PortailSIO

NOUVELLE FORMULE

TUTORIEL

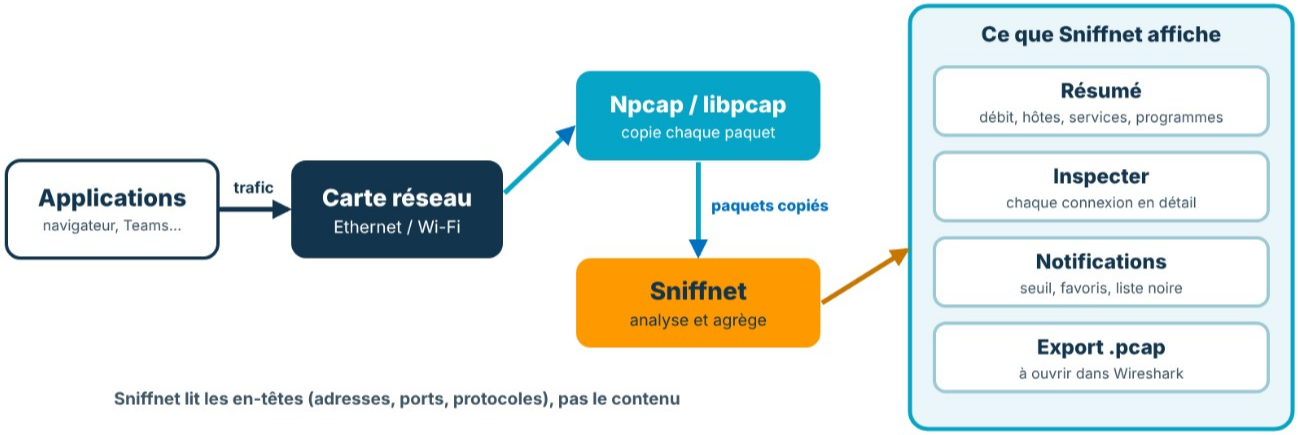
WINDOWS · DEBIAN · SNIFFNET 1.5

Analyser le trafic réseau avec SNIFFNET



NIVEAU
Débutant

Qui parle avec qui ? Un poste, une carte réseau, un tableau de bord



1. Comprendre l'écoute du trafic et préparer le poste
2. Installer Sniffnet (Windows et Debian)
3. Lancer une première capture
4. Lire le Résumé : hôtes, services, programmes
5. Inspecter les connexions une à une
6. Alerter, exporter et dépanner

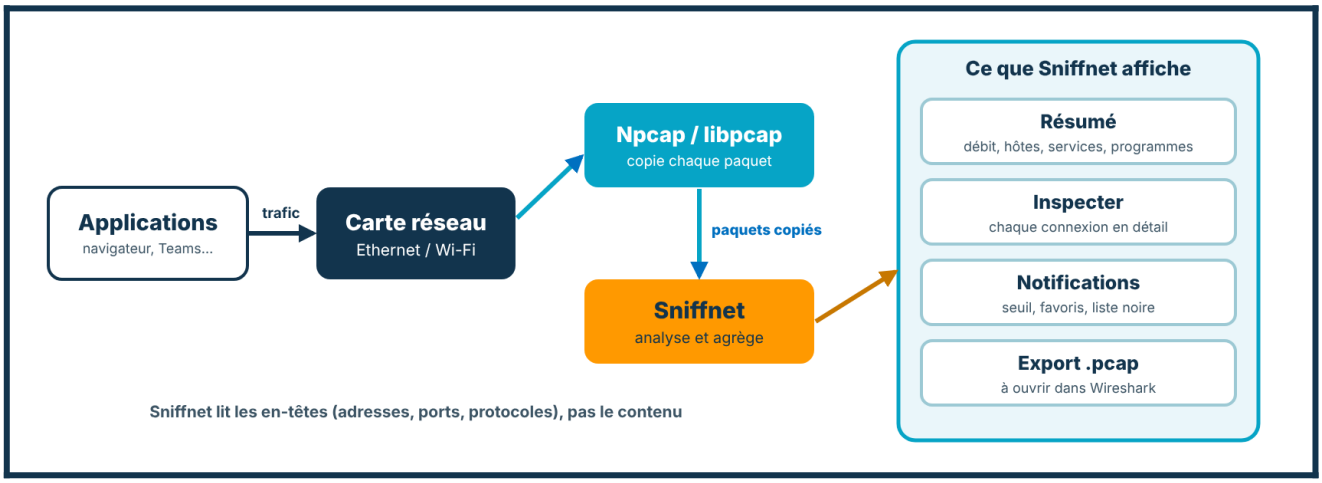
CC BY-NC
Utilisation commerciale interdite
© PortailSIO – 11/2026

Ce tutoriel en ligne
Scannez le QR code. Tous les tutoriels :
portail.sio-ndlp.fr/tutoriels.php

Ce tutoriel peut être réalisé sur un **poste Windows 11** (ou Windows 10) et/ou sur un **poste Debian 13 avec environnement de bureau**, physique ou machine virtuelle (hyperviseur © Proxmox VE, © VirtualBox ou © VMware Player). Aucun serveur n'est nécessaire : Sniffnet s'installe sur le poste dont on veut observer le trafic. Il faut simplement disposer d'un **compte administrateur** (Windows) ou autorisé à utiliser `sudo` (Debian), et d'un accès à Internet.

