GASSENDI

mardi 17 novembre 2020

TP monde connecté : cours du 12/11/2020 : NetScan et Putty

Élaboration	
17 novembre 2020	
Jean D	GASSENDI
Animateur	
Administration informatique	
Nom du fichier	TP_monde_connecte_cours_12_11_2020_generalites_Raspbian_installation_V0.1.odt

Outil Netscan

But :
Cet utilitaire affiche la liste des adresses logiciel (IPV4/IPV6) et des adresses physique (MAC) de tous les matériels informatique connectés au réseau local.

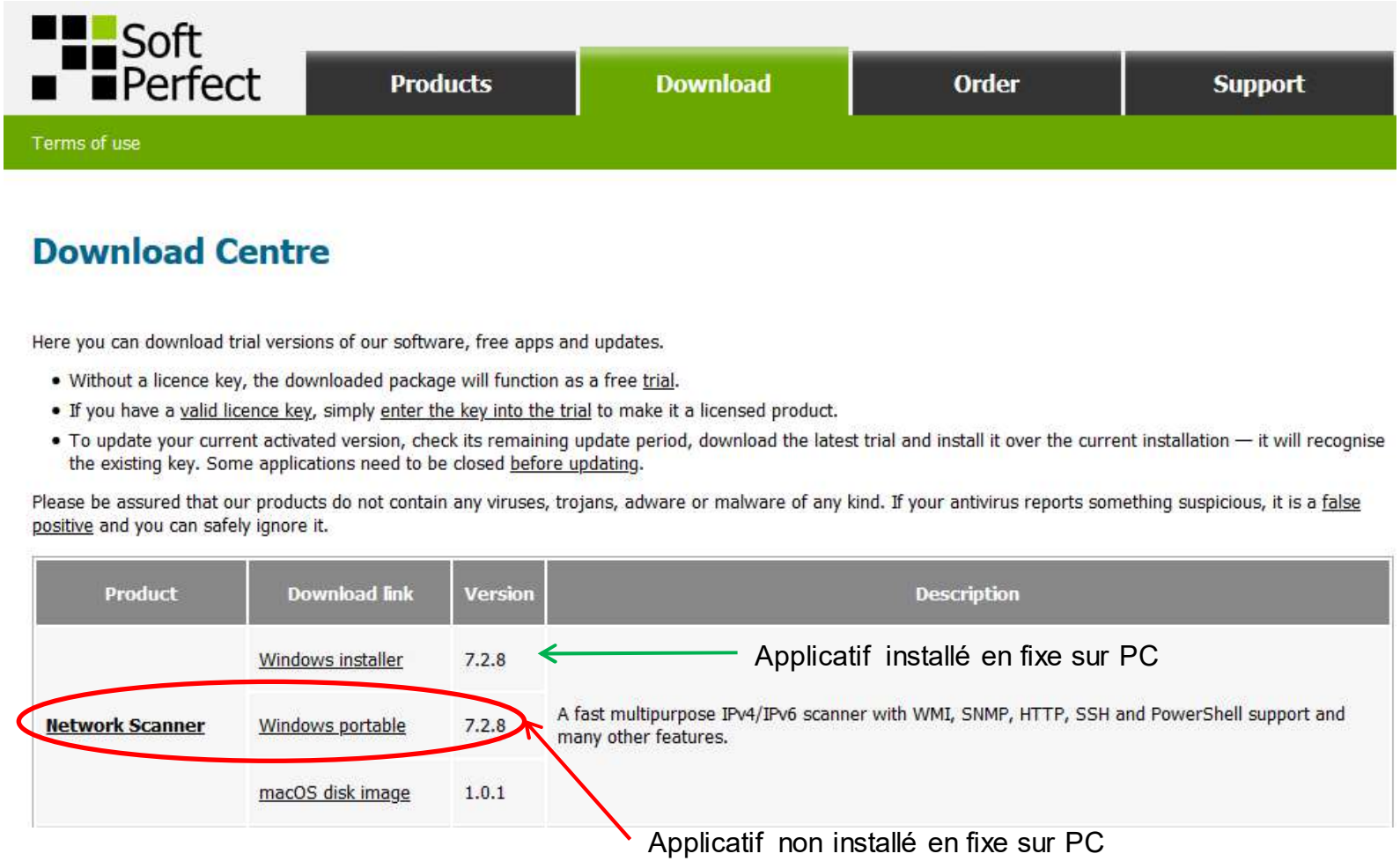
Il existe un autre outil en open-source cf. **angry**

Installation:

1. Allez sur le site suivant:
   https://www.softperfect.com/

Outil Netscan

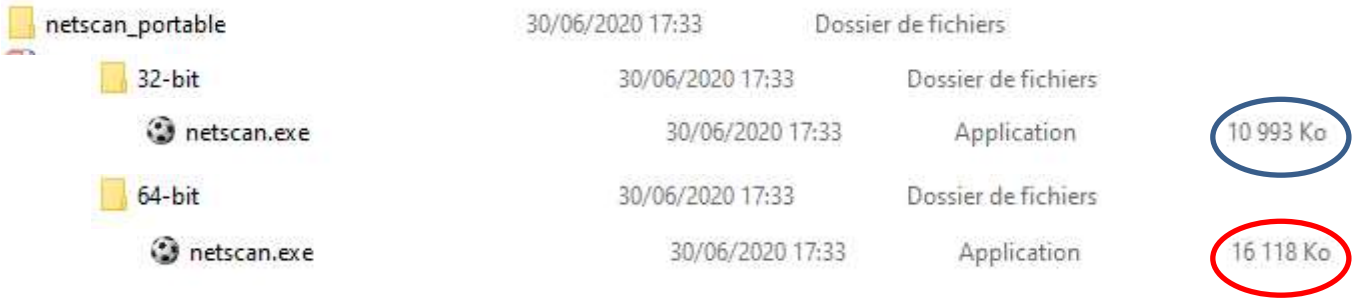
2. Choisir dans la fenêtre « Download »



Outil Netscan

3. Cliquer sur « Windows portable » pour télécharger le dossier :

4. Décompresser le dossier :



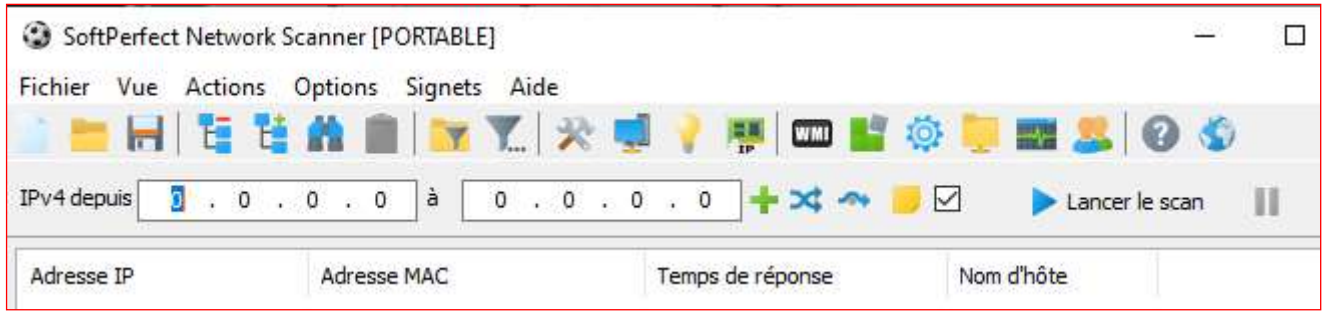
5. Ouvrir le « **netscan**.exe » choisit

Icône

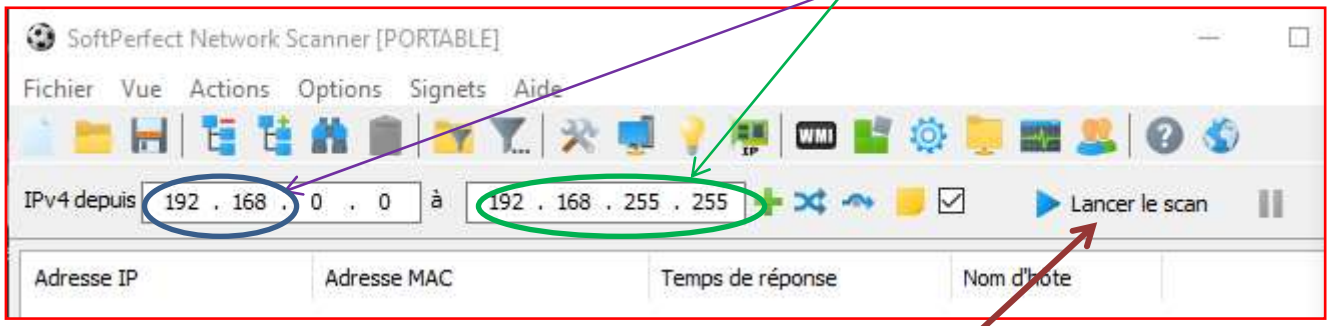
Outil Netscan

Paramétrage de Netscan:

