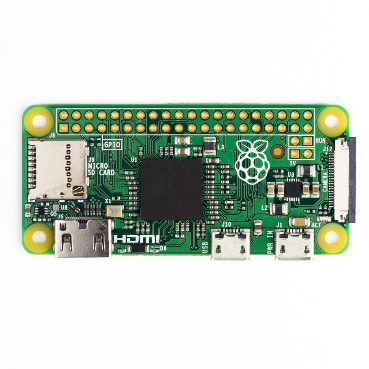
**Créer sa clé USB Rubber Ducky avec un Raspberry pi Zero**



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/UCqrxDV9EPOlI1YMhzIPed2g>

Ce tutoriel est disponible également au format vidéo sur YouTube :

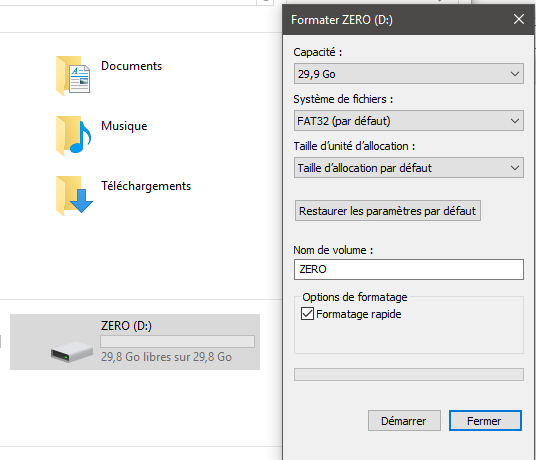
<https://www.youtube.com/watch?v=Xl2SdD1bS-0>

Lien vers mon site web :

<https://thiefin.fr>

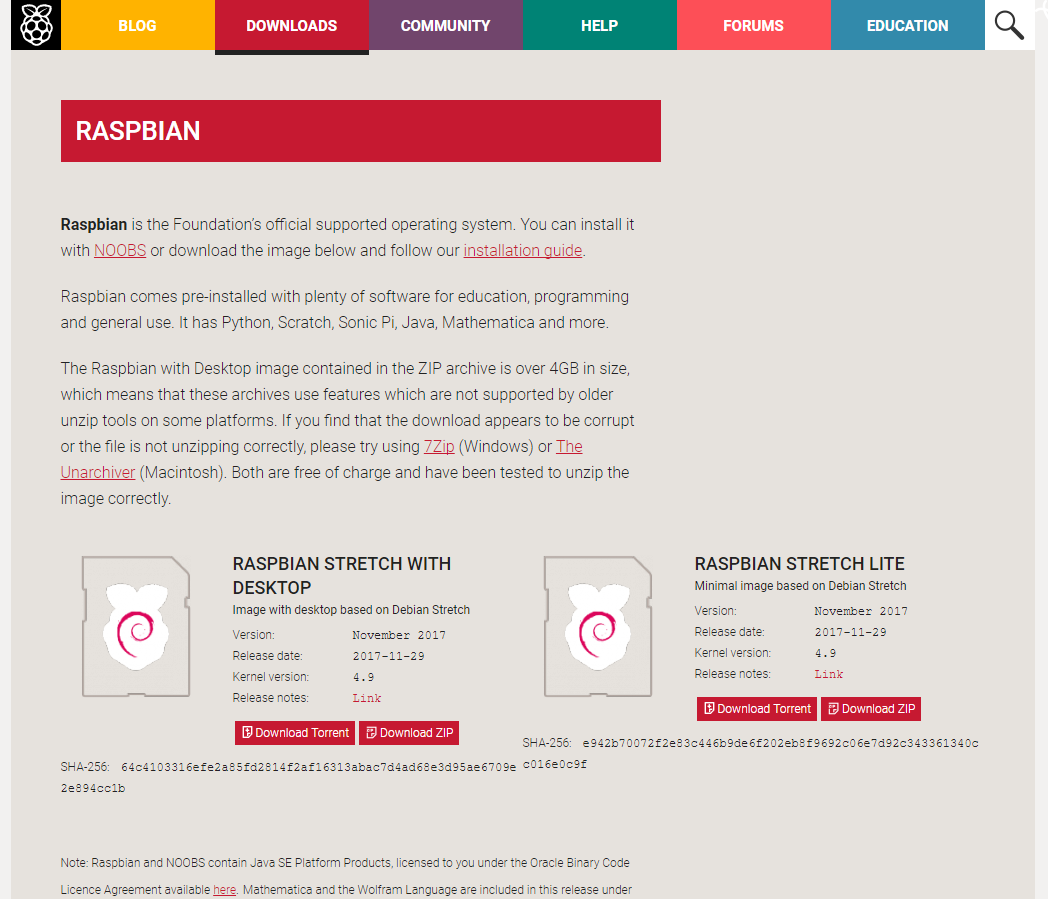
1. Formater la carte microSD au format FAT32

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



1. Télécharger le dernier iso d’installation du système d’exploitation Raspbian

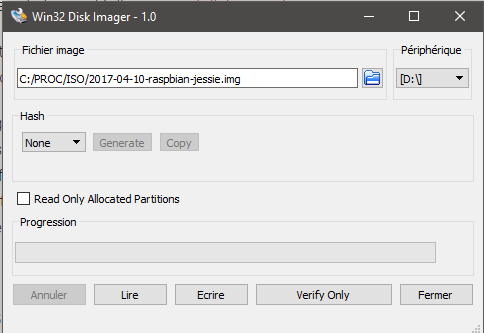
Site officiel : <https://www.raspberrypi.org>

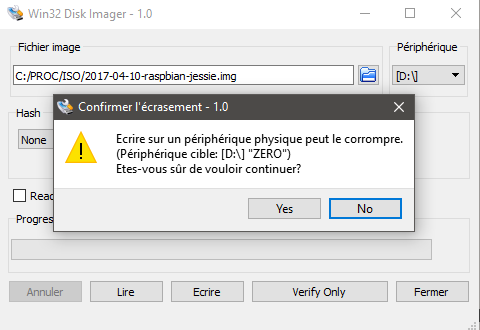


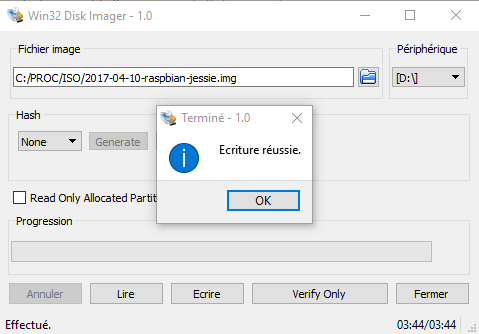
1. A l’aide du logiciel Win32 Disk Imager, installer l’iso Raspbian sur la carte microSD

Lien de téléchargement de Win32 Disk Imager :

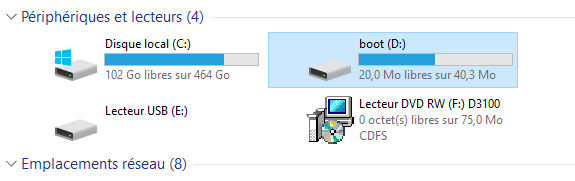
<https://sourceforge.net/projects/win32diskimager>



