

TP Wireshark



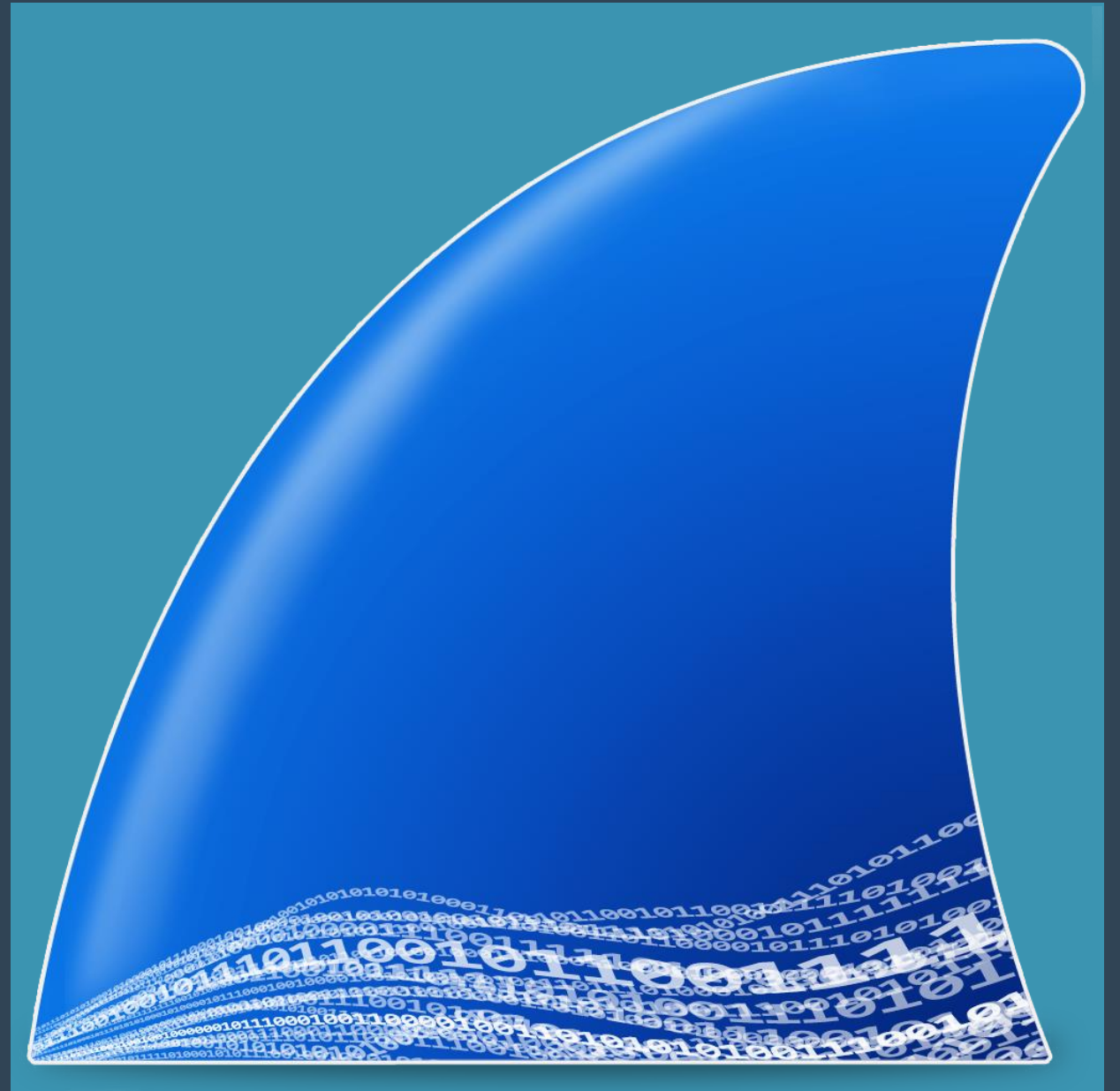
Qu'est-ce que Wireshark ?