1. Fenêtre au 1er démarrage



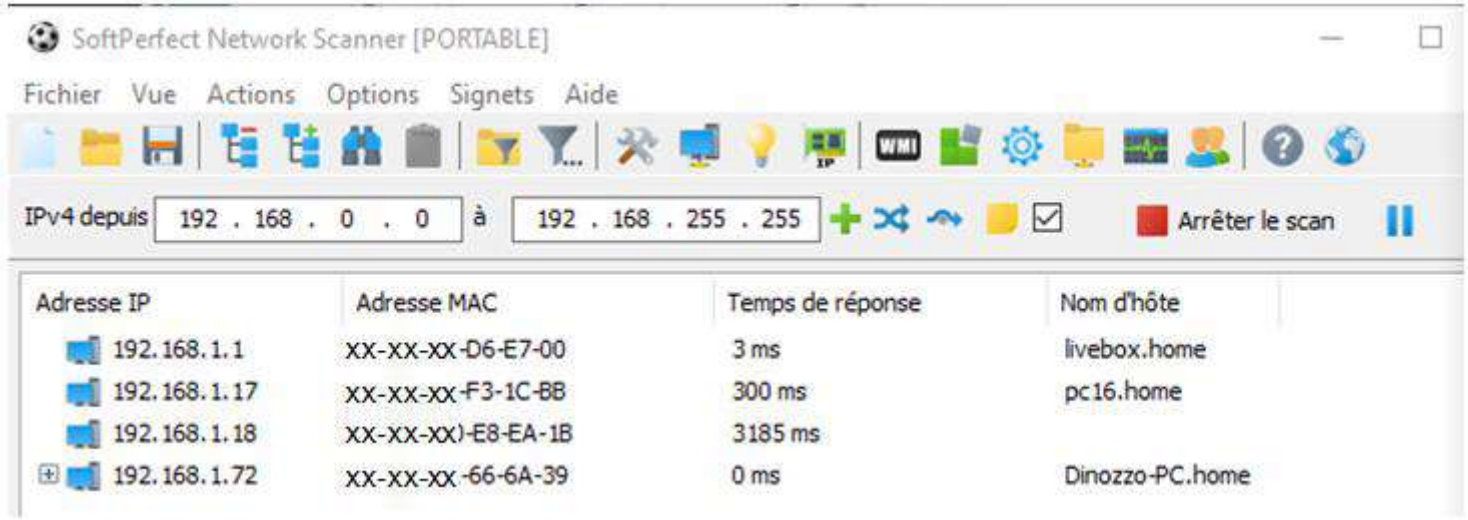
2. Renseigner les champs IPv4



3. Démarrer la recherche

Outil Netscan

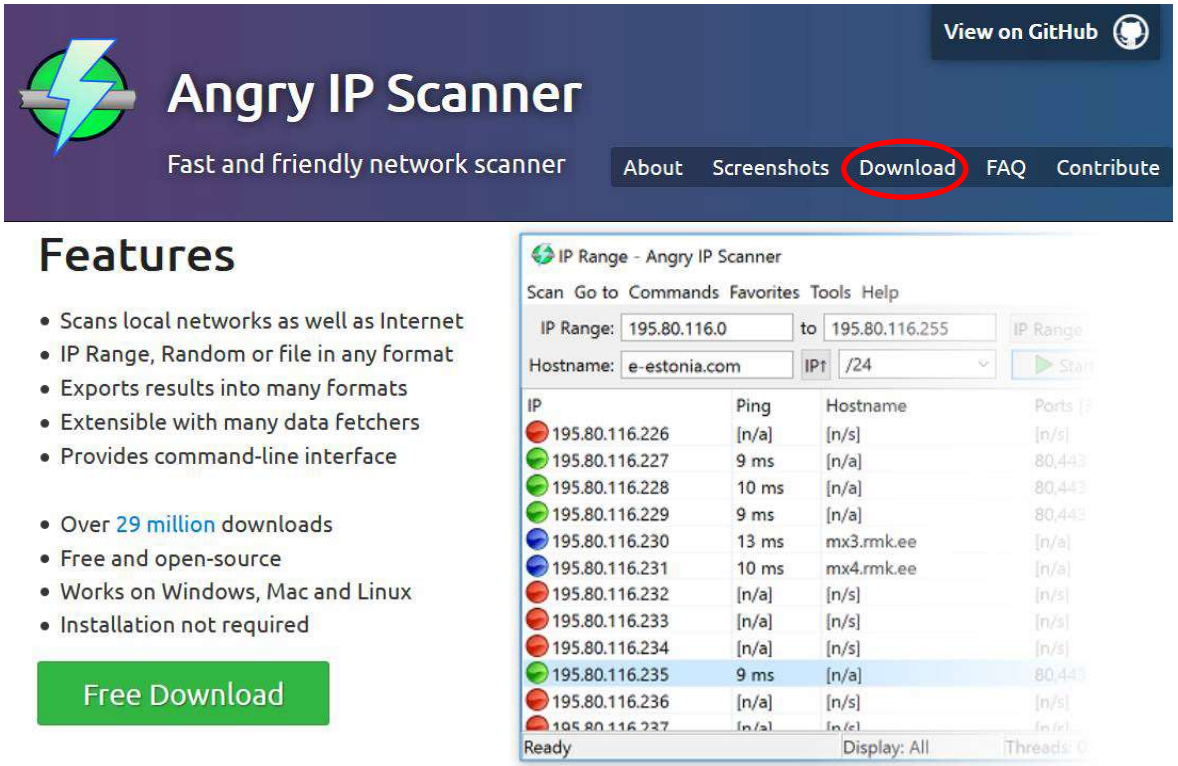
Résultat :



Outil Angryip

Installation:

1. Allez sur le site suivant:
   https://www.angryip.org/



Outil Angryip

Download for Windows, Mac or Linux

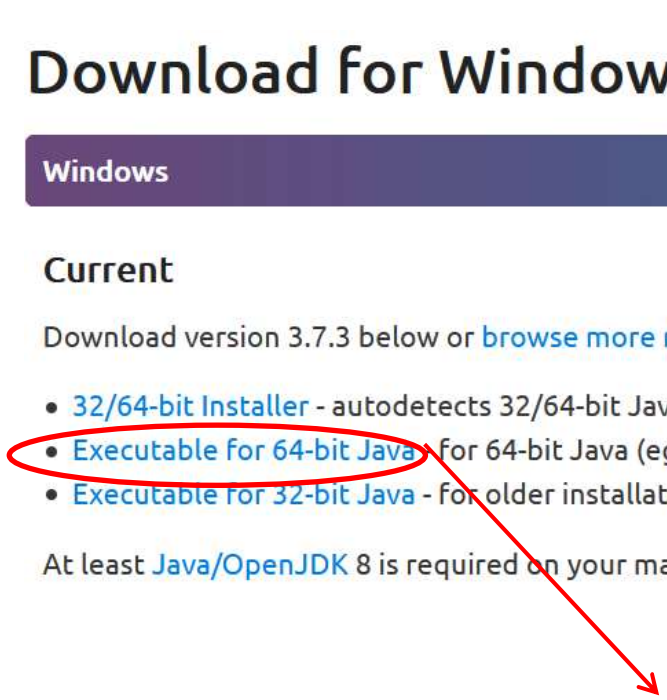
Windows

Current

Download version 3.7.3 below or browse more releases or even older releases.

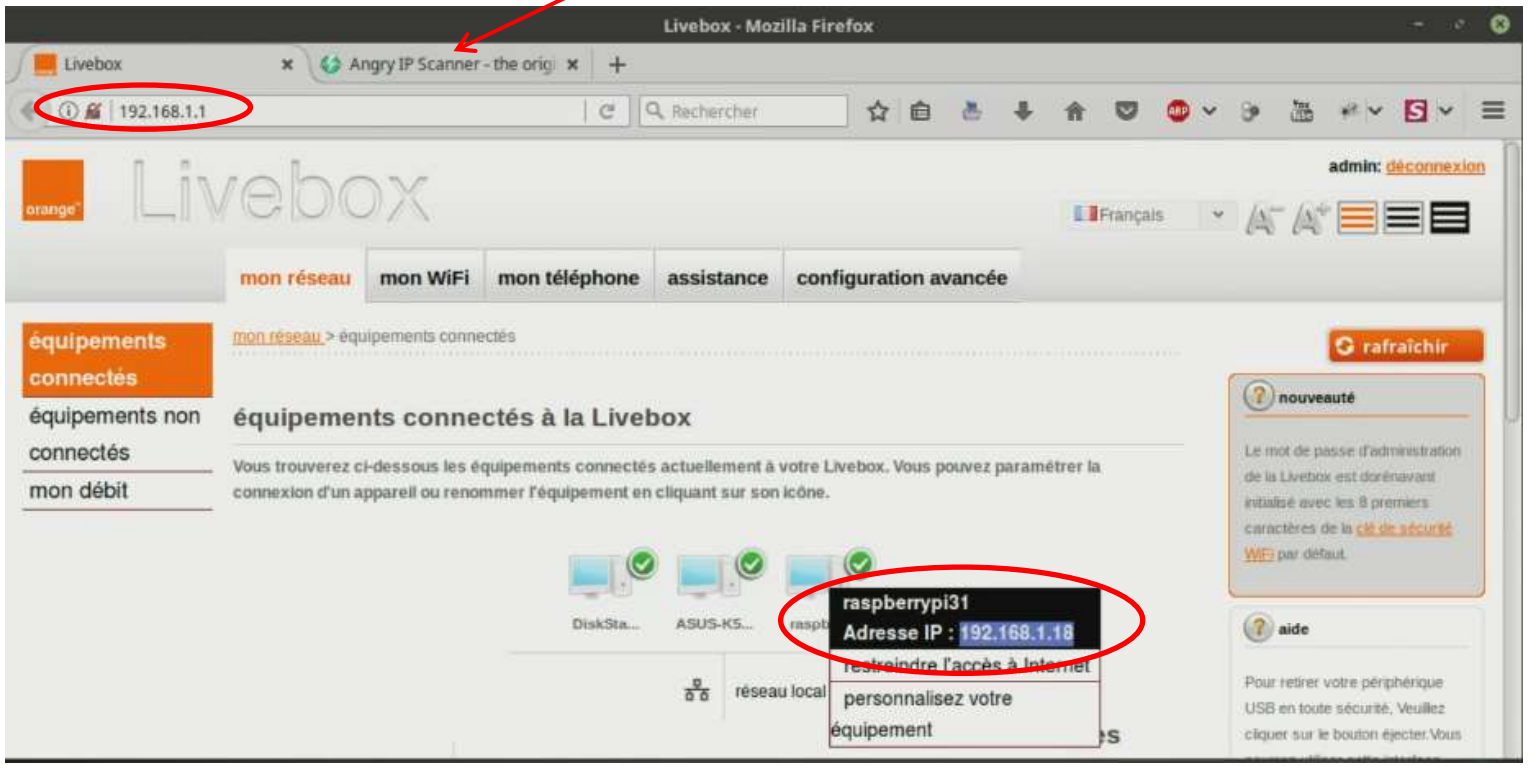
- 32/64-bit Installer - autodetects 32/64-bit Java, for Windows 7/8/10
- Executable for 64-bit Java - for 64-bit Java (eg AdoptOpenJDK) on Windows 7/8/10
- Executable for 32-bit Java - for older installations of Oracle Java for Windows

At least Java/OpenJDK 8 is required on your machine, but 11 is recommended.



