Stealing Credentials Using An ESP8266

-S Raghav Pillai

Disclaimer

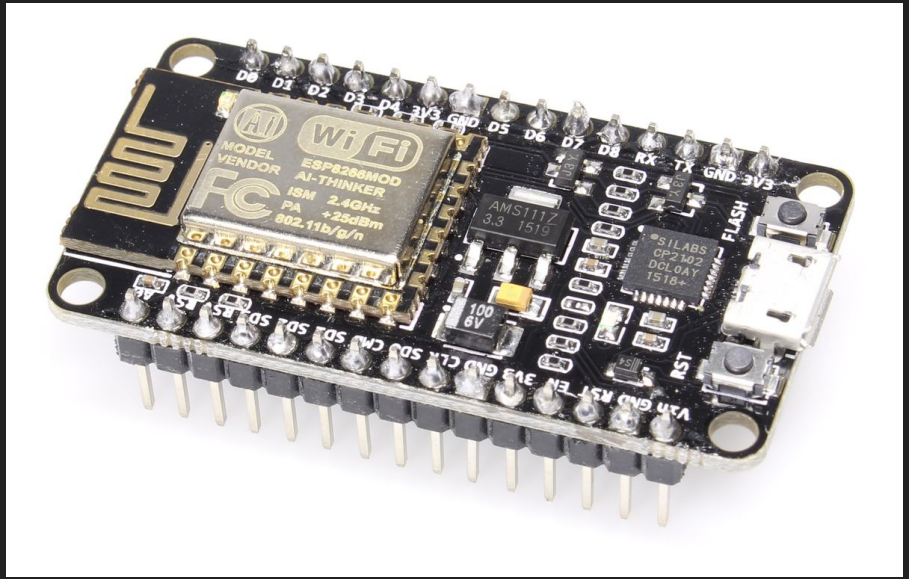
Whatever You learn and see here today is purely for educational purposes. The Author of this content is not liable in any way or form for any of the consequences!

What is a ESP2866?

ESP8266 is an Open source WIFI enabled SoC (System on Chip).

It is capable of receiving and transmitting data at a frequency of 2.4 GHz

(which is the standard frequency and is being replaced by 5 GHz)



What Makes it Special?

It Employs a 32-bit RISC CPU running at 80 MHz, which can be overclocked to 160 MHz.

It has a 64KB of Boot ROM

160 KB of Instruction + boot RAM

It has a lots of amazing features!

For a full list visit-
www.electronicwings.com/sensors-modules/esp8266-wifi-module

MicroPython

A minimal implementation of Python 3

Can be flashed and run on MicroControllers

It is compact enough to fit and run within just 256KB of code space and 16KB of RAM.

Flashing MicroPython - What you Need And How!

Flashing MicroPython - What you Need And How!

Flashing MicroPython - What you Need And How!

Firmware for ESP8266 boards

The following files are stable firmware for the ESP8266. Program your board using the esptool.py program as described in the tutorial.

- esp8266-20190125-v1.10.bin (elf, map) (latest)
- esp8266-20180511-v1.9.4.bin (elf, map)
- esp8266-20171101-v1.9.3.bin (elf, map)
- esp8266-20170823-v1.9.2.bin (elf, map)
- esp8266-20170612-v1.9.1.bin (elf, map)
- esp8266-20170526-v1.9.bin (elf, map)
- esp8266-20170108-v1.8.7.bin (elf, map)

You Can Find it At - micropython.org/download#esp8266

Flashing MicroPython - What you Need And How!

esptool.py

A Python-based, open source, platform independent, utility to communicate with the ROM bootloader in Espressif ESP8266 & ESP32 chips.

