

# Wireshark

## Description

Wireshark est un outil open source de capture et d'analyse de paquets réseau. Cet outil est principalement utilisé pour réaliser des captures de trafic réseau sur les interfaces d'une machine. Ces captures peuvent ensuite être enregistrées dans des fichiers PCAP (extension .pcap) pour analyse.

## Installation

- Sous Linux (Debian/Ubuntu) :

```
sudo apt-get install wireshark
```

- Sous Windows : vous pouvez télécharger l'installateur depuis le site officiel (<https://www.wireshark.org/download.html>) et suivre les instructions d'installation.

## Cas d'utilisation

- **Dépannage réseau** : pour identifier et résoudre les problèmes de réseau tels que les pertes de paquets, les retards et les erreurs de configuration ;
- **Sécurité réseau** : dans le cadre de la détection d'intrusion, de l'analyse de logiciels malveillants et de la surveillance de la sécurité réseau pour détecter les flux liés à des activités suspectes ;

## Fonctionnalités principales

- **Filtrage avancé** : permet de filtrer les paquets en fonction de critères tels que l'adresse IP, le port, le protocole, etc. pour se concentrer sur des éléments spécifiques.
- **Analyse détaillée** : offre une analyse approfondie des paquets, y compris l'inspection des en-têtes, le suivi des flux de données, la reconstitution de sessions, etc.
- **Support de nombreux protocoles** : prend en charge un large éventail de protocoles réseau, tels que TCP, UDP, HTTP, DNS, FTP, et bien d'autres.
- **Exportation de données** : les résultats de l'analyse peuvent être exportés dans divers formats tels que CSV, XML et PCAP.
- **Graphiques et statistiques** : permet de générer des graphiques et des statistiques pour visualiser les performances du réseau.

## TShark

**TShark** est une version CLI de Wireshark qui permet les mêmes actions d'enregistrement et d'analyse de captures réseau mais au travers de la ligne de commande uniquement. TShark peut se montrer utile dans de nombreux cas :

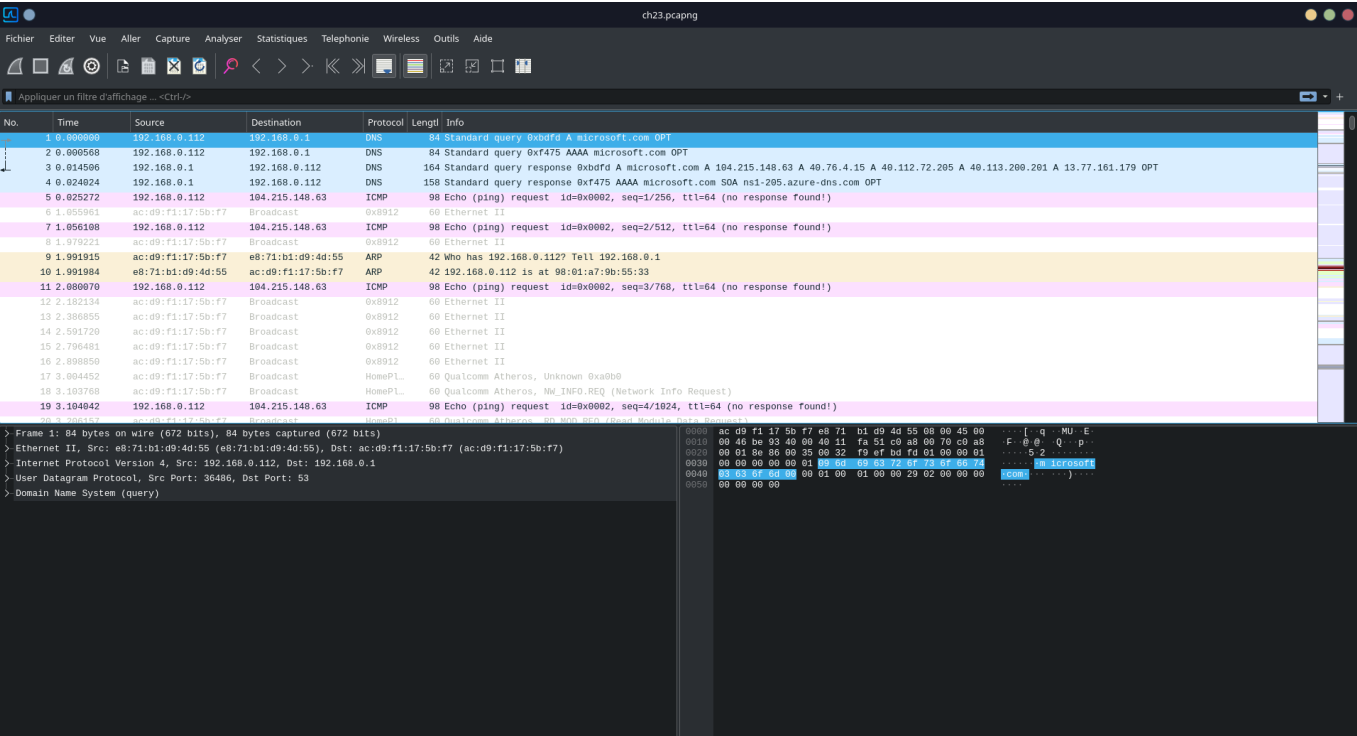
- Traitements automatisés via des scripts ;
- Extraction de données ;
- Usage sur serveurs ;
- ...

