Travaux pratiques– Explorer le trafic DNS

Partie 1 : Capturer le trafic DNS

Partie 2 : Découvrir le trafic des requêtes DNS

Partie 3 : Découvrir le trafic des réponses DNS

# Contexte/scénario

Wireshark est un outil open source de capture et d'analyse de paquets. Wireshark produit une répartition détaillée de la pile de protocole réseau. Wireshark vous permet de filtrer le trafic pour le dépannage du réseau, d'enquêter sur des problèmes de sécurité et d'analyser les protocoles réseau. Parce que Wireshark vous permet d'afficher les informations des paquets, il peut être utilisé comme un outil de reconnaissance pour un hacker.

Au cours de ces travaux pratiques, vous allez installer Wireshark sur un système Windows et l'utiliser pour filtrer les paquets DNS et afficher les détails des paquets de requête et de réponse DNS.

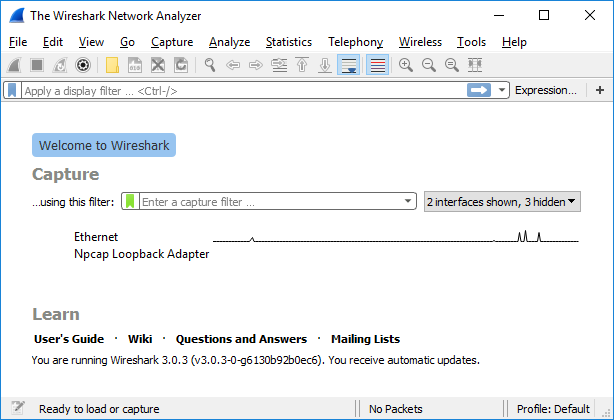
# Ressources requises

* 1 PC Windows avec accès Internet et Wireshark installé

# Instructions

## Capturer le trafic DNS.

* + 1. Ouvrez **Wireshark** et commencez une capture Wireshark en double cliquant sur une interface réseau avec du trafic.



* + 1. Dans l'invite de commande, tapez **ipconfig/flushdns** et appuyez sur Entrée pour effacer le cache DNS.

C:\Users\Student> **ipconfig /flushdns**

Configuration IP Windows

Successfully flushed the DNS Resolver Cache.

* + 1. Tapez **nslookup** dans l'invite pour passer au mode interactif nslookup.
    2. Saisissez le nom de domaine d'un site web. Dans cet exemple, nous utilisons le nom de domaine [www.cisco.com](http://www.cisco.com). Entrez **www.cisco.com** à l'invite > .

C:\Users\Student> **nslookup**

Default Server: UnKnown

Adress: 68.105.28.16

> **www.cisco.com**

Server: UnKnown

Adress : 68.105.28.16

Non-authoritative answer:

Name: e2867.dsca.akamaiedge.net

Adress: 2001:578:28:68d::b33

2001:578:28:685::b33

96.7.79.147

Aliases: www.cisco.com

www.cisco.com.akadns.net

wwwds.cisco.com.edgekey.net

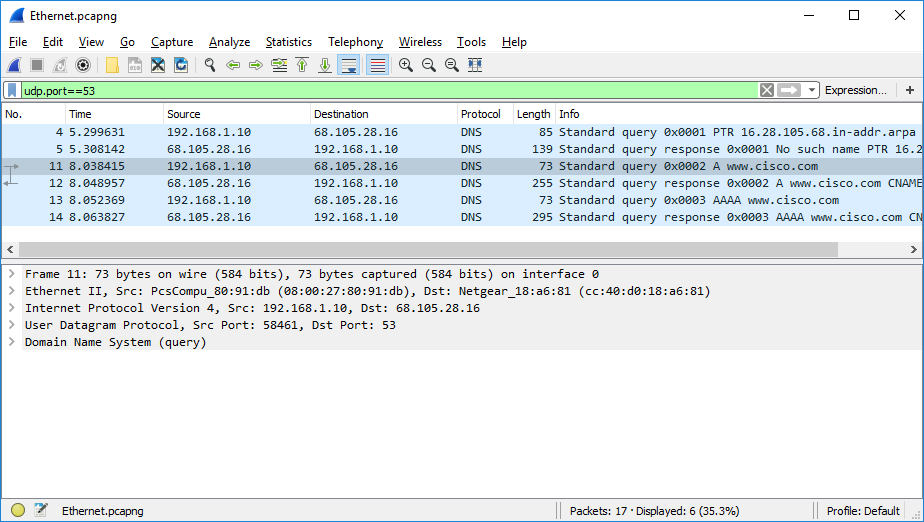
wwwds.cisco.com.edgekey.net.globalredir.akadns.net

