Bài viết hướng dẫn sử dụng giao thức SPI để dump firmware của thiết bị Hikvision Camera, thuận lợi, áp lực phải đối mặt khi làm nhưng điều mới trái ngọt lần đầu tiên đã tới.

2019 mình có nhiệm vụ thực hiện đánh giá thiết bị IoT `Camera DS-2CD2T21G0` của hãng Hikvision. Lúc đó mình chỉ mới tập tô mảng IoT lúc đó chỉ biết reverse, exploit và dumpfirmware thông qua UART và còn nhiều thứ mới may mắn mình đã không chịu thua cố gắng tới bây giờ.

(UART là giao thức hardware cho phép truy cập ứng dụng thường là bootloader. Bootloader thường có một số chức năng như boot kernel, dumpfirmware, upload firmware, ...).

Phân Tích Hoàn Cảnh Sự Kiện 11/2019

Một điều kiện cần để tìm các lỗ hổng trên thiết bị là ban cần phải có phần sụn hay còn firmware.
Câu hỏi bạn đã biết bao nhiêu cách để dump firmware

- Lấy firmware từ nhà cung cấp.
- Dump firmware từ các chương trình bootloader.
- Dump firmware trực tiếp từ các chip nhớ thông qua các giao thức I2C, SPI.
- Lấy ứng dụng firmware từ các lỗ hổng cơ bản như LFI, Command, ...
- Dump firmware từ công cụ debug như JTAG, SWD, ...