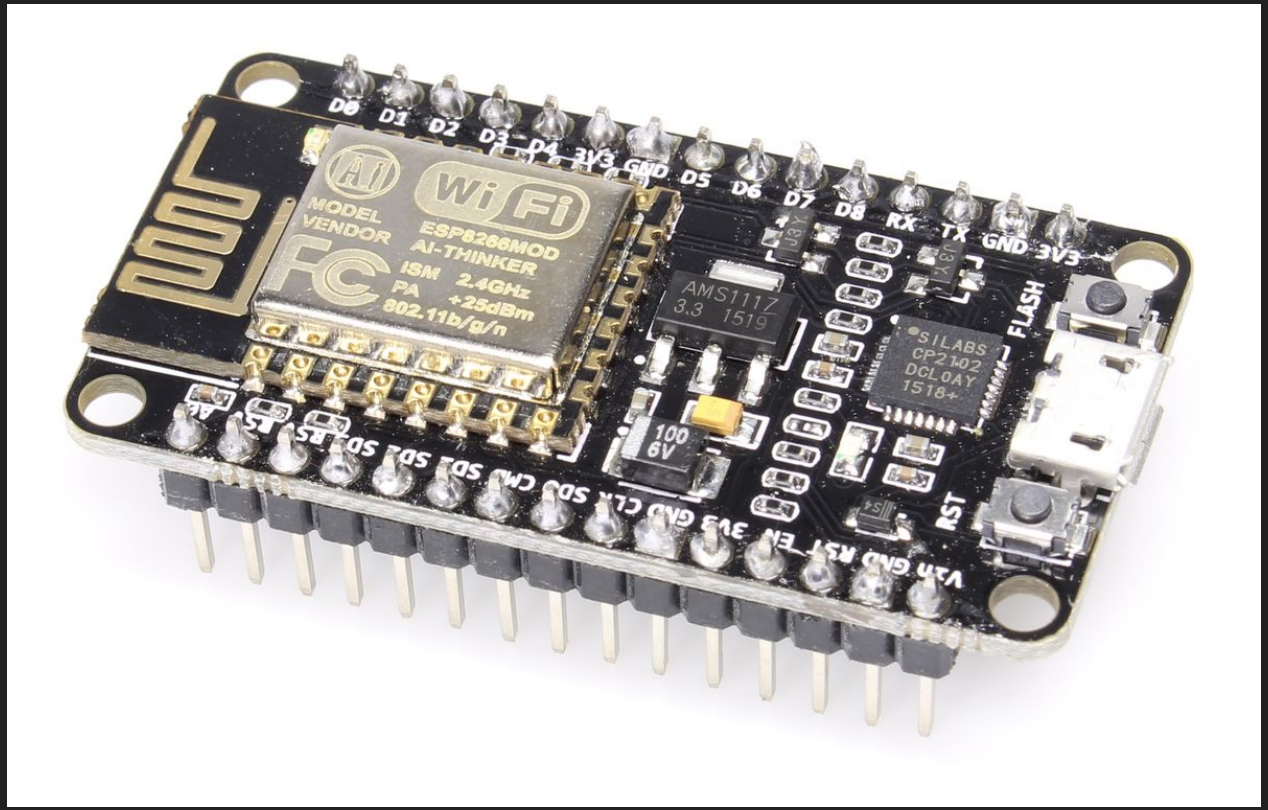
esptool.py was started by Fredrik Ahlberg (@themadinventor) as an unofficial community project. It is now also supported by Espressif. Current primary maintainer is Angus Gratton (@projectgus).

esptool.py is Free Software under a GPLv2 license.

build passing

You Can Find This At - github.com/espressif/esptool/

Flashing MicroPython - What you Need And How!



Flashing MicroPython - What you Need And How!

Step 1: Open up your Terminal and connect your ESP8266 to your device

Step 2: Make a note of the port its connected to (generally ‘/dev/ttyUSB0’ for linux and ‘COM0’ for Windows)

Step 3: Navigate to your directory with esptool.py and the flash file.

Step 4: Erase Flash!

Step 5: Flash MicroPython!

Flashing MicroPython - What you Need And How!

```
esptool.py --port /dev/ttyUSB0 erase_flash
```

