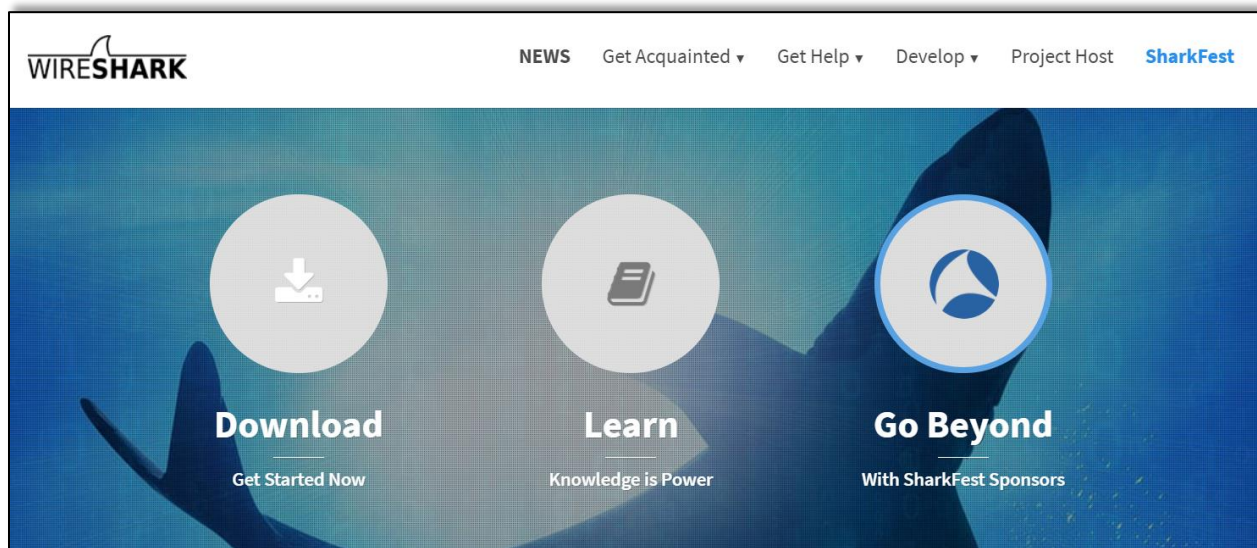


Travaux dirigés 6 - WIRESHARK

Capture, Filtrage et Analyse de trames ETHERNET
avec le logiciel Wireshark

Wireshark

Wireshark est apparenté aux logiciels appelés « Sniffer » ou « analyseur de trafic ».



- Un programme informatique libre de droit.
- Permet de capturer et d'analyser les trames d'information qui transitent par les interfaces de communication du terminal sur lequel il s'exécute.

Il est multi-OS et téléchargeable sur le site
<https://www.wireshark.org/>

Avec Wireshark , il est possible de :

- **Capturer des trames Ethernet** en temps réel directement sur les Cartes de communication du terminal,
- **Sauvegarder les résultats** de cette capture dans des fichiers qui peuvent être analysés ultérieurement hors ligne.

Wireshark supporte un très grand nombre de protocoles de communication et de formats de fichiers de capture

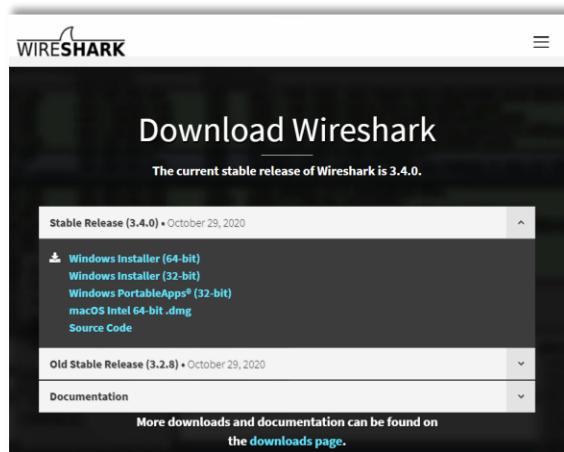
Ethernet	libpcap/tcpdump
ARP	Sun's snoop/atmsnoop
IP	Lanalyzer
TCP/UDP	MS Network Monitor
HDLC	HPUX nettl
<i>etc ...</i>	AIX iptrace
	Cisco Secure IDS
	<i>etc ...</i>

How Important is it to use a virtual Machine for using Wireshark?

<https://ask.wireshark.org/question/4057/how-important-is-it-to-use-a-virtual-machine-for-using-wireshark/>

As **Step 1** on the Wireshark [CaptureSetup](#) wiki page asks, the real question is ***Are you allowed to do this?*** If you're capturing packets on your own private network at home, then the answer is "Yes, of course", but if you're at work, your employer might tell you "No". If you use a virtual machine, then you avoid any legal issues of capturing and avoid breaking corporate policy, for example.

Installation de Wireshark



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

Un administrateur réseaux passe au moins 80% de son temps de travail à résoudre des problèmes techniques : dépannage de connexion internet, dépannage de serveur, de poste de travail ou encore d'application toujours divers et variés. Sans les outils adaptés, il est difficile d'observer et d'analyser véritablement les données qui transitent sur le réseau informatique, le travail devient très complexe avec un résultat aléatoire et une perte de productivité bien trop importante.

Pourquoi choisir Wireshark ?

Pourquoi choisir Wireshark ?

- Depuis 1998.
- Gratuit et open source Licence GNU
- Multiplateforme
- Force : analyse protocolaire
- Intégré dans certains simulateurs réseau

Durant ce TP, nous allons :

1. lancer le programme Wireshark
2. capturer et analyser une trame Ethernet
3. définir des filtres pour la capture et la visualisation des trames
4. Enregistrer le résultat de cette capture dans un fichier

