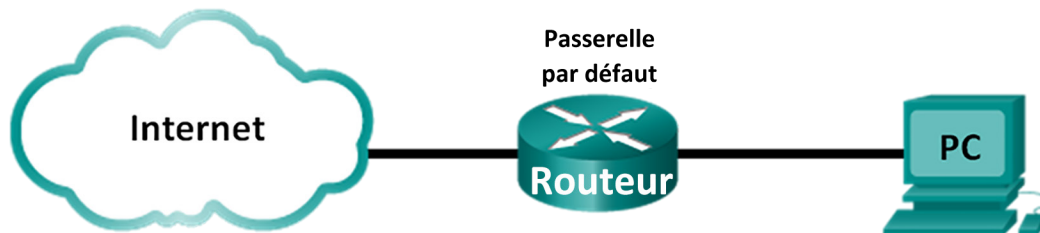


Travaux pratiques - Utilisation de Wireshark pour observer la connexion TCP en trois étapes

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 ne peuvent pas être effectués avec Netlab. Ces travaux pratiques supposent que vous avez accès à Internet.

Ressources requises

1 ordinateur (Windows 7, 8 ou 10, 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.

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

```
Physical Address. . . . . : 00-24-D7-1C-50-44
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80dd:5657:ad20:f4b3%16 (Preferred)
IPv4 Address. . . . . : 192.168.1.146 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

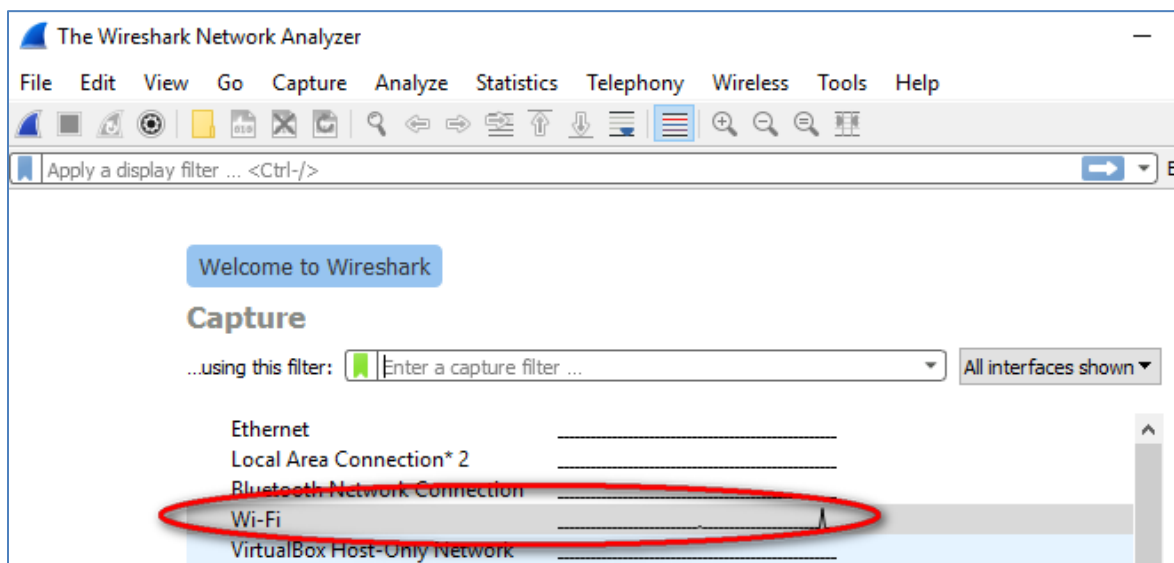
- b. Inscrivez les adresses IP et MAC associées à la carte Ethernet sélectionnée. Il s'agit de l'adresse source à rechercher lors de l'examen des paquets capturés.

Adresse IP de l'ordinateur hôte : _____

Adresse MAC de l'ordinateur hôte : _____

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

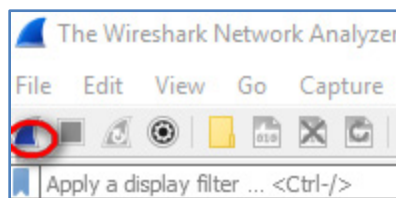
- a. Cliquez sur le bouton **Démarrer** de Windows. Dans le menu déroulant, double-cliquez sur **Wireshark**.
- b. Une fois Wireshark démarré, sélectionnez l'interface active pour la capture des données. L'interface active affiche les activités de trafic.



