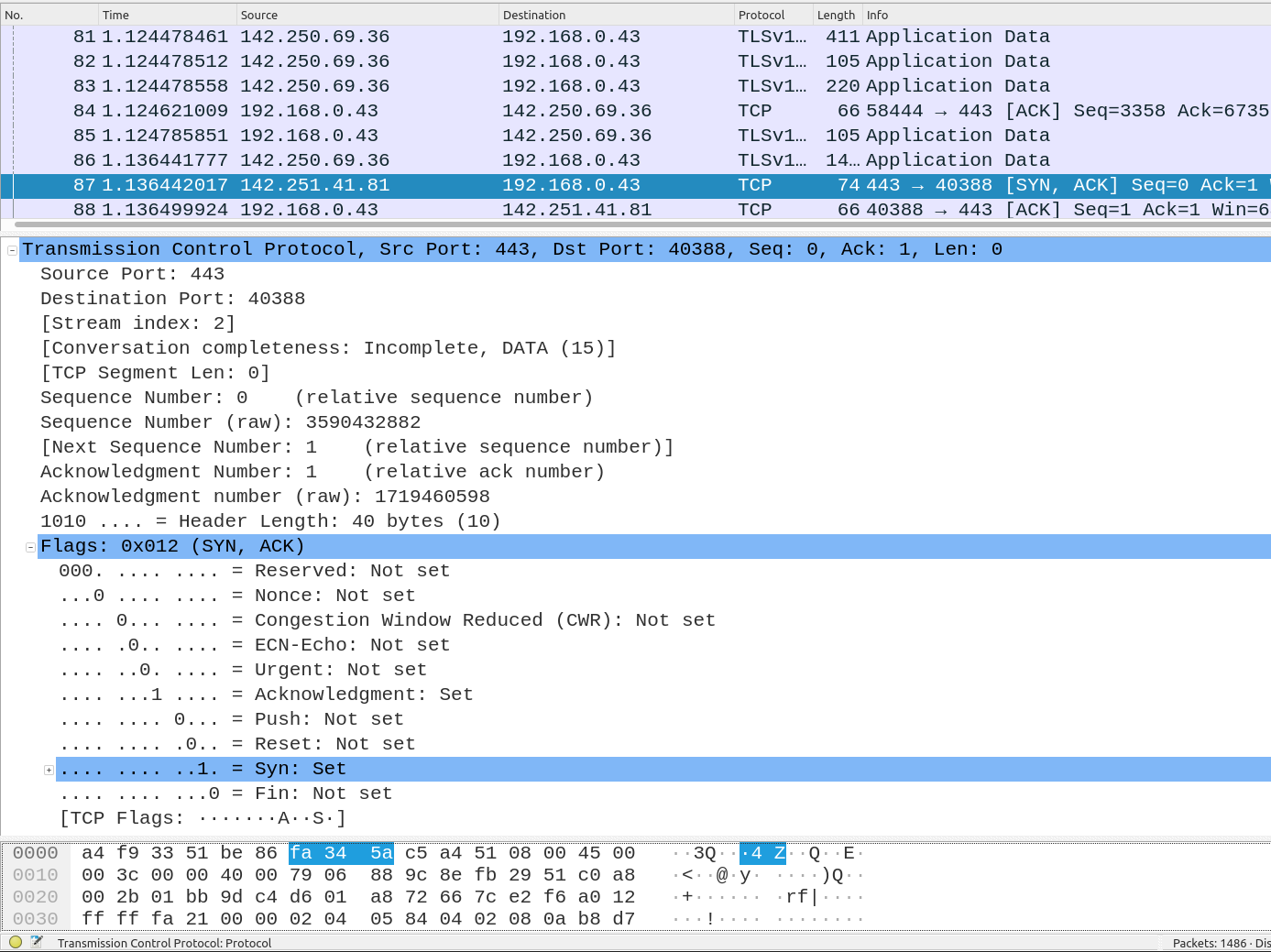
*2.4. Quel est le numéro du port de destination TCP ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*2.5. Comment classifieriez-vous le port de destination ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*2.6. Quel bit de contrôle est défini ? (plusieurs réponses possibles) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

