

Créer sa clé USB Rubber Ducky avec un Raspberry pi Zero



Ce tutoriel est basé sur le travail réalisé par Andrej Budincevic et Girst :

DroidDucky by Andrej Budincevic (<https://github.com/anbud/DroidDucky>)

hardpass by girst (<https://github.com/girst/hardpass>)

Le but de ce tutoriel est de modifier le HID du Raspberry afin qu'il soit détecté comme un périphérique de type « clavier USB ».

Ce tutoriel utilisera le système d'exploitation Raspbian, téléchargeable gratuitement depuis le site officiel :

<https://www.raspberrypi.org/downloads/raspbian>

Le logiciel Win32 Disk Imager sera utilisé pour installer l'iso Raspbian sur la carte microSD du Raspberry :

<https://sourceforge.net/projects/win32diskimager>

Le logiciel Putty sera utilisé pour accéder au Raspberry via le protocole SSH :

<http://www.putty.org>

Le Raspberry Pi utilisé dans ce tutoriel est un Raspberry Pi Zero v1.3, qui peut être acheté sur le site du revendeur officiel (lien suggéré) :

<https://www.kubii.fr/fr/kits-raspberry-pi/1411-raspberry-pi-zero-starter-kit-3272496003415.html>

Lien vers ma chaîne YouTube :

<http://www.youtube.com/channel/UCgrxDV9EPOLl1YMhziPed2g>

Ce tutoriel est disponible également au format vidéo sur YouTube :

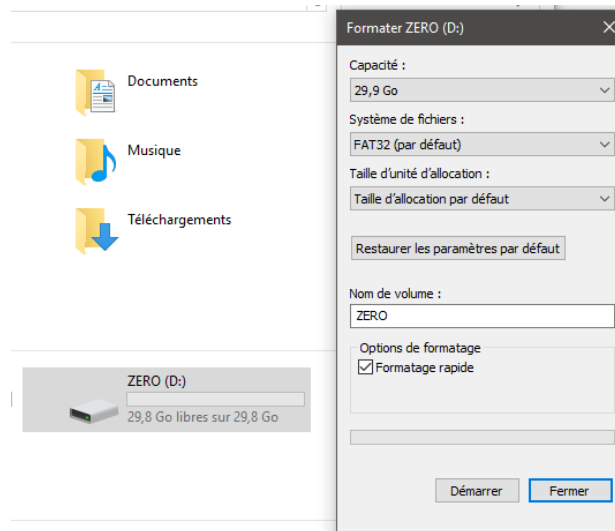
<https://www.youtube.com/watch?v=Xl2SdD1bS-0>

Lien vers mon site web :

<https://thiefin.fr>

1- Formater la carte microSD au format FAT32

Dans cet exemple, la carte sera identifiée en tant que lecteur D:

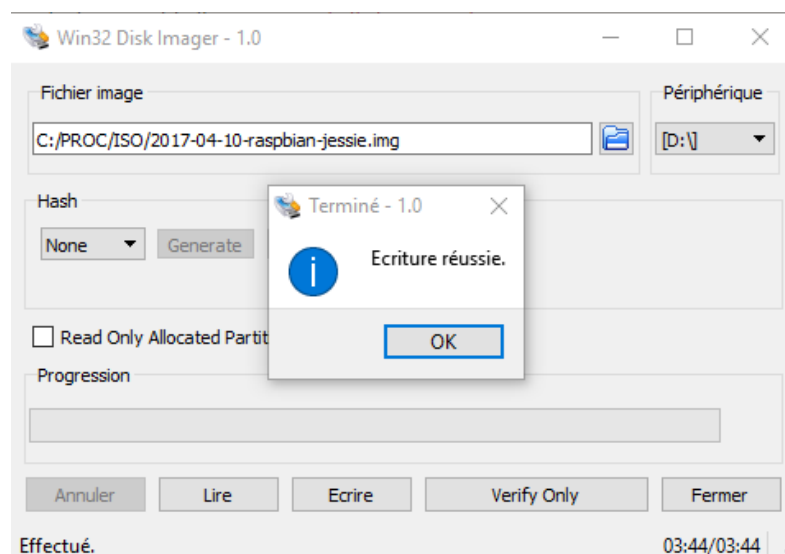
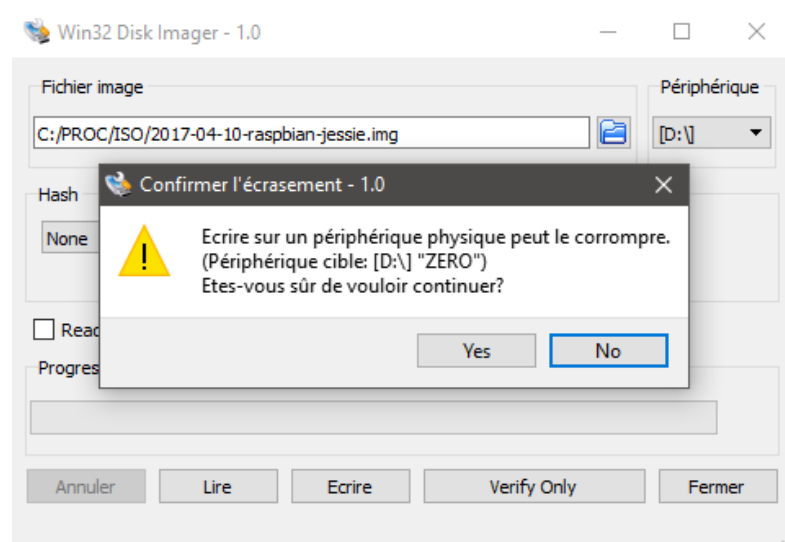
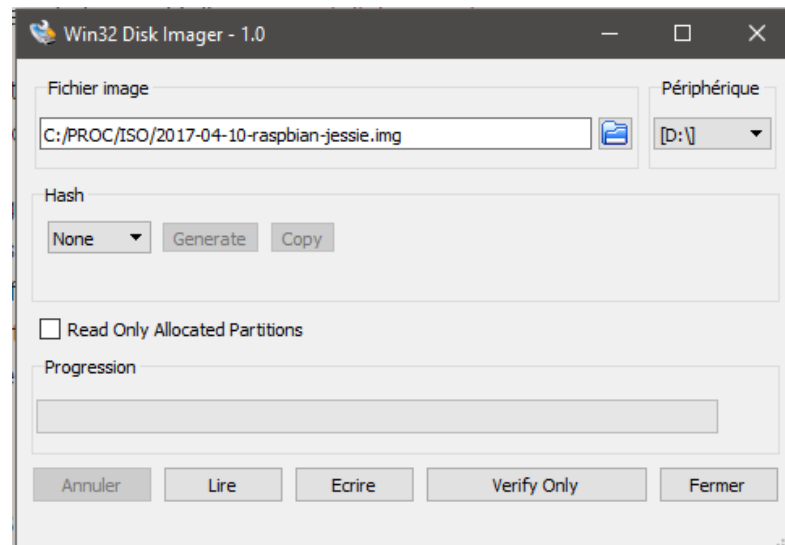


2- Télécharger le dernier iso d'installation du système d'exploitation Raspbian

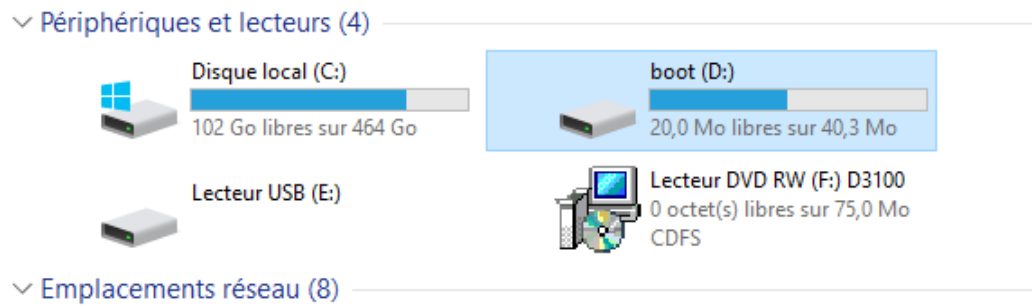
Site officiel : <https://www.raspberrypi.org>

A screenshot of the official Raspbian website. The top navigation bar includes links for BLOG, DOWNLOADS, COMMUNITY, HELP, FORUMS, and EDUCATION. The main heading is 'RASPBIAN'. Below this, text describes Raspbian as the Foundation's official supported operating system, available via NOOBS or direct download. It lists pre-installed software like Python, Scratch, and Java. Two download options are presented: 'RASPBIAN STRETCH WITH DESKTOP' and 'RASPBIAN STRETCH LITE'. Each option includes version information, release date, kernel version, and release notes. Download links for Torrent and ZIP are provided for both. A SHA-256 hash is displayed at the bottom of the download section. A note at the very bottom mentions Java SE Platform Products and the Wolfram Language.

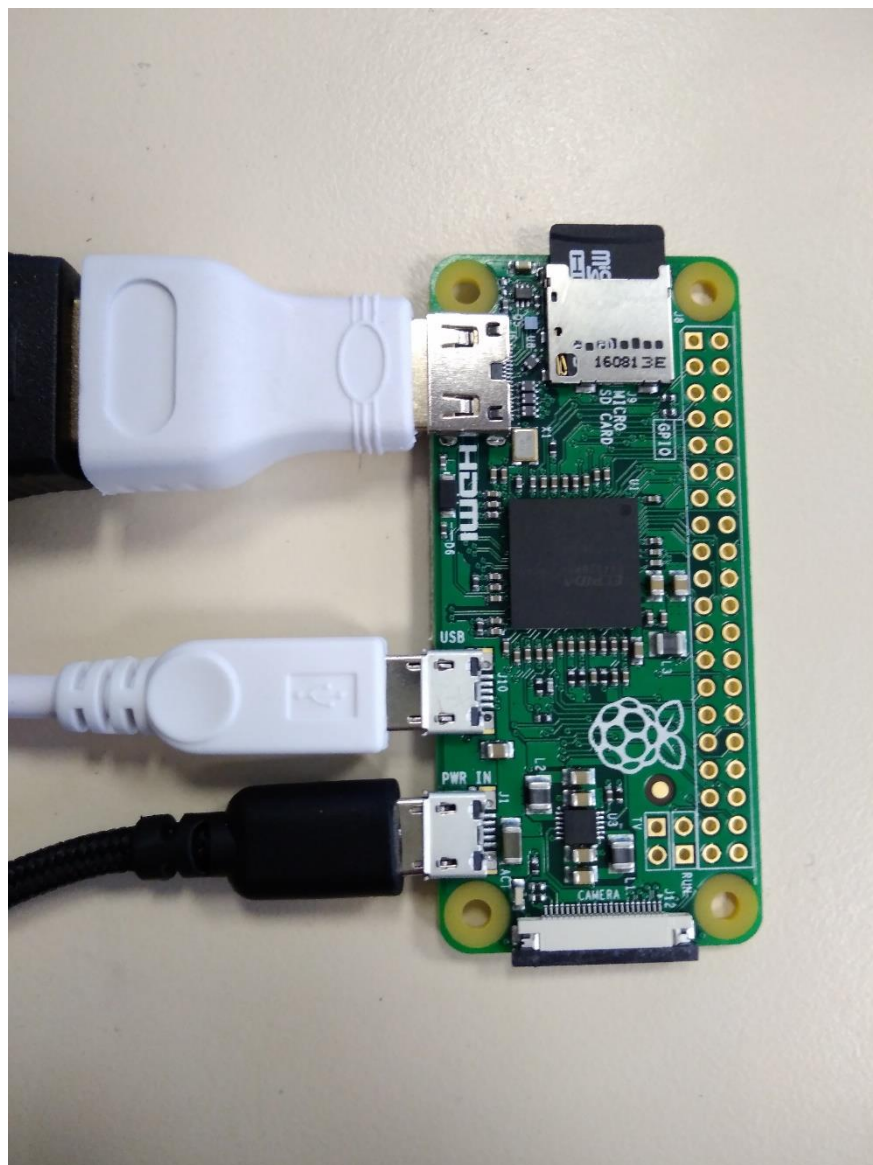
- 3- A l'aide du logiciel Win32 Disk Imager, installer l'iso Raspbian sur la carte microSD
- Lien de téléchargement de Win32 Disk Imager :
<https://sourceforge.net/projects/win32diskimager>



