Security in IoT Ecosystem

Module 7

Smart Socket Pentest
Part I

Prof.: Joaquín Recas

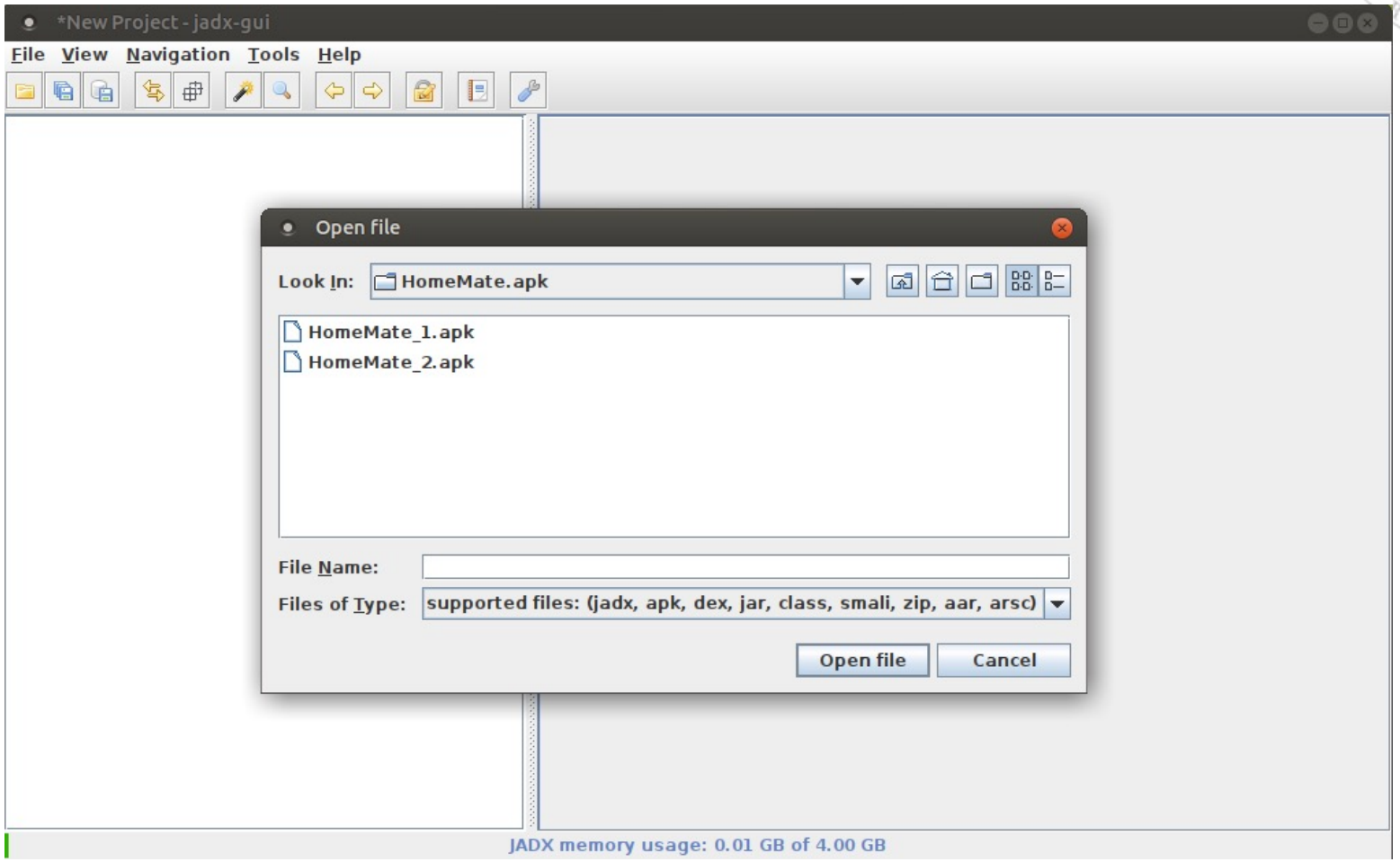
Smart Socket Initial Setup

1. Prepare the Linux Virtual Machine
2. Prepare the Raspberry Pi
3. Pair the Smart Socket

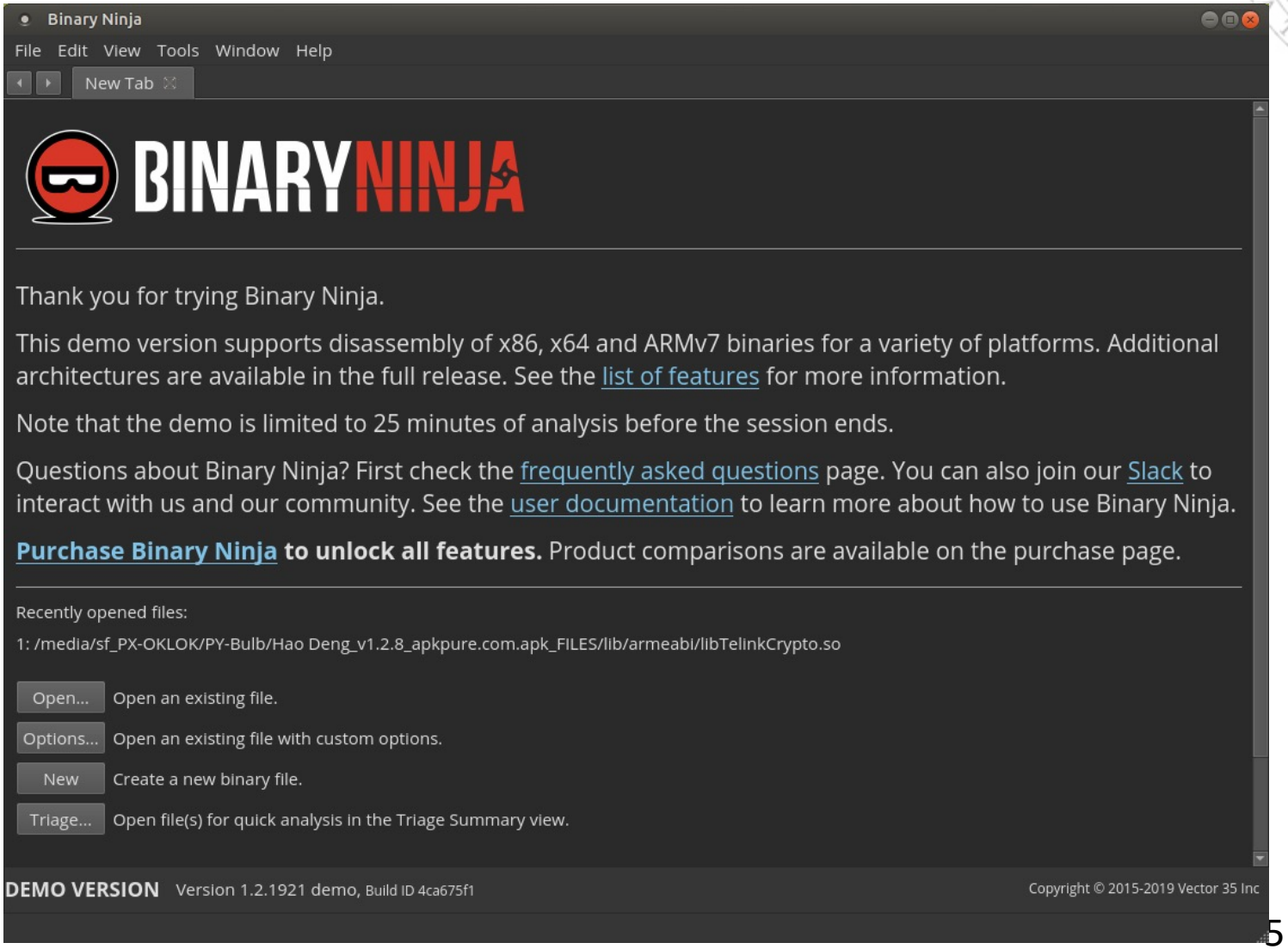
Initial Setup: Linux VM

1. Prepare the Linux Virtual Machine
   - Wireshark (already installed)
   - JADX Dex to Java decompiler:
     - github project homepage
     - Download releases from github
   - Binary Ninja homepage link
     - Demo version link

