Travaux pratiques 9.1.3 Utilisation de Wireshark pour examiner le fonctionnement d'une connexion TCP en trois étapes

Objectifs

- Utiliser Wireshark pour contrôler une interface Ethernet dans le cadre de l'enregistrement du flux de paquets
- Générer une connexion TCP à l'aide d'un navigateur Web
- Observer la connexion initiale en trois étapes du protocole TCP/IP

Contexte / Préparation

Dans le cadre de ces travaux pratiques, vous utiliserez l'analyseur de paquets réseau Wireshark (Wireshark Network Packet Analyzer) pour afficher les paquets TCP/IP générés par la connexion TCP en trois étapes. Lorsqu'une application utilisant le protocole TCP démarre initialement sur un hôte, le protocole utilise la connexion en trois étapes pour établir une connexion TCP fiable entre les deux hôtes. Les paquets initiaux du flux TCP sont présentés ici : le paquet SYN, puis le paquet SYN ACK et enfin, le paquet ACK.

Attention : l'installation ou l'utilisation d'une application Analyseur de paquets peut constituer une violation de la politique de sécurité d'une organisation, qui peut entraîner de graves conséquences légales et financières. Il est donc recommandé d'obtenir les autorisations requises avant de télécharger, d'installer ou d'exécuter une application Analyseur de paquets.

Remarque : le terme « paquet » est utilisé dans ces travaux pratiques. Wireshark capture les trames Ethernet, qui contiennent les paquets IP. L'application Wireshark utilise le terme « trame » lors de l'analyse des captures. Les deux termes sont souvent utilisés de manière interchangeable. Gardez néanmoins à l'esprit qu'une trame est un outil d'encapsulation de liaison de données de couche 2, et qu'un paquet est une encapsulation réseau de couche 3.

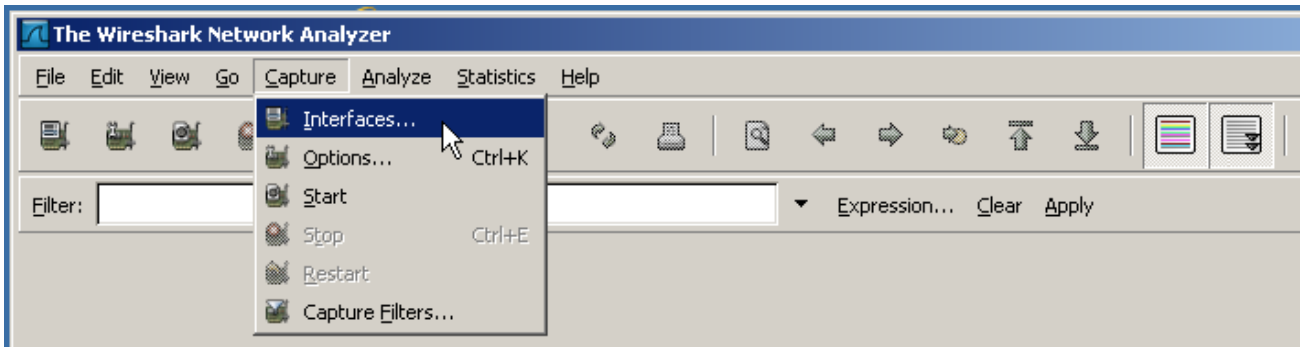
Tâche 1 : préparation de Wireshark pour la capture de paquets

Étape 1 : lancement de Wireshark

Double-cliquez sur l'icône Wireshark sur le Bureau.

Étape 2 : sélection de l'interface à utiliser pour la capture de paquets

a. Dans le menu **Capture**, cliquez sur **Interfaces**.