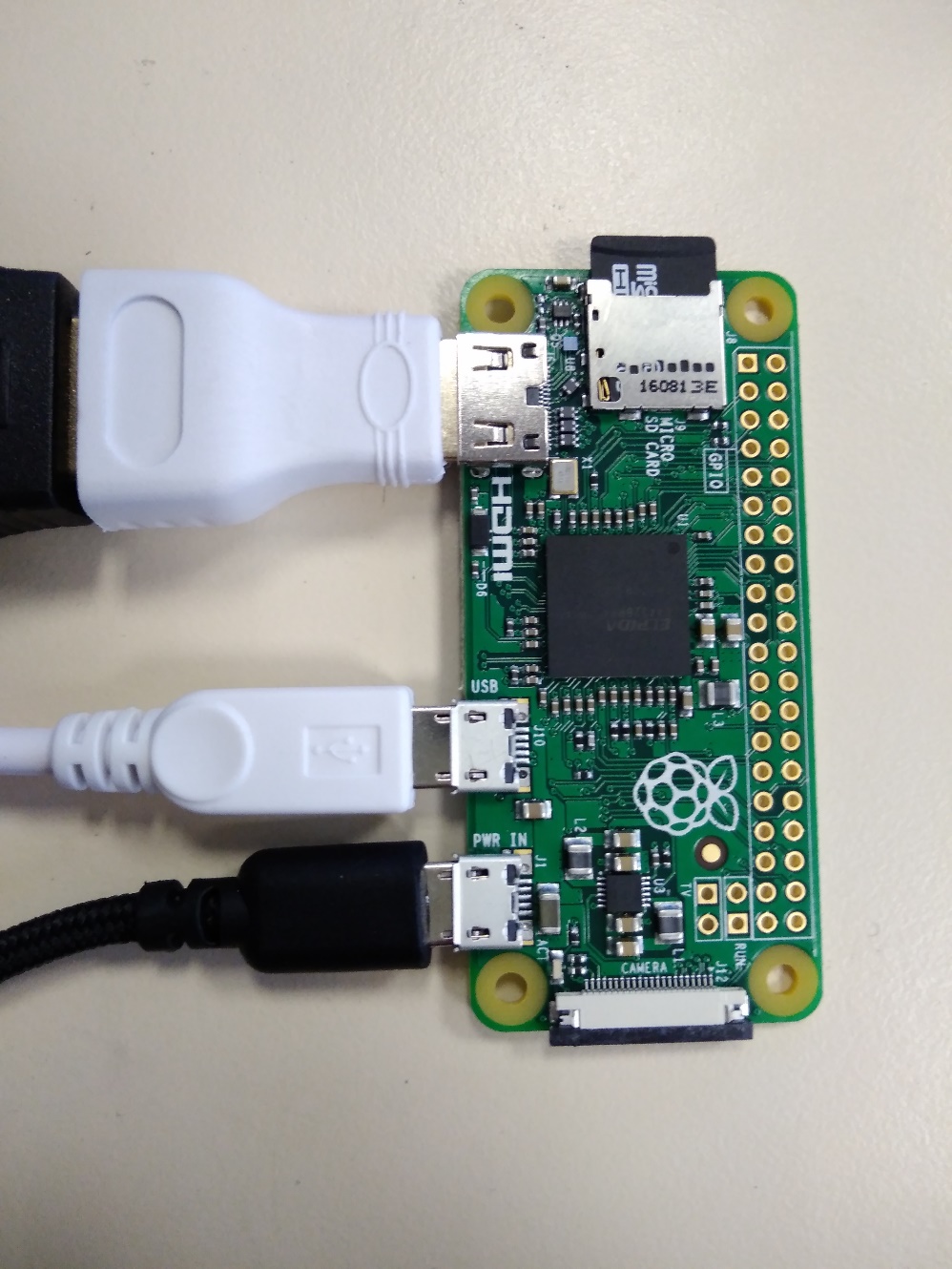




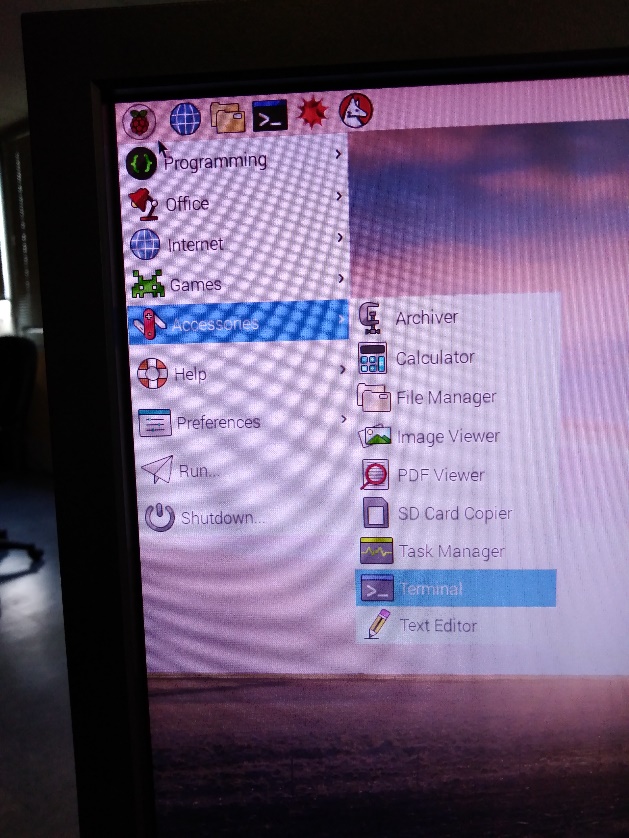
1. Une fois l’installation terminée, la partition de boot est accessible via l’explorateur de fichiers



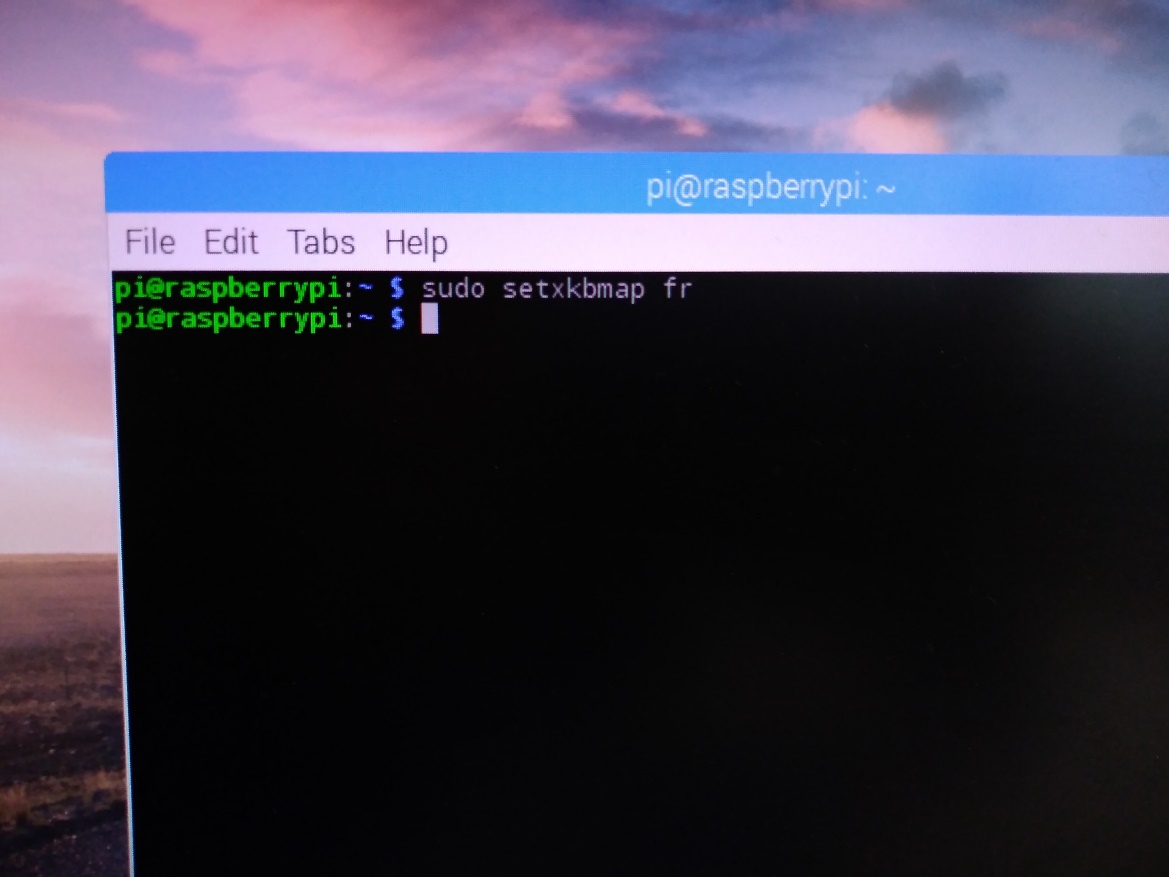
1. Brancher un écran sur le port HDMI du Raspberry grâce à l’adaptateur fourni, un clavier sur le port USB grâce à l’adaptateur fourni et un câble d’alimentation sur le port POWER



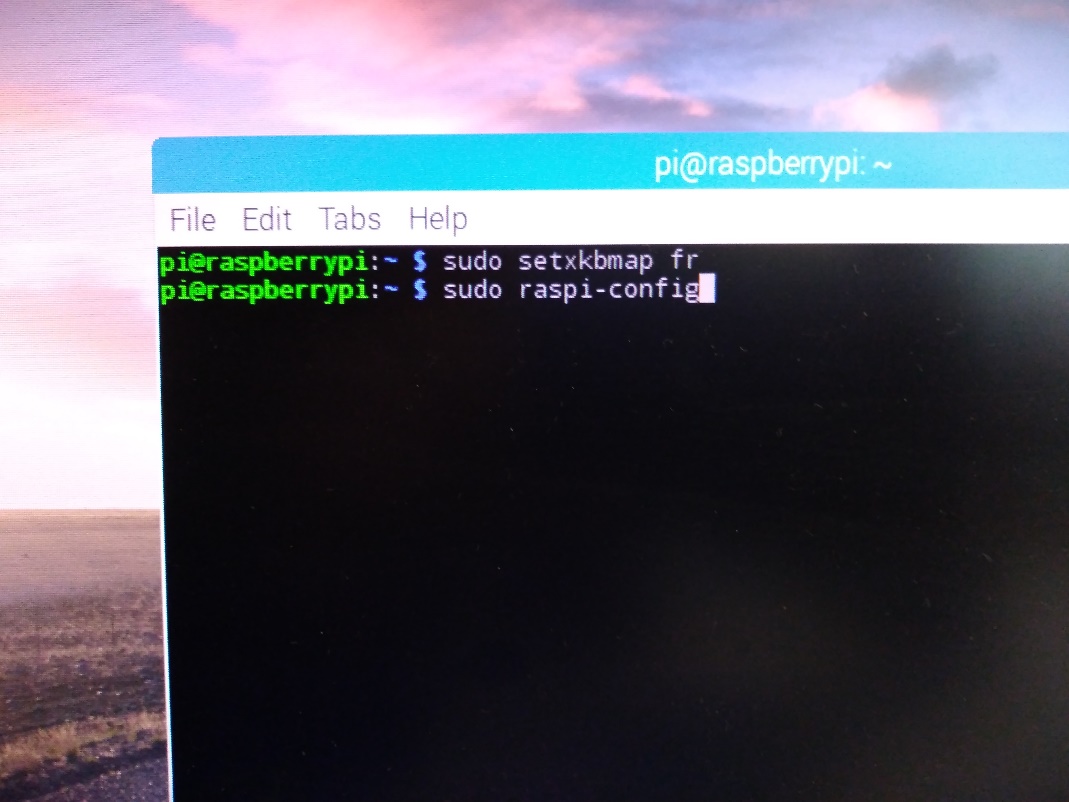
1. Ouvrez ensuite un terminal dans le menu de démarrage : Accessories > Terminal



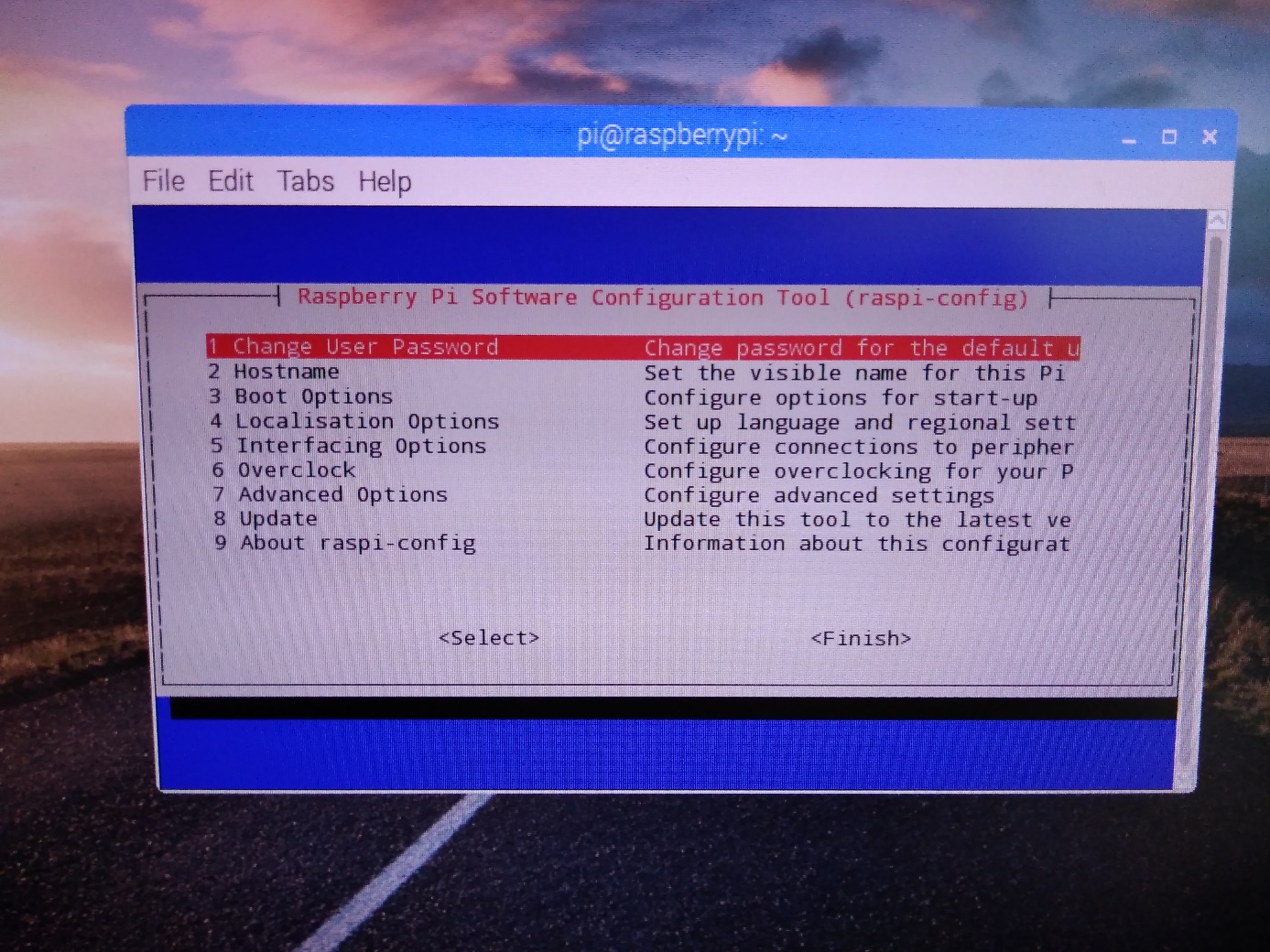
1. Par défaut, le clavier Raspbian est configuré en qwerty. Pour passer en disposition AZERTY, tapez la commande « sudo setxkbmap fr »



