

Travaux pratiques 8.3.2 Capture réseau avec Wireshark

Objectifs

- Réaliser la capture du trafic d'un réseau à l'aide de Wireshark pour se familiariser avec l'interface et l'environnement Wireshark
- Analyser le trafic vers un serveur Web
- Créer un filtre pour limiter la capture du réseau aux paquets ICMP (Internet Control Message Protocol)
- Utiliser la commande Ping sur un hôte distant pour observer comment le filtre de paquets ICMP fonctionne lors de la capture du réseau

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez installer Wireshark, outil bien connu de surveillance et d'analyse des protocoles réseau. Wireshark permet de capturer tous les paquets envoyés ou reçus par la carte réseau de l'ordinateur. Vous pouvez l'installer soit dans la salle de travaux pratiques, soit sur un PC à votre domicile. Vous allez l'utiliser pour suivre et afficher divers types de trafics et de protocoles réseau. Auparavant, Wireshark était connu sous le nom d'Ethereal.

Wireshark est un logiciel gratuit disponible sur www.wireshark.org. Le programme d'installation du logiciel, `wireshark-setup-0.99.6a.exe`, est en principe disponible sur le serveur local Networking Academy.

Vous pouvez réaliser ces travaux pratiques individuellement ou en équipe.

Ressources requises :

- un PC exécutant Windows XP, équipé d'un réseau Ethernet et comportant au moins deux hôtes ;
- le logiciel Wireshark, version 0.99.6 (ou une version plus récente) ;
- la connectivité Internet (optionnelle mais souhaitable) ;
- l'accès à l'invite de commandes du PC ;
- l'accès à la configuration réseau TCP/IP du PC.

Étape 1 : Installation et lancement de Wireshark

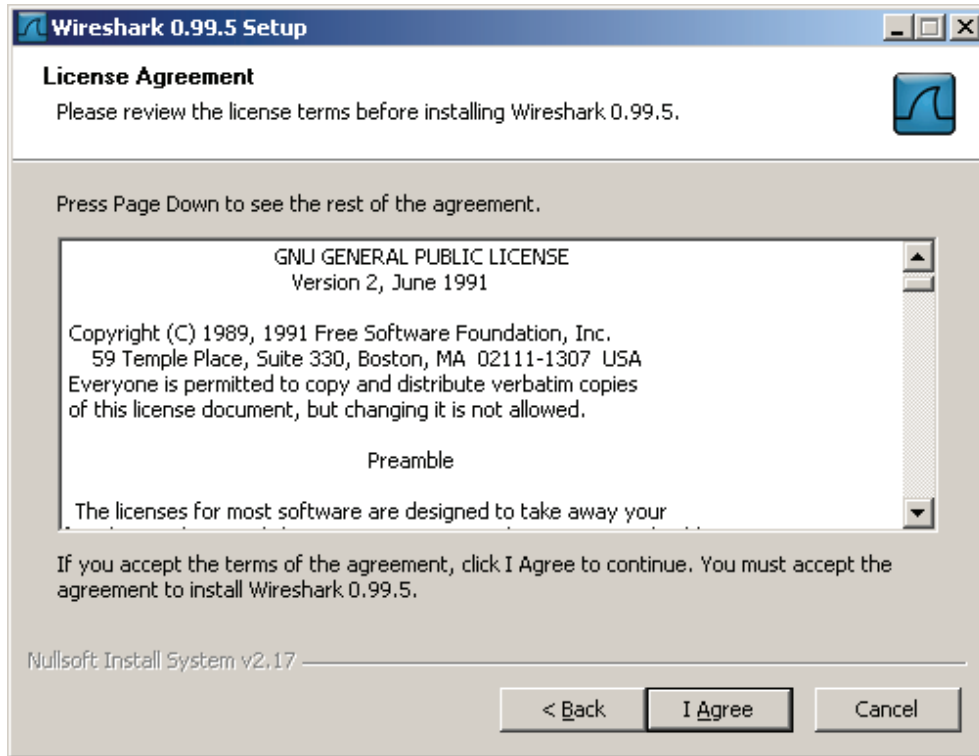
Si Wireshark est déjà chargé sur le PC, accédez au dossier du programme en cliquant sur **Démarrer > Tous les programmes > Wireshark > Wireshark**, puis cliquez sur l'icône de l'application.