## Exemple d'exploitation ou d'utilisation

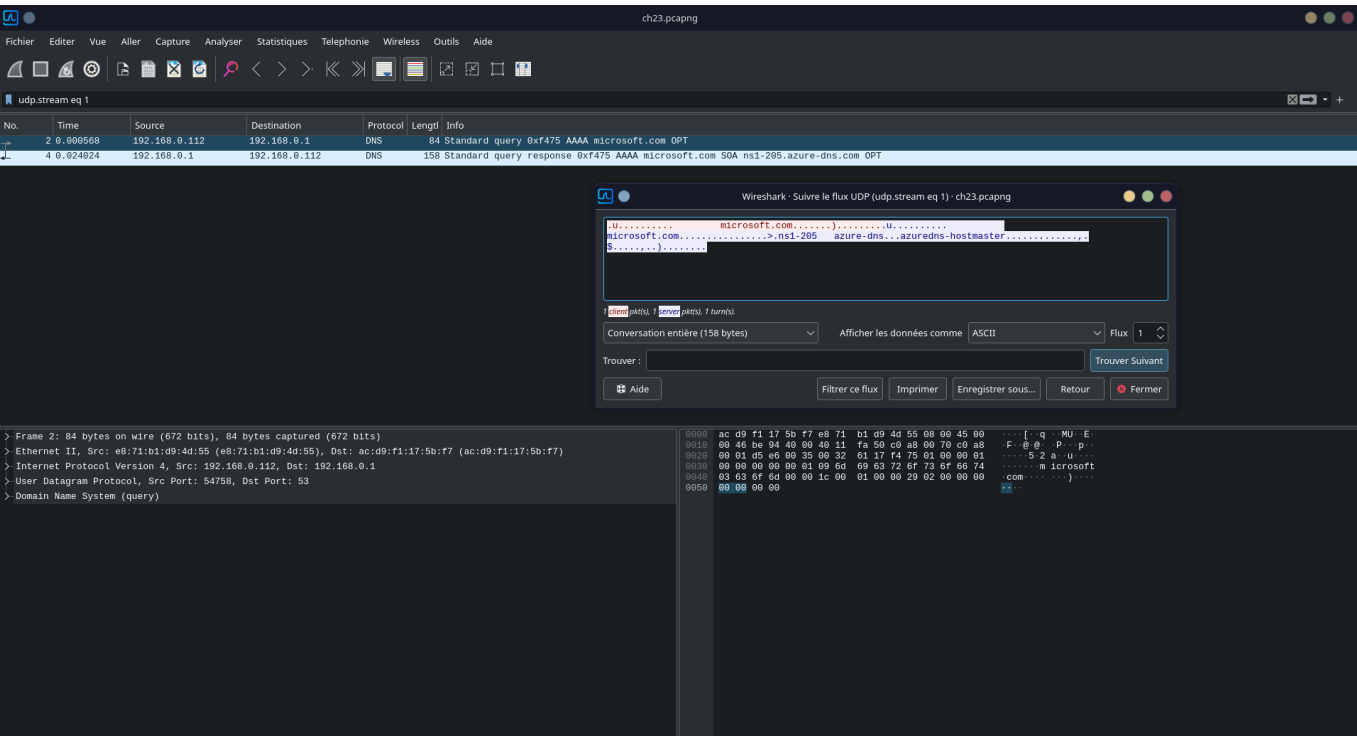
Supposons que vous êtes confronté à des problèmes de latence sur un réseau local, vous pouvez lancer Wireshark et sélectionner l'interface réseau à surveiller.

