

## TD2 : Utilisation de Wireshark pour étudier le trafic réseau

Rappel : ce TD doit faire l'objet d'un **Compte Rendu électronique à déposer sur GitLab** avant le début de séance suivante, à l'attention de l'enseignant responsable de votre groupe. Doivent y figurer les manipulations et configurations nécessaires, illustrées par des captures d'écran pertinentes !

### Objectifs

- Utiliser un outil d'observation du trafic réseau
- Explorer le contenu des paquets IP
- Identifier les données présentes dans l'en-tête d'un paquet
- Analyser le parcours des données sur un réseau

### Partie I : Les données ICMP locales

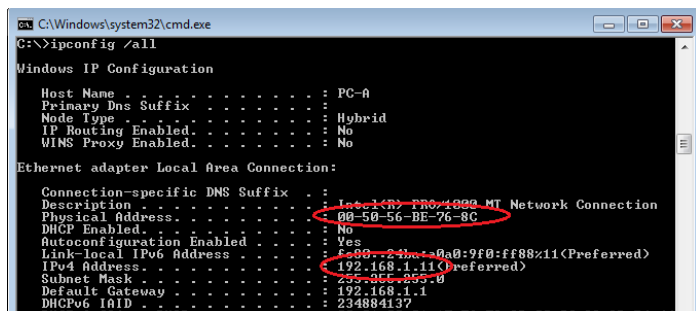
Pour ce TD, la configuration des postes de l'IUT nécessite de **travailler sous Windows**.

#### 1. Identifier les adresses d'interface de votre ordinateur

Dans le cadre de cet atelier, il faut récupérer l'adresse IP de votre ordinateur et l'adresse physique de sa carte réseau, également appelée adresse MAC.

- a) Ouvrir une fenêtre de commandes (**terminal** ou **cmd**) :

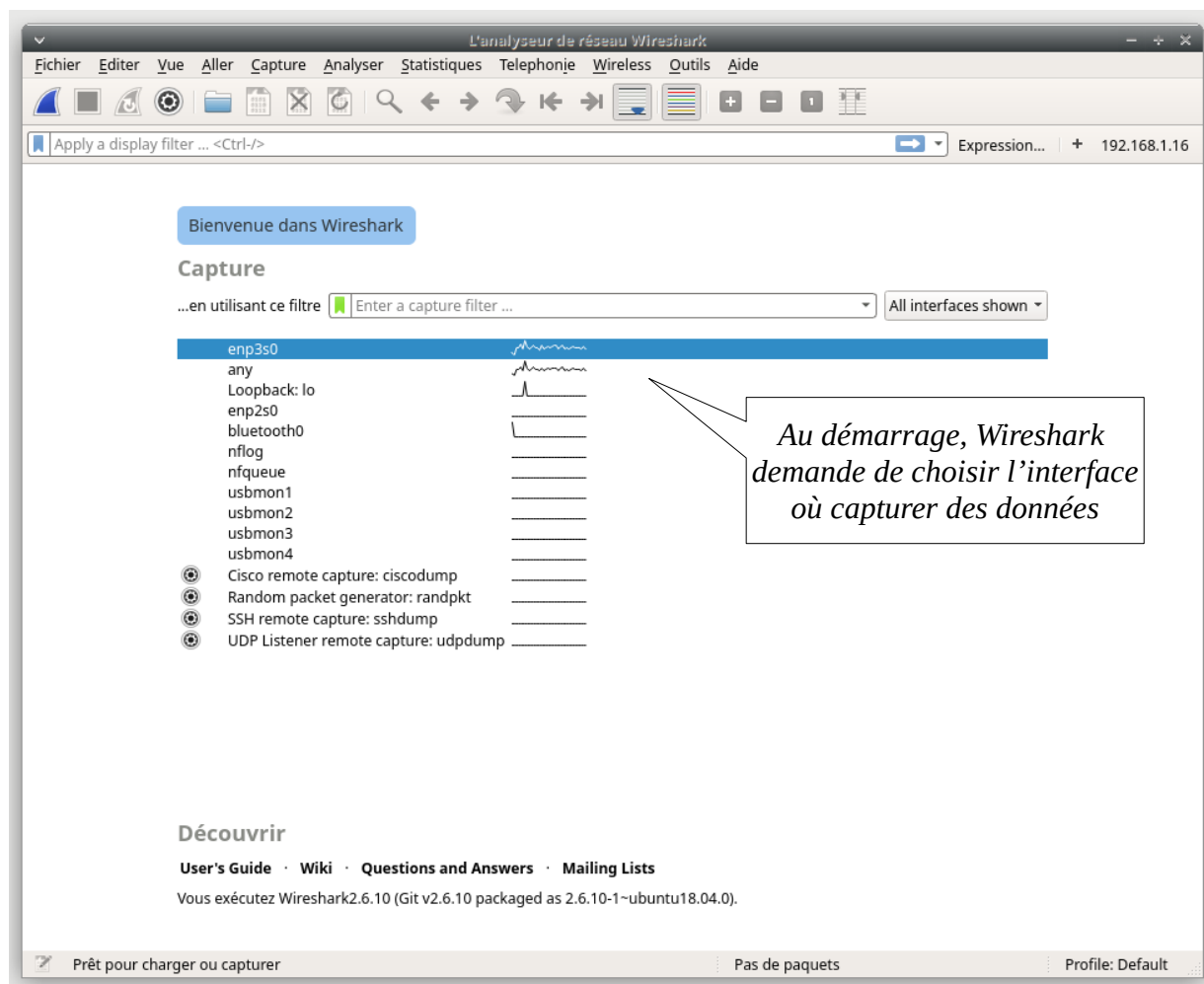
- Sous Windows, taper **ipconfig /all**
- Sous Linux, taper **ifconfig** ou **ip addr show**