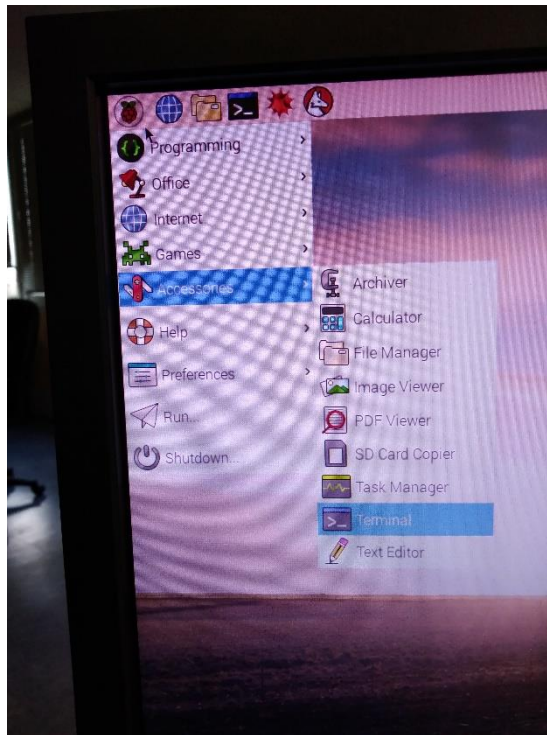
- 4- Une fois l'installation terminée, la partition de boot est accessible via l'explorateur de fichiers



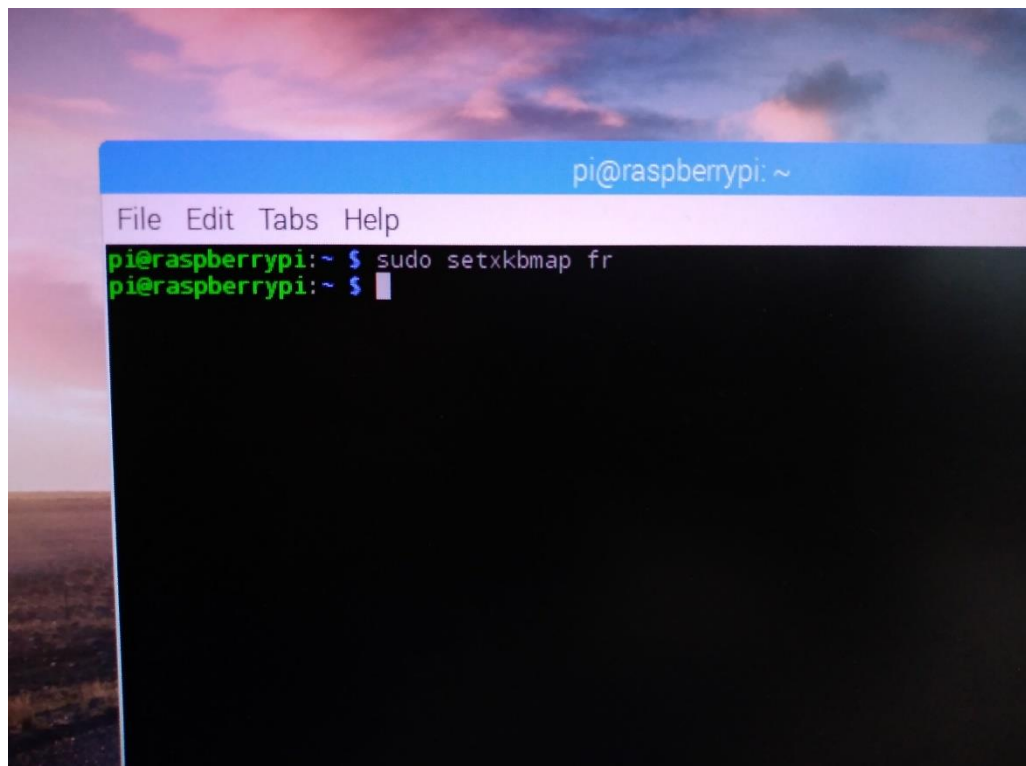
- 5- Brancher un écran sur le port HDMI du Raspberry grâce à l'adaptateur fourni, un clavier sur le port USB grâce à l'adaptateur fourni et un câble d'alimentation sur le port POWER



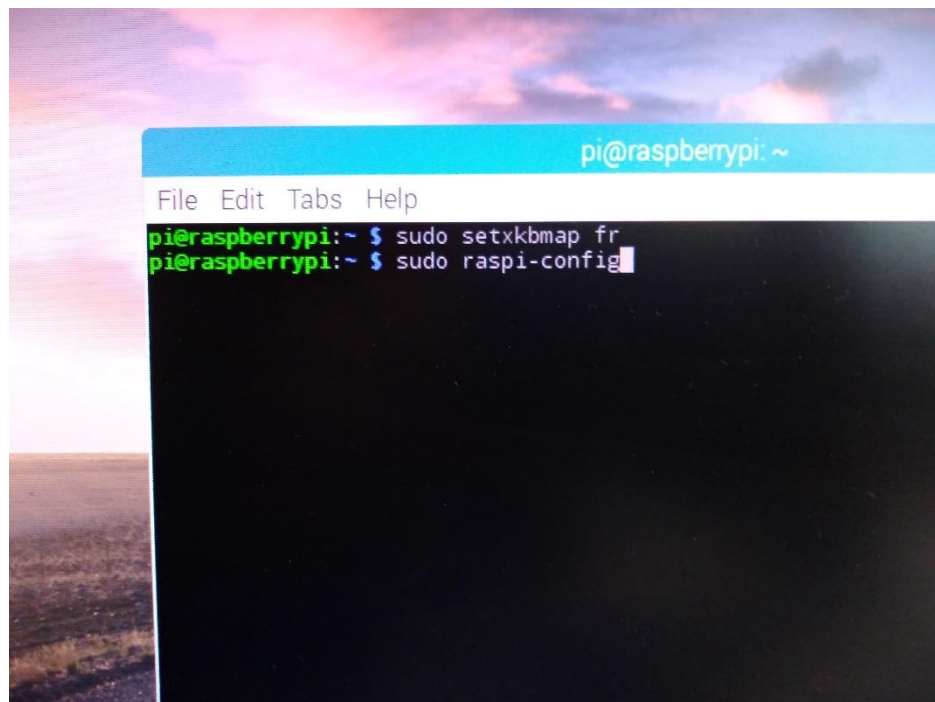
6- Ouvrez ensuite un terminal dans le menu de démarrage : Accessories > Terminal



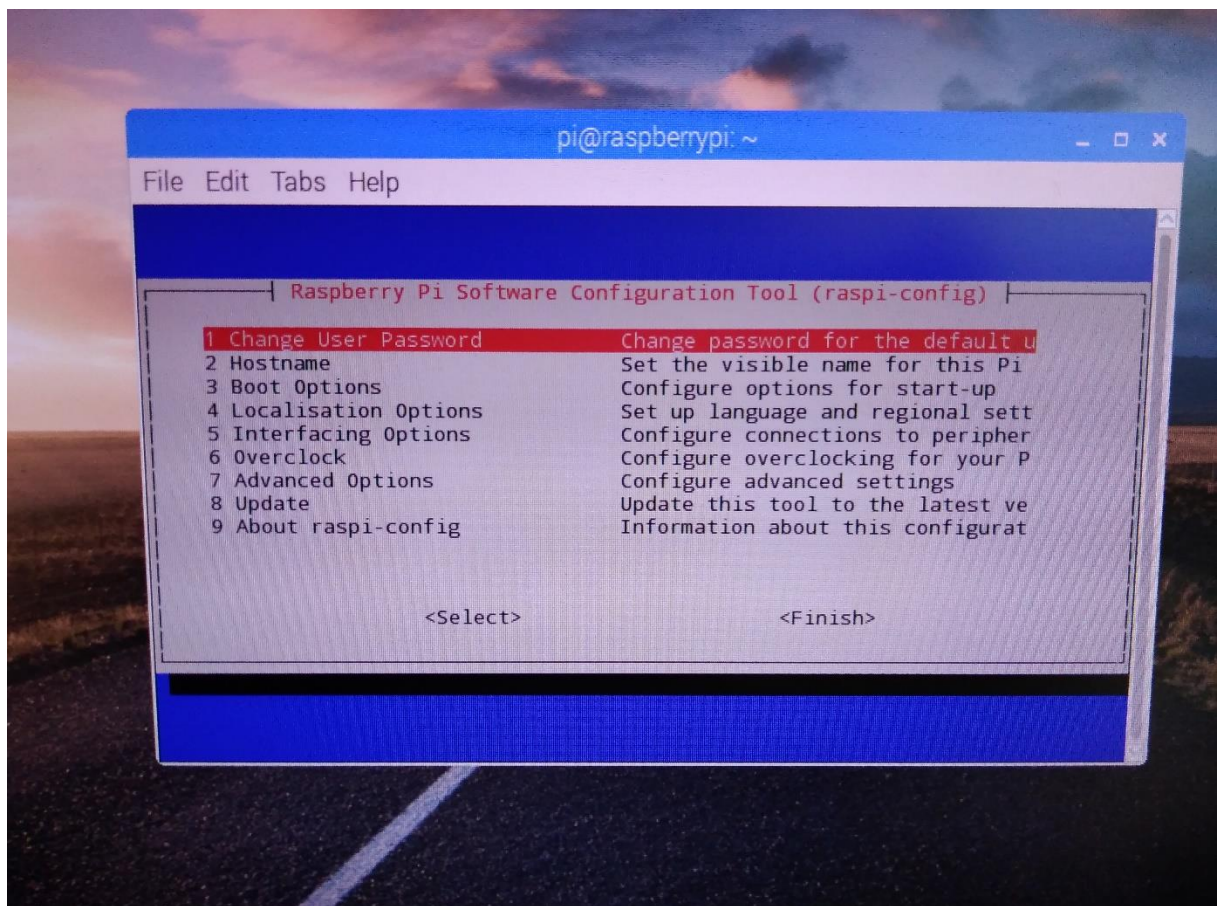
7- Par défaut, le clavier Raspbian est configuré en qwerty. Pour passer en disposition AZERTY, tapez la commande « sudo setxkbmap fr »



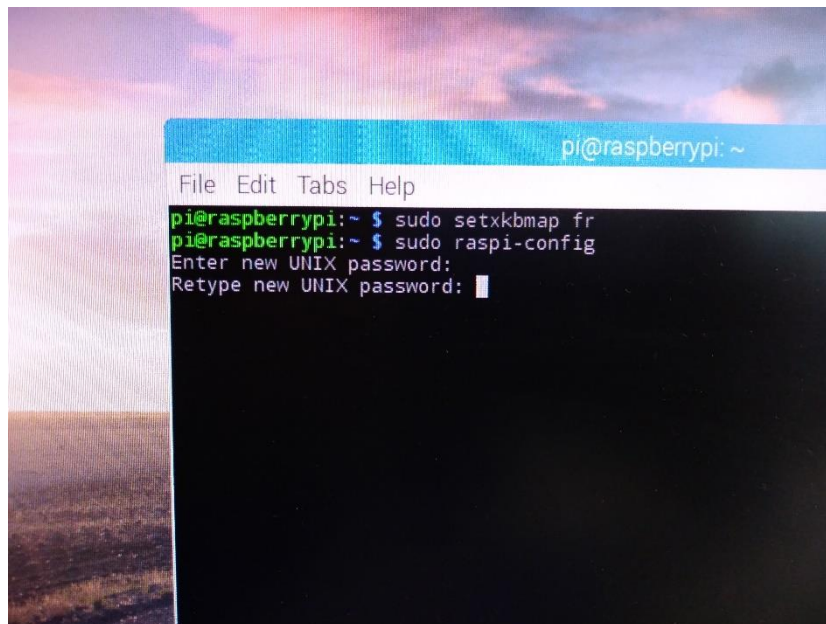
- 8- Ouvrez ensuite le menu de configuration de Raspbian en tapant la commande « sudo raspi-config »



