/SMART PLUG HACKING

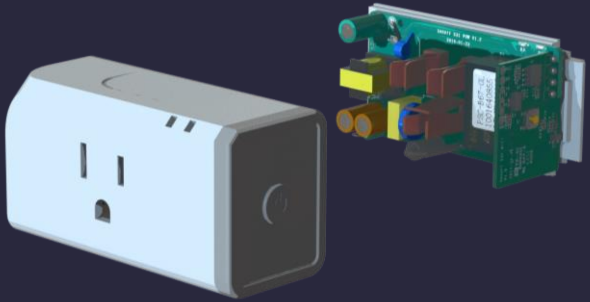
IEEE COMPUTER SOCIETY

Student Branch Chapter at the University of South Florida

Workshop by:

Myles Keller

myleskeller@usf.edu



IEEE COMPUTER SOCIETY @USF

/ITENERARY

/01

/BACKGROUND & MOTIVATION

The importance of personal security & Right to Repair

/02

/DISASSEMBLY & WIRING

Taking device apart & attaching FTDI converter wires

/03

/FLASHING & CONFIGURING

Running esptool.py, getting device MAC, & flashing firmware

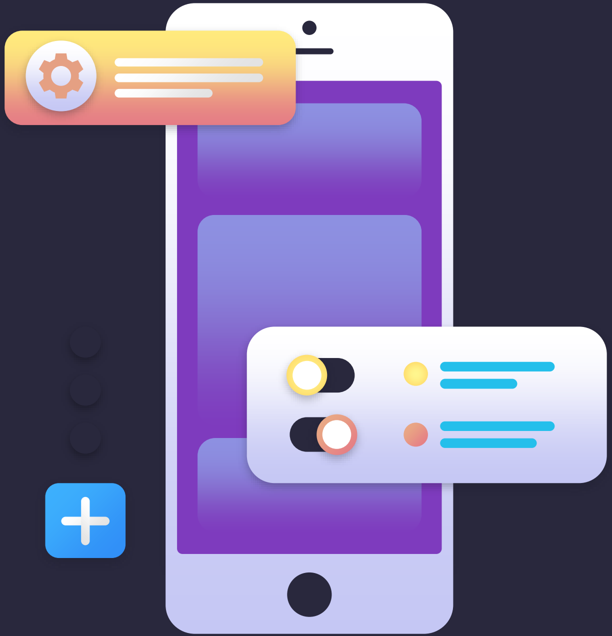
/04

/REASSEMBLY & TESTING

Confirming flashes, mass testing, & final reassembly

IEEE COMPUTER SOCIETY @USF

/01
/BACKGROUND & MOTIVAITON



/WHAT IS A SMART PLUG?

A smart plug is the cheapest, easiest way to remotely control any electrical device in your home.

Whether home or away, you can turn outlets on and off, have them trigger at scheduled times, or synchronize them with other linked smart devices.

/BENEFITS

/CONVENIENCE

Manage many devices in one user interface.

/REMOTE ACCESS

Don't have to be home to control devices.

/AUTOMATION

Automate the functionality of a smart home ecosystem.

/ENERGY EFFICIENCY

Reduce energy consumption and gain electricity usage insights.

/POTENTIAL ISSUES

/SECURITY & UPGRADABILITY

Is the device firmware upgradable/modifiable?

/INTERNET DEPENDENCE

Does the device function if the internet is down?

/DEVICE LIFESPAN

How long will the vendor support this device?

/DATA PRIVACY

What data is collected by companion apps? What online route do commands take?

/COMMAND DATA SECURITY & PRIVACY

/THE SCENIC ROUTE

Smart plug commands must travel across the world for your device to function.

More exposure to the internet = more opportunities for security breaches.

/PRODUCT/MANUFACTURER SUPPORT

/SUDDEN DEATH

Smart plugs must be able to communicate with their vendor to function.

If a manufacturer goes under or drops device support, you own a paperweight.

/INTERNET CONNECTION DEPENDENCE

/OFF THE GRID

Smart plugs require constant internet communication to function.

Even if your Wi-Fi is on and you're at home, no internet = no device control.

<APP DATA PRIVACY>

↓

“The company gathers certain information about you. Information about you is also used by our affiliated entities and group companies.”

—TP-Link’s EULA

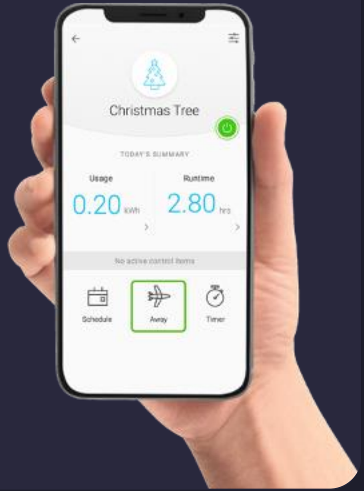
tp-link

tp-link

“Other information automatically collected may include:

- IP address
- location
- mobile device information
- operating system
- browser type
- demographic information
- application information
- URL information
- pages you interact with
- other information associated with how you interact with pages and service.”

—TP-Link’s EULA



<RIGHT TO REPAIR>

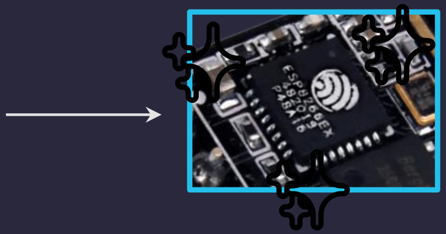
“You bought it. You own it. And you have the right to fix it.”

—LOUIS ROSSMAN

<RIGHT TO REPAIR>

> "You bought it. You own it. And you have the right to modify it."

—ME



/THE VICTIM

The model selected for this workshop is the Sonoff S31 by Itead. The S31 is a WiFi-enabled smart plug with energy monitoring functionality.

The S31 is ideal for hacking because its controller, the ESP8266, is very well established in the open-source community.