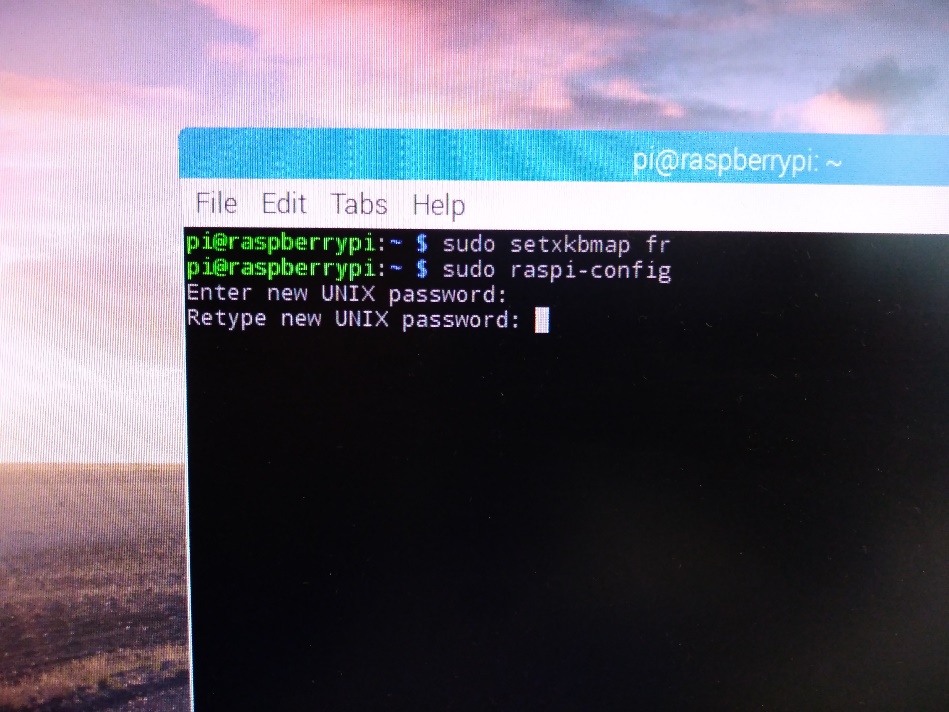
1. Ouvrez ensuite le menu de configuration de Raspbian en tapant la commande « sudo raspi-config »



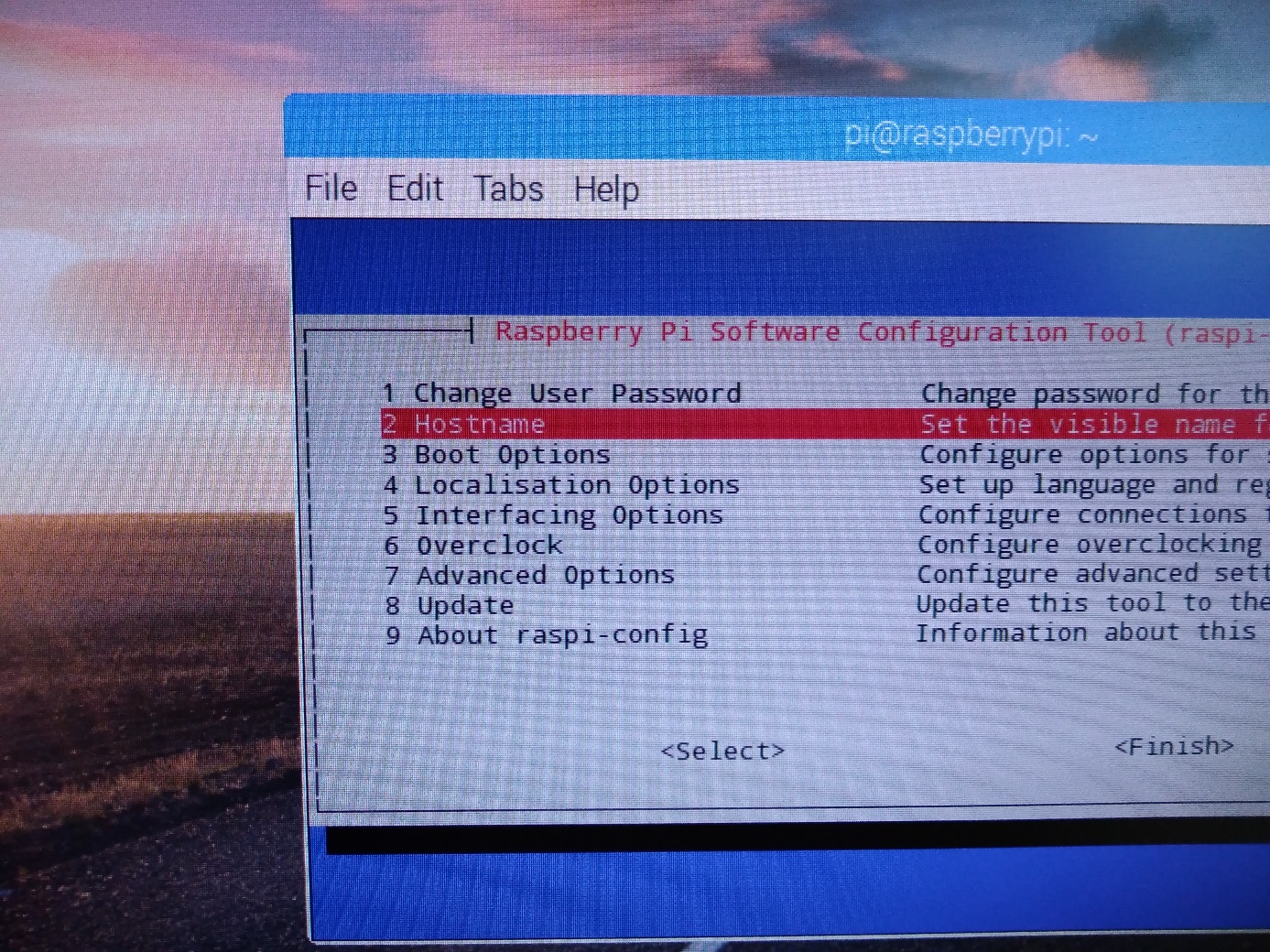
1. Dans un premier temps, sélectionnez « Change user password » afin de modifier le mot de passe par défaut du système



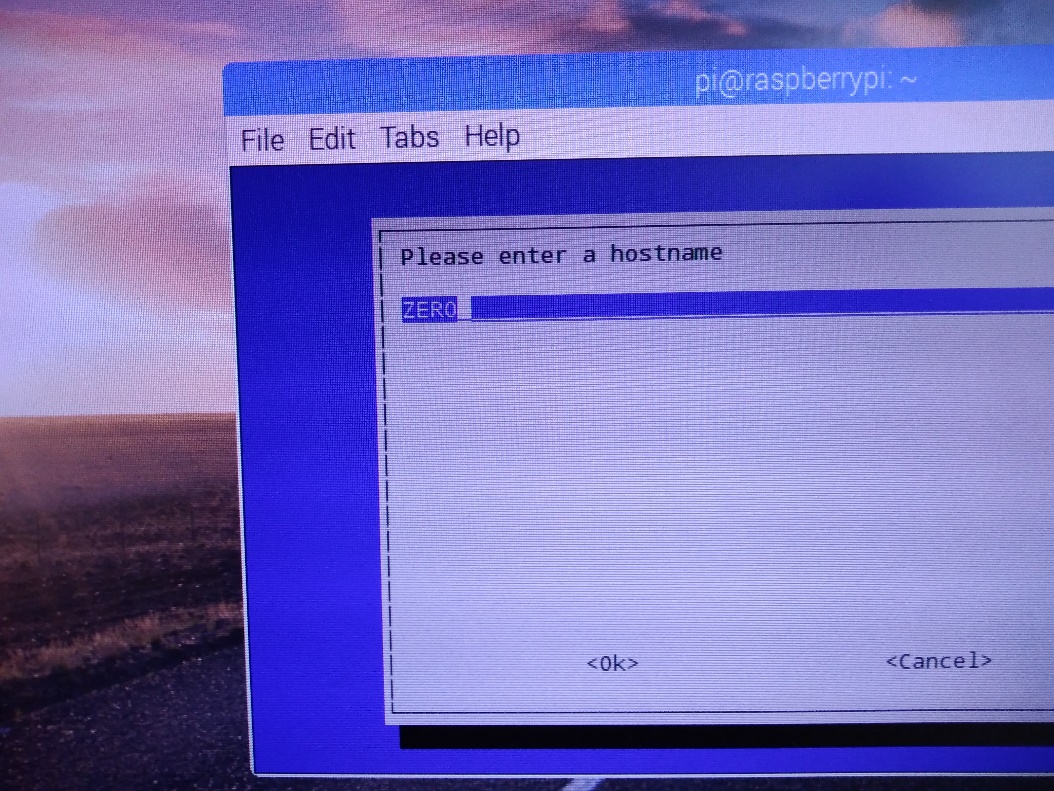
1. Entrez votre nouveau mot de passe. Une confirmation vous sera demandée.