JADX Dex to Java decompiler



Binary Ninja homepage



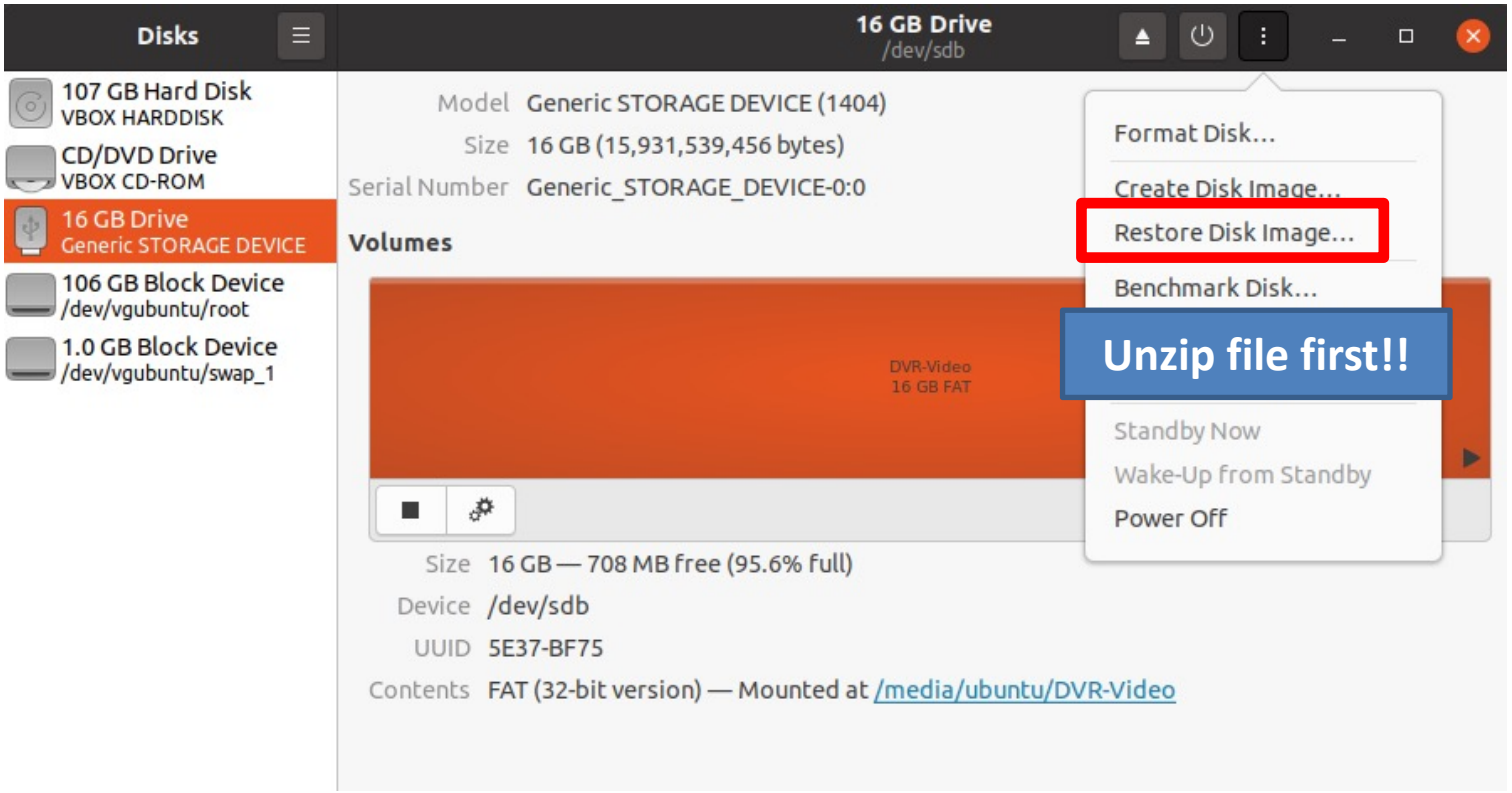
Smart Socket Initial Setup

1. Prepare the Linux Virtual Machine
2. Prepare the Raspberry Pi
3. Pair the Smart Socket

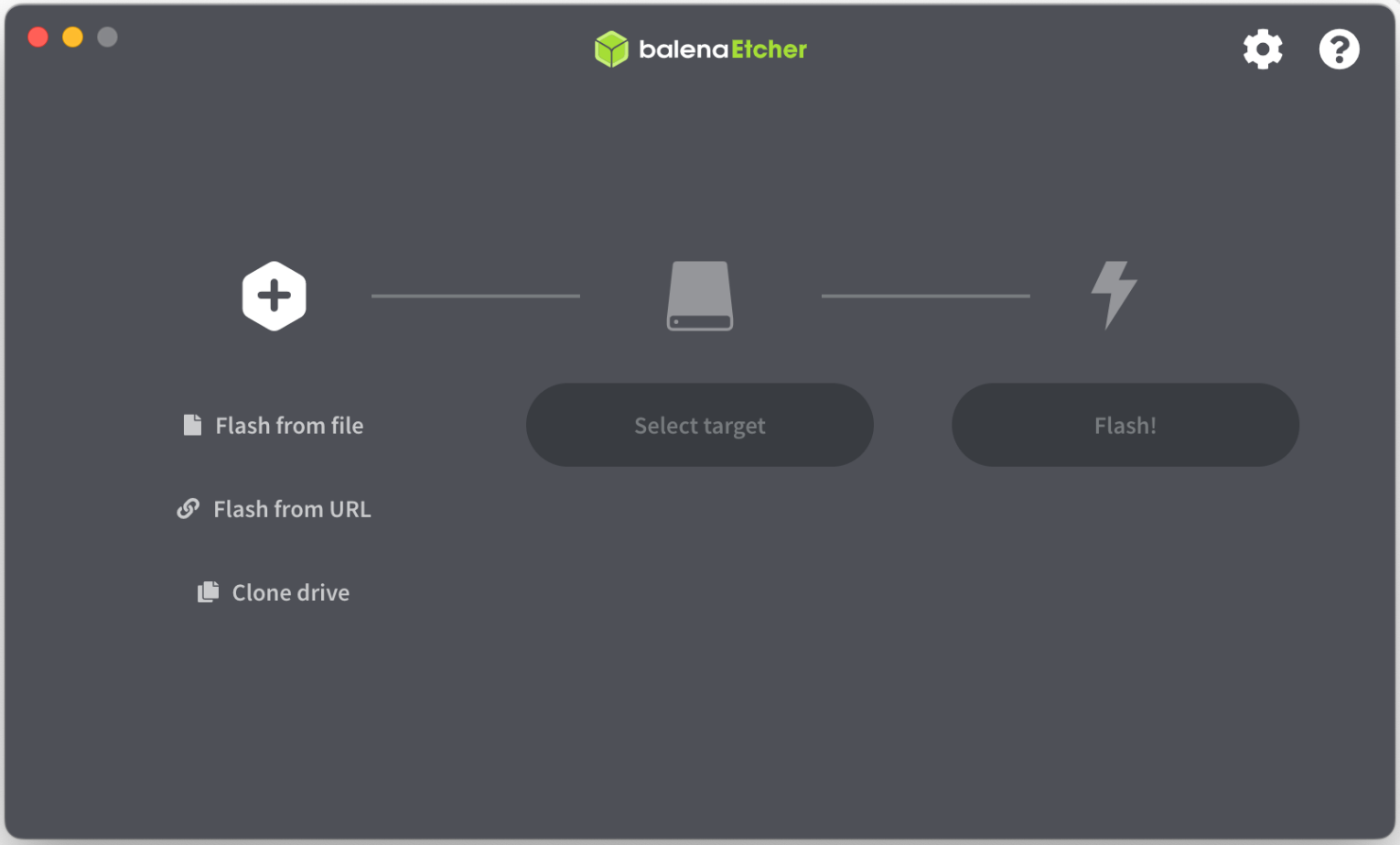
Initial Setup: raspberry Pi 4

2. Prepare the Raspberry Pi:
   - Download `Raspi-IoT-DA.img.zip` image
     - Link available in your email
   - Flash the image into the SD cart using:
     - Option 1: Use the Linux Virtual Machine or
     - Option 2: Raspberry Pi Imager: link or
     - Option 3: balenaEtcher: link