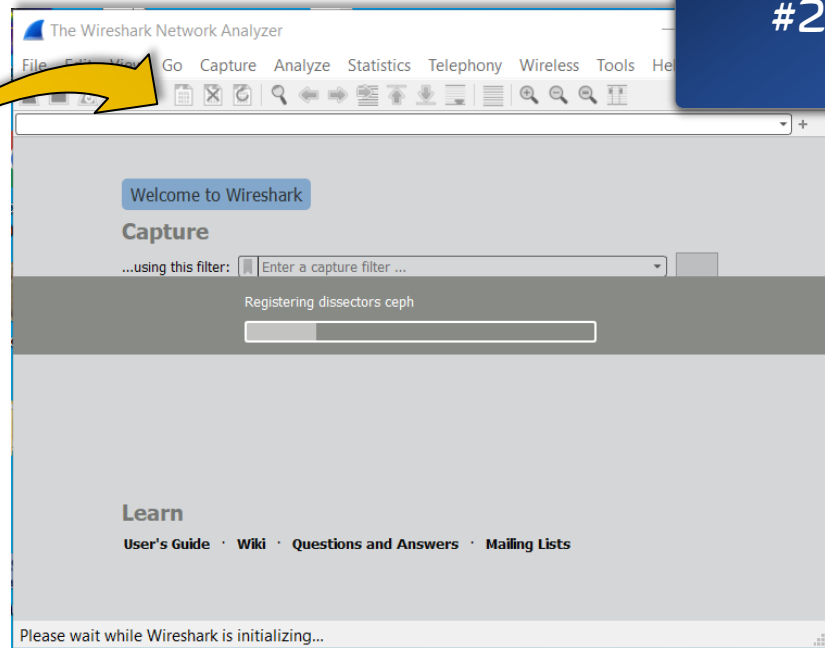
Etape 1

Lancement du programme Wireshark

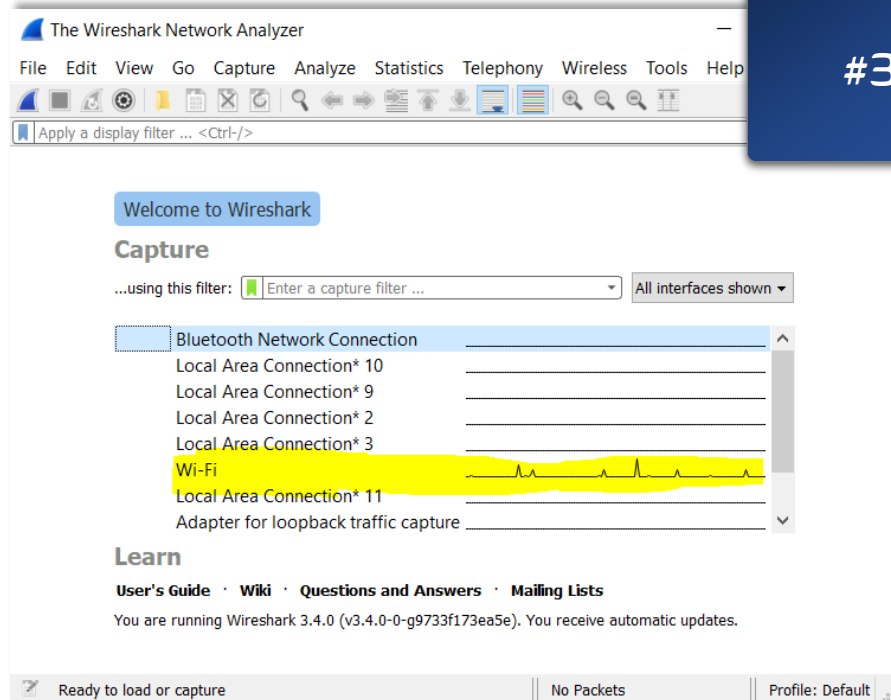
#1



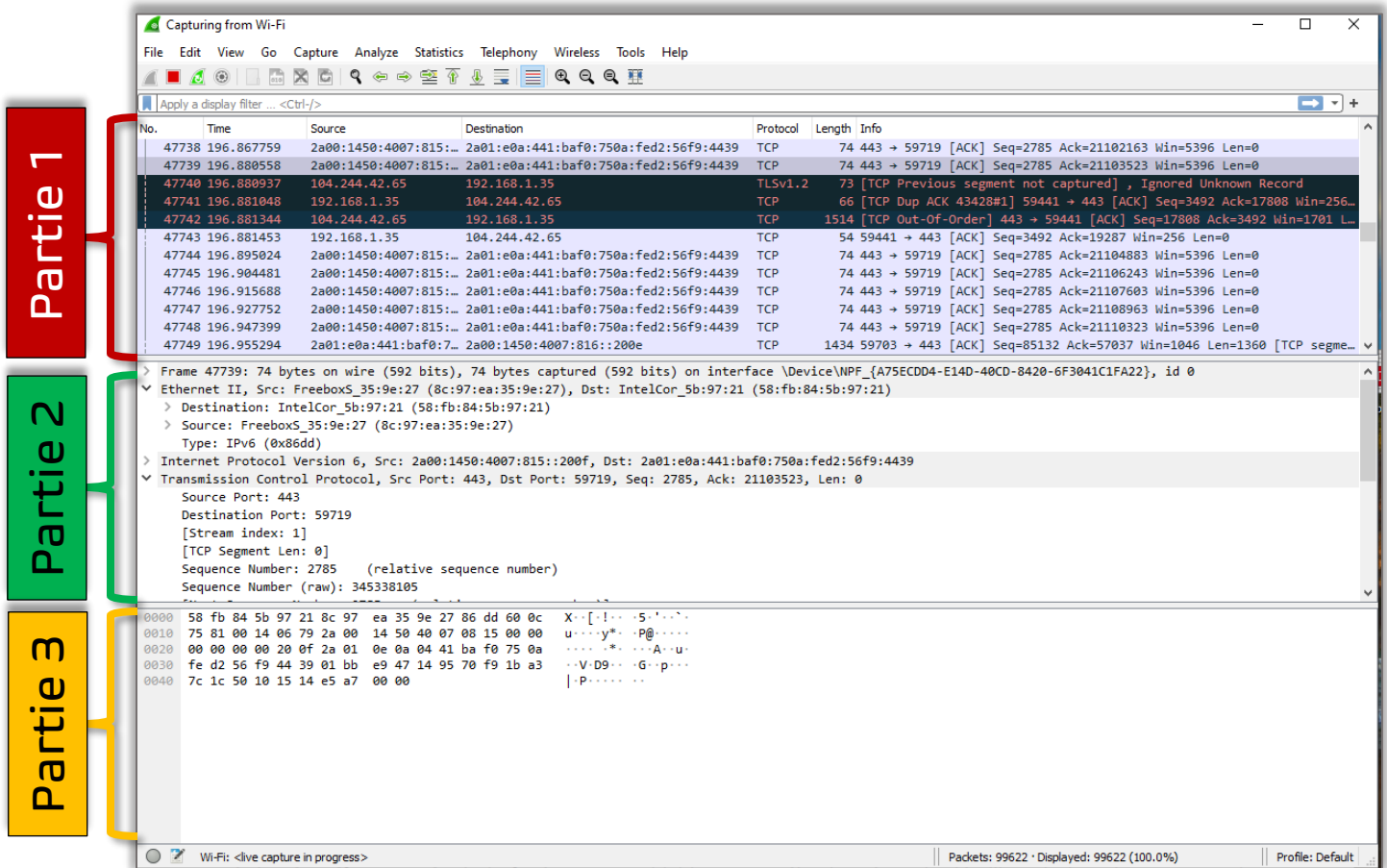
#2



#3



La fenêtre est divisée en trois parties.



1. La première partie est de type général, on y trouve des informations de type adresse IP des machines ou encore protocole utilisé lors de l'échange des données.

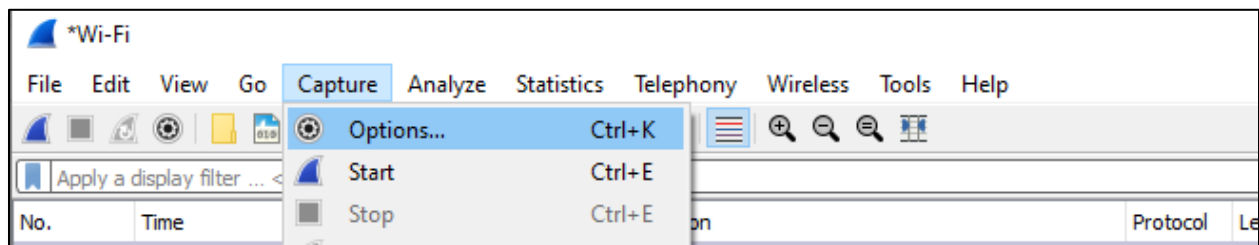
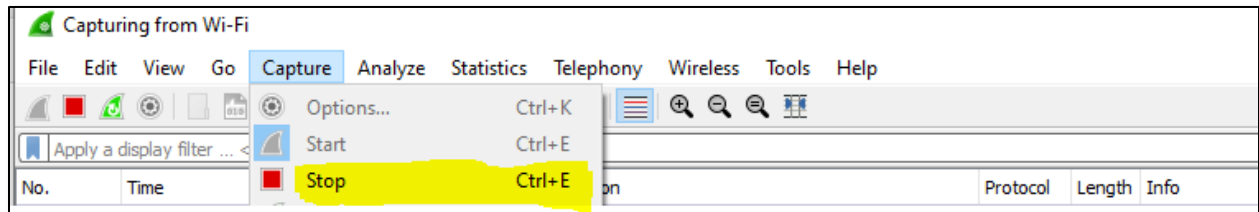
2. La deuxième partie de la fenêtre reprend ici la trame sélectionnée et la détaille soit dans les sept couches du modèles OSI ou dans les quatre couches du modèle IP. Pour plus d'informations à ce sujet des tutoriaux sont disponibles sur le net.