Si le programme Wireshark n'est pas installé, procédez comme suit :

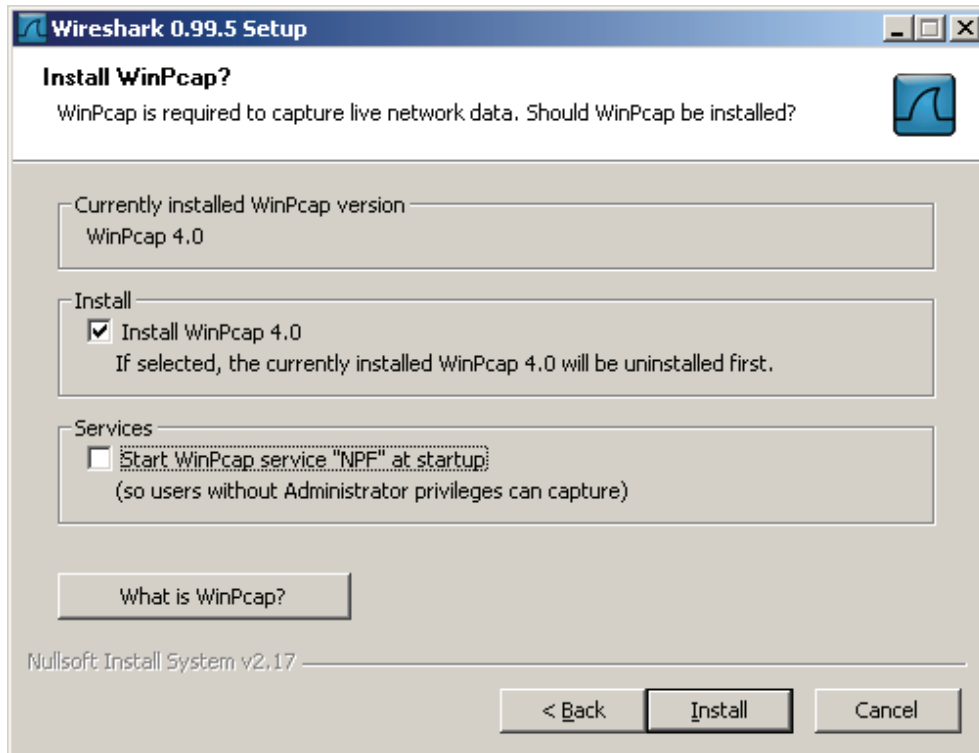
- a. Sur le réseau local, accédez au programme d'installation Wireshark, `wireshark-setup-0.99.5.exe`, et téléchargez-le sur le Bureau de votre PC.
- b. Cliquez deux fois sur le programme d'installation et suivez les instructions qui s'affichent, en acceptant les options par défaut.



- 1) Cliquez sur **I Agree**.



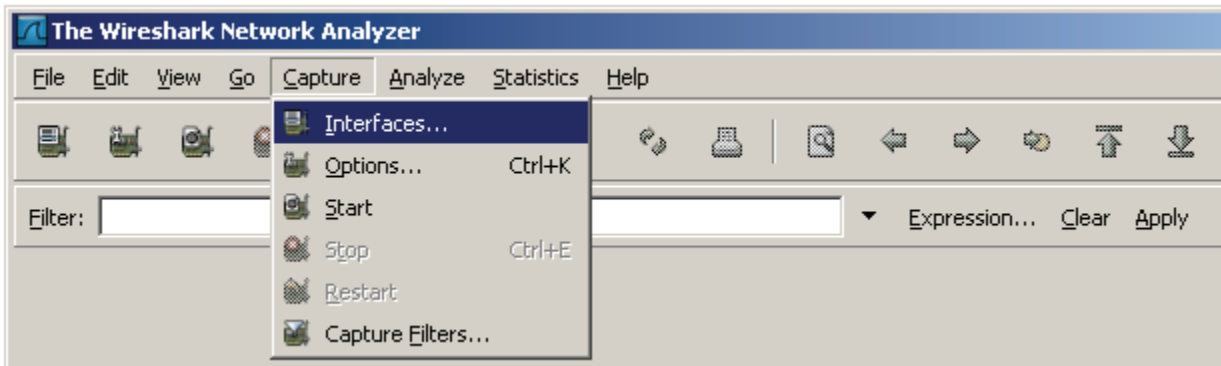
- 2) Assurez-vous d'installer WinPcap sur le PC. WinPcap comprend un pilote qui prend en charge la capture de paquets. Wireshark utilise cette bibliothèque pour capturer les données actives de réseau sous Windows.