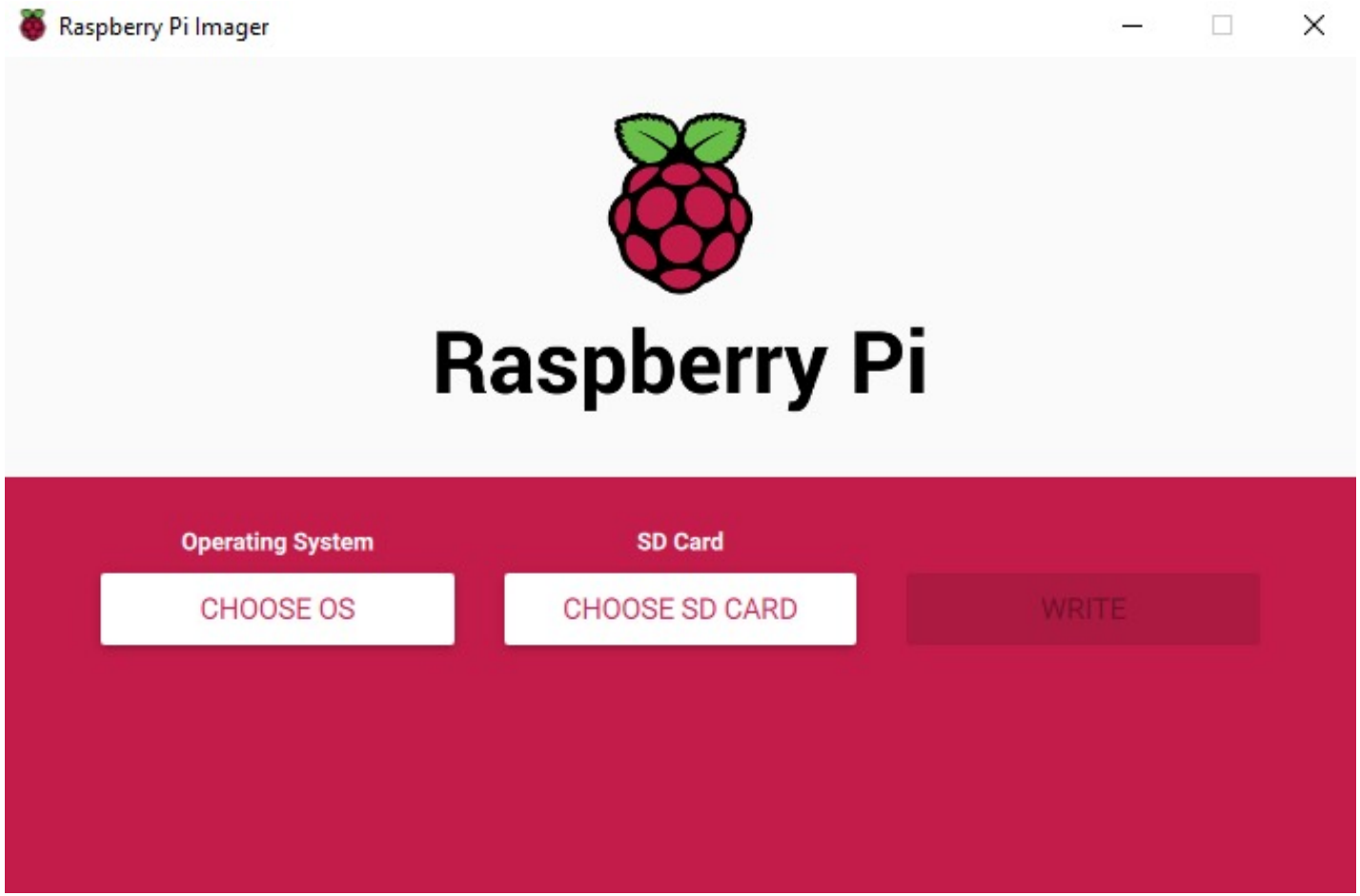
Flash the image: Virtual machine



Flash the image: balenaEtcher



Flash the image: Raspberry Pi Imager



Initial Setup: raspberry Pi 4

2. Prepare the Raspberry Pi:
   - Download Raspi-IoT-DA.img.zip image
   - Flash the image into the SD cart using:
   - Plug the SD card in the Raspberry Pi 4
     - Connect the ethernet cable (access to the Internet)
     - Optional: connect a mouse, keyboard, HDMI monitor
     - Connect the power supply and wait for 3min
       - User `'iot'`, password `'IoT-DA'`
     - Obtain IP address:
       - ping -c 4 raspy-iot-da
       - Access your router: http://192.168.1.1
       - nmap -sn 192.168.1.0/24

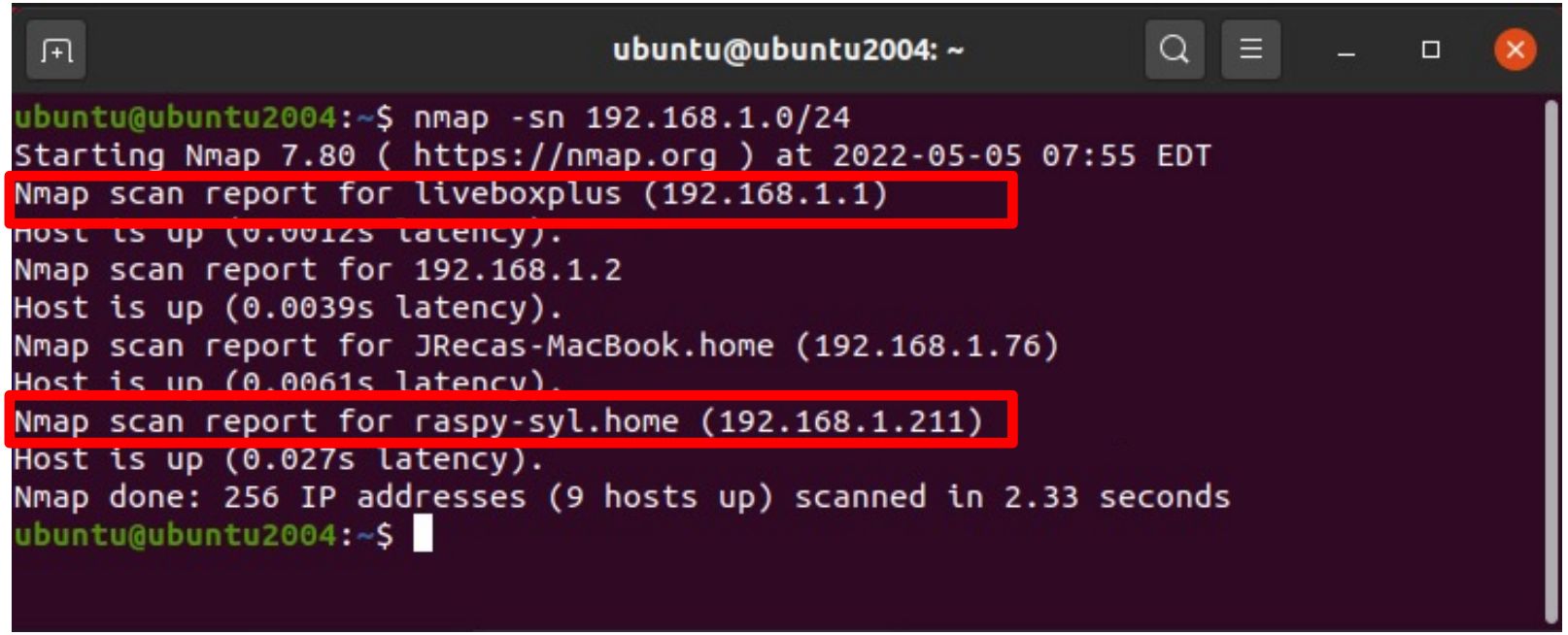
Obtain Raspberry Pi IP address

```
iot@raspy-iot-da: ~                                    ⌥⌘1
vpn-216-178:iot-da.github.io jrecas$ ping -c 4 raspy-iot-da
PING raspy-iot-da.home (192.168.1.211): 56 data bytes
64 bytes from 192.168.1.211: icmp_seq=0 ttl=64 time=0.642 ms
64 bytes from 192.168.1.211: icmp_seq=1 ttl=64 time=0.668 ms
64 bytes from 192.168.1.211: icmp_seq=2 ttl=64 time=0.664 ms
64 bytes from 192.168.1.211: icmp_seq=3 ttl=64 time=0.808 ms

--- raspy-iot-da.home ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.642/0.696/0.808/0.066 ms
vpn-216-178:iot-da.github.io jrecas$
```

