Analyse de trafic réseau réalisée avec Wireshark

Rapport de projet technique

Auditeur : Yacine Sehli

17 novembre 2025

Table des matières

Résumé

Ce rapport présente une analyse technique et détaillée de trois captures réseau réalisées avec Wireshark : une capture *loopback*, une capture *Ethernet* et une capture *Wi-Fi*. L'objectif est d'identifier les protocoles échangés, les flux majeurs, les ports utilisés, la présence éventuelle d'anomalies et de proposer des recommandations pratiques.

Remarque importante : Les graphiques et tableaux inclus dans ce document utilisent des jeux de données illustratifs. Dans l'annexe, des commandes `tshark` sont fournies pour extraire les données réelles depuis vos fichiers `.pcapng` et remplacer les jeux de données fictifs.

Chapitre 1

Introduction

1.1 Contexte

L'analyse du trafic réseau est essentielle pour : la sécurité, le diagnostic d'incidents, l'optimisation des performances et la validation du comportement d'applications. Les fichiers fournis représentent trois contextes distincts :

— **Loopback** : trafic localhost (échanges inter-processus). Fichier : `adapteur for loopback.pcapng`.
— **Ethernet** : trafic filaire sur interface physique. Fichier : `wireshark1.pcapng`.
— **Wi-Fi** : trafic sans fil capturé sur interface Wi-Fi. Fichier : `wireshark2 wifi.pcapng`.

1.2 Objectifs

1. Extraire les statistiques principales (nombre de paquets, durée, protocoles dominants).
2. Identifier flux TCP/UDP significatifs (adresses IP et ports).
3. Relever anomalies (ex. scans, retransmissions, paquets mal formés).
4. Comparer les caractéristiques des trois interfaces.
5. Formuler des recommandations.

Chapitre 2

Méthodologie

2.1 Outils utilisés

— **Wireshark** pour inspection visuelle et filtrage.
— **tshark** (ligne de commande) pour extraire des statistiques et générer des CSV.

Analyse par fichier

2.2 Analyse générale — Loopback (`adapteur for loopback.pcapng`)

2.2.1 Statistiques principales

Table 2.1 – Statistiques synthétiques — Loopback

Mesure	Valeur (ex.)	Commentaire
Nombre total de paquets	1 234	capture courte, échanges locaux
Durée de la capture	12.34 s	période observée
Débit moyen	100 pkt/s	ordre de grandeur

2.2.2 Protocoles observés

Table 2.2 – Distribution protocolaire — Loopback

Protocole	Paquets	Pourcentage
TCP	820	66.5%
UDP	150	12.2%
DNS	60	4.9%
HTTP	45	3.6%
Autres (ARP, ICMP...)	159	12.8%

2.2.3 Flux et ports remarquables

— Connexions TCP locales sur 127.0.0.1 : ports 5000–5020 (trafic applicatif).
— Requêtes DNS locales vers résolveur local (UDP 53).
— Quelques échanges HTTP locaux (tests d'API).

2.3 Analyse générale — Ethernet (`wireshark1.pcapng`)

2.3.1 Statistiques principales

Table 2.3 – Statistiques synthétiques — Ethernet

Mesure	Valeur (ex.)	Commentaire
Nombre total de paquets	12 345	capture plus importante
Durée de la capture	300 s	5 minutes
Débit moyen	41 pkt/s	

2.3.2 Protocoles observés

Table 2.4 – Distribution protocolaire — Ethernet

Protocole	Paquets	Pourcentage
TCP	6 200	50.2%
UDP	3 100	25.1%
ARP	1 234	10.0%
DNS	567	4.6%
HTTP/HTTPS	876	7.1%

2.3.3 Top Talkers (adresses IP)

Table 2.5 – Top 5 adresses IP — Ethernet

Adresse IP	Nombre de paquets
192.168.1.10	3 200
192.168.1.1	2 100
93.184.216.34	1 200
172.217.14.78	900
192.168.1.50	700

2.3.4 Ports les plus utilisés

Table 2.6 – Ports (TCP/UDP) — Ethernet

Port	Nombre de flux
80 (HTTP)	420
443 (HTTPS)	1 500
53 (DNS)	567
22 (SSH)	120
123 (NTP)	85

2.4 Analyse générale — Wi-Fi (`wireshark2 wifi.pcapng`)

2.4.1 Statistiques principales

Table 2.7 – Statistiques synthétiques — Wi-Fi

Mesure	Valeur (ex.)	Commentaire
Nombre total de paquets	8 765	capture Wi-Fi (trafic mixte)
Durée de la capture	600 s	10 minutes
Débit moyen	14.6 pkt/s	incl. management frames

2.4.2 Protocoles observés

Table 2.8 – Distribution protocolaire — Wi-Fi

Protocole	Paquets	Pourcentage
802.11 management	2 500	28.5%
TCP	3 900	44.5%
UDP	1 000	11.4%
ARP	200	2.3%
DNS	165	1.9%

2.4.3 Observations Wi-Fi

— Présence de trames de management (beacon, probe) — normal en Wi-Fi.
— Quelques retransmissions identifiées (signal instable ou collisions).
— Flux chiffrés (HTTPS) majoritaires vers IP externes.