This command will Clean out your ESP2866

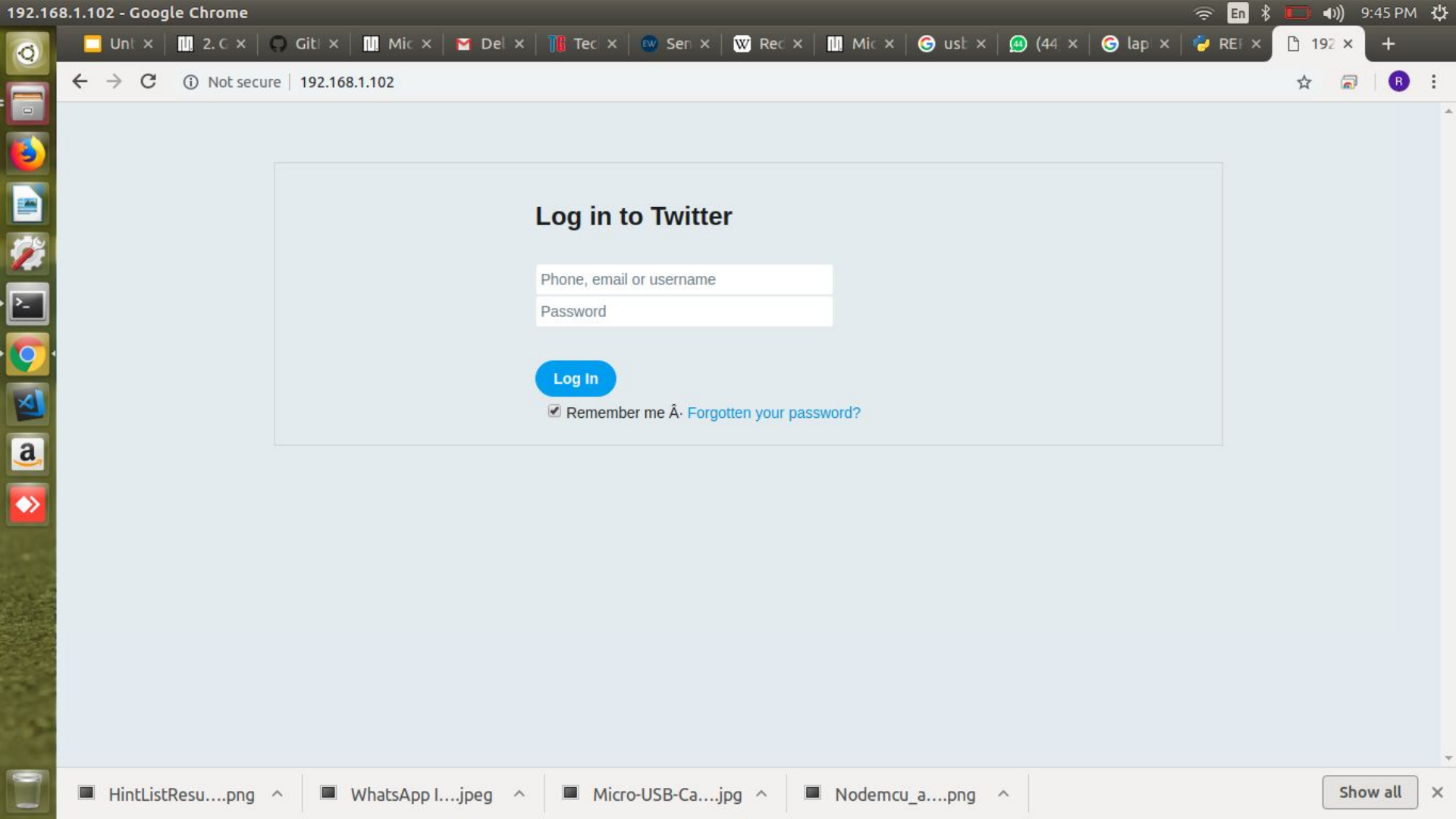
```
esptool.py --port <Port> --baud 115200 write_flash
--flash_size=detect 0 <File to Flash>
```

This Command will Flash the Firmware.

Lets Begin Coding!!

To Begin you need to access the REPL (Read, Eval, Print and Loop()) basically your Python shell!

$ Sudo screen <port> <Baudrate>


192.168.1.102 - Google Chrome
9:45 PM
Not secure
192.168.1.102
Log in to Twitter
Phone, email or username
Password
Log In
Remember me Â· Forgotten your password?
HintListResu....png
WhatsApp I....jpeg
Micro-USB-Ca....jpg
Nodemcu_a....png
Show all

```
"b'POST / HTTP/1.1\\r\\nHost: 192.168.1.102\\r\\nConnection: keep-alive
\\r\\nContent-Length: 38\\r\\nCache-Control: max-age=0\\r\\nOrigin: htt
p://192.168.1.102\\r\\nUpgrade-Insecure-Requests: 1\\r\\nContent-Type:
application/x-www-form-urlencoded\\r\\nUser-Agent: Mozilla/5.0 (X11; Li
nux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109
 Safari/537.36\\r\\nAccept: text/html,application/xhtml+xml,application
/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\\r\\nReferer: http://192.168
.1.102/\\r\\nAccept-Encoding: gzip, deflate\\r\\nAccept-Language: en-IN
,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\\r\\n\\r\\nusername=raghav&password=n
otmypassword'"
>>>
```

Thank You!