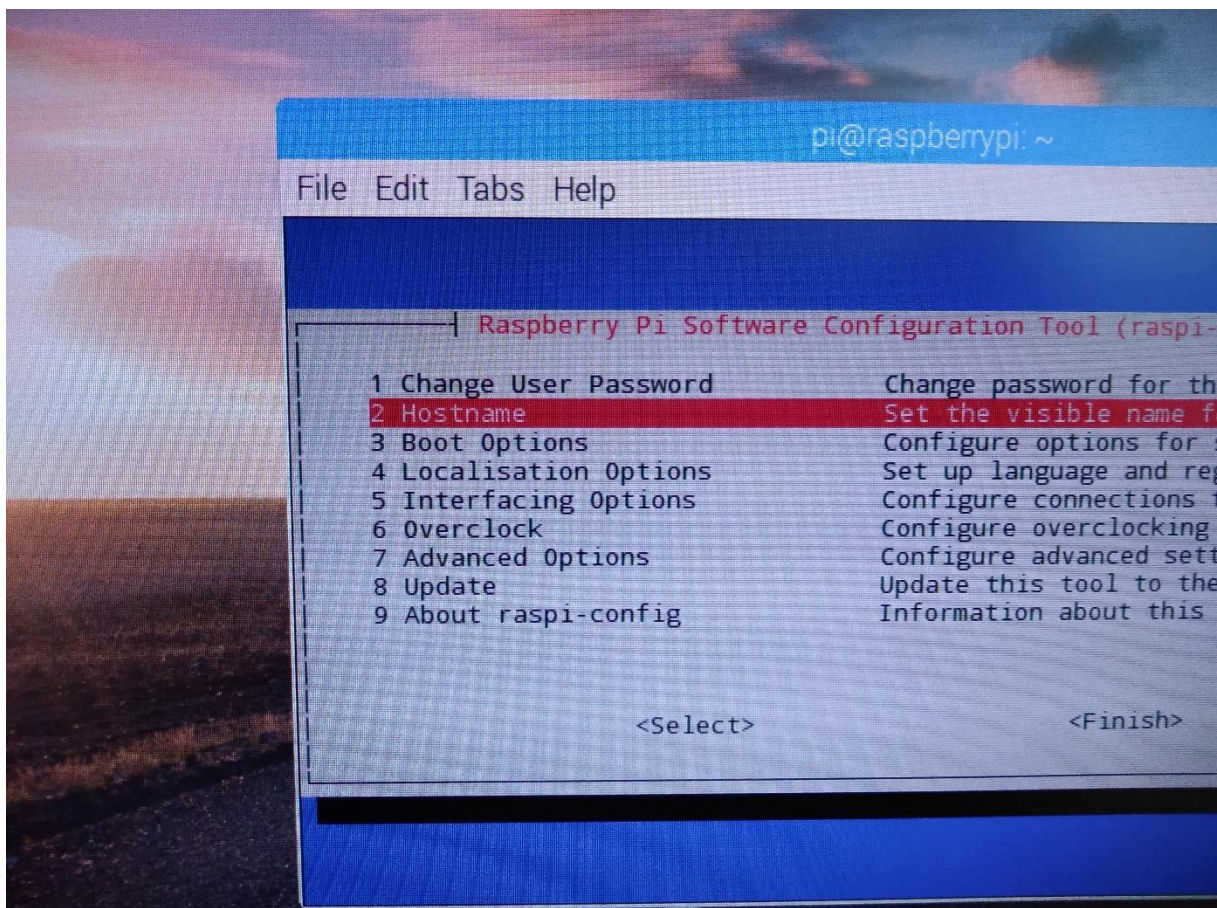
- 9- Dans un premier temps, sélectionnez « Change user password » afin de modifier le mot de passe par défaut du système



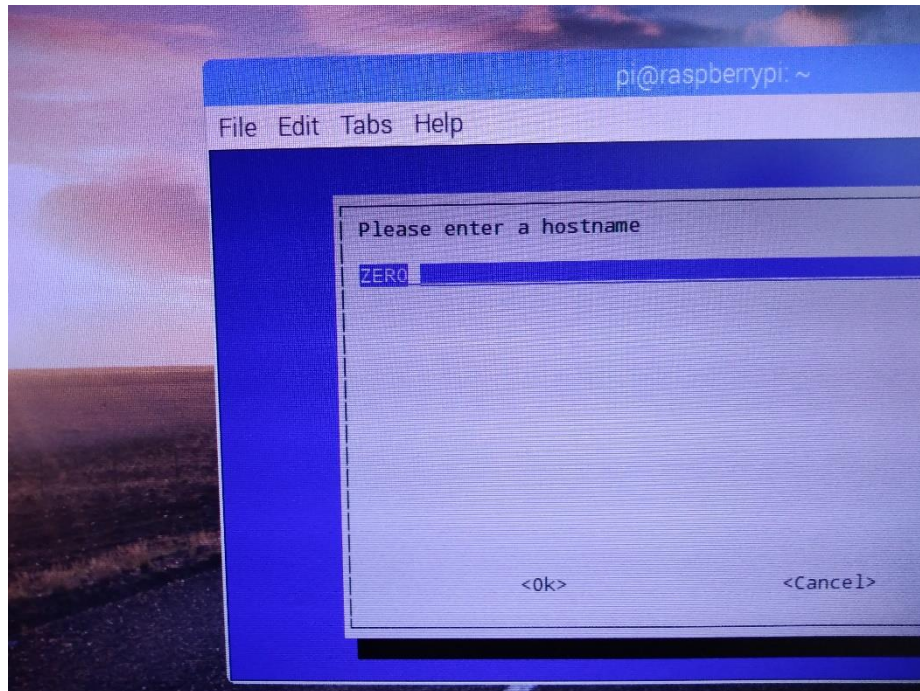
10- Entrez votre nouveau mot de passe. Une confirmation vous sera demandée.



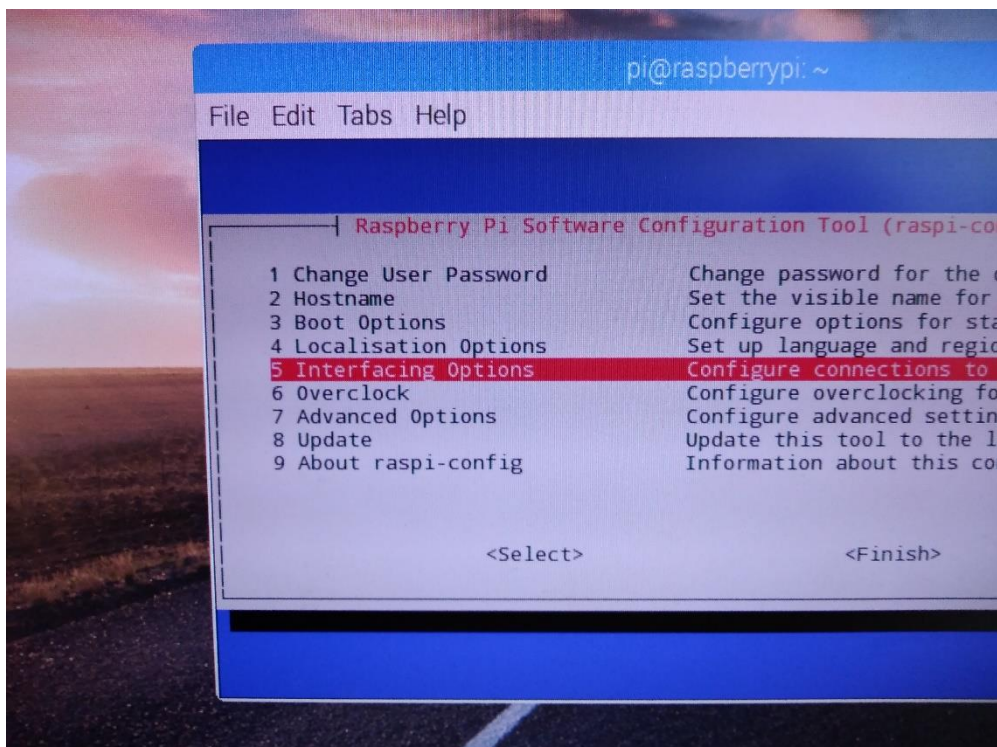
11- Choisissez ensuite l'option « Hostname » afin de modifier le nom de votre Raspberry



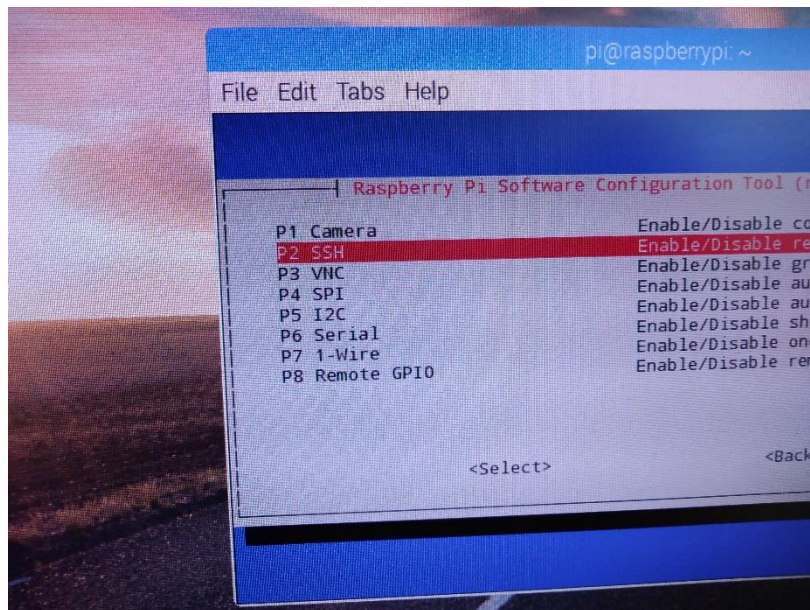
12- Dans ce tutoriel, le Raspberry s'appellera « ZERO »



