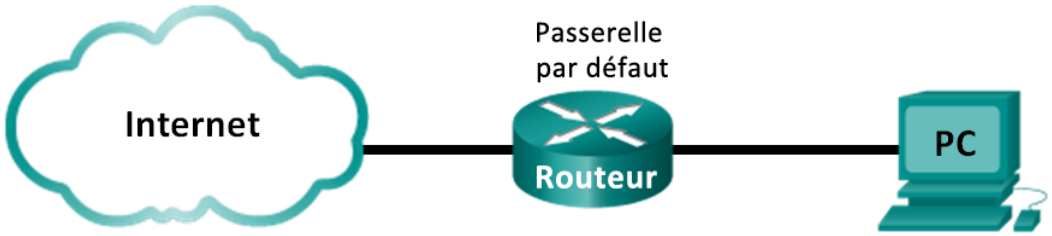
Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

Topologie



Objectifs

1re partie : PréparerWireshark pour capturer des paquets

- Sélectionnez une interface de carte réseau appropriée pour la capture de paquets.

2e partie : Capturer, localiser et examiner les paquets

- Capturez une session Web sur www.google.com.
- Localisez les paquets appropriés pour une session Web.
- Examinez les informations au sein des paquets, y compris les adresses IP, les numéros de port TCP et les indicateurs de contrôle TCP.

Contexte/scénario

Au cours de ces travaux pratiques, vous utiliserez Wireshark pour capturer et examiner les paquets générés entre le navigateur de l'ordinateur en utilisant le protocole HTTP (Hypertext Transfer Protocol) et un serveur Web, tel que www.google.com. Lorsqu'une application, telle que le protocole HTTP ou FTP (File Transfer Protocol) démarre d'abord sur un hôte, TCP utilise la connexion en trois étapes pour établir une session TCP fiable entre les deux hôtes. Par exemple, lorsqu'un ordinateur utilise un navigateur Web pour naviguer sur Internet, une connexion en trois étapes est lancée et une session est établie entre l'ordinateur hôte et le serveur Web. Un ordinateur peut avoir des sessions TCP actives, multiples et simultanées avec différents sites Web.

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 : Préparer Wireshark pour capturer des paquets

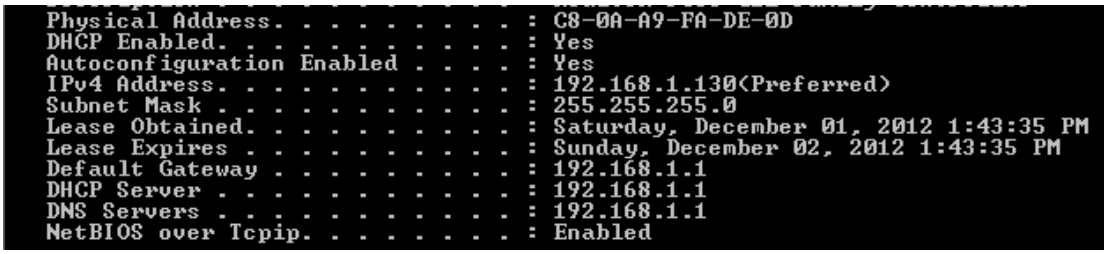
Dans la première partie, vousdémarrez le programmeWireshark et sélectionnezl'interfaceappropriée pour commencer à capturer des paquets.

Étape 1 : Récupérez les adresses d'interface de l'ordinateur.

Dans le cadre de ces travaux pratiques, vous devez récupérer l'adresse IP de votreordinateur et l'adresse physique de sa carte réseau, également appelée adresse MAC.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

a. Ouvrez une fenêtre d'invite de commandes, tapez **ipconfig /all** et appuyez sur Entrée.



b. Notez les adresses MAC et IP associées à la carte Ethernet sélectionnée, car il s'agit de l'adresse source à rechercher lors de l'inspection des paquets capturés.