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

```
j@sio06: ~  
j@sio06:~$ su -  
Mot de passe :  
root@sio06:~# apt update && apt install wireshark
```



```
Outil de configuration des paquets  
  
Configuration de wireshark-common  
  
Dumpcap can be installed in a way that allows members of the "wireshark" system group  
to capture packets. This is recommended over the alternative of running  
Wireshark/Tshark directly as root, because less of the code will run with elevated  
privileges.  
  
For more detailed information please see  
/usr/share/doc/wireshark-common/README.Debian.gz once the package is installed.  
  
Enabling this feature may be a security risk, so it is disabled by default. If in  
doubt, it is suggested to leave it disabled.  
  
Should non-superusers be able to capture packets?  
  
<Oui> <Non>
```

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

```
Invite de commandes
Microsoft Windows [version 10.0.19045.5131]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\J-Sio2024>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : sio.local
    Adresse IPv6 de liaison locale. . . . : fe80::7377:4086:d69a:716a%4
    Adresse IPv4. . . . . : 192.168.60.157
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.60.254

C:\Users\J-Sio2024>ping 192.168.60.157

Envoi d'une requête 'Ping' 192.168.60.157 avec 32 octets de données :
Réponse de 192.168.60.157 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.157 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.157 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.157 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.60.157:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\J-Sio2024>
```

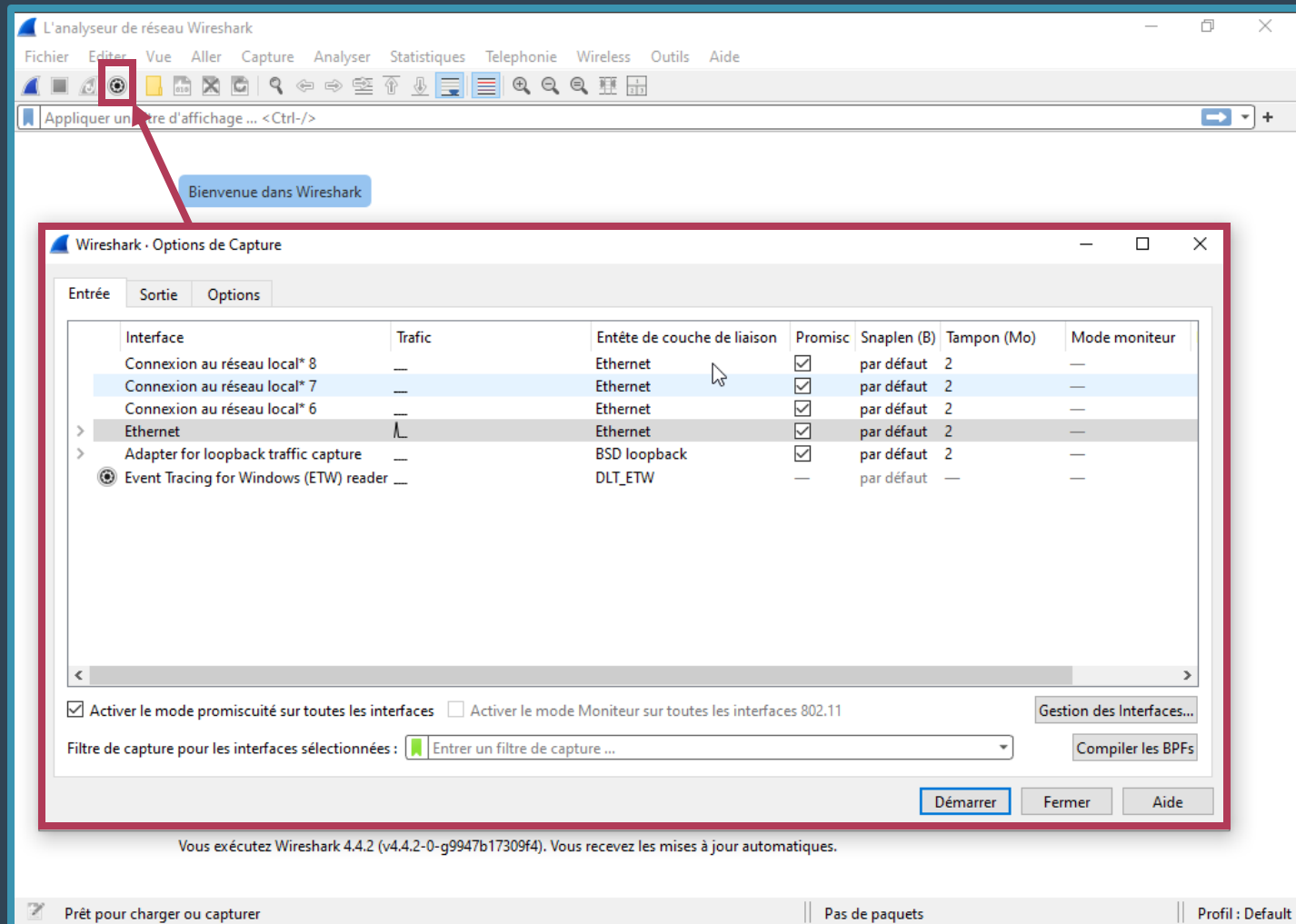
Aller dans l'invite de commande (se réitérer au TP découverte d'un réseau), puis faites une **ipconfig** afin de connaître votre adresse IP puis faites un ping sur cette même adresse. Si les requêtes s'envoient alors le réseau est opérationnel.

```
j@sio06: ~
root@sio06:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:91:71:c9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.30/24 brd 192.168.60.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7165sec preferred_lft 7165sec
    inet6 fe80::a00:27ff:fe91:71c9/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

root@sio06:~# ping 192.168.60.30
PING 192.168.60.30 (192.168.60.30) 56(84) bytes of data.
64 bytes from 192.168.60.30: icmp_seq=1 ttl=64 time=0.079 ms
64 bytes from 192.168.60.30: icmp_seq=2 ttl=64 time=0.036 ms
64 bytes from 192.168.60.30: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 192.168.60.30: icmp_seq=4 ttl=64 time=0.032 ms
^C
--- 192.168.60.30 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.032/0.045/0.079/0.019 ms
root@sio06:~#
```