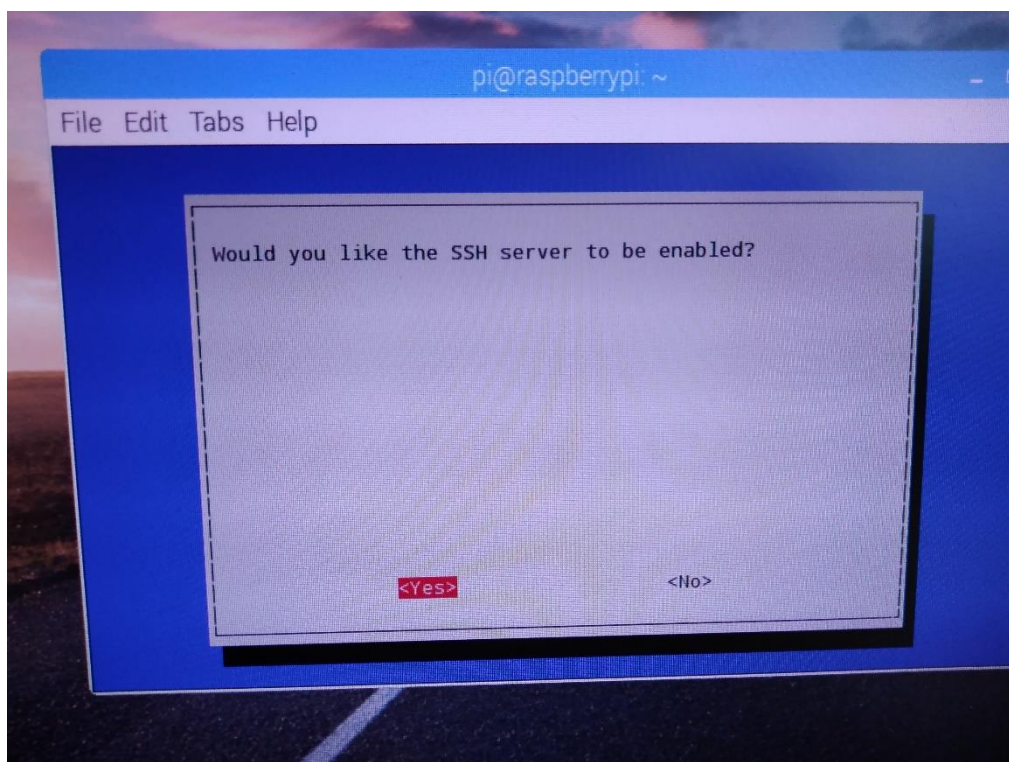
13- Choisissez ensuite l'option 5 : « Interfacing options »



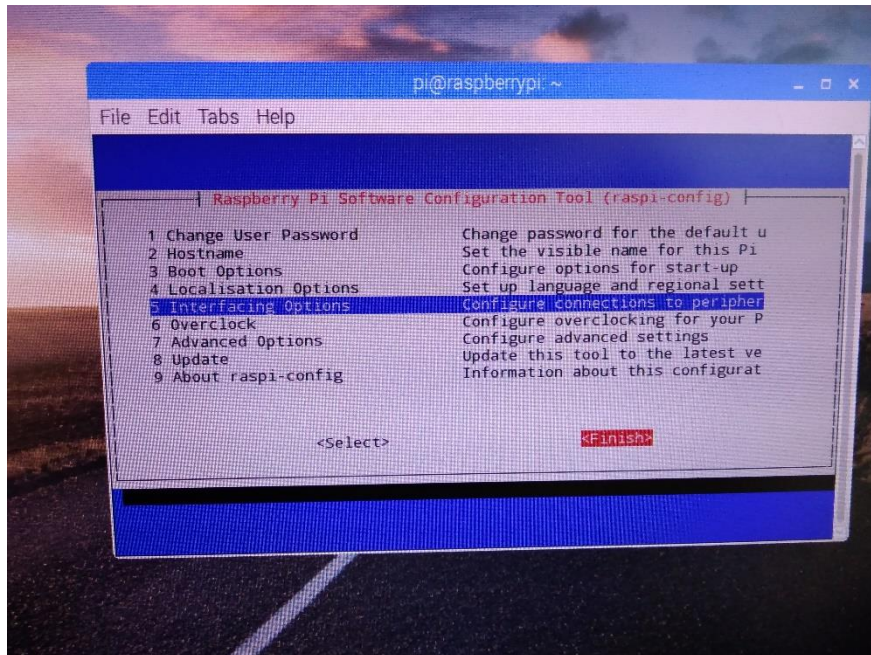
14- Sélectionnez ensuite l'option P2 : « SSH » afin d'activer le service SSH



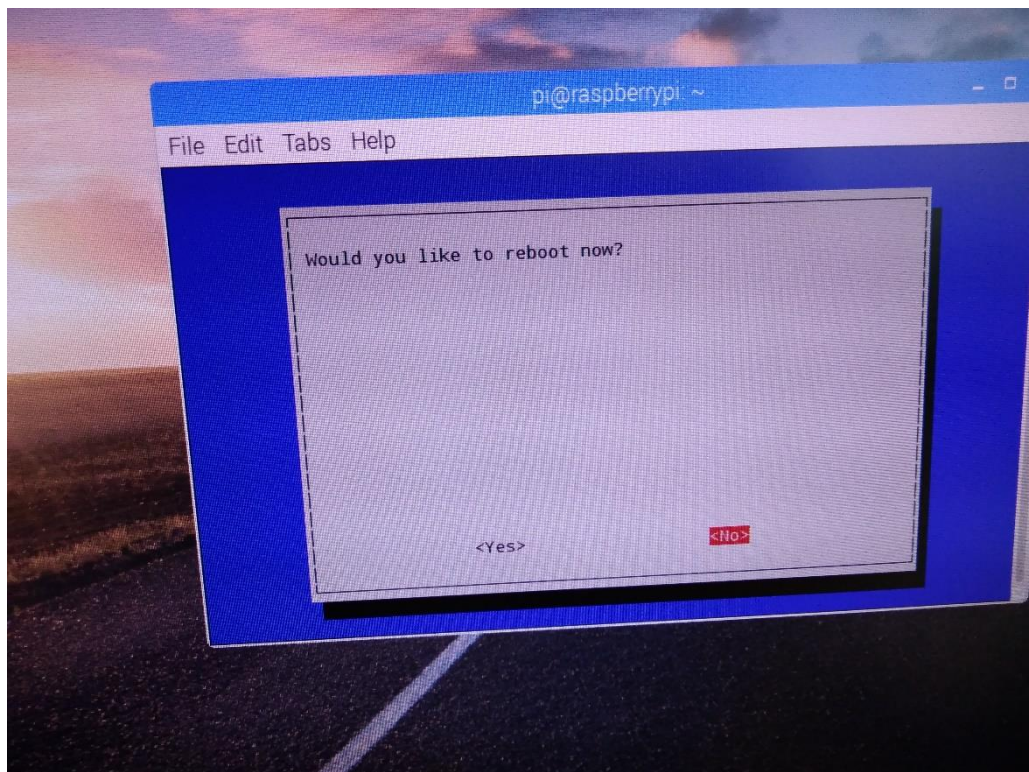
15- Confirmez l'activation du service SSH



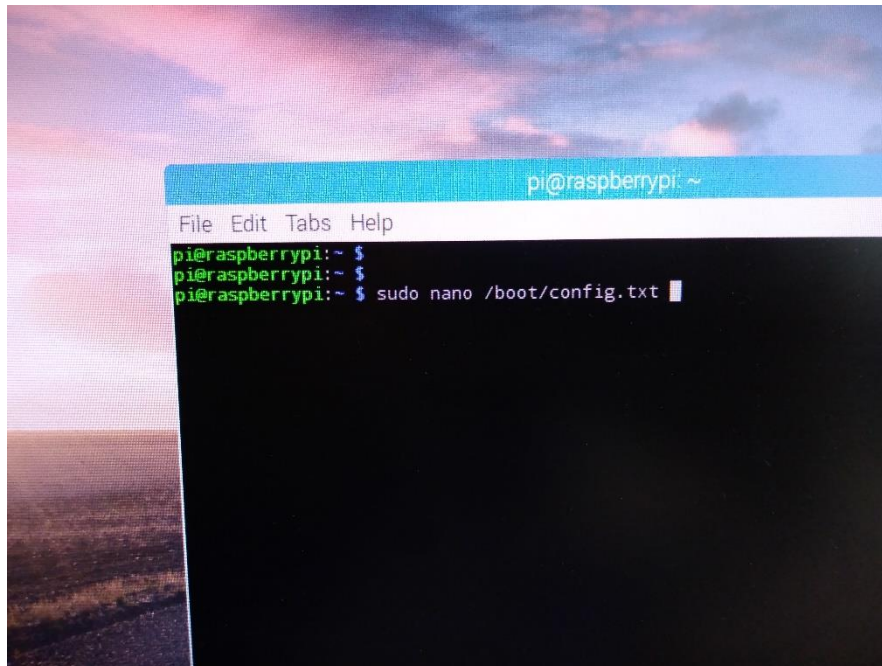
16- Sélectionnez « Finish » afin de quitter le menu de configuration



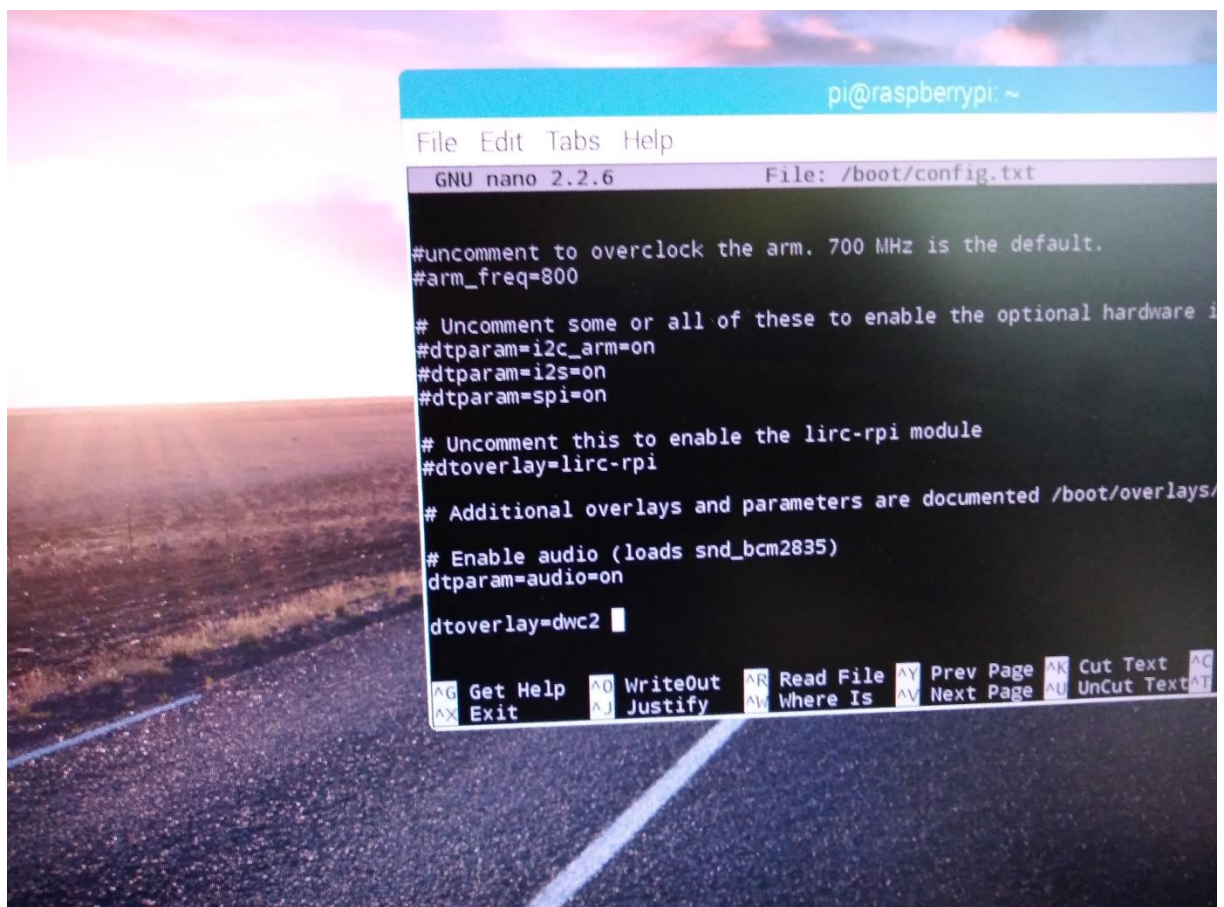
17- Une demande de redémarrage va apparaître, sélectionnez « Non » afin de ne pas redémarrer tout de suite