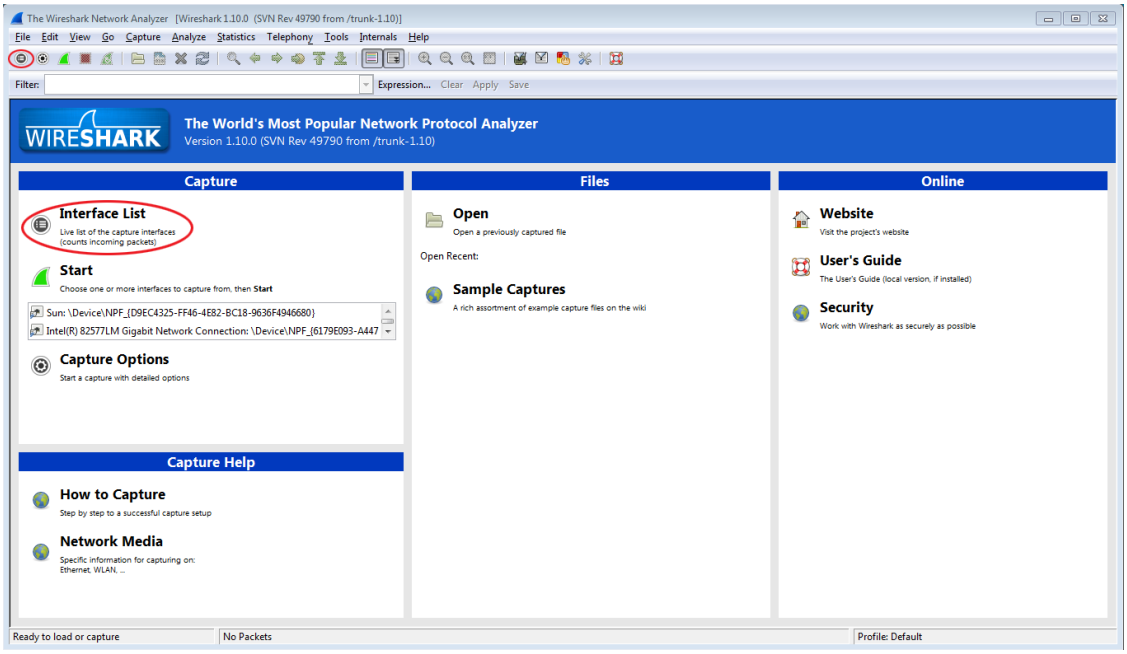
Adresse IP de l'ordinateur hôte :

Adresse MAC de l'ordinateur hôte :

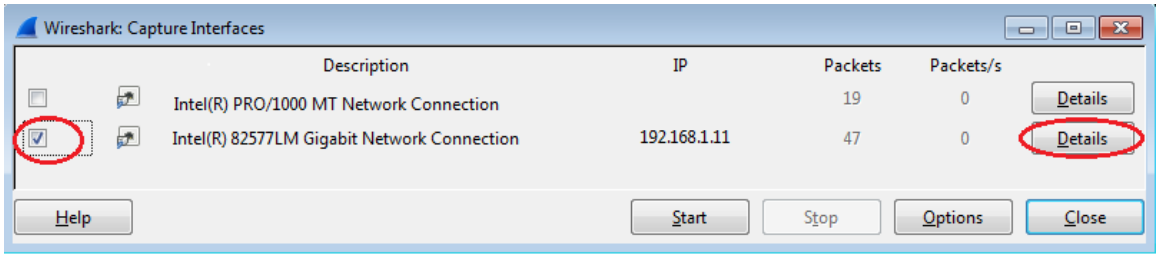
Étape 2 : Démarrez Wireshark et sélectionnez l'interface appropriée.

a. Cliquez sur le bouton **Démarrer** de Windows et, dans le menu contextuel, double-cliquez sur **Wireshark**.

b. Une fois que Wireshark démarre, cliquez sur **Interface List**.



c. Dans la fenêtre **Wireshark: Capture Interfaces (Wireshark : interfaces de capture)**, activez la case à cocher en regard de l'interface connectée à votre réseau local (LAN).



© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Remarque : si plusieurs interfaces sont répertoriées et que vous ne savez pas quel interface vérifier, cliquez sur **Details (Détails)**. Cliquez sur l'onglet **802.3 (Ethernet)**, et vérifiez que l'adresse MAC correspond à ce que vous avez noté à l'étape 1b. Fermez la fenêtre Interface Details (Détails d'interface) après vérification.