Sniffnet est un logiciel libre (licences MIT et Apache 2.0), écrit en Rust, qui **observe le trafic de la carte réseau** d'un poste et le présente dans une interface graphique claire : débit en direct, **machines contactées** (pays, nom de domaine, opérateur), **services** utilisés, **programmes** à l'origine du trafic, et **alertes**. La version **1.5.1** (juillet 2026) est utilisée ici ; Sniffnet fonctionne sous Windows, Linux et macOS.

Sniffnet répond à une question simple : **« qui parle avec qui, avec quel protocole, et combien ? »**. C'est un excellent premier outil pour **comprendre ce que fait un poste sur le réseau** avant de passer à un analyseur de paquets complet comme © Wireshark :



À quoi sert Sniffnet ?

- **Comprendre** ce qu'un poste envoie et reçoit réellement (mises à jour, télémétrie, navigateur, messagerie…)
- **Repérer** un comportement inhabituel : un programme inconnu qui émet beaucoup de données, une connexion vers un pays inattendu
- **Illustrer un cours** : DNS, TCP et UDP, ports et services, adresses IP et systèmes autonomes, filtres de capture
- **Garder une trace** : l'export au format `.pcap` se rouvre ensuite dans Wireshark pour une analyse paquet par paquet

Sniffnet ou Wireshark ?

	Sniffnet	Wireshark
Objectif	Vue d'ensemble : qui communique, combien, avec quel programme	Analyse fine : chaque paquet, chaque champ de chaque protocole
Prise en main	Immédiate (aucun filtre à écrire)	Demande de la pratique (filtres d'affichage, colonnes, décodeurs)
Contenu des échanges	Non affiché (en-têtes seulement)	Affiché (si le trafic n'est pas chiffré)
Alertes	Oui : seuil de débit, favoris, liste noire	Non
Quand l'utiliser	Premier regard, démonstration, surveillance ponctuelle	Diagnostic précis, étude d'un protocole, preuve

Dans le cadre de ce tutoriel, nous utilisons les machines suivantes (VLAN SERVEURS et postes, réseau 192.168.20.0 /24) :

Machine	Rôle	Système	Adresse IP
PC-ELEVE	Poste d'analyse (Sniffnet)	Windows 11	192.168.20.34
pc-sio	Poste d'analyse (Sniffnet), variante Debian	Debian 13 + bureau	192.168.20.35
SRV-DC1	Serveur DNS du domaine (interrogé par les postes)	Windows Server 2025	192.168.20.250

Les adresses, noms de machines et noms de fichiers sont des **exemples** à adapter à votre environnement. Les captures d'écran sont des schémas fidèles à l'organisation de Sniffnet 1.5 ; l'aspect exact dépend du thème choisi et du système.

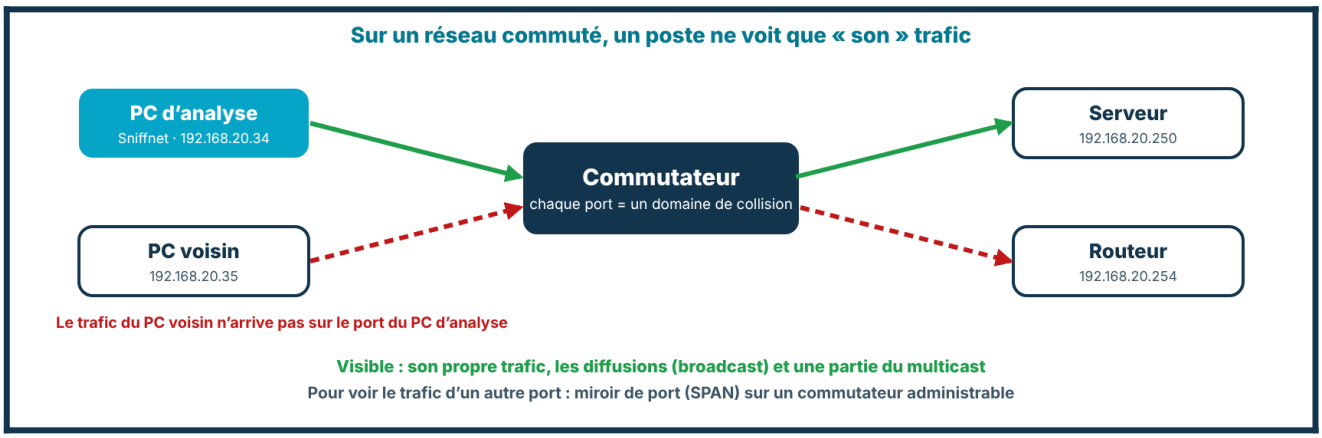
ÉTAPE 1 SUR 6

01 Comprendre l'écoute du trafic et préparer le poste

Écouter le trafic, c'est demander à la **carte réseau** de copier chaque paquet qui passe, puis de le transmettre à un programme d'analyse. Sous Windows, cette copie est assurée par le pilote **Npcap** ; sous Linux et macOS, par la bibliothèque **libpcap**. Sniffnet s'appuie sur ces briques : il **lit les en-têtes** des paquets (adresses IP, ports, protocole) et agrège le tout par connexion.

