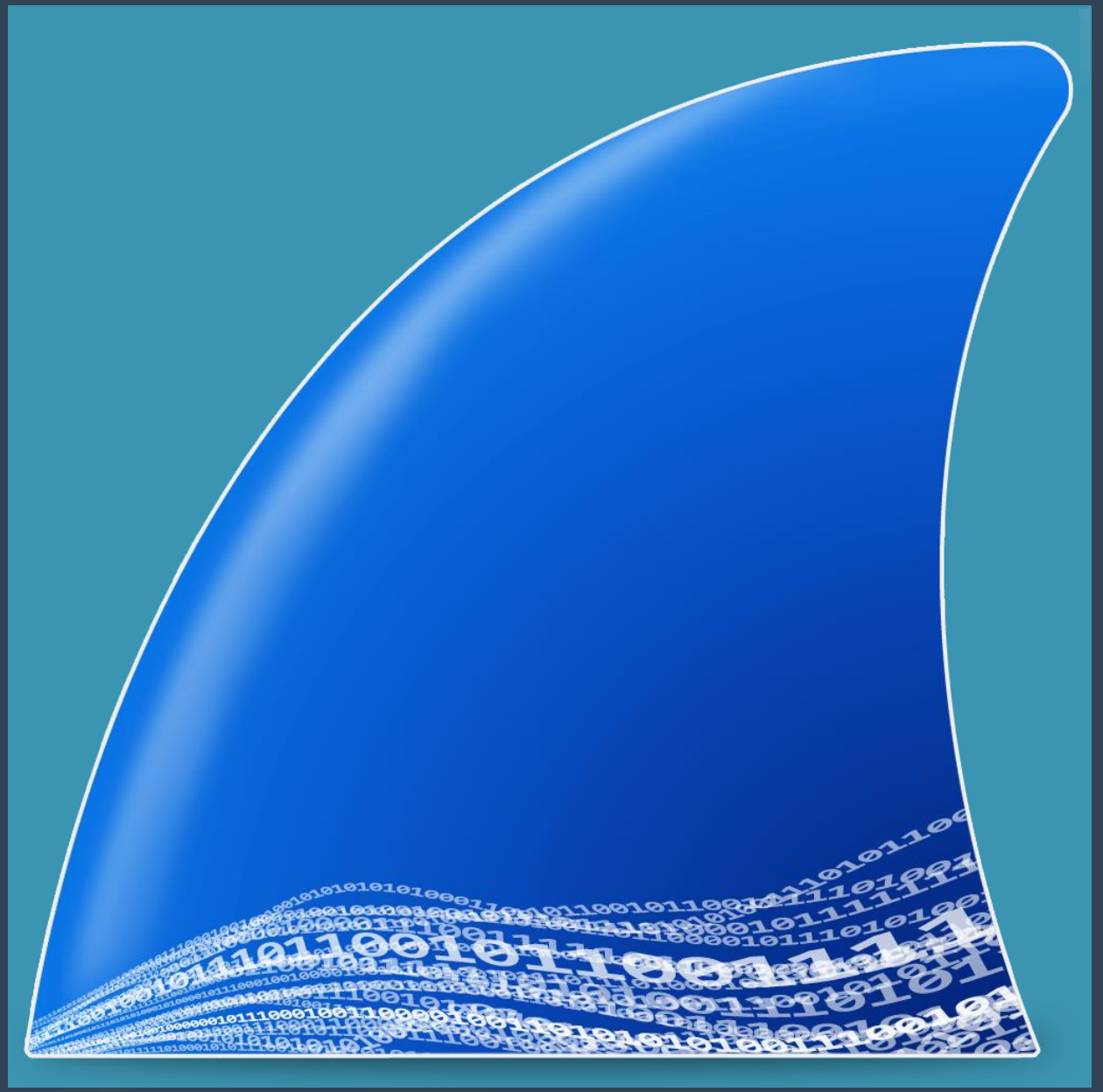
TP Wireshark

TRIOUX Jimmy – BTS SIO1

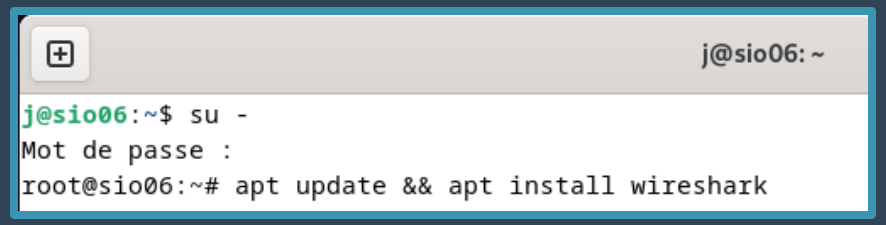
Qu’est-ce que Wireshark ?