3. La troisième et dernière partie est une vision de la trame en codage hexadécimal et ASCII

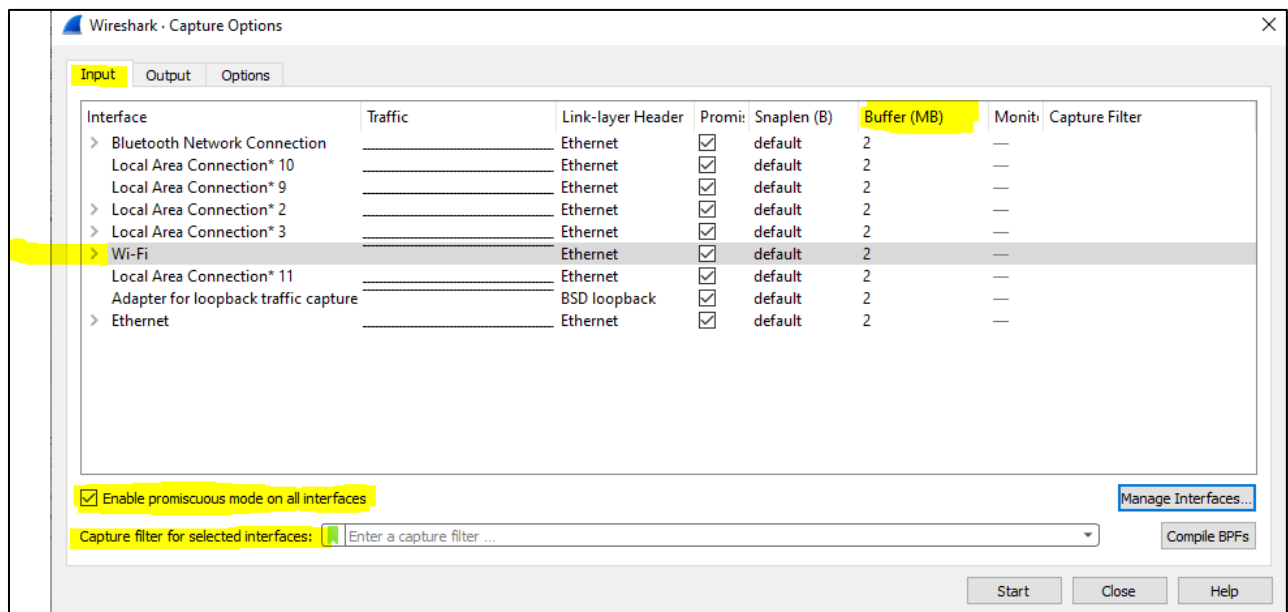
Nous allons voir maintenant comment capturer les trames sur le réseau sur lequel le sniffer est connecté.

Etape 2

Capture de trames sur le réseau



La fenêtre suivante s'ouvre.



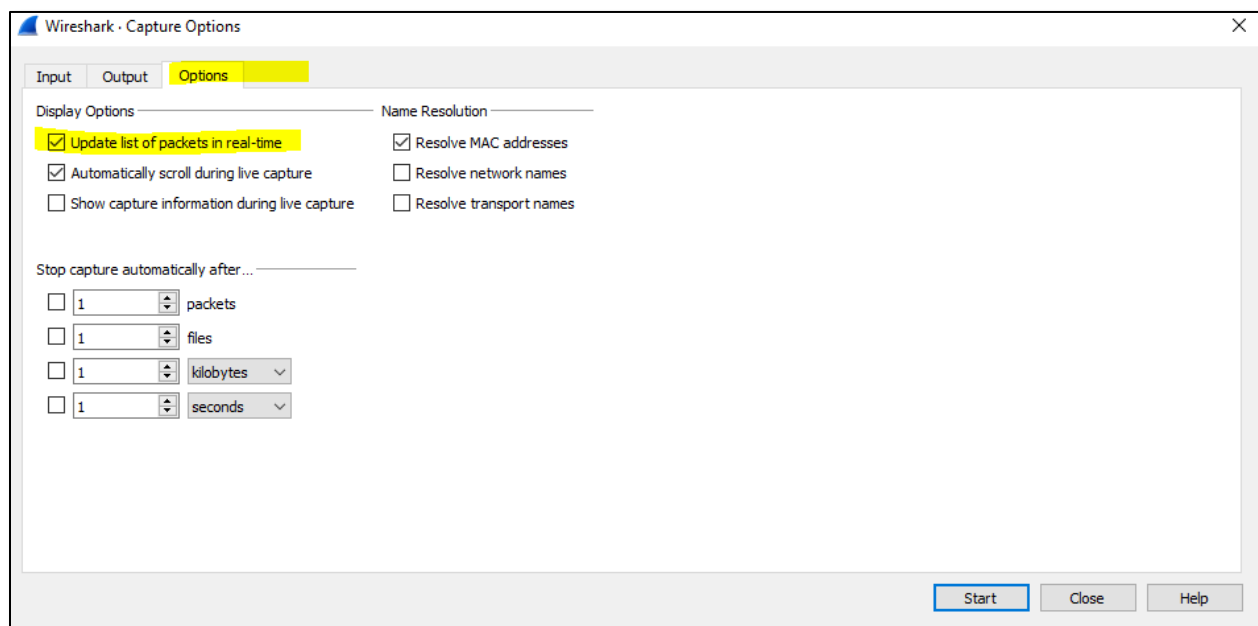
Choisissez l'interface sur laquelle vous voulez "écouter" le trafic. Si vous en avez qu'une le choix ne sera pas très difficile. Par défaut l'espace réservé à la collecte des données est défini à 2MB. Cela devrait être suffisant. Dans le cas contraire augmentez-le.

Choisissez l'interface sur laquelle vous voulez "écouter" le trafic. Si vous en avez qu'une le choix ne sera pas très difficile.

Par défaut l'espace réservé à la collecte des données est défini à 1MB. Cela devrait être suffisant. Dans le cas contraire augmentez-le.

Activer l'option "Capture packets in promiscuous mode". Cette option permet à la carte réseau de lire et d'intercepter tout le trafic sur le réseau. Dans le cas contraire celle-ci n'interceptera que les trames qui lui sont destinées et ainsi vous ne verrez pas toutes les trames Multicast et Broadcast.

Laissez le champ "Capture Filter" vide dans un premier temps. Nous verrons par la suite comment le remplir.



Nous ne toucherons pas aux autres options.

Il ne vous reste plus qu'à démarrer la capture en cliquant sur "Start".

Capturez environ 30 secondes de trafic entre le poste client et serveur. Puis cliquez sur "Stop". Wireshark va alors afficher les trames capturées par votre carte réseau dans un format lisible ci-dessous.

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of 11 captured packets. The first packet is selected, and its details are shown in the right-hand pane. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for file operations, capture control, and analysis.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2a00:1450:4007:80b::...	2a01:e0a:441:baf0:750a:fed2:56f9:4439	TCP	74	443 → 51466 [ACK] Seq=1 Ac
2	0.009449	2a00:1450:4007:80b::...	2a01:e0a:441:baf0:750a:fed2:56f9:4439	TCP	74	443 → 51466 [ACK] Seq=1 Ac
3	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1172
4	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1186
5	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1195
6	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1213
7	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1226
8	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1240
9	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1254
10	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1267
11	0.009901	2a01:e0a:441:baf0:7...	2a00:1450:4007:80b::200f	TCP	1434	51466 → 443 [ACK] Seq=1281

Sur la première partie de cette fenêtre les différentes trames capturées s'affichent et suivant les colonnes nous avons les informations suivantes :

- ✦ **Première colonne** : numéro de la trame.
- ✦ **Deuxième colonne** : temps écoulé depuis le départ de la capture et l'arrivée de la trame.
- ✦ **Troisième colonne** : adresse IP ou nom de la machine émettrice
- ✦ **Quatrième colonne** : adresse IP ou nom de la machine réceptrice
- ✦ **Cinquième colonne** : protocole utilisé entre les deux machines
- ✦ **Sixième colonne** : informations complémentaires

La quantité de données capturées peut vite devenir considérable, d'autant plus que plusieurs communications peuvent être établies en parallèle comme par exemple une connexion à www.google.fr et une autre à www.tplpc.com.