/SONOFF S31 SOFTWARE

/STOCK FIRMWARE

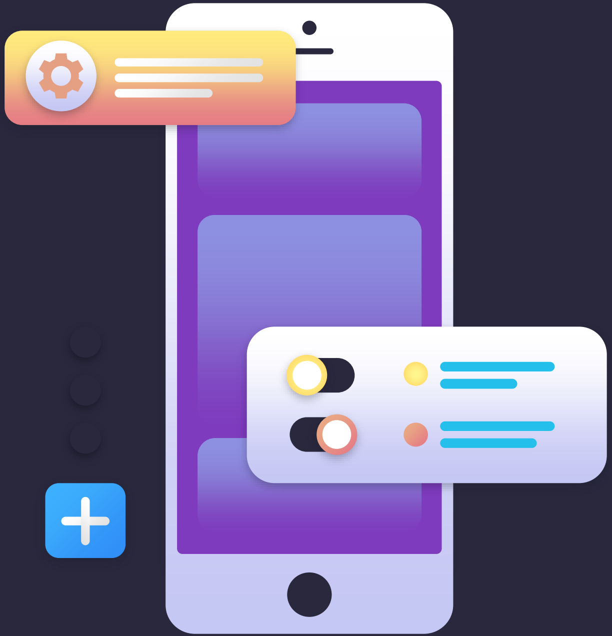
- Routes commands through servers outside US
- Requires constant internet connection
- Companion app requires account signup
- Cannot be modified

/TASMOTA FIRMWARE

- All comands are processed locally on LAN
- No internet required
- No specific app, HTTP is also supported natively
- Upgrade/downgrade/change firmware at any time

IEEE COMPUTER SOCIETY @USF

/DISASSEMBLY & WIRING /02



<WORKSHOP RULES>

DO NOT JUMP AHEAD

Do **NOT** do anything until the breakout sections.

IEEE COMPUTER SOCIETY @USF

<WORKSHOP RULES>

USE A SOFT TOUCH

The components in this device are delicate. We do NOT have spare parts.

<WORKSHOP RULES>

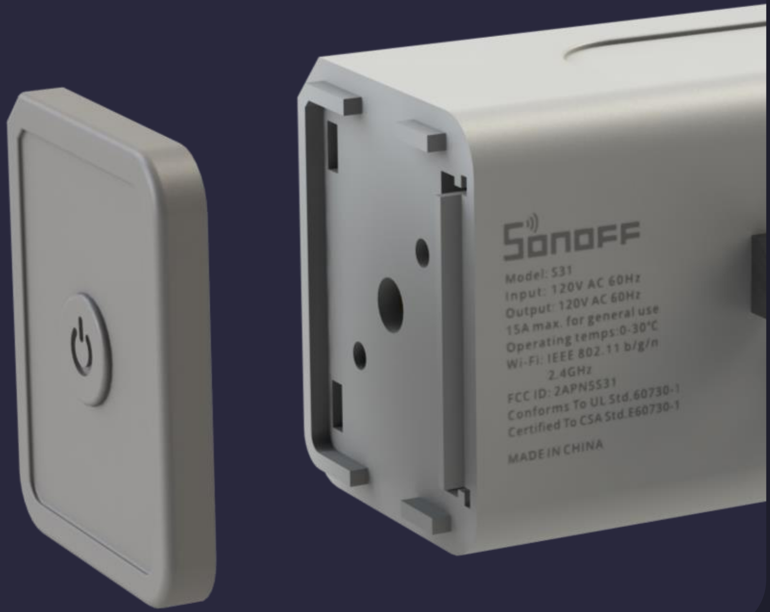
DO NOT PLUG ANYTHING IN

We'll all
do this
at the
same time
later.

/REMOVE GRAY CAP

Pry the gray plastic cap off the device shell. If having trouble, slip a flathead screwdriver or plastic card along the seam until you work one edge loose.

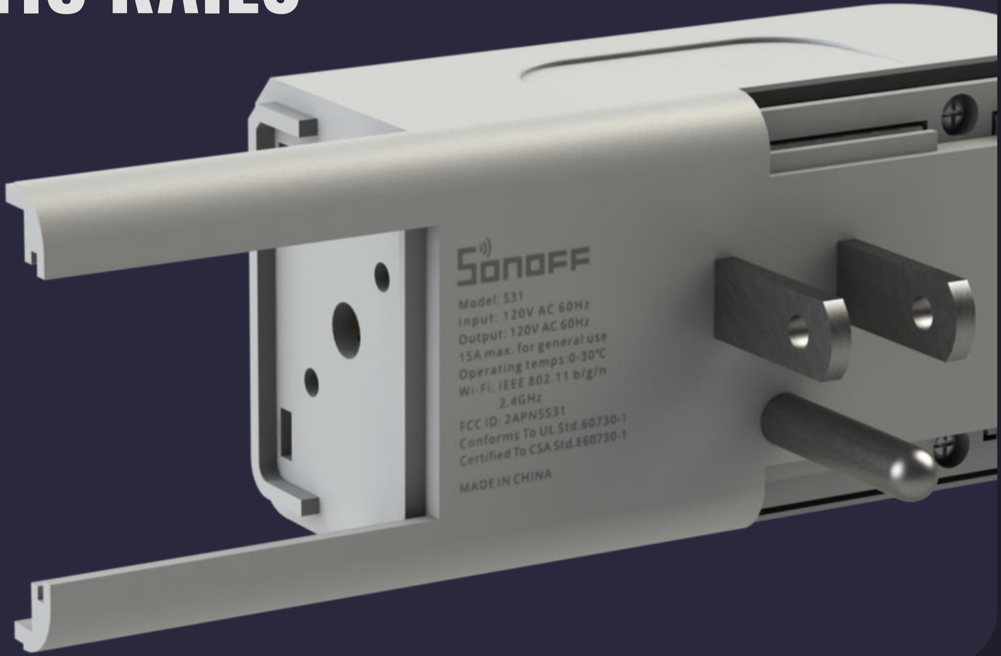
Place the cap in the provided clear plastic case.



/SLIDE OUT PLASTIC RAILS

Both plastic rails should slide out easily.