* + 1. Tapez **exit** quand vous finissez l'exécution du mode interactif nslookup. Fermez l'invite de commande.
    2. Cliquez sur **Stop capturing packets** pour arrêter la capture Wireshark.

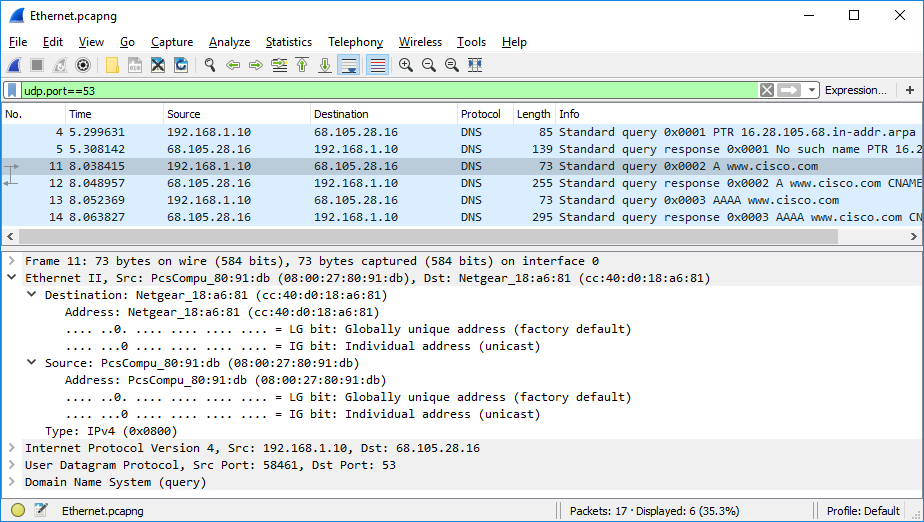
## Découvrir le trafic des requêtes DNS

* + 1. Examinez le trafic capturé dans le volet de la liste des paquets Wireshark. Saisissez **udp.port == 53** dans la zone de filtre et cliquez sur la flèche (ou appuyez sur Entrée) pour afficher uniquement les paquets DNS.
    2. Sélectionnez le paquet DNS identifié **Standard query 0x0002 A www.cisco.com**.

Dans le volet des détails des paquets, notez que les informations Ethernet II, Internet Protocol Version 4, User Datagram Protocol et Domain Name System (query) sont indiquées pour ce paquet.



* + 1. Développez **Ethernet II** pour afficher les détails. Examinez les champs de source et de destination.