C'est pourquoi nous allons voir comment définir un filtre pour capturer une partie de tout ce que voit la carte réseau.

Etape 3

Les filtres

Il y a deux sortes de filtres : **les filtres à la capture** **les filtres à l'affichage**

#1 Filtres d'affichage

Capturer toutes les trames dans un premier temps et de filtrer par la suite.
L'avantage de cette solution est d'avoir toujours la capture de départ et d'y appliquer par la suite autant de filtres que l'on souhaite.

- ✚ Les expressions sont basées sur les champs disponibles dans un paquet.
- ✚ Le simple ajout d'un champ veut dire que l'on garde le paquet si ce champ est disponible.
- ✚ Maintenant, on peut aussi utiliser les opérateurs ==, !=, >, = et <= pour comparer les champs avec des valeurs.
- ✚ Les expressions ainsi fabriquées peuvent être combinées avec les opérateurs && (pour un et logique), || (pour un ou logique), ^^ (pour le ou exclusif) et ! Pour la négation.
- ✚ L'usage des parenthèses est possible.

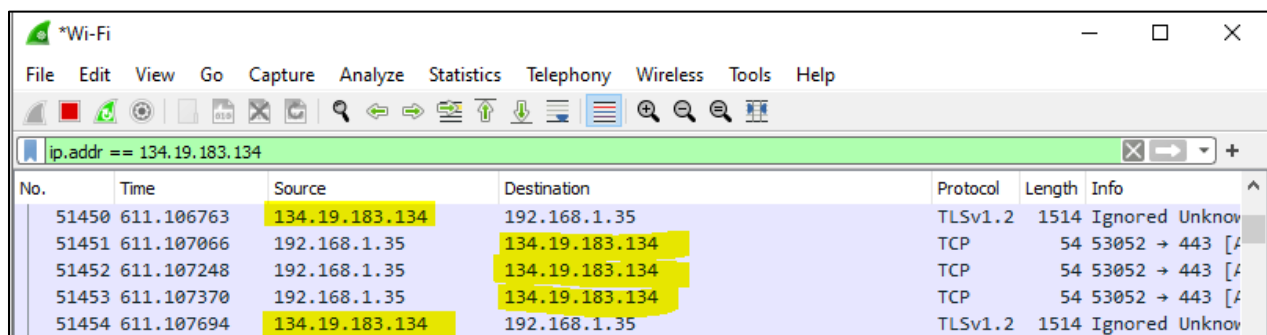
Voici quelques exemples de champs disponibles

Champ	Fonction	Signification
<code>ip.addr</code>	adresse IPv4	Adresse IP source ou destination
<code>ip.dst</code>	adresse IPv4	Adresse IP destination
<code>ip.flags.df</code>	booléen	Drapeau IP, ne pas fragmenter
<code>ip.flags.mf</code>	booléen	Drapeau IP, fragments a venir
<code>ip.ttl</code>	entier non signé sur 8 bits	Time to live
<code>nbdgm.src.ip</code>	adresse IPv4	adresse IP source d'un paquet Netbios Datagram
<code>nbdgm.src.port</code>	entier non signé sur 16 bits	port IP source d'un paquet Netbios Datagram
<code>http.request</code>	booléen	requête HTTP
<code>http.reponse</code>	booléen	réponse HTTP
<code>icmp.code</code>	entier non signé sur 8 bits	numéro du code d'une commande ICMP
<code>icmp.type</code>	entier non signé sur 8 bits	numéro du type d'une commande ICMP

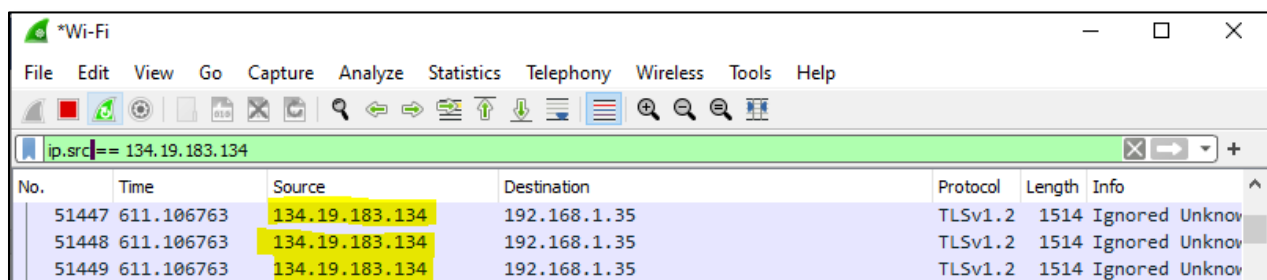
<code>ftp.request</code>	booléen	requête FTP
<code>ftp.request.command</code>	chaîne de caractères	commande FTP
<code>ftp.reponse.data</code>	chaîne de caractères	donnée de transfert FTP
<code>dns.query</code>	booléen	requête DNS
<code>dns.response</code>	booléen	réponse d'une requête DNS

Voici quelques exemples de filtres

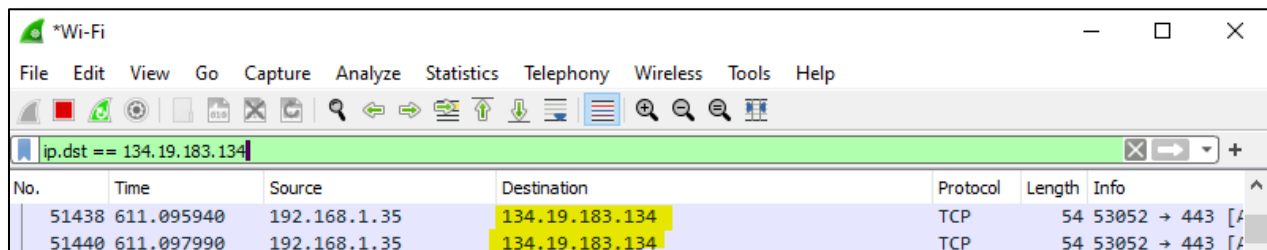
Champ	Signification
<code>ip.addr == 172.16.0.100</code>	Tous les paquets IP en provenance ou à destination de la machine 172.16.0.100
<code>(ip.addr == 172.16.0.100) && (dns.reponse)</code>	Tous les paquets IP en provenance ou à destination de la machine 172.16.0.100 qui sont des réponses À des requêtes DNS
<code>(ip.addr >= 172.16.0.100) && (ip.addr <= 172.16.0.123)</code>	Tous les paquets IP en provenance ou À destination des machines comprises entre l'adresse IP 172.16.0.100 et l'adresse IP 172.16.0.123 (comprises)



No.	Time	Source	Destination	Protocol	Length	Info
51450	611.106763	134.19.183.134	192.168.1.35	TLSv1.2	1514	Ignored Unknow
51451	611.107066	192.168.1.35	134.19.183.134	TCP	54	53052 → 443 [A
51452	611.107248	192.168.1.35	134.19.183.134	TCP	54	53052 → 443 [A
51453	611.107370	192.168.1.35	134.19.183.134	TCP	54	53052 → 443 [A
51454	611.107694	134.19.183.134	192.168.1.35	TLSv1.2	1514	Ignored Unknow



No.	Time	Source	Destination	Protocol	Length	Info
51447	611.106763	134.19.183.134	192.168.1.35	TLSv1.2	1514	Ignored Unknow
51448	611.106763	134.19.183.134	192.168.1.35	TLSv1.2	1514	Ignored Unknow
51449	611.106763	134.19.183.134	192.168.1.35	TLSv1.2	1514	Ignored Unknow



No.	Time	Source	Destination	Protocol	Length	Info
51438	611.095940	192.168.1.35	134.19.183.134	TCP	54	53052 → 443 [A
51440	611.097990	192.168.1.35	134.19.183.134	TCP	54	53052 → 443 [A

#2 Filtres de capture

Ne seront conservés que les paquets pour lesquels le filtre est vrai.