Partie 2 : Capturer, localiser et examiner des paquets

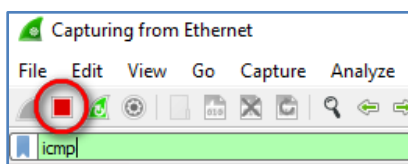
Étape 1 : Capturez les données.

- a. Cliquez sur le bouton **Start** (Démarrer) pour démarrer la capture des données.



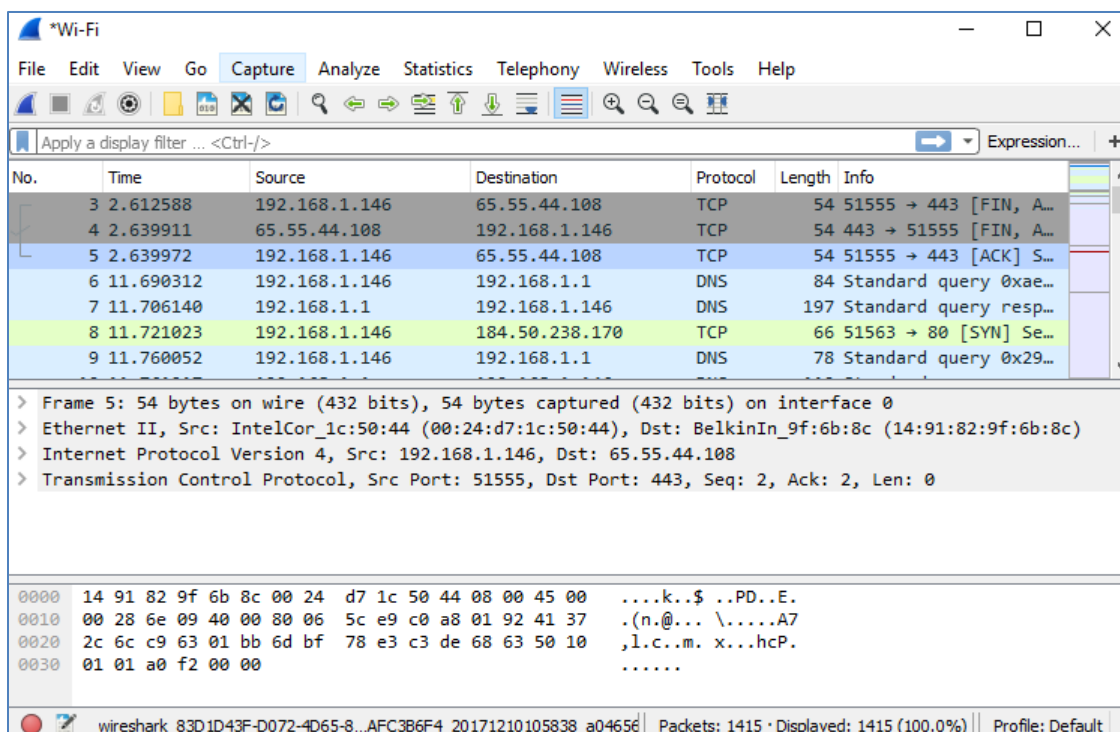
- b. Ouvrez un navigateur web et tapez www.google.com.

- c. 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).



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. Il a donc commencé par la requête DNS afin de résoudre `www.google.com`.

- a. La trame 6 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.