Ce que Sniffnet voit… et ne voit pas

Sur un réseau **commuté** (le cas de tous les réseaux Ethernet actuels), le commutateur n'envoie à chaque port que le trafic qui le concerne :



- **Visible** : tout le trafic **émis et reçu par le poste** où Sniffnet est installé, plus les diffusions (broadcast) et une partie du multicast
- **Invisible** : le trafic des **autres postes** (sauf si le commutateur copie leur port vers le vôtre : « miroir de port » ou SPAN, réservé aux commutateurs administrables)
- **Illisible** : le contenu des échanges **chiffrés** (HTTPS, SSH, VPN). Sniffnet n'affiche d'ailleurs jamais le contenu, seulement qui parle avec qui

Cadre légal et bonnes pratiques

REMARQUE IMPORTANTE

N'analysez que votre propre poste, ou un réseau pour lequel vous avez une autorisation écrite. L'interception de correspondances échangées par voie électronique est une infraction pénale (article 226-15 du Code pénal), et la charte informatique de l'établissement interdit en général l'installation d'outils d'écoute sur un poste ou un réseau partagé. Pour un TP, demandez l'accord de l'administrateur du réseau et travaillez de préférence sur des machines virtuelles du laboratoire.

Préparer le poste

Avant d'installer quoi que ce soit, relevez le nom et l'adresse IP de la carte à observer : ce sont eux qui permettront de **reconnaître la bonne carte** dans Sniffnet (étape 3). Ouvrez une session avec un compte administrateur puis :

1. **Windows** – ouvrez PowerShell (clic droit sur le menu Démarrer › Terminal) et affichez la configuration IP :

POWERSHELL

```
Get-NetIPConfiguration | Select-Object InterfaceAlias,
@{n='IPv4';e={$_.IPv4Address.IPAddress}}
```

2. **Debian** – ouvrez un terminal et affichez les cartes et leurs adresses :

TERMINAL

```
ip -br address
```

3. Vérifiez que le poste **atteint Internet et le DNS** (ces échanges serviront de trafic de test) :

TERMINAL

```
ping -n 2 portail.sio-ndlp.fr      # Windows
ping -c 2 portail.sio-ndlp.fr      # Debian
```

✔ **POINT DE CONTRÔLE**

- Vous savez dire quelle carte (nom et adresse IP) porte le trafic du poste
- `ping portail.sio-ndlp.fr` répond : le DNS et Internet fonctionnent
- Vous disposez d'un compte administrateur (Windows) ou de `sudo` (Debian)
- Vous avez l'autorisation d'observer le trafic de ce poste

ÉTAPE 2 SUR 6

02 Installer Sniffnet (Windows et Debian)

Sniffnet se présente sous forme d'**installateurs** pour chaque système. Windows demande en plus **Npcap**, le pilote de capture. Choisissez la partie qui correspond à votre poste (les deux sont indépendantes).

A – Windows : Npcap, puis Sniffnet

1. Téléchargez la dernière version de Sniffnet depuis la page des versions du projet : `https://github.com/GyulyVGC/sniffnet/releases/latest`. Pour un PC Intel ou AMD 64 bits, prenez le fichier `Sniffnet_Windows_x64.msi` :

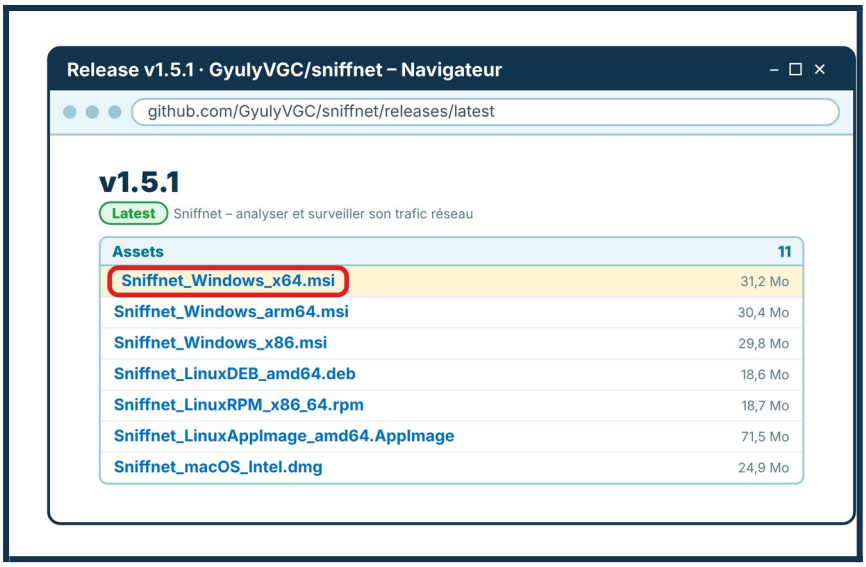


Figure 1 – Page des versions de Sniffnet : fichiers à télécharger

À SAVOIR

Les autres fichiers correspondent à d'autres systèmes : `arm64` pour un PC Windows sur ARM, `.deb` et `.rpm` pour Debian/Ubuntu et Fedora, `.AppImage` pour toute distribution Linux, `.dmg` pour macOS.

REMARQUE IMPORTANTE

Si le navigateur signale un fichier « peu téléchargé » ou si SmartScreen affiche « Windows a protégé votre ordinateur », vérifiez que l'adresse est bien celle du projet **GyulyVGC/sniffnet** sur github.com, puis choisissez **Conserver** (Keep anyway), ou **Informations complémentaires › Exécuter quand même**.