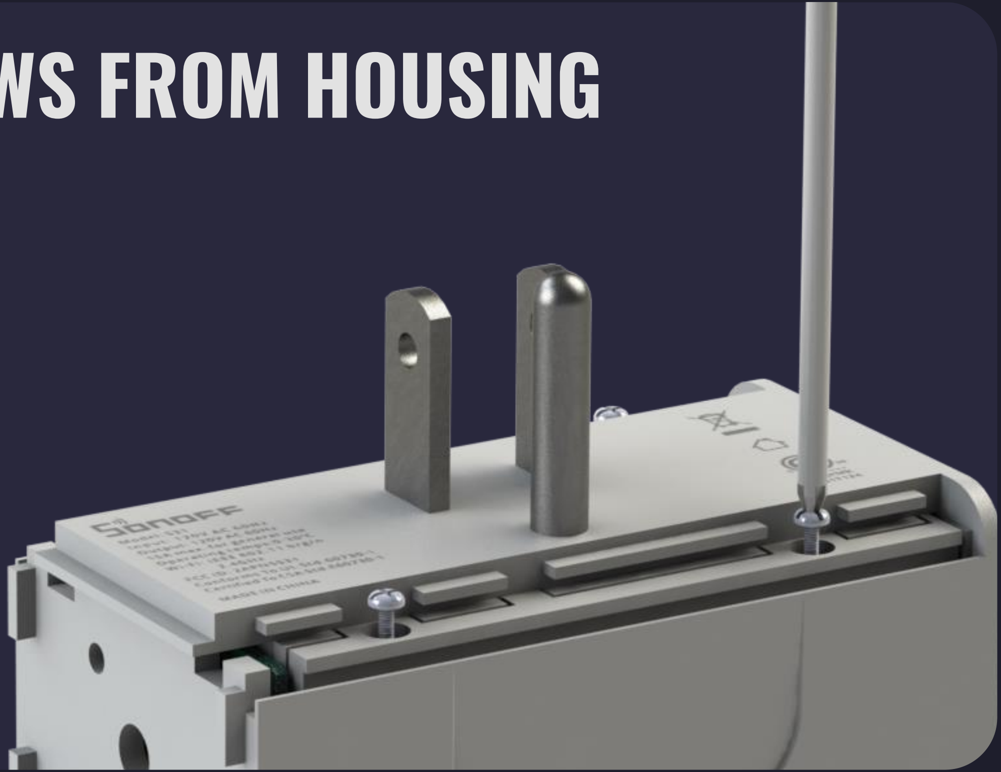
Place both rails in the provided clear plastic case.



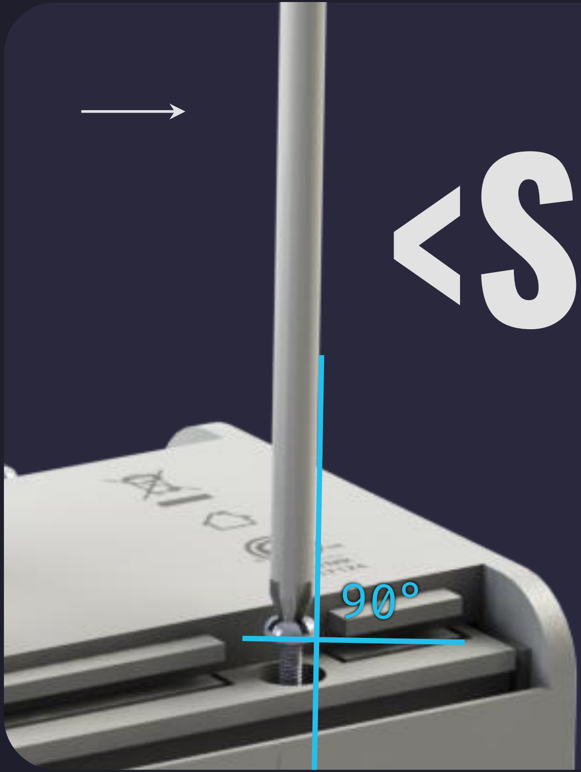
/REMOVE 3 SCREWS FROM HOUSING

Place the device “face-down” on a flat surface. Keep your screwdriver perpendicular to the screw head and apply firm pressure while unscrewing the 3 screws.

We have no spare screws. Place the removed screws in the provided clear plastic case and secure it shut.



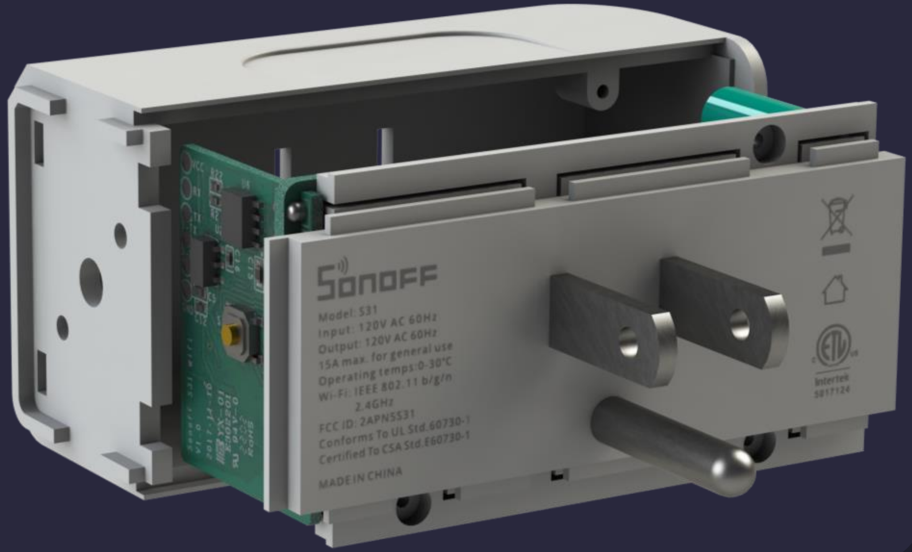
<STRIPPERS>



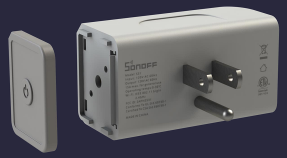
These screws are prone to stripping. Keep the screwdriver perpendicular to the screw head to avoid stripping.

/DETACH HOUSING FROM SHELL

Firmly grasp the prongs of the outlet and gradually wiggle the housing loose from the outer shell.

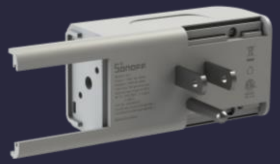


/BREAKOUT (DISASSEMBLY)



