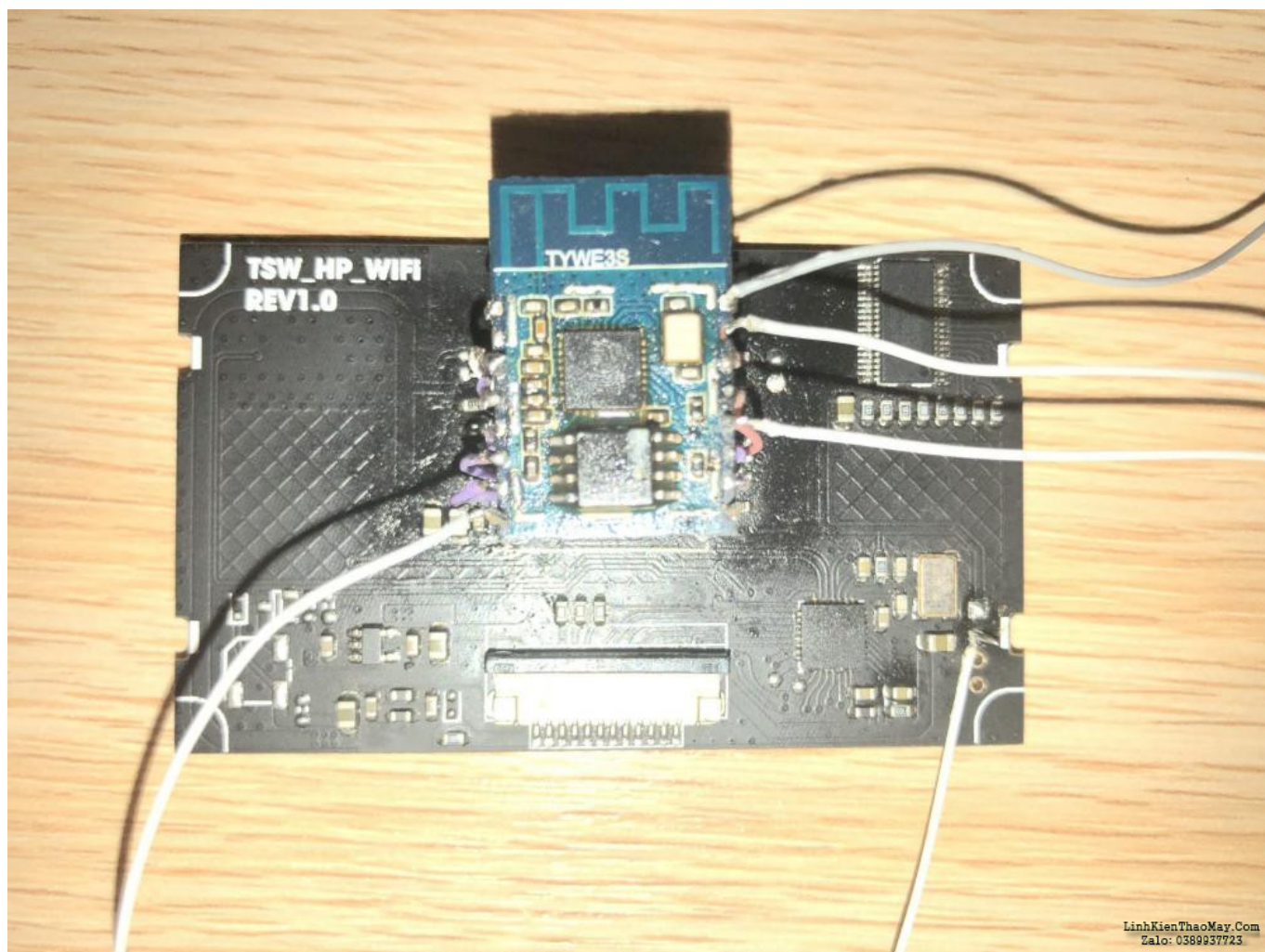


Bài viết hướng dẫn dump firmware công tắc wifi tuya với UART và áp dụng được cho các module esp8266, esp32. Phục vụ cho việc dịch ngược mã nguồn của các thiết bị smarthome tuya hoặc các sản phẩm dựa trên chip espxx.