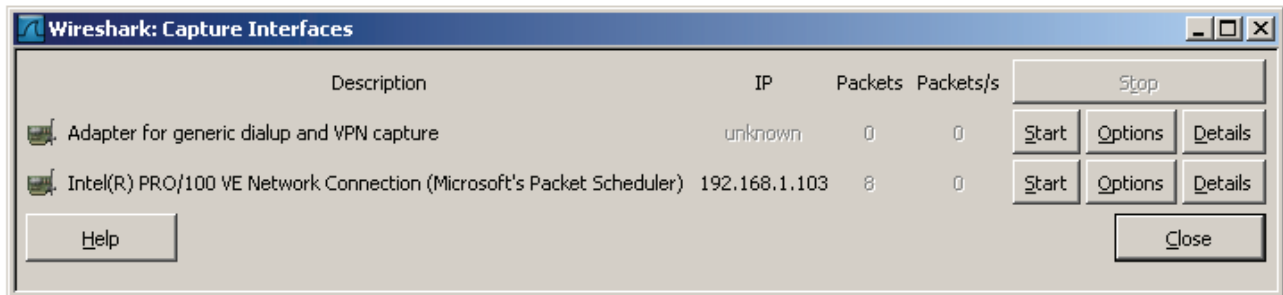
- c. Cliquez sur **Install** et suivez le reste des instructions pour terminer la procédure d'installation.
- d. Une fois le logiciel installé, cochez la case à cocher pour lancer Wireshark.

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

- a. Démarrez l'application Wireshark.
- b. Dans le menu **Capture**, cliquez sur **Interfaces**.

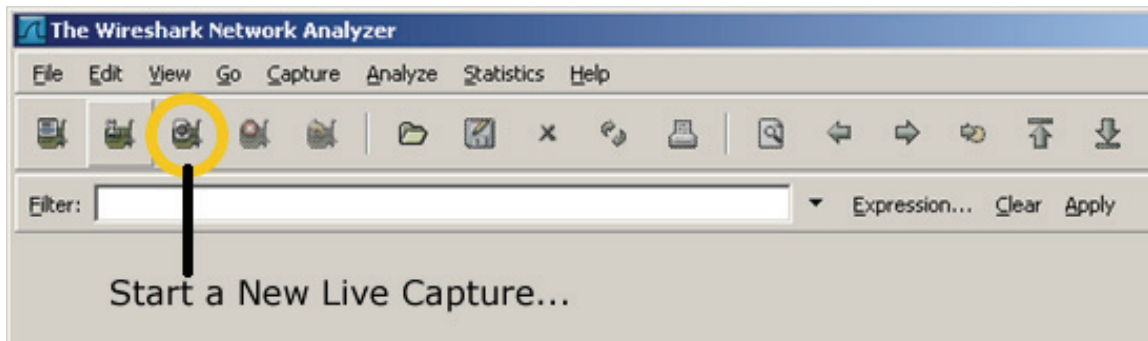


- 3) Cliquez sur le bouton **Start** en regard de l'interface Ethernet (carte réseau) dont vous voulez capturer le trafic réseau.



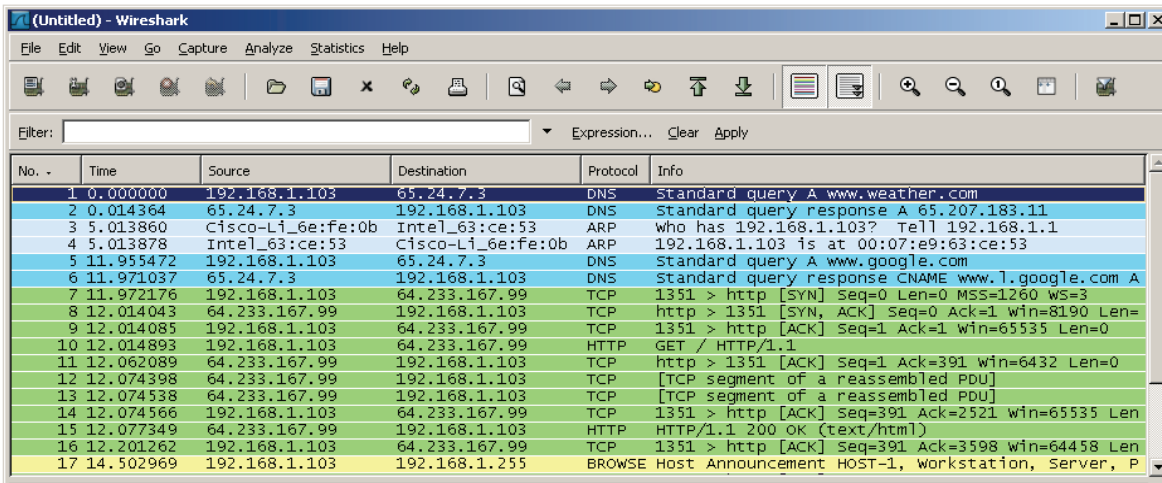
Étape 3 : Démarrage d'une capture de réseau

- a. Faites défiler les menus et affichez la barre d'outils dans l'interface de démarrage Wireshark.
- b. Cliquez sur le bouton **New Live Capture** et observez les informations collectées par Wireshark. Laissez la capture se poursuivre pendant quelques minutes afin d'observer les différents types de trafics sur le réseau.