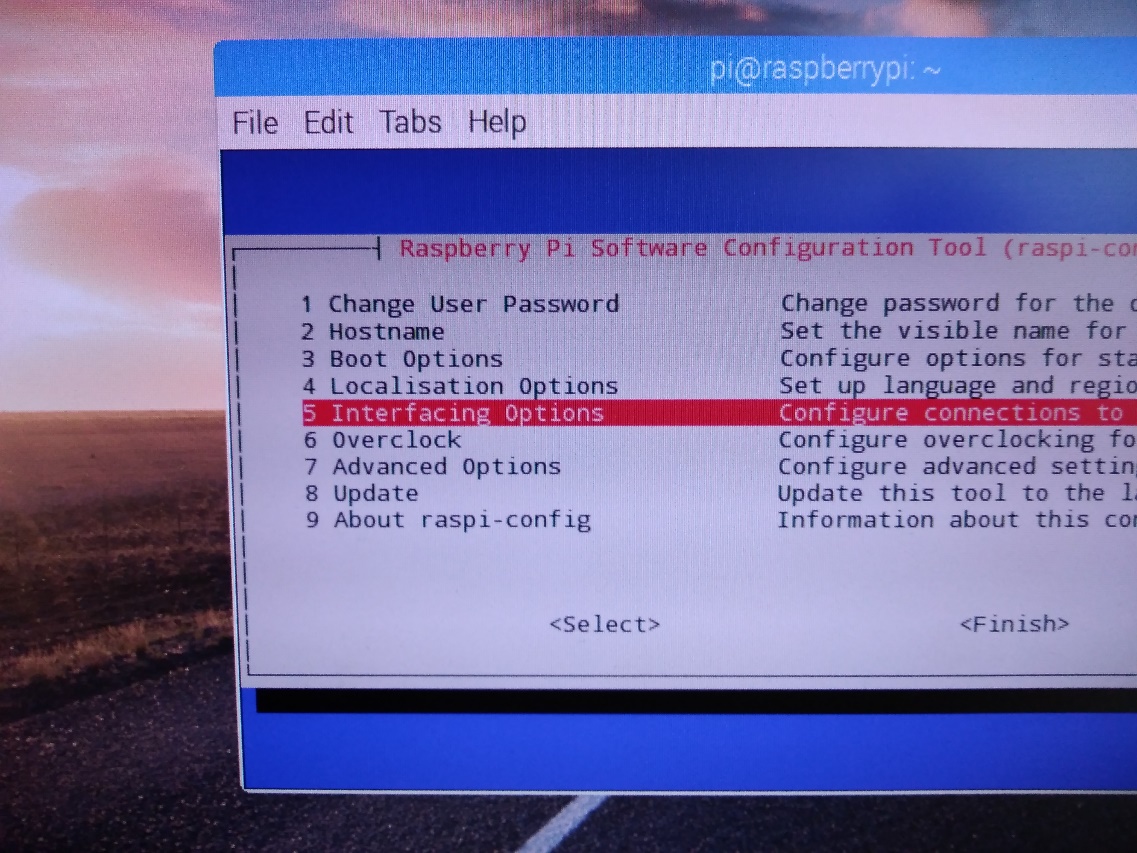
1. Choisissez ensuite l’option « Hostname » afin de modifier le nom de votre Raspberry



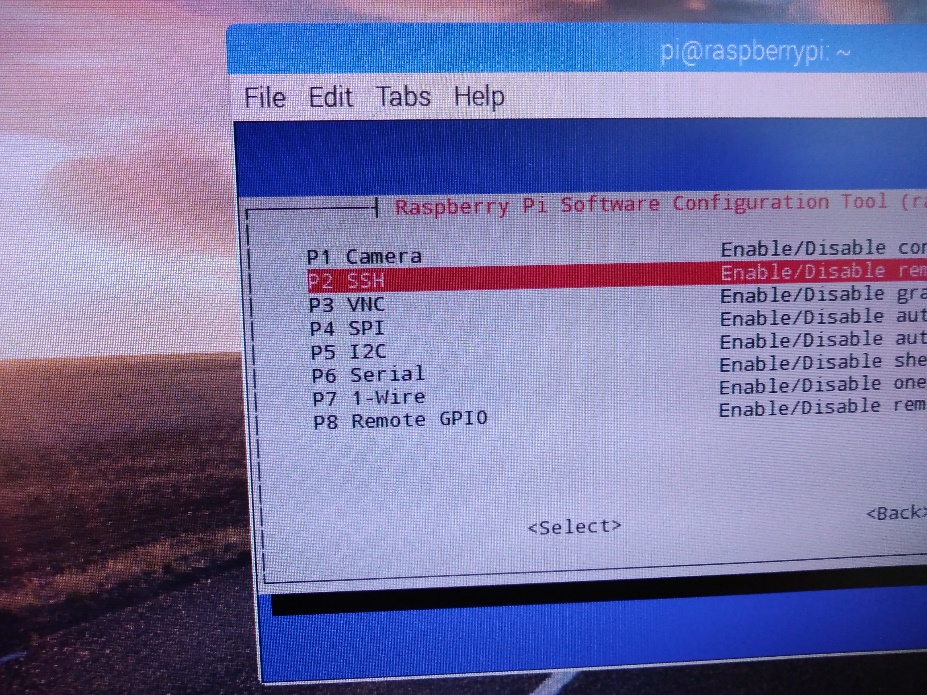
1. Dans ce tutoriel, le Raspberry s’appellera « ZERO »



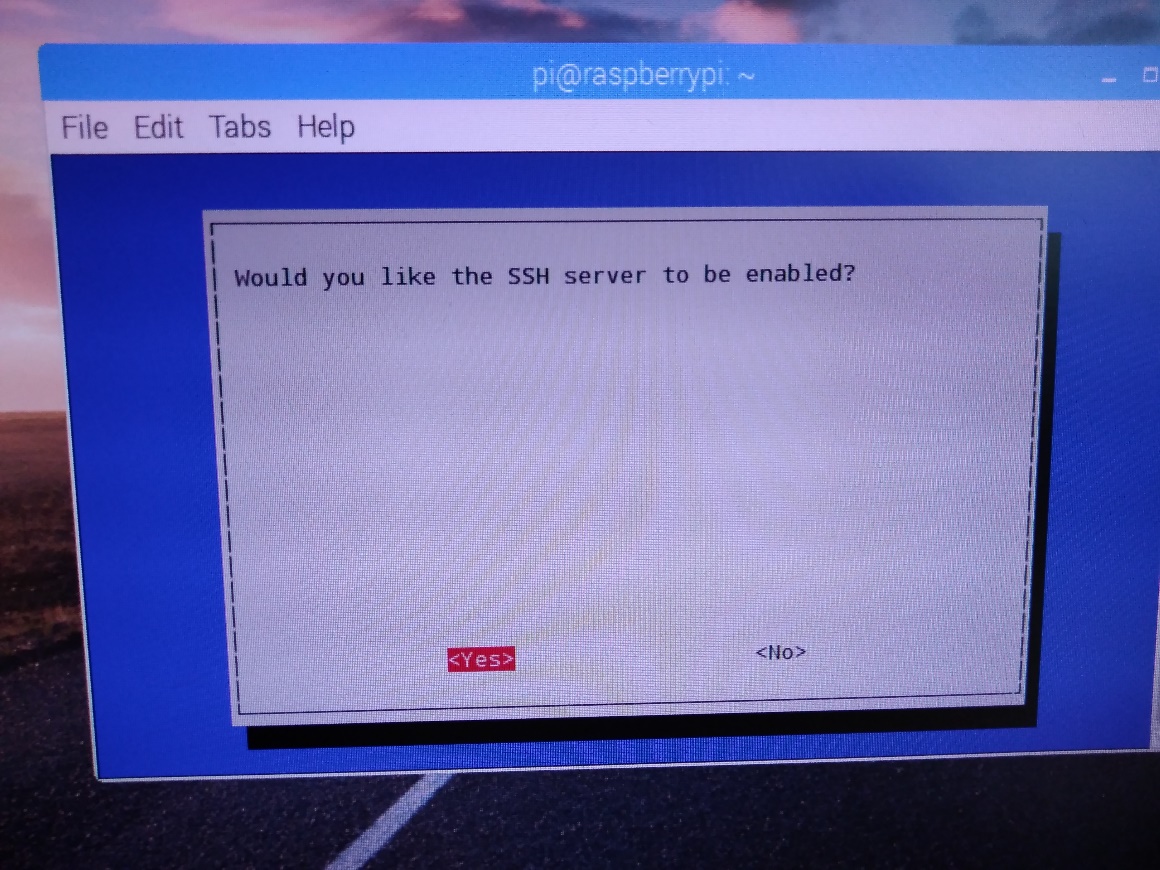
1. Choisissez ensuite l’option 5 : « Interfacing options »



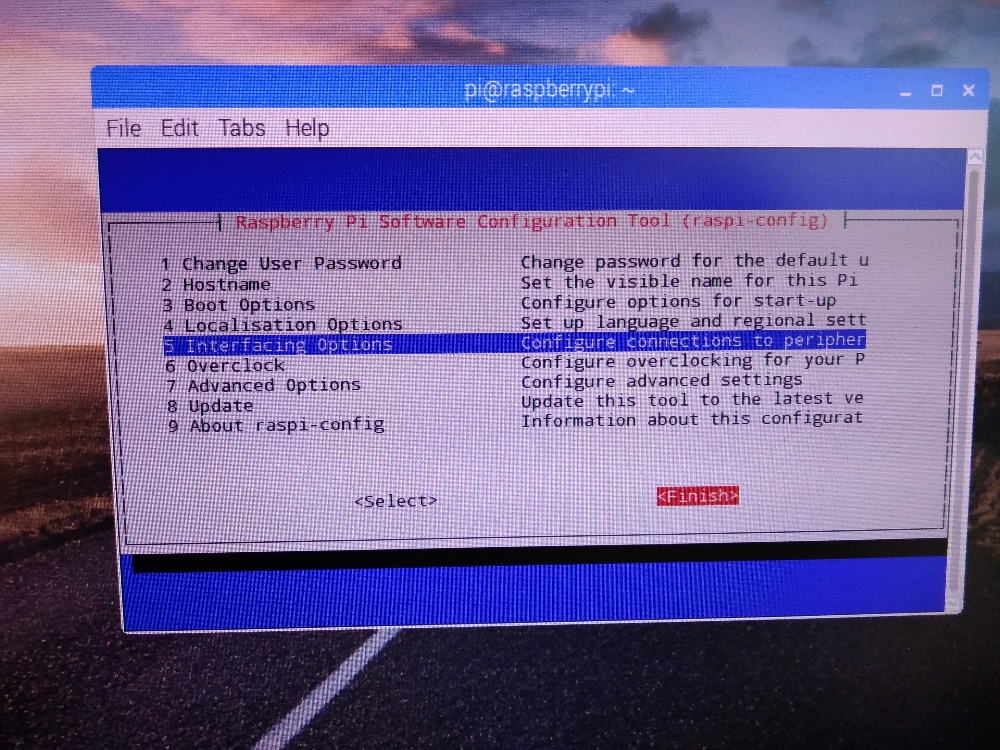
1. Sélectionnez ensuite l’option P2 : « SSH » afin d’activer le service SSH