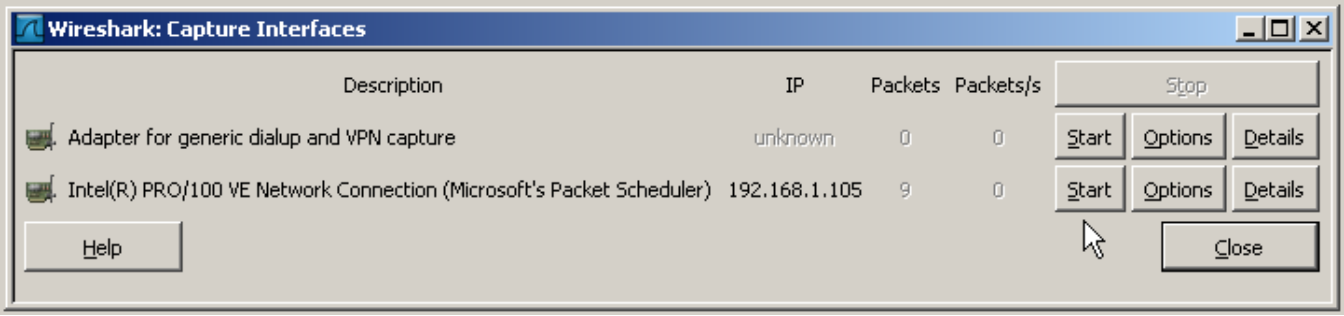


Étape 3 : démarrage d'une capture réseau

a. Choisissez l'adaptateur d'interface Ethernet du réseau local pour la capture du trafic réseau. Cliquez sur le bouton **Start** de l'interface choisie.

b. Renseignez l'adresse IP associée à l'adaptateur Ethernet, car il s'agit de l'adresse IP source à rechercher lors de l'examen des paquets capturés.

Adresse IP de l'hôte : _____



Tâche 2 : génération et analyse des paquets capturés

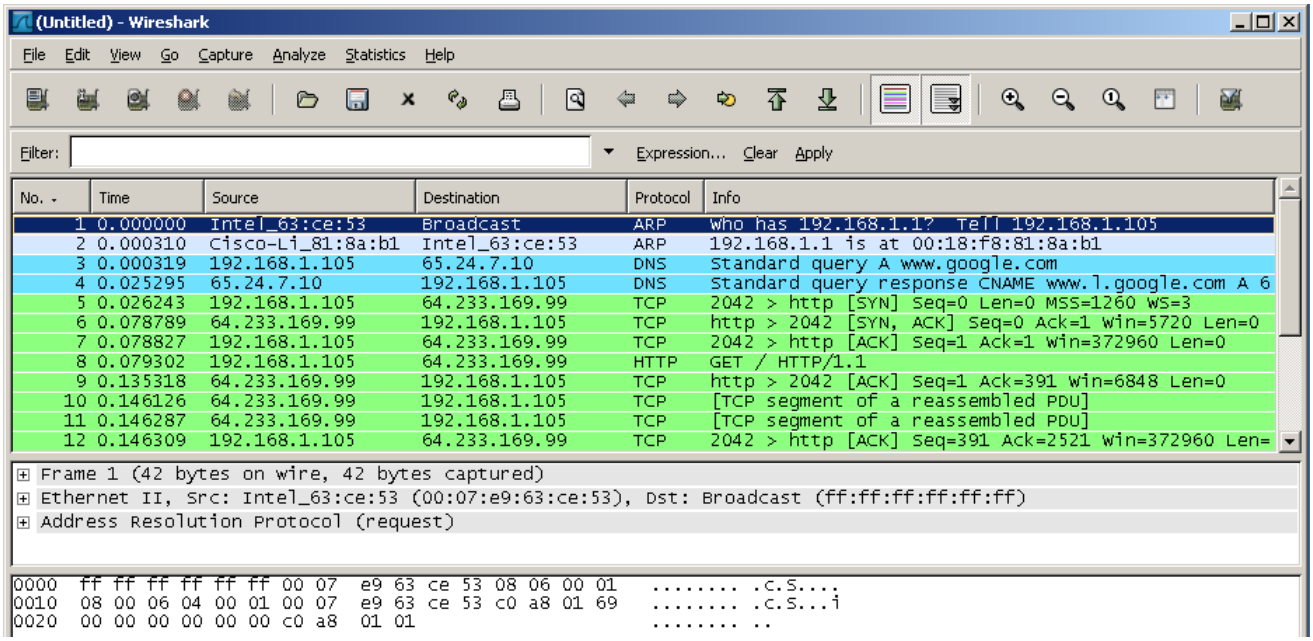
Étape 1 : ouverture d'un navigateur et accès à un site Web