*2.7. Sur quoi le numéro d’ordre relatif est-il défini ? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

Pour sélectionner la trame suivante dans la connexion en trois étapes, sélectionnez ***Go*** dans le menu Wireshark et sélectionnez ***Next Packet In Conversation***. Dans cet exemple, il s’agit de la trame 87. C’est la réponse du serveur Web Google à la requête initiale (SYN) de démarrage d’une session.

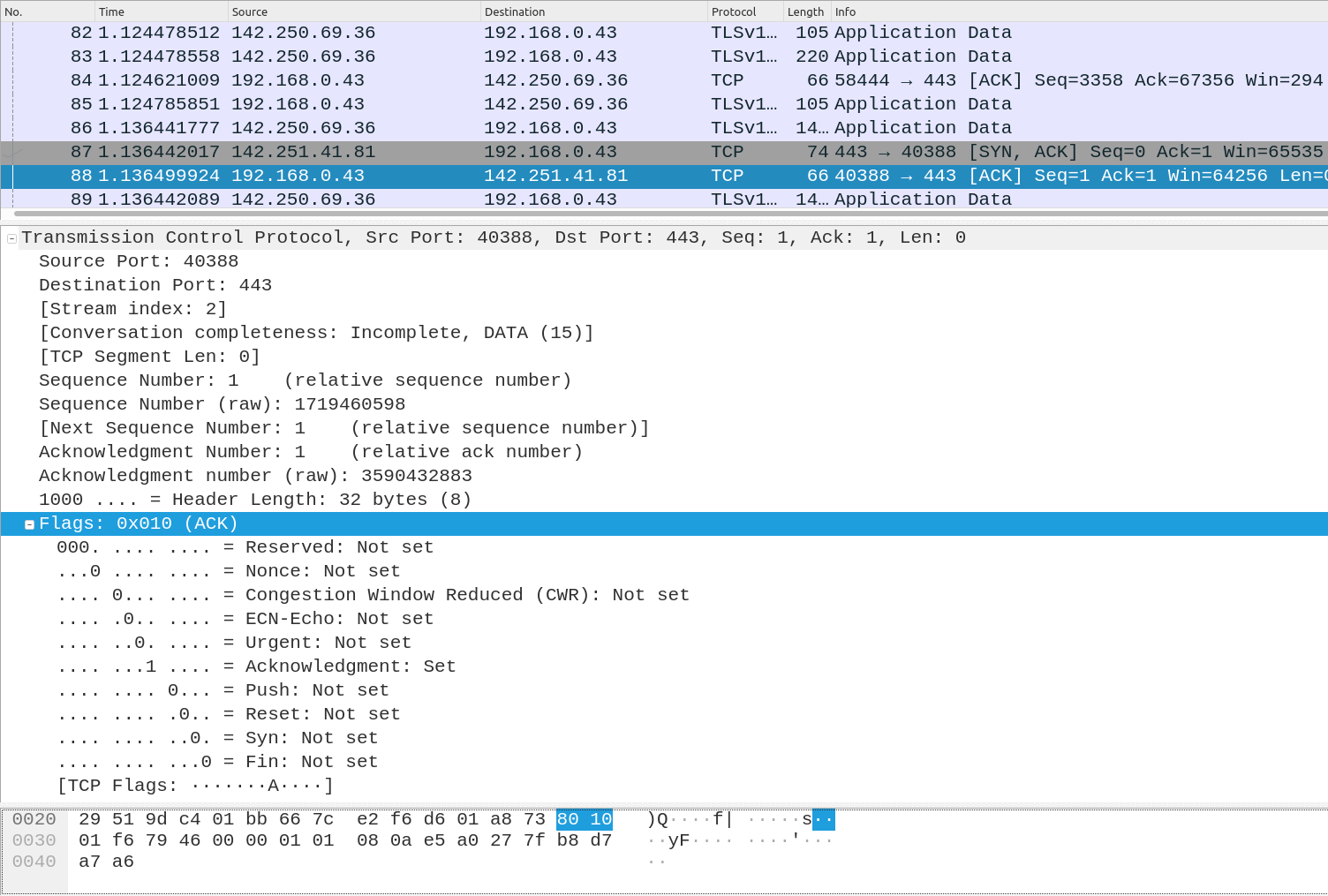


*2.8. Quelles sont les valeurs des ports source et de destination ?* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*2.9. Sur quoi les numéros d’ordre relatif et d’accusé de réception sont-ils définis ?