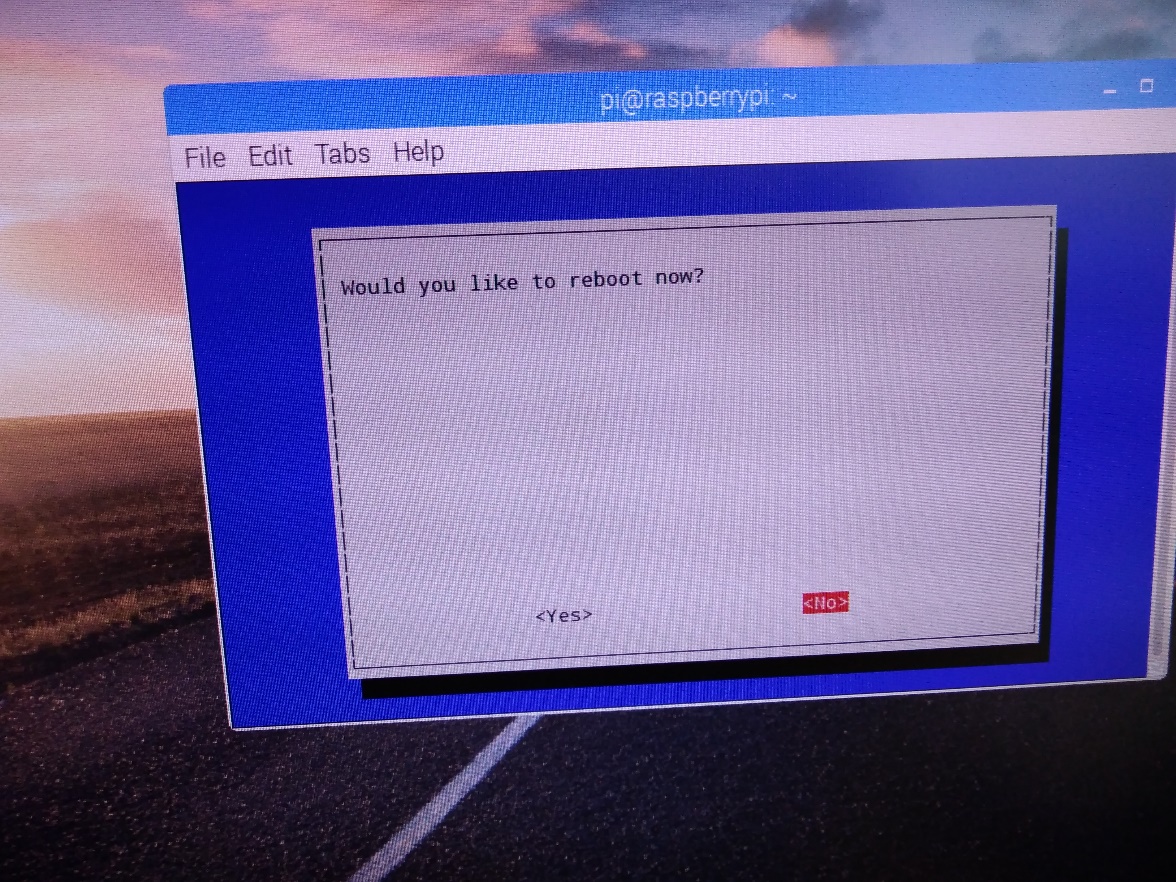
1. Confirmez l’activation du service SSH



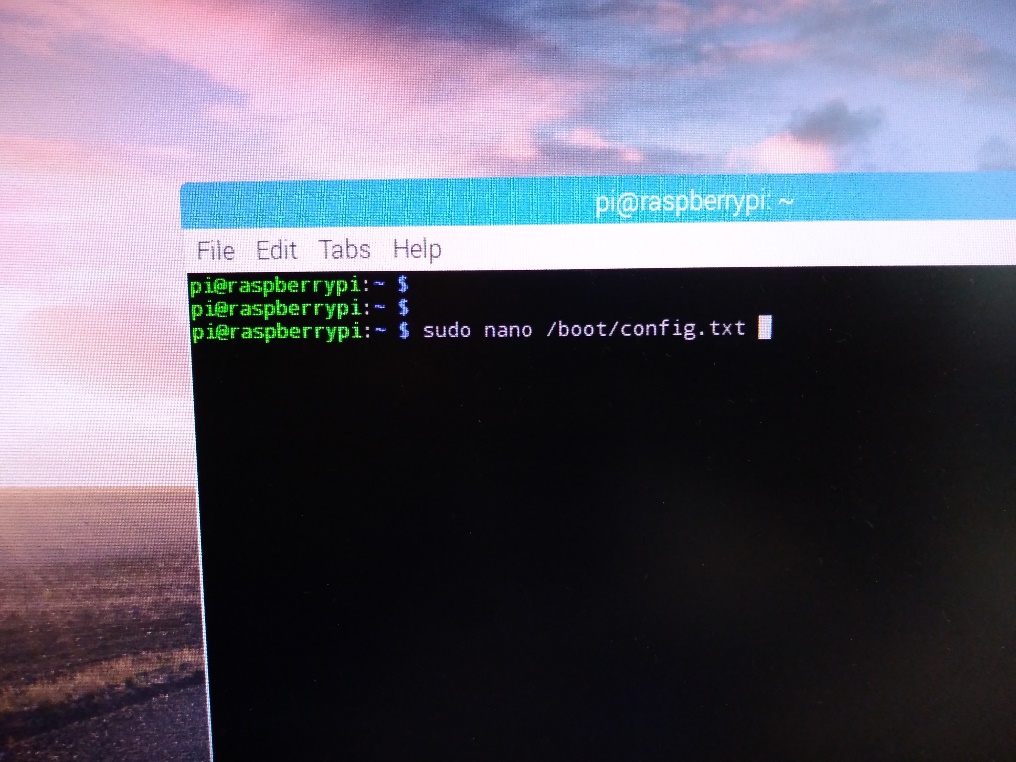
1. Sélectionnez « Finish » afin de quitter le menu de configuration



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



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



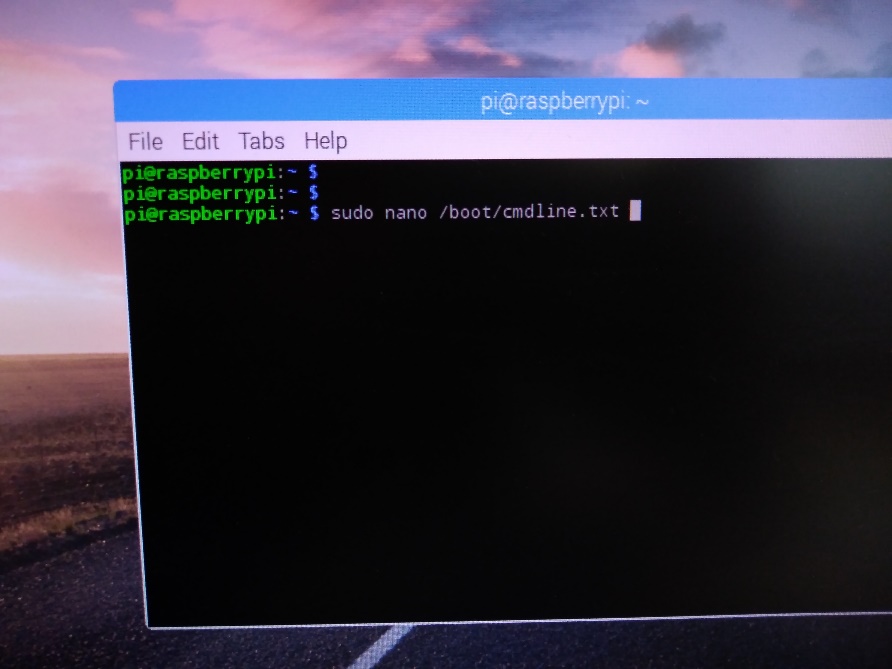
1. A la fin du fichier, ajoutez la ligne « dtoverlay=dwc2 » puis sauvegardez le fichier