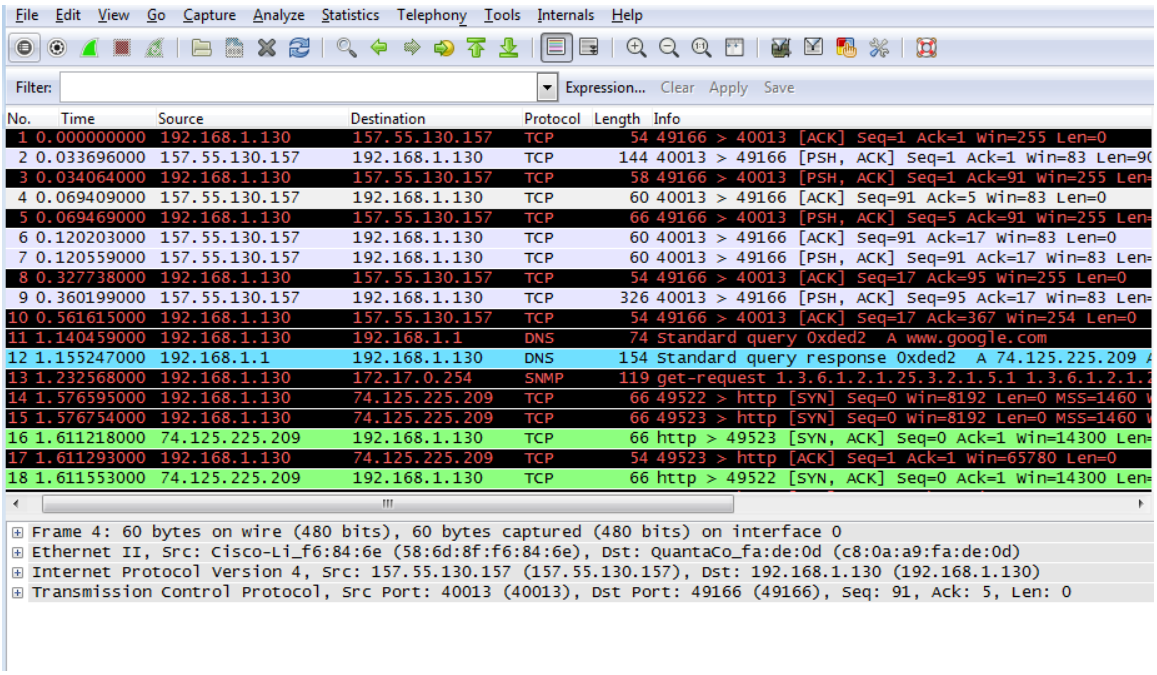
2e partie : Capturer, localiser et examiner les paquets

Étape 1 : Cliquez sur le bouton Start (Démarrer) pour démarrer la capture des données.

a. Rendez-vous à l'adresse www.google.com. Réduisez la fenêtre Google et retournez dans Wireshark. Arrêtez la capture des données. Le trafic capturé qui s'affiche doit être similaire à celui illustré ci-dessous à l'étape b.

Remarque : votre instructeur peut vous fournir un site Web différent. Dans ce cas, tapez l'adresse ou le nom du site Web ici :

b. La fenêtre de capture est désormais activée. Localisez les colonnes **Source**, **Destination**, et **Protocol**.



Étape 2 : Localisez les paquets appropriés pour la session Web.

Si l'ordinateur a démarré récemment et qu'il n'y a eu aucune activité en lien avec des accès à Internet, vous pouvez consulter le processus entier dans le résultat capturé, y compris le protocole ARP (Address Resolution Protocol), le système de noms de domaine (DNS) et la connexion TCP en trois étapes. L'écran de capture dans l'étape 1 de la deuxième partie affiche tous les paquets que l'ordinateur doit obtenir pour accéder à www.google.com. Dans ce cas, l'ordinateur disposait déjà d'une entrée ARP pour la passerelle par défaut ; par conséquent, il a commencé par la requête DNS afin de résoudre www.google.com.

a. La trame 11 affiche la requête DNS depuis l'ordinateur vers le serveur DNS, en essayant de résoudre le nom de domaine www.google.com sur l'adresse IP du serveur Web. L'ordinateur doit disposer de l'adresse IP avant de pouvoir envoyer le premier paquet au serveur Web.