*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Enfin, examinez le troisième paquet de la connexion en trois étape. Dans l’exemple ci-dessous, c’est la trame 88 :



*2.10. Quel bit de contrôle est défini ? (plusieurs réponses possibles)*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Faites une capture d’écran de votre résultat :

*Votre capture d’écran ici*

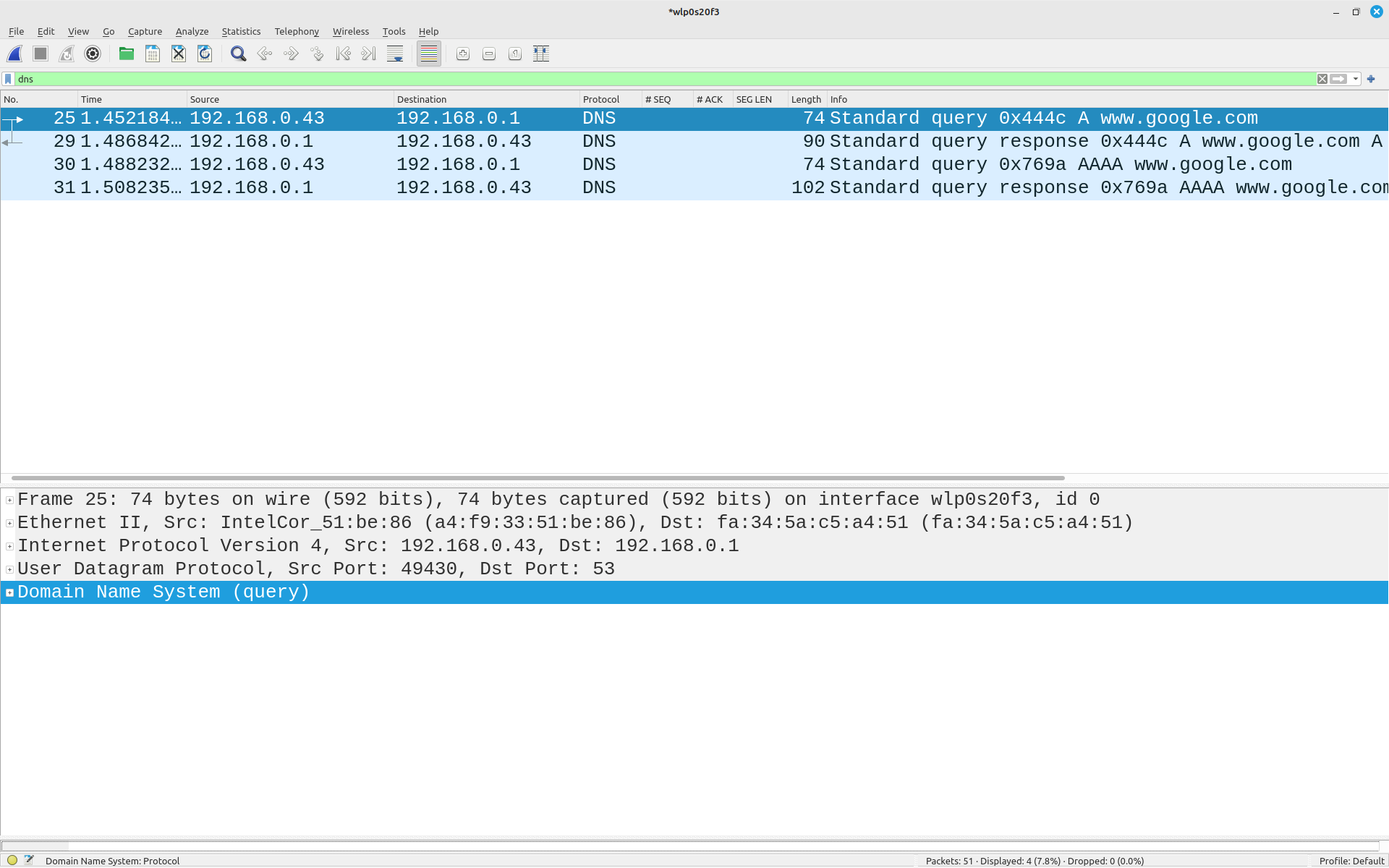
Les numéros d’ordre relatif et d’accusé de réception sont définis sur 1 comme point de départ. La connexion TCP est désormais établie, et la communication entre l’ordinateur source et le serveur Web peut commencer.

