



TP- initiation wireshark

1 – Téléchargement de Wireshark

On télécharge Wireshark sur le site officiel :

[Wireshark](https://www.wireshark.org/)



Download Wireshark

The current stable release of Wireshark is latest development release (3.6.0rc3) and

Stable Release (3.4.10)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS Intel 64-bit.dmg
- Source Code

2- Vérifications de la bonne connectivité du réseau

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

On peut ensuite taper la commande ping suivie de l'adresse IP trouvée précédemment. La commande répond donc une somme bien connecter au réseau.

```
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. . . . . :
```

```
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)

No.	Time	Source	Destination	Protocol	Length	Info
171	21.777600	192.168.60.39	192.168.60.38	ICMP	74	Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (...)
172	21.777890	192.168.60.38	192.168.60.39	ICMP	74	Echo (ping) reply id=0x0001, seq=45/11520, ttl=128 (...)
179	22.790886	192.168.60.39	192.168.60.38	ICMP	74	Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (...)
180	22.791319	192.168.60.38	192.168.60.39	ICMP	74	Echo (ping) reply id=0x0001, seq=46/11776, ttl=128 (...)
184	23.799816	192.168.60.39	192.168.60.38	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (...)
185	23.800227	192.168.60.38	192.168.60.39	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=128 (...)
192	24.820115	192.168.60.39	192.168.60.38	ICMP	74	Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (...)
193	24.820544	192.168.60.38	192.168.60.39	ICMP	74	Echo (ping) reply id=0x0001, seq=48/12288, ttl=128 (...)

Adresse MAC source et destinataire :
(identifiant physique stocké dans la
carte réseau)

```
▼ Ethernet II, Src: HewlettP_e0:73:ab (f0:92:1c:e0:73:ab), Dst: HewlettP_94:40:23 (a0:48:1c:94:40:23)
  Destination: HewlettP_94:40:23 (a0:48:1c:94:40:23)
    Address: HewlettP_94:40:23 (a0:48:1c:94:40:23)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: HewlettP_e0:73:ab (f0:92:1c:e0:73:ab)
    Address: HewlettP_e0:73:ab (f0:92:1c:e0:73:ab)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Adresse IP source et destinataire :
(numéro d'identification attribué à chaque
Périphérique informatique du réseau)

```
Source Address: 192.168.60.39
Destination Address: 192.168.60.38
```

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

```
▼ Internet Protocol Version 4, Src: 192.168.60.39, Dst: 192.168.60.38
  0100 .... = Version: 4
  ....0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xdb1f (56095)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
```

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)

```
▼ Frame 171: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4D8}
  > Interface id: 0 (\Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4D8})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 22, 2021 08:53:25.502897000 Paris, Madrid
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1637567605.502897000 seconds
    [Time delta from previous captured frame: 0.000033000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 21.777600000 seconds]
    Frame Number: 171
    Frame Length: 74 bytes (592 bits)
```

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)

```
▼ Frame 171: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4D8}
  > Interface id: 0 (\Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4D8})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 22, 2021 08:53:25.502897000 Paris, Madrid
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1637567605.502897000 seconds
    [Time delta from previous captured frame: 0.000033000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 21.777600000 seconds]
    Frame Number: 171
    Frame Length: 74 bytes (592 bits)
```

Taille des données :

```
▼ Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
[Length: 32]
```

Code type ICMP :

(code du protocole de signalement d'erreurs)

```
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d2e [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 45 (0x002d)
Sequence Number (LE): 11520 (0x2d00)
[Response frame: 172]
```

4 – Modifications des paramètres IP

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

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

☐ Valider les paramètres en quittant

Avancé...

OK Annuler

La commande ping ne trouve pas l'hôte (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 :

☒ Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

La commande est fonctionnelle

```
C:\Users\HP>ping 172.16.200.200

Envoi d'une requête 'Ping' 172.16.200.200 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 172.16.200.200:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

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](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/1.1	781	POST /lib/ajax/service.php?sesskey=I43VrUUE7u&inf...
317	13.040523	192.168.60.39	87.98.154.146	HTTP/1.1	794	POST /lib/ajax/service.php?sesskey=I43VrUUE7u&inf...
320	13.149378	87.98.154.146	192.168.60.39	HTTP/1.1	464	HTTP/1.1 200 OK , JavaScript Object Notation (app...
321	13.163308	87.98.154.146	192.168.60.39	HTTP/1.1	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-w...

```
> Frame 273: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4C}
> Ethernet II, Src: HewlettP_e0:73:ab (f0:92:1c:e0:73:ab), Dst: HewlettP_14:b7:1d (e8:39:35:14:b7:1d)
> Internet Protocol Version 4, Src: 192.168.60.39, Dst: 87.98.154.146
> Transmission Control Protocol, Src Port: 64612, Dst Port: 80, Seq: 3231, Ack: 16719, Len: 588
> Hypertext Transfer Protocol
```

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...

```
> Frame 4: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{CDE4A7CA-BB98-49D3-8D5A-BF8279E1C4DB},
> Ethernet II, Src: HewlettP_14:b7:1d (e8:39:35:14:b7:1d), Dst: HewlettP_e0:73:ab (f0:92:1c:e0:73:ab)
> Internet Protocol Version 4, Src: 184.51.104.126, Dst: 192.168.60.39
> Transmission Control Protocol, Src Port: 443, Dst Port: 57266, Seq: 1, Ack: 1, Len: 24
> Transport Layer Security
```

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.