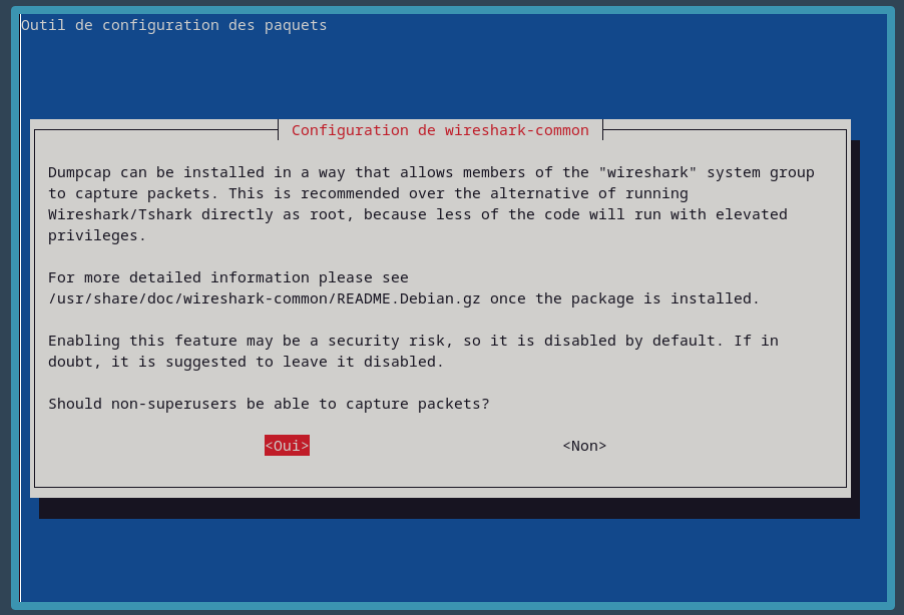
Wireshark est un logiciel gratuit qui permet d’analyser des paquets disponibles pour Windows, Mac, Unix et Linux.

Il est souvent utilisé dans le dépannage et l’analyse de réseaux informatiques, dans le développement de protocoles, dans l’éducation et dans la rétro-ingénierie.



Installation de Wireshark





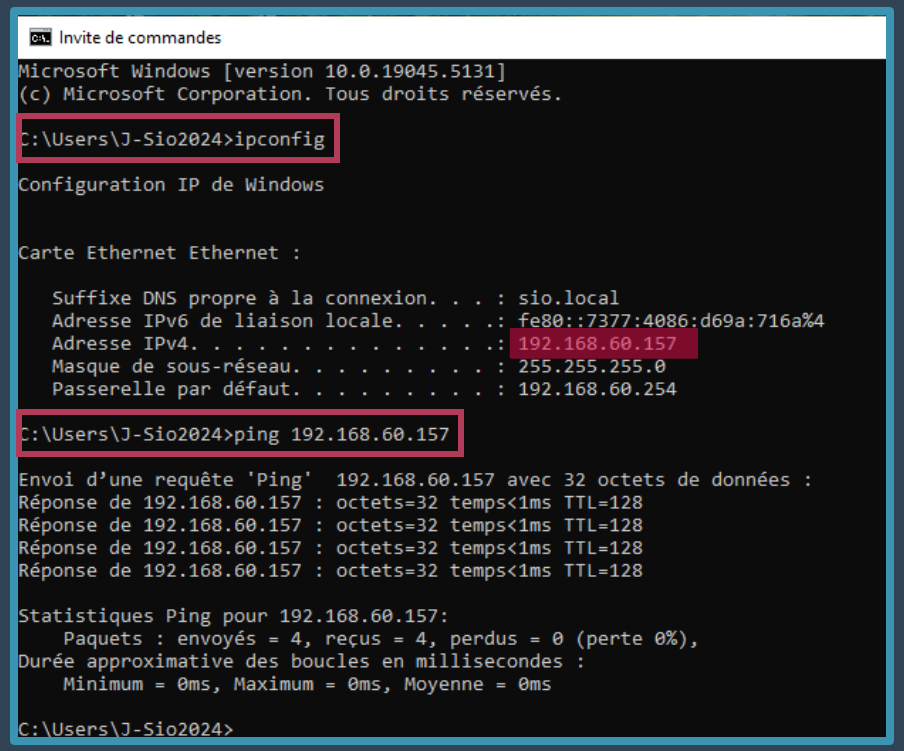
Pour installer Wireshark sur un système sous Linux, il faut d'abord se donner les droits de super-utilisateur puis rentrer la commande suivante : "**apt update && apt install wireshark**" pour mettre à jour les paquets puis de télécharger Wireshark.

Ensuite, on vous demandera si vous souhaitez que tous les utilisateurs puissent lire les trames.
Et enfin pour lancer wireshark, il suffit de rentrer simplement "**wireshark**".