Obtain Raspberry Pi IP address

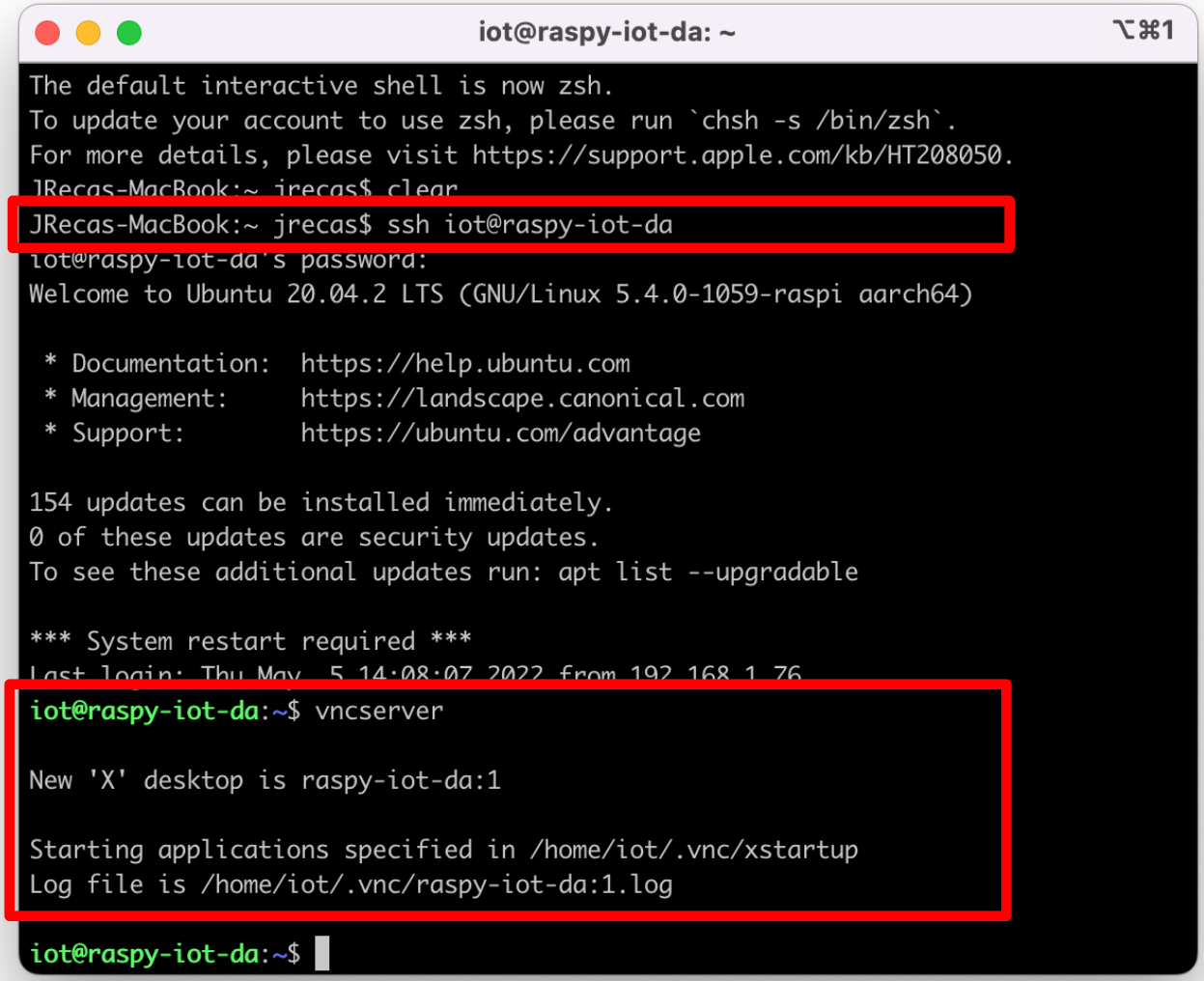
```
$ sudo apt-get install nmap
```



Initial Setup: raspberry Pi 4

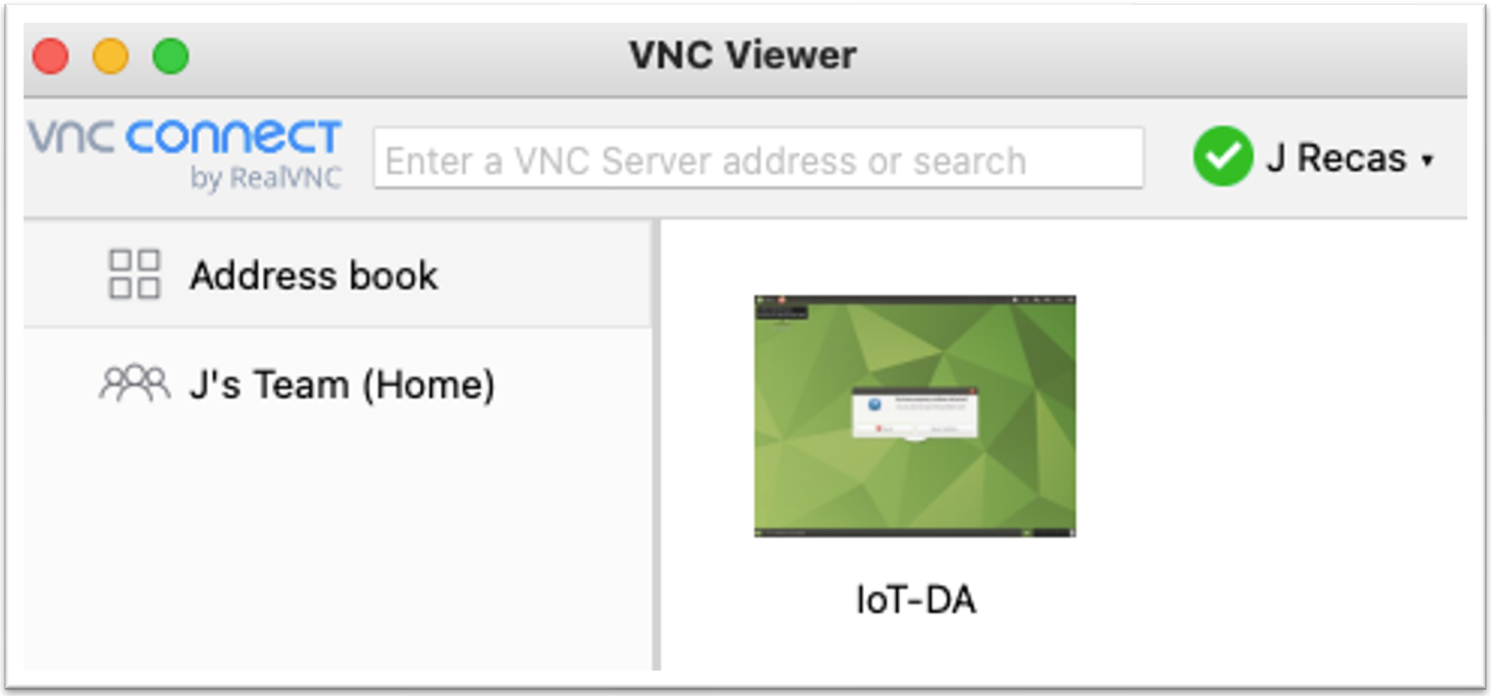
2. Prepare the Raspberry Pi:
   - Download Raspi-IoT-DA.img.zip image
   - Flash the image into the SD cart using:
   - Plug the SD card in the Raspberry Pi 4
   - Log in:
     - Option 1: Mouse, keyboard, HDMI monitor
     - Option 2: remote ssh access
     - Option 3: use VNC viewer