2 Téléchargez et installez **Npcap** depuis `https://npcap.com` (fichier « Npcap installer »). **Sans Npcap, Sniffnet ne peut pas capturer** sous Windows. Dans l'assistant, acceptez la licence, puis, sur la page des options, **cochez « Install Npcap in WinPcap API-compatible Mode »** et laissez les deux autres cases décochées :

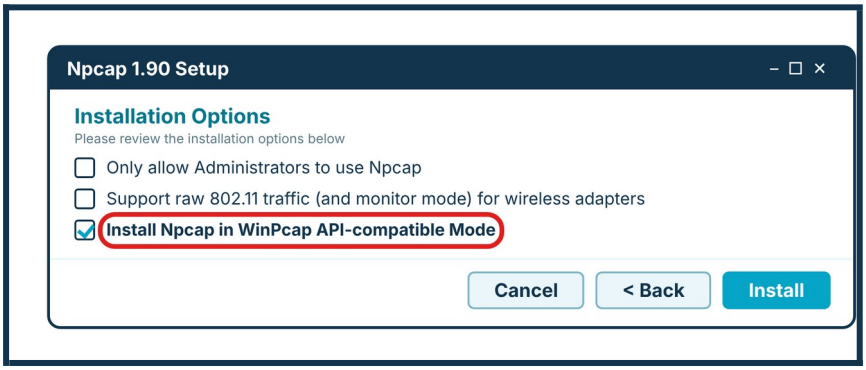


Figure 2 – Options de l'installateur de Npcap

À SAVOIR

Case « Only allow Administrators » cochée : seuls les administrateurs pourront capturer. Décochée, un utilisateur normal peut lancer Sniffnet. Attention à la licence : la version gratuite de Npcap est limitée à **5 postes** (hors usage avec Nmap ou Wireshark) d'après npcap.com ; pour une salle entière, vérifiez la licence.

3 Double-cliquez sur `Sniffnet_Windows_x64.msi` et suivez l'assistant (acceptation de la licence, **Install**, validation de la demande de droits administrateur). À la fin, l'assistant peut proposer d'ouvrir le site de Npcap : **décochez** cette option puisque Npcap est déjà installé

4 Lancez **Sniffnet** depuis le menu Démarrer. Avec Npcap installé comme ci-dessus, il n'est pas nécessaire de l'exécuter « en tant qu'administrateur »

B – Debian 13 : paquet .deb

1 Téléchargez le paquet pour l'architecture **amd64** (navigateur, ou `wget`), puis installez-le **avec** `apt` qui ajoute automatiquement les dépendances (dont `libpcap`) :

TERMINAL

```
cd ~/Téléchargements
wget
https://github.com/GyulyVGC/sniffnet/releases/latest/download/Sniffnet_LinuxDEB_amd64.deb
sudo apt install ./Sniffnet_LinuxDEB_amd64.deb
```

2 Sans droits particuliers, un utilisateur normal ne peut pas ouvrir une capture. Donnez à l'**exécutable** (et à lui seul) les deux « capabilities » nécessaires. Le chemin se lit avec `dpkg -L` ; adaptez la commande s'il diffère :

TERMINAL

```
dpkg -L sniffnet | grep /bin/
sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/sniffnet
getcap /usr/bin/sniffnet
```



Figure 3 – Installation du paquet et droits de capture

À SAVOIR

`cap_net_raw` autorise l'ouverture d'une capture brute, `cap_net_admin` les réglages de la carte. Ces droits sont attachés au fichier : **ils sont perdus à chaque mise à jour du paquet**, il faut alors relancer la commande `setcap`.

REMARQUE IMPORTANTE

`setcap` donne ces droits à **tous les utilisateurs** du poste. Sur un poste partagé, on peut préférer ne rien configurer et lancer Sniffnet à la demande avec `sudo -E sniffnet` (l'option `-E` conserve votre environnement graphique). C'est aussi la méthode à utiliser avec le fichier **AppImage**.

3 Lancez Sniffnet depuis le menu des applications (catégorie Réseau) ou en tapant `sniffnet` dans un terminal

À SAVOIR

Sous **macOS** (fichier `.dmg`), Sniffnet demande des droits d'administrateur au lancement. Sous **Fedora** et dérivés, utilisez le fichier `.rpm`. Pour construire Sniffnet depuis les sources (Rust), consultez le dépôt GitHub : ce n'est pas nécessaire ici.

✔ **POINT DE CONTRÔLE**

- Sous Windows, **Npcap** et **Sniffnet** apparaissent dans « Applications installées »
- Sous Debian, `getcap /usr/bin/sniffnet` affiche `cap_net_admin,cap_net_raw=eip` (ou vous utiliserez `sudo -E sniffnet`)
- Sniffnet s'ouvre sur sa page d'accueil sans message d'erreur

03 ÉTAPE 3 SUR 6 Lancer une première capture

La page d'accueil de Sniffnet sert à **régler la capture avant de la lancer** : quelle source observer, avec quel filtre, et faut-il en garder une copie dans un fichier. Les réglages sont tous facultatifs sauf un : le choix de la carte réseau.

A – Choisir la carte réseau

1 Dans le panneau de gauche, laissez la source sur **Carte réseau**. Sniffnet liste vos cartes, **classées par trafic récent**, chacune avec un mini-graphique des 30 dernières secondes. Cliquez sur celle qui porte votre trafic (ici **Ethernet**, 192.168.20.34) :



Figure 4 – Page d'accueil : choix de la carte réseau

À SAVOIR

La bonne carte est celle dont la courbe **bouge quand vous naviguez**. Ignorez les cartes virtuelles (WSL, Hyper-V, Docker, VPN) tant que vous n'observez pas leur trafic. L'autre source, **Fichier de capture**, sert à relire un fichier `.pcap` existant.