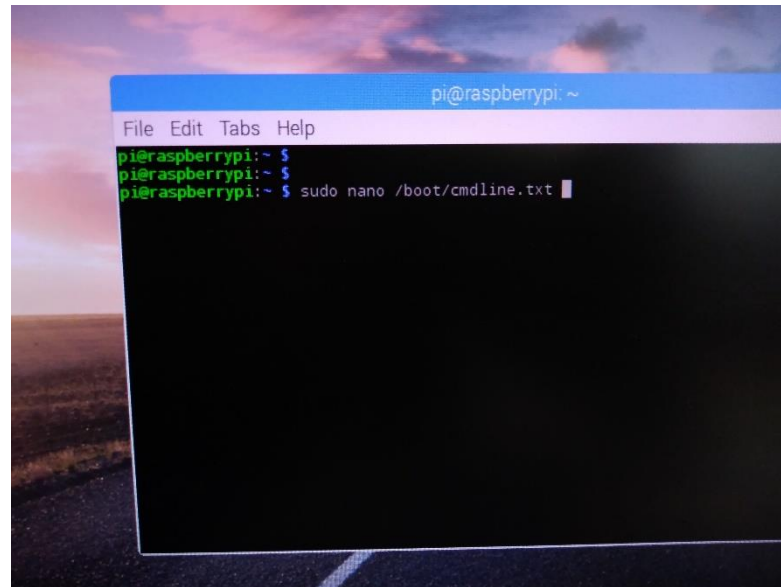
18- Exécutez ensuite la commande « sudo nano /boot/config.txt »



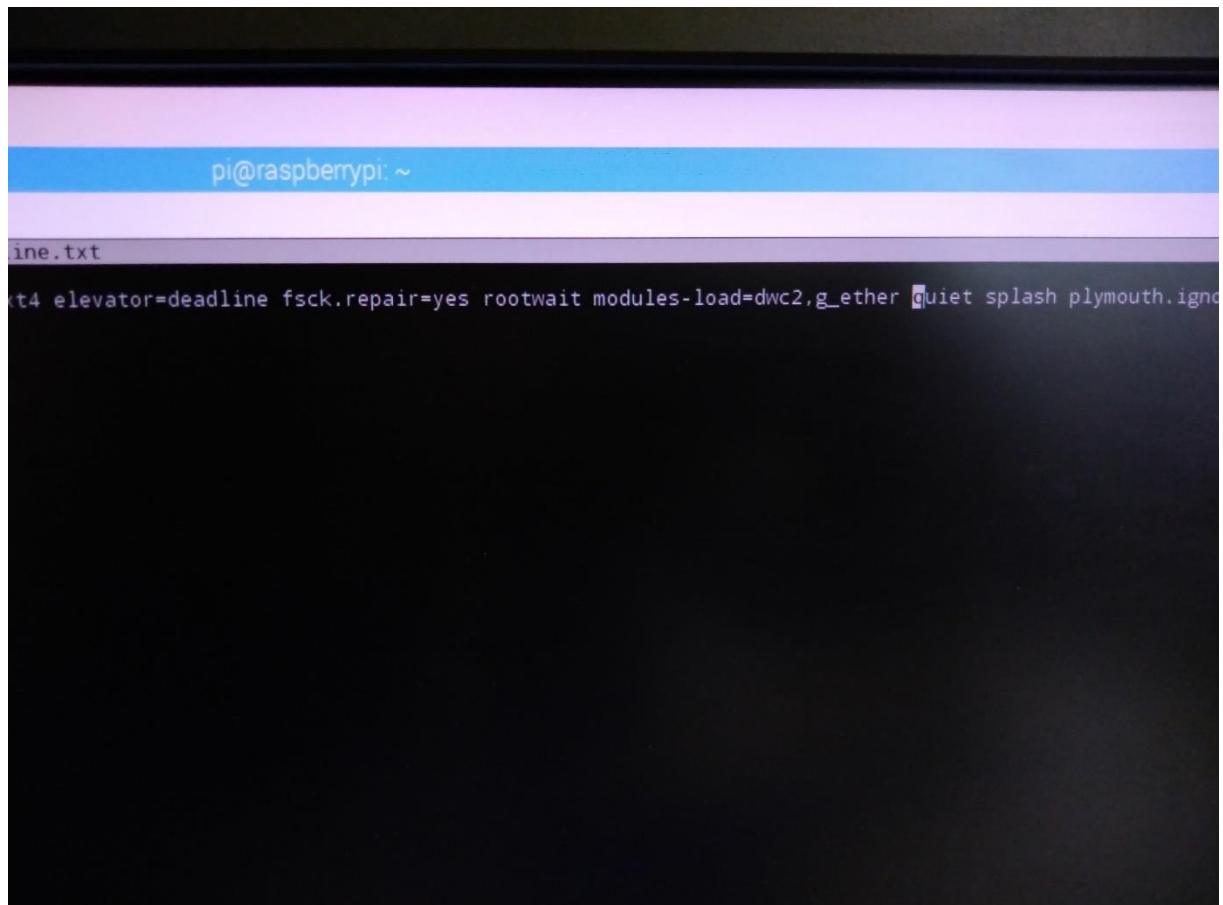
19- A la fin du fichier, ajoutez la ligne « dtoverlay=dwc2 » puis sauvegardez le fichier (Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)



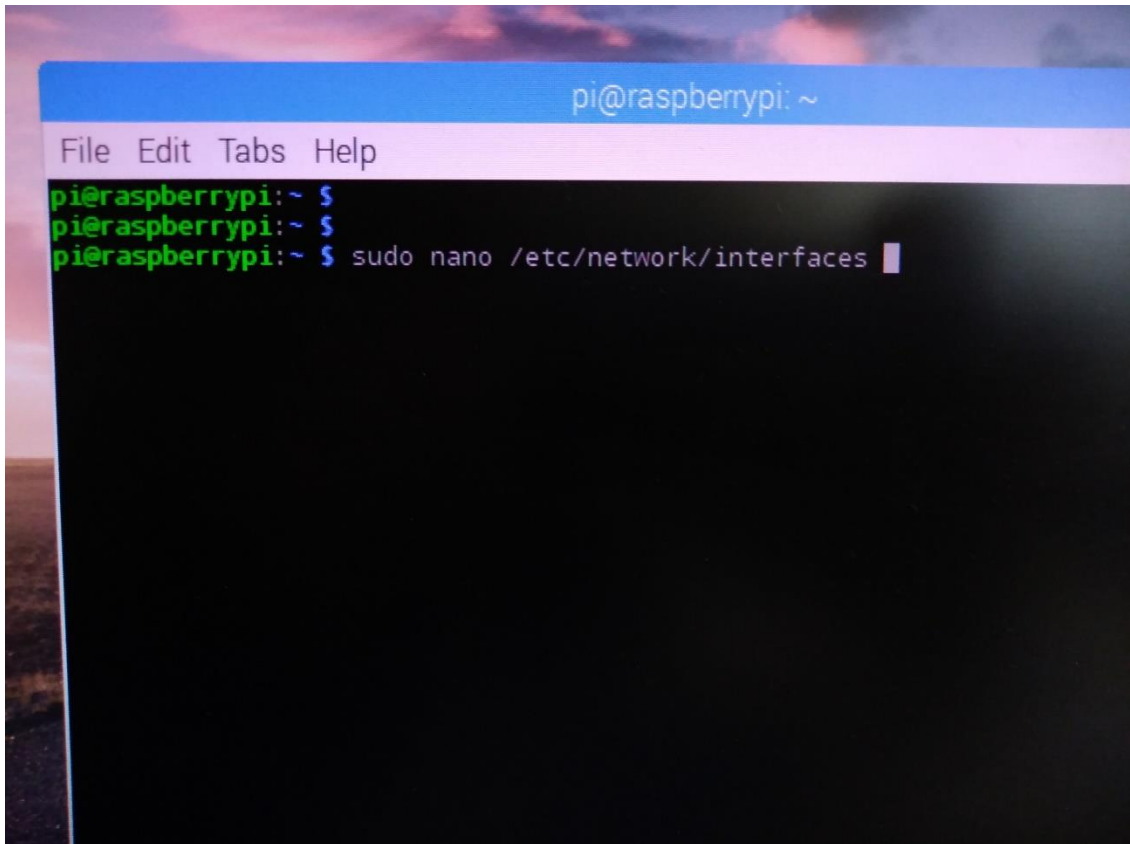
- 20- Modifier de la même manière le fichier *cmdline.txt* en exécutant la commande
« `sudo nano /boot/cmdline.txt` »



- 21- Rajoutez entre les éléments **rootwait** et **quiet** :
« `modules-load=dwc2,g_ether` » puis sauvegardez le fichier
(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)



22- Modifiez la configuration réseau de votre Raspberry en exécutant la commande :
« sudo nano /etc/network/interfaces »

A screenshot of a terminal window on a Raspberry Pi. The window has a blue title bar with the text 'pi@raspberrypi: ~'. Below the title bar is a menu bar with 'File', 'Edit', 'Tabs', and 'Help'. The terminal shows three lines of text: 'pi@raspberrypi: ~ \$', 'pi@raspberrypi: ~ \$', and 'pi@raspberrypi: ~ \$ sudo nano /etc/network/interfaces'. The cursor is at the end of the third line. The background of the terminal is black, and the text is green and white. The window is set against a background image of a sunset or sunrise over a body of water.

23- Ajoutez les lignes suivantes à la fin du fichier, en respectant les tabulations :

« auto usb0

iface usb0 inet static

 address 10.254.1.1

 netmask 255.255.255.0

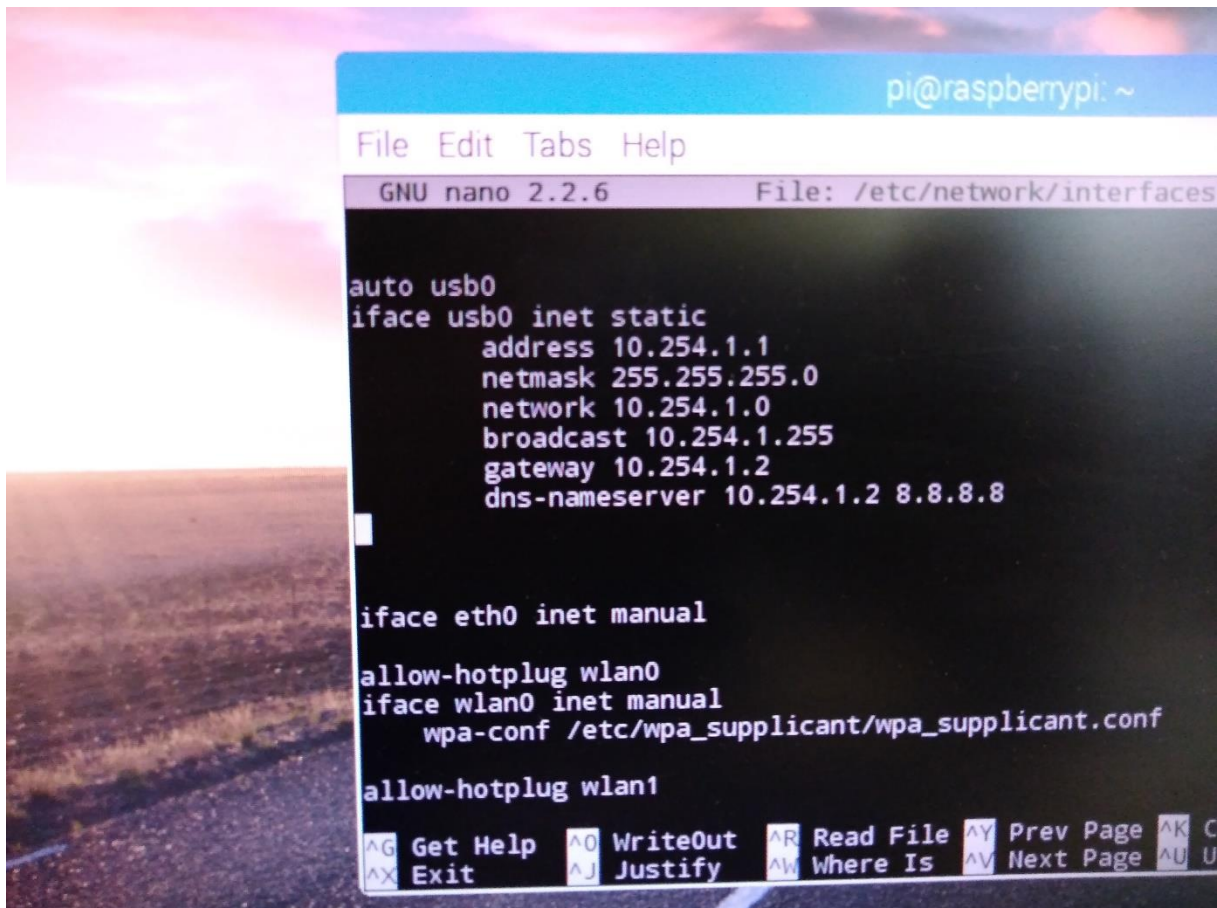
 network 10.254.1.0

 broadcast 10.254.1.255

 gateway 10.254.1.2

 dns-nameserver 10.254.1.2 8.8.8.8 » puis sauvegardez le fichier

(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)