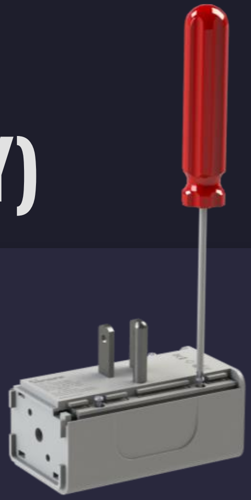
/REMOVE GRAY CAP

Pry around edges with flathead/card to pop loose



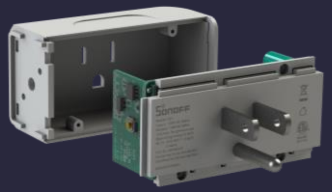
/SLIDE OUT WHITE RAILS

Should slide out freely after cap has been removed



/REMOVE 3 SCREWS

Keep driver perpendicular -screws can strip easily

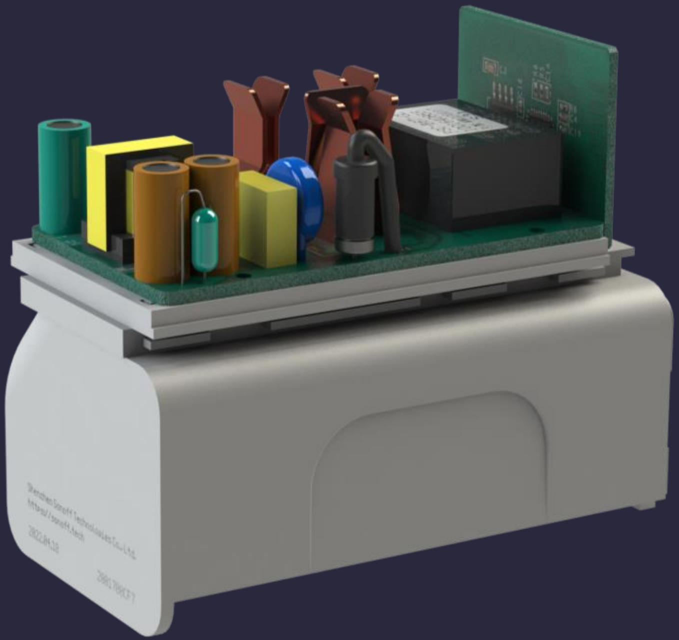


/DETACH HOUSING

Grip prongs of plug and wiggle loose plastic shell

/INSERT PLUG INTO HOUSING

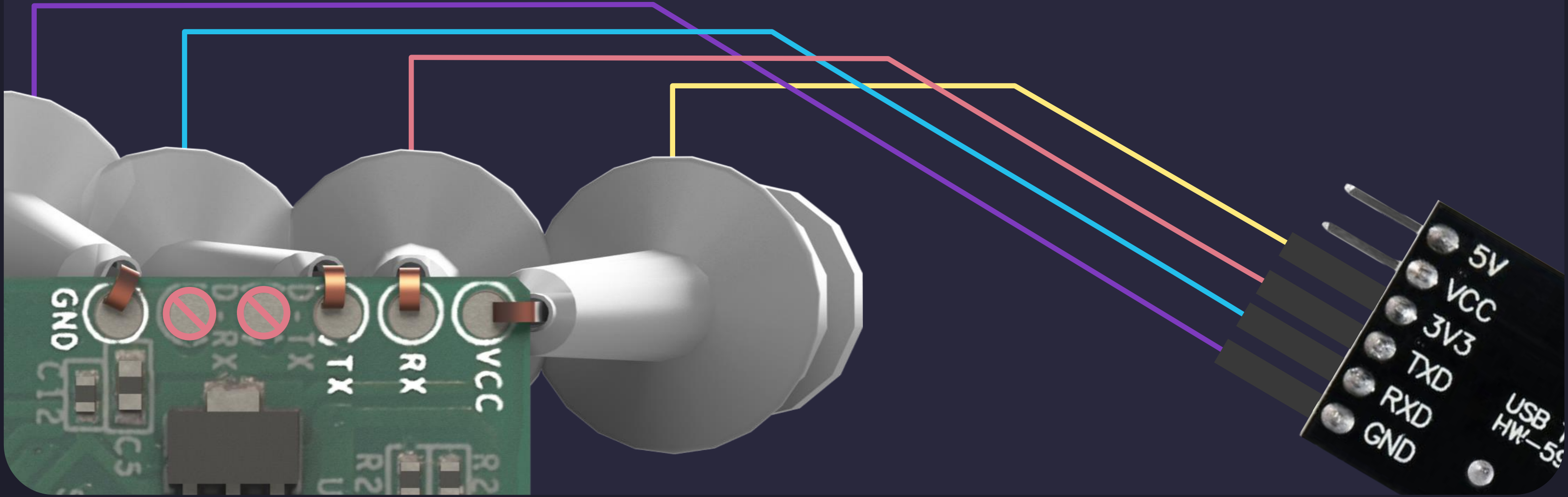
This will help maintain stability while plugging in the FTDI converter.



IEEE COMPUTER SOCIETY @USF

/CONNECT WIRES BETWEEN S31 AND FTDI CONVERTER

TX	->	RXD
RX	->	TXD
VCC	->	3V3
GND	->	GND

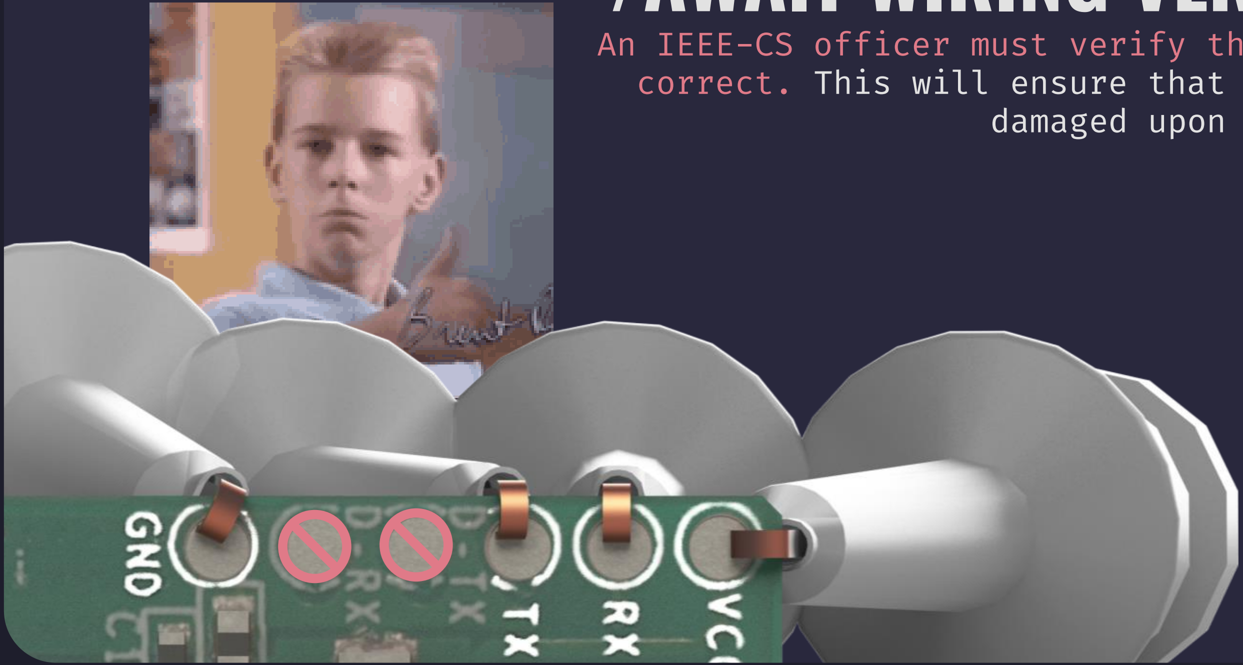


<DEATH>

DO NOT plug in the USB FTDI converter.
Incorrect wiring can *destroy the device*.
We will perform this together after
everyone’s wiring has been verified.