Quelle est l'adresse IP du serveur DNS que l'ordinateur a interrogé ?

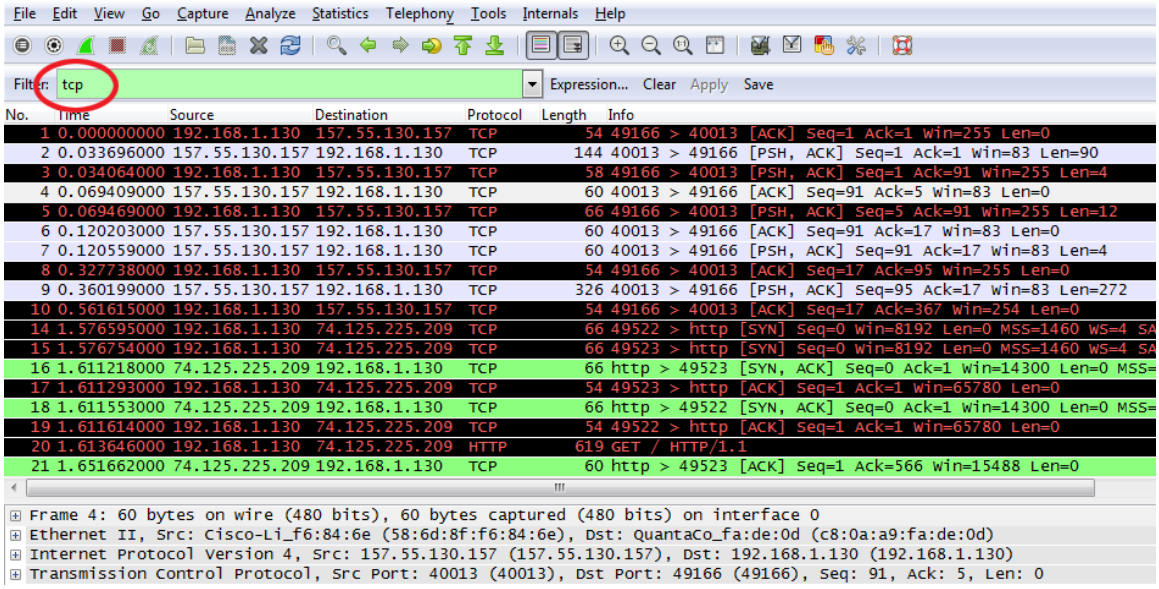
b. La trame 12 est la réponse du serveur DNS avec l'adresse IP de www.google.com.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

c. Recherchez le paquet approprié pour le début de votre connexion en trois étapes. Dans cet exemple, la trame 15 correspond au début de la connexion TCP en trois étapes.

Quelle est l'adresse IP du serveur Web de Google ?

d. 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.



Étape 3 : Examinez les informations au sein des paquets, y compris les adresses IP, les numéros de port TCP et les indicateurs de contrôle TCP.