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.

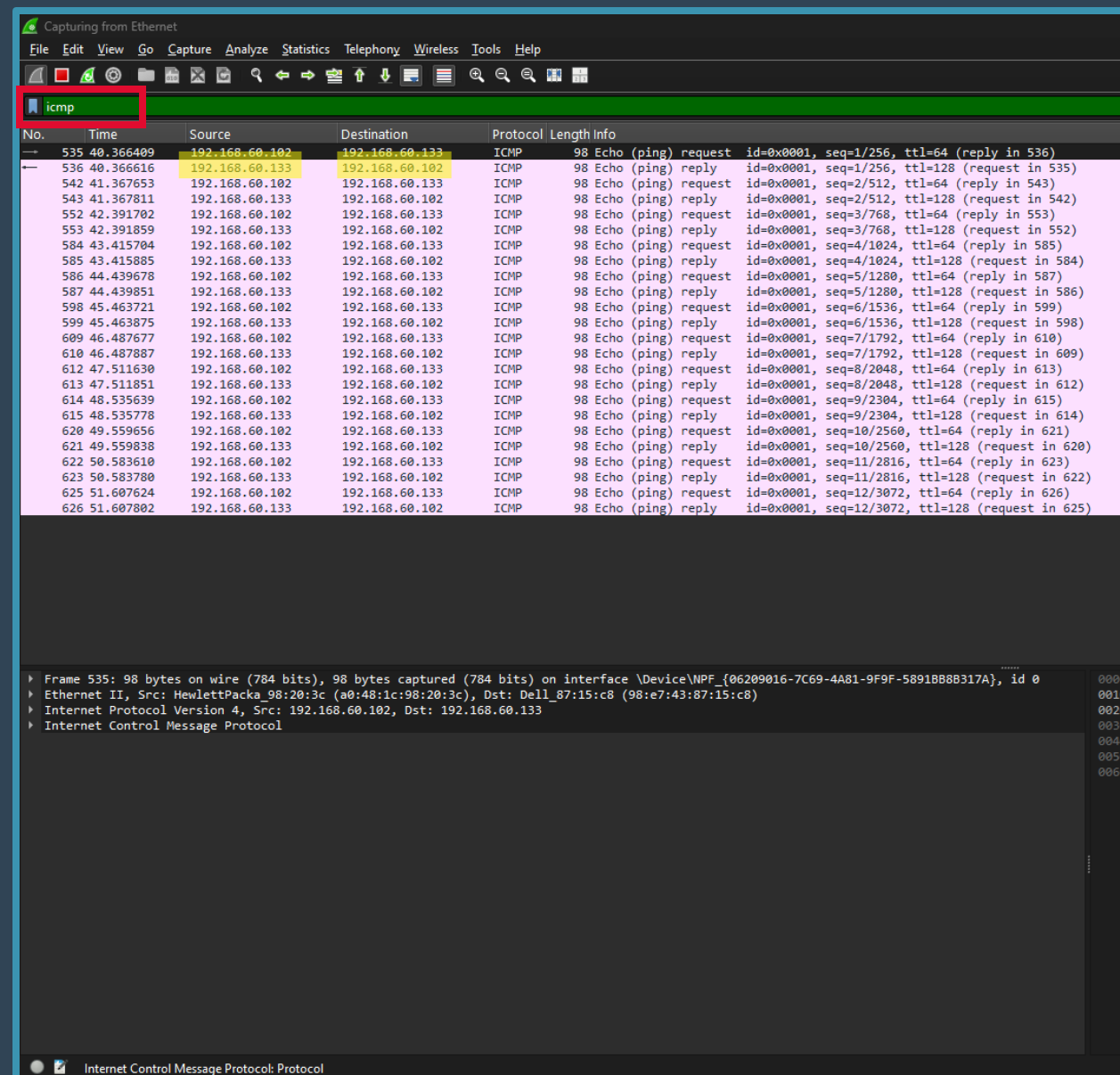
Utilisation de Wireshark



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

```
▶ Frame 535: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}, id 0
▶ Ethernet II, Src: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
▶ Internet Protocol Version 4, Src: 192.168.60.102, Dst: 192.168.60.133
▶ Internet Control Message Protocol
```

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

Également visible ici.

Onglet Frame

```
▼ Frame 535: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A})
    Interface name: \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}
    Interface description: Ethernet