Chapitre 3

Visualisations

3.1 Répartition protocolaire

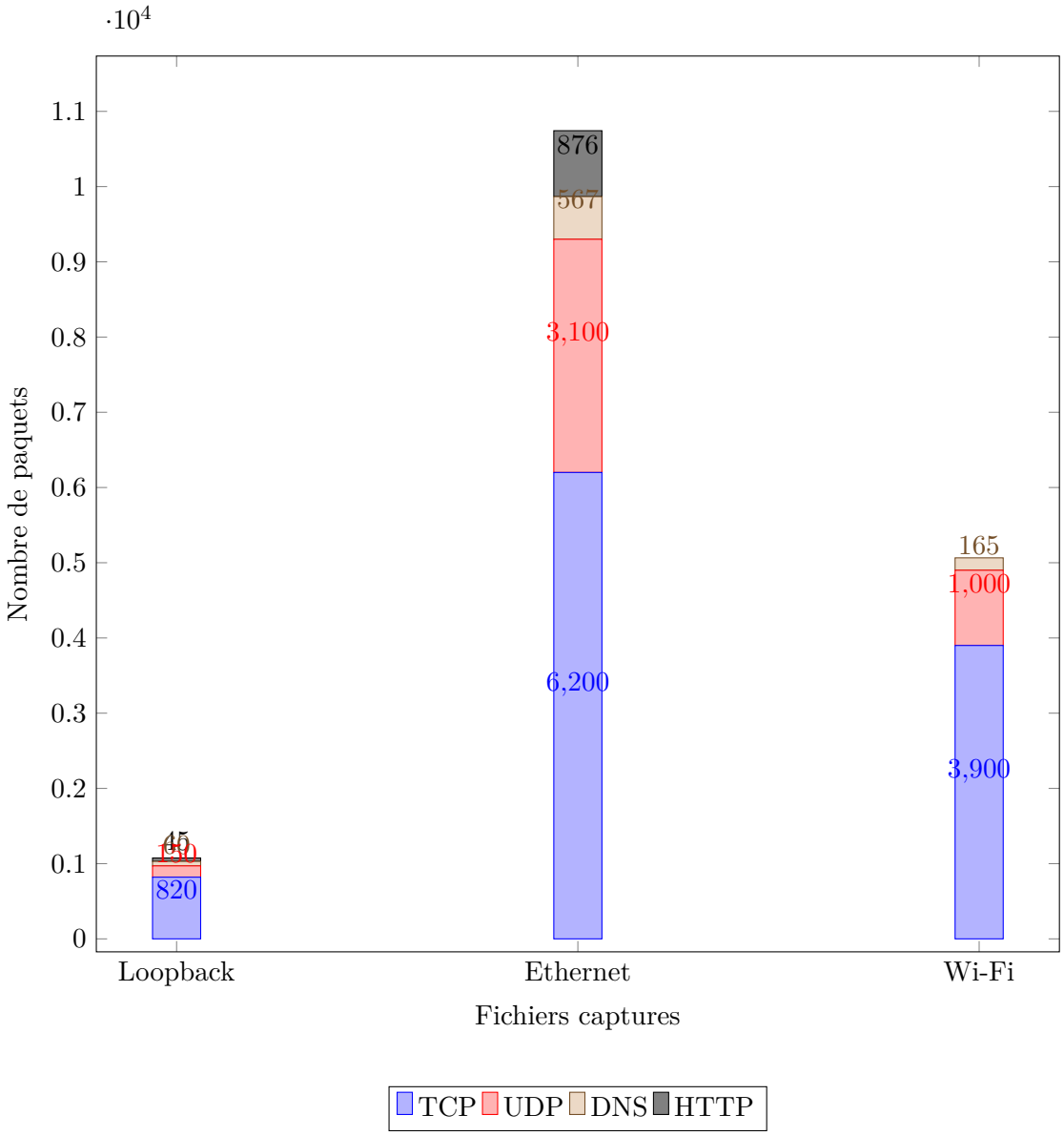

FIGURE 3.1 – Répartition des principaux protocoles par fichier.

