Guide d'installation et de prise en main de Wireshark (Windows)

Ce guide explique comment installer Wireshark sur Windows, puis comment capturer et analyser du trafic réseau avec quelques exemples concrets (filtres, export, bonnes pratiques).

1. Prérequis et recommandations

- **Droits administrateur** : l'installation (et parfois la capture) nécessite des droits admin.
- **Windows 10/11** (ou Windows Server) à jour.
- **Accès Internet** pour télécharger l'installeur.
- **Contexte d'utilisation** : sur un poste d'entreprise, vérifiez les règles internes (sécurité, confidentialité, autorisations).

2. Installation de Wireshark sur Windows

2.1 Télécharger l'installeur

1. Ouvrez le site officiel de Wireshark.
2. Allez dans la section *Download* puis choisissez **Windows Installer (64-bit)** (dans la majorité des cas).
3. Téléchargez le fichier *.exe* et enregistrez-le dans un dossier connu (ex. Téléchargements).

2.2 Lancer l'installation

1. Double-cliquez sur l'installeur Wireshark (ou clic droit > *Exécuter en tant qu'administrateur*).
2. Acceptez la licence.
3. Conservez les composants par défaut (Wireshark + outils associés) sauf besoin spécifique.
4. Quand l'assistant le propose, installez **Npcap** : c'est le pilote qui permet de capturer le trafic réseau sur Windows (indispensable pour l'usage standard).
5. Terminez l'installation puis lancez Wireshark.

2.3 Vérifier que tout fonctionne

1. Ouvrez Wireshark.
2. Sur l'écran d'accueil, repérez les interfaces réseau (Wi-Fi, Ethernet…).
3. Double-cliquez sur l'interface active : la capture démarre et les paquets défilent.
4. Arrêtez la capture avec le bouton **Stop**.
5. Enregistrez le fichier au format **.pcapng** (format courant pour partager/analyser plus tard).

3. Prise en main (les bases)

Wireshark affiche généralement 3 zones : (1) la **liste des paquets** (une ligne par paquet), (2) les **détails** du paquet (couches Ethernet/IP/TCP/HTTP, etc.), et (3) les **octets bruts** (vue hexadécimale).

3.1 Choisir la bonne interface

- Si vous êtes en Wi-Fi, choisissez l'interface **Wi-Fi** ; en câble, **Ethernet**.
- Un graphique/indicateur d'activité aide à repérer l'interface qui "bouge".
- Si vous analysez uniquement le trafic de votre machine, vous verrez surtout des échanges entre votre IP et des serveurs (DNS, web, etc.).

3.2 Comprendre les filtres (essentiel)

Filtre de capture : s'applique *avant* la capture (réduit ce qui est enregistré). **Filtre d'affichage** : s'applique *après* la capture (réduit ce que vous voyez). Pour débuter, utilisez surtout les **filtres d'affichage**.

- **http** : affiche le trafic HTTP (si présent).
- **dns** : affiche les requêtes/réponses DNS.
- **tcp** / **udp** : affiche uniquement TCP ou UDP.
- **ip.addr == 192.168.1.10** : affiche les paquets impliquant cette adresse IP.
- **tcp.port == 443** : trafic TCP sur le port 443 (souvent HTTPS).
- **tcp.flags.reset == 1** : repère des connexions réinitialisées (RST).

4. Exemples d'utilisation (pas à pas)

Exemple 1 : vérifier une résolution DNS

1. Démarrez une capture sur l'interface active.
2. Dans Windows, ouvrez **Invite de commandes** et lancez une résolution, par exemple : *nslookup example.com*.

3. Revenez dans Wireshark et appliquez le filtre d'affichage : **dns**.
4. Cliquez sur une requête DNS puis, dans les détails du paquet, développez **Domain Name System** pour voir : le nom demandé, le type (A/AAAA), et la réponse (adresse IP).

Exemple 2 : identifier à qui votre PC se connecte

1. Démarrez une capture.
2. Ouvrez votre navigateur et allez sur un site (ex. un portail interne ou un site public).
3. Dans Wireshark, vous pouvez filtrer par port : **tcp.port == 443** (souvent HTTPS) ou **tcp.port == 80** (HTTP).
4. Pour obtenir une vue "qui parle à qui", utilisez le menu **Statistiques** > **Conversations** ou **Endpoints** afin de lister les IP/ports les plus actifs.

Exemple 3 : "Suivre" un échange et enregistrer une preuve

1. Appliquez un filtre pour réduire la vue (par ex. **ip.addr == 192.168.1.10** ou **tcp**).
2. Cliquez sur un paquet intéressant d'une connexion TCP.
3. Clic droit > **Follow** > **TCP Stream** pour reconstituer l'échange (utile en HTTP non chiffré, ou pour voir des bannières/protocoles en clair).
4. Pour partager l'analyse, enregistrez la capture : **Fichier** > **Enregistrer sous** (format .pcapng).
5. Optionnel : exportez seulement une partie : **Fichier** > **Exporter les paquets spécifiés** (par exemple "paquets affichés").

5. Bonnes pratiques, confidentialité et dépannage

- **Confidentialité** : une capture peut contenir des données sensibles (noms d'hôtes, IP, requêtes, parfois des contenus en clair). Partagez-la uniquement avec les personnes autorisées.
- **HTTPS** : le contenu applicatif est chiffré ; vous verrez surtout les IP, ports, SNI/Certificats, volumes, timings (sauf configuration spécifique de déchiffrement).
- **Captures courtes** : commencez par 30–60 secondes et notez l'heure de vos tests (plus simple à retrouver).
- **Nommer vos fichiers** : incluez date, machine, scénario (ex. 2026-03-31_test_dns.pcapng).
- **Si aucune interface n'apparaît** : relancez Wireshark en admin et vérifiez que **Npcap** est bien installé.

- **Si vous ne voyez pas le trafic attendu** : vérifiez que vous capturez sur la bonne interface (Wi-Fi vs Ethernet) et que vous générez réellement du trafic (ouvrir une page, ping, nslookup).

Mémo : filtres utiles (affichage)

- **dns**
- **http**
- **tcp** / **udp**
- **ip.addr == x.x.x.x**
- **tcp.port == 80** / **tcp.port == 443**
- **tcp.analysis.retransmission** (retransmissions)