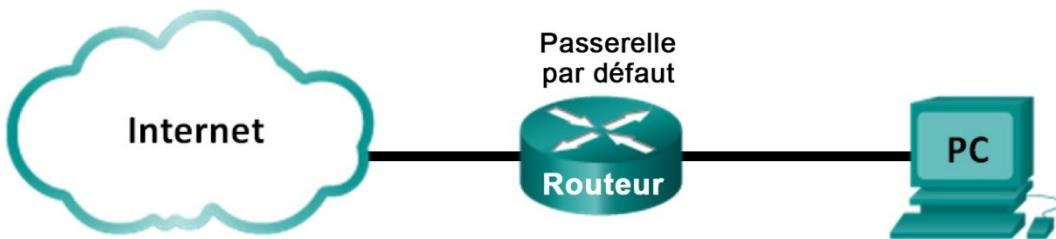


Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

Topologie



Objectifs

Partie 1 : Préparer Wireshark pour capturer des paquets

Partie 2 : Capturer, localiser et examiner les paquets

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.

Remarque : Ces travaux pratiques supposent que vous avez accès à Internet.

Ressources requises

1 ordinateur (Windows 7 ou 8, équipé d'un accès à Internet, d'un accès aux invites de commandes et de Wireshark)

Partie 1: Préparer Wireshark pour capturer des paquets

Dans la première partie, vous allez démarrer le programme Wireshark et sélectionner l'interface appropriée 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 votre ordinateur et l'adresse physique de sa carte réseau, également appelée adresse MAC.

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

```
Physical Address . . . . . : 00-1A-73-EA-63-8C
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%14(PREFERRED)
IPv4 Address . . . . . : 192.168.1.130(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
```

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

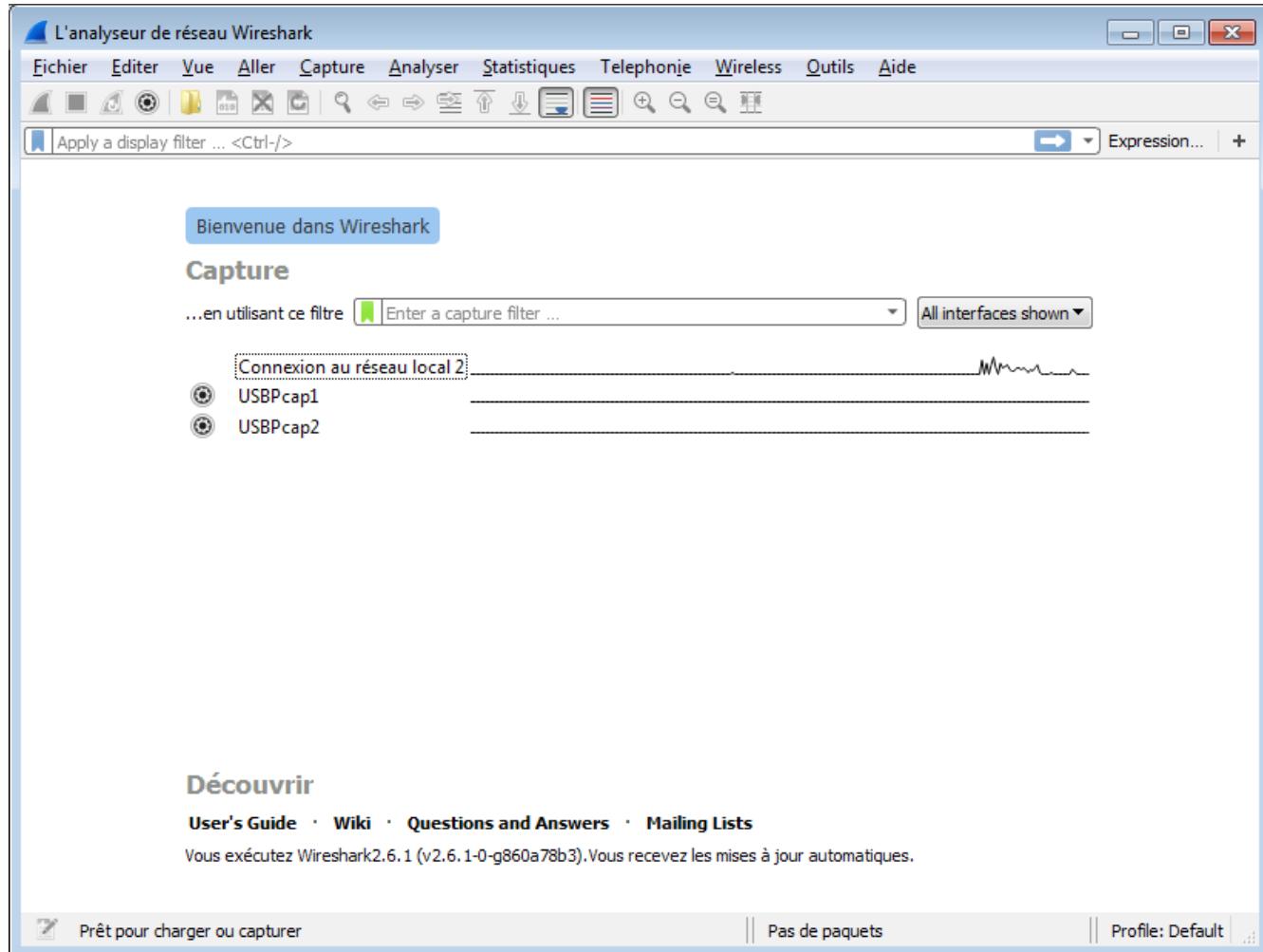
- b. Inscrivez les adresses IP et MAC associées à la carte Ethernet sélectionnée. Il s'agit de l'adresse source à rechercher lors de l'examen des paquets capturés.