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 12, 2024 14:14:38.706828000 Paris, Madrid
    UTC Arrival Time: Dec 12, 2024 13:14:38.706828000 UTC
    Epoch Arrival Time: 1734009278.706828000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000247000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 40.366409000 seconds]
    Frame Number: 535
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  ▶ Ethernet II, Src: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
  ▶ Internet Protocol Version 4, Src: 192.168.60.102, Dst: 192.168.60.133
  ▶ Internet Control Message Protocol
```

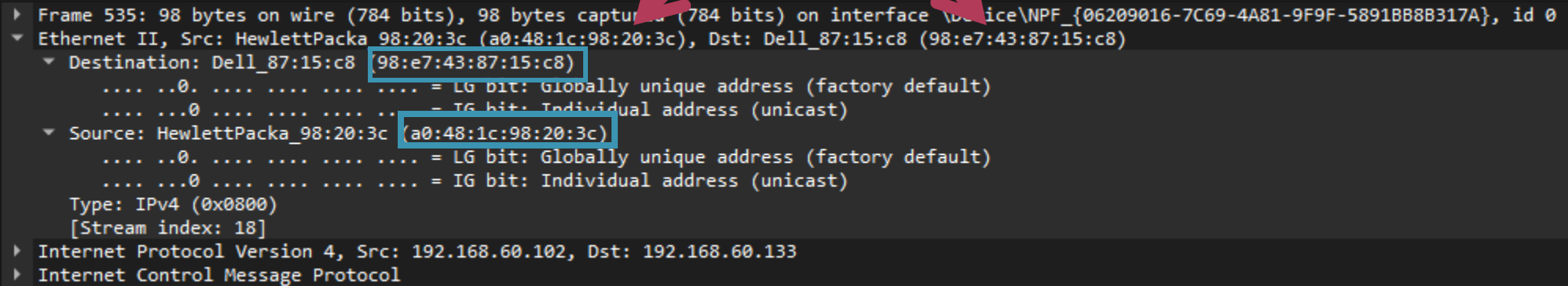
L'onglet Frame, nous renseigne sur la date et l'heure de capture du paquet selon l'horloge de l'ordinateur ainsi que sur la taille des données et son numéro.