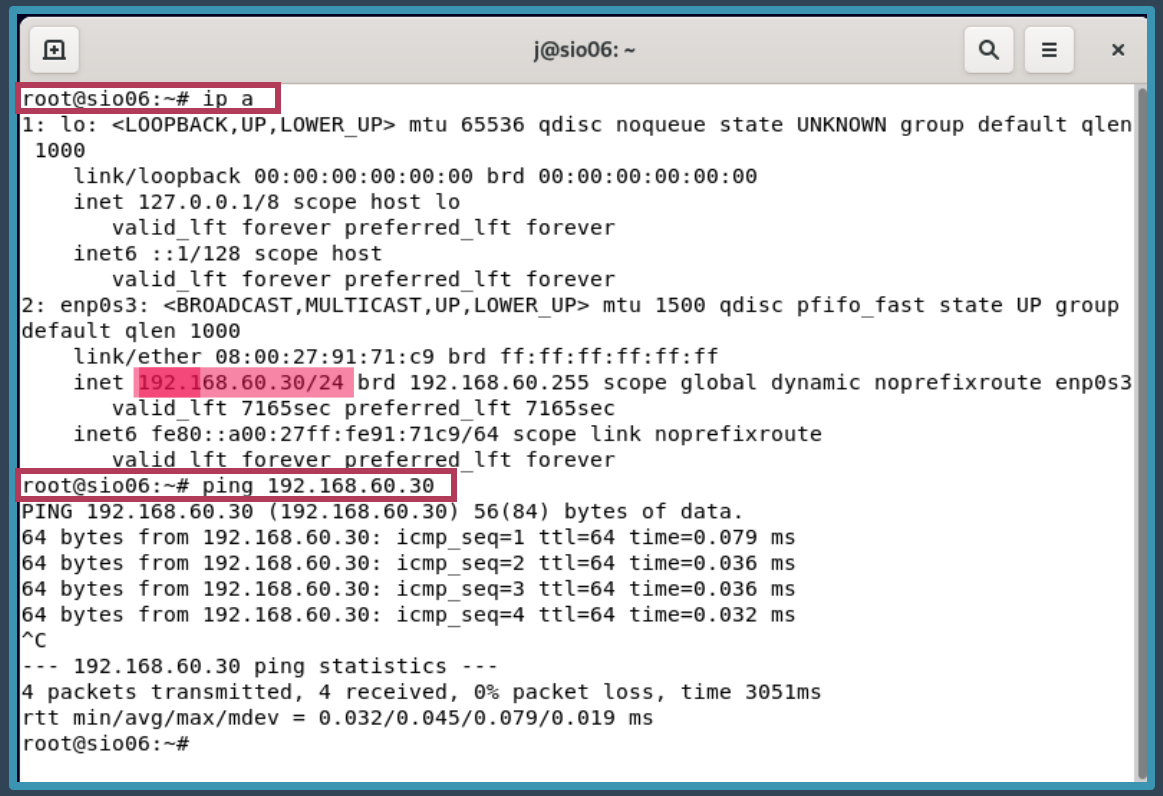
Pour Windows, aller sur le site :
https://www.wireshark.org/download.html

Puis sélectionner "Windows x64 Installer" et installer le logiciel en faisant suivant et en paramétrant selon vos exigences.