a. Accédez à la page www.google.com. Réduisez la fenêtre Google et revenez dans Wireshark. Le trafic capturé qui s'affiche doit être similaire à celui illustré ci-dessous.

Remarque : votre formateur peut vous diriger vers un autre site Web. Dans ce cas, entrez le nom ou l'adresse du site Web ci-dessous :

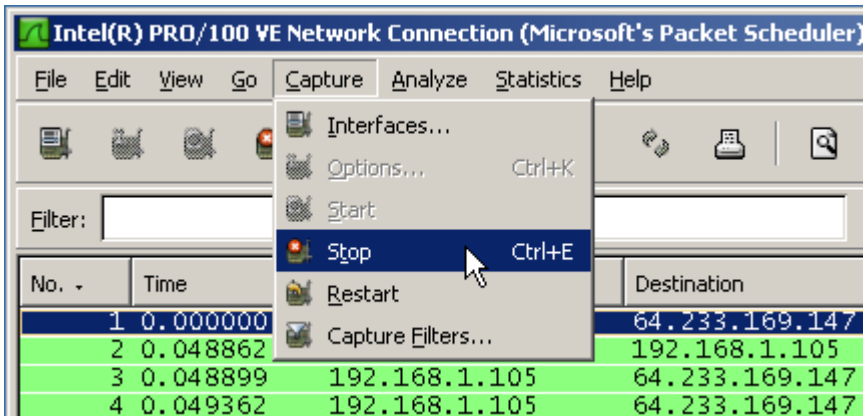
_____

b. Les fenêtres de capture sont désormais actives. Dans la fenêtre Wireshark, localisez les colonnes **Source**, **Destination** et **Protocol**. Les données HTTP transportant le texte et les graphiques de la page Web utilisent la fonction de fiabilité de TCP.



Étape 2 : interruption de la capture

Dans le menu Wireshark Capture, cliquez sur **Stop**.



Étape 3 : analyse de la capture

Si l'ordinateur a été démarré récemment et qu'aucune activité d'accès à Internet n'y a été enregistrée, le processus complet est visible dans la capture, notamment ARP, DNS et la connexion en trois étapes du protocole TCP.

L'écran de capture de l'étape 1 de la tâche 2 présente tous les paquets nécessaires au système pour accéder à un site Web, en commençant par le protocole initial ARP pour l'adresse MAC de l'interface du routeur de la passerelle. (Plusieurs captures d'écran sont possibles.)

a. Dans la capture d'écran, le processus commence par la trame 1, qui est une diffusion ARP provenant de l'ordinateur source et qui permet de déterminer l'adresse MAC de la passerelle par défaut du routeur. La passerelle correspond à l'interface Fast Ethernet de réseau local du routeur. L'ordinateur doit convertir l'adresse IP de la passerelle par défaut en adresse MAC de l'interface pour pouvoir envoyer la première trame ou le premier paquet au routeur.

   Quelle est l'adresse IP de la passerelle par défaut du routeur ? _____

b. La seconde trame constitue la réponse du routeur, indiquant au système l'adresse MAC de son interface Fast Ethernet.

   Quelle est l'adresse MAC ? _____

c. La troisième trame est une requête DNS transmise de l'ordinateur vers le serveur DNS configuré, qui tente de convertir le nom de domaine www.google.com en adresse IP du serveur Web. L'ordinateur doit disposer de l'adresse IP pour pouvoir envoyer la première trame au serveur Web.