Les filtres se décomposent en 3 parties :

- Le protocole à capturer

Exemples : ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp ou udp.

- L'identifiant

peut être src ou dst.

- Un champ qui peut être host, net ou port suivi d'une valeur.

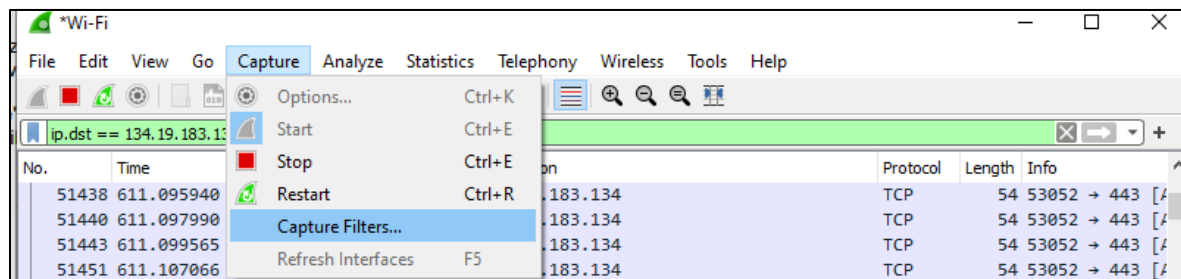
Les opérateurs **and**, **or** et **not** peuvent être utilisés pour combiner des filtres.

Filtre	Fonction
host 172.16.0.1 and tcp	Ne conserve que les paquets TCP à destination ou en provenance de la machine 172.16.0.1
udp port 53	Ne conserve que les paquets UDP en provenance ou à destination du port 53
udp port 53 and dst host 172.16.0.1	Ne conserve que les paquets UDP en provenance ou à destination du port 53 et à destination de la machine 172.16.0.1
tcp dst port 80 and dst host 172.16.0.1 and src net 172.16.0.0 mask 255.255.255.0	Ne conserve que les paquets TCP à destination de la machine 172.16.0.1 sur le port 80 et en provenance des machines du sous réseau 172.16.0/24

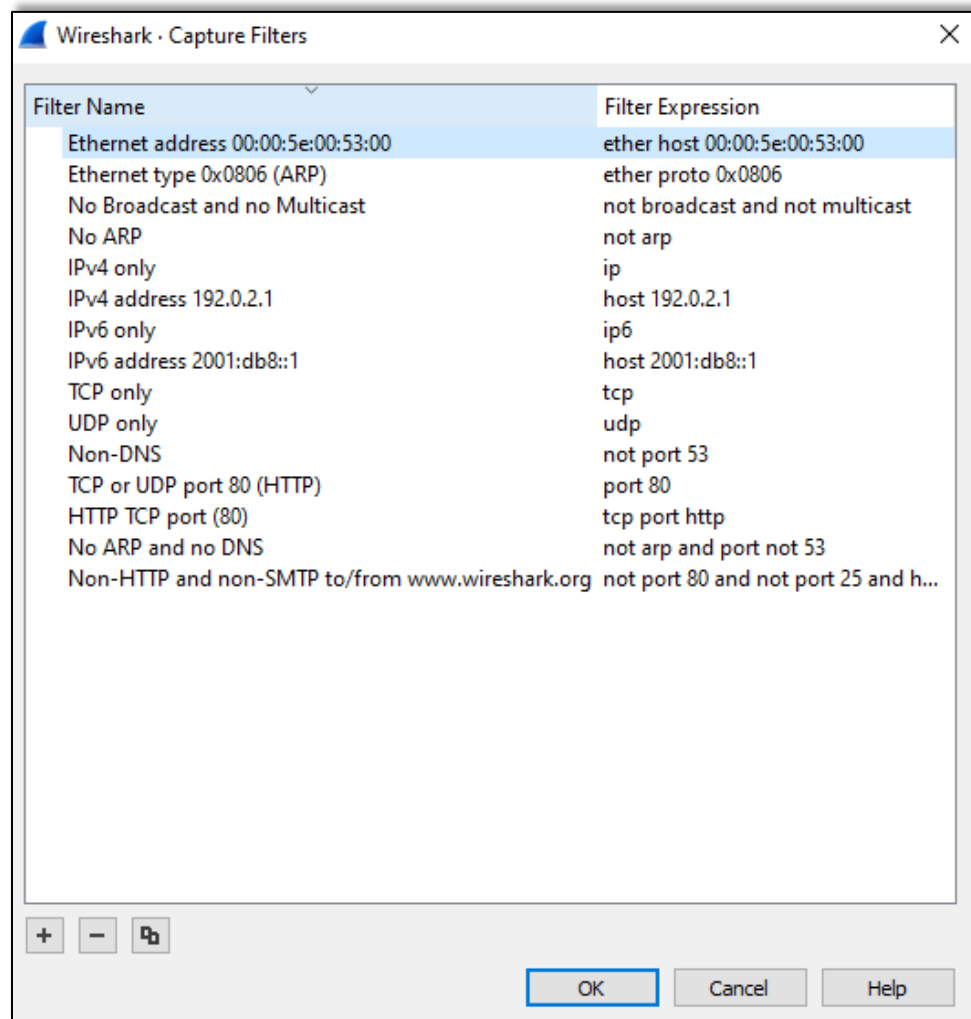
Comment définir un filtre pour la capture des trames

[Capture Filter]

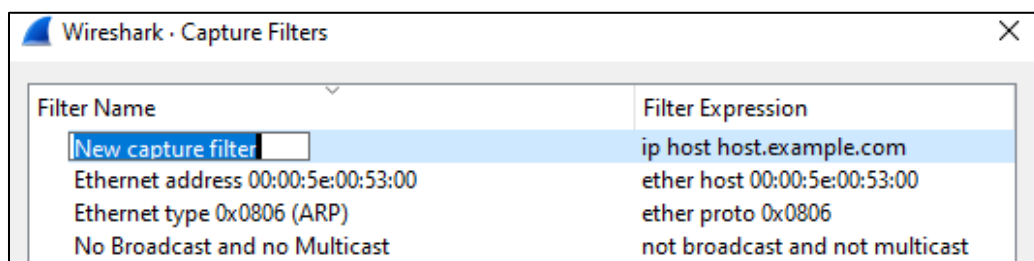
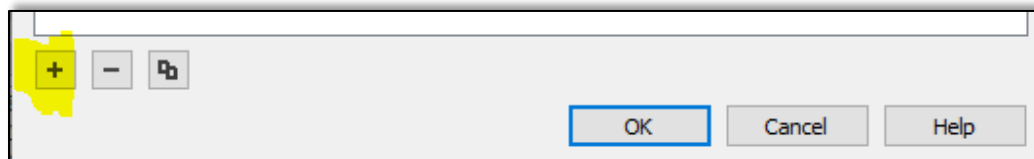
1 Allez dans le menu "Capture". Puis cliquez sur « Capture Filters ».



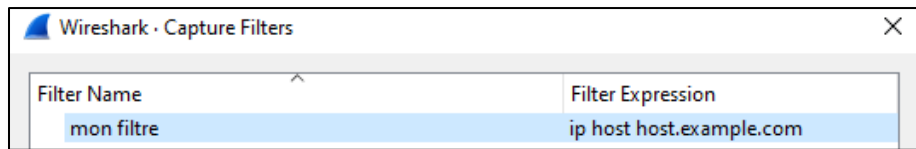
2 La fenêtre suivante s'ouvre.