Vérifier la connectivité de son réseau

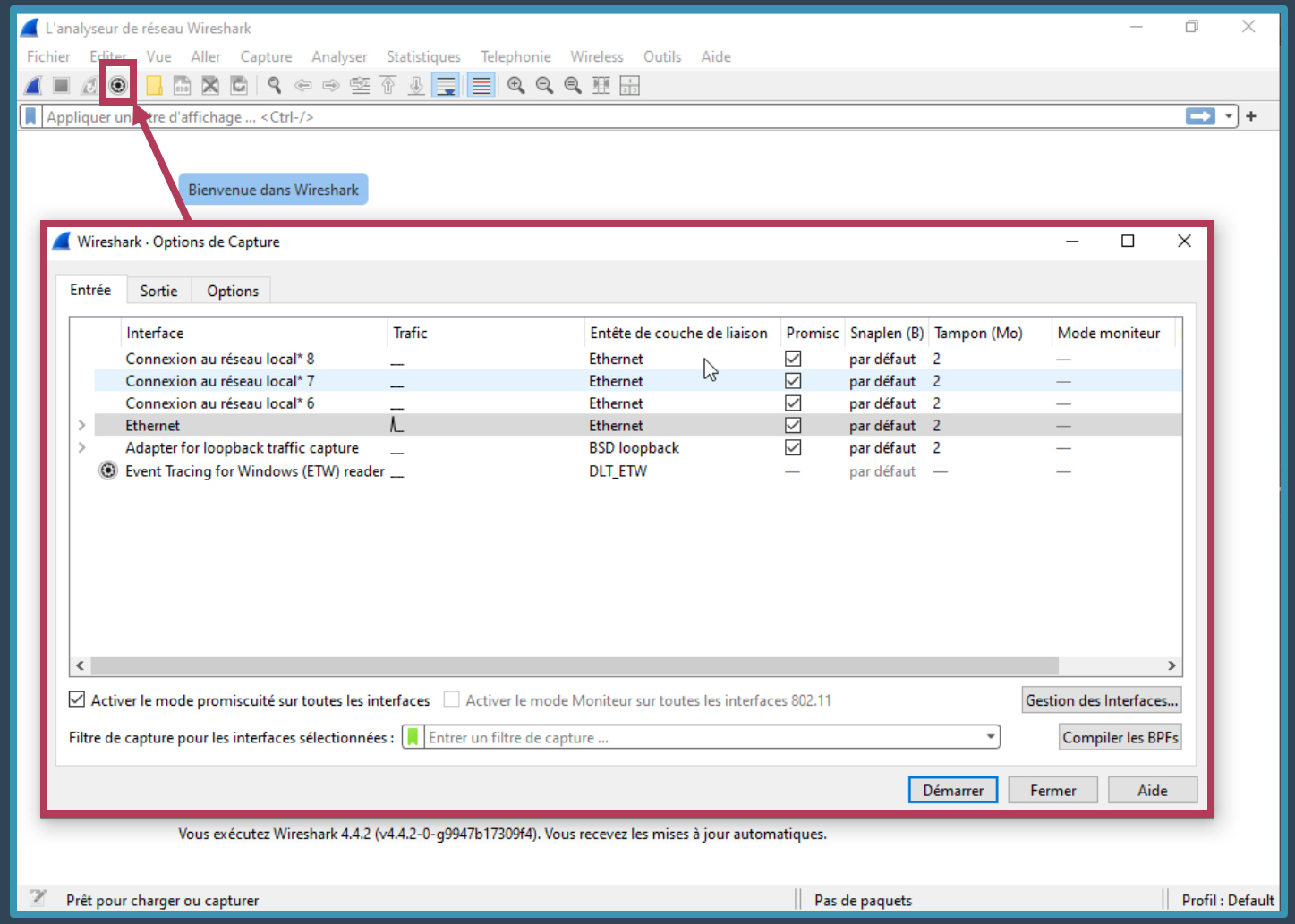


Aller dans l'invite de commande (se réitérer au TP découverte d'un réseau), puis faites une **ipconfig** afin de connaître votre adresse IP puis faites un ping sur cette même adresse.
Si les requêtes s'envoient alors le réseau est opérationnel.



Sous **Debian**, aller dans l'interface de commande puis taper « **ip a** » afin de connaître l'adresse IP puis comme sur Windows, faites un ping vers votre adresse IP, si les paquets s'envoient alors le réseau est opérationnel.

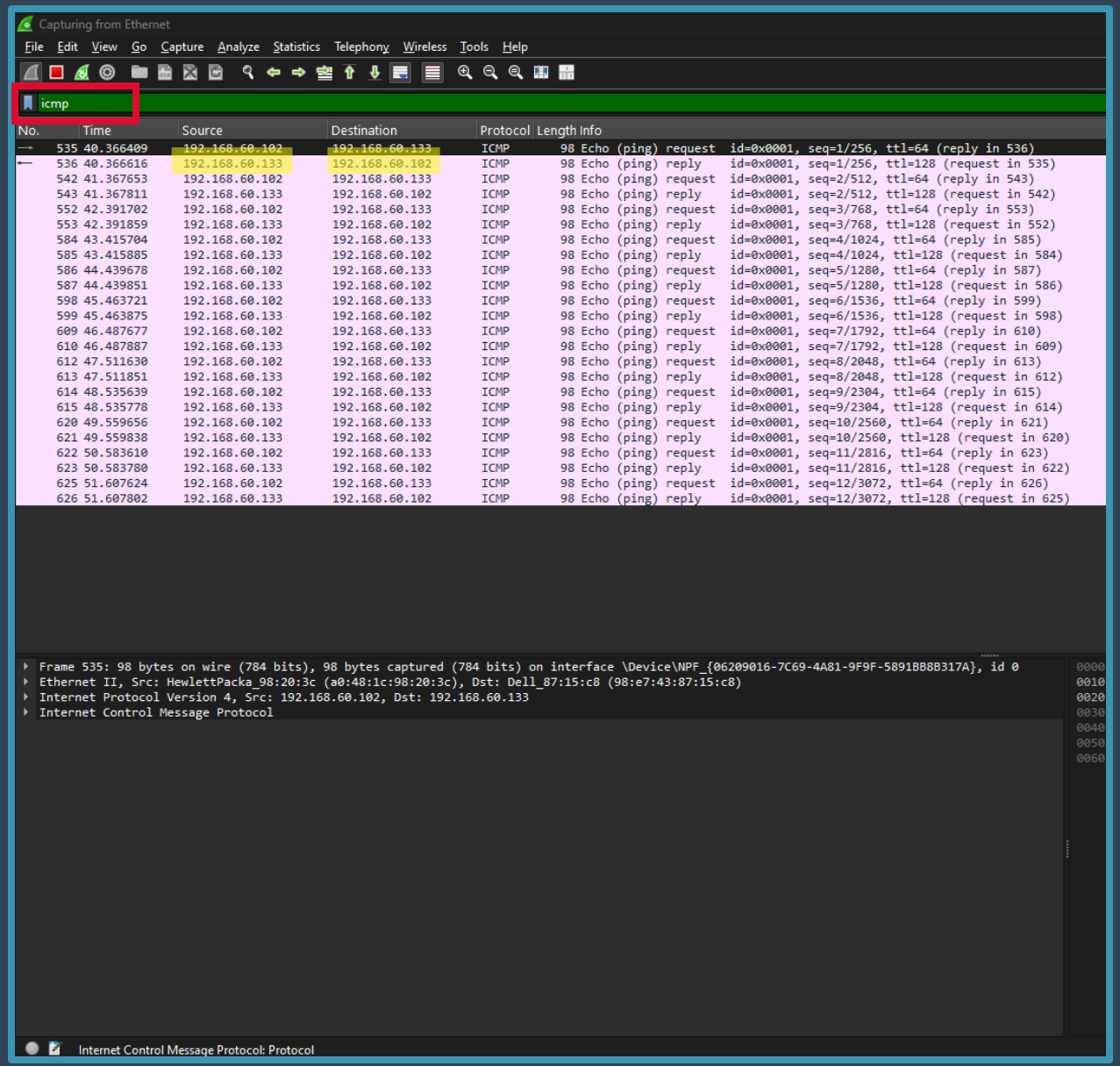
Utilisation de Wireshark



Dans un premier temps, cliquer sur l'icône ressemblant à une roue puis une fenêtre va apparaître.

Dans cette fenêtre, choisissez l'interface réseau que vous souhaitez sniffer.