   Quelle est l'adresse IP du serveur DNS requise par l'ordinateur ? _____

d. La quatrième trame est la réponse du serveur DNS, avec l'adresse IP de www.google.com. Vous devez faire défiler l'affichage vers la droite pour afficher l'adresse IP du serveur Google dans la réponse DNS, mais vous ne le visualiserez que dans la prochaine trame.

e. La cinquième trame est le début de la connexion en trois étapes du protocole TCP [SYN].

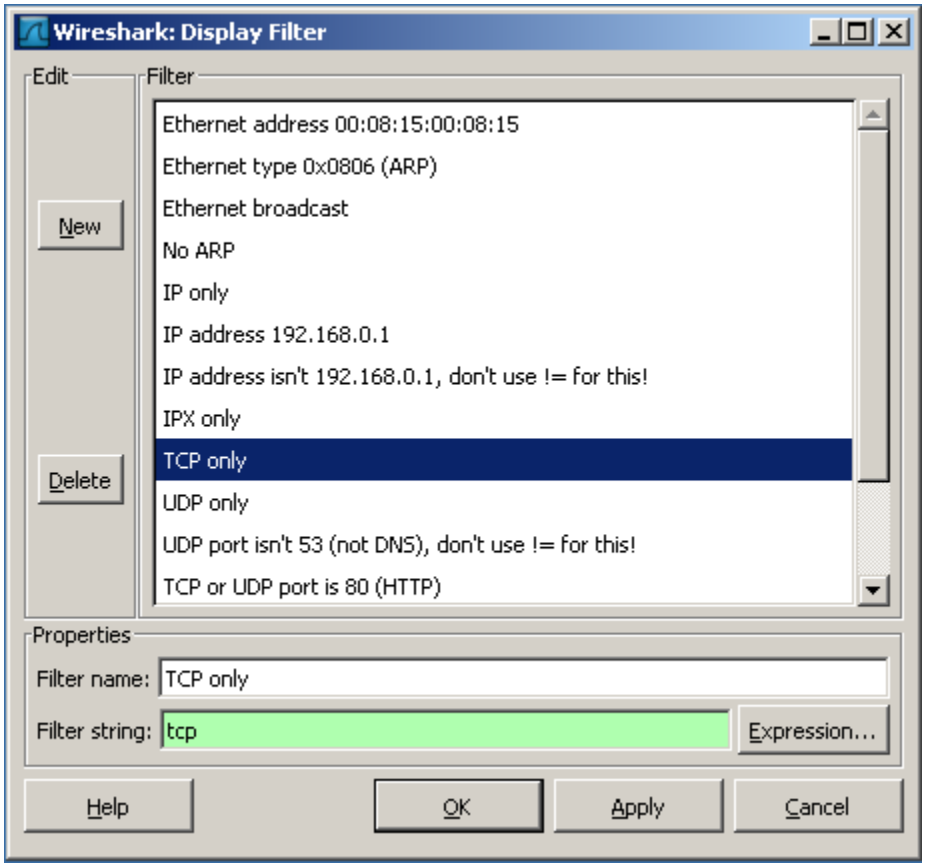
   Quelle est l'adresse IP du serveur Web de Google ? _____