Mạch PCB công tắc Tuya

Sau khi unbox công tắc ta sẽ tách được khối xử lý nguồn và khối mạch xử lý bao gồm PCB có đèn, nút công tắc, ... và module TYWE3S sử dụng chip esp8266.



Chuẩn Bị các Công Cụ

Mạch USB UART

Trên mỗi chip esp8266 được cài đặt chương trình bootloader cho phép dùng uart để truy cập vào.

Chương trình bootloader cho phép truy cập rất nhiều thông tin như thông tin chip, flash, read, write, ... Có quá trời chức năng cho bạn nghiên cứu.

mình sẽ lợi dụng tính năng read để dump firmware từ module ra.



ESP Tools

Công cụ esptool.py là công cụ được sử dụng rất nhiều để truy cập vào bootloader và thực hiện

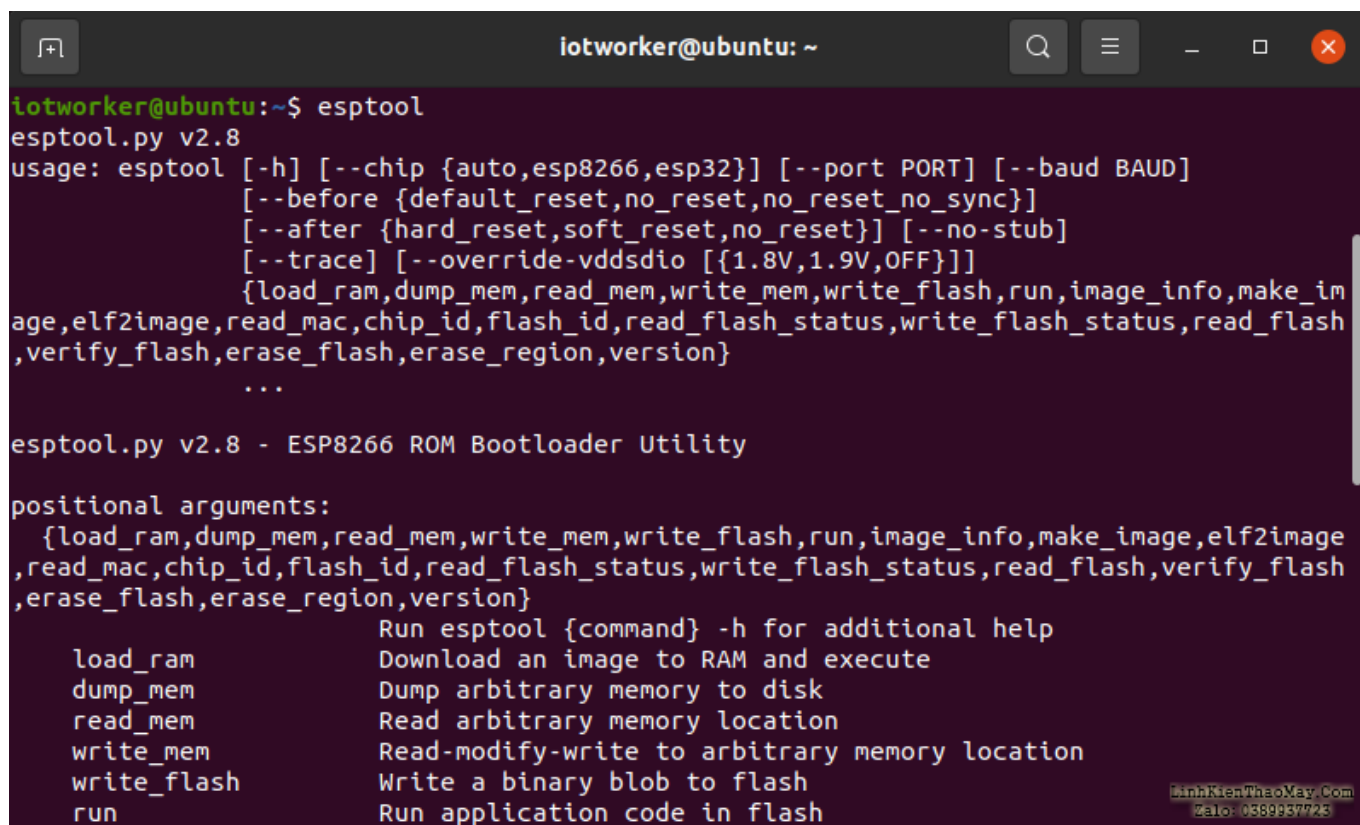
Tài liệu này được tải từ website: <http://linhkienthaomay.com>. Zalo hỗ trợ: 0389937723

các chức năng cần thiết như write chương trình vào flash sau mỗi lần bạn lập trình xong.