Adresse IP de l'ordinateur hôte :

Adresse MAC de l'ordinateur hôte :

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

- Cliquez sur le bouton **Démarrer** de Windows. Dans le menu déroulant, double-cliquez sur **Wireshark**.
- Lorsque Wireshark démarre, cliquez sur « Connexion au réseau local ».



Partie 2: Capturer, localiser et examiner des paquets

Étape 1: Capturez les données.

- Cliquez sur le bouton **Start** (Démarrer) pour démarrer la capture des données.
- Accédez à www.google.com. Réduisez la fenêtre du navigateur et revenez à Wireshark. Arrêtez la capture des données.

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

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

The screenshot shows the Wireshark interface with a list of captured network frames. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The Info column provides detailed descriptions of each frame, such as 'Name query NB ISATAP<00>' for a DNS request and 'HTTP/1.1 302 Found (text/html)' for a response. Below the main list are two expanded sections: 'Frame 1...' and 'User Datagram Protocol...'. The bottom section shows the raw hex and ASCII data for the selected frame, which is a DNS request for 'apis.google.com'.

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'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.

- 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.

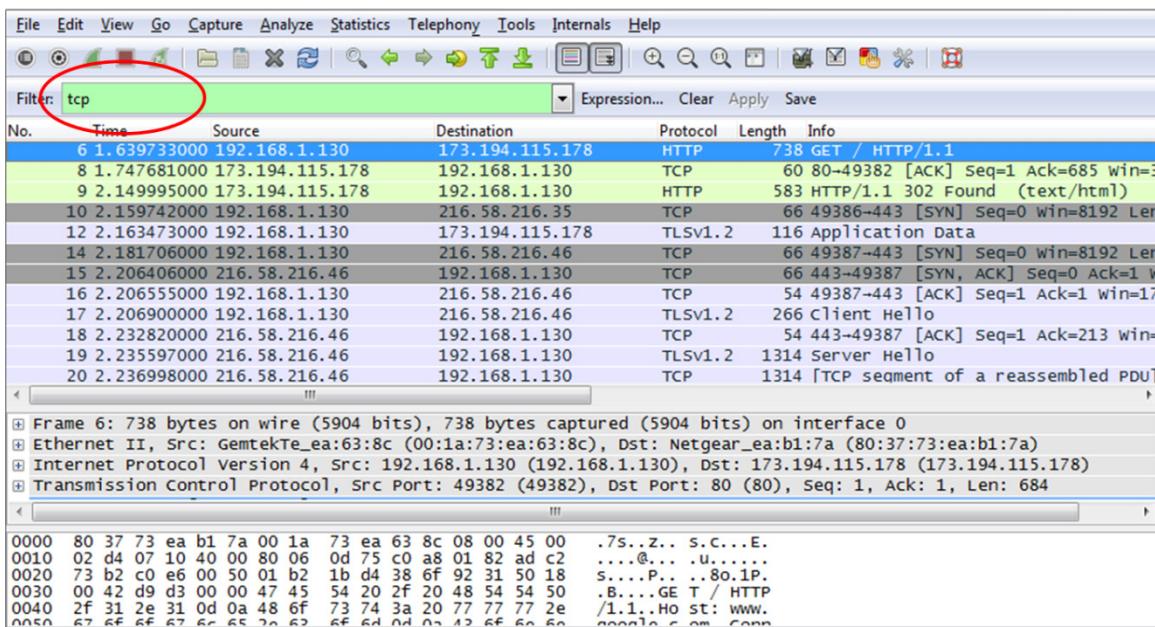
Quelle est l'adresse IP du serveur DNS que l'ordinateur a interrogé ?