Étape 4 : filtrage de la capture pour afficher uniquement les paquets TCP

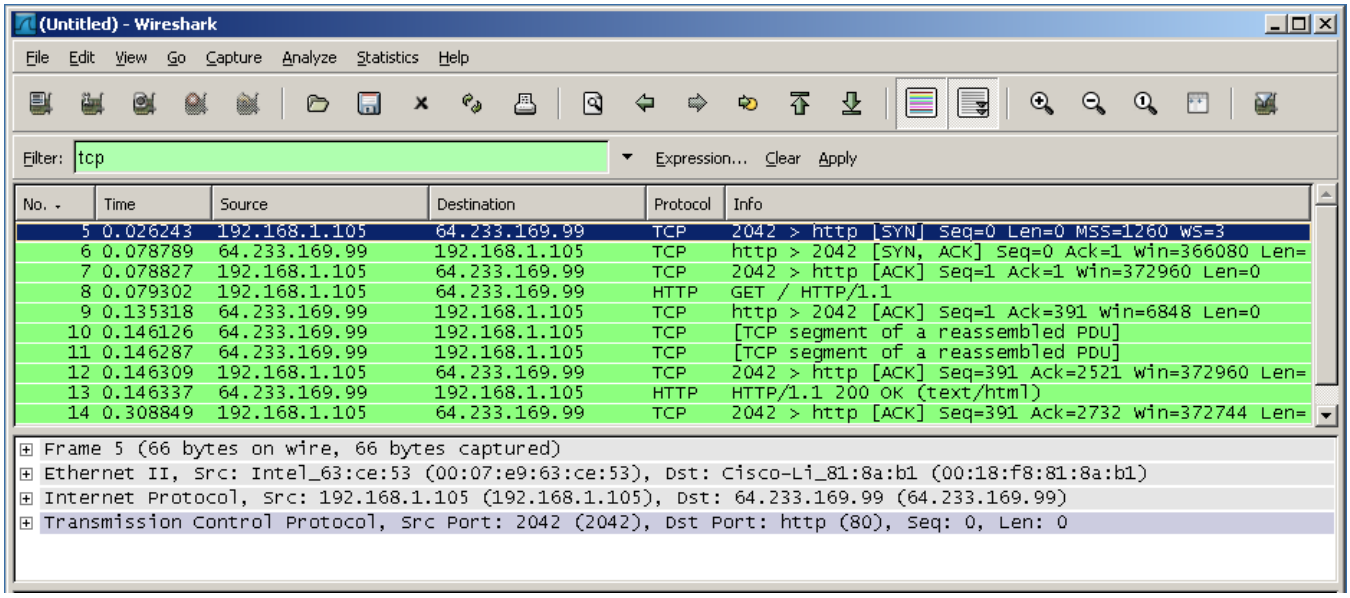
Si plusieurs paquets ne sont pas associés à la connexion TCP, il se peut qu'il soit nécessaire d'utiliser la fonction de filtrage de Wireshark.

a. Pour utiliser un filtre préconfiguré, cliquez sur l'option **Analyze** dans le menu, puis cliquez sur **Display Filters**.

b. Dans la fenêtre **Display Filter**, cliquez sur **TCP only**, puis sur **OK**.



c. Dans la fenêtre Wireshark, faites défiler l'affichage jusqu'au premier paquet TCP capturé. Il s'agit du premier paquet du flux.



d. Dans la colonne Info, recherchez trois paquets similaires aux trois premiers affichés dans la fenêtre ci-dessus. Le premier paquet TCP est le paquet [SYN] provenant de l'ordinateur source. Le second paquet est la réponse [SYN, ACK] du serveur Web. Le troisième paquet est le paquet [ACK] de l'ordinateur source, qui termine la connexion en trois étapes.