/AWAIT WIRING VERIFICATION

An IEEE-CS officer must verify that your wiring is correct. This will ensure that the device is not damaged upon being plugged in.



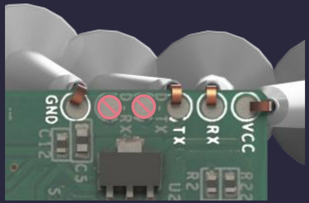
/BREAKOUT (WIRING)

/PLUG HOUSING IN TO OUTER SHELL

Place the housing into the removed outer shell to give the device more stability.

/CONNECT HOOK CLIP WIRES

Connect the wires according to their labels and the diagram.

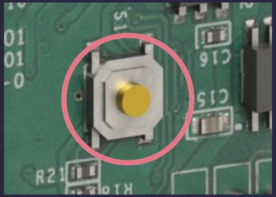


/AWAIT HOOK CLIP VERIFICATION

DO NOT PLUG IN THE FTDI CONVERTER. Incorrect wiring can destroy the device.

IEEE COMPUTER SOCIETY @USF

/BREAKOUT (BOOTLOADER MODE)

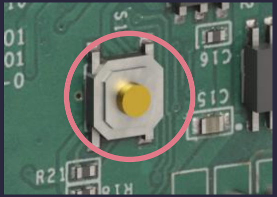


/PRESS AND HOLD GOLD BUTTON (S1)

Keep holding until USB is plugged in.

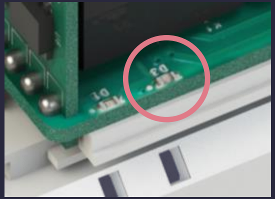
/PLUG FTDI CONVERTER INTO PC

Check orientation of USB port first.



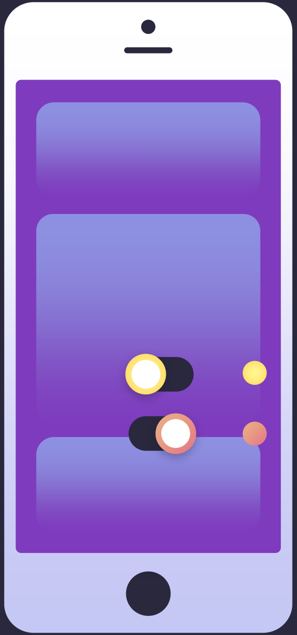
/WAIT 3 SEC TO RELEASE BUTTON (S1)

The extra time is just a precaution.



/BLUE LED (D3) SHOULD REMAIN OFF

If D3 illuminates, repeat.



/03 /FLASHING & CONFIGURING

/FLASHING

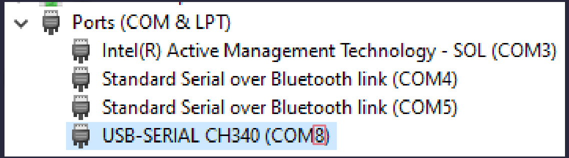
/DOWNLOAD THE REPOSITORY

Access tinyurl.com/sonshot
Extract the downloaded .zip to a convenient folder.
Open that folder in a new window.

/INSTALL PYTHON

Open the cmd shortcut and enter ‘python’.
If this opens the Microsoft Store, click Get and wait for the install to complete.
Alternatively, open ‘install python.lnk’ in the folder.

/FLASHING



Ports (COM & LPT)
Intel(R) Active Management Technology - SOL (COM3)
Standard Serial over Bluetooth link (COM4)
Standard Serial over Bluetooth link (COM5)
USB-SERIAL CH340 (COM8)

/FIND THE COM PORT

In the cmd, run devmgmt.msc. This will open the Device Manager window.

Under Ports, look for: 'USB-SERIAL CH340 (COM#)' Take note of this number.

/INSTALL PYSERIAL

In the cmd, enter 'pip install pyserial'.

```
Collecting pyserial
  Using cached pyserial-3.5-py2.py3-none-any.whl (90 kB)
Installing collected packages: pyserial
Successfully installed pyserial-3.5
```

/FLASHING

/GET THE MAC ADDRESS

In cmd, run ‘python esptool.py --port COM# read_mac’
WRITE DOWN THE MAC ADDRESS.
You will need it later.

```
python esptool.py --port COM8 read_mac
esptool.py v4.6-dev
Serial port COM8
Connecting....
Detecting chip type... Unsupported detection protocol,
switching and trying again...
Connecting...
Detecting chip type... ESP8266
Chip is ESP8266EX
Features: WiFi
Crystal is 26MHz
MAC: c4:5b:be:e0:f5:68
Uploading stub...
Running stub...
Stub running...
MAC: c4:5b:be:e0:f5:68
Hard resetting via RTS pin...
```

/FLASHING

/ERASE THE FLASH

In cmd, run ‘python esptool.py --port COM# erase_flash’

```
python esptool.py --port COM8 erase_flash
esptool.py v4.6-dev
Serial port COM8
Connecting...
Detecting chip type... Unsupported detection protocol,
switching and trying again...
Connecting...
Detecting chip type... ESP8266
Chip is ESP8266EX
Features: WiFi
Crystal is 26MHz
MAC: c4:5b:be:e0:f5:68
Stub is already running. No upload is necessary.
Erasing flash (this may take a while)...
Chip erase completed successfully in 13.7s
Hard resetting via RTS pin...
```