3 Cliquez sur « + » (Create a new filter)

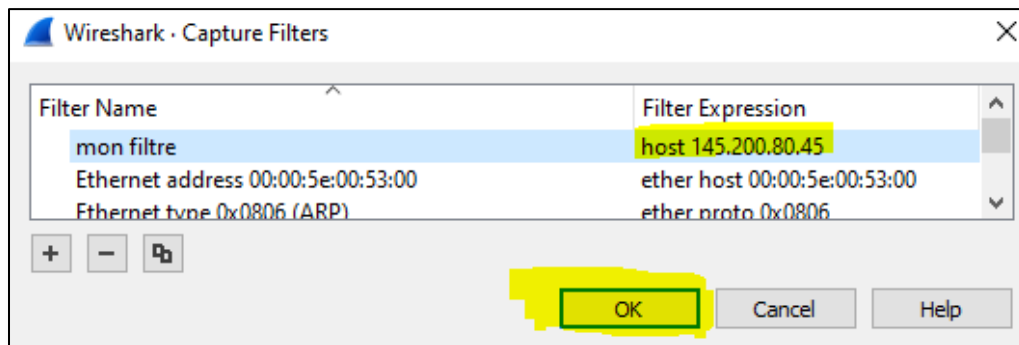


- ✚ Dans le champ "Filter Name"
entrez le nom de votre filtre : mon filtre (par exemple).



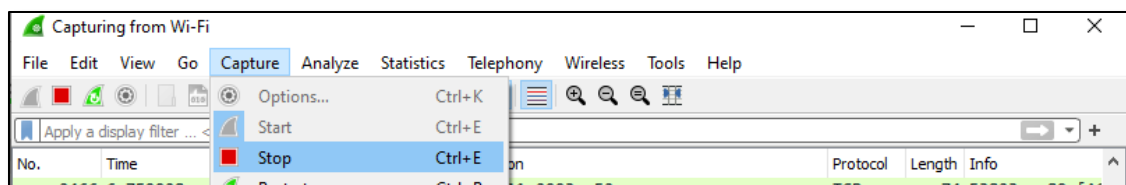
- ✚ Dans le champ "Filter Expression"
entrez la chaîne suivante : **host 145.200.80.45**

Considérons que notre machine à l'adresse IP **192.168.1.33**.
Nous voulons capturer uniquement les trames échangées entre celle-ci et la machine avec l'adresse IP **145.200.80.45**.

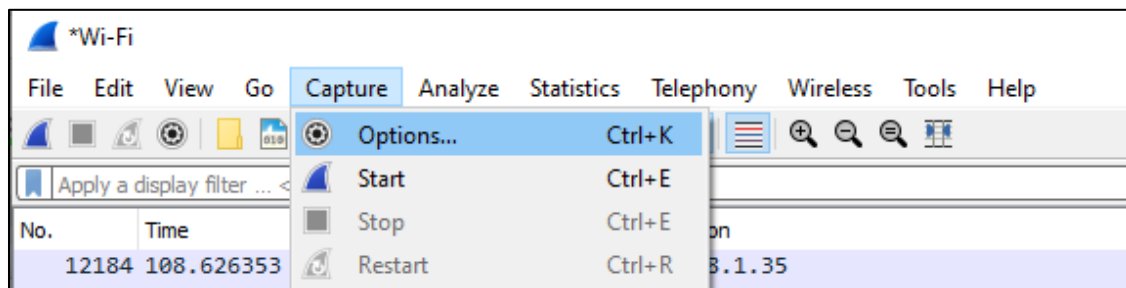


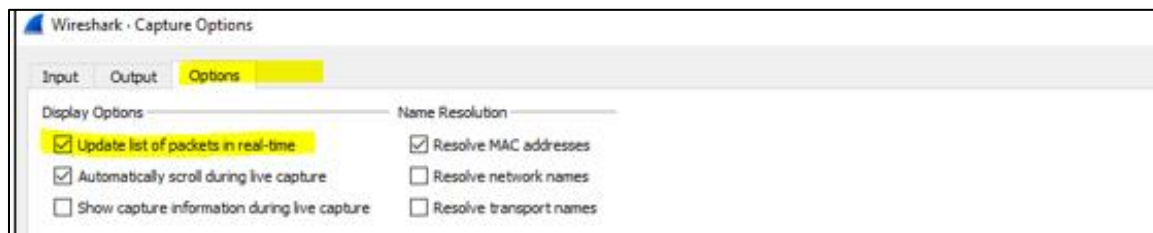
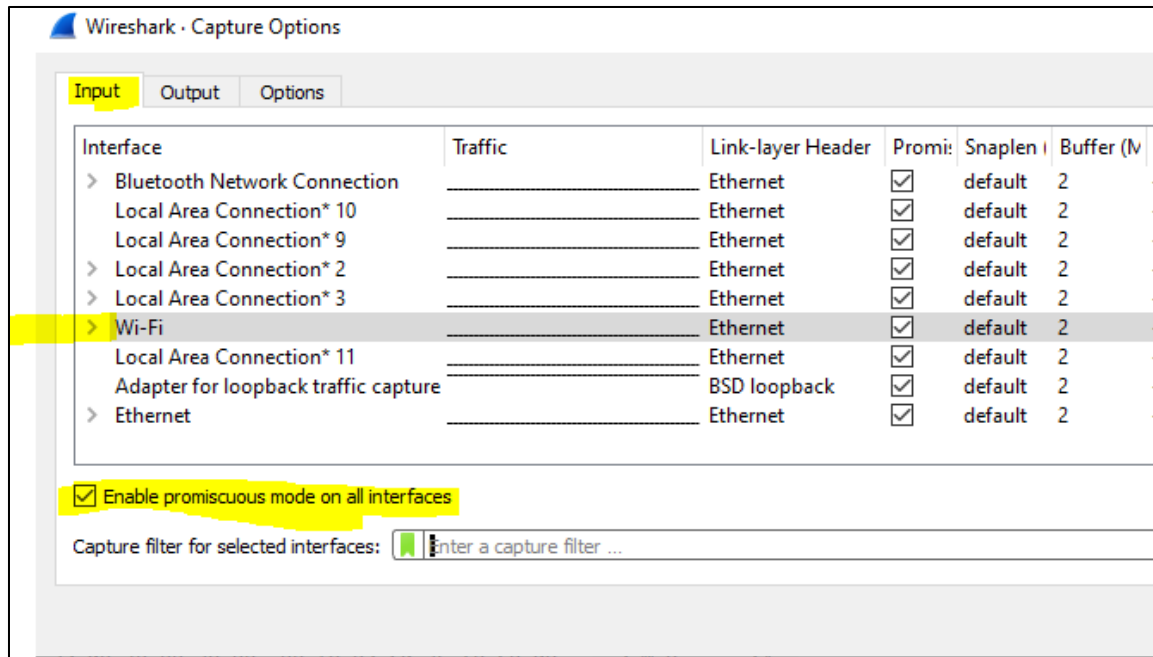
- ✚ Cliquez maintenant sur "save" et voilà votre filtre est défini.

- ✚ Retournez dans le menu "Capture" et cliquez sur "Stop".