- Noter l'**adresse IP** (notée **inet** avec **ifconfig**) et l'adresse **physique** (**MAC**, notée **ether**) de l'interface de votre ordinateur.

- b) Demandez à un binôme voisin de fournir **l'adresse IP de son ordinateur** et **donnez-lui la votre**. Ne lui fournissez pas votre adresse MAC pour le moment.

## 2. Commencer à capturer des données avec Wireshark



a) Sélectionner l'interface correspondant au réseau local.



En cas de doute, *survoler* avec la souris le nom de chaque interface : l'info-bulle indique l'adresse IP et l'adresse MAC de l'interface (choisir celle qui correspond au réseau du Département : **10.31.4.xxx** ou **10.31.5.xxx**)

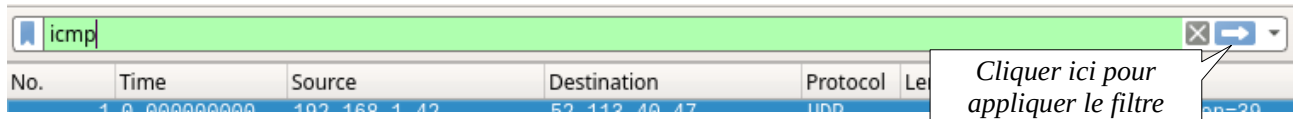
b) Cliquer sur l'aileron de requin  pour démarrer la capture !

Les lignes de données s'affichent en différentes couleurs selon le protocole :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.42	52.113.40.47	UDP	81	50745 → 3480 Len=39
2	0.026655272	192.168.1.1	192.168.1.255	BROWSER	232	Browser Election Request
3	0.055087556	192.168.1.42	52.113.40.47	STUN	142	Binding Request user: z4EL:7UUD
4	0.102608130	192.168.1.42	52.113.40.47	UDP	81	50745 → 3480 Len=39
5	0.106378913	192.168.1.1	224.0.0.251	IGMPv2	60	Membership Report group 224.0.0.251
6	0.138445274	52.113.40.47	192.168.1.42	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 90.
7	0.184224125	192.168.1.42	52.113.40.47	UDP	64	50745 → 3480 Len=22
8	0.195071130	192.168.1.42	52.113.40.47	UDP	81	50745 → 3480 Len=39
9	0.287190452	192.168.1.42	52.113.40.47	UDP	64	50745 → 3480 Len=22

- c) Pour faciliter l'affichage et la manipulation, il est nécessaire de filtrer les données capturées, par exemple selon une adresse (source ou destination) ou un protocole.

Pour cet atelier, il suffit de limiter l'affichage aux données **ICMP** (correspondant au **ping**) :



Ce filtre fait disparaître toutes les données, mais la capture du trafic se poursuit ...