Do các bạn thường lập trình trên các IDE như Arduino, Eclipse, Visualcode nên không biết tới esptool vì sau khi các lập trình chương trình sẽ được build và upload chỉ bằng các kích chuột nên không biết tool esptool.py được các IDE gọi trong background các bạn không để ý.

Trên ubuntu bạn có thể dùng câu lệnh sau để cài đặt:

```
sudo apt-get install esptool
```



```
iotworker@ubuntu:~$ esptool
esptool.py v2.8
usage: esptool [-h] [--chip {auto,esp8266,esp32}] [--port PORT] [--baud BAUD]
               [--before {default_reset,no_reset,no_reset_no_sync}]
               [--after {hard_reset,soft_reset,no_reset}] [--no-stub]
               [--trace] [--override-vddsdio [{1.8V,1.9V,OFF}]]
               {load_ram,dump_mem,read_mem,write_mem,write_flash,run,image_info,make_image,elf2image,read_mac,chip_id,flash_id,read_flash_status,write_flash_status,read_flash,verify_flash,erase_flash,erase_region,version}
               ...

esptool.py v2.8 - ESP8266 ROM Bootloader Utility

positional arguments:
  {load_ram,dump_mem,read_mem,write_mem,write_flash,run,image_info,make_image,elf2image,read_mac,chip_id,flash_id,read_flash_status,write_flash_status,read_flash,verify_flash,erase_flash,erase_region,version}
                                Run esptool {command} -h for additional help
  load_ram                    Download an image to RAM and execute
  dump_mem                    Dump arbitrary memory to disk
  read_mem                    Read arbitrary memory location
  write_mem                   Read-modify-write to arbitrary memory location
  write_flash                  Write a binary blob to flash
  run                          Run application code in flash
```

