SIO1
B1

Cuvilliez Antoine BTS SIO 1

TP- initiation wireshark

1 – Téléchargement de Wireshark

On télécharge Wireshark sur le site officiel :

Wireshark

2- Vérifications de la bonne connectivité du réseau

Il est nécessaire de vérifié la bonne connectivité du réseau, pour cela il faut connaitre l'adresse IP de notre machine (cf TP adressage IP) donc on ouvre un invite de commande et on tape la commande ipconfig.

```
C:\Users\HP>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : sio.local
   Adresse IPv6 de liaison locale. . . . .: fe80::edee:c105:bbbe:fadd%14
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.60.39
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.60.254

Carte Ethernet VirtualBox Host-Only Network :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::3d6c:c2be:5a39:a5e9%16
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

On peux ensuite taper la commande ping suivie de l'adresse IP trouvé précédemment. La commande répond donc une sommes bien connecter au réseau.

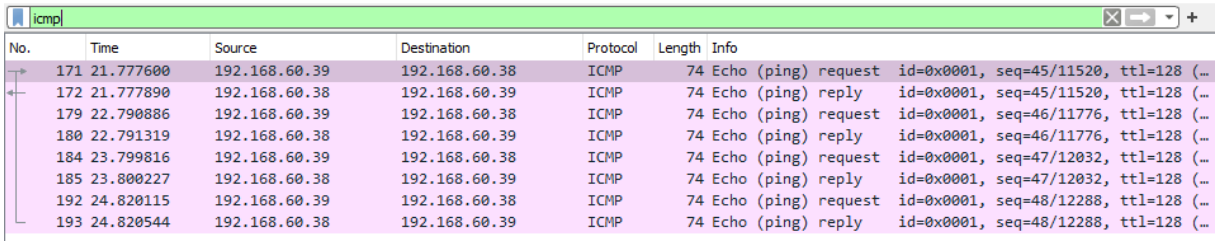
```
C:\Users\HP>ping 192.168.60.39

Envoi d'une requête 'Ping'  192.168.60.39 avec 32 octets de données :
Réponse de 192.168.60.39 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.39 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.39 : octets=32 temps<1ms TTL=128
Réponse de 192.168.60.39 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.60.39:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

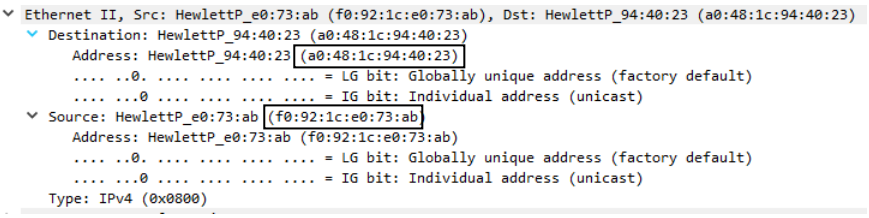
3- Utilisation de Wireshark

On lance une capture des paquets puis on ping nos machines dans l'invite de commande, ensuite on filtre par protocole ICMP (Internet Control Message Protocol)



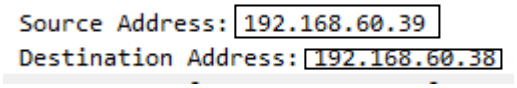
Adresse MAC source et destinataire :

(identifiant physique stocké dans la carte réseau)



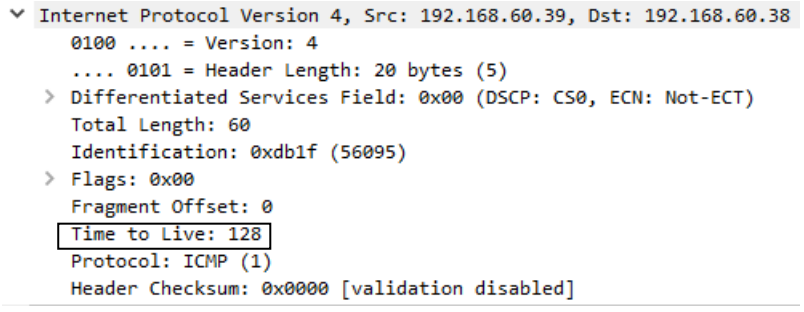
Adresse IP source et destinataire :

(numéro d'identification attribué à chaque Périphérique informatique du réseau)