- d) Afficher la fenêtre d'invite de commandes ouverte précédemment et envoyer une requête **ping à l'adresse IP du voisin** : les données commencent à apparaître à nouveau ...

No.	Time	Source	Destination	Protocol	Length	Info
19288	767.039048068	192.168.1.42	192.168.1.26	ICMP	98	Echo (ping) request id=0x3891, seq=1/256, ttl=64
19293	767.138943623	192.168.1.26	192.168.1.42	ICMP	98	Echo (ping) reply id=0x3891, seq=1/256, ttl=64
19312	768.040103816	192.168.1.42	192.168.1.26	ICMP	98	Echo (ping) request id=0x3891, seq=2/512, ttl=64
19316	768.163900243	192.168.1.26	192.168.1.42	ICMP	98	Echo (ping) reply id=0x3891, seq=2/512, ttl=64
19349	769.041889268	192.168.1.42	192.168.1.26	ICMP	98	Echo (ping) request id=0x3891, seq=3/768, ttl=64

- e) Arrêter la capture en cliquant sur le gros carré rouge ...  
(et stopper les **ping** si vous êtes sous Linux ...)

### 3. Examiner les données capturées

Liste des trames capturées  
= paquets IP = PDU

Informations correspondant  
à la trame sélectionnée  
en fonction de ses couches  
de protocole

Données brutes  
de chaque couche

L'interface de Wireshark

- a) Cliquer sur la première trame de requête ICMP dans la partie supérieure de Wireshark.

**À quel ordinateur correspondent les adresses IP Source et Destination ?**

- b) Toujours dans cette trame, accéder à la section centrale de l'interface.  
Cliquer sur le triangle ► à gauche de la ligne **Ethernet II** pour afficher les adresses MAC de la destination et de la source.

- c) L'adresse MAC de la **source** correspond-elle à l'interface de votre ordinateur ?
- d) L'adresse MAC de la **destination** correspond-elle à celle de l'ordinateur de votre voisin ?
- e) **Comment votre ordinateur obtient-il l'adresse MAC de l'ordinateur destinataire des requêtes ping ?**

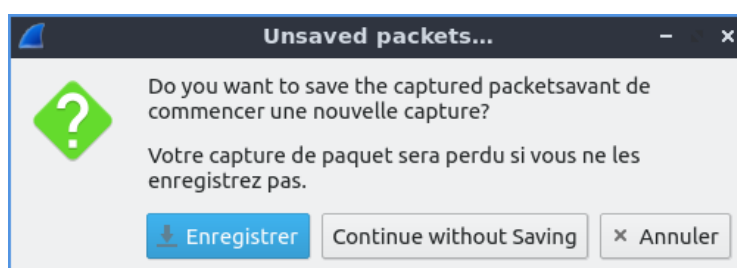
## Partie II : les données ICMP distantes

Dans cette partie, nous allons adresser des requêtes ping à des hôtes distants (ne figurant pas sur le réseau local) et examiner les données générées.

### 1. Nouvelle capture

- a) Cliquer à nouveau sur l'aileron pour relancer la capture.

**Enregistrer les données de la première partie pour un TD ultérieur :**



(par exemple sous le nom **captureTD2.pcapng**)

- b) Le processus de capture étant actif, envoyez une requête **ping** aux trois URL de sites web suivantes :
  - **www.yahoo.com**
  - **www.cisco.com**
  - **www.google.com**

**Remarque :** lors de l'envoi de la requête ping aux URL indiquées, noter que le serveur de noms de domaine (DNS) traduit l'URL en adresse IP. Garder en mémoire l'adresse IP reçue pour chaque URL.

## 2. Examen et analyse des données des hôtes distants

a) Examiner les données capturées dans Wireshark, les adresses IP et MAC des trois sites auxquels vous avez envoyé des requêtes **ping**.

b) Indiquer les adresses IP et MAC de destination pour les trois sites :

1er site : IP : \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC : \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

2ème site : IP : \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC : \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

3ème site : IP : \_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_.\_\_\_\_\_ MAC : \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_\_

c) Qu'y a-t-il d'important à retenir de ces informations ? **En quoi ces informations diffèrent-elles** des informations de requêtes **ping** locales reçues dans la partie I ?