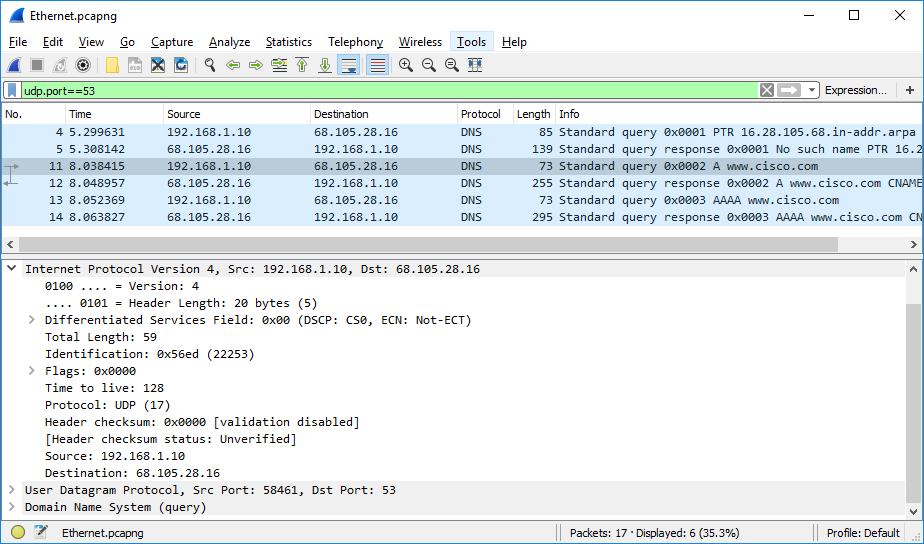


### Question :

Quelles sont les adresses MAC source et de destination ? À quelles interfaces réseau ces adresses MAC sont-elles associées ?

Saisissez vos réponses ici

* + - 1. Développez **Internet Protocol Version 4**. Examinez les adresses IPv4 de source et de destination.

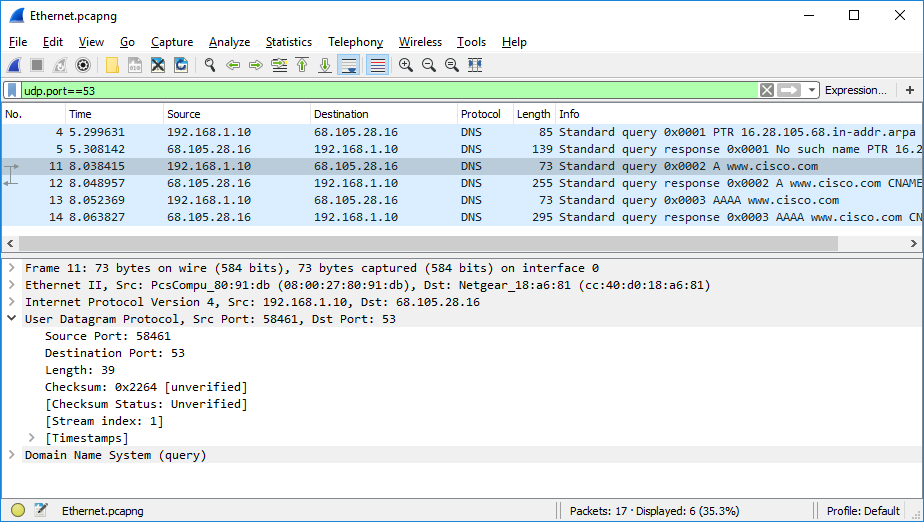


### Question :

Quelles sont les adresses IP de source et de destination ? À quelles interfaces réseau ces adresses IP sont-elles associées ?

Saisissez vos réponses ici

* + - 1. Développez le protocole **User Datagram Protocol**. Examinez les ports de source et de destination.



### Question :

Quels sont les ports de source et de destination ? Quel est le numéro du port DNS par défaut ?

Saisissez vos réponses ici

* + - 1. Ouvrez une invite de commande et saisissez **arp – a** et **ipconfig/all** pour enregistrer les adresses MAC et IP de l'ordinateur.

C:\Users\Student> **arp -a**

Interface: 192.168.1.10 --- 0x4

Internet Adress Physical Adress Type

192.168.1.1 cc-40-d0-18-a6-81 dynamic

192.168.1.122 b0-a7-37-46-70-bb dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

C:\Users\Student> **ipconfig /flushdns**

Configuration IP Windows

Host name. . . . . . . . . . . . : DESKTOP

Primary Dns Suffix . . . . . . . :

Node Type . . . . . . . . . . . . : Hybrid

IP Routing Enabled. . . . . . . . : No

Proxy WINS activated. . . . . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :

Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter

Physical Address. . . . . . . . . : 08-00-27-80-91-DB

DHCP Enabled. . . . . . . . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%4(Preferred)

IPv4 Address. . . . . . . . . . . : 192.168.1.10 (Preferred)