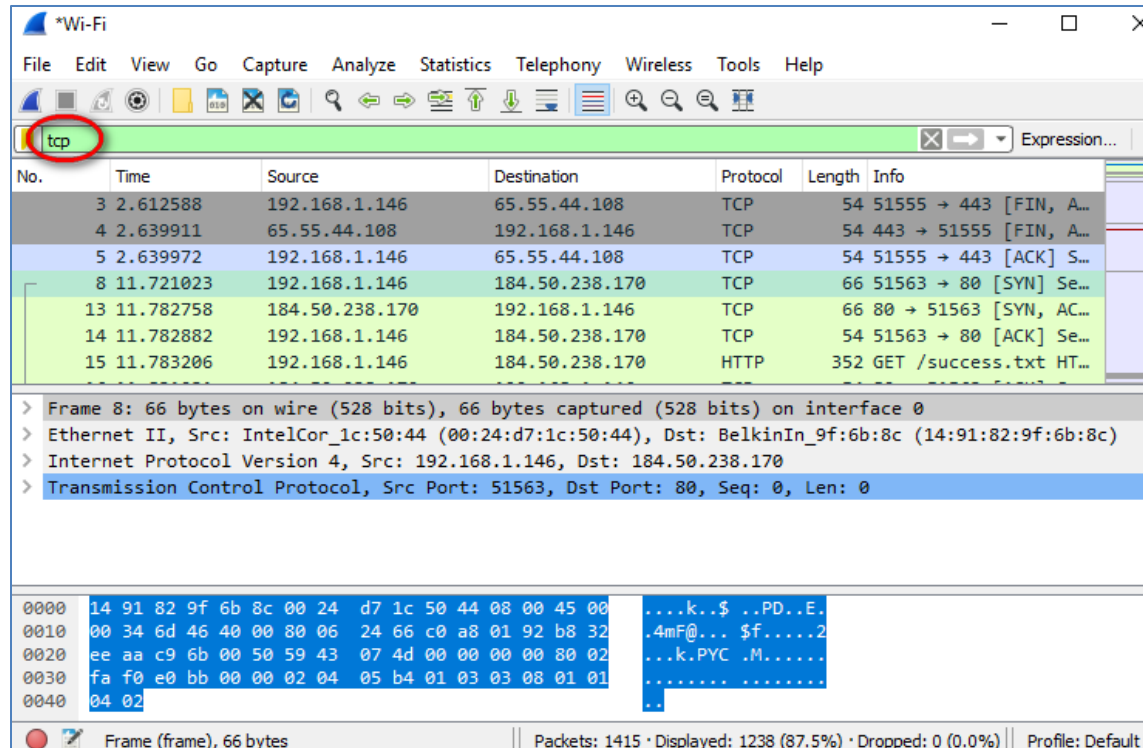
Quelle est l'adresse IP du serveur DNS que l'ordinateur a interrogé ? _____

- b. La trame 7 est la réponse du serveur DNS. Elle contient l'adresse IP de `www.google.com`.

- c. Recherchez le paquet approprié pour le début de votre connexion en trois étapes. Dans cet exemple, la trame 8 correspond au début de la connexion TCP en trois étapes.

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

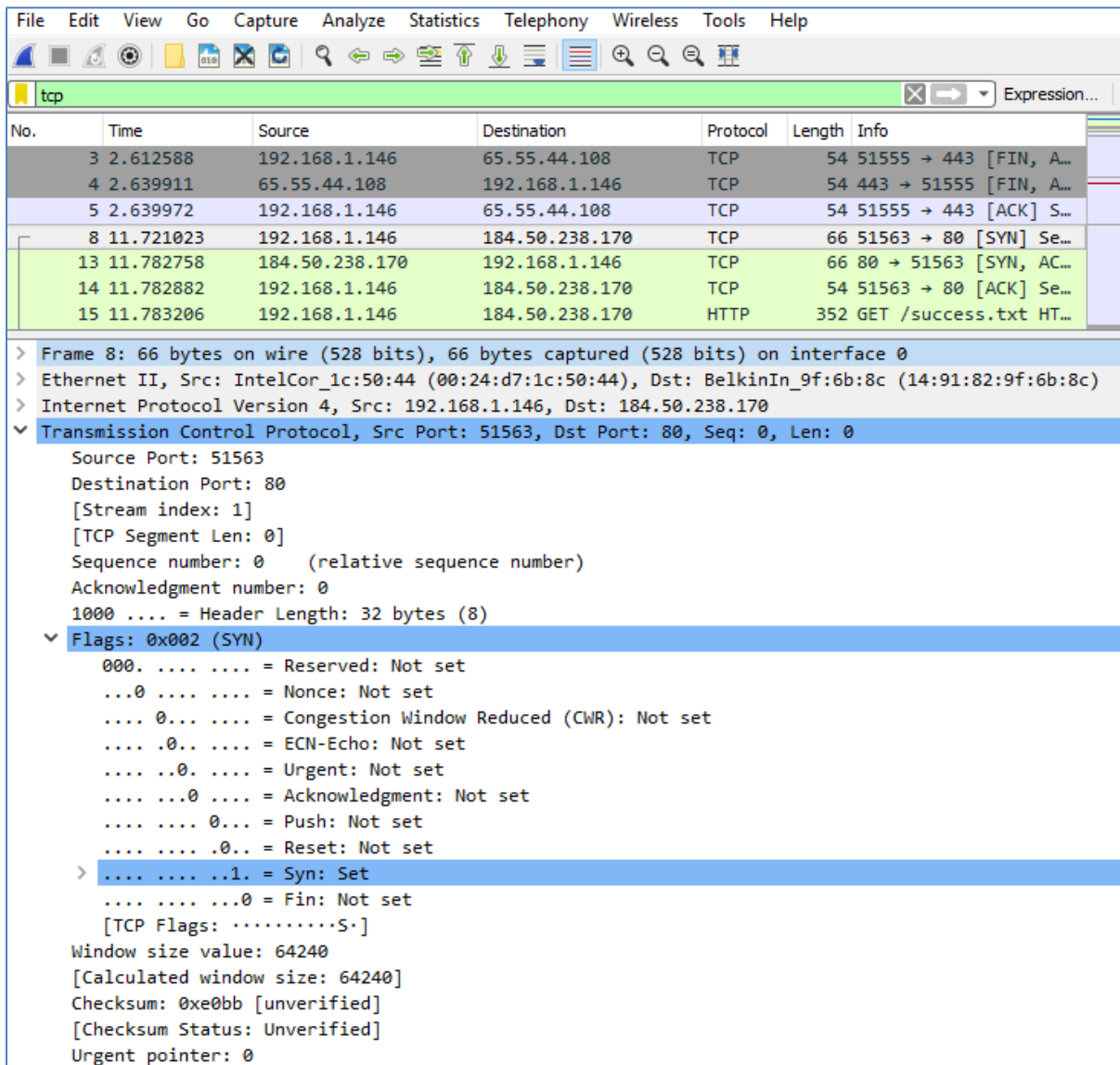
- d. Si vous avez de nombreux paquets qui ne sont pas liés à la connexion TCP, il peut être nécessaire d'utiliser la fonction de filtre de Wireshark. Saisissez **tcp** dans la zone de saisie du filtre dans Wireshark et appuyez sur **Entrée**.



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.

- Dans notre exemple, la trame 8 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.



The screenshot shows the Wireshark interface with a packet capture of a TCP connection. The packet list at the top shows several packets, with packet 8 selected. The packet details pane shows the structure of the TCP segment, including source and destination ports, sequence number, and flags.

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
Internet Protocol Version 4, Src: 192.168.1.146, Dst: 184.50.238.170
Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 0, Len: 0
Source Port: 51563
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
000. = Reserved: Not set
...0 = Nonce: Not set
... 0... = Congestion Window Reduced (CWR): Not set
... .0.. = ECN-Echo: Not set
... ..0. = Urgent: Not set
... ...0 = Acknowledgment: Not set
... 0... = Push: Not set
...0.. = Reset: Not set
... ..1. = Syn: Set
... 0 = Fin: Not set
[TCP Flags:S.]
Window size value: 64240
[Calculated window size: 64240]
Checksum: 0xe0bb [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

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** dans le menu Wireshark et sélectionnez **Next Packet In Conversation**. Dans cet exemple, il s'agit de la trame 13. C'est la réponse du serveur web Google à la requête initiale de démarrage d'une session.