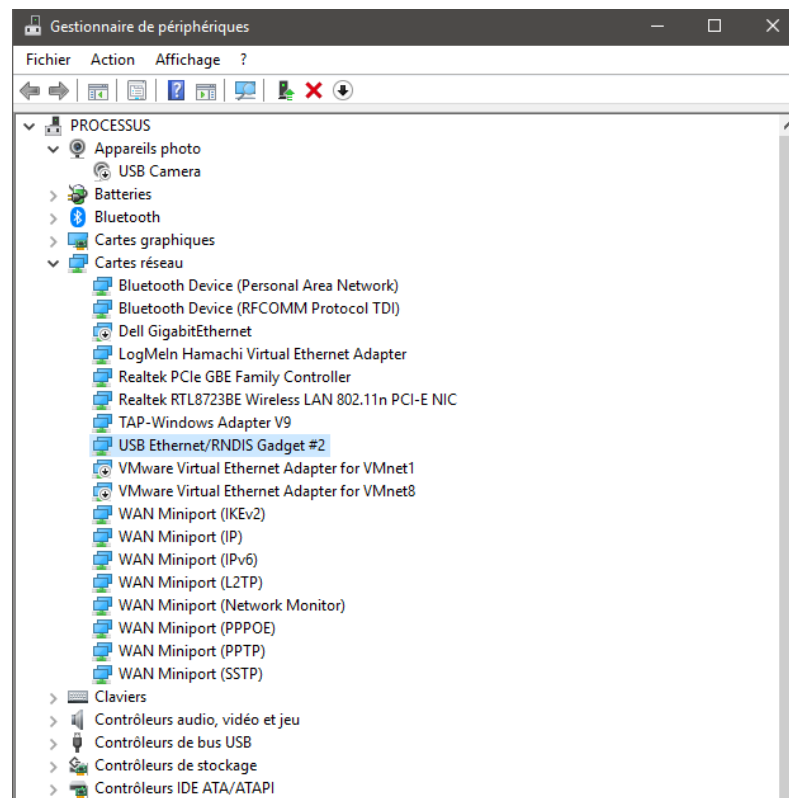
```
pi@raspberrypi: ~  
File Edit Tabs Help  
GNU nano 2.2.6 File: /etc/network/interfaces  
  
auto usb0  
iface usb0 inet static  
    address 10.254.1.1  
    netmask 255.255.255.0  
    network 10.254.1.0  
    broadcast 10.254.1.255  
    gateway 10.254.1.2  
    dns-nameserver 10.254.1.2 8.8.8.8  
  
iface eth0 inet manual  
  
allow-hotplug wlan0  
iface wlan0 inet manual  
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf  
  
allow-hotplug wlan1  
  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K C  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U U
```

24- Arrêtez ensuite votre Raspberry en exécutant la commande « `sudo shutdown -h now` »

Une fois complètement arrêté, débranchez les câbles de votre Raspberry et connectez-le à votre ordinateur à l'aide d'un câble microUSB vers USB que vous brancherez sur le port USB de votre Raspberry Zéro



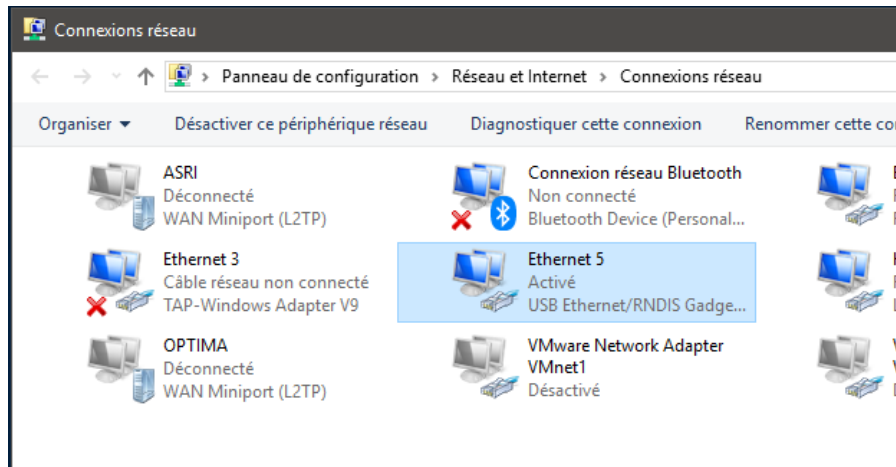
25- Une fois branché, votre Raspberry démarrera automatiquement et sera détecté en tant que périphérique de type Carte réseau



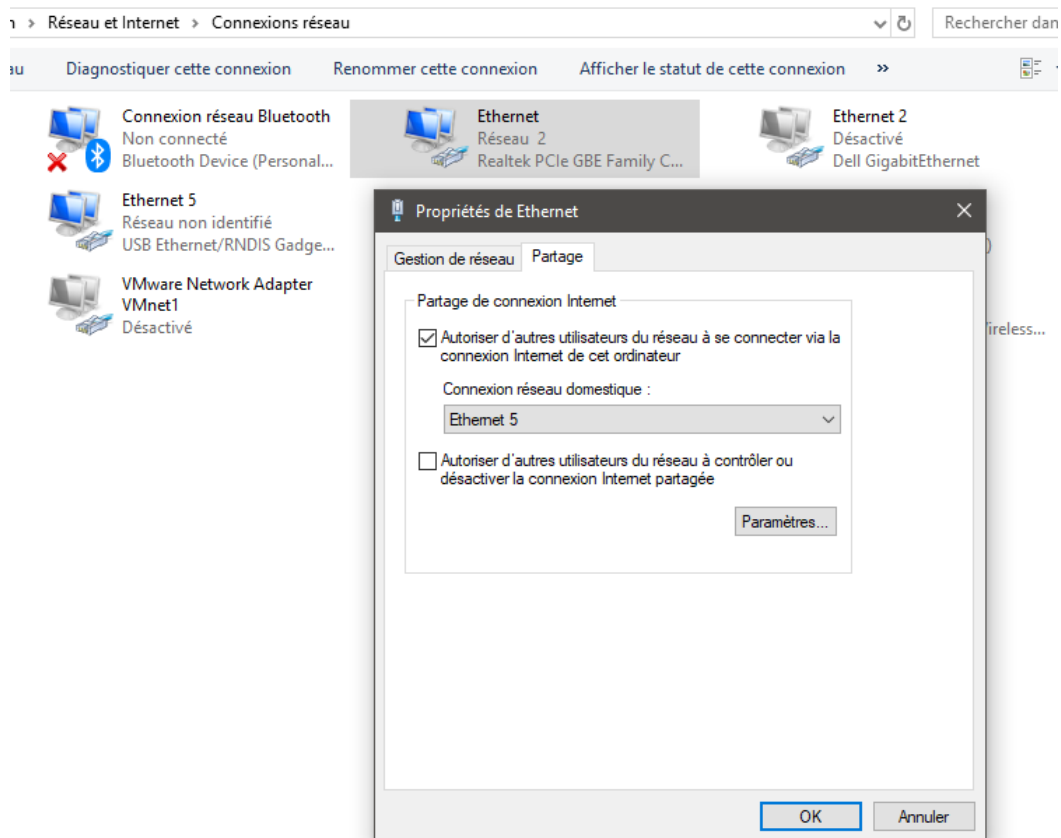
Pour les utilisateurs de Windows 10 il est nécessaire d'installer le pilote RNDIS afin que le Raspberry soit détecté en tant que tel.

Vous pouvez le télécharger à cette adresse : <https://thiefin.fr/zerodrivers.zip>

- 26- Ouvrez le panneau de configuration et naviguez jusqu'à « Connexions réseau ». Identifiez le nom de la carte réseau de type USB Ethernet/RNDIS Gadget
Dans cet exemple, la carte s'appelle « Ethernet 5 »

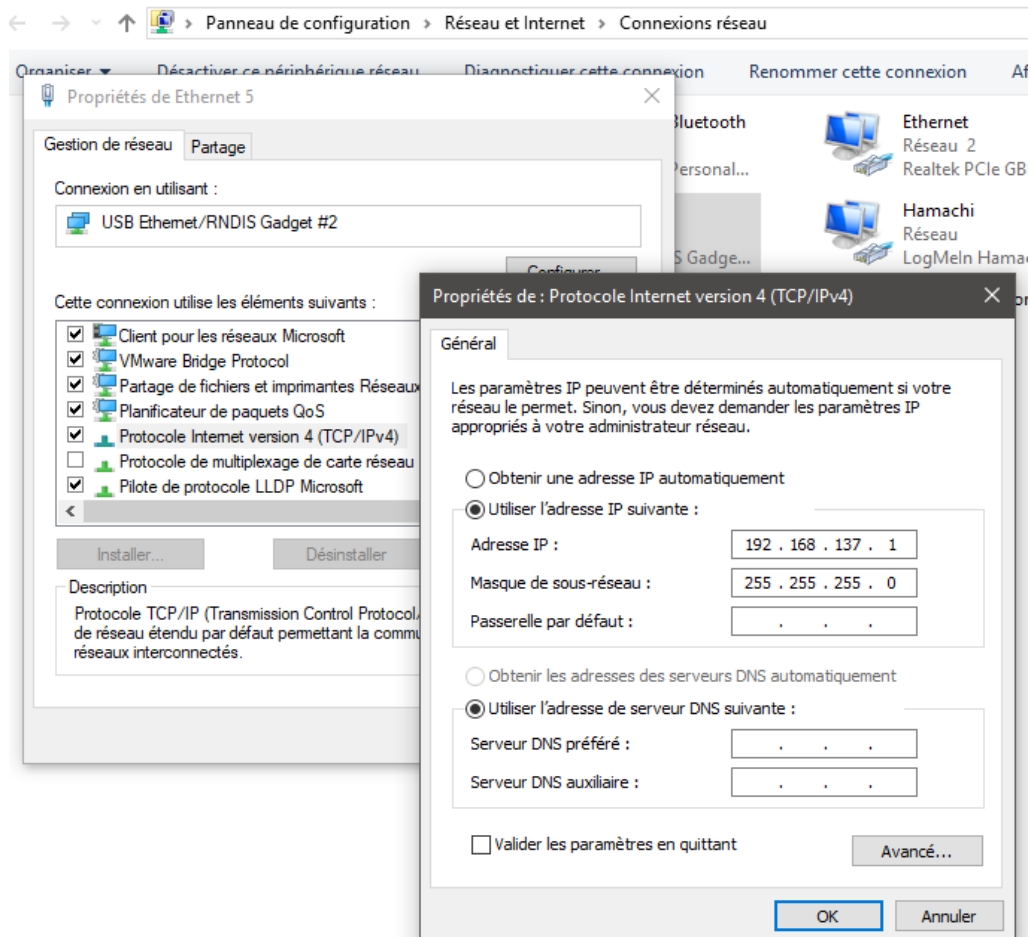


- 27- Identifiez maintenant la carte réseau qui correspond à l'interface qui vous fournit votre accès internet, puis faites un clic droit dessus et choisissez « Propriétés ». Sélectionnez ensuite l'onglet « Partage » et activez le partage de connexion internet pour la carte réseau de votre Raspberry
Dans cet exemple, il s'agit de la carte réseau « Ethernet 2 »



28- Faites un clic droit sur la carte réseau de votre Raspberry et sélectionnez « Propriétés ». Sélectionnez ensuite la ligne « Protocole Internet version 4 (TCP/IPv4) » et cliquez sur « Propriétés ».