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



1. Modifier de la même manière le fichier *cmdline.txt* en exécutant la commande

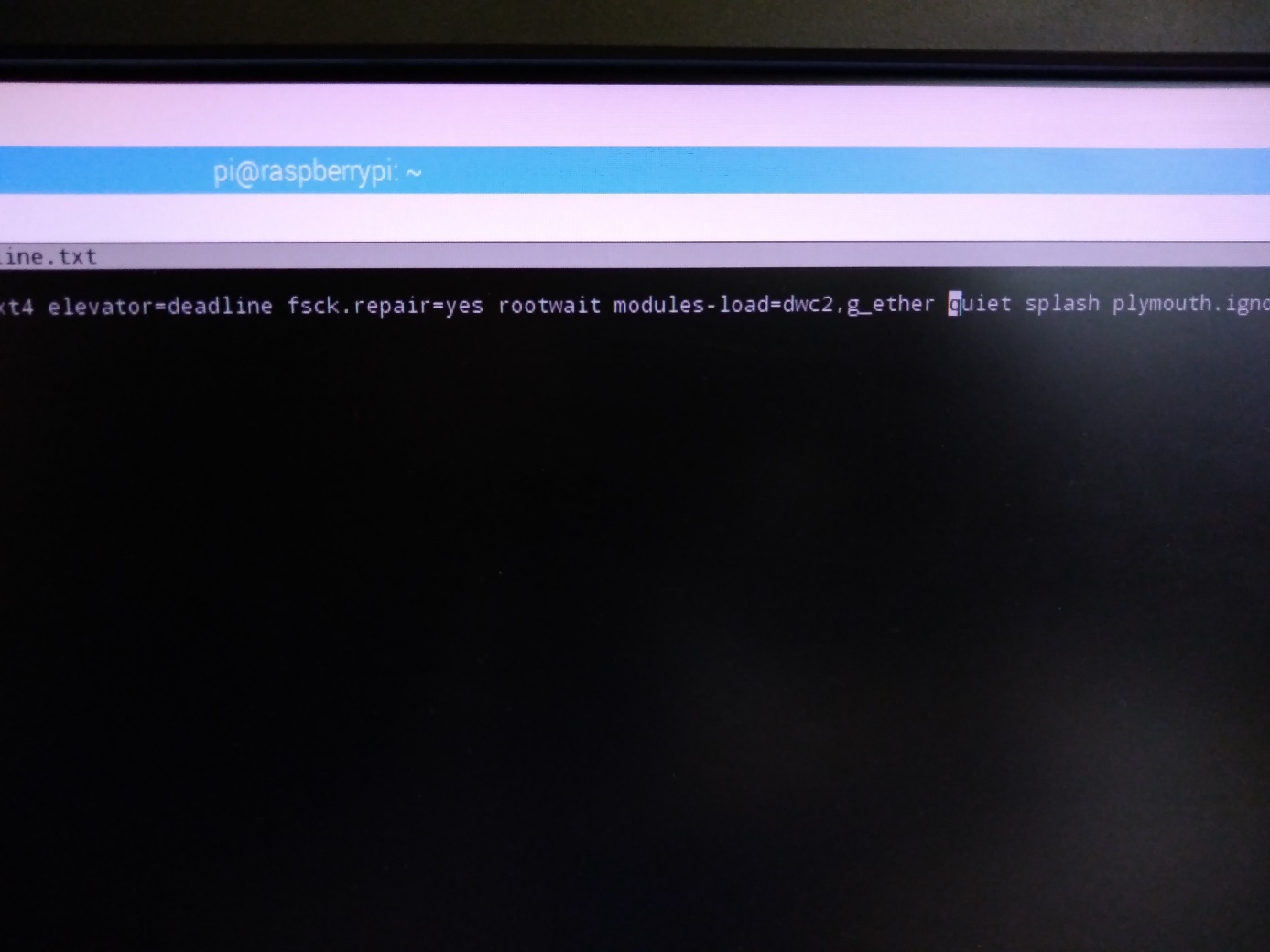
« sudo nano /boot/cmdline.txt »



1. Rajoutez entre les éléments ***rootwait*** et ***quiet*** :

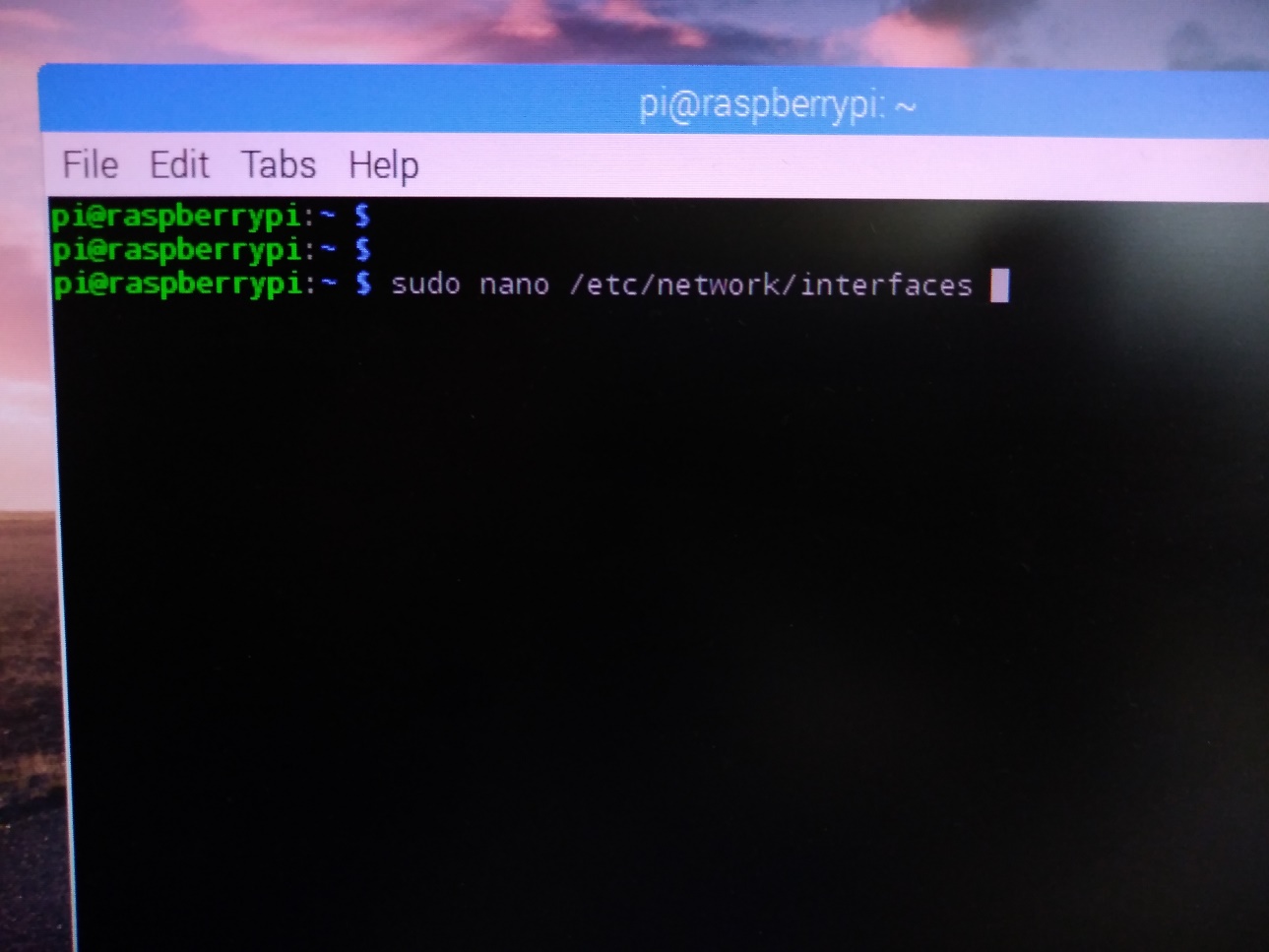
« modules-load=dwc2,g\_ether » puis sauvegardez le fichier

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



1. Modifiez la configuration réseau de votre Raspberry en exécutant la commande :

« sudo nano /etc/network/interfaces »



1. 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

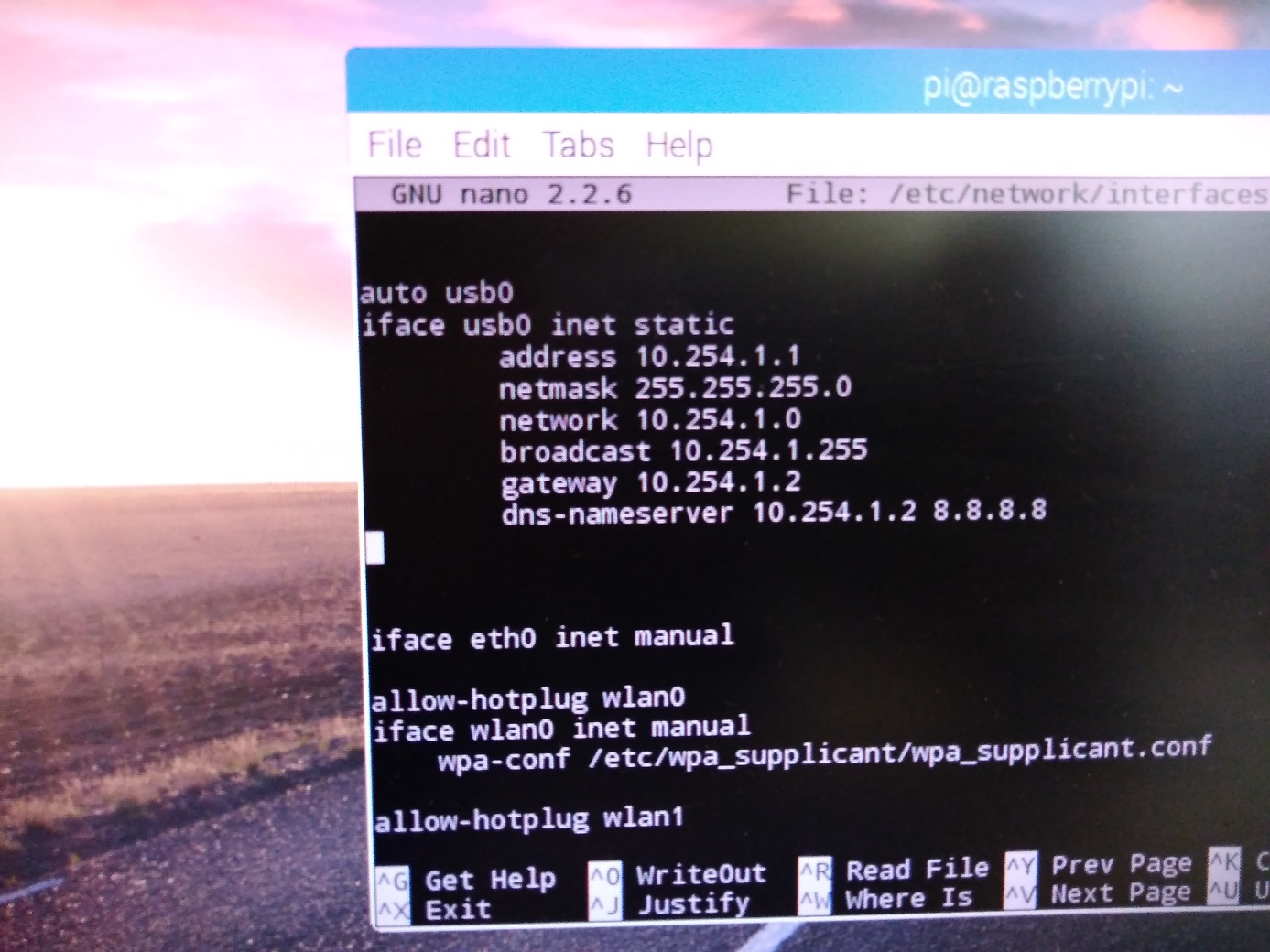
network 10.254.1.0

broadcast 10.254.1.255

gateway 10.254.1.2

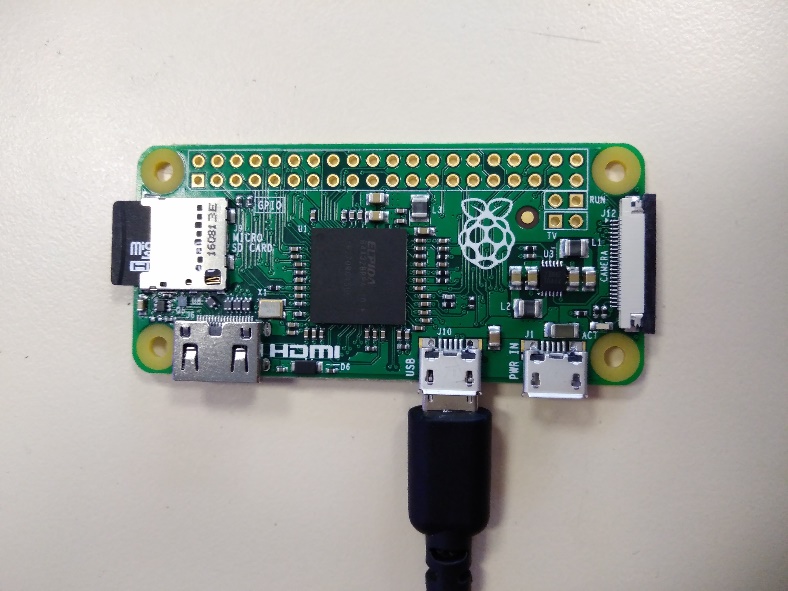
dns-nameserver 10.254.1.2 8.8.8.8 » puis sauvegardez le fichier