## Partie III - Examiner une capture DNS UDP (/4)

Dans cette partie, vous examinerez les paquets UDP générés lors de la communication avec le serveur DNS afin de récupérer les adresses IP associées au domaine www.google.com.

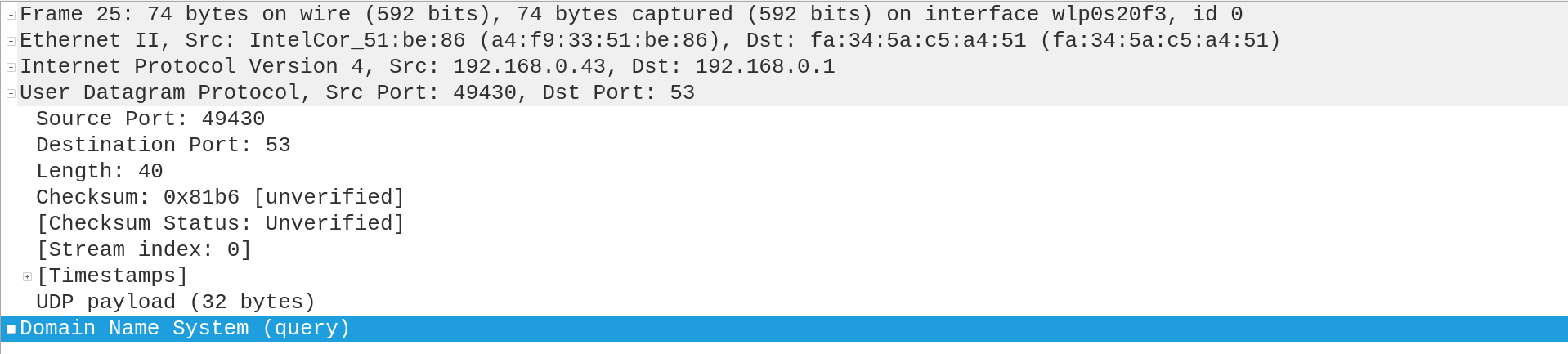
Dans la fenêtre principale de Wireshark, tapez**dns** dans la zone de saisie de la barre de filtre. Cliquez sur **Apply** ou appuyez sur Entrée.

***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 de la partie I. 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.*



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 25 ci-dessus comme exemple).

Examinez le segment UDP de la requête DNS capturée par Wireshark. Dans cet exemple, la trame 25 est sélectionnée pour l’analyse. Les protocoles dans cette requête apparaissent Les entrées de protocole sont mises en surbrillance en gris :



Dans le volet de détails des paquets, on peut voir que la trame 25 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 et demander les adresses IP de [www.google.com](http://www.google.com).

La ligne **Ethernet II** affiche les adresses MAC source et de destination. L’adresse MAC provient de votre PC, 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.