The screenshot shows the Wireshark interface with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 13 details:

- Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
- Internet Protocol Version 4, Src: 184.50.238.170, Dst: 192.168.1.146
- Transmission Control Protocol, Src Port: 80, Dst Port: 51563, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 51563
 - [Stream index: 1]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - 1000 = Header Length: 32 bytes (8)
 - 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. = Urgent: Not set
 -1 = Acknowledgment: Set
 - 0... = Push: Not set
 -0.. = Reset: Not set
 - >1. = Syn: Set
 -0 = Fin: Not set
 - [TCP Flags:A..S.]
 - Window size value: 29200
 - [Calculated window size: 29200]
 - Checksum: 0x3a72 [unverified]
 - [Checksum Status: Unverified]
 - 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 14 dans la fenêtre du haut pour afficher les informations suivantes dans cet exemple :

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

> Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 > Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
 > Internet Protocol Version 4, Src: 192.168.1.146, Dst: 184.50.238.170
 > Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 51563
 Destination Port: 80
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Acknowledgment number: 1 (relative ack number)
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
 000. = Reserved: Not set
 ...0 = Nonce: Not set
 0... = Congestion Window Reduced (CWR): Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
1 = Acknowledgment: Set
 0... = Push: Not set
0.. = Reset: Not set
0. = Syn: Not set
0 = Fin: Not set
 [TCP Flags:A....]
 Window size value: 256
 [Calculated window size: 65536]
 [Window size scaling factor: 256]
 Checksum: 0xec52 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0

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 ?