B – Filtrer et exporter (facultatif)

Deux cases à droite adaptent la capture. Les **filtres** sont écrits en **BPF** (Berkeley Packet Filter), la syntaxe commune à `tcpdump` et à Wireshark pour les filtres de capture :

Filtre BPF	Ce qui est capturé
`port 443`	Tout le trafic sur le port 443 (HTTPS, TCP et UDP)
`tcp port 443 or udp port 53`	HTTPS en TCP **ou** DNS en UDP
`host 192.168.20.250`	Tout ce qui est échangé avec le serveur 192.168.20.250
`net 192.168.20.0/24`	Tout ce qui concerne le sous-réseau 192.168.20.0 /24
`not port 22`	Tout sauf le trafic SSH
`icmp`	Les messages ICMP (ping, erreurs de routage)

1. Cochez **Filtrer le traffic** et saisissez un filtre BPF, par exemple `tcp port 443 or udp port 53`
2. Cochez **Exporter le fichier de capture** si vous voulez conserver les paquets. Indiquez le **nom du fichier** (`sniffnet.pcap` par défaut) et le **répertoire** (par défaut votre dossier personnel) :



Figure 5 – Filtre BPF et export du fichier de capture

À SAVOIR

Le fichier `.pcap` contient les paquets capturés : **il grossit autant que le trafic**. Ne laissez pas l'export activé pendant des heures. Un filtre BPF trop strict est la première cause d'écran vide : au premier essai, ne filtrez rien.

REMARQUE IMPORTANTE

Un filtre BPF invalide empêche la capture de démarrer. Au moindre doute, décochez **Filtrer le traffic** : vous pourrez toujours **trier et chercher** ensuite dans les onglets Résumé et Inspecter, sans rien perdre.

3. Cliquez sur **Commencer !** : la page Résumé s'ouvre et les compteurs se mettent à bouger

C – Générer du trafic de test

Sur un poste au repos, il y a peu de trafic. Provoquez-en en alternant **navigation** (ouvrez deux ou trois sites) et **commandes** réseau :

POWERSHELL (WINDOWS)

```
nslookup portail.sio-ndlp.fr
ping -n 4 portail.sio-ndlp.fr
curl.exe -I https://portail.sio-ndlp.fr
```

TERMINAL (DEBIAN)

```
nslookup portail.sio-ndlp.fr
ping -c 4 portail.sio-ndlp.fr
curl -I https://portail.sio-ndlp.fr
```

✔ POINT DE CONTRÔLE

- La carte choisie est celle dont la courbe varie
- Après **Commencer !**, la page **Résumé** s'affiche et le graphique bouge
- Si l'export est coché, le fichier `.pcap` apparaît dans le répertoire choisi
- Vous savez revenir à la page d'accueil (**Ctrl + Retour arrière**) pour changer de carte ou de filtre

04 ÉTAPE 4 SUR 6 Lire le Résumé : hôtes, services, programmes

La page **Résumé** est le tableau de bord de la capture. Elle se lit **de haut en bas** : le volume de trafic en direct, puis, en dessous, trois classements qui répondent à trois questions : **avec qui** (hôtes), **pour quoi faire** (services), **par qui** (programmes).

A – Le graphique et les compteurs

1. Générez un peu de trafic (une page web, une commande `ping`) puis observez le **graphique** du haut : il montre les **30 dernières secondes**, en bleu pour le trafic **entrant** et en orange pour le trafic **sortant**
2. Changez l'unité du graphique avec le sélecteur : **octets**, **bits** ou **paquets** par seconde. Les octets servent à parler de volume, les bits de débit de ligne, les paquets de charge pour le matériel
3. À droite, le panneau d'information rappelle la **carte** observée et les **filtres actifs**, et l'anneau répartit le trafic en **entrant**, **sortant** et **perdus** (paquets abandonnés par le système avant d'avoir pu être analysés)

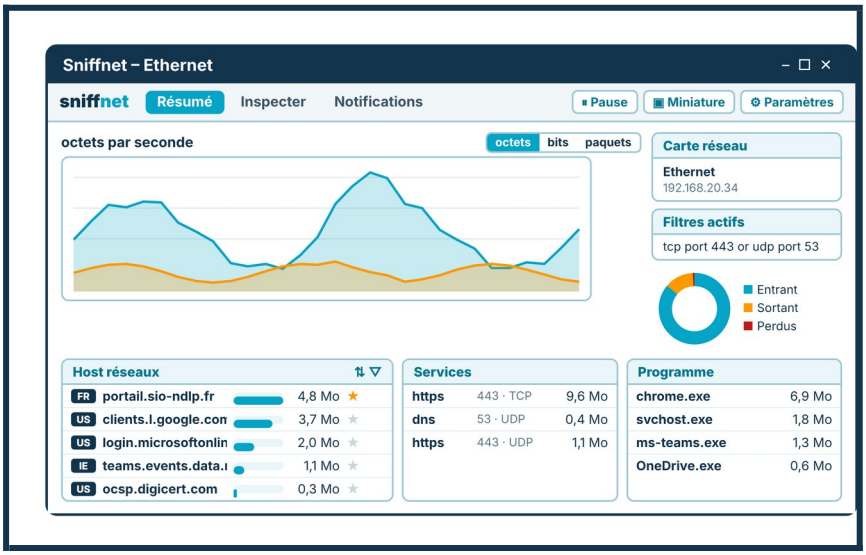


Figure 6 – Page Résumé : débit en direct, répartition et trois classements

À SAVOIR

Un trafic « perdu » non nul signifie que la carte reçoit plus vite que Sniffnet ne peut analyser : appliquez un **filtre BPF** pour réduire le volume observé.