Effectuez une capture d’écran de votre résultat :

*Votre capture d’écran ici*

*3.1 L’adresse MAC source est-elle identique à celle enregistrée dans la première partie pour le PC ?*

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

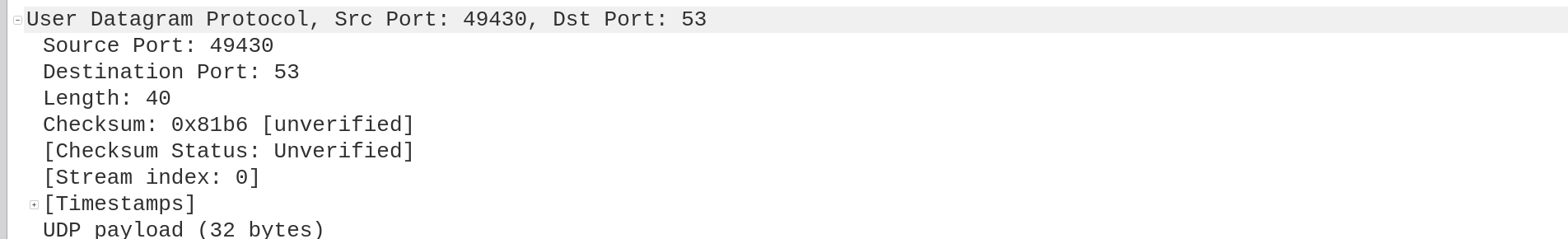
Sur la ligne **Internet Protocol Version 4**, la capture Wireshark de paquets IP indique que l’adresse IP source de cette requête DNS est *192.168.0.43* et l’adresse IP de destination est *192.168.0.1*. Dans cet exemple, l’adresse de destination est la passerelle par défaut. Le routeur est la passerelle par défaut sur ce réseau. Associez les adresses MAC et IP pour les périphériques source et destination :

| **Périphérique** | **Adresse IP** | **Adresse MAC** |
| --- | --- | --- |
| **Votre PC** |  |  |
| **Passerelle par défaut** |  |  |

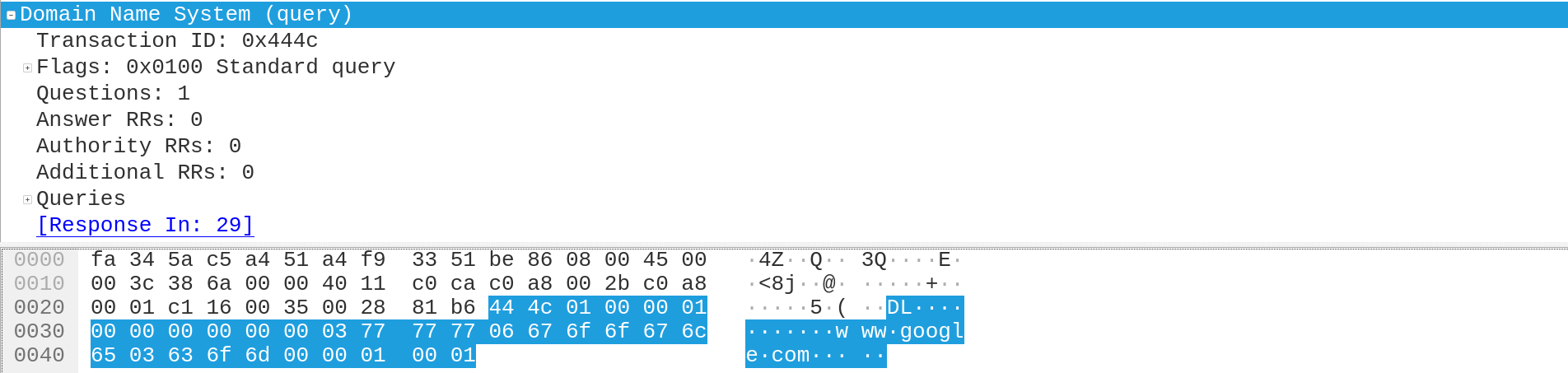
Faites une capture d’écran montrant où vous avez trouvé les informations entrées dans le tableau ci-dessus :

*Votre capture d’écran ici*

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 49430. Le port source a été généré aléatoirement par votre PC 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.