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

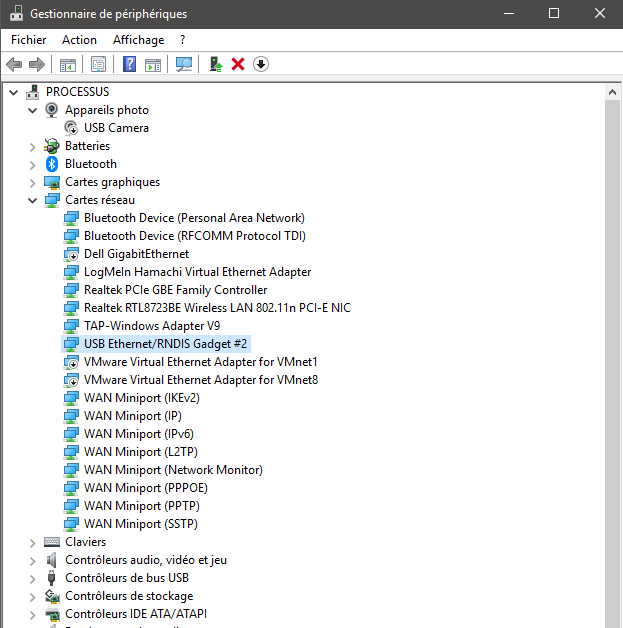


1. Arrêtez ensuite votre Raspberry en exécutant la commande « sudo shutdown –h now »

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



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

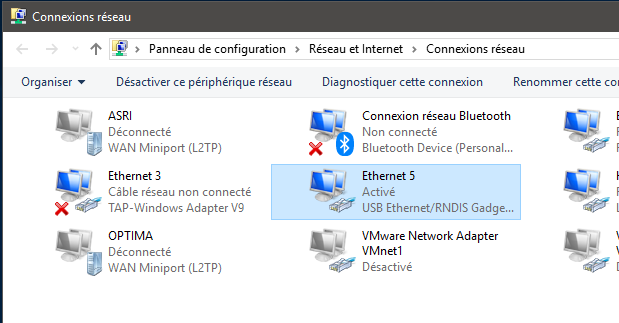


Pour les utilisateurs de Windows 10 il est nécessaire d’installer le pilote RNDIS afin que le Raspberry soit détecté en tant que tel.

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

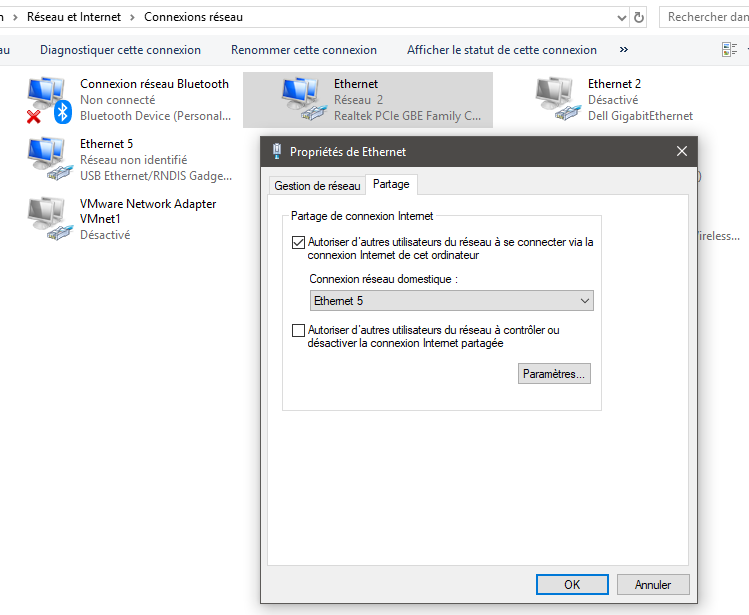
1. Ouvrez le panneau de configuration et naviguez jusqu’à « Connexions réseau ». Identifiez le nom de la carte réseau de type USB Ethernet/RNDIS Gadget

Dans cet exemple, la carte s’appelle « Ethernet 5 »



1. 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

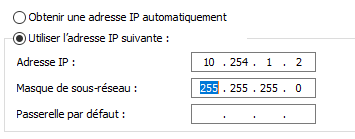
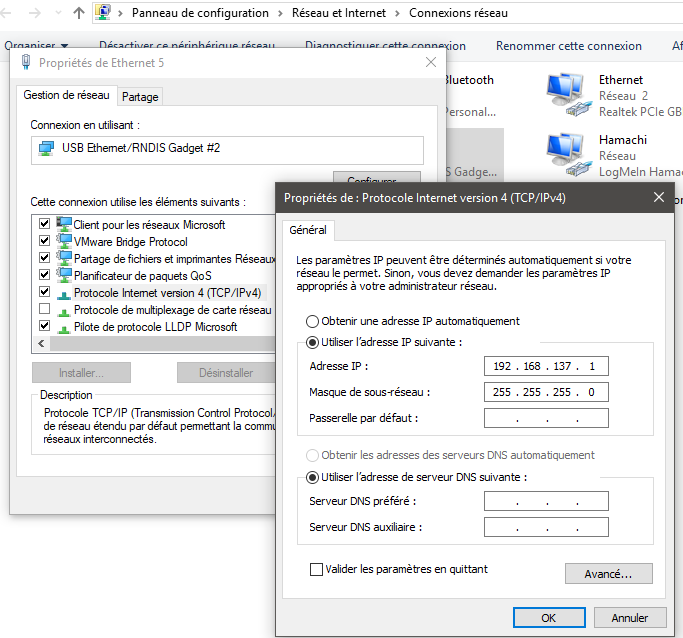
Dans cet exemple, il s’agit de la carte réseau « Ethernet 2 »



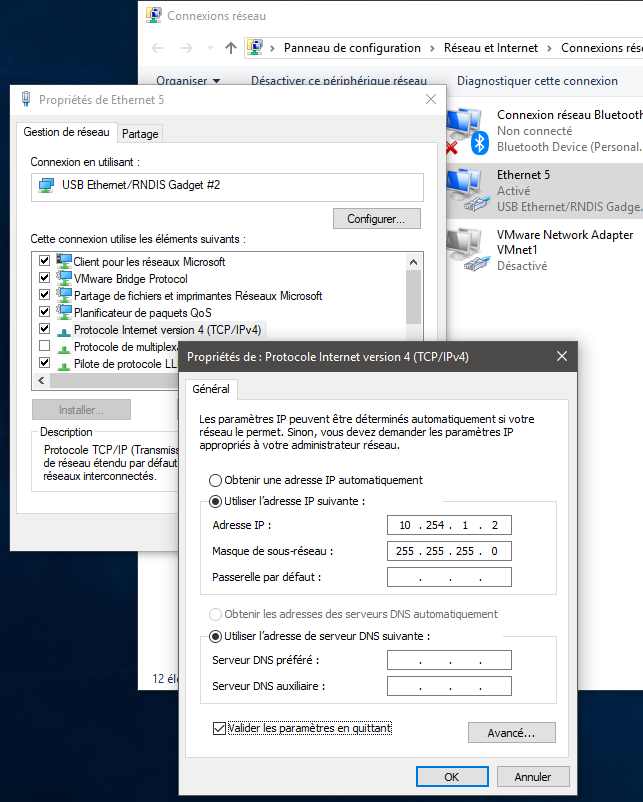
1. Faites un clic droit sur la carte réseau de votre Raspberry et sélectionnez « Propriétés ».

Sélectionnez ensuite la ligne « Protocole Internet version 4 (TCP/IPv4 » et cliquez sur « Propriétés ».

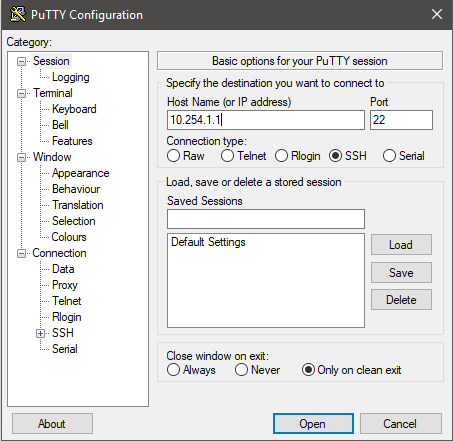
Remplacez la ligne Adresse IP en remplaçant « 192.168.137.1 » par « 10.254.1.2 »



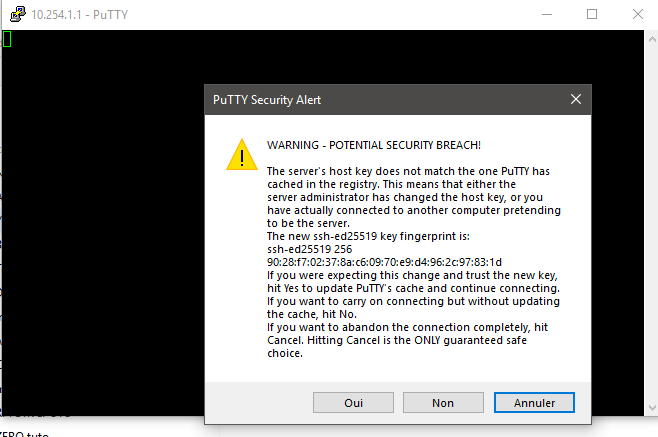
1. Sélectionnez « Valider les paramètres en quittant » puis cliquez sur « OK »