En appliquant un filtre pour ne capturer que le trafic pertinent et en filtrant le trafic vers ou depuis une adresse IP spécifique par exemple, vous pourrez, en analysant les résultats, identifier les sources de latence telles que des retards de transmission ou des pertes de paquets.

- Analyse de paquets de données capturés sur un réseau



- Fonctionnalité de suivi de Flux (UDP, TCP...)
- Analyse de paquets de données capturés sur un réseau



- Filtrage des paquets par adresse IP
- Analyse de paquets de données capturés sur un réseau

The screenshot shows the Wireshark network protocol analyzer interface. The top pane (Packet List) displays a list of 20 captured packets, all of which are DNS queries or responses. The middle pane (Packet Details) shows the hierarchical structure of the selected packet (No. 1), which is an Ethernet II frame containing an IPv4 packet and a UDP packet. The bottom pane (Packet Bytes) shows the raw data of the selected packet in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.112	192.168.0.1	DNS	84	Standard query 0xbdf4 A microsoft.com OPT
2	0.000508	192.168.0.112	192.168.0.1	DNS	84	Standard query 0xf475 AAAA microsoft.com OPT
3	0.014596	192.168.0.1	192.168.0.112	DNS	164	Standard query response 0xbdf4 A microsoft.com A 104.215.148.63 A 40.76.4.15 A 40.112.72.205 A 40.113.200.201 A 13.77.161.179 OPT
4	0.024024	192.168.0.1	192.168.0.112	DNS	158	Standard query response 0xf475 AAAA microsoft.com SOA nsl-205.azure-dns.com OPT
34	15.168478	192.168.0.112	192.168.0.1	DNS	81	Standard query 0xb963 A google.com OPT
35	15.183801	192.168.0.1	192.168.0.112	DNS	97	Standard query response 0xb963 A google.com A 172.217.13.174 OPT
36	15.185280	192.168.0.112	192.168.0.1	DNS	81	Standard query 0x202c AAAA google.com OPT
38	15.197990	192.168.0.1	192.168.0.112	DNS	109	Standard query response 0x202c AAAA google.com AAAA 2607:f8b6:4920:805::200e OPT
39	15.223167	192.168.0.112	192.168.0.1	DNS	85	Standard query 0x94bf A www.amazon.com OPT
40	15.223390	192.168.0.112	192.168.0.1	DNS	85	Standard query 0xef0b AAAA www.amazon.com OPT
41	15.233906	192.168.0.1	192.168.0.112	DNS	180	Standard query response 0x94bf A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukh62yn.cloudfront.net A 13.225.196.169 OPT
42	15.240958	192.168.0.1	192.168.0.112	DNS	235	Standard query response 0xef0b AAAA www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3ag4hukh62yn.cloudfront.net SOA ns-190.awsdns-16.com OPT
43	15.242876	192.168.0.112	192.168.0.1	DNS	100	Standard query 0x054f AAAA d3ag4hukh62yn.cloudfront.net OPT
44	15.243278	192.168.0.1	192.168.0.112	DNS	100	Standard query response 0x054f AAAA d3ag4hukh62yn.cloudfront.net OPT
75	15.378933	192.168.0.112	192.168.0.1	DNS	85	Standard query 0xc492 A tools.ietf.org OPT
76	15.379589	192.168.0.112	192.168.0.1	DNS	85	Standard query 0x0f66 AAAA tools.ietf.org OPT
83	15.633377	192.168.0.1	192.168.0.112	DNS	133	Standard query response 0xc492 A tools.ietf.org A 64.170.98.42 A 4.31.198.61 A 4.31.198.62 OPT
85	15.718384	192.168.0.1	192.168.0.112	DNS	169	Standard query response 0x0f66 AAAA tools.ietf.org AAAA 2001:1900:3001:11::3d AAAA 2001:1900:3001:11::3e AAAA 2001:1900:126c:11::2a OPT
208	16.719948	192.168.0.112	192.168.0.1	DNS	86	Standard query 0xc68e A one.one.one.one OPT
209	16.720370	192.168.0.112	192.168.0.1	DNS	86	Standard query 0x7a7a AAAA one.one.one.one OPT