Faites une capture d’écran de votre résultat :

*Votre capture d’écran ici*

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.

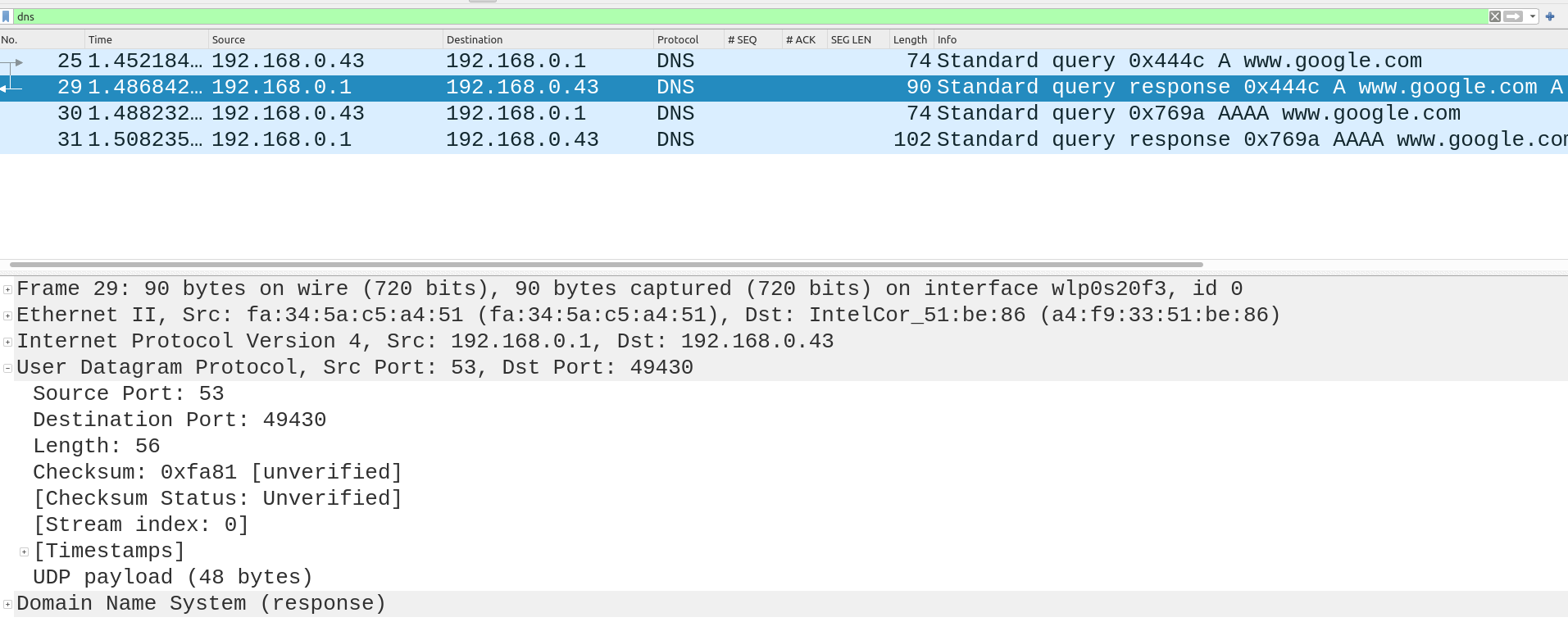
Notez les résultats de Wireshark dans la table ci-dessous

| **Taille de la trame** |  |
| --- | --- |
| **Adresse MAC source** |  |
| **Adresse MAC de destination** |  |
| **Adresse IP source** |  |
| **Adresse IP de destination** |  |
| **Port source** |  |
| **Port de destination** |  |

Ensuite, examinez le paquet de réponse DNS et vérifiez que ce paquet utilise aussi le protocole UDP.