Applicatif non installé en fixe sur PC

Outil Angryip



@IPv4/IPv6

IP : Internet **P**rotocol

Rubrique	Nb bits	Nb d'adresses	Constitution
IPv4	32	4.3 10^9 4 294 967 296	192.168.1.72
Codage	4 octets	128-64-32-16-8-4-2-1 1 1 0 0 0 0 0 0	128-64-32-16-8-4-2-1 1 0 1 0 1 0 0 0 • 128-64-32-16-8-4-2-1 0 0 0 0 0 0 0 1 • 128-64-32-16-8-4-2-1 0 1 0 0 1 0 0 0
Localhost			127.0.0.1
IPv6	128	3.4 10^38 3 402 823 669 209 380 10^23	FE80 :: 3D45 : 345 : E844 : 69F2%16

Détail d'allocation des adresses IPv4

Classe A :

pour réseaux de grande envergures

de l'@ **1**.0.0.0 à l'@ **126**.0.0.0 soit 126 réseaux de 16 777 214 machines

1 octet fixe

Classe B :

pour réseaux moyens (universités)

de l'@ **128.1**.0.0 à l'@ **191.254**.0.0 soit 16 382 réseaux de 65 535 machines

2 octets fixe

Classe C :

pour réseaux régionaux (PME/PMI)

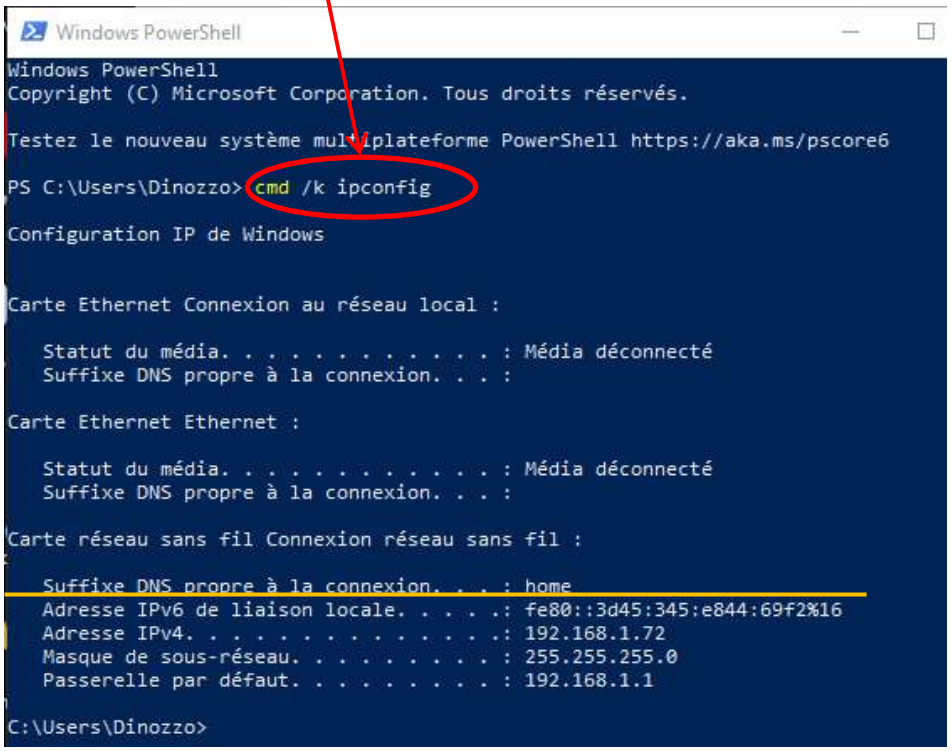
de l'@ **192.0.1**.0 à l'@ **223.255.254**.0 soit 2 097 150 réseaux de 254 machines

3 octets fixe

@IPv4/IPv6

Pour connaître son IP privée ou locale de son PC

1. Clique droit sur : 
2. Ouvrir une console en sélectionnant « Windows PowerShell »
3. Taper la commande: cmd /k ipconfig
4. Résultat



@IPv4/IPv6

Votre box haut débit possède une adresse **IP privée** et une adresse **IP publique**.

Adresse IP publique

C'est l'adresse IP « tournée vers l'extérieur » et matérialisant l'adresse de la box sur le réseau Internet.

Les adresses IP publique servent aux ordinateurs du réseau pour communiquer entre eux.
Ainsi, chaque ordinateur d'un réseau possède une adresse IP unique. C'est cette adresse que « voit » par exemple un serveur sur lequel vous allez faire des transactions.

Adresse IP privée

C'est l'adresse IP « tournée vers l'intérieur », c'est-à-dire permettant de connecter un ou plusieurs ordinateurs.

Comment connaître son IP publique

L'adresse IP publique est délivrée par votre FAI (Fournisseur d'Accès à Internet) au moment de l'installation et synchronisation de la box.

Voici comment faire pour connaître son IP publique :

Se connecter sur sa box :

Allez dans Mes Services → Accès Internet → État de la connexion Internet

Ou allez sur le site :

http://www.whatismyip.com

@MAC

MAC : **M**edia **A**ccess **C**ontrol

Les adresses MAC sont des adresses physiques uniques propres à chaque périphérique réseau. Elles sont inscrites dans la trame normée 802.3 qui en gère l'accès.

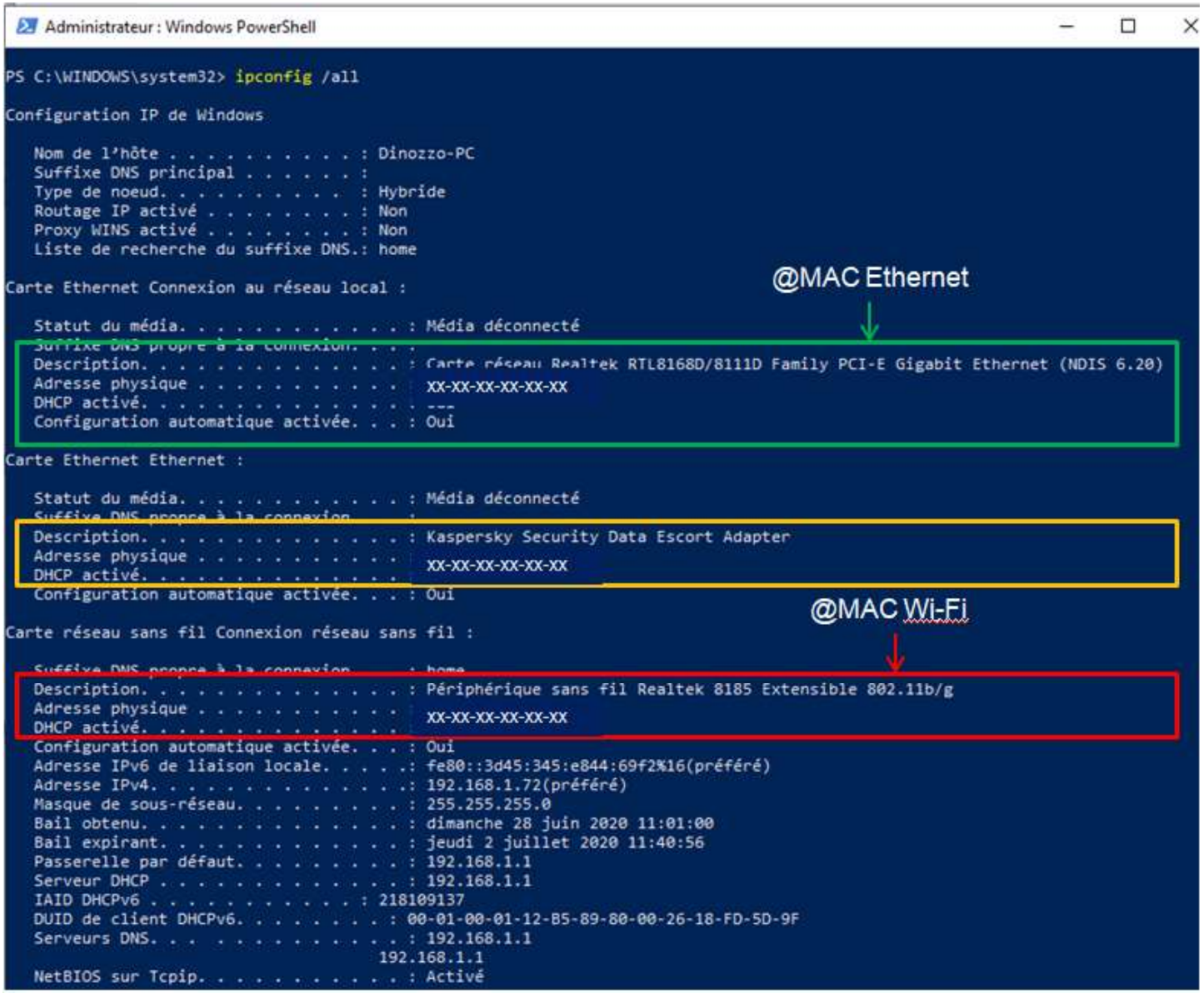
Pour connaître l'adresse MAC de son PC

Aller sur le site : **http://coffer.com/mac_find/**

Ou :

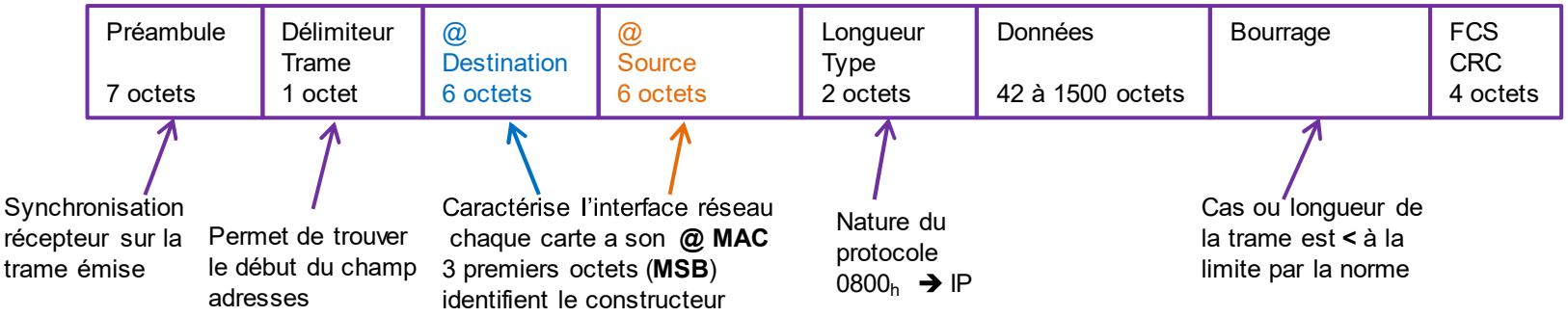
1. Clique droit sur : 
2. Ouvrir une console en sélectionnant « Windows PowerShell (admin) »
3. Taper la commande: ipconfig /all
4. Résultat