Subnet Mask . . . . . . . . . . . : 255.255.255.0

Lease Obtained. . . . . . . . . . : Tuesday, August 20, 2019 5:39:51 PM

Lease Expires . . . . . . . . . . : Wednesday, August 21, 2019 5:39:50 PM

Default Gateway . . . . . . . . . : 192.168.1.1

DHCP Server . . . . . . . . . . . : 192.168.1.1

DHCPv6 IAID . . . . . . . . . . . : 50855975

DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB

DNS Servers . . . . . . . . . . . : 68.105.28.16

68.105.29.16

NetBIOS over Tcpip. . . . . . . . : Enabled

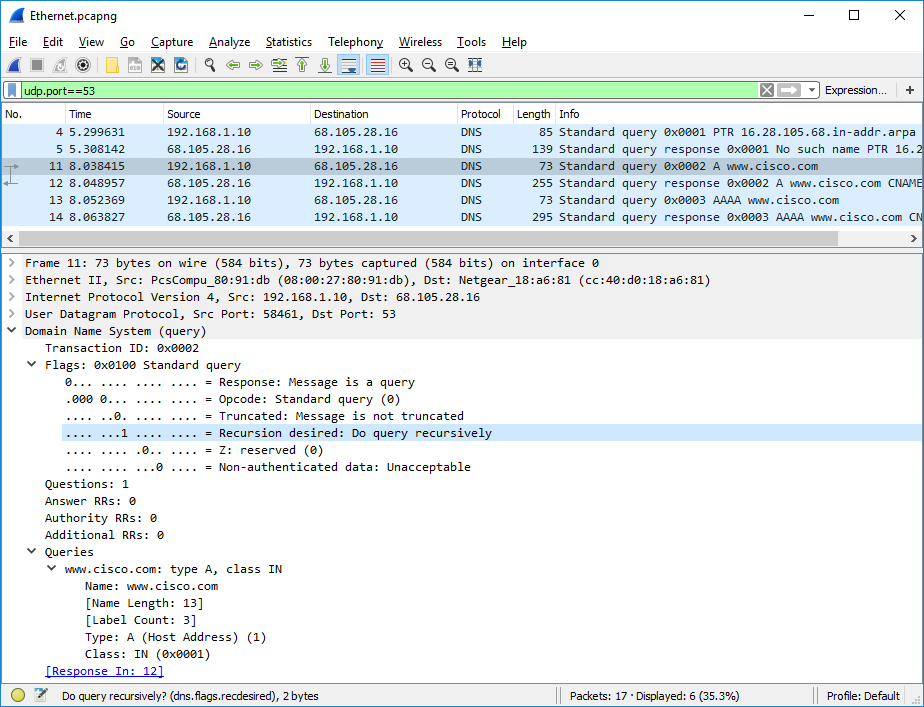
### Question :

Comparez les adresses MAC et IP des résultats de Wireshark aux résultats de **ipconfig/all**. Que remarquez-vous ?

Saisissez vos réponses ici

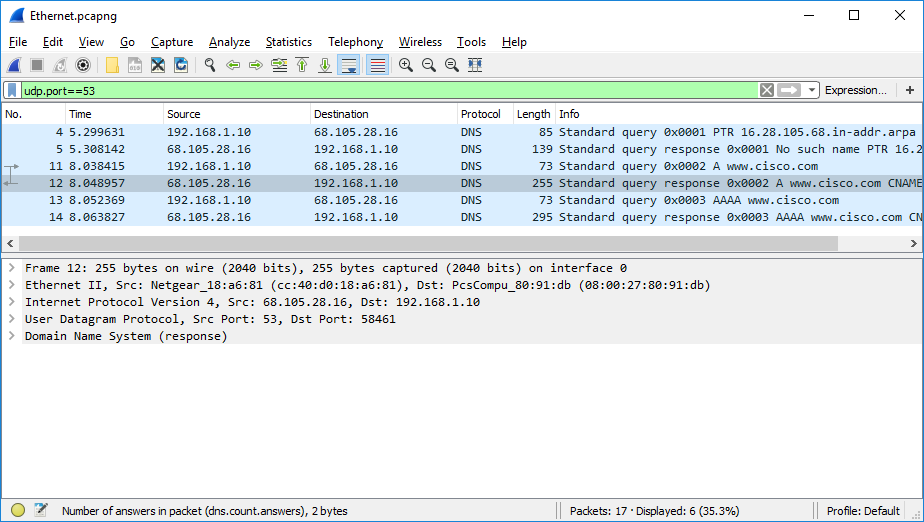
* + - 1. Développez **Domain Name System (query**) dans le volet des détails des paquets. Puis développez **les indicateurs** et **les requêtes**(Flags and Queries).