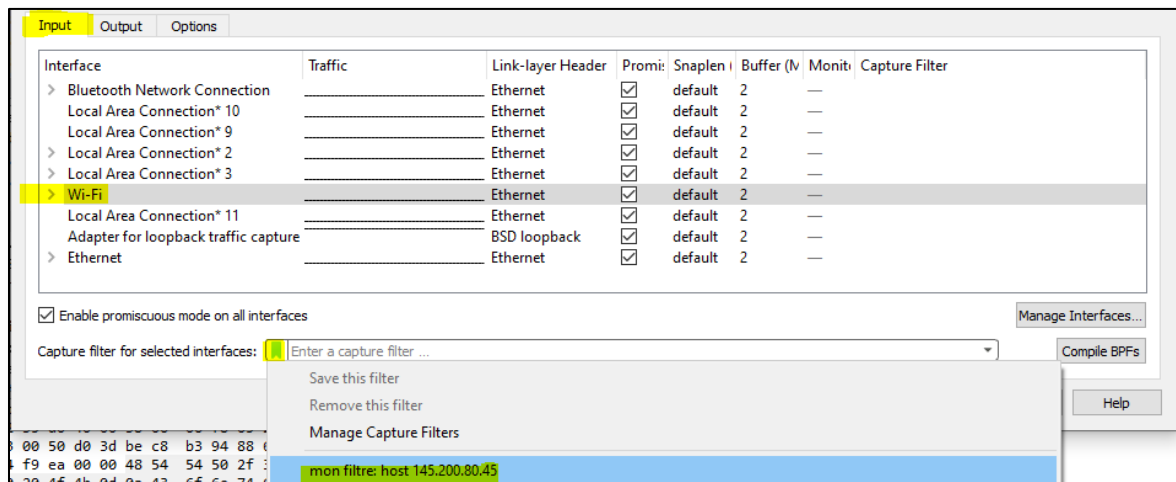


- ✚ Reprenez les mêmes options que précédemment.

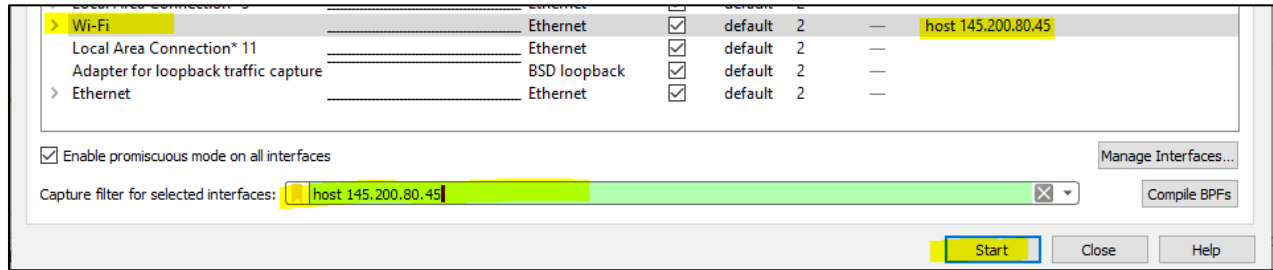




Cliquez sur le bouton "Capture Filter" et sélectionnez votre filtre.



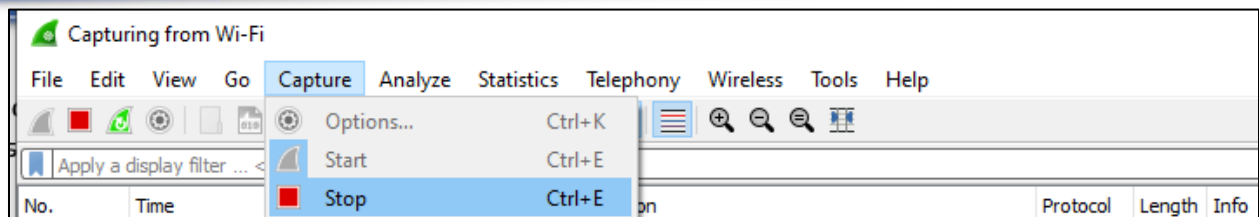
Cliquez sur le bouton "Start" pour démarrer la capture avec le filtre en question.



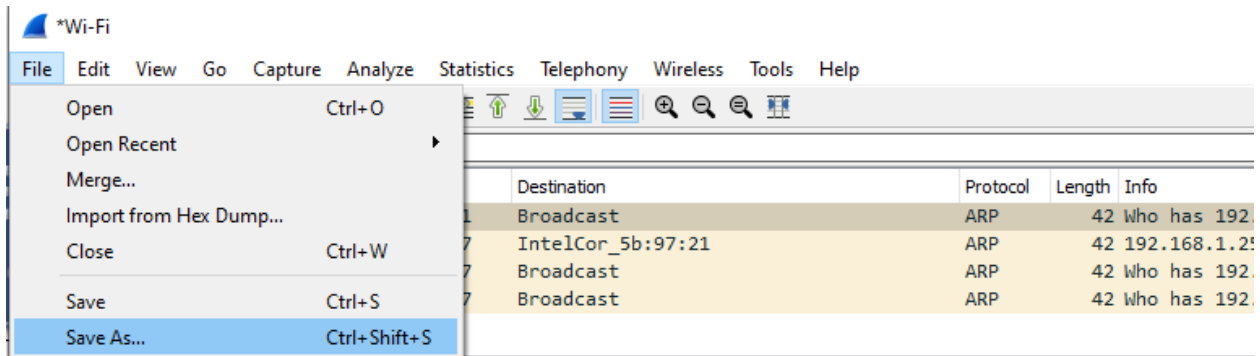
Pour plus de détail sur la structure des filtres vous pouvez consulter l'aide en appuyant sur la touche F1 et en allant sur l'onglet "Capture Filter"

Etape 4

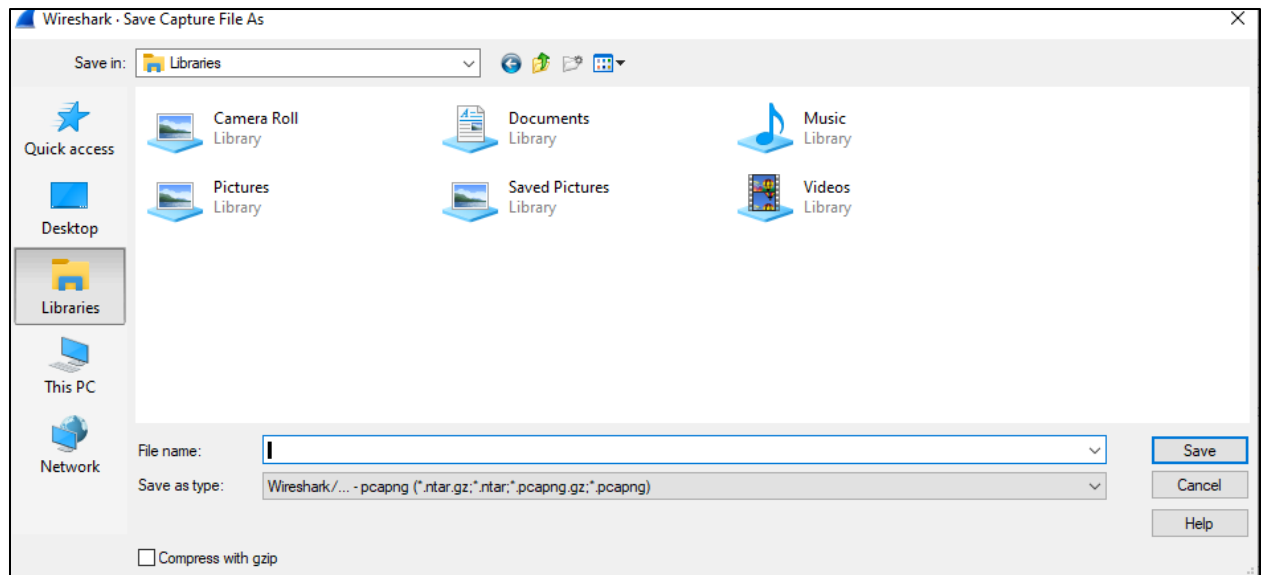
sauvegarde d'un résultat de capture



Pour sauvegarder le résultat d'une capture dans un fichier, il faut sélectionner la commande « Save as » dans le menu « File ».



Une fenêtre nous proposer de choisir le répertoire et le nom du fichier.