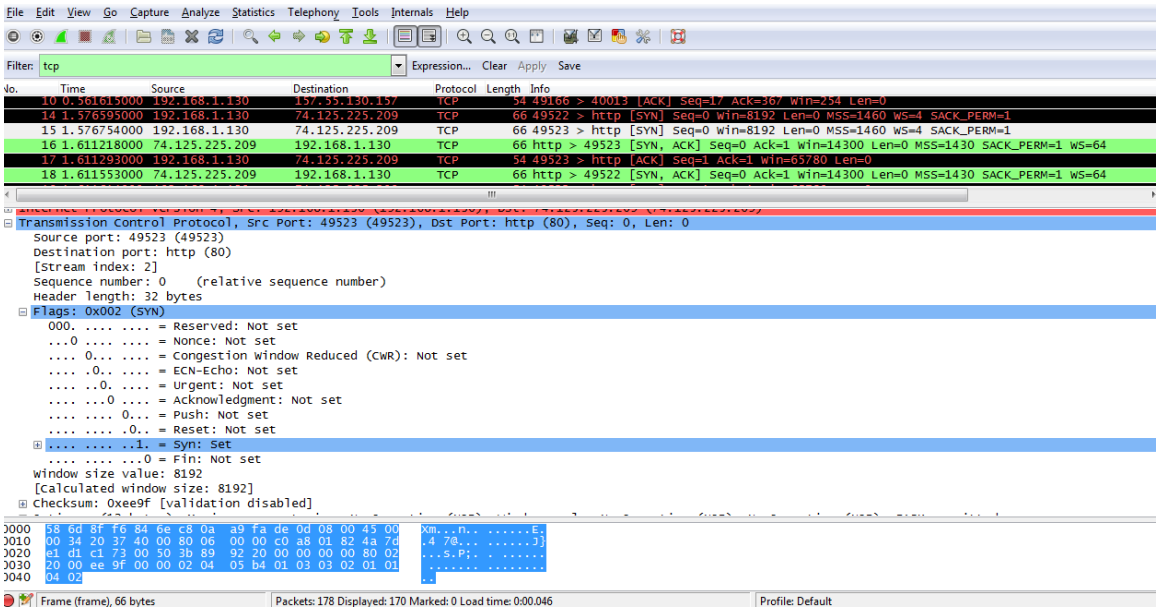
a. Dans notre exemple, la trame 15 correspond au début de la connexion en trois étapes entre l'ordinateur et le serveur Web de Google. Dans le volet de la liste des paquets (section supérieure de la fenêtre principale), sélectionnez la trame. Cette action met en surbrillance la ligne et affiche les informations décodées de ce paquet dans les deux volets inférieurs. Examinez les informations du protocole TCP dans le volet de détails des paquets (section centrale de la fenêtre principale).

b. 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.

c. Cliquez sur l'icône **+** à gauche des indicateurs. Examinez les ports source et de destination ainsi que les indicateurs qui sont définis.

Remarque : il vous faudra peut-être modifier la taille des fenêtres du haut et du milieu dans Wireshark pour afficher les informations nécessaires.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.



Quel est le numéro du port source TCP ?

Comment classifieriez-vous le port source ?

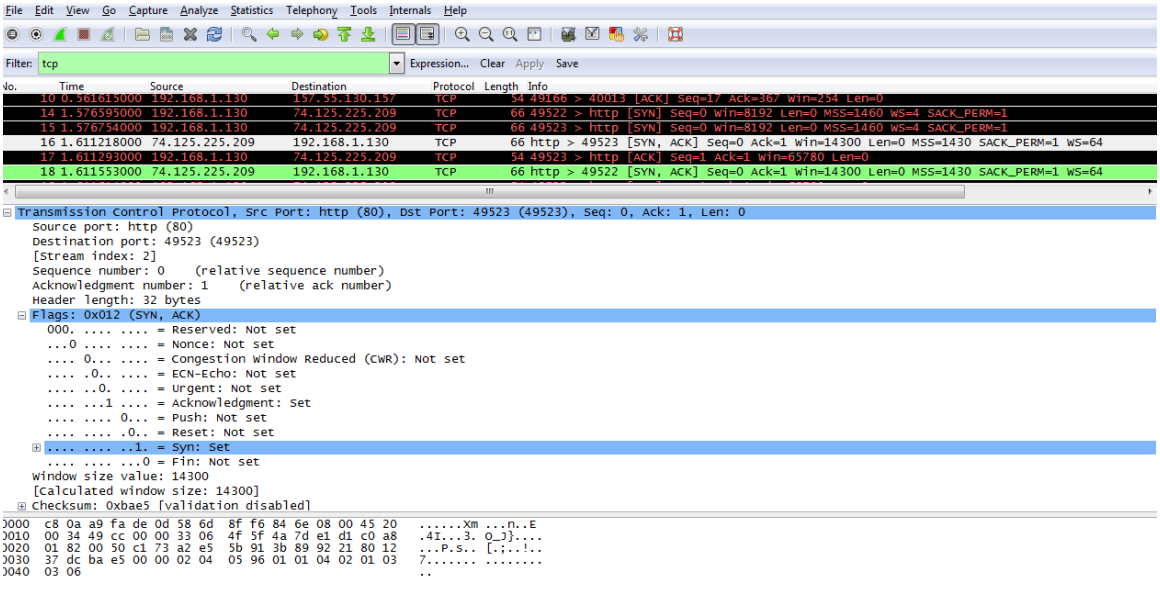
Quel est le numéro du port de destination TCP ?