Frame 2: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0  
 Ethernet II, Src: e8:71:b1:d9:4d:55 (e8:71:b1:d9:4d:55), Dst: ac:d9:f1:17:5b:f7 (ac:d9:f1:17:5b:f7)  
 Internet Protocol Version 4, Src: 192.168.0.112, Dst: 192.168.0.1  
 User Datagram Protocol, Src Port: 54758, Dst Port: 53  
 Domain Name System (query)

```

0000  ac d9 f1 17 5b f7 e8 71  b1 d9 4d 55 08 00 45 00  ...[.q..MU..E
0010  00 45 be 94 00 00 00 11  fa 50 c0 a8 08 70 c0 a8  F..0..P..p
0020  00 01 d5 e6 00 35 00 32  61 17 f4 75 01 00 00 01  ....5.2 a..u
0030  00 00 00 e0 00 01 09 6d  69 63 72 6f 73 6f 66 74  ....m icrosoft
0040  00 03 6f 4d 00 00 3c 00  01 00 00 29 02 00 00 00  ...com.....)
0050  00 00 00 00 00
  
```

- Analyse en profondeur d'une trame

The screenshot displays the Wireshark application window. At the top, there's a menu bar with options like Fichier, Edit, Vue, Aller, Capture, Analyseur, Statistiques, Telephone, Wireless, Outils, Aide. Below it is a toolbar with various icons for file operations, capture control, and packet navigation. The main pane shows a packet list on the left, a packet details pane in the middle, and a packet bytes pane at the bottom. The packet list shows several DNS queries from 192.168.0.1 to various servers. The selected packet (packet 327) is expanded in the details pane, showing its encapsulation type as Ethernet II, arrival time, epoch time, frame number, length, and capture length. The packet bytes pane shows the raw data of the captured packet. The status bar at the bottom indicates the current filter is 'ip.addr == 192.168.0.1'.

- Usage de TShark

Voici un exemple d'usage de tshark. Imaginons une importante capture réseau comprenant un très grand nombre de paquets, mais seuls les protocoles DNS et HTTP nous intéressent. Nous pouvons extraire les paquets comprenant ces protocoles dans une nouvelle capture en utilisant Tshark :

```
tshark -r capture example.pcapng -Y 'http || dns' -w out.pcapng
```

Nous pouvons ensuite lire la capture avec tshark :

```
tshark -r out.pcapng
```

```
1 0.000000000 192.168.121.3 → 192.168.202.49 DNS 103 Standard query response 0x6f3d A perdu.com A
104.21.5.178 A 172.67.133.176
```

```
2 0.000000209 192.168.121.3 → 192.168.202.49 DNS 127 Standard query response 0x8802 AAAA perdu.com AAAA
2606:4700:3033::6815:5b2 AAAA 2606:4700:3037::ac43:85b0
3 0.009499422 192.168.5.74 → 104.21.5.178 HTTP 141 GET / HTTP/1.1
4 0.377068826 104.21.5.178 → 192.168.5.74 HTTP 73 Continuation
```

## References

URL :

- <https://www.wireshark.org/docs/>
- <https://www.wireshark.org/docs/man-pages/tshark.html>

## Retour fiches outils

- [Cyber fiches outils](#)

From:

/ - **Les cours du BTS SIO**

Permanent link:

</doku.php/cyber/outils/wireshark>

Last update: **2025/06/27 14:57**