Thực Hiện DUMP FIRMWARE

Xác định các chân của module



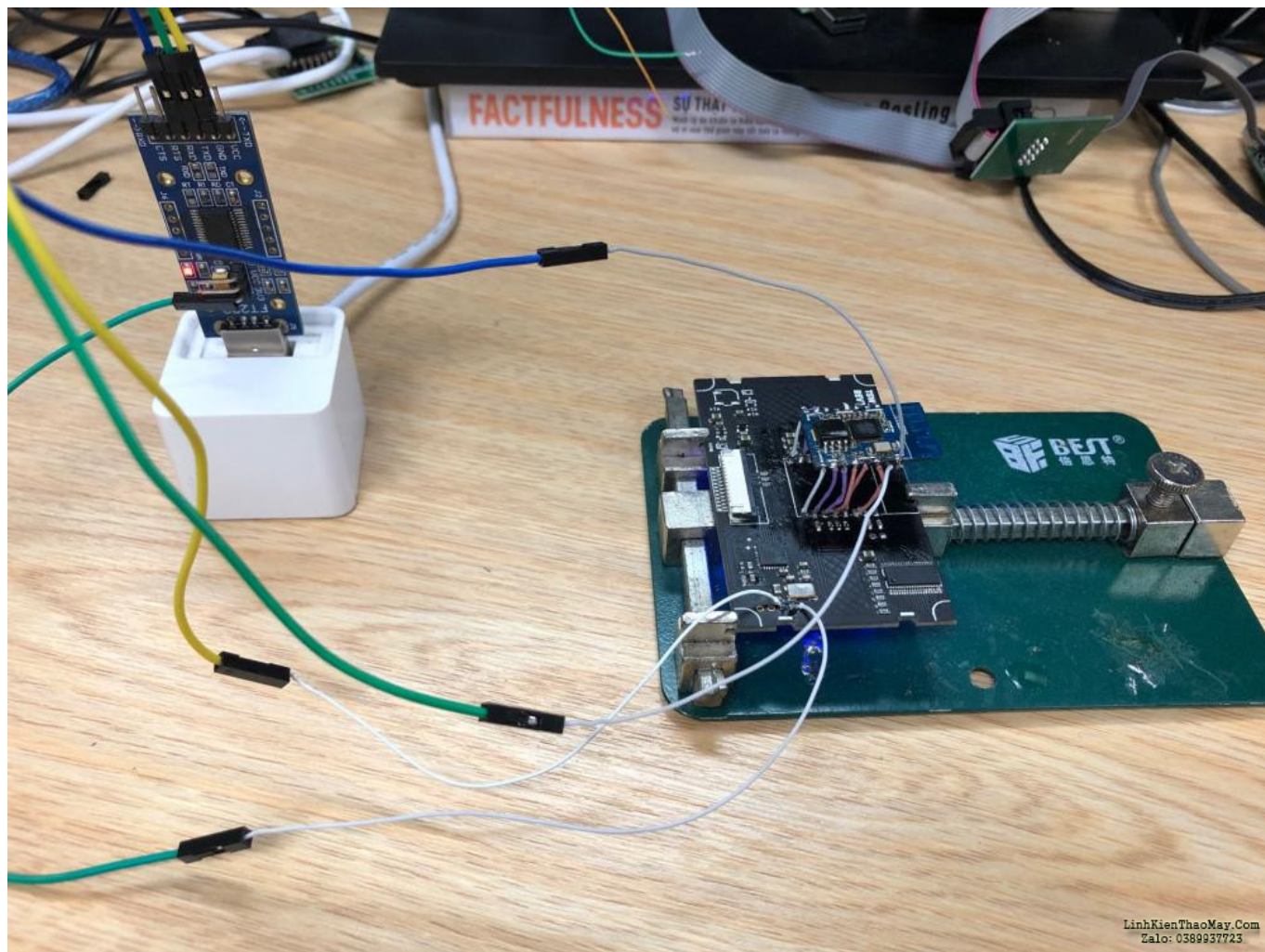
mình lấy ví dụ trên module TYWE3S có sơ đồ chân như sau:

Module TYWE3S đều sử dụng chip esp8266 việc dump trên các module có chip esp8266, esp32 là tương tự. Chỉ cần xác định đúng các PIN tín hiệu: RX, TX, GPIO0, GND, VCC.

Thực hiện đấu kết nối Module vs USB UART.

USB UART SERIAL Module ESP

TX	RX
RX	TX
GND	GPIO0
Vout 3.3(v)	Vin
GND	GND



Kết quả như sau:

Cơ Chế truy cập Bootloader

Để truy cập được vào bootloader bạn cần thực hiện các bước như sau:
mình lấy ví dụ đọc thông tin chip_id.

- Chạy tool `esptool.py --baudrate 9600 --port /dev/ttyUSB0 chip_id`
- Chân GPIO 0 phải được kéo xuống GND (khi boot chương trình sẽ sử dụng GPIO0 để active truy cập chế độ bootloader).
- Reset module esp (bạn có thể tự thiết kế nút reset hoặc đơn giản là ngắt nguồn và cấp nguồn lại).

```
lotworkers@ubuntu:~$ esptool --baud 9600 --port /dev/ttyUSB0 chip_id
esptool.py v2.8
Serial port /dev/ttyUSB0
Connecting.....
Detecting chip type... ESP8266
Chip is ESP8266EX
Features: WiFi
Crystal is 26MHz
MAC: bc:dd:c2:ec:1a:24
Enabling default SPI flash mode...
Chip ID: 0x66000024
Hard resetting via RTS pin...
```

LinhKienThaoMay.Com
Zalo: 0389937723

DUMP FRIMWARE

TRUNG TÂM SỬA CHỮA ĐIỆN TỬ QUẢNG BÌNH

MR. XÔ - 0901.679.359 - 80 Võ Thị Sáu, Phường Quảng Thuận, tx Ba Đồn, tỉnh Quảng Bình

GIÁ RẺ

NHANH CHÓNG

LINH KIỆN CHÍNH HÃNG



TRUNG TÂM SỬA CHỮA ĐIỆN TỬ XÔ NGUYỄN

- Dịch vụ sửa chữa điện tử tại nhà
- Cung cấp linh kiện điện tử
- Tư vấn lắp đặt nhà thông minh

Đc: Quảng Thuận, tx Ba Đồn,
tỉnh Quảng Bình - 0901.679.359

Lắp lại lần nữa với chức năng đọc bộ nhớ flash.