B – Avec qui ? Le panneau Host réseaux

Chaque ligne est une machine distante avec laquelle le poste a échangé des données. Sniffnet affiche pour chacune :

- le **pays** (drapeau), déduit de l'adresse IP grâce à une base de géolocalisation (**GeoLite2**) ;
- le **nom de domaine**, obtenu par **résolution DNS inverse** de l'adresse ;
- l'**opérateur** ou **système autonome** (numéro **ASN** et nom, par exemple AS16276 OVH SAS) ;
- une **barre** et un **total** proportionnels au volume échangé ;
- une **étoile** pour mettre l'hôte en **favori** (le filtre en forme d'entonnoir n'affiche alors que les favoris).

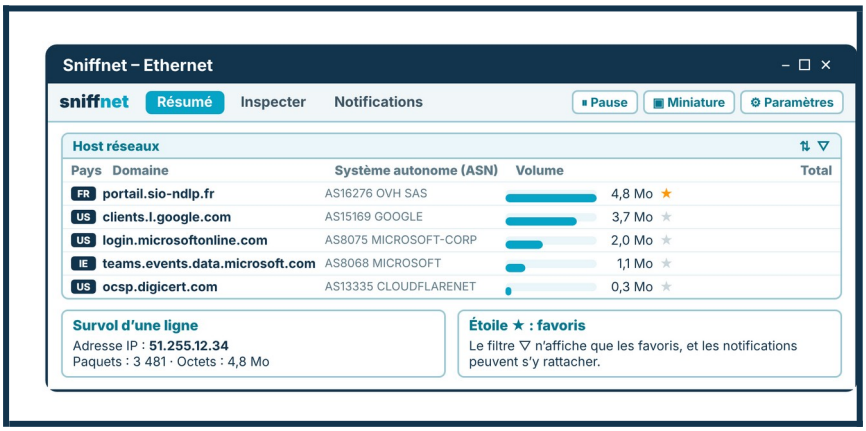


Figure 7 – Le panneau Host réseaux en détail

À SAVOIR

Le nom affiché est celui de la **résolution inverse**, pas forcément celui du site visité : derrière un site se trouvent souvent un CDN ou un cloud. L'ASN, plus stable, dit à **quel opérateur** appartient l'adresse. La géolocalisation est **approximative**.

C – Pour quoi faire, et par qui ? Services et programmes

1. Le panneau **Services** déduit le service (`https`, `dns`, `http`, `ntp`…) du **numéro de port et du protocole** (base de plus de 6 000 services). C'est un **indice, pas une preuve** : rien n'empêche d'utiliser le port 443 pour autre chose que du HTTPS
2. Le panneau **Programme** associe le trafic au **programme** qui l'a généré (nom, icône, et chemin complet au survol de la ligne). C'est le moyen le plus rapide de savoir **quelle application** consomme la bande passante

Mise en pratique : relier une action à ce que Sniffnet affiche

Action	Où regarder	Ce que vous devez trouver
Ouvrir `https://portail.sio-ndlp.fr`	Host réseaux, Services, Programme	Un hôte français (ASN OVH) ; le service `https` ; le navigateur comme programme
`nslookup portail.sio-ndlp.fr`	Services	Du trafic `dns` (port 53) vers 192.168.20.250 ; très peu d'octets
`ping -n 4 portail.sio-ndlp.fr`	Onglet Inspecter (étape 5)	Du trafic ICMP ; pas de port, donc pas de service
Ouvrir un second site	Host réseaux	De nouveaux hôtes apparaissent, avec d'autres ASN (CDN, publicité, statistiques)

✔ **POINT DE CONTRÔLE**

- Vous lisez le graphique et savez changer son unité (octets, bits, paquets)
- Vous identifiez pour un hôte son **pays**, son **domaine** et son **ASN**
- Vous savez dire quel **programme** génère le plus de trafic
- Vous distinguez ce qui est **observé** (ports, volumes) de ce qui est **déduit** (service, domaine, pays)

05 ÉTAPE 5 SUR 6 Inspecter les connexions une à une

Le Résumé agrège, l'onglet **Inspecter** détaille : il affiche **une ligne par connexion**, c'est-à-dire par combinaison d'adresse et port source, adresse et port de destination et protocole. C'est ici que l'on cherche une adresse précise, un port inhabituel ou un volume anormal.

A – Lire et filtrer la liste

1. Cliquez sur l'onglet **Inspecter**. Chaque ligne indique les **adresses et ports** source et destination, le **protocole** (TCP, UDP, ICMP…), le **service** déduit, le volume de **données** et la **date** du dernier paquet. Cliquez sur un en-tête pour **trier**
2. Utilisez les champs de **recherche** au-dessus du tableau : chaque champ s'applique à une colonne. Un **préfixe** change le sens de la recherche :

Saisie	Effet	Exemple
`texte`	La colonne **contient** le texte (recherche partielle)	`192.168.20` : toutes les adresses du sous-réseau
`=texte`	La colonne est **exactement** égale au texte	`=443` : le port 443 uniquement
`!texte`	La colonne **ne contient pas** le texte	`!192.168.` : exclut les adresses privées
`!=texte`	La colonne **n'est pas égale** au texte	`!=192.168.20.250` : masque le serveur DNS

3. Les boutons **Favoris** et **Liste noire** restreignent l'affichage aux connexions concernant vos hôtes favoris ou les adresses de votre liste noire (étape 6)