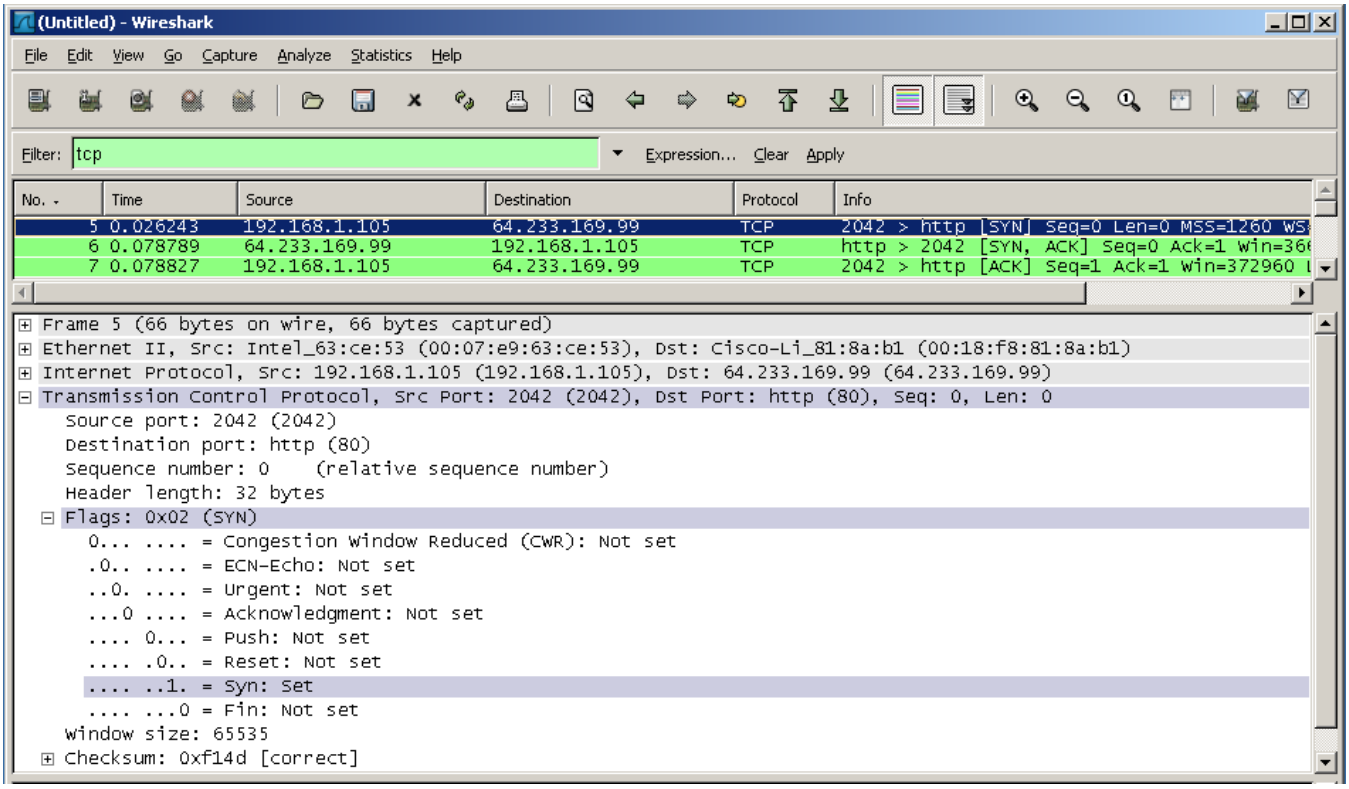
Étape 5 : inspection de la séquence d'initialisation TCP

a. Dans la fenêtre Wireshark supérieure, cliquez sur la ligne contenant le premier paquet identifié au cours de l'étape 4. La ligne est mise en surbrillance et les informations décodées provenant de ce paquet s'affichent dans les deux fenêtres inférieures.