Frame number : 535

Frame Length : 98 bytes (784 bits)

Onglet Ethernet II

Également visible ici.



```
▶ Frame 535: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}, id 0
▼ Ethernet II, Src: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
  ▼ Destination: Dell_87:15:c8 (98:e7:43:87:15:c8)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 18]
▶ Internet Protocol Version 4, Src: 192.168.60.102, Dst: 192.168.60.133
▶ Internet Control Message Protocol
```

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

```
▶ Frame 535: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}, id 0
▶ Ethernet II, Src: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
▼ Internet Protocol Version 4, Src: 192.168.60.102, Dst: 192.168.60.133
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xb0f5 (45301)
    ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x8f77 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.60.102
    Destination Address: 192.168.60.133
    [Stream index: 31]
▶ Internet Control Message Protocol
```

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

```
▶ Frame 535: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{06209016-7C69-4A81-9F9F-5891BB8B317A}, id 0
▶ Ethernet II, Src: HewlettPacka_98:20:3c (a0:48:1c:98:20:3c), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
▶ Internet Protocol Version 4, Src: 192.168.60.102, Dst: 192.168.60.133
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf8e3 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 1 (0x0001)
  Sequence Number (LE): 256 (0x0100)
  [Response frame: 536]
  Timestamp from icmp data: Dec 12, 2024 14:14:05.917050000 Paris, Madrid
  [Timestamp from icmp data (relative): 32.789778000 seconds]
▶ Data (40 bytes)
```

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

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide						
ftp						
No.	Time	Source	Destination	Protocol	Length	Info
23	5.168988830	192.168.60.71	192.168.60.133	FTP	74	Response: 220 (vsFTPd 3.0.5)
24	5.169310889	192.168.60.133	192.168.60.71	FTP	64	Request: AUTH TLS
26	5.169721869	192.168.60.71	192.168.60.133	FTP	92	Response: 530 Please login with USER and PASS.
27	5.169978328	192.168.60.133	192.168.60.71	FTP	64	Request: AUTH SSL
28	5.170069184	192.168.60.71	192.168.60.133	FTP	92	Response: 530 Please login with USER and PASS.
86	10.674958159	192.168.60.133	192.168.60.71	FTP	66	Request: USER admin
87	10.675156456	192.168.60.71	192.168.60.133	FTP	88	Response: 331 Please specify the password.
88	10.675883733	192.168.60.71	192.168.60.133	FTP	65	Request: PASS root
89	10.686654521	192.168.60.71	192.168.60.133	FTP	77	Response: 230 Login successful.
90	10.689910150	192.168.60.133	192.168.60.71	FTP	60	Request: PWD
91	10.690017926	192.168.60.71	192.168.60.133	FTP	88	Response: 257 "/" is the current directory

Frame 23: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_4a:92:f0 (08:00:27:4a:92:f0), Dst: Dell_87:15:c8 (98:e7:43:87:15:c8)
Internet Protocol Version 4, Src: 192.168.60.71, Dst: 192.168.60.133
Transmission Control Protocol, Src Port: 21, Dst Port: 50721, Seq: 1, Ack: 1, Len: 20
File Transfer Protocol (FTP)
[Current working directory:]