Remplacez la ligne Adresse IP en remplaçant « 192.168.137.1 » par « 10.254.1.2 »



☐ Obtenir une adresse IP automatiquement

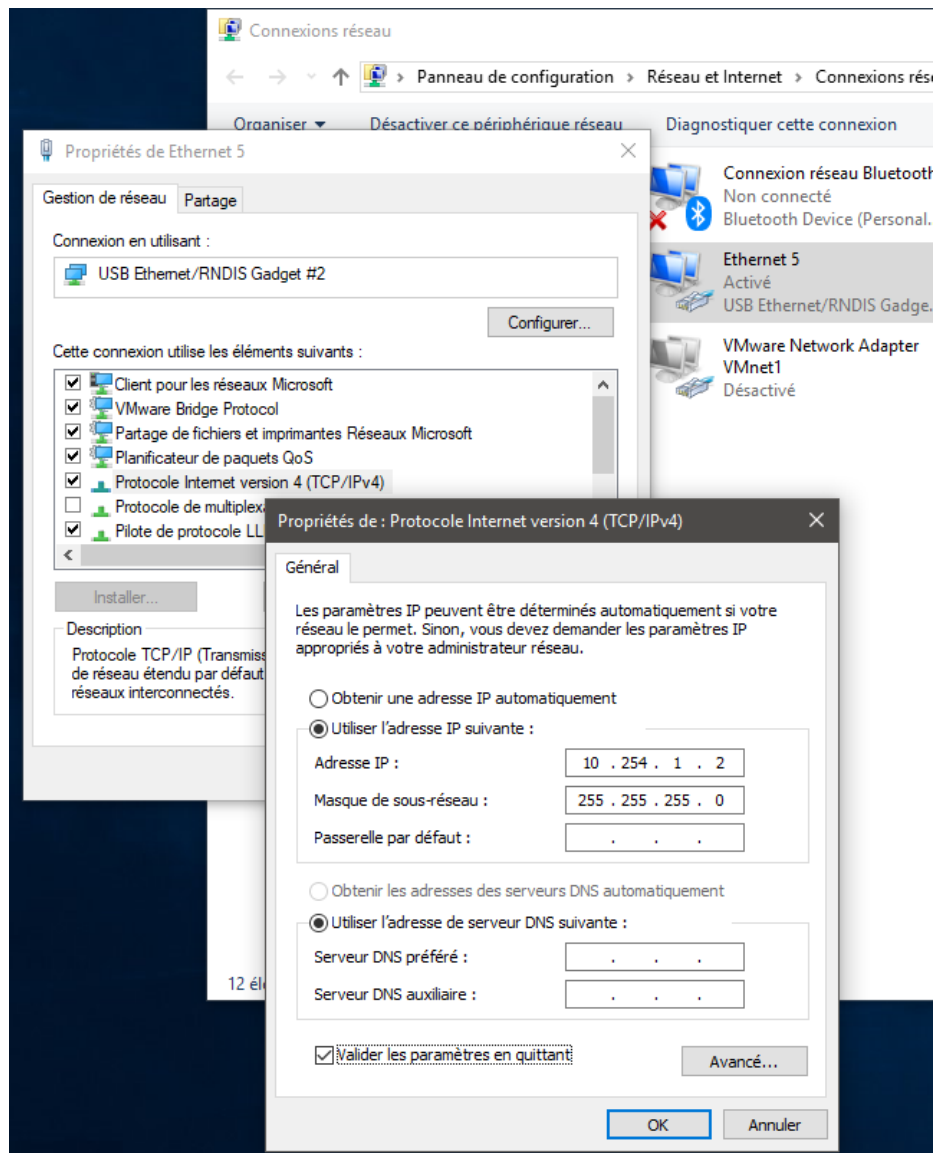
☒ Utiliser l'adresse IP suivante :

Adresse IP :

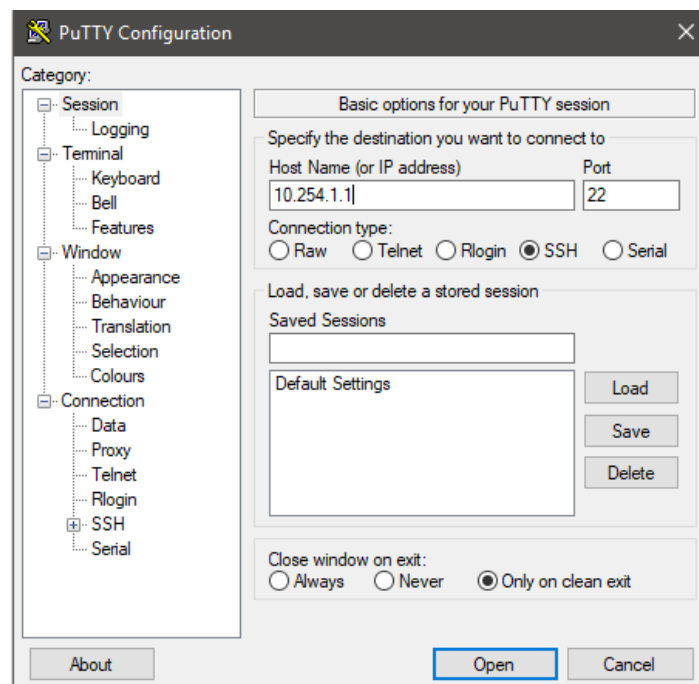
Masque de sous-réseau :

Passerelle par défaut :

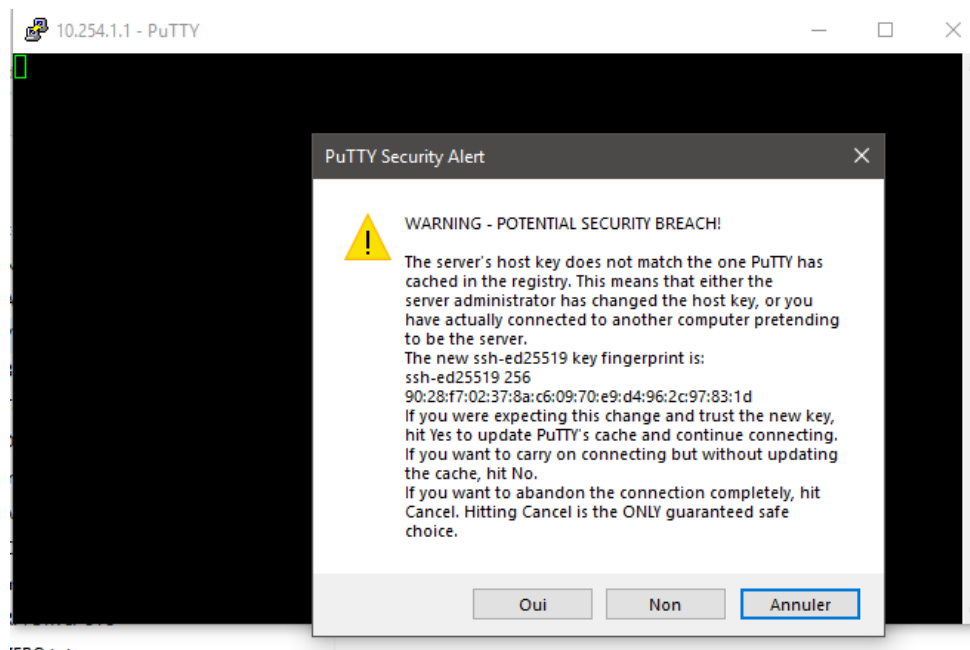
29- Sélectionnez « Valider les paramètres en quittant » puis cliquez sur « OK »



30- Exécutez ensuite le logiciel *PuTTY* et renseignez dans le champ « Host Name (or IP address) » l'adresse IP « 10.254.1.1 » puis cliquez sur *Open*



31- Lors de la première connexion, une alerte de sécurité va apparaître, cliquez simplement sur « Oui »



- 32- Identifiez-vous avec le nom d'utilisateur « pi » et le mot de passe que vous avez choisi lors de la configuration initiale
Si vous n'avez pas changé de mot de passe, celui par défaut est « raspberrypi »

```
pi@ZERO: ~
login as: pi
pi@10.254.1.1's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 10 10:20:15 2017
pi@ZERO:~ $
```

- 33- A ce stade, votre Raspberry a accès à internet au travers du partage de connexion de votre ordinateur. Exécutez la commande « sudo apt-get update » afin de mettre à jour la liste des dépôts de Raspbian

```
pi@ZERO: ~
pi@ZERO:~ $
pi@ZERO:~ $
pi@ZERO:~ $ sudo apt-get update
Get:1 http://mirrordirector.raspbian.org jessie InRelease [14.9 kB]
Get:2 http://archive.raspberrypi.org jessie InRelease [22.9 kB]
Get:3 http://mirrordirector.raspbian.org jessie/main armhf Packages [9,536 kB]
Get:4 http://archive.raspberrypi.org jessie/main armhf Packages [171 kB]
```

- 34- Ce tutoriel nécessite l'utilisation d'un pilote spécifiquement développé pour un noyau en version 4.4.0. Exécutez donc la commande suivante afin de mettre à jour votre noyau :
« sudo BRANCH=next rpi-update c053625 »

```
pi@ZERO: ~
pi@ZERO:~ $
pi@ZERO:~ $
pi@ZERO:~ $
pi@ZERO:~ $ sudo BRANCH=next rpi-update c053625
```

- 35- Une fois tous les fichiers téléchargés, vous pourrez redémarrer afin d'appliquer les changements. Si des erreurs apparaissent dans la console, reprenez depuis l'étape précédente, sinon exécutez la commande « `sudo reboot` »

```
*** Updating firmware
*** Updating kernel modules
*** depmod 4.4.0-v7+
*** depmod 4.4.0+
*** Updating VideoCore libraries
*** Using HardFP libraries
*** Updating SDK
*** Running ldconfig
*** Storing current firmware revision
*** Deleting downloaded files
*** Syncing changes to disk
*** If no errors appeared, your firmware was successfully updated to c
*** A reboot is needed to activate the new firmware
pi@ZERO:~ $ sudo reboot
```

- 36- Une fois votre Raspberry redémarré, reconnectez-vous à l'aide du logiciel *Putty* comme vu précédemment. Exécutez ensuite la commande « `sudo uname -a` »
Si tout s'est bien passé, votre nouveau noyau doit être en version 4.4.0+

```
pi@ZERO: ~
login as: pi
pi@10.254.1.1's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Dec 27 12:23:24 2017
pi@ZERO:~ $ uname -a
Linux ZERO 4.4.0+ #833 Mon Jan 11 18:33:20 GMT 2016 armv6l GNU/Linux
pi@ZERO:~ $
```