Étape 4 : Analyse des informations de trafic Web (optionnel)

- Si vous disposez d'une connexion Internet, ouvrez un navigateur et accédez au site 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. Dans la fenêtre Wireshark, localisez les colonnes **Source**, **Destination** et **Protocol**.



No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-Li_6e:fe:0b	Intel_63:ce:53	ARP	who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-Li_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.1.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 win=8190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 win=65535 Len
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 win=64458 Len
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, Workstation, Server, P

- La connexion au serveur Google commence par une requête au serveur de noms de domaine (DNS) pour rechercher l'adresse IP de serveur. L'adresse IP du serveur de destination commence très probablement par 65.x.x.x. Quelles sont la source et la destination du premier paquet envoyé au serveur Google ?

- Ouvrez une autre fenêtre de navigateur et accédez à la base de données **ARIN Whois** à l'adresse <http://www.arin.net/whois/> ou utilisez un autre outil de recherche **whois** et entrez l'adresse IP du serveur de destination. À quelle organisation cette adresse IP est-elle attribuée ?

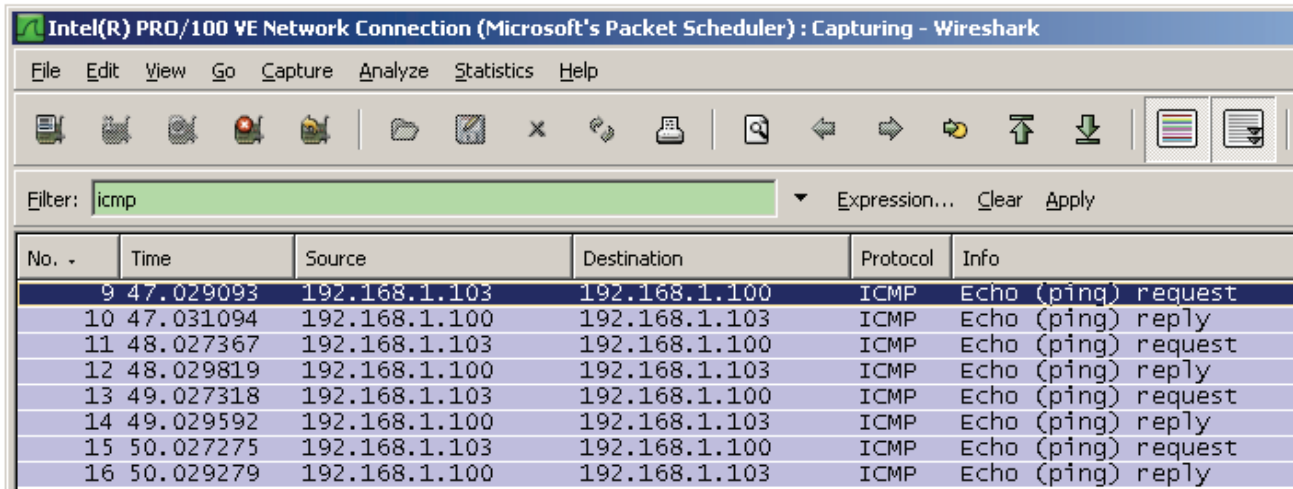
- Quels sont les protocoles utilisés pour établir la connexion au serveur Web et livrer la page Web sur votre hôte local ? _____

- Quelle est la couleur utilisée pour mettre en surbrillance le trafic entre votre hôte et le serveur Web Google ?

Étape 5 : Filtrage d'une capture de réseau

- Ouvrez une fenêtre d'invite de commandes en cliquant sur **Démarrer > Tous les programmes > Exécuter** et en tapant **cmd**. Vous pouvez également cliquer sur **Démarrer > Tous les programmes > Accessoires** et sélectionner **Invite de commandes**.
- Envoyez une requête ping à une adresse IP d'hôte sur votre réseau local et observez la fenêtre de capture Wireshark. Faites défiler, vers le haut et vers le bas, la fenêtre dans laquelle s'affiche le trafic. Quels sont les types de protocoles utilisés ?

- c. Dans la zone de texte **Filter**, tapez **icmp** et cliquez sur **Apply**. ICMP (Internet Control Message Protocol) est le protocole utilisé par la requête **ping** pour tester la connectivité du réseau à un autre hôte.



- d. Lorsque vous tapez **icmp** dans la zone de texte **Filter**, quel type de trafic s'affiche ?

- e. Cliquez sur le bouton **Filter: Expression** dans la fenêtre Wireshark. Faites défiler la liste vers le bas et affichez les possibilités de filtrage. Les protocoles TCP, HTTP, ARP et d'autres sont-ils répertoriés dans la liste ? _____

Étape 6 : Remarques générales

- a. Des centaines de filtres sont répertoriés dans l'option Filter: Expression. Dans le cas d'un vaste réseau, le volume du trafic peut être énorme et les types de trafics nombreux et variés. Dans cette longue 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.