Dans cet exemple, la trame 29 est le paquet de réponse DNS. Notez que le nombre d’octets sur le câble correspond à 90 octets. Il s’agit d’un paquet plus gros par rapport au paquet de

requête.



Faites une capture d’écran de votre résultat :

*Votre capture d’écran ici*

Dans la trame **Ethernet II** de la réponse DNS, de quel périphérique provient l’adresse MAC source et à quel périphérique correspond l’adresse MAC de destination ?

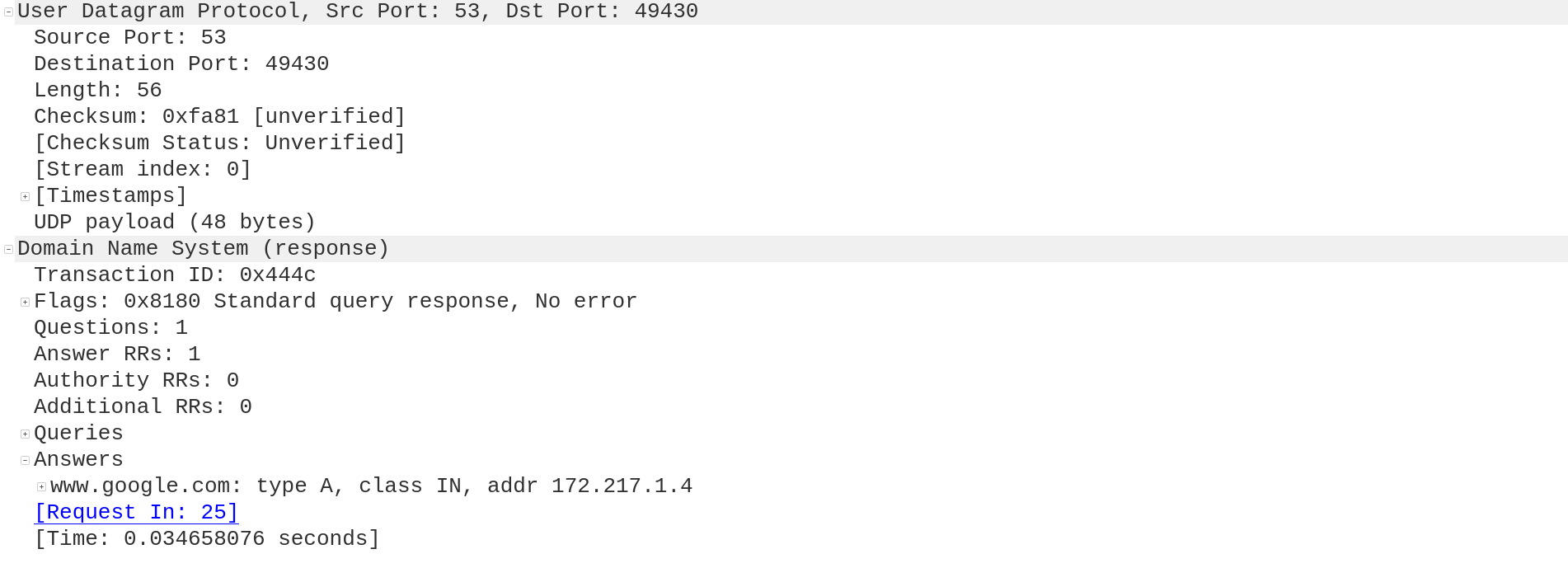
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dans le segment UDP, le rôle des numéros de port a également été inversé. Le numéro du port de destination est 49430. Le numéro de port 49430 est le même port que celui qui a été généré par votre PC lorsque la requête DNS a été envoyée au serveur DNS. Votre PC a attendu 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)**.



Faites une capture d’écran de votre résultat :

*Votre capture d’écran ici*