@MAC

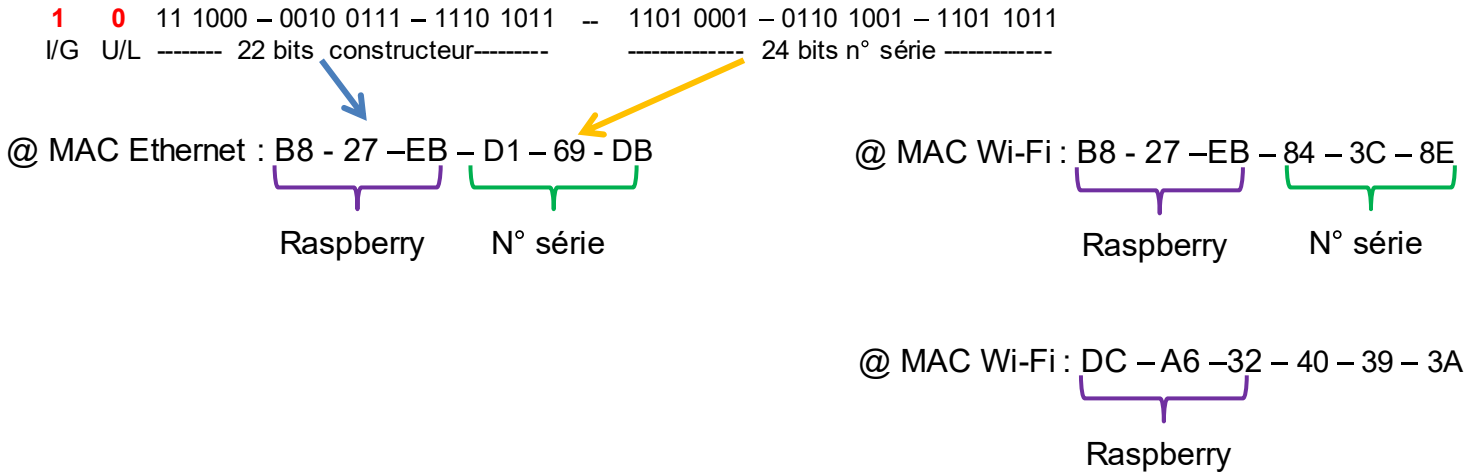

Administrateur : Windows PowerShell
PS C:\WINDOWS\system32> ipconfig /all
Configuration IP de Windows
Nom de l'hôte . . . . . : Dinozzo-PC
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: home
@MAC Ethernet
Carte Ethernet Connexion au réseau local :
Statut du média. . . . . : Média déconnecté
Description. . . . . : Carte réseau Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet (NDIS 6.20)
Adresse physique . . . . . : XX-XX-XX-XX-XX-XX
DHCP activé. . . . . : ---
Configuration automatique activée. . . : Oui
Carte Ethernet Ethernet :
Statut du média. . . . . : Média déconnecté
Description. . . . . : Kaspersky Security Data Escort Adapter
Adresse physique . . . . . : XX-XX-XX-XX-XX-XX
DHCP activé. . . . . :
Configuration automatique activée. . . : Oui
@MAC Wi-Fi
Carte réseau sans fil Connexion réseau sans fil :
Description. . . . . : Périphérique sans fil Realtek 8185 Extensible 802.11b/g
Adresse physique . . . . . : XX-XX-XX-XX-XX-XX
DHCP activé. . . . . :
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . .: fe80::3d45:345:e844:69f2%16(préféré)
Adresse IPv4. . . . . : 192.168.1.72(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : dimanche 28 juin 2020 11:01:00
Bail expirant. . . . . : jeudi 2 juillet 2020 11:40:56
Passerelle par défaut. . . . . : 192.168.1.1
Serveur DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 218109137
DUID de client DHCPv6. . . . . : 00-01-00-01-12-B5-89-80-00-26-18-FD-5D-9F
Serveurs DNS. . . . . : 192.168.1.1
192.168.1.1
NetBIOS sur Tcpip. . . . . : Activé

@MAC

Constitution de la Trame 802.3 qui porte l'@ MAC



l'@ MAC est constituée de 6 octets soit 48 bits



Glossaire

Sigle	
CRC	**C**yclic **R**edundancy **C**heck (Check-Sum)
FAI	**F**ournisseur d'**A**ccès à **I**nternet
FCS	**F**rame **C**heck **S**equence (Code Détection d'Erreurs)
IP	**I**nternet **P**rotocol
MAC	**M**edia **A**ccess **C**ontrol
MSB	**M**ost **S**ignificant **B**it

PuTTY / SSH

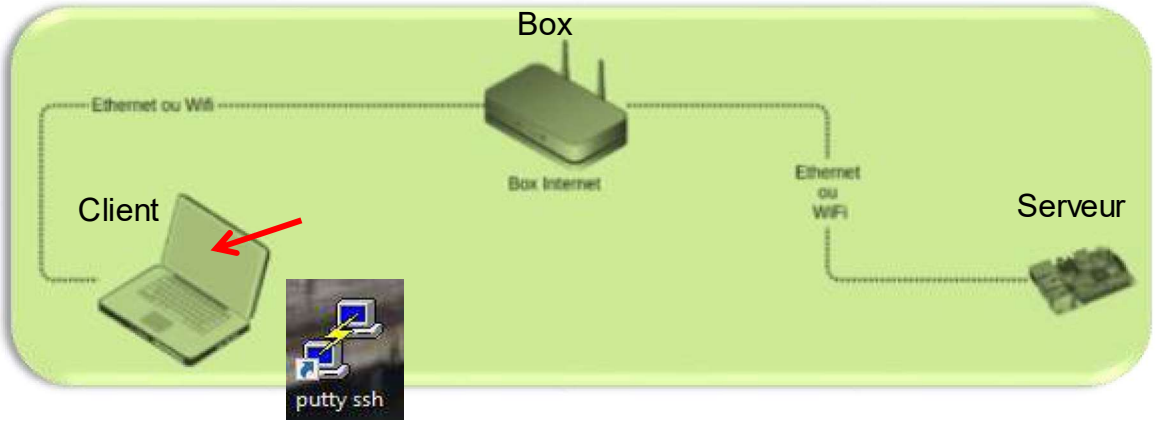
Généralité :

Une des grandes forces de Linux est que l'on peut s'en servir même si l'on est à des centaines de kilomètres de la machine.

Aujourd'hui, si j'habite à Paris, je peux très bien contrôler un ordinateur sous Linux situé à Tokyo, en même temps qu'un autre ordinateur situé à San Francisco. Je peux même ordonner à l'ordinateur de Tokyo d'envoyer un fichier à celui de San Francisco.

Le PC qui se connecte au serveur est appelé le client

Synoptique d'une utilisation à distance d'une machine

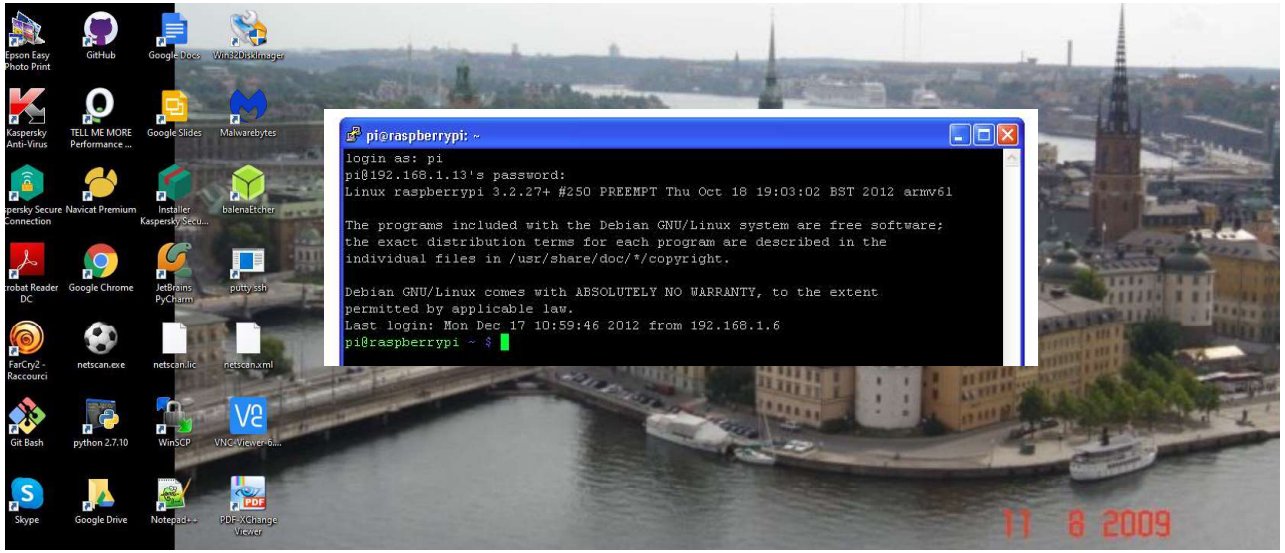


Nota: pour plus d'informations sur SSH cliquer **SSH**

Outil PuTTY

But :
Cet utilitaire permet à un client Windows de se connecter directement à des serveurs distants Linux à travers une liaison Ethernet sécurisé (SSH).

Ci-dessous le résultat de l'accès à la Raspberry Pi en mode console depuis un PC Windows.