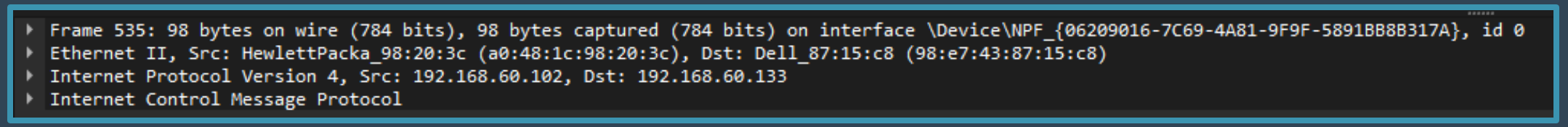
Filtrer sur Wireshark



Dans l'interface de réseau, nous allons filtrer pour ne recevoir que les pings en rentrant « **icmp** » dans la barre de recherche.

Comme nous pouvons le voir, je reçois des paquets de la source « **192.168.60.102** » vers mon adresse (**192.168.60.133**)

Analyse d’une trame

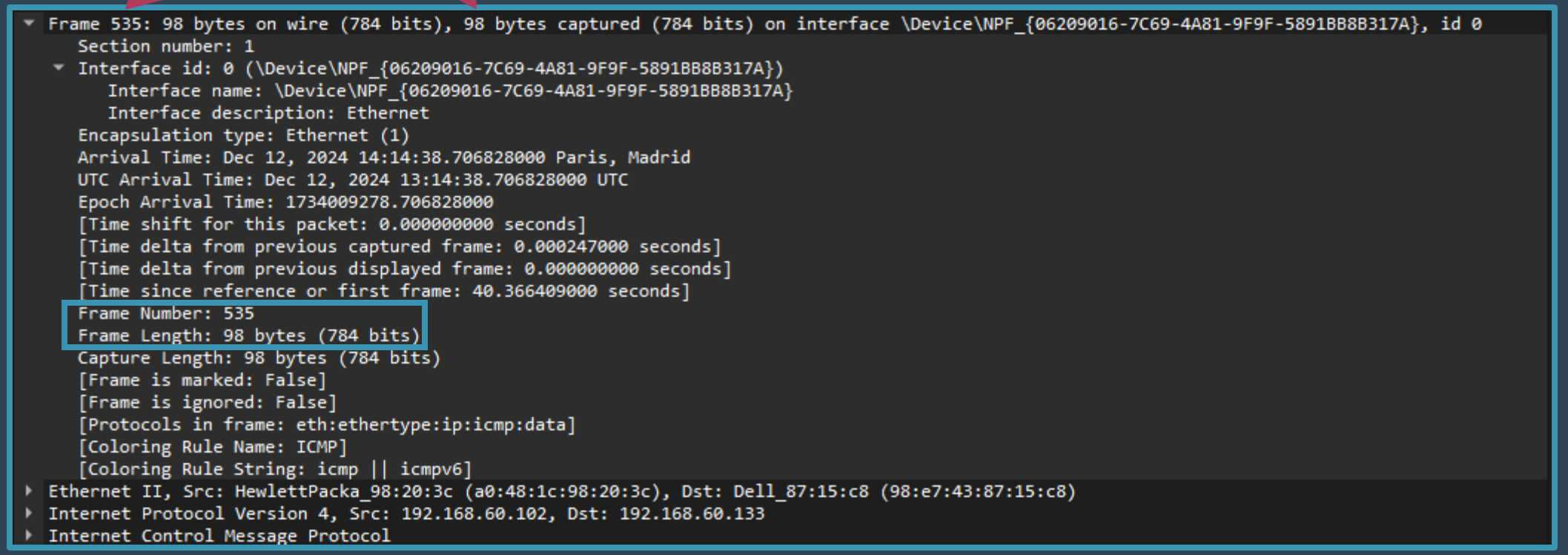


Voici la fenêtre d’analyse qui permet de récupérer diverses informations comme l’adresse MAC, l’adresse IP, le nom d’hôte, la taille des données et bien d’autres.

Nous allons pouvoir identifier l’adresse mac, l’adresse IP, l’heure, la date, et bien d’autres

Onglet Frame

Également visible ici.