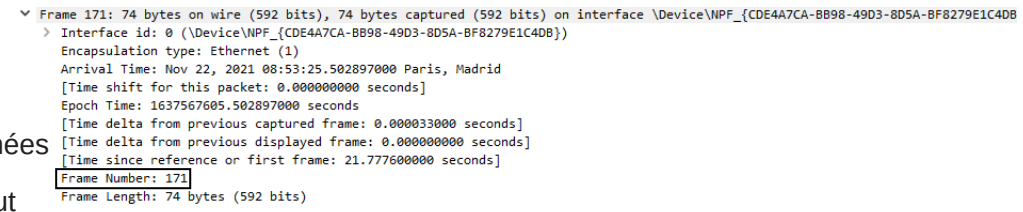
Time to live :

(temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache)



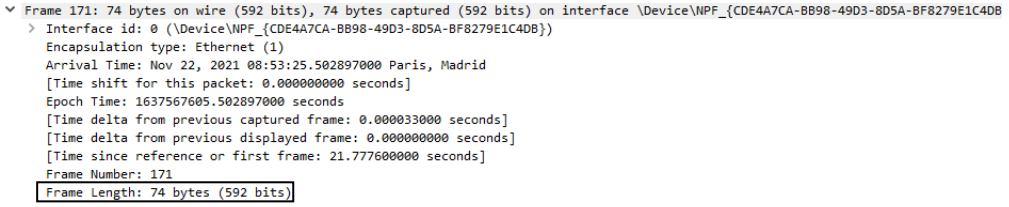
Numéro de la trame :

(numéro de la structure de base d'un ensemble de données encadré par des bits de début et des bits de fin)

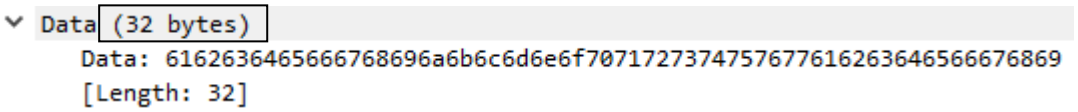


Taille de la trame :

(taille de la structure de base d'un ensemble de données encadré par des bits de début et des bits de fin)

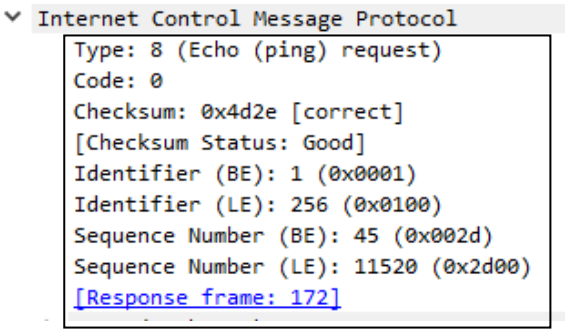


Taille des données :



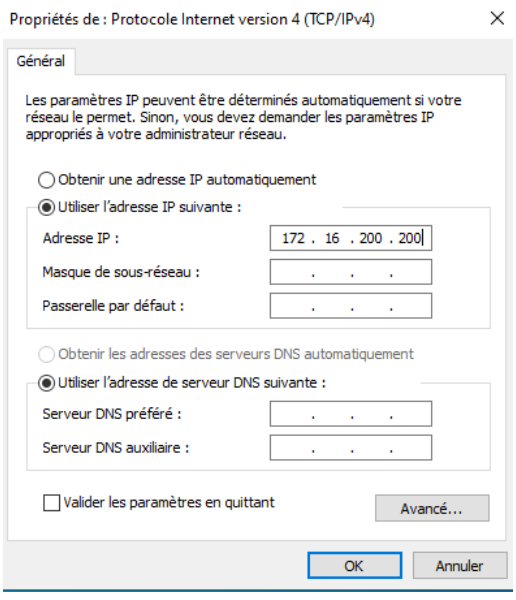
Code type ICMP :

(code du protocole de signalement d'erreurs)



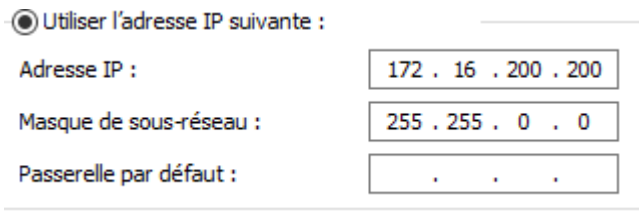
4 – Modifications des paramètres IP

On modifie les paramètres IP dans les propriétés du Protocol internet TCP/IPv4 :

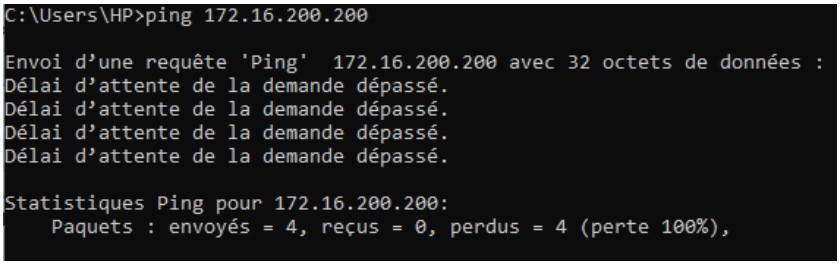


La commande ping ne trouve pas l'hote (erreur), il est nécessaire d'indiquer le masque de sous réseau.