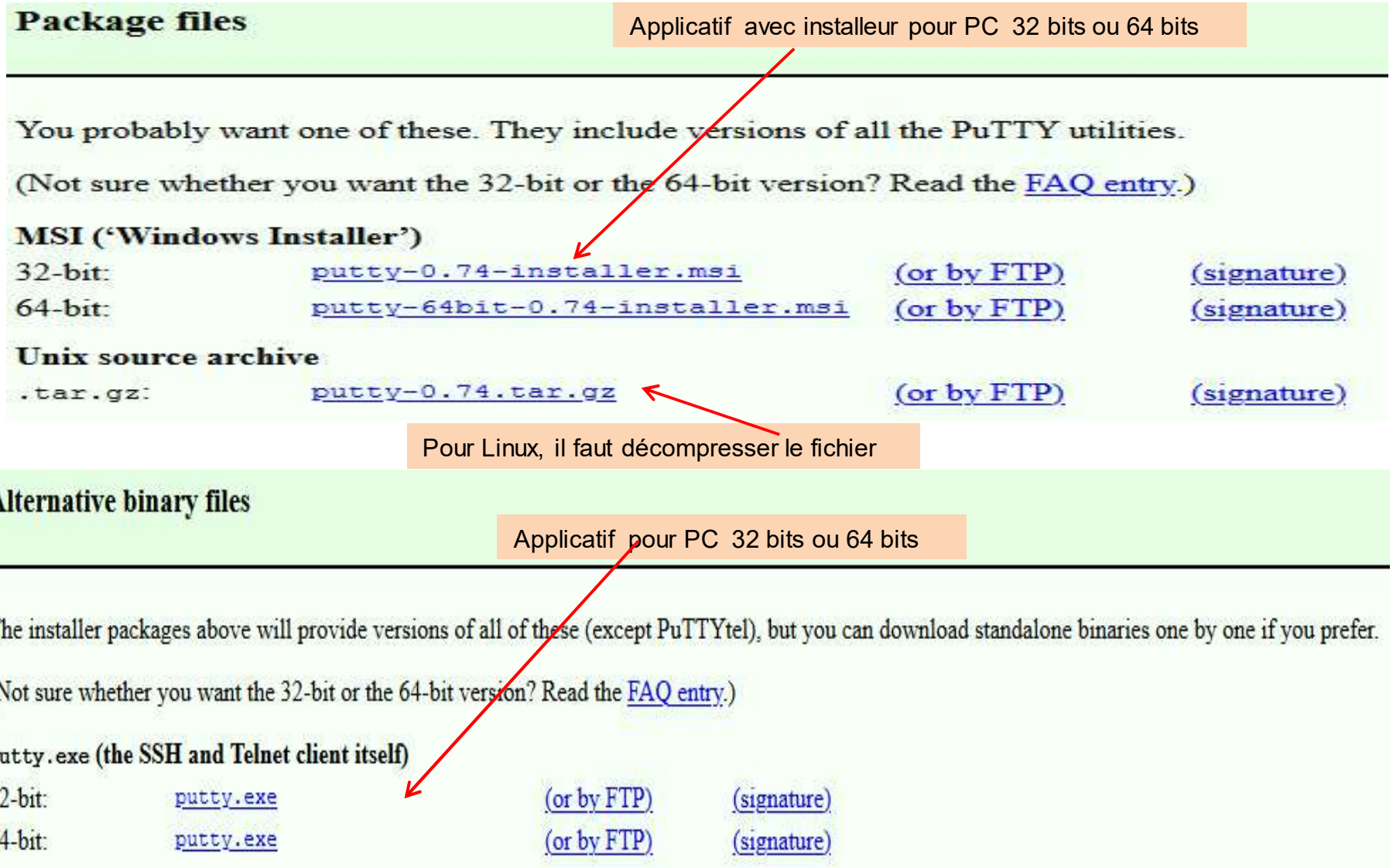


Installation:

1. Allez sur le site suivant:
   https://www.putty.org/

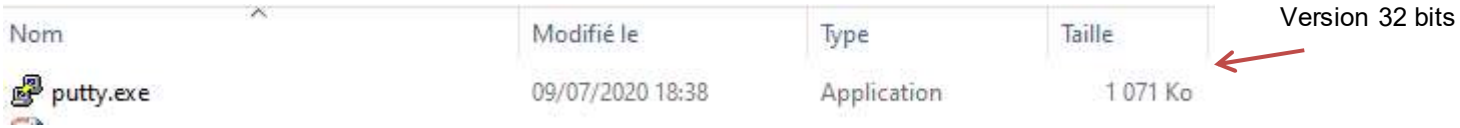
Outil PuTTY

2. Choisir la version à télécharger :



Outil PuTTY

3. Téléchargement de la version « putty.exe » choisit:



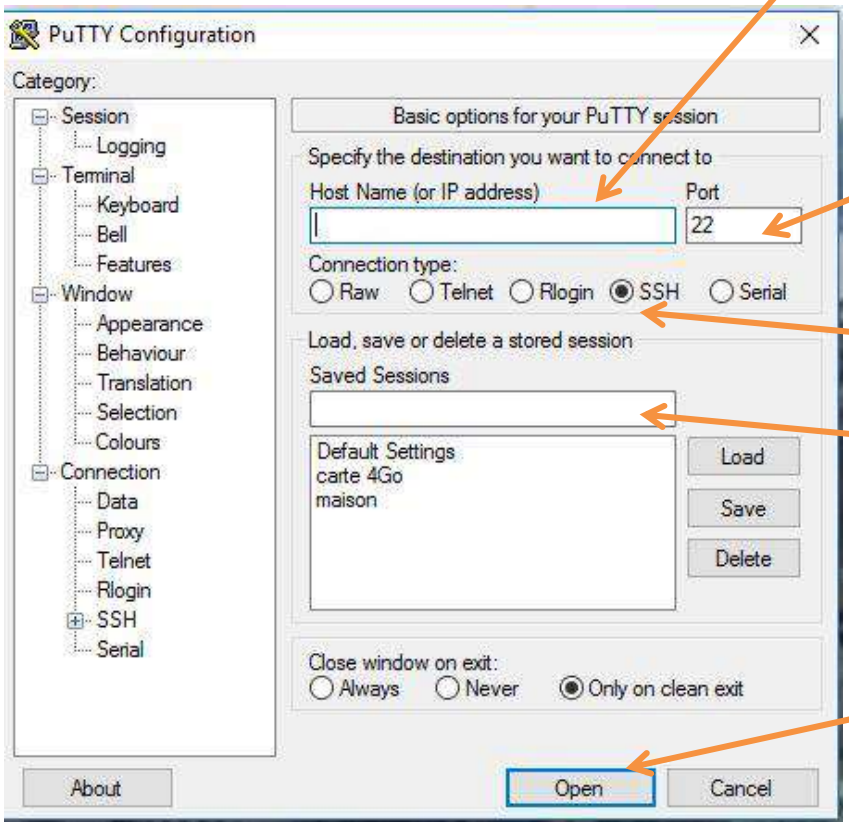
4. Ouvrir la version « putty.exe » choisit:

Icône

Outil PuTTY

Paramétrage de PuTTY:

Lorsque vous démarrez PuTTY, vous obtenez la boîte de dialogue ci-dessous :



1 - renseigner la fenêtre Host Name avec l'@ IP de votre PI
192.168.1.24 (@ donnée par Netscan)

2 – vérifier que la fenêtre Port affiche **22**
SSH

3 – vérifier que **SSH** soit coché

4 – pour sauvegarder l'@IP (option)
cliquer sur « Load »
donner un nom significatif
cliquer sur « Save »

5 – lancer l'applicatif

Outil PuTTY

5. Commandes système:

New Session démarre une nouvelle instance de PuTTY, et affiche la boîte de dialogue de configuration habituelle.

Duplicate Session démarre une session dans une nouvelle fenêtre, avec exactement les mêmes réglages que la session courante (connexion au même serveur, avec le même protocole, les mêmes réglages, etc.).

Restart Session utilisée dans une fenêtre inactive fait pareil que 'Duplicate Session', mais dans la fenêtre courante.

Reset Terminal provoque une réinitialisation complète de l'émulateur de terminal.

Le sous-menu **Saved Sessions** vous permet d'accéder rapidement à des ensembles de réglages de session sauvegardés auparavant.

7. Modification des réglages de session:

Change Settings

fait apparaître une version allégée de la boîte de dialogue de configuration initiale et permet d'ajuster la plupart des propriétés de la session en cours.

. changer la taille du terminal,
. la police de caractères,
. les couleurs,
. les actions associées à différentes combinaisons de touches, etc..
. sauvegarder les réglages de la session courante.