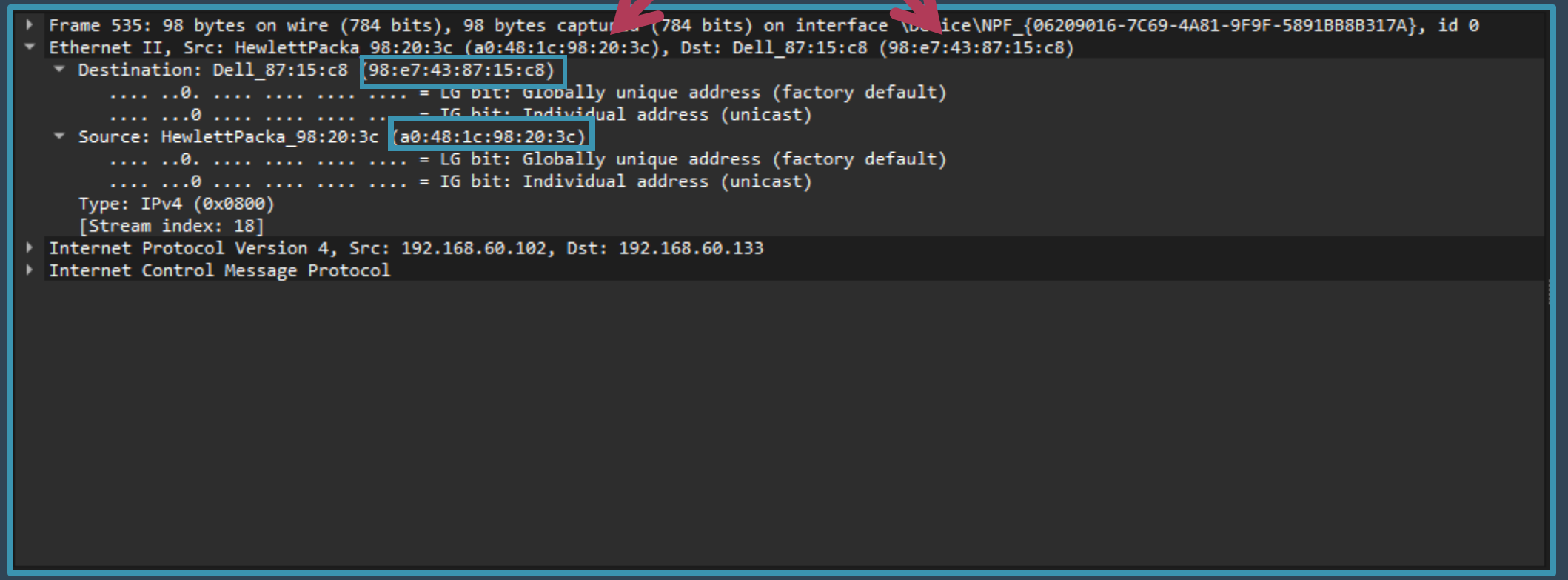


L'onglet Frame, nous renseigne sur la date et l'heure de capture du paquet selon l'horloge de l'ordinateur ainsi que sur la taille des données et son numéro.

Frame number : 535
Frame Length : 98 bytes (784 bits)

Onglet Ethernet II

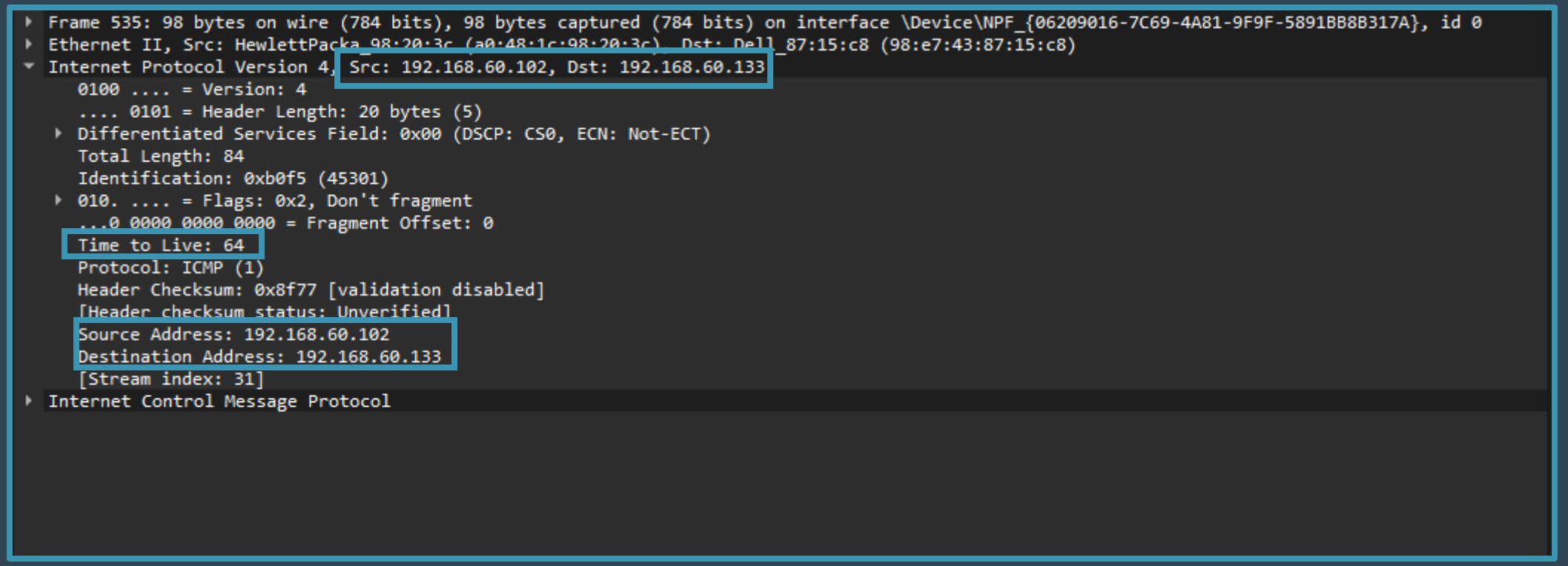
Également visible ici.



L'onglet Ethernet II permet d'avoir des informations sur l'adresse mac d'une source et de son destinataire.