On indique le masque de sous-réseau, soit 255.255.0.0 puis on relance une commande ping 172.16.200.200 :



La commande est fonctionnelle

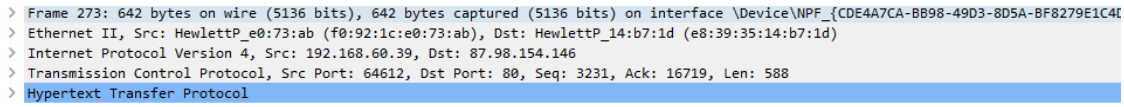


On sait que le masque de sous-réseau est utilisé par le protocole TCP/IP pour déterminer si un hôte se trouve sur le sous-réseau local ou sur un réseau distant. Ici on se trouve sur un réseau local alors il est nécessaire d'indiqué ce masque de sous-réseau.

5 – Analyse du protocole http et https

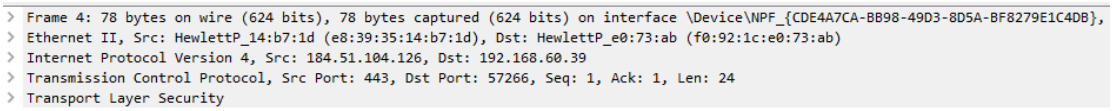
Voici plusieurs trame lors de la visite du site http btssio.fr :

No.	Time	Source	Destination	Protocol	Length	Info
310	12.807278	87.98.154.146	192.168.60.39	HTTP	1514	Continuation
311	12.807278	87.98.154.146	192.168.60.39	HTTP	69	Continuation
316	13.038724	192.168.60.39	87.98.154.146	HTTP/J…	781	POST /lib/ajax/service.php?sesskey=I4JVrUUE7u&inf…
317	13.040523	192.168.60.39	87.98.154.146	HTTP/J…	794	POST /lib/ajax/service.php?sesskey=I4JVrUUE7u&inf…
320	13.149378	87.98.154.146	192.168.60.39	HTTP/J…	464	HTTP/1.1 200 OK , JavaScript Object Notation (app…
321	13.163308	87.98.154.146	192.168.60.39	HTTP/J…	463	HTTP/1.1 200 OK , JavaScript Object Notation (app…
362	14.301524	192.168.60.39	87.98.154.146	HTTP	769	POST /login/logout.php HTTP/1.1 (application/x-w…
372	14.408858	87.98.154.146	192.168.60.39	HTTP	1021	HTTP/1.1 303 See Other (text/html)
378	14.413595	192.168.60.39	87.98.154.146	HTTP	642	GET /login/index.php HTTP/1.1
399	14.567593	87.98.154.146	192.168.60.39	HTTP	1471	HTTP/1.1 200 OK (text/html)
538	20.351787	192.168.60.39	87.98.154.146	HTTP	794	POST /login/index.php HTTP/1.1 (application/x-ww…



Voici les trames https provenant d'un site possédant un certificat SSL :

No.	Time	Source	Destination	Protocol	Length	Info
4	1.140188	184.51.104.126	192.168.60.39	TLSv1.2	78	Application Data
30	4.600804	192.168.60.39	45.60.121.229	TLSv1.2	389	Application Data
31	4.600843	192.168.60.39	45.60.121.229	TLSv1.2	93	Application Data
37	4.607356	192.168.60.39	184.51.104.126	TLSv1.3	656	Client Hello
42	4.609729	192.168.60.39	184.51.104.243	TLSv1.3	678	Client Hello
43	4.609938	192.168.60.39	184.51.104.126	TLSv1.3	657	Client Hello
47	4.617279	184.51.104.126	192.168.60.39	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Dat…
48	4.617799	192.168.60.39	184.51.104.126	TLSv1.3	134	Change Cipher Spec, Application Data
49	4.617971	192.168.60.39	184.51.104.126	TLSv1.3	146	Application Data
50	4.618229	192.168.60.39	184.51.104.126	TLSv1.3	1145	Application Data
53	4.619557	184.51.104.243	192.168.60.39	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Dat…



On remarque que la taille de la trame est beaucoup plus grande dans la trame d’un site http, le protocole http possède un hypertext transfer protocole qui n’est pas sécurisé contrairement au site https qui possède un transport Layer Security.