VNC Server



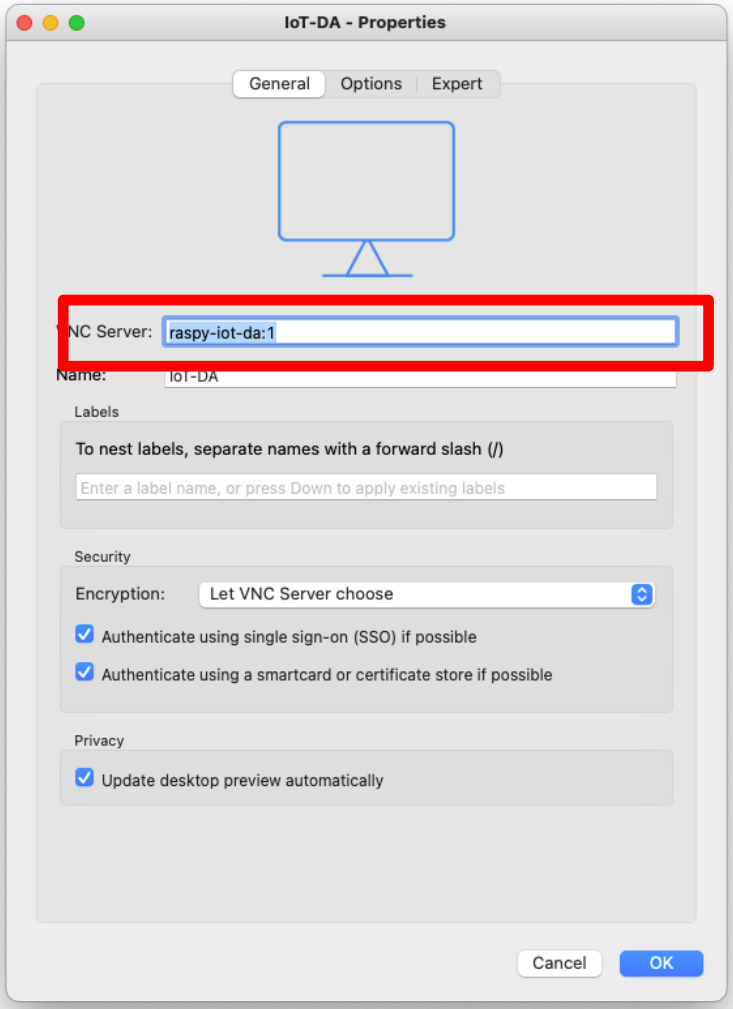

```
$ vncserver -kill :1
```

VNC Viewer

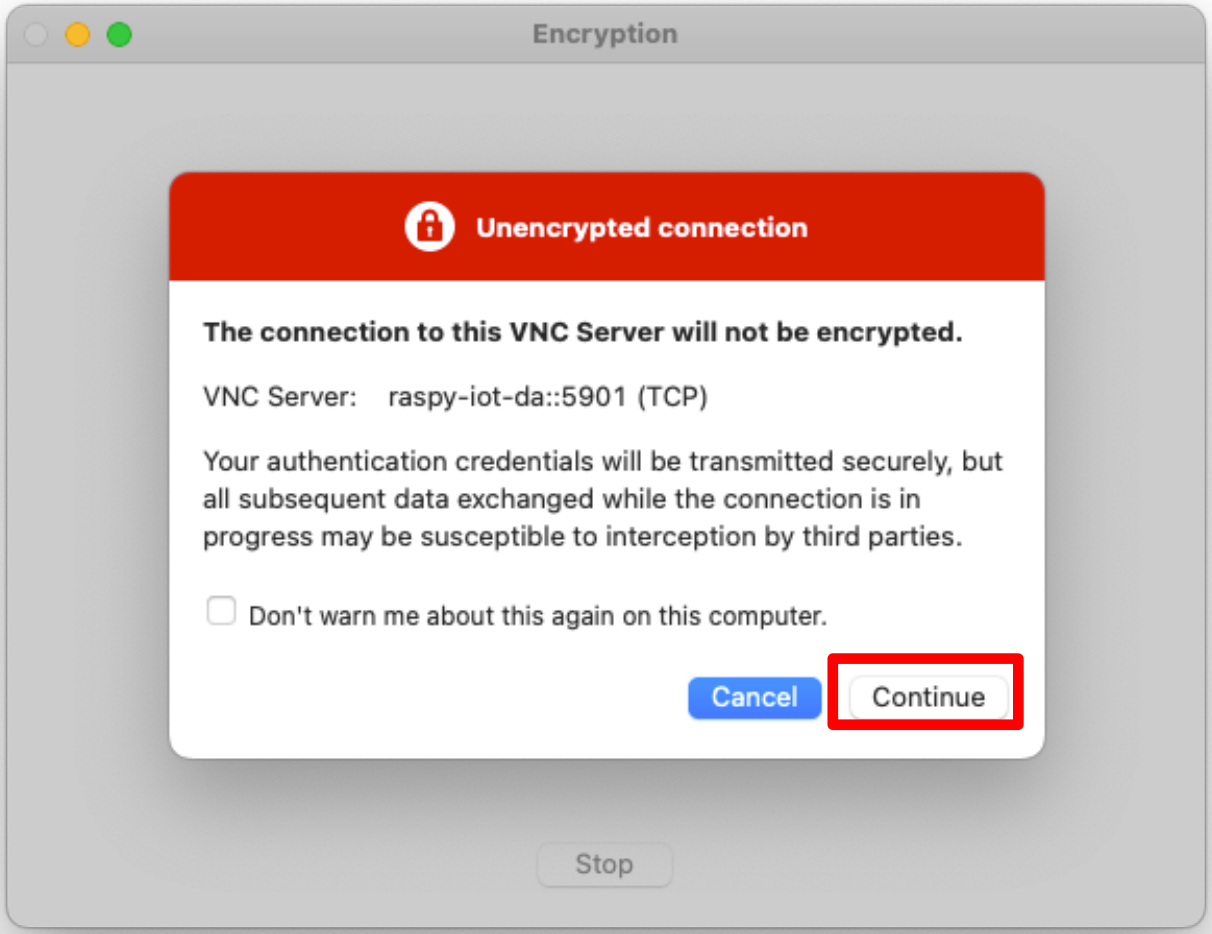


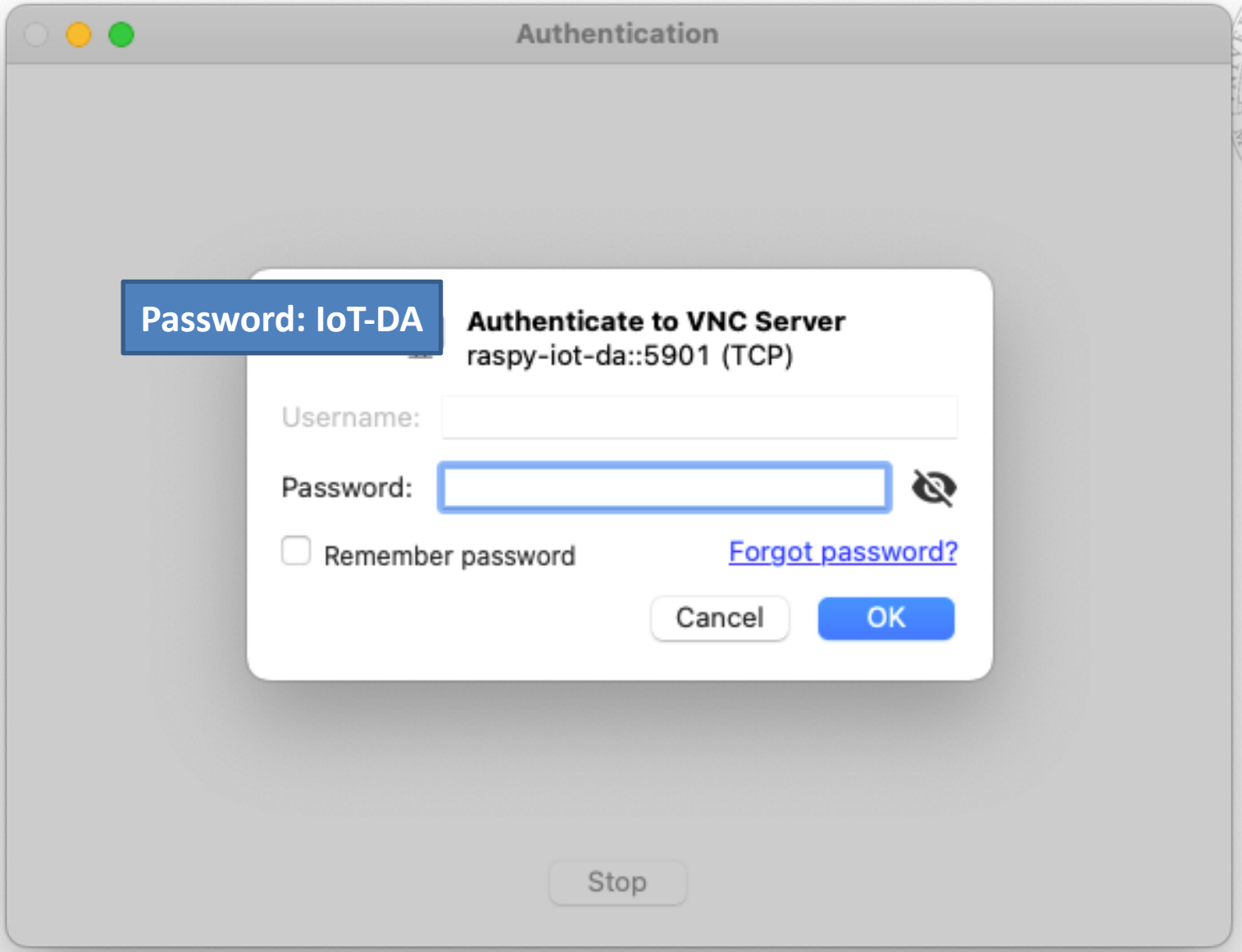
Real VNC Viewer

VNC Viewer


IoT-DA - Properties
General
Options
Expert
VNC Server:
raspy-iot-da:1
Name:
IoT-DA
Labels
To nest labels, separate names with a forward slash (/)
Enter a label name, or press Down to apply existing labels
Security
Encryption:
Let VNC Server choose
Authenticate using single sign-on (SSO) if possible
Authenticate using a smartcard or certificate store if possible
Privacy
Update desktop preview automatically
Cancel
OK

VNC Viewer


Encryption
Unencrypted connection
The connection to this VNC Server will not be encrypted.
VNC Server: raspy-iot-da::5901 (TCP)
Your authentication credentials will be transmitted securely, but all subsequent data exchanged while the connection is in progress may be susceptible to interception by third parties.
Don't warn me about this again on this computer.
Cancel
Continue
Stop


Authentication
Password: IoT-DA
Authenticate to VNC Server
raspy-iot-da::5901 (TCP)
Username:
Password:
Remember password
Forgot password?
Cancel
OK
Stop

Initial Setup: raspberry Pi 4

2. Prepare the Raspberry Pi:
   - Download Raspi-IoT-DA.img.zip image
   - Flash the image into the SD cart using:
   - Plug the SD card in the Raspberry Pi 4
   - Log in
   - By default the Raspi creates a WiFi Access Point
     - SSID: `MasterIoT`
     - Password: `MasterIoT`
   - Connect to the AP and check internet access

Smart Socket Initial Setup

1. Prepare the Linux Virtual Machine
2. Prepare the Raspberry Pi
3. Pair the Smart Socket

Initial Setup: Smart Socket

3. Pair the Smart Socket
   - Download the android App (HomeMate.apk)
   - Install it in your Android device
     - If you do not have and Android device contact me
   - Register into the App by creating a new user

Initial Setup: S20C/S30C devices

- WIFI Smart Socket ORVIBO-S20C/S30C
- Wifi 2,4 GHz b/g/n
  - WEP/WPA-PSK/WPA2-PSK
  - Power cons.: ≦0. 3 W
- Input/output:
  - 100-240V ~, 50 H, 8A

ORVIBO Home

HomeMate 365 Co., Ltd. House & Home

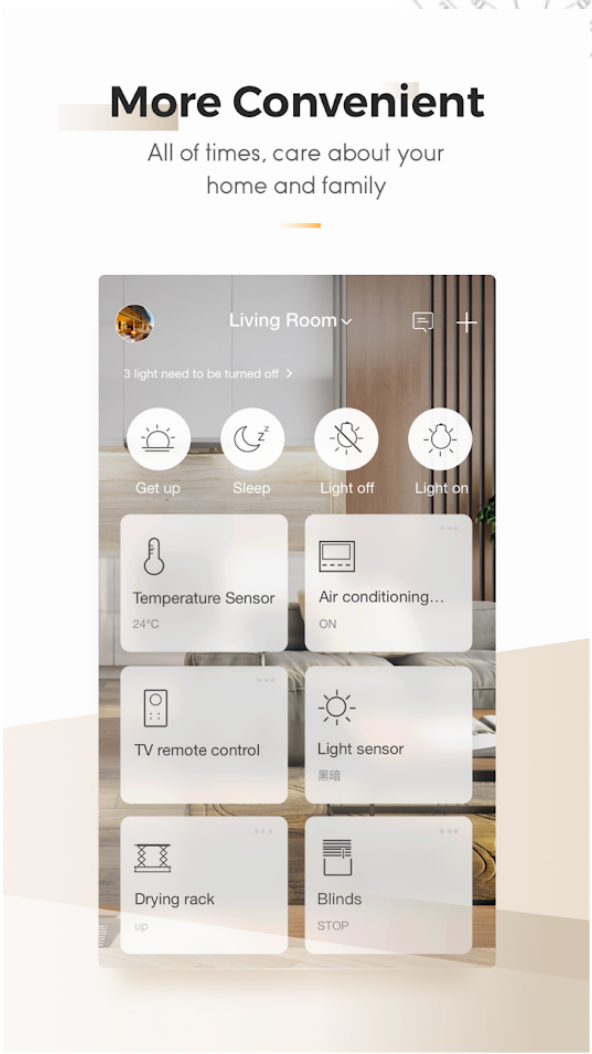
★★★☆☆ 1,968

Everyone

This app is available for some of your devices

You can share this with your family. Learn more about Family Library

Add to Wishlist



- With smart home platform ORVIBO Home, you can many controls as follow:
  - Control and manage all kinds of devices like curtains, air conditioners, TV, lights, switches, sockets and etc in one APP.
  - Create different scenes to control multiple devices.
  - Make ‘If this then that’ synchronizations scenario.