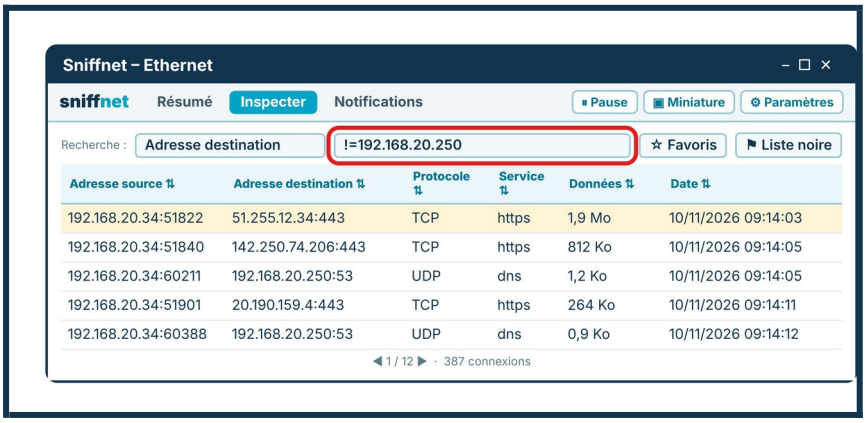


Figure 8 – Onglet Inspecter : une ligne par connexion

À SAVOIR

Ici, la recherche `!=192.168.20.250` sur la colonne « Adresse destination » masque tout le trafic DNS vers le serveur du domaine pour ne garder que le reste. Les valeurs de date et de volume évoluent en direct.

B – Ouvrir le détail d'une connexion

1 **Cliquez sur une ligne** : la fenêtre « **Détails de la connexion** » s'ouvre. Elle ajoute aux informations du tableau l'**horodatage** du premier et du dernier paquet, le **nombre de paquets** et d'octets dans chaque sens, le **domaine** et le **système autonome** de l'hôte distant, le **programme**, et, depuis la version 1.5.1, la **latence** (temps d'aller-retour) :



Figure 9 – Détails d'une connexion

À SAVOIR

Une latence de quelques millisecondes indique un hôte **proche** (même ville ou CDN local), plusieurs centaines un hôte lointain ou une liaison saturée. Fermez la fenêtre avec la touche **Échap**.

C – Interpréter ce que l'on voit

Ce que vous observez	Interprétation probable	Réflexe
Nombreuses connexions TCP vers le port 443 de plusieurs hôtes	Navigation web normale (une page appelle de nombreux serveurs)	Rien à faire
Du trafic `dns` (UDP 53) vers une adresse autre que le DNS du domaine	Un programme contourne le DNS de l'entreprise	Identifier le programme, vérifier la configuration
Gros volume sortant **vers un seul hôte**	Envoi de fichiers (sauvegarde, cloud) ou fuite de données	Identifier le programme et l'hôte (ASN, pays)
Connexions sortantes vers un port rare (4444, 8080, 31337…)	Outil de contrôle à distance ou logiciel peu courant	Rechercher l'exécutable (chemin au survol)
Trafic régulier, à intervalles fixes, vers le même hôte	Mise à jour, télémétrie… ou « balise » d'un logiciel malveillant	Comparer avec les domaines connus de l'éditeur

REMARQUE IMPORTANTE

Sniffnet **ne prouve rien** : il montre des communications, pas leurs intentions. Un hôte étranger n'est pas forcément malveillant (CDN, cloud), et un logiciel malveillant peut utiliser le port 443. Servez-vous de ces indices pour **poser une question**, puis vérifiez (programme, éditeur, signature) avant de conclure.

✔ **POINT DE CONTRÔLE**

- Vous triez et filtrez la liste des connexions avec les préfixes `=`, `!` et `!=`
- Vous ouvrez le **détail** d'une connexion et lisez horodatages, volumes, domaine, ASN et latence
- Vous savez expliquer pourquoi un service ou un pays affiché n'est qu'un indice

06

ÉTAPE 6 SUR 6

Alerter, exporter et dépanner

A – Activer les notifications

Les notifications sont **désactivées par défaut**. Ouvrez ⚙️ **Paramètres › Notifications** (raccourci **Ctrl + ,**) pour choisir ce qui doit déclencher une alerte :

- **Seuil de donnée atteint** : une alerte quand le trafic dépasse une valeur par seconde (en octets, bits ou paquets). Utile pour repérer un envoi massif de données
- **Données d'un favori** : une alerte dès qu'un hôte mis en favori (étoile ★) échange des données
- **Données d'une adresse de la liste noire** : une alerte dès qu'une adresse que vous avez bannie apparaît

1. Choisissez le **son** et le **volume** de la notification (ou coupez le son)



Figure 10 – Paramètres › Notifications

> **À SAVOIR**
>
> Les notifications apparaissent en bas de l'écran et dans l'historique de l'onglet **Notifications**. Le raccourci **Ctrl + D** les efface. Sniffnet peut aussi envoyer des notifications **à distance** (webhook) : voir la documentation du projet.

B – Constituer une liste noire

1. Ouvrez ⚙️ **Paramètres › Général**. Dans la zone « Liste noire », saisissez **une adresse IP ou un bloc CIDR par ligne** (les blocs CIDR sont acceptés depuis la version 1.5.1), ou **importez un fichier** :



Figure 11 – Paramètres : liste noire d'adresses IP

> **À SAVOIR**
>
> Pour **tester** sans danger, ajoutez l'adresse d'un site que vous allez justement ouvrir (relevée avec `nslookup` ou dans l'onglet Inspecter) : l'alerte doit se déclencher à la première connexion.