Adresse mac source : a0:48:1c:98:20:3c
Adresse mac destinataire : 98:e7:43:87:15:c8

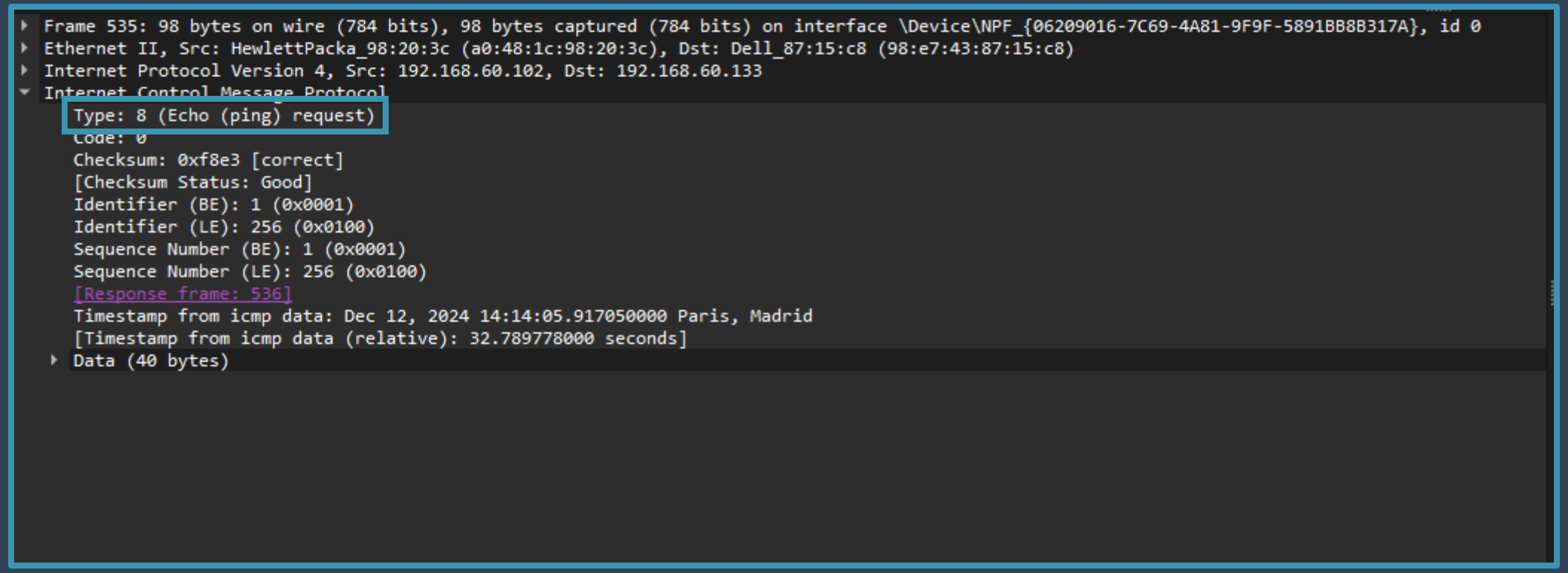
Onglet Internet Protocol Version 4



L'onglet Internet Protocol Version 4 permet d'avoir des informations sur l'adresse IP d'une source et de son destinataire ainsi que le time to live.

IP source : 192.168.60.102
IP destinataire : 192.168.60.133
Time to Live : 64

Onglet Internet Control Message Protocol



L'onglet Internet Control Message Protocol permet de récupérer le type de requête avec le code type ICMP.

Code type ICMP : 8 (Echo (ping) request)

Et si on modifiait l'adresse IP ?

L'onglet Internet Control Message Protocol permet de récupérer le type de requête avec le code type ICMP.

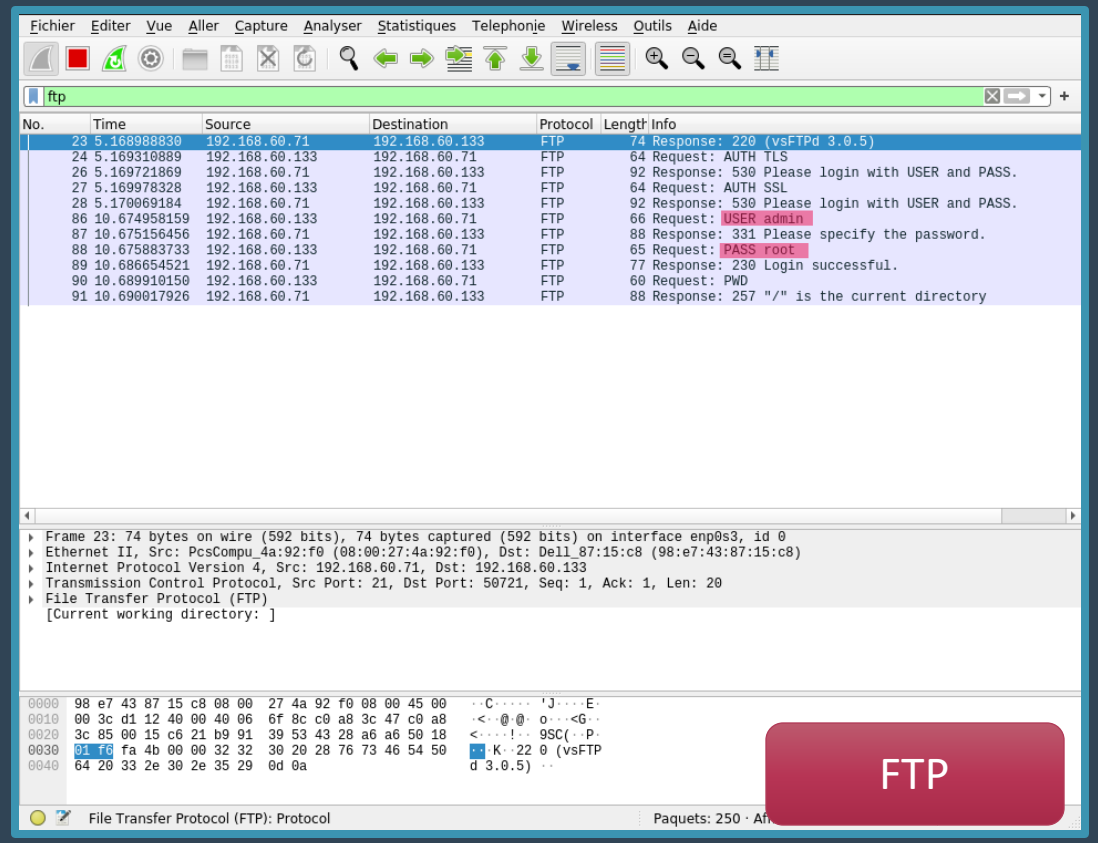
Code type ICMP : 8 (Echo (ping) request)