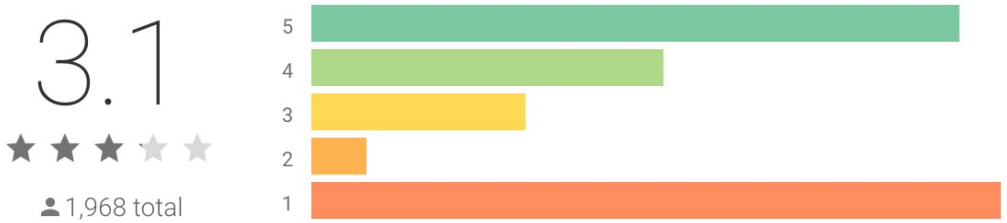
ORVIBO Home

ADDITIONAL INFORMATION

Updated	Size	Installs
April 29, 2022	150M	100,000+
Current Version	**Requires Android**	**Content Rating**
5.0.6.304	4.4 and up	Everyone Learn more
Permissions	**Report**	**Offered By**
View details	Flag as inappropriate	HomeMate 365 Co., Ltd.

REVIEWS

Review policy and info



ORVIBO Home has access to:

Device & app history
- retrieve running apps
- read your Web bookmarks and history

Identity
- find accounts on the device

Contacts
- modify your contacts
- read your contacts

Location
- approximate location (network-based)
- precise location (GPS and network-based)

Phone
- read phone status and identity

Photos/Media/Files
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Microphone
- record audio

Storage
- read the contents of your USB storage
- modify or delete the contents of your USB storage

Camera
- take pictures and videos

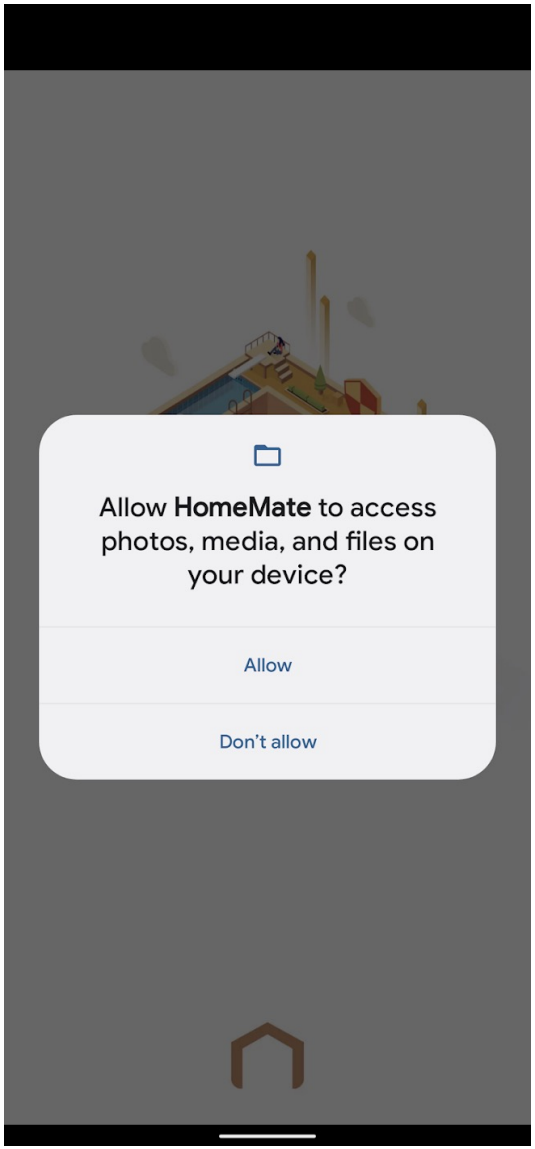
Wi-Fi connection information
- view Wi-Fi connections

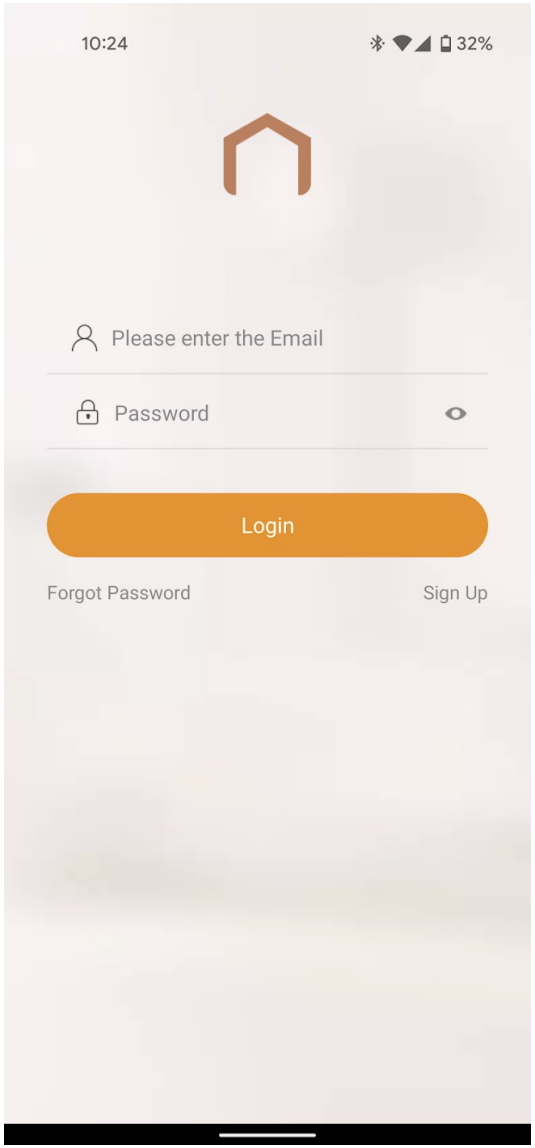
Device ID & call information
- read phone status and identity

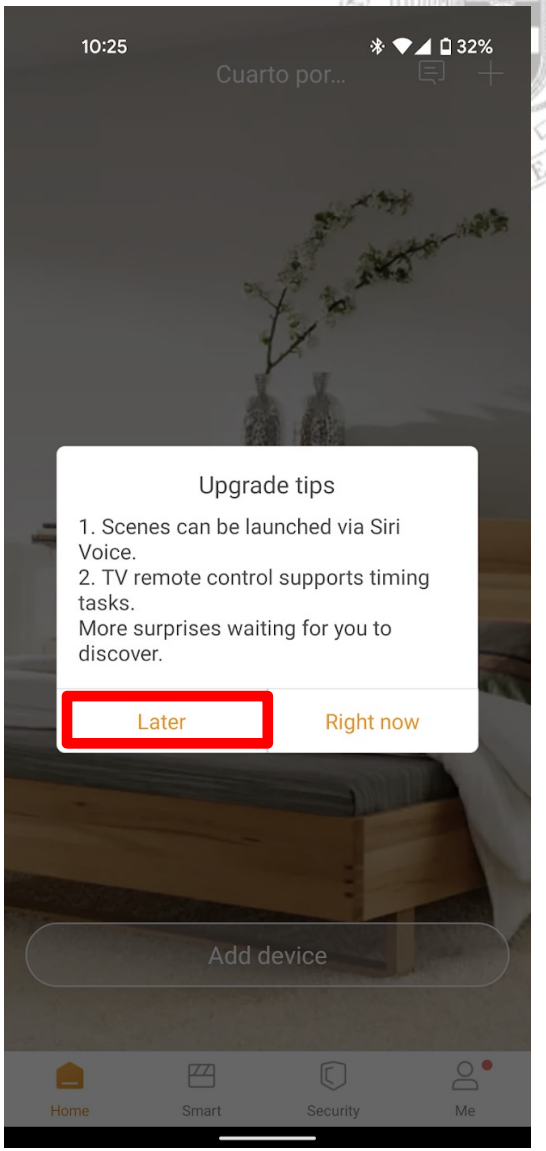
Other
- download files without notification
- view network connections
- pair with Bluetooth devices
- access Bluetooth settings
- connect and disconnect from Wi-Fi
- full network access
- control Near Field Communication
- control vibration
- prevent device from sleeping