/FLASHING

/FLASH TASMOTA FIRMWARE

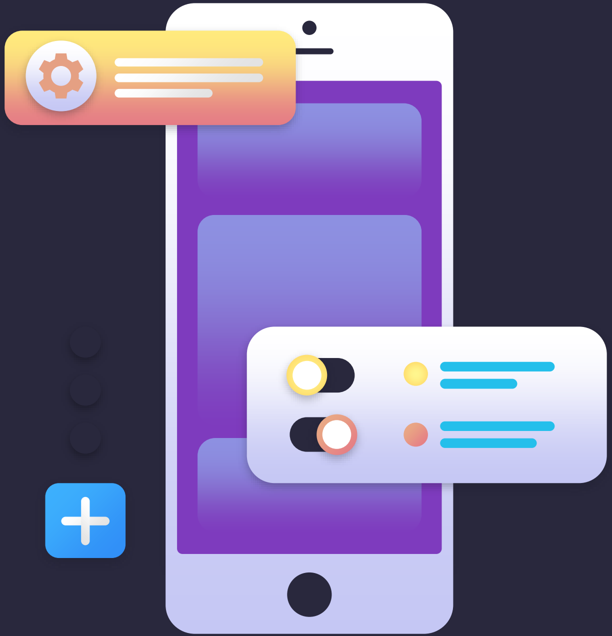
In cmd, run ‘python esptool.py --port COM# write_flash -fs 1MB -fm dout 0x0 tasmota.bin’

```
python esptool.py --port COM8 write_flash -fs 1MB -fm
dout 0x0 tasmota.bin
esptool.py v4.6-dev
Serial port COM8
Connecting...
Detecting chip type... Unsupported detection protocol,
switching and trying again...
Connecting...
Detecting chip type... ESP8266
Chip is ESP8266EX
Features: WiFi
Crystal is 26MHz
MAC: c4:5b:be:e0:f5:68
Stub is already running. No upload is necessary.
Configuring flash size...
Flash will be erased from 0x00000000 to 0x0009efff...
Compressed 647232 bytes to 461525...
Wrote 647232 bytes (461525 compressed) at 0x00000000 in
40.7 seconds (effective 127.1 kbit/s)...
Hash of data verified.

Leaving...
Hard resetting via RTS pin...
```

/REASSEMBLY & TESTING

/04

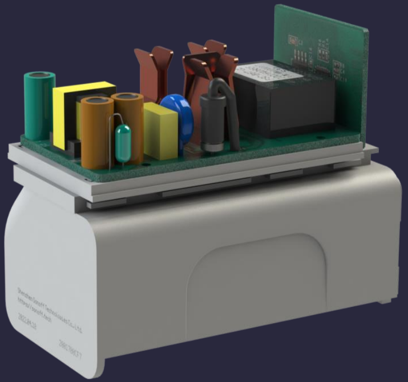


IEEE COMPUTER SOCIETY @USF

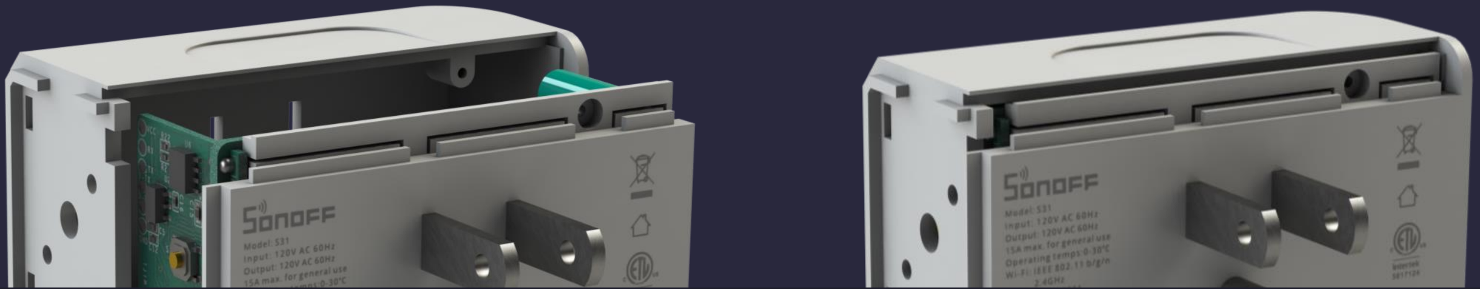
UNPLUG FTDI USB & DETACH HOOK CLIPS

Detach the wires from the S31.

Do not disconnect them from the FTDI converter yet!