Comment classifieriez-vous le port de destination ?

Quel indicateur est défini ? (plusieurs réponses possibles)

Sur quoi le numéro d'ordre relatif est-il défini ?

d. Pour sélectionner la trame suivante dans la connexion en trois étapes, sélectionnez **Go (Exécuter)** dans le menu Wireshark et sélectionnez **Next Packet In Conversation (Paquet suivant dans la conversation)**. Dans cet exemple, il s'agit de la trame 16. C'est la réponse du serveur Web Google à la requête initiale de démarrage d'une session.



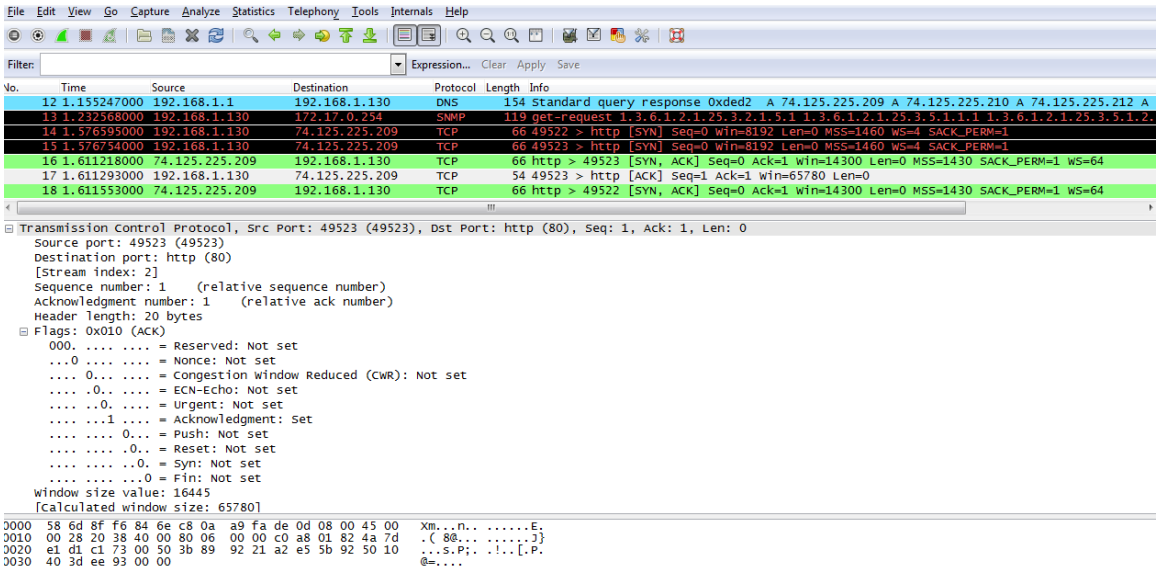
Quelles sont les valeurs des ports source et de destination ?

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Quels indicateurs sont-ils définis ?

Sur quoi les numéros d'ordre relatif et d'accusé de réception sont-ils définis ?

e. Enfin, examinez le troisième paquet de la connexion en trois étapes dans l'exemple. Cliquez sur la trame 17 dans la fenêtre du haut pour afficher les informations suivantes dans cet exemple :



Examinez le troisième et dernier paquet de la connexion.

Quel indicateur est défini ? (plusieurs réponses possibles)

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.

f. Fermez le programme Wireshark.

Remarques générales

1. Des centaines de filtres sont disponibles dans Wireshark. Un réseau de grande taille peut avoir de nombreux filtres et de nombreux types de trafic. Dans la liste, quels sont les trois filtres qui peuvent être les plus utiles pour un administrateur réseau ?

2. De quelles autres façons Wireshark pourrait-il être utilisé dans un réseau de production ?

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.