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

Objectifs

Analyser les paquets à l'aide de Wireshark

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, comme 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.

Ressources requises

- Poste de travail avec Wireshark

Analyser les paquets à l'aide de Wireshark

Étape 1: Appliquez un filtre à la capture enregistrée.

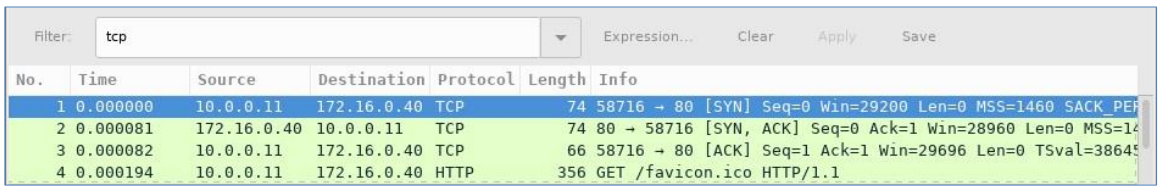
a. Lancez Wireshark sur votre ordinateur.

b. Lancez une capture

c. Depuis votre navigateur, accédez à un site Web

d. Dès que la page d'accueil s'affiche, arrêter la capture sous Wireshark

e. Appliquez un filtre **tcp** à la capture. Dans cet exemple, les 3 premières trames représentent un exemple de trafic.



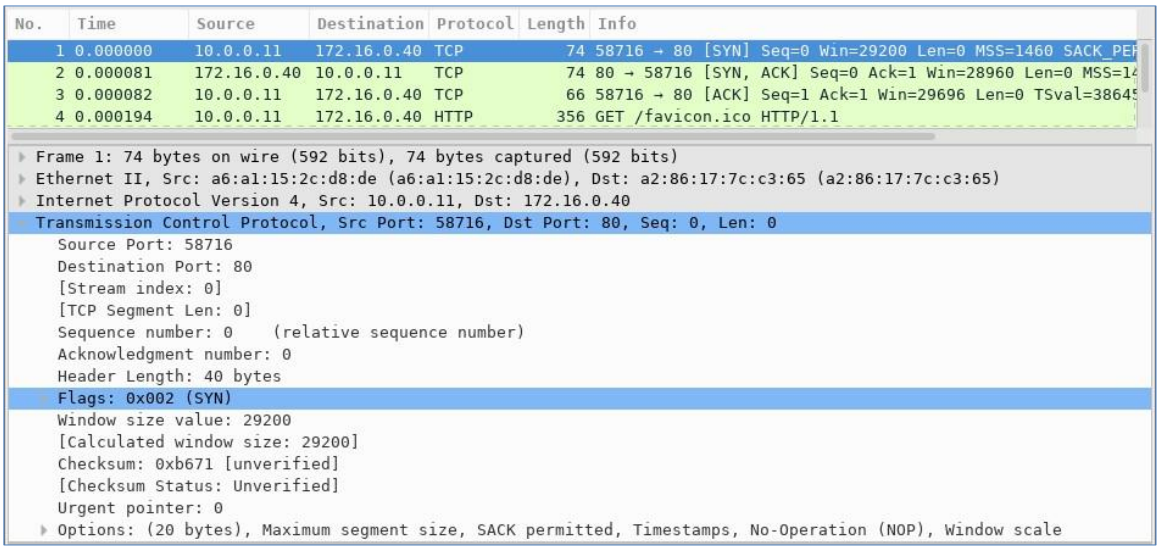
Étape 2: Examinez les informations au sein des paquets, y compris les adresses IP, les numéros de port TCP et les indicateurs de contrôle TCP.

a. Dans cet exemple, la trame 1 correspond au début de la connexion en trois étapes entre l'ordinateur et le serveur sur H4. Dans le volet de la liste des paquets (section supérieure de la fenêtre principale), sélectionnez le premier paquet, le cas échéant.

b. Cliquez sur la **flèche**à gauche du protocole TCP (Transmission Control Protocol) dans le volet de détails des paquets pour développer et examiner les données TCP. Localisez les informations sur les ports source et de destination.

c. Cliquez sur la **flèche** à gauche des indicateurs. Une valeur de 1 signifie que l'indicateur est défini. Repérez l'indicateur défini dans ce paquet.

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



Quel est le numéro du port source TCP ?

Comment classifieriez-vous le port source ?