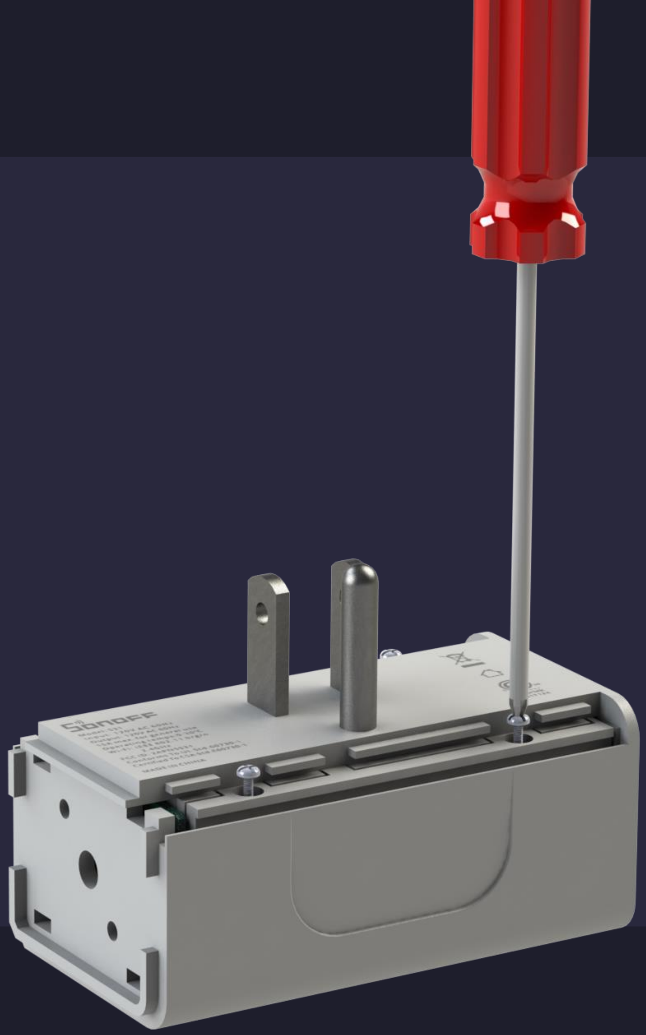


PLACE HOUSING BACK IN SHELL



REATTACH THE 3 SCREWS

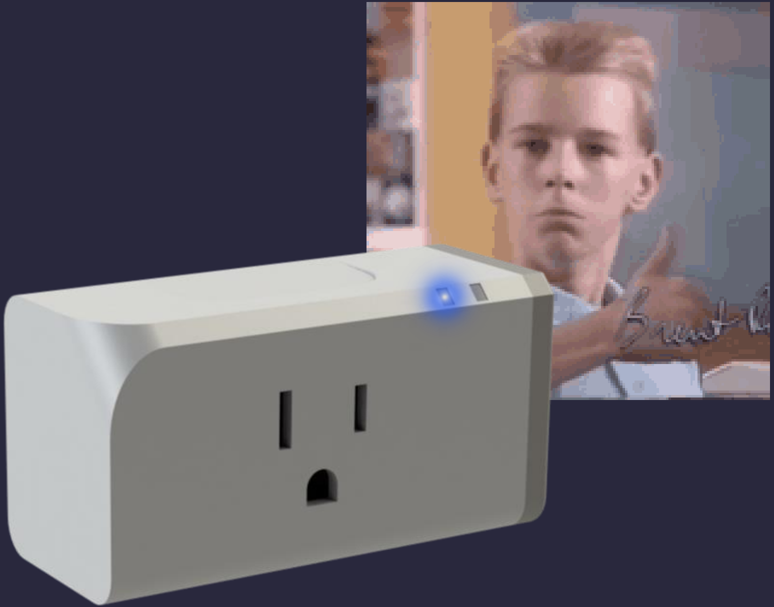
Place the device “face-down” to improve stability.
This will make it more likely that the screws go back in straight.



PLUG THE DEVICE INTO A NEARBY OUTLET.

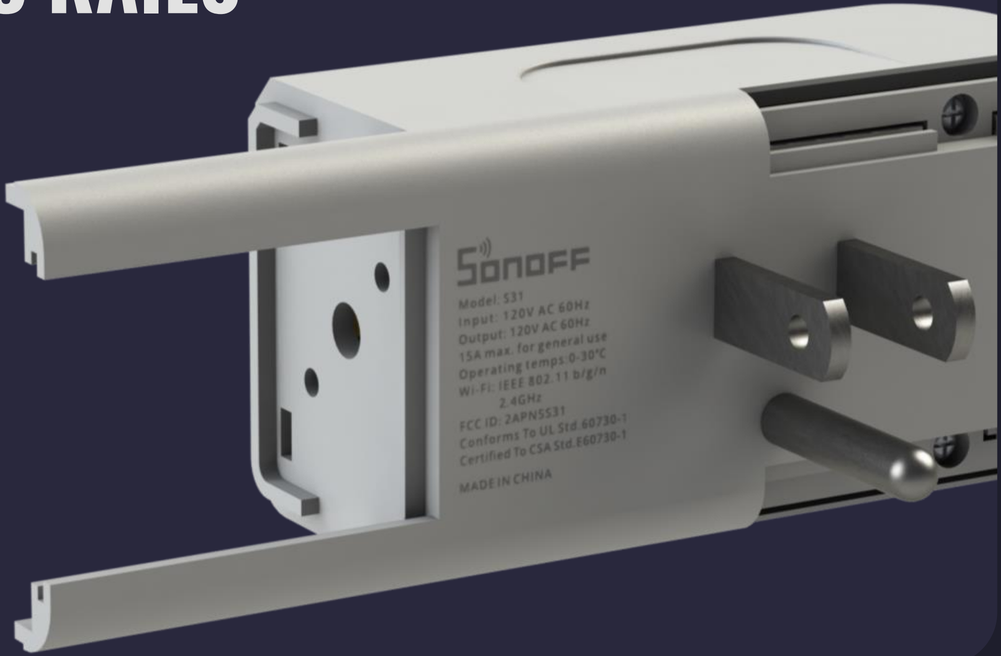
CHECK IF BLUE LIGHT IS BLINKING

If the blue light is blinking, the flash was successful. If not, please notify an IEEE-CS officer.



/SLIDE IN PLASTIC RAILS

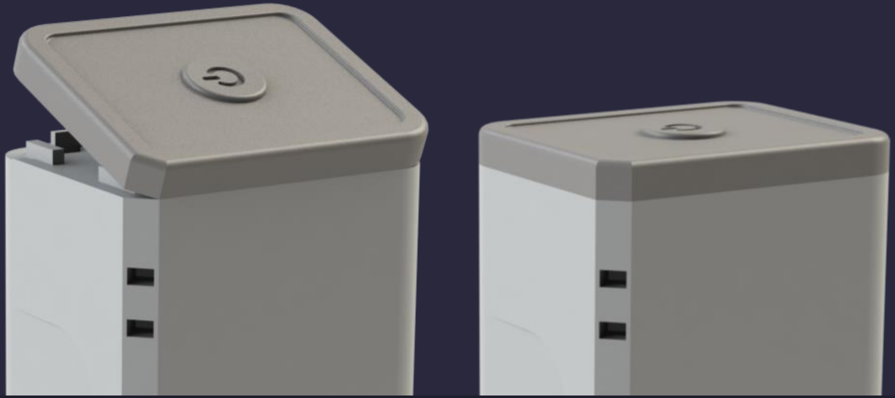
Both plastic rails should slide back in easily.



IEEE COMPUTER SOCIETY @USF

REATTACH THE GRAY CAP

Align be sure to align the notched edge.



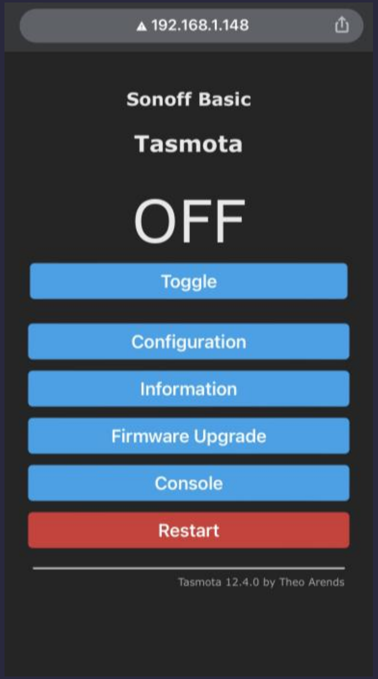
<PHONES>

We will be using our smart phones to connect to the device and the local network for the next steps.

CONNECT YOUR PHONE TO SSID:

tasmota-*MACLast6-####*

You should see this page ->



▲ 192.168.1.148

Sonoff Basic

Tasmota

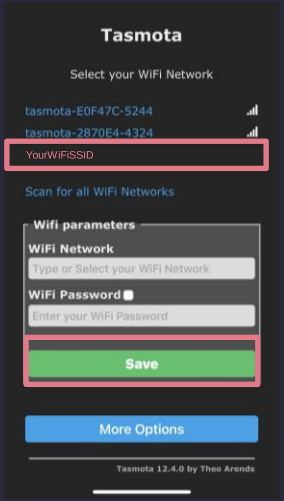
OFF

Tasmota 12.4.0 by Theo Arends

SELECT YOUR PERSONAL WIFI

Select your WiFi SSID.Then click ‘Save’.