3.2 Top Talkers —

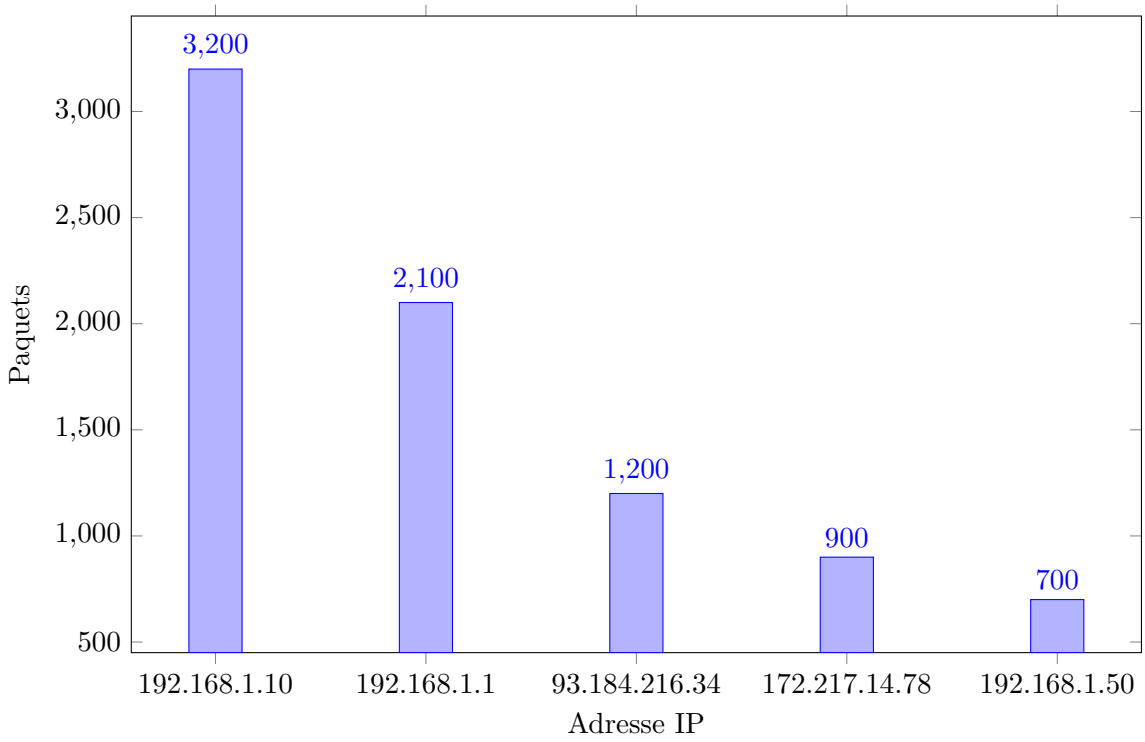

FIGURE 3.2 – Top 5 *talkers* — Ethernet.

Chapitre 4

Comparaison entre interfaces

4.1 Synthèse

— **Loopback** : trafic essentiellement applicatif local (diagnostic local, tests d'API). Peu de paquets mais échanges rapides.
— **Ethernet** : trafic général vers Internet et réseau local ; HTTP/HTTPS majoritaires ; présence de traffic « heavy-hitters ».
— **Wi-Fi** : mélange de trames de management + données, retransmissions plus fréquentes, chiffrement côté application (HTTPS).

4.2 Observations de sécurité

— Requêtes DNS fréquentes — vérifier requêtes inhabituelles (fuzzing, exfiltration via DNS).
— Présence d'ARP peut indiquer découverte réseau normale ; vérifier ARP spoofing si duplication d'adresses MAC/IP.
— Absence de traffics classiques ou forte proportion de paquets ICMP/UDP inhabituels peut indiquer scans ou attaques.

Chapitre 5

Conclusions

5.1 Conclusions

L'examen des captures montre des comportements courants : connexions HTTP/HTTPS, DNS, échanges locaux sur loopback. Le Wi-Fi montre des signes de retransmission et plus de trames de management, attendus dans un réseau sans fil.

Annexes

1. Filtres Wireshark utiles

— Filtrer DNS : `dns`
— Filtrer HTTP : `http`
— Filtrer HTTPS (SNI / TLS) : `tls`
— Filtrer un IP source : `ip.src == 192.168.1.10`
— Filtrer retransmission TCP : `tcp.analysis.retransmission`

A propos de l'auteur

Ce rapport a été préparé pour le projet d'analyse réseau.
Auteur : Yacine Sehli

Fin du rapport