- La trame 13 est la réponse du serveur DNS. Elle contient l'adresse IP de www.google.com.
- Recherchez le paquet approprié pour le début de votre connexion en trois étapes. Dans cet exemple, la trame 14 correspond au début de la connexion TCP en trois étapes.

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

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

- 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.

- Dans notre exemple, la trame 14 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).
- 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 indicateurs. Examinez les ports source et de destination ainsi que les indicateurs qui sont définis.

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

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

Wireshark screenshot showing a TCP connection conversation. The selected packet is a SYN from port 49387 to port 443. The packet details pane shows the flags: 0x0000 0000 0010 = Flags: 0x002 (SYN).

No.	Time	Source	Destination	Protocol	Length	Info
8	1.747681000	173.194.115.178	192.168.1.130	TCP	60	80-49382 [ACK] Seq=1 Ack=685 Win=17
9	2.149995000	173.194.115.178	192.168.1.130	HTTP	583	HTTP/1.1 302 Found (text/html)
10	2.159742000	192.168.1.130	216.58.216.35	TCP	66	49386-443 [SYN] Seq=0 Win=8192 Len=0
12	2.163473000	192.168.1.130	173.194.115.178	TLSV1.2	116	Application Data
14	2.181706000	192.168.1.130	216.58.216.46	TCP	66	49387-443 [SYN] Seq=0 Win=8192 Len=0
15	2.206406000	216.58.216.46	192.168.1.130	TCP	66	443-49387 [SYN, ACK] Seq=0 Ack=1 Win=17
16	2.206555000	192.168.1.130	216.58.216.46	TCP	54	49387-443 [ACK] Seq=1 Ack=1 Win=17
17	2.206555000	192.168.1.130	216.58.216.46	TLSV1.2	266	Client Hello

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 15. C'est la réponse du serveur web Google à la requête initiale de démarrage d'une session.

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

The screenshot shows a Wireshark capture of a TCP connection. The packet list pane shows several frames, with frame 15 selected. The details pane shows the following information for frame 15:

- Frame 15: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)
- Internet Protocol Version 4, Src: 216.58.216.46 (216.58.216.46), Dst: 192.168.1.130 (192.168.1.130)
- Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49387 (49387), Seq: 0, Ack: 1, Len: 0

Source Port: 443 (443)
Destination Port: 49387 (49387)
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes

.... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)
000. = Reserved: Not set
....0 = Nonce: Not set
....0.... = Congestion Window Reduced (CWR): Not set
....0.. = ECN-Echo: Not set
....0..0 = Urgent: Not set
....0..1 = Acknowledgment: Set
....0....0 = Push: Not set
....0....0.. = Reset: Not set
....0....0..1. = Syn: Set
....0....0 = Fin: Not set
window size value: 42900
[calculated window size: 42900]

Checksum: 0xf159 [validation disabled]
Urgent pointer: 0

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, examinez le troisième paquet de la connexion en trois étapes de l'exemple. Cliquez sur la trame 16 dans la fenêtre du haut pour afficher les informations suivantes dans cet exemple :

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

Wireshark screenshot showing a TCP connection between 192.168.1.130 and 216.58.216.46. The packet list shows the three steps of the TCP handshake: SYN, SYN-ACK, and ACK. The details pane for the third packet (ACK) shows the TCP header fields: Source Port: 49387, Destination Port: 443, Sequence number: 1, Acknowledgment number: 1, Header Length: 20 bytes, and flags: ACK. It also shows the window size value: 68, calculated window size: 17408, and window size scaling factor: 256.

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. Indiquez trois filtres qui pourraient être utiles à un administrateur réseau.
2. De quelles autres façons Wireshark pourrait-il être utilisé dans un réseau de production ?