Take note of the IP address, the page may reload soon!



Tasmota

Select your WiFi Network

tasmota-E0F47C-5244

tasmota-2870E4-4324

YourWiFiSSID

Scan for all WiFi Networks

Wifi parameters

WiFi Network

Type or Select your WiFi Network

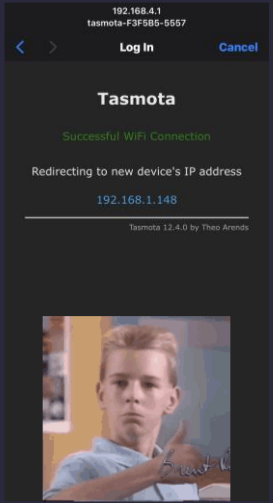
WiFi Password

Enter your WiFi Password

Save

More Options

Tasmota 12.4.0 by Theo Arends



192.168.4.1
tasmota-F3F5B5-5557

Log In Cancel

Tasmota

Successful WiFi Connection

Redirecting to new device's IP address

192.168.1.148

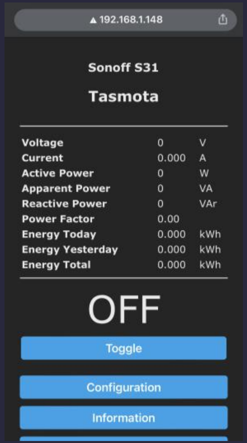
Tasmota 12.4.0 by Theo Arends

CONNECT YOUR PHONE TO YOUR PERSONAL WIFI

This may happen automatically
after the previous step.

ACCESS THIS WEB ADDRESS IN A MOBILE BROWSER:

192.168.1.*yourIPaddress*



▲192.168.1.148

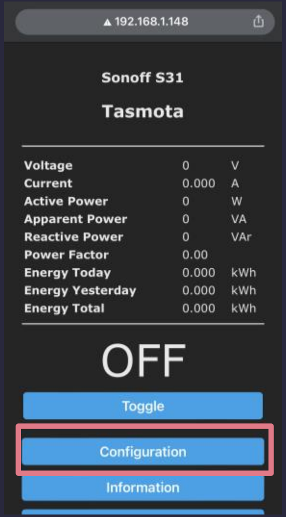
Sonoff S31

Tasmota

Voltage	0	V
Current	0.000	A
Active Power	0	W
Apparent Power	0	VA
Reactive Power	0	VAr
Power Factor	0.00	
Energy Today	0.000	kWh
Energy Yesterday	0.000	kWh
Energy Total	0.000	kWh

OFF

CHANGE DEVICE CONFIGURATION



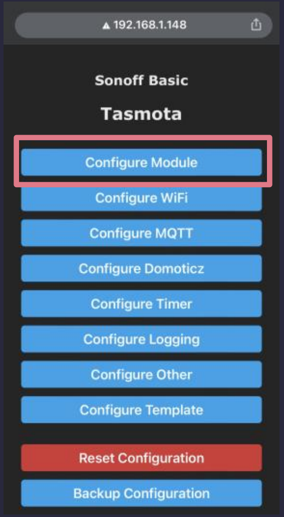
192.168.1.148

Sonoff S31

Tasmota

Voltage	0	V
Current	0.000	A
Active Power	0	W
Apparent Power	0	VA
Reactive Power	0	VAr
Power Factor	0.00	
Energy Today	0.000	kWh
Energy Yesterday	0.000	kWh
Energy Total	0.000	kWh

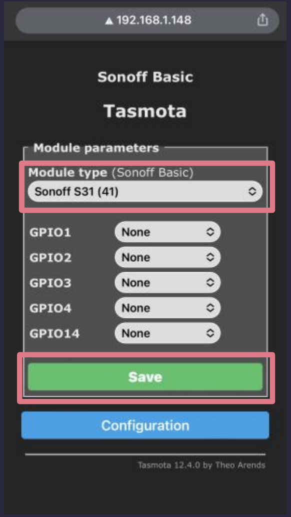
OFF



192.168.1.148

Sonoff Basic

Tasmota



192.168.1.148

Sonoff Basic

Tasmota

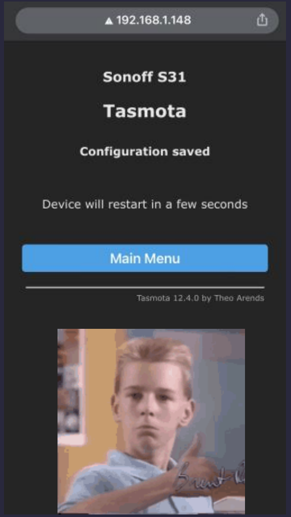
Module parameters

Module type (Sonoff Basic)

Sonoff S31 (41)

GPIO1	None
GPIO2	None
GPIO3	None
GPIO4	None
GPIO14	None

Tasmota 12.4.0 by Theo Arends



192.168.1.148

Sonoff S31

Tasmota

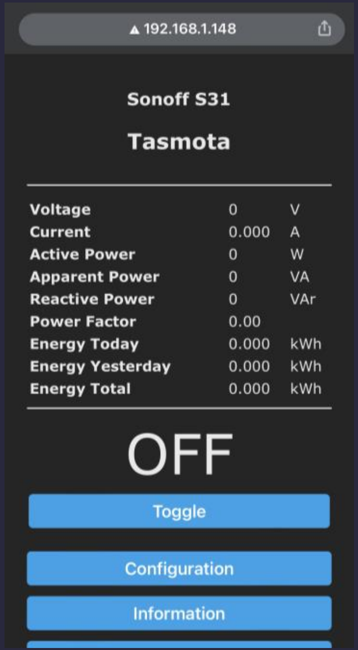
Configuration saved

Device will restart in a few seconds

Tasmota 12.4.0 by Theo Arends

EXPLORE YOUR HACKED SMART PLUG

Check out the interface!
Plug something in to observe
the energy monitoring!



192.168.1.148

Sonoff S31

Tasmota

Voltage	0	V
Current	0.000	A
Active Power	0	W
Apparent Power	0	VA
Reactive Power	0	VAr
Power Factor	0.00	
Energy Today	0.000	kWh
Energy Yesterday	0.000	kWh
Energy Total	0.000	kWh

OFF

Click storm

/THANKS!

/DO YOU HAVE ANY QUESTIONS?

myleskeller@usf.edu

@ieeecs_usf

IEEEComputerSocietyUSF