Etape 5

Répondre aux questions suivantes

5.2/ taper sur la console de l'ordinateur 1 la commande « ifconfig »
[voir le manuel man pour la syntaxe de la commande ifconfig]

LINUX

Il faut taper la commande « `$ifconfig -a` » pour obtenir les différents paramètres de configuration réseaux

WINDOWS

Il faut taper la commande `ipconfig /all`

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165  
Physical Address. . . . . : 58-FB-84-5B-97-21  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
IPv6 Address. . . . . : 2a01:e0a:441:baf0:750a:fed2:56f9:4439(Preferred)  
Temporary IPv6 Address. . . . . : 2a01:e0a:441:baf0:dd60:768a:653e:8f42(Deprecated)  
Temporary IPv6 Address. . . . . : 2a01:e0a:441:baf0:e4a0:2d06:77a5:df6(Deprecated)  
Link-local IPv6 Address . . . . . : fe80::750a:fed2:56f9:4439%14(Preferred)  
IPv4 Address. . . . . : 192.168.1.35(Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Tuesday, December 8, 2020 10:20:36 PM  
Lease Expires . . . . . : Saturday, December 12, 2020 10:47:43 AM  
Default Gateway . . . . . : fe80::8e97:eaff:fe35:9e27%14  
                            192.168.1.254  
DHCP Server . . . . . : 192.168.1.254  
DHCPv6 IAID . . . . . : 123272068  
DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-B0-BF-7A-18-DB-F2-3C-D6-56  
DNS Servers . . . . . : 192.168.1.254  
NetBIOS over TcpiP. . . . . : Enabled
```

➤ Combien d'interfaces trouvez-vous ?

LINUX

Nous trouvons deux interfaces « eth0 » et « lo »

WINDOWS

Nous avons 4 interfaces : Wifi, Bluetooth, Ethernet, VPN

➤ A quoi correspond l'interface « eth0 », l'interface « lo » ?

L'interface **eth0** correspond à la première interface Ethernet du serveur.

L'interface « **lo** » correspond à l'interface de boucle locale (127.0.0.1) servant aux communications internes du terminal.

➤ Identifier les adresses Ethernet (eth0) du serveur.

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165  
Physical Address. . . . . : 58-FB-84-5B-97-21
```

➤ Identifier les adresses IP et le masque réseaux du serveur.

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 3165  
Physical Address. . . . . : 58-FB-84-5B-97-21  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
IPv6 Address. . . . . : 2a01:e0a:441:baf0:750a:fed2:56f9:4439(Preferred)  
Temporary IPv6 Address. . . . . : 2a01:e0a:441:baf0:dd60:768a:653e:8f42(Deprecated)  
Temporary IPv6 Address. . . . . : 2a01:e0a:441:baf0:e4a0:2d06:77a5:df6(Deprecated)  
Link-local IPv6 Address . . . . . : fe80::750a:fed2:56f9:4439%14(Preferred)  
IPv4 Address. . . . . : 192.168.1.35(Preferred)  
Subnet Mask . . . . . : 255.255.255.0
```

LINUX

Il faut ajouter l'option « **-a** » pour obtenir l'adresse physique (MAC)

WINDOWS

Il faut ajouter l'option « **/all** » pour obtenir l'adresse physique (MAC)

➤ Quel est le type d'adresse IP (publique/privée) utilisé par le serveur ?

IP PUBLIC vs IP PRIVE

→ **Site web : <http://monip.org/>**

L'adresse IP qu'on récupère est une adresse IP public. En tant que particulier on ne peut pas changer notre IP public.

→ **ipconfig**

L'adresse IP qu'on récupère en t'appelant ipconfig : Adresse IP privé qu'on a reçue de notre « BOX ».

Donc la box joue aussi un rôle de fournisseur d'IP privé sur notre LAN : donc elle fait le rôle d'un serveur DHCP – attribuer dynamiquement des adresse sur notre LAN. **Le routeur (la BOX) attribue dynamiquement des IP au différent terminaux et stations**

LINUX

IP privée de classe C

WINDOWS

IP privée de classe B

➤ Réitérer les mêmes opérations avec l'ordinateur 2

```

C:\>ipconfig /all

Wireless LAN adapter WiFi:

    Connection-specific DNS Suffix . . . : 
    Description . . . . . : Broadcom BCM43142 802.11 bgn Wi-Fi Adapter
    Physical Address. . . . . : D8-5D-E2-DF-84-B5
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2a01:e0a:441:baf0:518e:4b55:bd2:5004(Pref
erred)
    Temporary IPv6 Address. . . . . : 2a01:e0a:441:baf0:fc52:c80c:46f2:e5a(Pref
erred)
    Link-local IPv6 Address . . . . . : fe80::518e:4b55:bd2:5004%3(Preferred)
    IPv4 Address. . . . . : 192.168.1.24(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, December 12, 2020 11:12:03 AM
    Lease Expires . . . . . : Saturday, December 12, 2020 11:12:01 PM
    Default Gateway . . . . . : fe80::8e97:eaff:fe35:9e27%3
    . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.254
    DHCPv6 IAD . . . . . : 64511458
    DHCPv6 Client DUID. . . . . : 00-01-00-01-26-DF-E8-9A-D8-5D-E2-DF-84-B5

    DNS Servers . . . . . : 192.168.1.254
    NetBIOS over Tcpip. . . . . : Enabled
  
```

	Adresse IP	Masque	Adresse MAC
Ordinateur1	192.168.1.35	255.255.255.0	58-FB-84-5B-97-21
Ordinateur2	192.168.1.24	255.255.255.0	D8-5D-E2-DF-84-B5

5.4/ Sur le poste Ordinateur2, taper une commande de type « ping » à destination de l'ordinateur 1 et capturer environ 30 secondes de trafic sur l'ordinateur 1

Ping est une commande système qui permet de tester la disponibilité d'un hôte (PC, serveur, routeur, imprimante, ...) utilisant le protocole de communication IP. Ping transmet des requêtes ICMP (ICMP echo), et l'hôte distant doit répondre avec des réponses ICMP (ICMP reply)

```

C:\Users\admin>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\admin>
  
```

No.	Time	Source	Destination	Protocol	Length	Info
8	2.985218	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (no response found!)
9	7.944867	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (no response found!)
12	13.096103	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (no response found!)
18	17.975598	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (no response found!)

No.	Time	Source	Destination	Protocol	Length	Info
8	2.985218	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request
9	7.944867	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request
12	13.096103	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request
18	17.975598	192.168.1.24	192.168.1.35	ICMP	74	Echo (ping) request

No.	Time	Source	Destination
8	2.985218	192.168.1.24	192.168.1.35
9	7.944867	192.168.1.24	192.168.1.35
12	13.096103	192.168.1.24	192.168.1.35
18	17.975598	192.168.1.24	192.168.1.35

> Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
 > Ethernet II, Src: HonHaiPr_df:84:b5 (d8:5d:e2:df:84:b5), Dst: IntelCor_5b:97:2
 > Internet Protocol Version 4, Src: 192.168.1.24, Dst: 192.168.1.35

▼ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4d44 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 23 (0x0017)
 Sequence Number (LE): 5888 (0x1700)
 > [No response seen]
 ▼ Data (32 bytes)
 Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
 [Length: 32]

```

0000  58 fb 84 5b 97 21 d8 5d e2 df 84 b5 08 00 45 00  X·[!·] ······E·
0010  00 3c 2c 27 00 00 80 01 8b 0e c0 a8 01 18 c0 a8  ·<,'·····
0020  01 23 08 00 4d 44 00 01 00 17 61 62 63 64 65 66  ·#·MD· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

Etape 1 : Lancement des machines virtuelles VMWARE et de

Question 1

→ avec les adr

Combien de types d'adresses IP différentes connaissez-vous ?
Citez les et donnez un exemple pour chacun d'eux.

Question 2