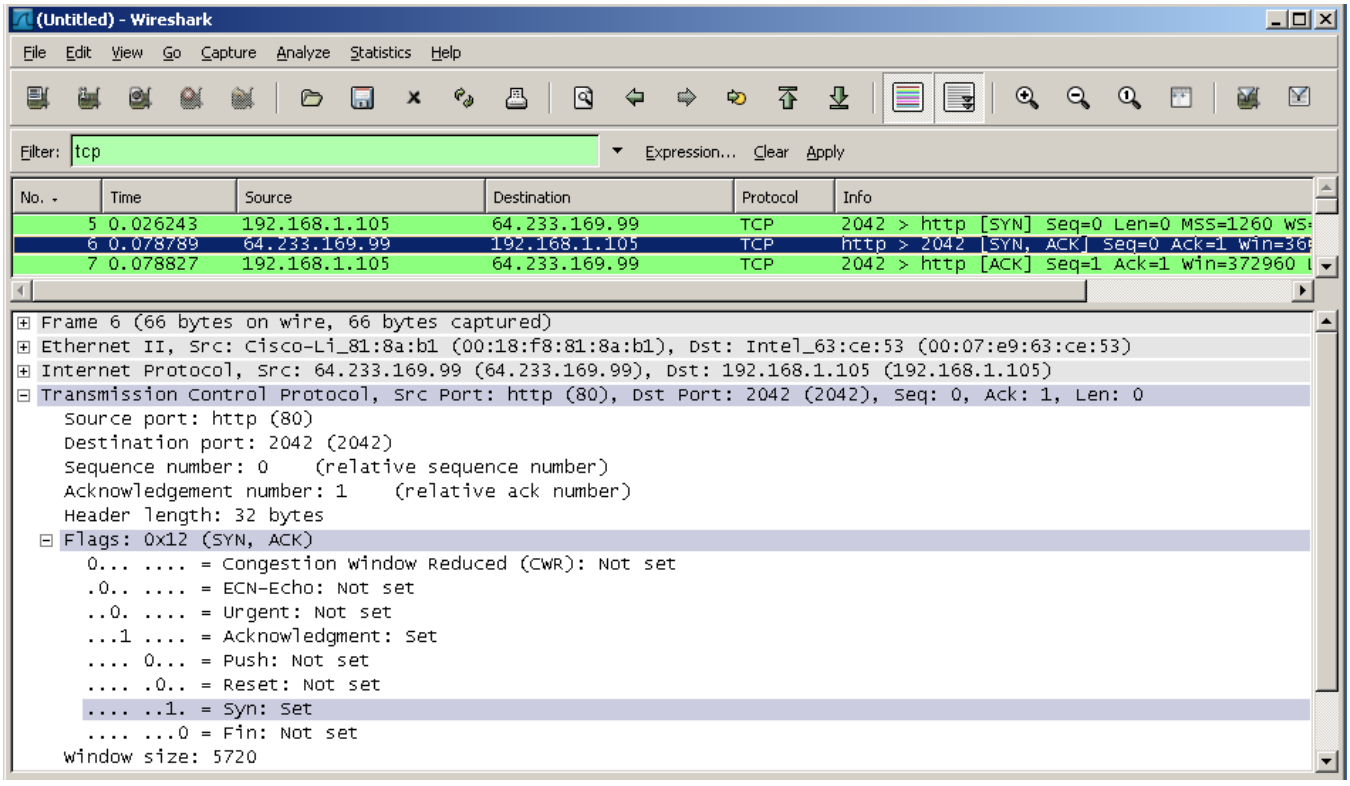
Remarque : les fenêtres Wireshark ci-dessous ont été redimensionnées pour permettre l'affichage dans un format compact. La fenêtre du milieu contient le décodage détaillé du paquet.

b. Cliquez sur l'icône **+** pour développer l'affichage des informations TCP. Pour réduire l'affichage, cliquez sur l'icône **–**.