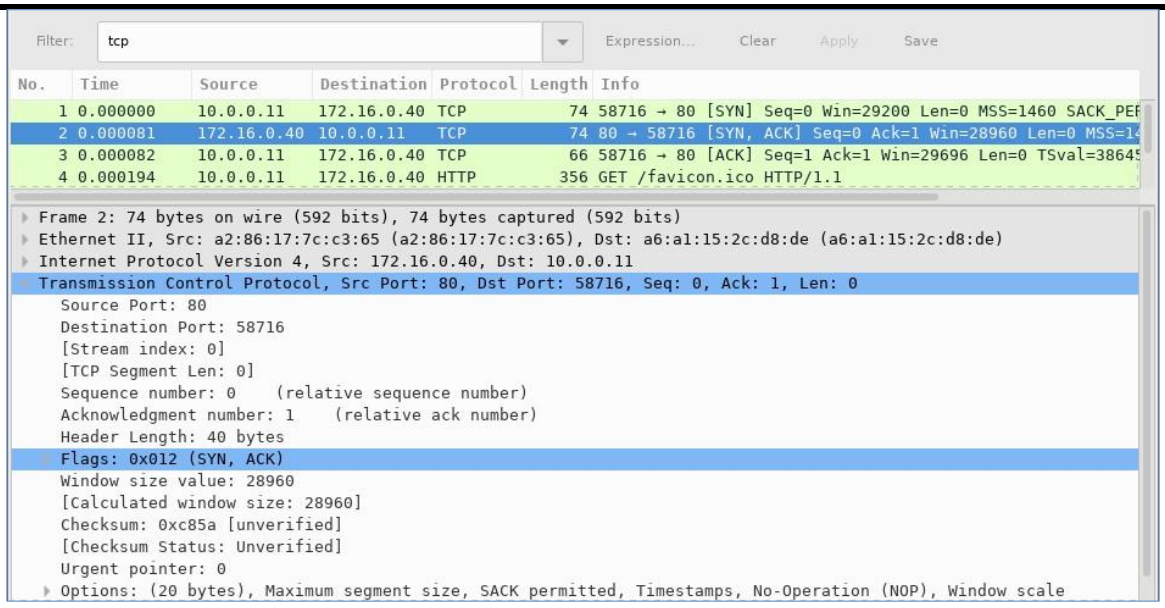
Quel est le numéro du port de destination TCP ?

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. Sélectionnez le paquet suivant dans la connexion en trois étapes. Dans cet exemple, il s'agit de la trame 2. C'est la réponse du serveur web à la requête initiale de démarrage d'une session.

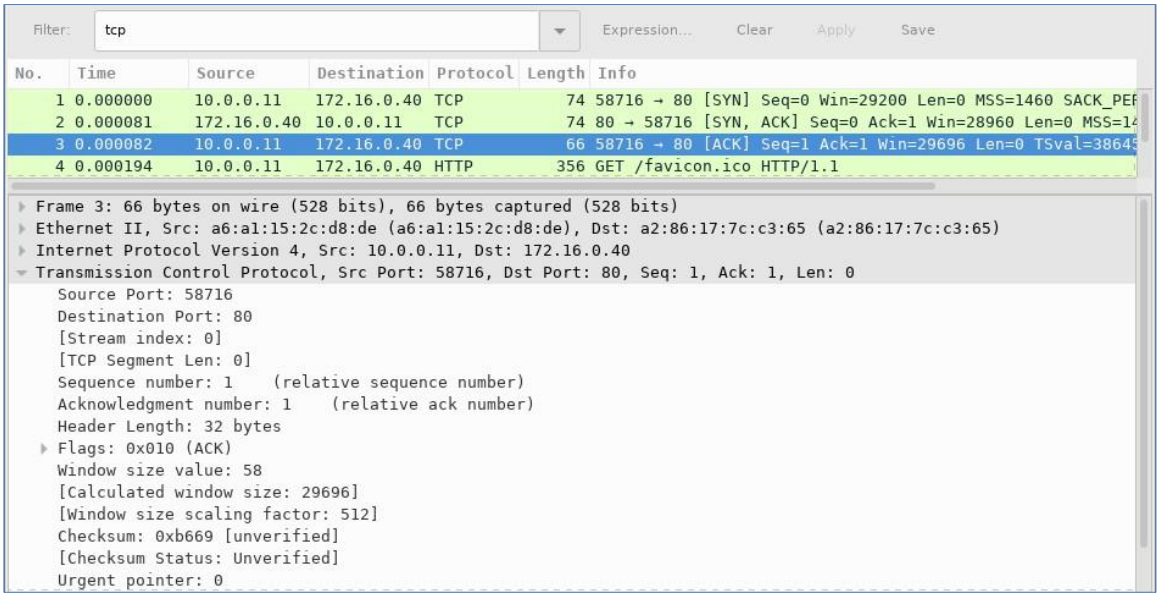


Quelles sont les valeurs des ports source et de destination ?

Quels sont les indicateurs définis ?

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

e. Enfin, sélectionnez le troisième paquet dans la connexion en trois étapes.



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.