- 37- Télécharger ensuite les outils nécessaires au tutoriel (pilote HID, script principal...etc) en exécutant la commande « `sudo wget https://thiefin.fr/rspiducky.zip` »

```
pi@ZERO: ~  
pi@ZERO:~ $  
pi@ZERO:~ $ sudo wget https://thiefin.fr/rspiducky.zip  
--2017-12-27 12:28:49-- https://thiefin.fr/rspiducky.zip  
Resolving thiefin.fr (thiefin.fr)... 78.201.2.129  
Connecting to thiefin.fr (thiefin.fr)|78.201.2.129|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 21198 (21K) [application/zip]  
Saving to: 'rspiducky.zip'  
  
rspiducky.zip      100%[=====>]  20.70K  128KB/s  in 0.2s  
2017-12-27 12:28:50 (128 KB/s) - 'rspiducky.zip' saved [21198/21198]  
  
pi@ZERO:~ $ █
```

- 38- Décompressez ensuite l'archive en exécutant la commande « `sudo unzip rspiducky.zip` »

```
pi@ZERO:~ $ sudo unzip rspiducky.zip  
Archive:  rspiducky.zip  
c2719a1879068b467fb2f487b5ff8152d8f0e4a9  
  creating: rspiducky-master/  
  inflating: rspiducky-master/.gitattributes  
  inflating: rspiducky-master/.gitignore  
  inflating: rspiducky-master/duckpi.sh  
  inflating: rspiducky-master/g_hid.ko  
  inflating: rspiducky-master/hid-gadget-test  
  inflating: rspiducky-master/hid-gadget-test.c  
  inflating: rspiducky-master/readme.txt  
  inflating: rspiducky-master/usleep  
  inflating: rspiducky-master/usleep.c  
pi@ZERO:~ $ ls rspiducky-master/  
duckpi.sh  hid-gadget-test  readme.txt  usleep.c  
g_hid.ko  hid-gadget-test.c  usleep  
pi@ZERO:~ $ █
```

- 39- Déplacez-vous dans le répertoire de l'archive grâce à la commande « `cd rspiducky-master` » puis modifier les droits des fichiers avec la commande « `sudo chmod 777 *` »
Copiez ensuite l'ensemble des fichiers dans le répertoire par défaut de l'utilisateur pi en exécutant la commande « `sudo cp * /home/pi/` »
Copiez enfin le pilote HID dans le répertoire des pilotes usb du nouveau noyau en exécutant la commande « `sudo cp g_hid.ko /lib/modules/4.4.0+/kernel/drivers/usb/gadget/legacy/` »

```
pi@ZERO: ~/rspiducky-master
pi@ZERO:~$ 
pi@ZERO:~$ cd rspiducky-master/
pi@ZERO:~/rspiducky-master$ sudo chmod 777 *
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$ sudo cp * /home/pi/
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$ sudo cp g_hid.ko /lib/modules/4.4.0+/kernel/drivers/usb/gadget/legacy
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$
```

- 40- Modifiez la liste des modules chargés au démarrage du système pour y ajouter les modules `dwc2` et `g_hid` en effectuant les 2 commandes suivantes (en respectant leur ordre) :
- « `echo "dwc2" | sudo tee /etc/modules` »
 - « `echo "g_hid" | sudo tee -a /etc/modules` »

```
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$ echo "dwc2" | sudo tee /etc/modules
dwc2
pi@ZERO:~/rspiducky-master$ echo "g_hid" | sudo tee -a /etc/modules
g_hid
pi@ZERO:~/rspiducky-master$
```

- 41- Modifiez à nouveau le fichier `cmdline.txt` dans le répertoire de démarrage de votre Raspberry en exécutant la commande « `sudo nano /boot/cmdline.txt` »

```
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$ 
pi@ZERO:~/rspiducky-master$ sudo nano /boot/cmdline.txt
```


42- Recherchez les éléments « modules-load=dwc2,g_ether »
et remplacez les par « modules-load=dwc2,g_hid » puis sauvegardez le fichier

(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)

```
pi@ZERO: ~/rspiducky-master
GNU nano 2.2.6 File: /boot/cmdline.txt
$.repair=yes rootwait modules-load=dwc2,g_ether quiet splash plymouth.ignore-serial-consoles
```

```
pi@ZERO: ~/rspiducky-master
GNU nano 2.2.6 File: /boot/cmdline.txt
$.repair=yes rootwait modules-load=dwc2,g_hid quiet splash plymouth.ignore-serial-consoles
```

43- Ajoutez une tâche planifiée en modifiant le fichier *rc.local* en exécutant la commande
« sudo nano /etc/rc.local »

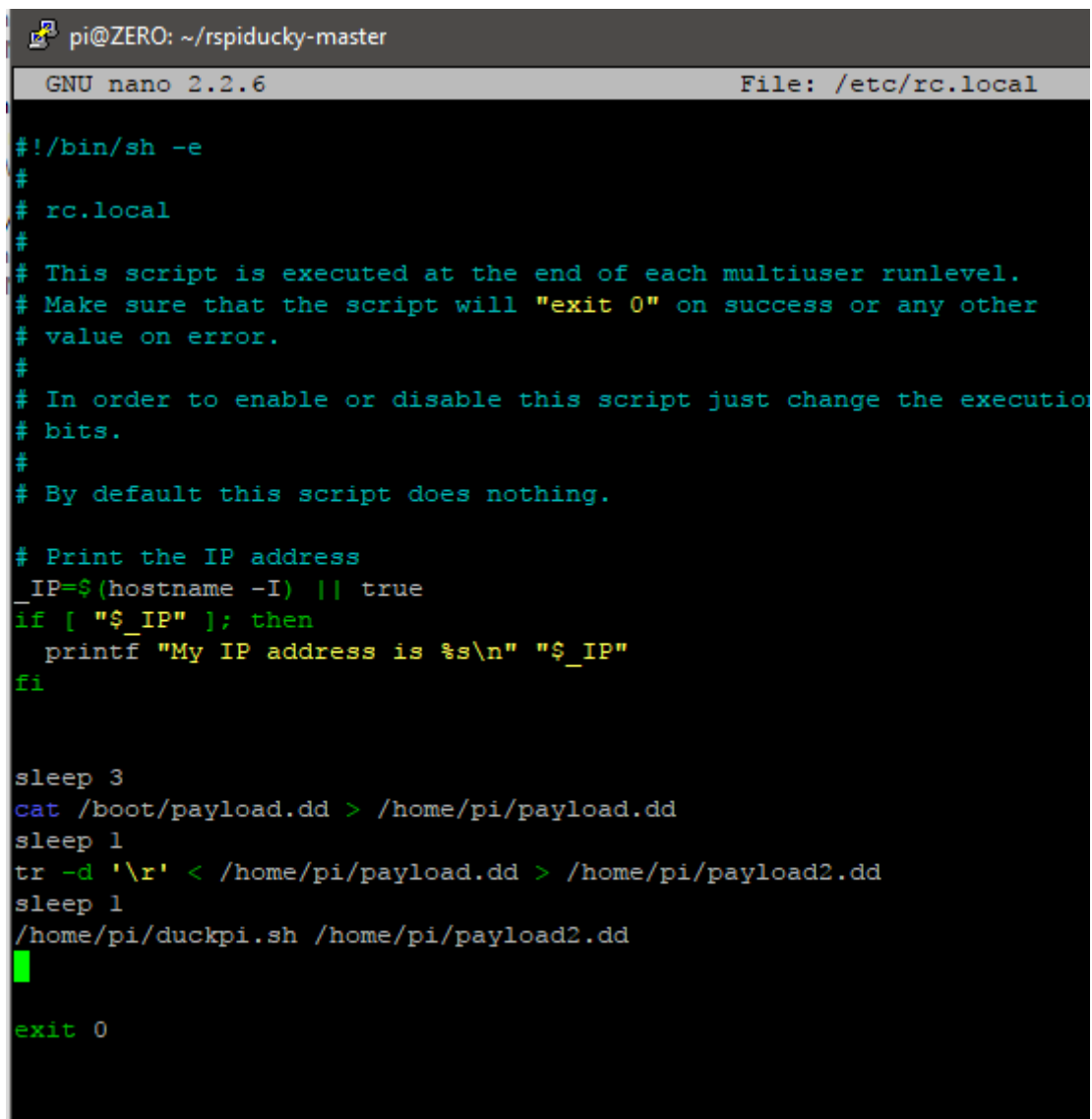
```
pi@ZERO:~/rspiducky-master $
pi@ZERO:~/rspiducky-master $
pi@ZERO:~/rspiducky-master $ sudo nano /etc/rc.local
```

44- Ajoutez le script qui permettra de mettre à jour votre payload Rubber Ducky, juste avant la ligne contenant « exit 0 » :

```
« sleep 3
cat /boot/payload.dd > /home/pi/payload.dd
sleep 1
tr -d '\r' < /home/pi/payload.dd > /home/pi/payload2.dd
sleep 1
/home/pi/duckpi.sh /home/pi/payload2.dd »

puis sauvegardez le fichier
```

(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)



```
pi@ZERO: ~/rspiducky-master
GNU nano 2.2.6 File: /etc/rc.local

#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
    printf "My IP address is %s\n" "$_IP"
fi

sleep 3
cat /boot/payload.dd > /home/pi/payload.dd
sleep 1
tr -d '\r' < /home/pi/payload.dd > /home/pi/payload2.dd
sleep 1
/home/pi/duckpi.sh /home/pi/payload2.dd

exit 0
```

- 45- Créez ensuite votre premier script Rubber Ducky en exécutant la commande
« sudo nano /boot/payload.dd »

```
pi@ZERO: ~/rspiducky-master
pi@ZERO:~/rspiducky-master $
pi@ZERO:~/rspiducky-master $
pi@ZERO:~/rspiducky-master $
pi@ZERO:~/rspiducky-master $ sudo nano /boot/payload.dd
```

- 46- Vous pouvez ajouter dans ce fichier le script Rubber Ducky de votre choix.
Dans notre exemple, le script va simplement lancer une page web dans le navigateur par défaut et simuler un appui sur la touche « F11 ».
ATTENTION : Le pilote fournit est compilé pour un clavier à disposition QWERTY, il faudra donc faire correspondre les caractères de vos scripts

Si vous n'avez pas de script personnalisé, ajoutez simplement ces lignes :

```
« GUI r
DELAY 500
STRING zzz<youtube<co;>chqnnel>UCarxDV(EPOlI!Y:hwIPed@g
ENTER
DELAY 1000
F11 »
```

puis sauvegardez le fichier

(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)

```
GNU nano 2.2.6          Fichier : /boot/payload.dd

GUI r
DELAY 50
STRING zzz<youtube<co;>chqnnel>UCarxDV(EPOlI!Y:hwIPed@g
ENTER
DELAY 1000
F11
█
```

- 47- Modifiez ensuite les droits d'accès au fichier en exécutant la commande :
« `sudo chmod 777 /boot/payload.dd` »

```
pi@ZERO:~/rspiducky-master $  
pi@ZERO:~/rspiducky-master $ sudo chmod 777 /boot/payload.dd  
pi@ZERO:~/rspiducky-master $  
pi@ZERO:~/rspiducky-master $
```

- 48- Il ne vous reste plus qu'à redémarrez votre Raspberry afin qu'il soit détecté comme un périphérique de type « Clavier » et exécute le script `payload.dd`

```
pi@ZERO:~/rspiducky-master $  
pi@ZERO:~/rspiducky-master $ sudo reboot
```

Si vous souhaitez modifier le script Rubber Ducky, il vous suffit simplement de débrancher votre Raspberry, puis déconnectez la carte microSD et branchez-la sur votre ordinateur.

Le fichier `payload.dd` étant sur la partition de démarrage formatée en FAT32, vous pourrez facilement le remplacer même depuis un poste Windows, sans logiciel tiers.

Il vous suffira ensuite de reconnecter la carte microSD à votre Raspberry afin qu'il mette à jour le script au prochain démarrage.

Bon courage ! ☺

Proc.