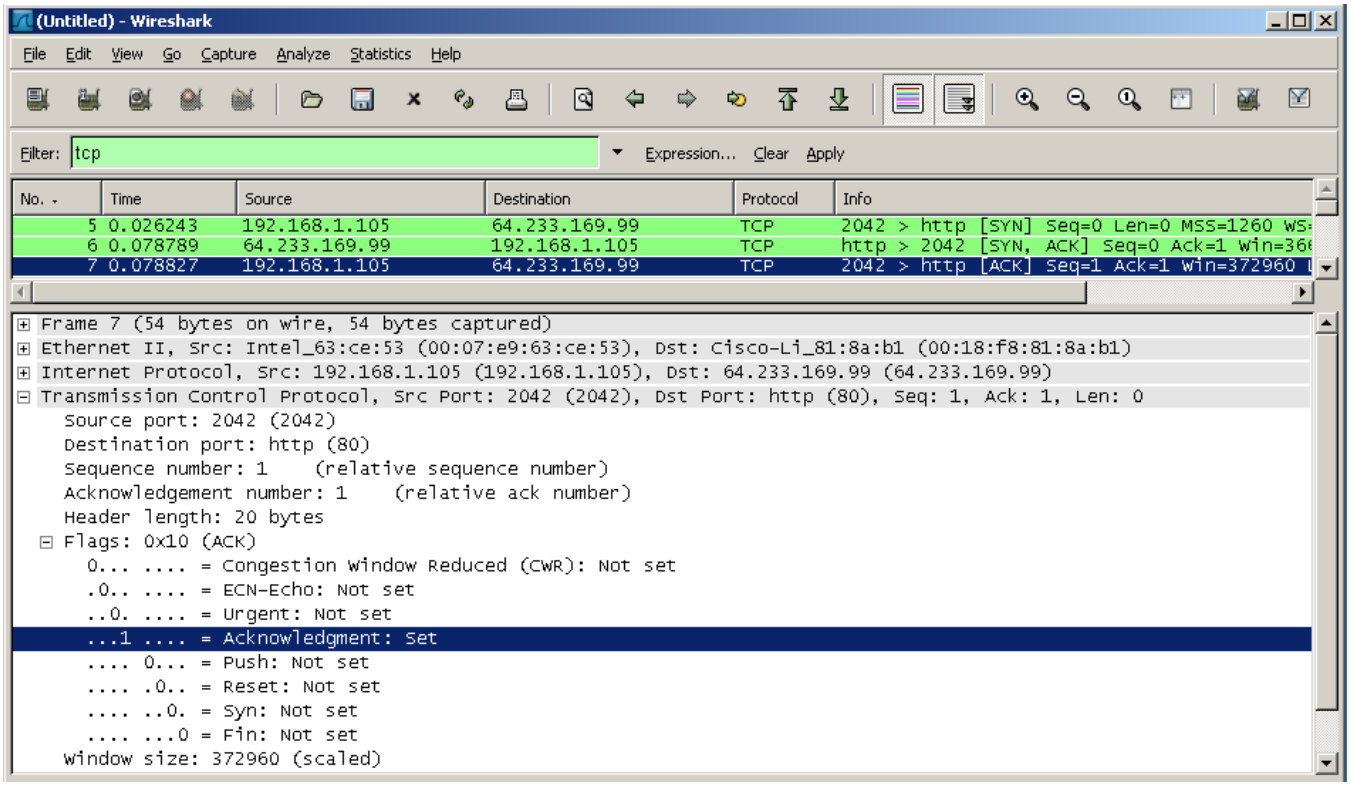
c. Notez que dans le premier paquet TCP, le numéro d'ordre relatif est défini sur 0, et que le bit SYNC est défini sur 1 dans le champ Indicateurs.



d. Notez que dans le second paquet TCP de la connexion en trois étapes, le numéro d'ordre relatif est défini sur 0, et que le bit SYNC et le bit ACK sont définis sur 1 dans le champ Indicateurs.



e. Dans la troisième et dernière trame de la connexion en trois étapes, seul le bit ACK est défini, et le numéro d'ordre est défini sur le point de départ 1. Le numéro de reçu est également défini sur le point de départ 1. La connexion TCP est désormais établie, et la communication entre l'ordinateur source et le serveur Web peut commencer.



f. Fermez Wireshark.

Tâche 3 : remarques générales

a. Des centaines de filtres sont disponibles dans Wireshark. Un grand réseau peut avoir un grand nombre de filtres et plusieurs types de trafic. Dans cette liste, quels sont les trois filtres qui, selon vous, seraient les plus utiles à un administrateur réseau ?

_____

b. Wireshark est-il un outil de surveillance hors bande ou intrabande d'un réseau ? _____

Expliquez votre réponse.

_____

_____