Outil PuTTY

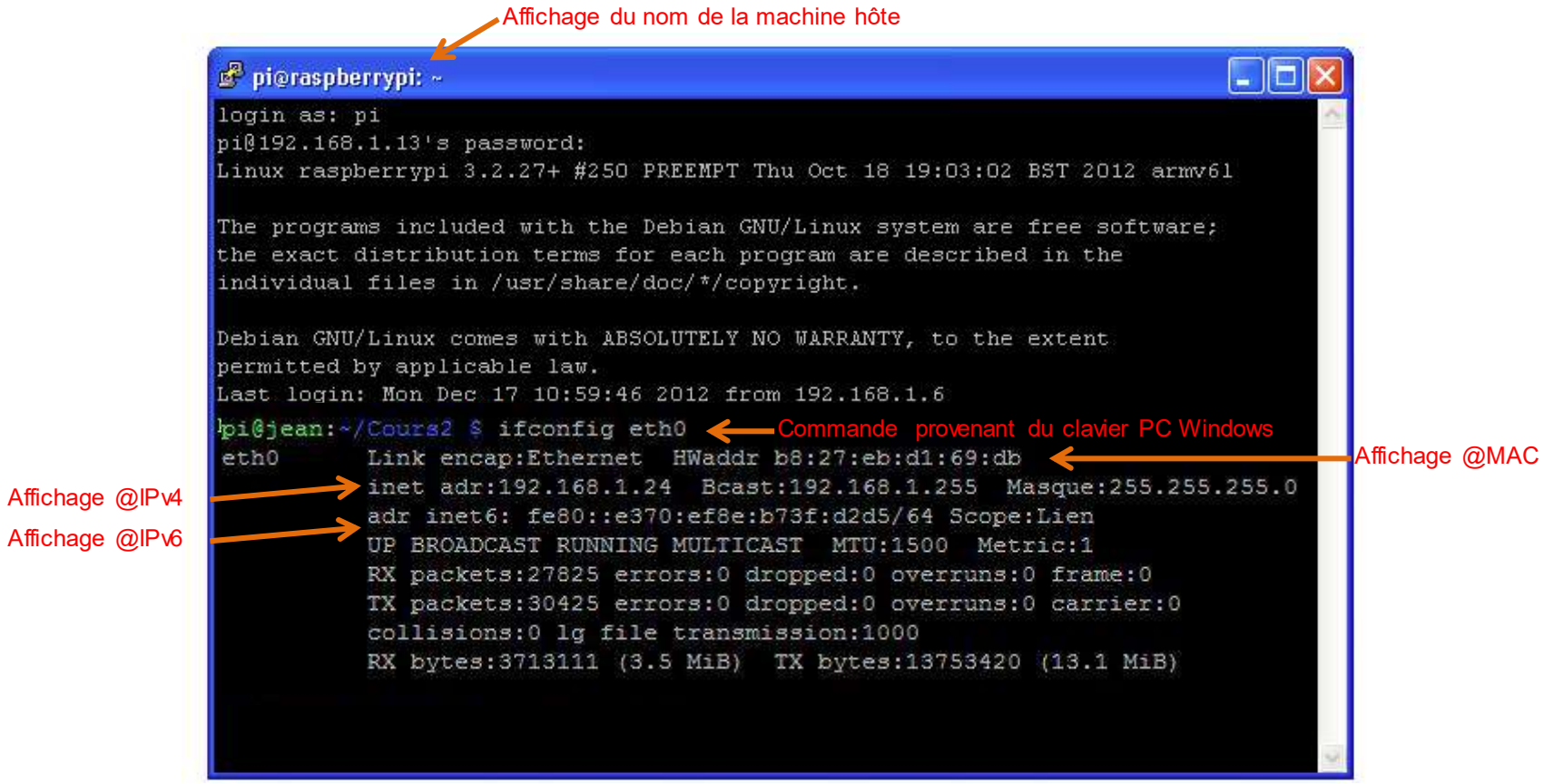
6. Journal de session:

Logging permet de conserver la trace de tout ce qui s'affiche sur votre écran.
Voir panneau *Logging* de la boîte de dialogue de configuration.

Pour enregistrer des traces de la session courante dans un journal de session,
Cliquez sur *Change Settings*, dans le menu système, et allez dans le panneau *Logging*.
Choisir un nom de fichier journal, et un mode d'enregistrement des traces (soit tout le trafic ou texte imprimable).
Cliquez sur *Apply* pour démarrer l'enregistrement.
Sélectionner *Logging turned off completely* pour arrêter l'enregistrement. Le fichier journal est lisible à la guise

Outil PuTTY

7. Une fenêtre type « console » s'affiche



Outil PuTTY

Connection via SSH à partir de Windows (PuTTY) :

La 1ére fois que vous utilisez **SSH** pour vous connecter à un serveur, vous verrez ce message

Comme **PuTTY** n'a aucun moyen de savoir si la clé d'hôte envoyée par la machine distante est la bonne, ou pas, il vous affiche l'avertissement ci-dessus, et vous demande si oui ou non, vous estimez pouvoir faire confiance à cette clé d'hôte.
Cela sert à vous protéger d'une attaque réseau connue sous le nom de ***spoofing*** (usurpation d'identité).

Le ***spoofing*** consiste à détourner secrètement votre tentative de connexion vers un ordinateur autre que celui auquel vous voulez vous connecter, de façon à ce que le pirate qui est à l'origine de ce détournement puisse prendre connaissance de votre mot de passe, et s'en servir ensuite pour ouvrir une session sur la machine à laquelle vous vouliez vous connecter, en se faisant passer pour vous.

SSH

SSH affecte à chaque serveur un identifiant unique, que l'on appelle une clé d'hôte. Ces clés sont conçues de telle façon qu'il est impossible pour une machine de se fabriquer une clé d'hôte qui corresponde à une autre machine qu'elle-même, ceci empêche toute usurpation d'identité entre machines.

Ainsi, si vous essayez de vous connecter à un serveur et qu'il vous envoie une clé d'hôte différente de celle que vous attendiez, **PuTTY** peut vous prévenir que la machine distante n'est pas celle que vous pensez, et que vous faites peut-être l'objet d'une tentative de détournement de connexion.

Comme **PuTTY** garde trace, dans la base de registres de Windows, de la clé d'hôte de chaque serveur auquel vous vous connectez, donc à chaque fois que vous vous connectez à un serveur, il vérifie que la clé d'hôte envoyée par le serveur est bien la même que celle qu'il avait envoyée la dernière fois que vous vous y êtes connecté.

Si ce n'est pas le cas, vous verrez s'afficher un avertissement et vous aurez la possibilité d'abandonner la tentative de connexion avant même d'avoir envoyé à la machine distante quoi que ce soit de confidentiel, comme votre mot de passe, par exemple.

SSH

Activer le client SSH dans Windows :

Windows 10 prend en charge SSH mais il faut l'activer

client SSH se trouve dans « Gérer les fonctionnalités facultatives »

Procédure d'installation du client SSH :

Clic gauche pour ouvrir menu Windows 

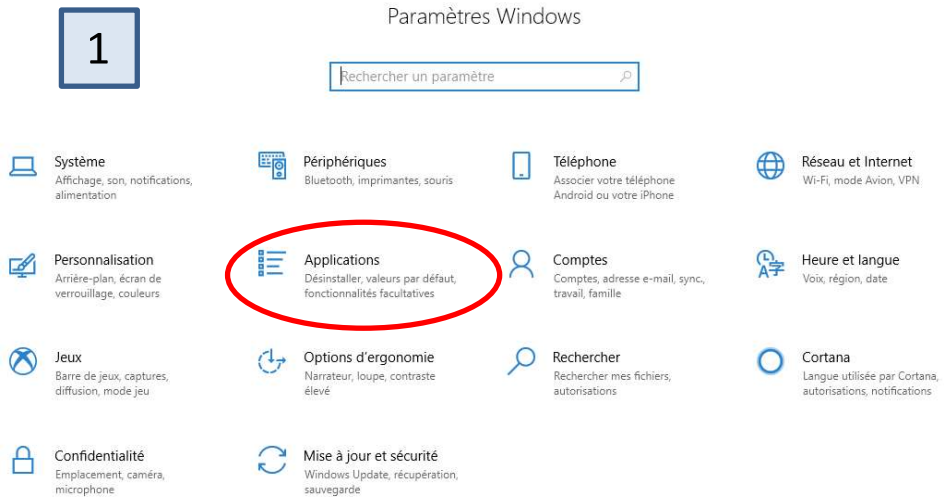
ouvrir Paramètres

suivre les étapes 1 – 2 – 3 – 4 de la planche suivante

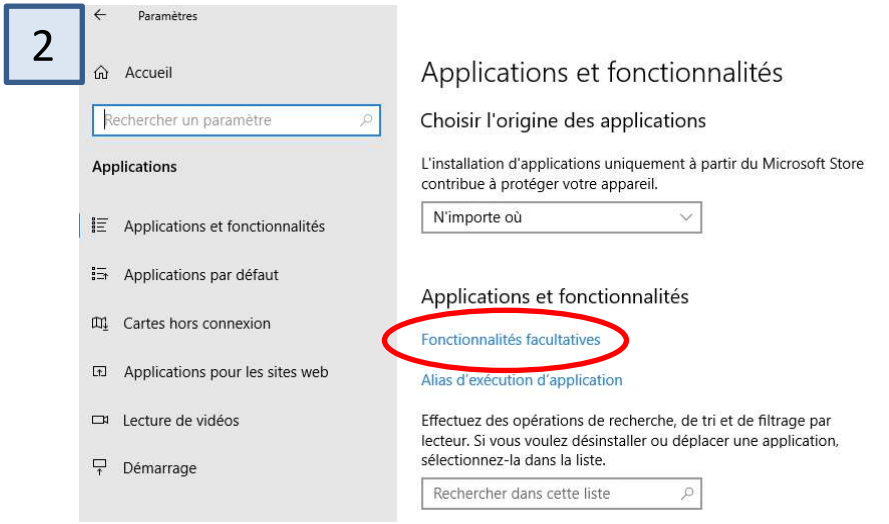
SSH

Procédure d'installation du client SSH :

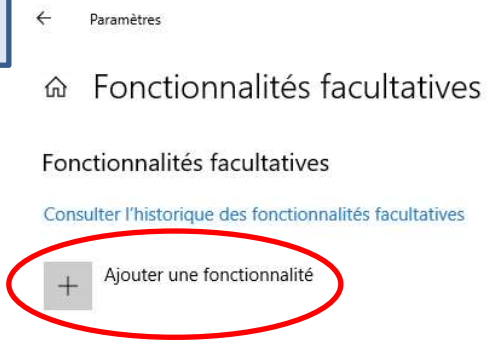
1



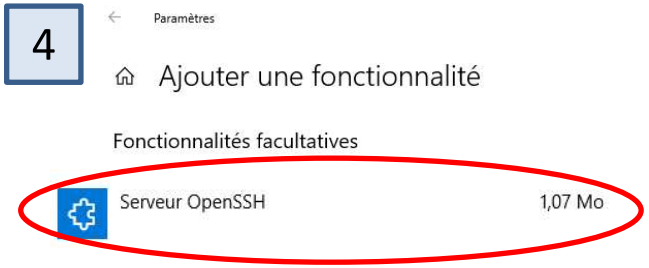
2



3



4



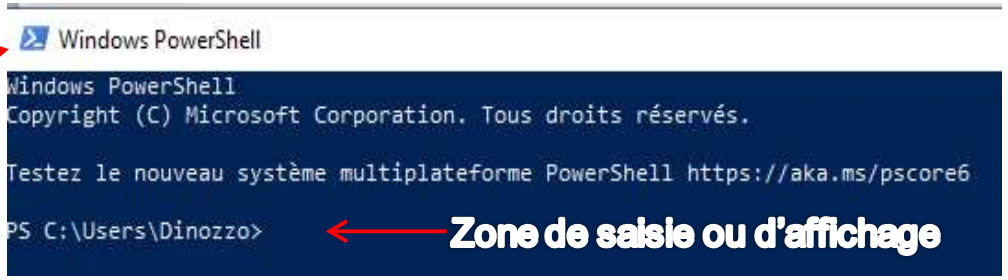
SSH

Généralités :

SSH est une technologie pour les réseaux qui facilite l'accès sécurisé à une session sur un ordinateur multi-utilisateurs, depuis un autre ordinateur.