Chạy tool esptool.py --baudrate 9600 --port /dev/ttyUSB0 read_flash 0x000000 0x100000 fwbackup.bin

- 0x100000 tương đương với kích thước flash 1M để xem flash có kích thước bao nhiêu bạn lại sử dụng công cụ esptool hoặc tra mã ghi trên flash.

```
abcd@ubuntu:~/lotworks$ esptool.py --baud 9600 -p /dev/ttyUSB0 read_flash 0x000000 0x100000 fwbackup.bin
esptool.py v3.0
Serial port /dev/ttyUSB0
Connecting....
Detecting chip type... ESP8266
Chip is ESP8266EX
Features: WiFi
Crystal is 26MHz
MAC: bc:dd:c2:ec:1a:24
Uploading stub...
Running stub...
Stub running...
49152 (4 %)
811296 (29 %)
```

LinhKienThaoMay.Com
Zalo: 0389937723

Dịch ngược chương trình

Xin hẹn các bạn trong phần tiếp theo nhé!

Các bài viết tương tự:

1. [acnos SK419HDMI - bác có firmware v3.5 không.cho e xin với](#)
2. [Dai kin invecter 1chieu 12000. - Em có con điều hòa Daikin invecter 12000btu 1 chiều. Khi khiển đèn nguồn sáng khoảng 10 s là báo lỗi. Dàn lạnh, dàn nóng ko có động tĩnh j. Ấn nút tets ở mạch dàn nóng thì quạt và bloc chạy bt. Dàn lạnh vẫn báo loi. Thay mạch dàn nóng khác vào thì chạy bt. Có pro nào giúp em ca này với. Bác nào có mạch dàn nóng, lạnh daikin inverter 12000 1 chiều báo giá cho em với. Cả mạch sống và mạch chết. Lh. 0969.625.829](#)
3. [Dump Firmware Hikvision Camera với SPI Flash Hardware Protocol](#)
4. [ESP8266 điều khiển bật tắt 4 LED qua Webserver](#)
5. [Extract Firmware thiết bị TP-Link](#)
6. [Hệ thống nông nghiệp thông minh phiên bản ESP8266](#)
7. [Hướng dẫn Flash firmware Tasmota cho SONOFF một cách đơn giản nhất](#)
8. [Hướng dẫn làm mạch điều khiển các thiết bị điện trong gia đình bằng wifi \(ESP8266-01 + Atmega8\)](#)
9. [toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhưng khong ket noi dc voi may in va may tinh khong tim dc thiet bi - toi co may in canon2900 khi ket noi may tinh thi bao co nhan USnhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi B nhưng khong ket noi dc voi may in va may tinh khong tim dc thiet bi](#)
10. [tu lanh sanyo - tủ lạnh chạy bình thường...gas lên dàn nóng đều nhưng gas chỉ lên 1 co dàn lạnh đợi 20phut vẫn dấy. z là máy bị tuột bom hay bị nghẹt z các bạn??? với lại cho mình hỏi tủ lạnh chạy bao lâu thì gas lên đầy dàn???](#)
11. [tulanv vtb quá gio vn - tu bi thung dan nong,minh đa thay dan moi,khi bom ga thay dan nong, nong nua dan con nua dan ve phin kg nong.đau dan lanh co it tuyet bam.minh đa kiểm tra 2dan nonglanh thay kg bi tuc.](#)
12. [xin ý kiến góp ý từ dân thợ - em làm nghề dc 1 năm mà thấy mình sửa chữa lấy rẻ nghe người dân nghe loáng thoáng đến tai ko biết giá cả thực hư sửa chữa nên nào cho hợp với anh em dân thợ nhiều khi thay thế hư hỏng mất thời gian mà ko biết nên lấy nhiều sợ họ kêu đắt rẻ hỏi nào giờ sửa nói tiền ít ai kêu đắt.,](#)