2. Rouvrez le site de test : la notification apparaît, et la connexion est repérable dans **Inspecter › Liste noire**

À SAVOIR

Sniffnet ne fournit pas de liste de menaces toute faite : **c'est à vous de l'alimenter**. On peut importer des listes publiques d'adresses ou de blocs malveillants (par exemple la liste DROP de Spamhaus ou les listes de botnets d'abuse.ch), à récupérer **depuis la source officielle** et à actualiser régulièrement : une liste ancienne génère des fausses alertes.

C – Exporter la capture et l'ouvrir avec Wireshark

Si l'**export** était coché à l'étape 3, le fichier `.pcap` contient tous les paquets capturés. Il s'ouvre dans **Wireshark** (analyse graphique) ou avec **tshark** (version en ligne de commande, installée avec Wireshark) :

TERMINAL

```
tshark -r tp-sniffnet.pcap -c 5
```

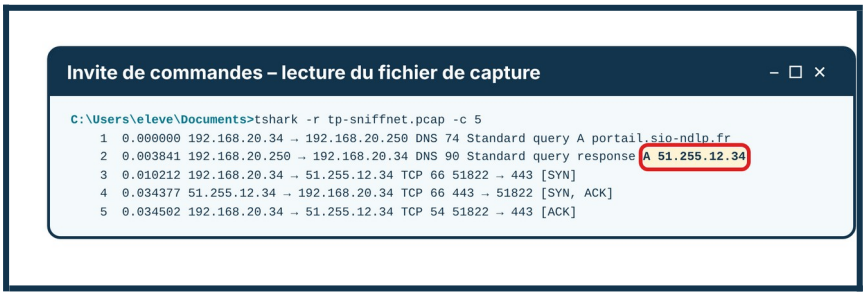


Figure 12 – Lecture du fichier de capture avec tshark

À SAVOIR

On retrouve le **détail que Sniffnet n'affiche pas** : la requête DNS, sa réponse, puis l'ouverture de la connexion TCP (SYN, SYN-ACK, ACK). Le fichier se rouvre aussi dans Sniffnet : à l'accueil, choisissez la source **Fichier de capture**.

REMARQUE IMPORTANTE

Un fichier `.pcap` peut contenir des **données personnelles** (adresses, noms de domaine, parfois des mots de passe de protocoles non chiffrés). Protégez-le, ne le diffusez pas et supprimez-le quand l'analyse est terminée.

D – Raccourcis et mode miniature

Raccourci	Action
Ctrl + Espace	Mettre en **pause** ou reprendre la capture
Ctrl + Retour arrière	Arrêter l'analyse et revenir à la page d'accueil
Ctrl + T	Basculer en **mode miniature** : une petite fenêtre toujours visible avec le graphique
Ctrl + ,	Ouvrir les **paramètres**
Ctrl + D	Effacer les notifications
Échap	Fermer la fenêtre ou le menu ouvert
Ctrl + Q	Quitter Sniffnet
Ctrl + + / Ctrl + -	Agrandir ou réduire l'affichage (⌘ à la place de Ctrl sous macOS)

E – Dépanner

Symptôme	Cause probable	Solution
Windows : Sniffnet ne trouve aucune carte ou refuse de capturer	**Npcap** absent ou installé sans le mode WinPcap	Installer ou réinstaller Npcap en cochant « WinPcap API-compatible Mode »
Windows : erreur « libpcap returned invalid UTF-8 »	Page de codes du système non UTF-8	**Paramètres › Heure et langue › Langue et région › Paramètres de langue administrative › Modifier les paramètres régionaux du système** : cocher « Bêta : Utiliser Unicode UTF-8 », puis redémarrer
Debian : échec au démarrage de la capture, « permission denied »	Droits de capture manquants, ou perdus après une mise à jour du paquet	Relancer la commande `setcap` de l'étape 2, ou utiliser `sudo -E sniffnet`
Affichage déformé ou fenêtre vide	Pilote graphique incompatible avec le rendu par défaut	Lancer avec le rendu logiciel : `ICED_BACKEND=tiny-skia sniffnet` (sous Windows, définir cette variable d'environnement)
Aucun trafic affiché	Mauvaise carte, filtre BPF trop strict, ou trafic de **cartes virtuelles**	Revenir à l'accueil (Ctrl + Retour arrière), choisir la carte dont la courbe bouge, retirer le filtre
Je ne vois pas le trafic des autres postes	Réseau **commuté** : le commutateur ne vous envoie pas ce trafic	Observer le poste lui-même, ou configurer un **miroir de port** (SPAN) vers le poste d'analyse
Je ne vois pas le contenu des pages	Normal : Sniffnet n'affiche que les en-têtes, et HTTPS est chiffré	Exporter en `.pcap` pour une analyse approfondie dans Wireshark

Pour aller plus loin

Sniffnet est un outil d'**observation ponctuelle sur un poste**. Pour **surveiller en continu** la disponibilité de serveurs et de services et être prévenu en cas de panne, installez plutôt un outil de supervision : voir le tutoriel « **Installer Uptime Kuma avec Docker Compose** » (sondes HTTP, ping, TCP, DNS, alertes et page de statut) ou « **Installer Zabbix** » (mesures détaillées et seuils). Pour une **analyse paquet par paquet**, poursuivez avec Wireshark et ses filtres d'affichage.

✔ POINT DE CONTRÔLE

- Les **notifications** sont activées et une alerte de test s'est déclenchée
- La **liste noire** contient au moins une adresse et une connexion vers elle est repérable dans **Inspecter**
- Vous avez relu un fichier **.pcap** avec tshark ou Wireshark
- Vous savez dépanner les trois causes courantes : Npcap absent, droits Linux, filtre trop strict