Les systèmes d'exploitation multi-utilisateurs, présentent à l'utilisateur une interface de type console.

Sous Windows10
Windows PowerShell

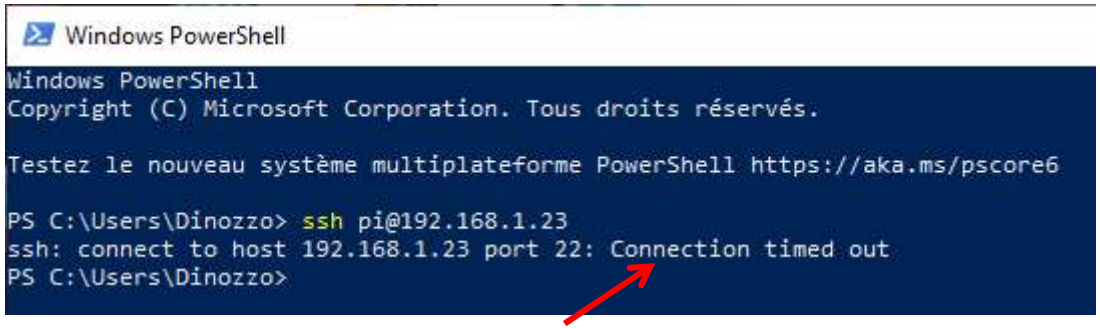


Avec ce type d'interface, pas besoin d'être assis devant la machine, les commandes, et leurs résultats, peuvent provenir d'une autre machine distante en transitant via un réseau.

Sur la machine devant laquelle vous êtes assis, vous utilisez ce qu'on appelle un ***client***, qui établit une connexion réseau avec l'autre ordinateur, que l'on appelle le ***serveur***.
La connexion réseau achemine les séquences de touches et les commandes que vous tapez sur le clavier de la machine cliente jusqu'au serveur, et vous ramène en retour les réponses du serveur.

SSH

Résultat:



Pi non connecté

SSH

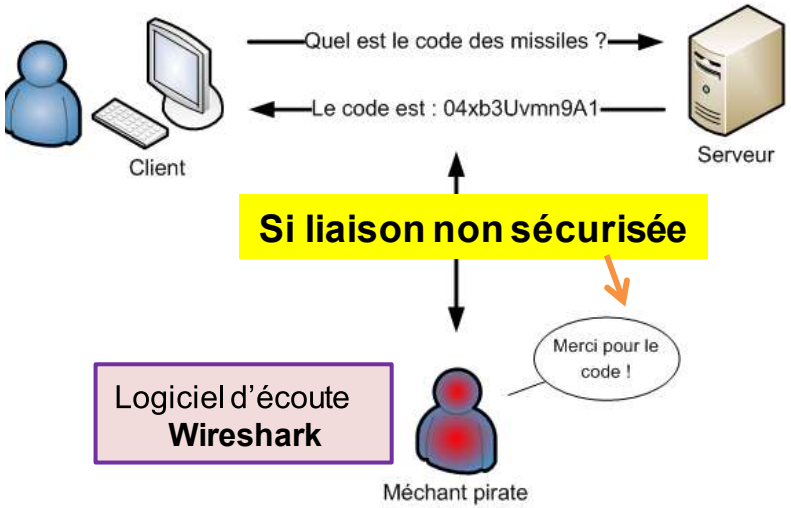
Les protocoles :

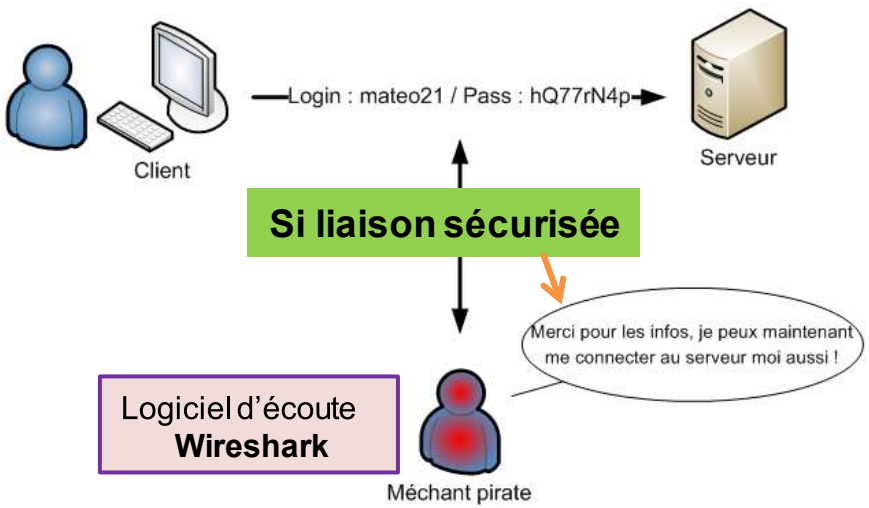
Pour communiquer entre eux en réseau, deux ordinateurs doivent utiliser le même **protocole**.

Par ex: HTTP (*HyperText Transfer Protocol*). Pages web
FTP (*File Transfer Protocol*, protocole de transfert de fichiers)
IMAP (*Internet Message Access Protocol*, utilisé pour s'échanger des e-mails)
SSH (*Secure Socket Shell,* utilisé pour sécuriser une liaison)

Internet est un environnement hostile, et la sécurité est notre l'affaire. Alors si vous vous connectez à une machine via Internet, il est recommandé d'utiliser le protocole **SSH** car c'est la solution pour sécuriser les données

La sécurité :





SSH

Avantages :

. SSH est un protocole hautement sécurisé qui fait appel à la cryptographie forte pour protéger votre connexion contre les écoutes, les détournements et autres attaques.

. La méthode employée par SSH est sûre, car pour accéder à votre compte utilisateur sur le serveur, *l'attaquant* doit d'abord réussir à accéder à votre machine client.

. SSH permet d'ouvrir une session sur le serveur sans avoir à taper un mot de passe.

. SSH vous permet de vous connecter au serveur et de passer une commande dans la foulée, de façon à ce que le serveur exécute la commande puis ferme la connexion tout de suite après, ce qui permet d'utiliser SSH pour des traitements automatisés, sans intervention humaine.

Le chiffrement :

Comment sont chiffrés les échanges avec SSH ?

SSH utilise les deux catégories suivantes de chiffrement pour garantir la sécurité.

- symétriques
- asymétriques

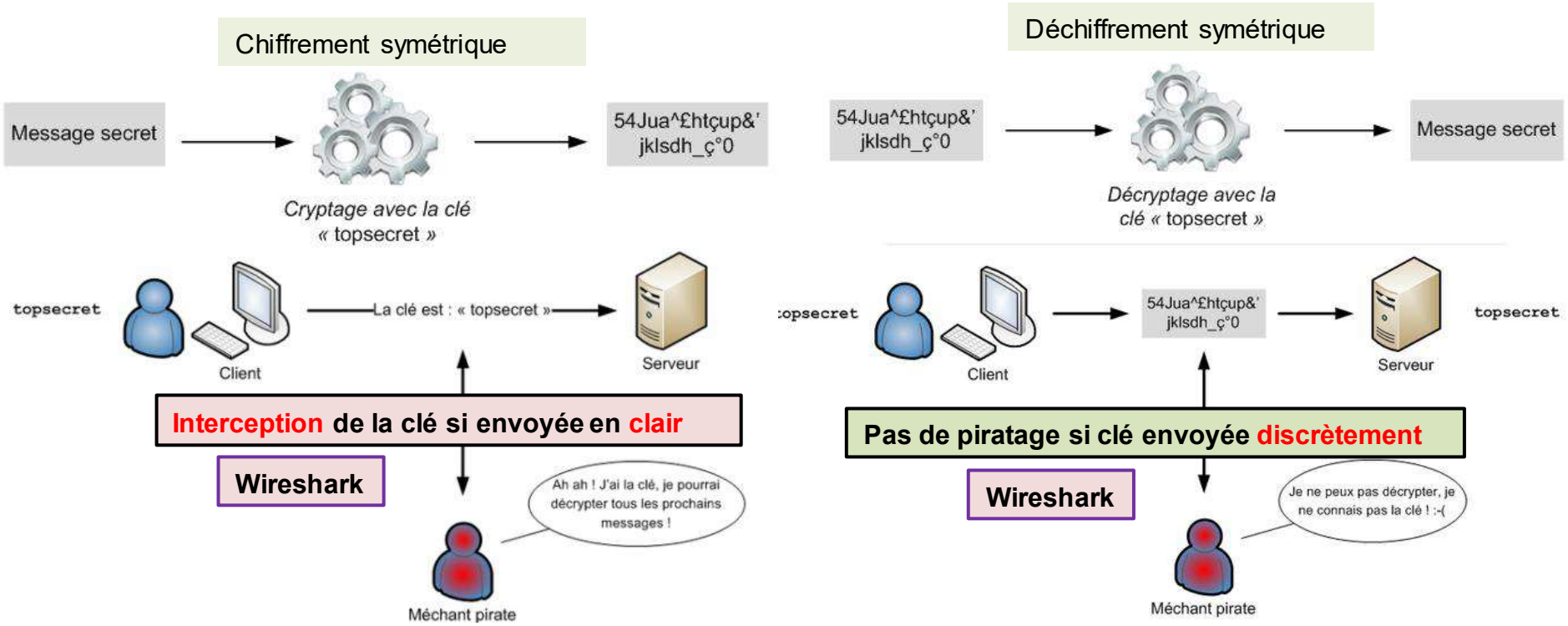
SSH

Le chiffrement symétrique:

Méthode de chiffrement la plus simple car facile à comprendre.