98 e7 43 87 15 c8 08 00 27 4a 92 f0 08 00 45 00 --C----- 'J---E-
0010 00 3c d1 12 40 00 00 06 6f 8c c0 a8 3c 47 c0 a8 <---@-@- o---<G-
0020 3c 85 00 15 c6 21 b9 91 39 53 43 28 a6 a6 50 18 <-----!-- 9SC(-P-
0030 01 76 fa 4b 00 00 32 32 30 20 28 76 73 46 54 50 K--22 0 (vsFTP
0040 64 20 33 2e 30 2e 35 29 0d 0a d 3.0.5) --

File Transfer Protocol (FTP): Protocol Paquets: 250 · Aff

FTP

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide						
ftp						
No.	Time	Source	Destination	Protocol	Length	Info
102	14.251517042	192.168.60.133	192.168.60.71	FTP	84	Request: \027\003\003\000\031,00u\02700000-0001YY00\0v\033
103	14.252437312	192.168.60.71	192.168.60.133	FTP	96	Response: \027\003\003\000%\0036Sq\0300j_t00
104	14.252699261	192.168.60.133	192.168.60.71	FTP	84	Request: \027\003\003\000\031\v0^v<:\02600\0201mac\032P000r\...
105	14.253263962	192.168.60.71	192.168.60.133	FTP	99	Response: \027\003\003\000(:U0R\0200/00)lp0\003\00091"F0E\000...
106	14.254060738	192.168.60.133	192.168.60.71	FTP	81	Request: \027\003\003\000\026u0\0240\003y0\002000f0\021#0(o\t
107	14.254456034	192.168.60.71	192.168.60.133	FTP	110	Response: \027\003\003\000300rN0Sa0\fe\0210\002a0Ff^;\000000...
108	14.255493025	192.168.60.133	192.168.60.71	FTP	84	Request: \027\003\003\000\0310\030u0y000\024\v0
109	14.255893673	192.168.60.71	192.168.60.133	FTP	107	Response: \027\003\003\00000000\00400\023300\v0b0\000000
110	14.256470797	192.168.60.133	192.168.60.71	FTP	82	Request: \027\003\003\000\0270\v000\000000000"0000r00\032\022T
111	14.257556556	192.168.60.71	192.168.60.133	FTP	127	Response: \027\003\003\000D000ki00p0\02100\03200\fi000sU0008...
112	14.258081436	192.168.60.133	192.168.60.71	FTP	82	Request: \027\003\003\000\02700)sV0 Ra"00<f0.0\0343\0220
118	14.260399837	192.168.60.71	192.168.60.133	FTP	115	Response: \027\003\003\00080)0;08E0+004\0v0020,A\036000\0200...
133	14.265261598	192.168.60.71	192.168.60.133	FTP	100	Response: \027\003\003\000)E000\004'n000-0 0000f0)0^0\0020\0f...

Frame 102: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface enp0s3, id 0
Ethernet II, Src: Dell_87:15:c8 (98:e7:43:87:15:c8), Dst: PcsCompu_4a:92:f0 (08:00:27:4a:92:f0)
Internet Protocol Version 4, Src: 192.168.60.133, Dst: 192.168.60.71
Transmission Control Protocol, Src Port: 50705, Dst Port: 21, Seq: 1030, Ack: 2743, Len: 30
File Transfer Protocol (FTP)
[Current working directory:]

0000 08 00 27 4a 92 f0 08 e7 43 87 15 c8 08 00 45 00 --'J--- C---E-
0010 00 46 d3 14 40 00 00 06 2d 80 c0 a8 3c 85 c0 a8 -F-@--- -<-<-
0020 3c 47 c6 11 00 15 12 97 60 3f 6b 48 8c 91 50 18 <G-----?kH-P-
0030 03 fe 93 b6 00 00 17 03 03 00 19 2c d2 d1 75 17-...-u-
0040 f0 f2 e8 e1 81 e8 a2 3e a4 8e ef 6c 59 59 b2 a8>-...1YY-
0050 5d d8 76 1b j-v-

FTPs

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.