Examinez les résultats. L'indicateur est défini pour demander de manière récursive pour chercher l'adresse IP sur www.cisco.com.



## Découvrir le trafic des réponses DNS

* + 1. Sélectionnez le paquet DNS de réponse correspondant libellé **Standard query response 0x000# A www.cisco.com**.

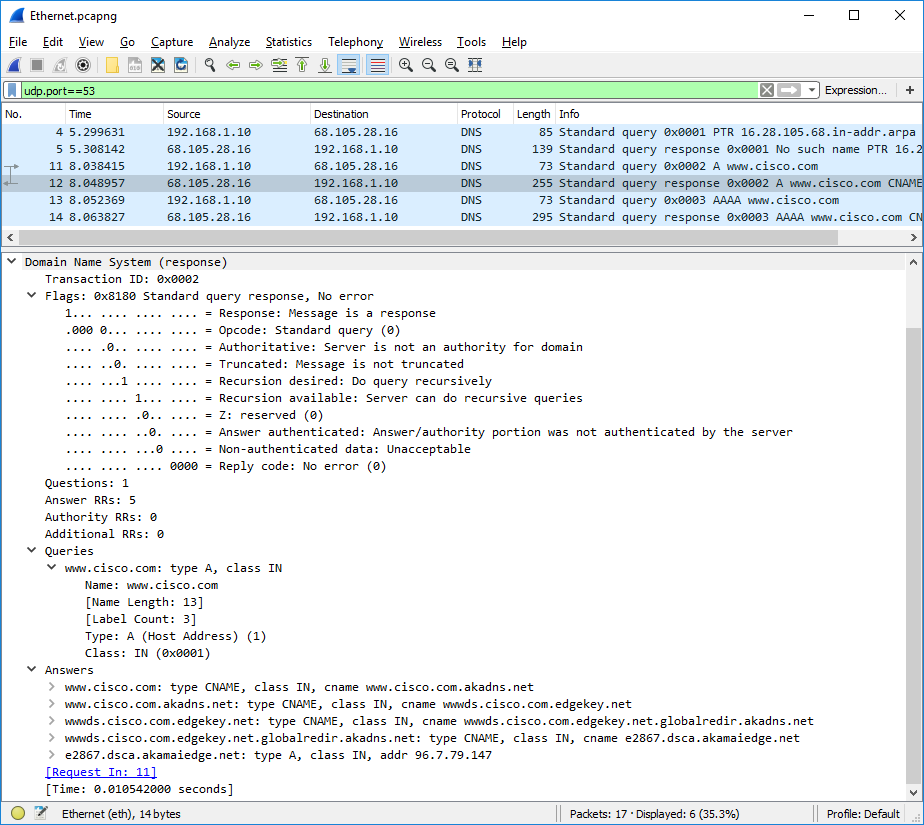


### Questions :

Quelles sont les adresses MAC et IP source et de destination et les numéros de port ? Que remarquez-vous par rapport aux adresses dans les paquets de requête DNS ?

Saisissez vos réponses ici

* + 1. Développez **Domain Name System (response)**. Puis développez **les indicateurs**, **les requêtes** et **les réponses** (Flags, Queries and Answers). Examinez les résultats.



### Question :

Le serveur DNS peut-il envoyer des requêtes récursives ?

Saisissez vos réponses ici

* + 1. Examinez les enregistrements CNAME et A dans les détails des réponses.

### Question :

Comment les résultats se comparent-ils aux résultats de nslookup ?

Saisissez vos réponses ici

# Question de réflexion

* 1. D'après les résultats de Wireshark, que pouvez-vous apprendre du réseau lorsque vous enlevez le filtre ?

Saisissez vos réponses ici

* 1. Comment un pirate peut-il utiliser Wireshark pour compromettre la sécurité de votre réseau ?

Saisissez vos réponses ici

Fin du document