Utilisation d'une **clé** (un mot secret) pour chiffrer un message et le déchiffrer. (clé = topsecret)

Défaut : *Il faut transmettre la clé de chiffrement* ***(topsecret)*** ***discrètement*** *sinon piratage*



SSH

Le chiffrement asymétrique:

Pour palier la contrainte d'envoi de la clé de chiffrement discrètement, il faut chiffrer également la clé lors de l'envoi.

Pour chiffrer la clé de chiffrement symétrique, utilisation de la méthode : **le chiffrement asymétrique**.

Le chiffrement asymétrique, utilise une clé pour chiffrer, et une autre pour déchiffrer. (2 clés)

une clé dite « **publique** » qui sert à **chiffrer** ;
une clé dite « **privée** » qui sert à **déchiffrer**.

Fonctionnement :

L'ordinateur génère une paire de clés : une privée et une publique. Elles vont ensemble.

La clé publique peut être transmise en **clair sur le réseau**

La clé privée, qui permet donc de déchiffrer, doit **rester secrète**.

SSH

Exemple :

la clé publique 74A48vXX
la clé privée 99o0pn9.

Chiffrement avec la clé publique

Déchiffrement avec la clé privée

L'algorithme de chiffrement asymétrique le plus connu s'appelle **RSA**.

SSH

La création d'un tunnel sécurisé avec SSH

SSH utilise les deux chiffrements : asymétrique et symétrique dans cet ordre.

1. Utilisation d'abord du chiffrement asymétrique pour s'échanger discrètement une clé secrète de chiffrement symétrique.

2. Ensuite, utilisation tout le temps de la clé de chiffrement symétrique pour chiffrer les échanges.

Les ordinateurs s'échangent donc la clé de chiffrement symétrique de manière sécurisée (grâce au chiffrement asymétrique) et peuvent ensuite communiquer plus rapidement en utilisant en permanence le chiffrement symétrique.

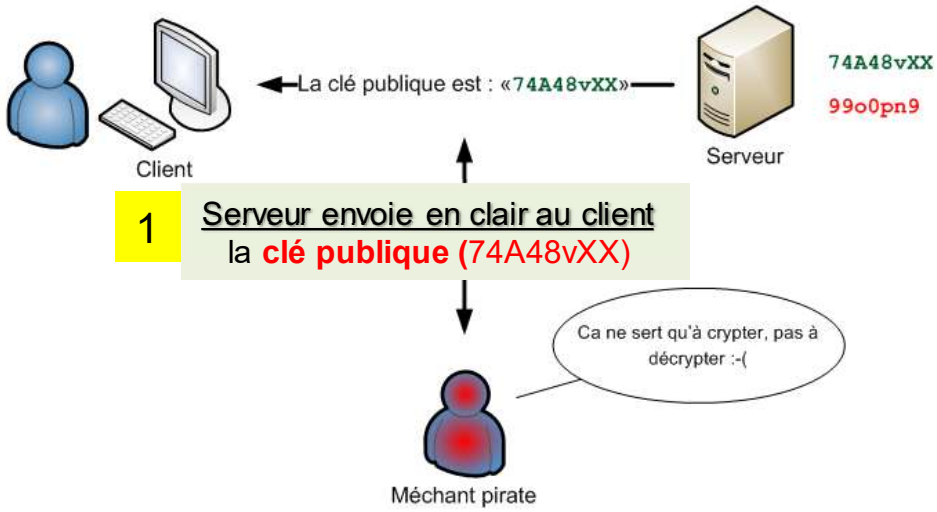
Etapes

Au début de la communication les ordinateurs s'échangent donc la clé de chiffrement symétrique de manière sécurisée (grâce au chiffrement asymétrique)

ils peuvent ensuite communiquer plus rapidement en utilisant en permanence le chiffrement symétrique.

SSH

.Les étapes de la création d'un canal sécurisé avec SSH en images

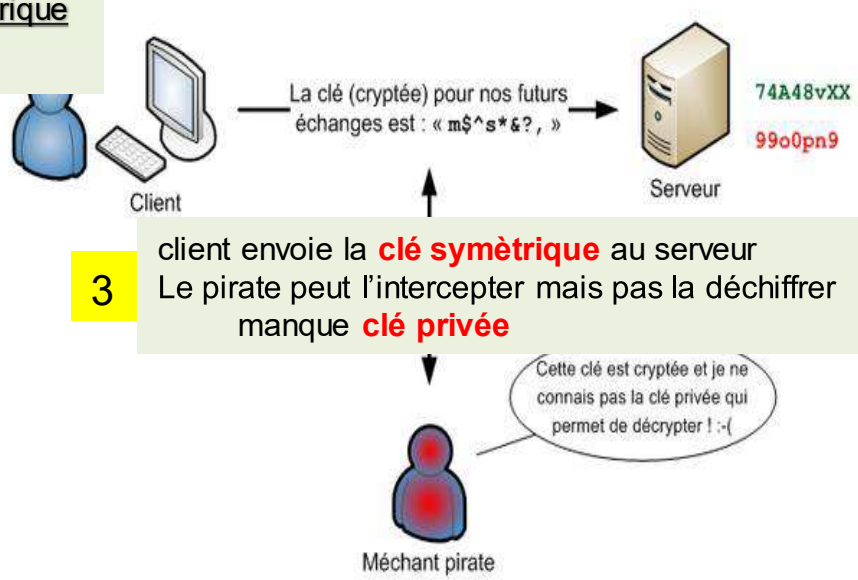


1 Serveur envoie en clair au client la **clé publique** (74A48vXX)

2 Client génère une **clé chiffrement symètrique** (*topsecret*) à partir de la **clé publique**

clé symètrique chiffrée

topsecret



3 client envoie la **clé symètrique** au serveur
Le pirate peut l'intercepter mais pas la déchiffrer manque **clé privée**

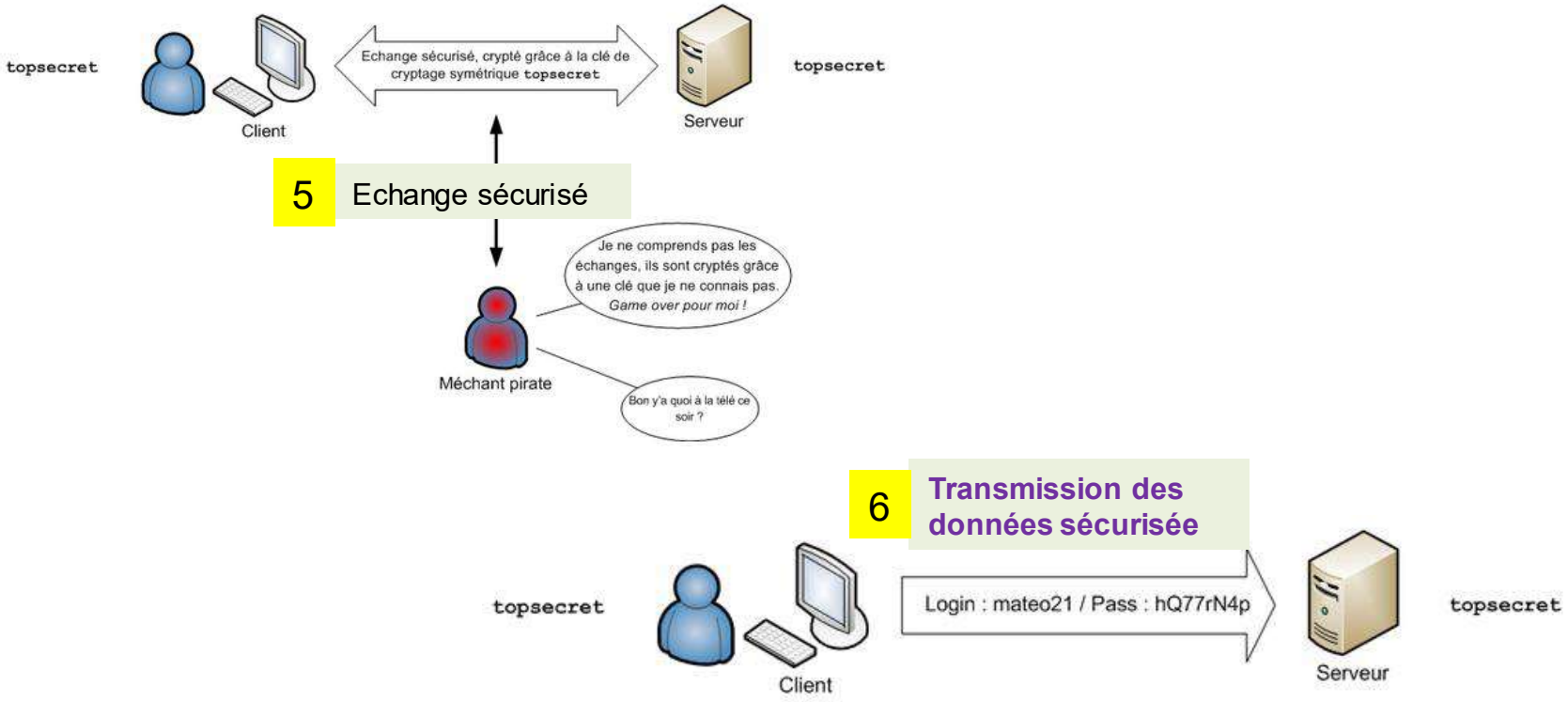
4 Serveur déchiffre la **clé reçue** avec sa **clé privée** (99o0pn9)

SSH

Le client et le serveur connaissent maintenant tous les deux la clé symétrique *topsecret,*
et à aucun moment ils ne l'ont échangée en clair sur le réseau.
Ils peuvent donc s'envoyer des messages chiffrés de manière symétrique en toute tranquillité.

Tout est chiffré grâce à la clé symétrique que le client et le serveur se sont **astucieusement** communiquée.

Maintenant qu'ils discutent de manière sécurisée, le client peut se connecter au serveur :
il peut donner son login et son mot de passe sans craindre de se les faire voler par le pirate.



Glossaire

Sigle	
FTP	**F**ile **T**ransfer **P**rotocol
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
IMAP	**I**nternet **M**essage **A**ccess **P**rotocol
IP	**I**nternet **P**rotocol
MAC	**M**edia **A**ccess **C**ontrol
SSH	**S**ecure **S**ocket S**H**ell