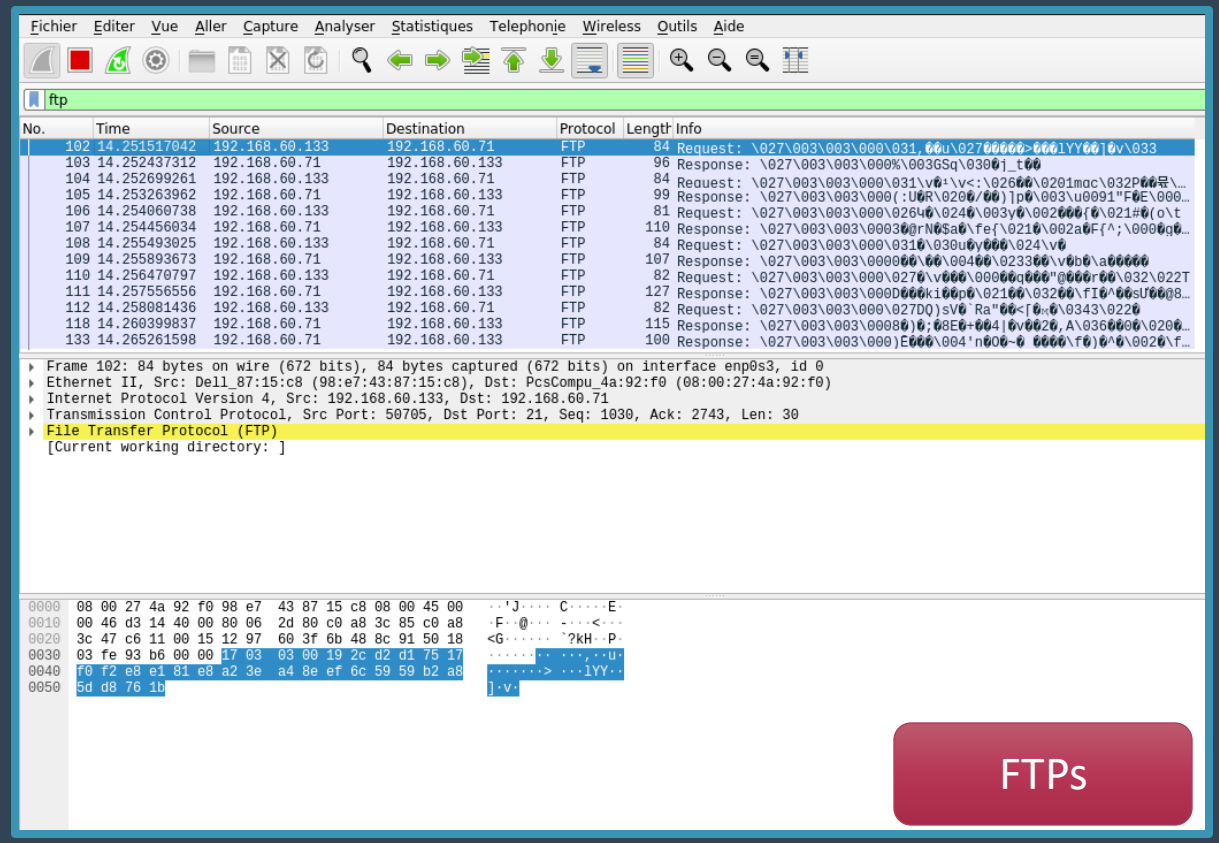
Différence HTTP/HTTPS

Sur un serveur FTP standard, l'accessibilité aux informations est non protégée, ce qui peut permettre à une personne mal intentionnée de récupérer des identifiants de connexion.

Le serveur FTPs, qui est chiffré par SSL, permet de crypter les données qui circulent. Ainsi, en reproduisant la même chose que sur un serveur non protégé, nous remarquons que les données sont sécurisées.

Différence serveur FTP sans/avec SSL





Sur un serveur FTP standard, l'accessibilité aux informations est non protégée, ce qui peut permettre à une personne mal intentionnée de récupérer des identifiants de connexion.

Le serveur FTPs, qui est chiffré par SSL, permet de crypter les données qui circulent. Ainsi, en reproduisant la même chose que sur un serveur non protégé, nous remarquons que les données sont sécurisées.