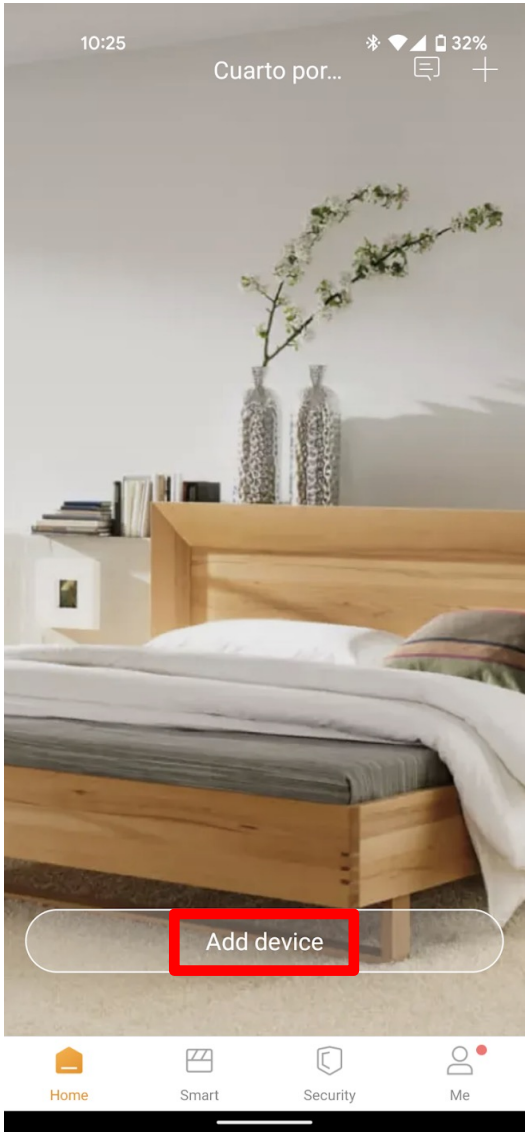
Initial Setup: Smart Socket

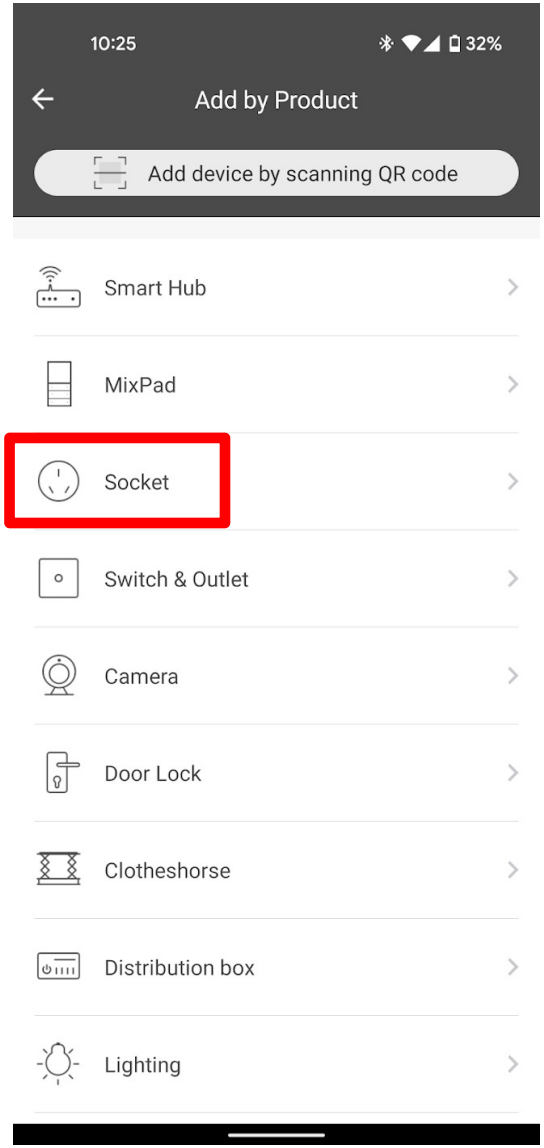
3. Pair the Smart Socket
   - Download the android App (HomeMate.apk)
   - Install it in your Android device
     - If you do not have and Android device contact me
   - Register into the App by creating a new user
   - Pair the socket

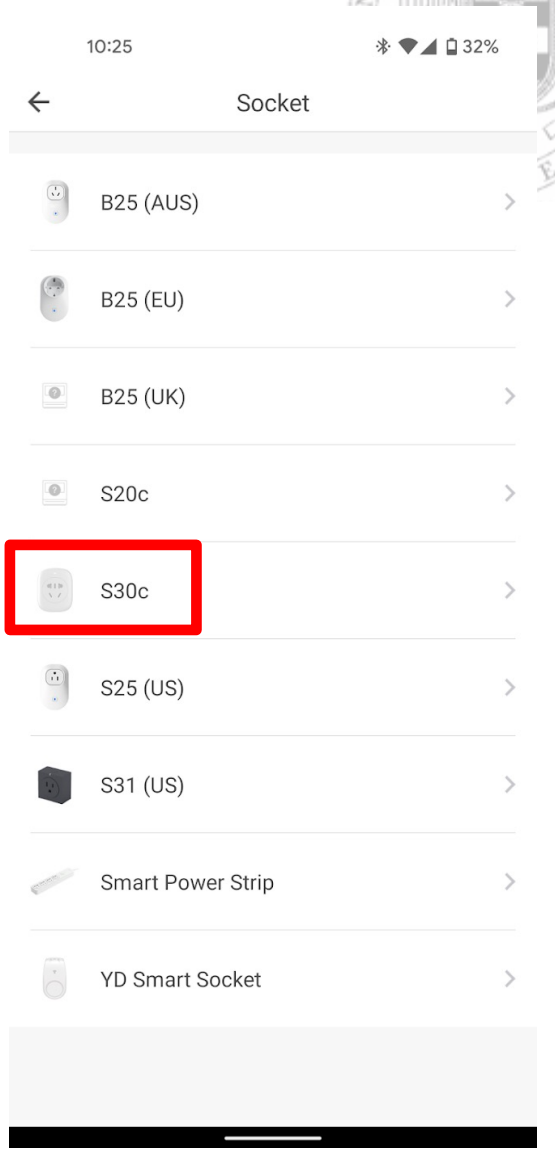

Allow HomeMate to access photos, media, and files on your device?
Allow
Don't allow

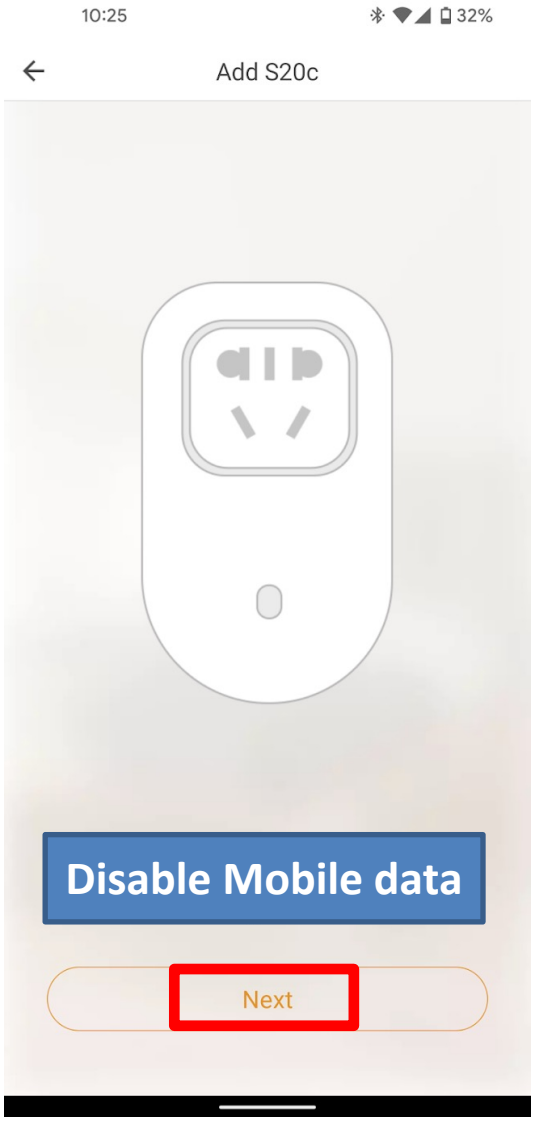

10:24
32%
Please enter the Email
Password
Login
Forgot Password
Sign Up

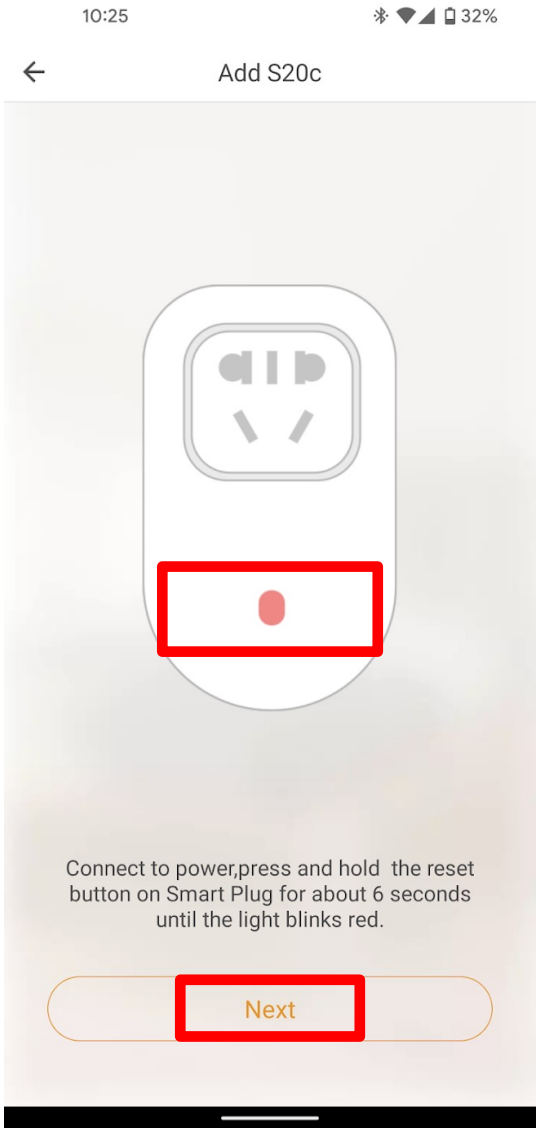

10:25
32%
Cuarto por...
Upgrade tips
1. Scenes can be launched via Siri Voice.
2. TV remote control supports timing tasks.
More surprises waiting for you to discover.
Later
Right now
Add device
Home
Smart
Security
Me