1. 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*

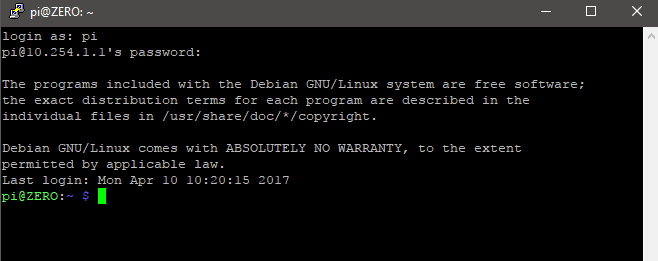


1. Lors de la première connexion, une alerte de sécurité va apparaître, cliquez simplement sur « Oui »

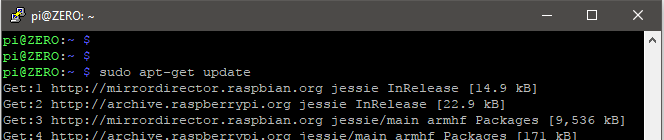


1. Identifiez-vous avec le nom d’utilisateur « pi » et le mot de passe que vous avez choisi lors de la configuration initiale

Si vous n’avez pas changé de mot de passe, celui par défaut est « raspberrypi »

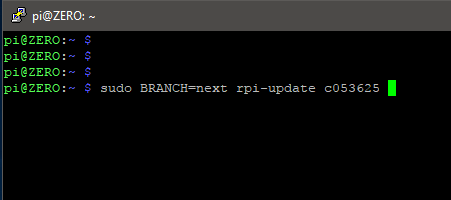


1. A ce stade, votre Raspberry a accès à internet au travers du partage de connexion de votre ordinateur. Exécutez la commande « sudo apt-get update » afin de mettre à jour la liste des dépôts de Raspbian

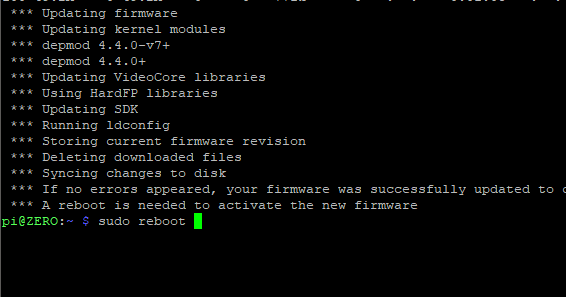


1. Ce tutoriel nécessite l’utilisation d’un pilote spécifiquement développé pour un noyau en version 4.4.0. Exécutez donc la commande suivante afin de mettre à jour votre noyau :

« sudo BRANCH=next rpi-update c053625 »

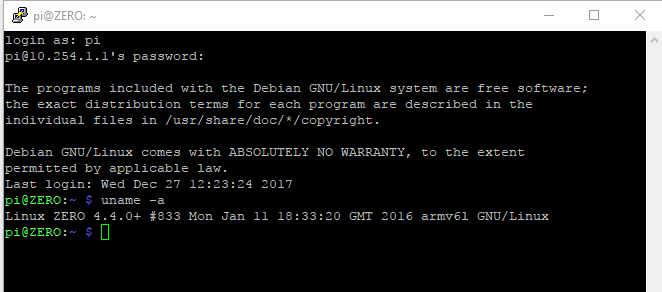


1. Une fois tous les fichiers téléchargés, vous pourrez redémarrer afin d’appliquer les changements. Si des erreurs apparaissent dans la console, reprenez depuis l’étape précédente, sinon exécutez la commande « sudo reboot »

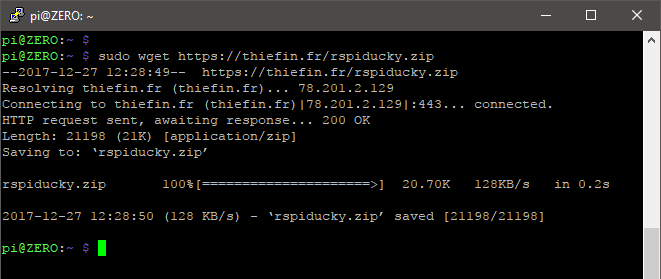


1. Une fois votre Raspberry redémarré, reconnectez-vous à l’aide du logiciel *Putty* comme vu précédemment. Exécutez ensuite la commande « sudo uname –a »

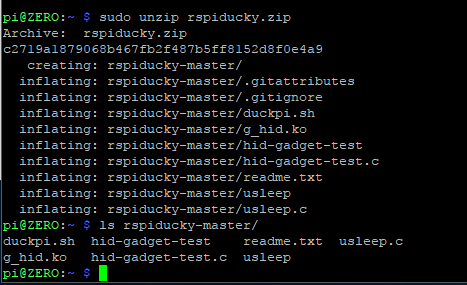
Si tout s’est bien passé, votre nouveau noyau doit être en version 4.4.0+



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



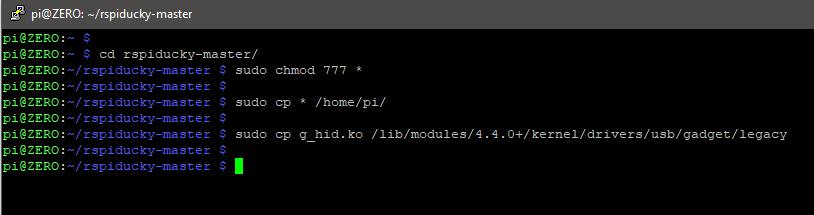
1. Décompressez ensuite l’archive en exécutant la commande « sudo unzip rspiducky.zip »



1. 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/ »

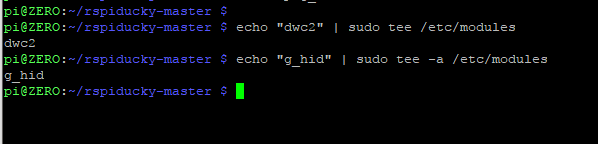
Copiez enfin le pilote HID dans le répertoire des pilotes usb du nouveau noyau en exécutant la commande « sudo cp g\_hid.ko /lib/modules/4.4.0+/kernel/drivers/usb/gadget/legacy/ »



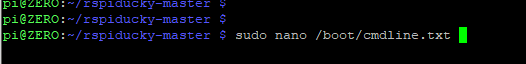
1. Modifiez la liste des modules chargés au démarrage du système pour y ajouter les modules *dwc2* et *g\_hid* en effectuant les 2 commandes suivantes (en respectant leur ordre) :

« echo "dwc2 " | sudo tee /etc/modules »

« echo "g\_hid " | sudo tee –a /etc/modules »



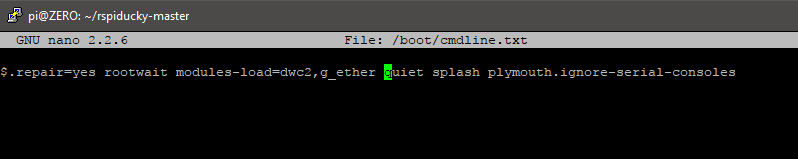
1. Modifiez à nouveau le fichier *cmdline.txt* dans le répertoire de démarrage de votre Raspberry en exécutant la commande « sudo nano /boot/cmdline.txt »

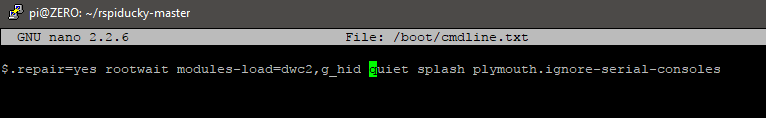


1. Recherchez les éléments « modules-load=dwc2,**g\_ether** »

et remplacez les par « modules-load=dwc2,**g\_hid**» puis sauvegardez le fichier

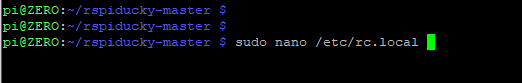
(Ctrl+x pour quitter, puis Y ou O pour enregistrer et Entrer pour valider)





1. Ajoutez une tâche planifiée en modifiant le fichier *rc.local* en exécutant la commande

« sudo nano /etc/rc.local »



1. 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

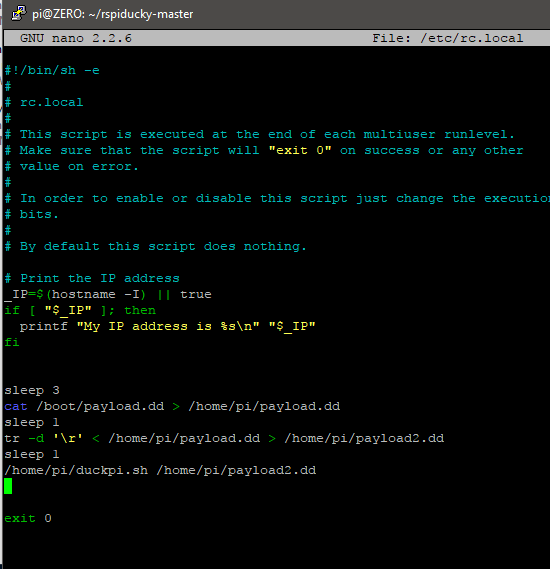
tr –d '\r ' < /home/pi/payload.dd > /home/pi/payload2.dd

sleep 1

/home/pi/duckpi.sh /home/pi/payload2.dd »

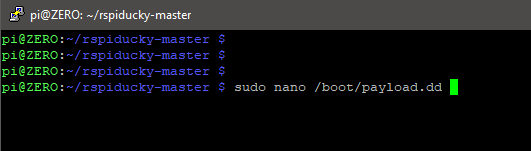
puis sauvegardez le fichier

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



1. Créez ensuite votre premier script Rubber Ducky en exécutant la commande

« sudo nano /boot/payload.dd »



1. 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

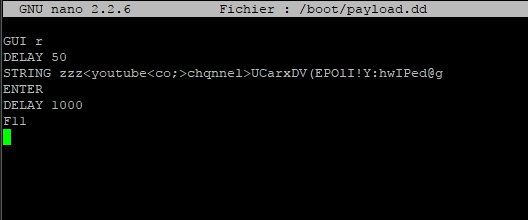
ENTER

DELAY 1000

F11 »

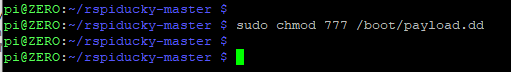
puis sauvegardez le fichier

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

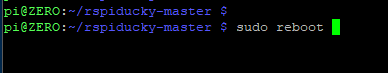


1. Modifiez ensuite les droits d’accès au fichier en exécutant la commande :

« sudo chmod 777 /boot/payload.dd »



1. 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



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.