

Wireshark - TP de découverte

Ce logiciel est un analyseur de trafic réseau (sniffer). Ce TP se déroule en 3 parties :

1. Découverte de l'interface
2. Capture et analyse de trafic généré par la commande **ping**
3. Analyse d'un fichier de capture fourni.

Wireshark est un logiciel gratuit, on peut le télécharger ici :

<https://www.wireshark.org/download.html>

Pour une utilisation avancée la documentation est disponible ici :

<https://www.wireshark.org/docs/>

1. Découverte de l'interface de wireshark

Wireshark fonctionne à la manière d'un enregistreur numérique : on lance un enregistrement, on l'arrête, et on analyse ensuite le trafic capturé.

- Télécharger, installer, et exécuter Wireshark,
- Lancer ensuite une capture (bouton bleu),
- Accepter les propositions par défaut de la capture (généralement c'est la carte réseau installée),
- Stopper la capture au bout de quelques secondes (bouton rouge).

No.	Time	Source	Destination	Protocol	Length	Info
5	0.716489	192.168.1.50	192.168.1.27	ICMP	98	Echo (ping) request
6	0.720607	192.168.1.27	192.168.1.50	ICMP	98	Echo (ping) reply
7	1.721737	192.168.1.50	192.168.1.27	ICMP	98	Echo (ping) request
8	1.725304	192.168.1.27	192.168.1.50	ICMP	98	Echo (ping) reply
9	2.481200	2a01:cb20:1b:7100:...	2607:f8b0:4008:802...	UDP	1392	63570 → 443 Len=1330
10	2.481201	2a01:cb20:1b:7100:...	2607:f8b0:4008:802...	UDP	471	63570 → 443 Len=409
11	2.538108	2607:f8b0:4008:802...	2a01:cb20:1b:7100:...	UDP	1392	443 → 63570 Len=1330

The details pane for the selected packet (Frame 20) shows:

- ▶ Frame 20: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
- ▶ Ethernet II, Src: 9a:de:d0:07:c9:44 (9a:de:d0:07:c9:44), Dst: Apple_ea:dd:17 (a4:5e:60:ea:dd:17)
- ▶ Internet Protocol Version 4, Src: 192.168.1.27, Dst: 192.168.1.50
- ▶ Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 a4 5e 60 ea dd 17 9a de d0 07 c9 44 08 00 45 00  .^.....D.E.
0010 00 54 9b 61 00 00 40 01 5b aa c0 a8 01 1b c0 a8  .T.a..@[.....
0020 01 32 00 00 f2 76 0d 3e 00 02 5d 7d 6b 0f 00 08  .2...v.>..}k..
0030 4c b1 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  L.....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....! "#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 67
```

De haut en bas, on va trouver :

- La barre des menus
- La barre des icônes (raccourcis permettant d'éviter de passer par les menus)
- La zone de filtrage (un filtre permet de choisir le trafic que l'on veut observer)
- La liste des trames numérotées et chronométrées dans l'ordre chronologique de la capture. Les adresses IPv4 ou IPv6 de l'émetteur et du destinataire sont indiquées, ainsi que le protocole utilisé.
- La fenêtre d'affichage de la pile des protocoles pour la trame sélectionnée. On peut dérouler chaque protocole pour obtenir le détail des informations contenues.
- Fenêtre d'affichage brut de la trame sélectionnée (tous les octets de la trame en hexadécimal).

2. Capture et analyse de trafic généré par la commande ping

Pour cet exercice, il est demandé de noter son adresse IPv4 ainsi que celle de sa passerelle. On va pour cela utiliser la commande **ipconfig** dans la console de commande de Windows (voir <https://fr.wikipedia.org/wiki/Ipconfig>) :

```
C:>ipconfig
```

```
Configuration IP de Windows
```

```
Carte réseau sans fil Connexion réseau sans fil :
```

```
Statut du média. . . . . : Média déconnecté  
Suffixe DNS propre à la connexion. . . :
```

```
Carte Ethernet Connexion au réseau local :
```

```
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::89c9:7d53:f73:c8c4%11  
Adresse IPv4. . . . . : 192.168.1.2  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle [[par défaut]]. . . . . : 192.168.1.1
```

- Adresse IP de votre ordinateur :
- Adresse IP de votre passerelle :

La commande **ping** utilise le protocole **ICMP**
(https://fr.wikipedia.org/wiki/Internet_Message_Protocol)

On va maintenant observer le trafic réseau généré par la commande ping :

- Lancer une nouvelle capture avec Wireshark (on acceptera de ne pas sauvegarder la précédente)
- Dans la console de commande de Windows, exécuter la commande **ping x.x.x.x** (remplacer x.x.x.x par l'@IPv4 de la passerelle)
- Une fois les 4 réponses obtenues, stopper la capture.
- Appliquer le filtre **icmp** pour n'afficher que les trames générées par la commande **ping**.

On peut maintenant analyser le trafic capturé :

- Nombre de trames générées :
- @IP source d'une trame request :
- @IP destination d'une trame request :
- @IP source d'une trame reply :
- @IP destination d'une trame reply :
- Durée écoulée entre la trame request et la trame reply du premier échange :
- Nombre d'octets de données de la trame request :
- Nombre d'octets de données de la trame reply :

3. Analyse d'un fichier de capture fourni

Avec Wireshark, ouvrir le fichier **http-wget-iana-ipv4.pcap** disponible sur le site de ressources. Ce fichier contient les trames capturées lors du chargement d'une page web.

- @IPv4 du client HTTP :
- @IPv4 du serveur HTTP :
- @IPv4 du serveur DNS :
- Rôle des trames 1 & 2 :
- Rôle des trames 3 à 5 :
- Rôle de la trame 6 :
- Rôle de la trame 12 :
- Rôle des trames 13 à 15 :

On peut récupérer l'adresse IP publique d'un serveur avec son nom de domaine, en utilisant <https://mxtoolbox.com/DNSLookup.aspx>

- Pourquoi une requête DNS est-elle nécessaire ?
- Adresse IPv4 de google.fr :