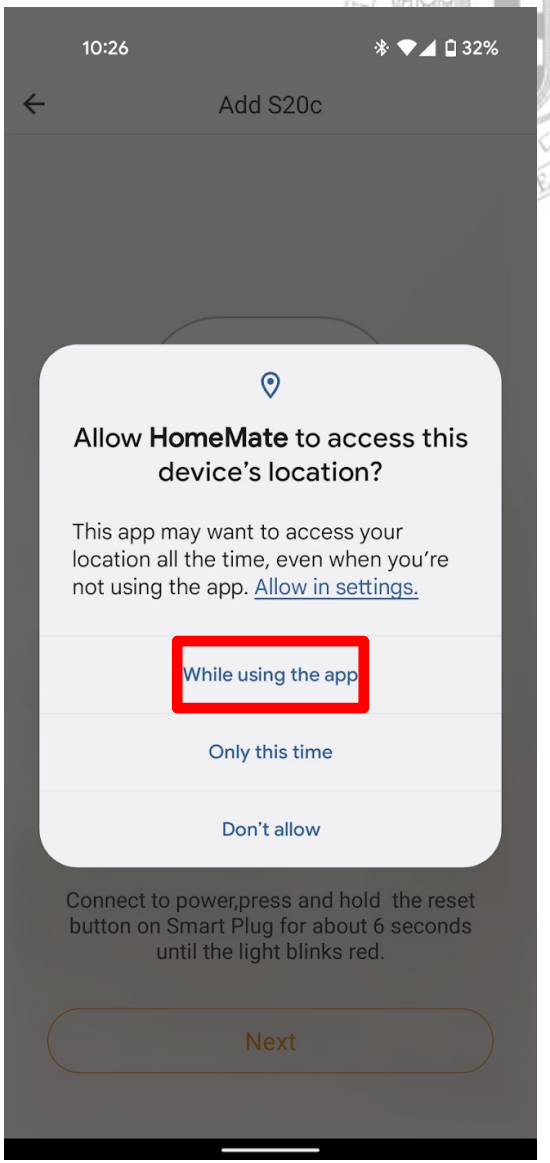

10:25
32%
Cuarto por...
Add device
Home
Smart
Security
Me

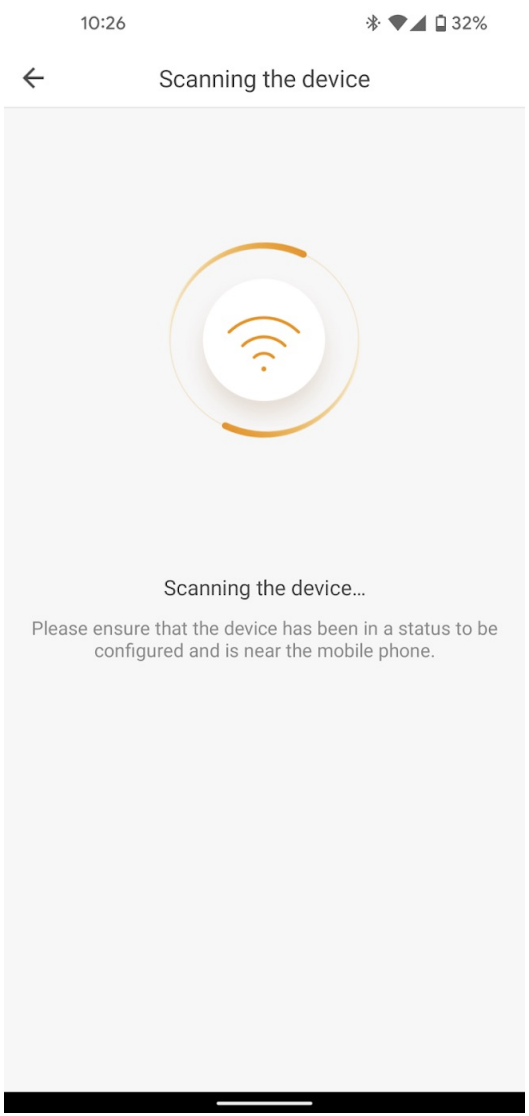

10:25
32%
Add by Product
Add device by scanning QR code
Smart Hub
MixPad
Socket
Switch & Outlet
Camera
Door Lock
Clotheshorse
Distribution box
Lighting

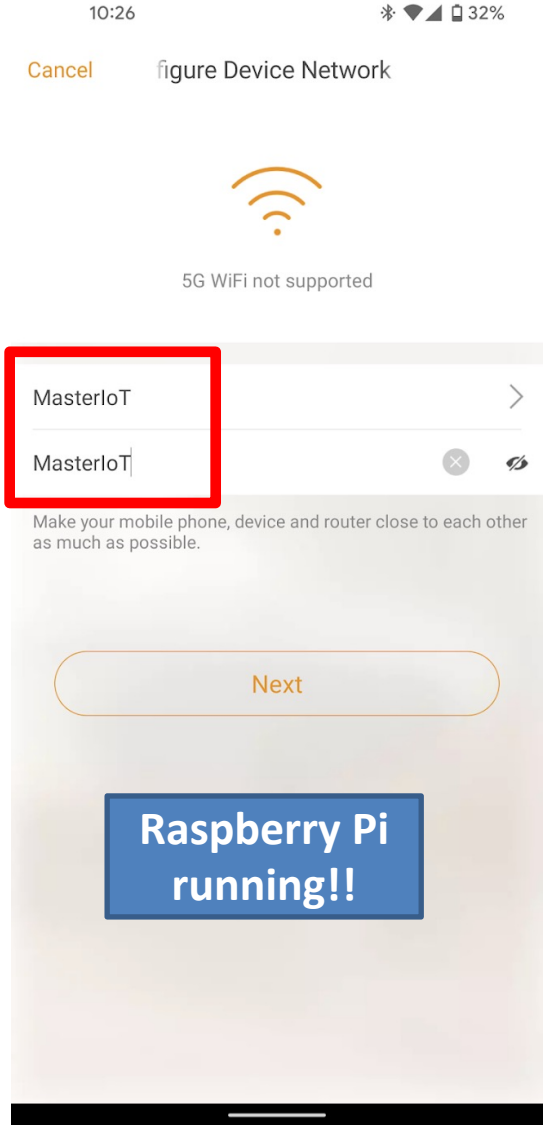

10:25
32%
Socket
B25 (AUS)
B25 (EU)
B25 (UK)
S20c
S30c
S25 (US)
S31 (US)
Smart Power Strip
YD Smart Socket

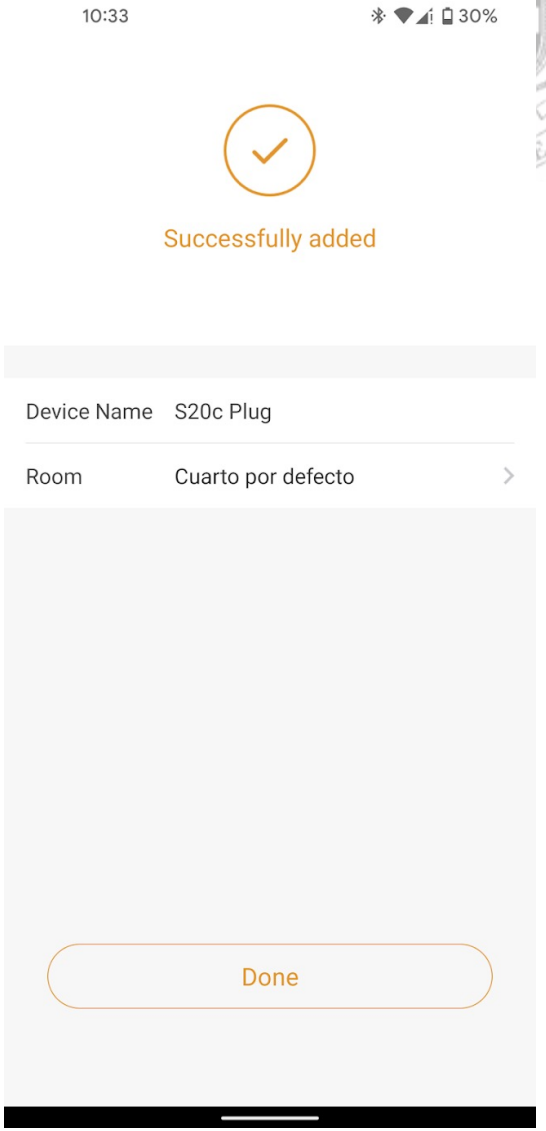

10:25
32%
Add S20c
Disable Mobile data
Next


10:25
32%
Add S20c
Connect to power,press and hold the reset button on Smart Plug for about 6 seconds until the light blinks red.
Next


10:26
32%
Add S20c
Allow HomeMate to access this device's location?
This app may want to access your location all the time, even when you're not using the app. Allow in settings.
While using the app
Only this time
Don't allow
Connect to power,press and hold the reset button on Smart Plug for about 6 seconds until the light blinks red.
Next


10:26
32%
Scanning the device
Scanning the device...
Please ensure that the device has been in a status to be configured and is near the mobile phone.


10:26
32%
Cancel
figure Device Network
5G WiFi not supported
MasterIoT
MasterIoT
Make your mobile phone, device and router close to each other as much as possible.
Next
Raspberry Pi running!!


10:33
30%
Successfully added
Device Name
S20c Plug
Room
Cuarto por defecto
Done

Setup completed!!!

- ✓ The Smart Plug is paired to our App
- ✓ The Smartphone and the Smart Socket are connected to the Raspberry Pi Access Point
- ✓ We can turn on/off the Smart Socket using the App