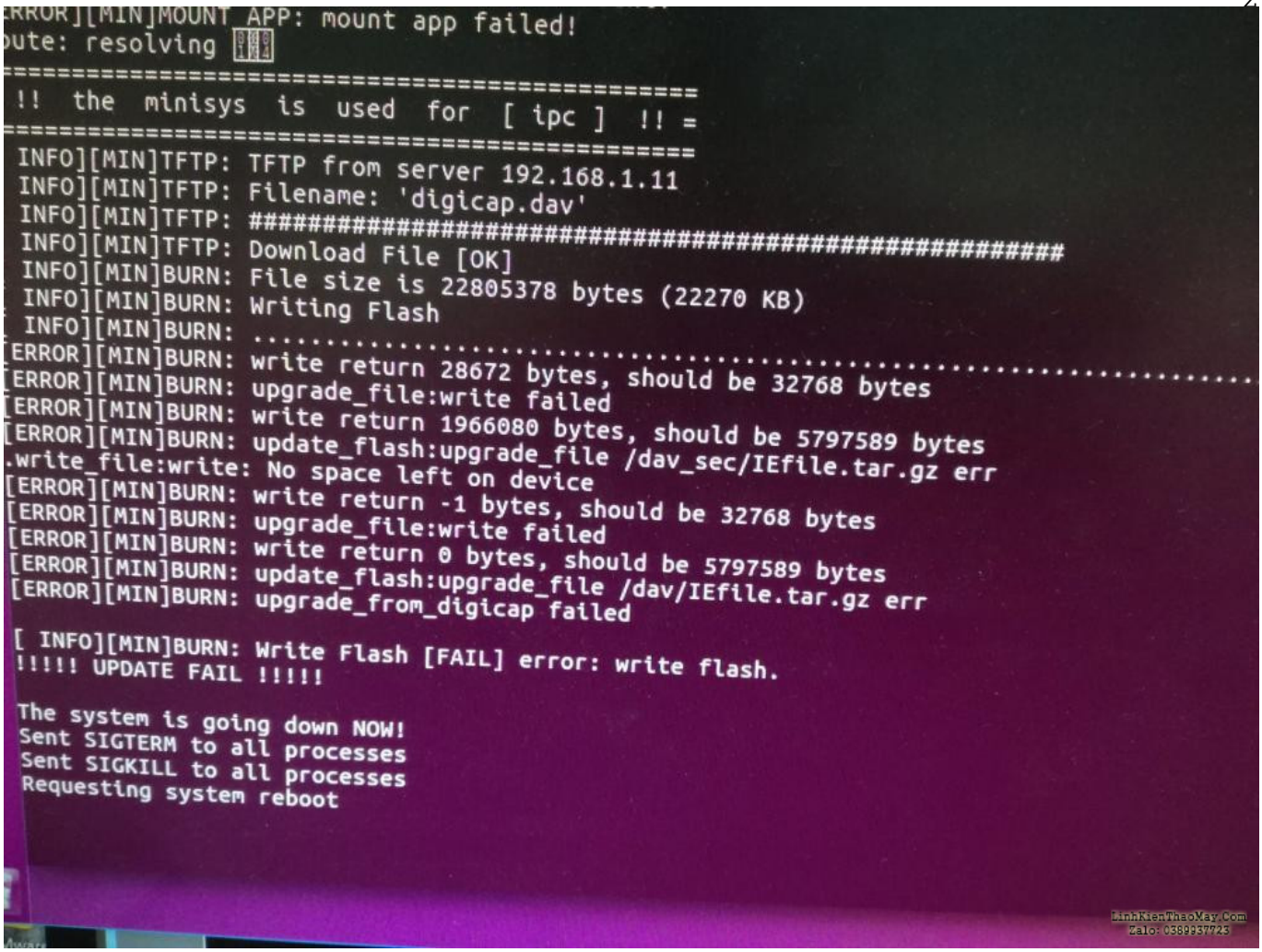
Phân Tích Dump Firmware

Cách lấy firmware	Trang Thái
Lấy firmware từ nhà cung cấp	Firmware đã bị mã hoá và không thể lấy được ứng dụng để tìm lỗ hổng
Dump firmware từ các trương trình bootloader (Uboot)	Các tính năng dump firmware hoặc bypass get root đều đã được fix
Lấy ứng dụng thông qua các lỗ hổng cơ bản	Không có phát hiện được những lỗ hổng web hoặc lỗ hổng đặc biệt khác
Dumpfirmware từ các công cụ debug	Hikvision sử dụng chip được phối hợp nhà cung cấp khác và đã xoá các thông tin và không xác định được tên fccid chip dẫn tới việc không xác định được các có tồn tại debug và nếu có thì ở chỗ nào
Dummp Firmware trực tiếp từ các giao thức SPI, I2C	Việc dump firmware là hoàn toàn được thiết bị sử dụng flash rời

Thử Các Giả Định

- Trong Uboot có tính năng run một subsystem (yêu cầu biết build version để có thể tạo đk subsystem) do không biết nên mình tử một số subsystem nhưng đều thất bại.

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



- mình có tìm kiếm được một số password default để truy cập ssh và qua boot serial`root/hiklinux or root/your_admin_password, root/12345 admin/12345 and oddly, in Hikvision CN firmware root/duhao ToCOv8qxP13qs:hiklinux`Kết quả cũng là thất bại.
- mình có tìm được một số cách bypass vào root bằng cách sử đổi biến môi trường vào phía cuối `bootargs` ví dụ như `bootargs=init=/bin/sh`. Lỗ này đã được fix và không thể sửa đổi thông qua serial. (Các bạn gim cái này tý nữa sẽ sử dụng tới ở phần kế tiếp).
  --> Một lần nữa lại thất bại
- mình tìm được một số tool decrypt một phần firmware được sử dụng để thây đổi ngôn ngữ nhưng nó không hỗ trợ cho firmware của mình `hikpack`.
- mình ra các lỗ hổng web trên cổng website nhưng không có kết quả gì.

Đâu đó đã một tháng trôi qua và báo cáo bằng miệng của mình có rất nhiều chữ nhưng.

Kết Luận

- mình sẽ tận dụng việc read, write trực tiếp từ flash thông qua giao tiếp phần cứng SPI.
- Chỉnh sửa biến môi trường.
- Một thông tin hữu ích thu thập được là thông tin partition trên flash.

```
[ 1.612980] nand: Winbond W25N01GV
```

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

```
[ 1.616460] nand: 128MiB, SLC, page size: 2048
[ 1.620901] Nand(Auto): OOB:64B ECC:4bit/512
[ 1.625111] nand: ECC provided by Flash Memory Controller
[ 1.630824] Creating 14 MTD partitions on "hinand":
[ 1.635761] 0x000000000000-0x000000100000 : "bld"
[ 1.642993] 0x000000100000-0x000000180000 : "env"
[ 1.649935] 0x000000180000-0x000000200000 : "enc"
[ 1.657018] 0x000000200000-0x000000280000 : "sysflg"
[ 1.664148] 0x000000280000-0x000000380000 : "dpt"
[ 1.671242] 0x000000380000-0x000000b80000 : "rcvy"
[ 1.681896] 0x000000b80000-0x000001380000 : "sys0"
[ 1.692478] 0x000001380000-0x000001b80000 : "sys1"
[ 1.703118] 0x000001b80000-0x000003d80000 : "app0"
[ 1.727432] 0x000003d80000-0x000005f80000 : "app1"
[ 1.752781] 0x000005f80000-0x000006580000 : "cfg0"
[ 1.764507] 0x000006580000-0x000006b80000 : "cfg1"
[ 1.775091] 0x000006b80000-0x000007780000 : "syslog"
[ 1.788864] 0x000007780000-0x000007f80000 : "resv"
```

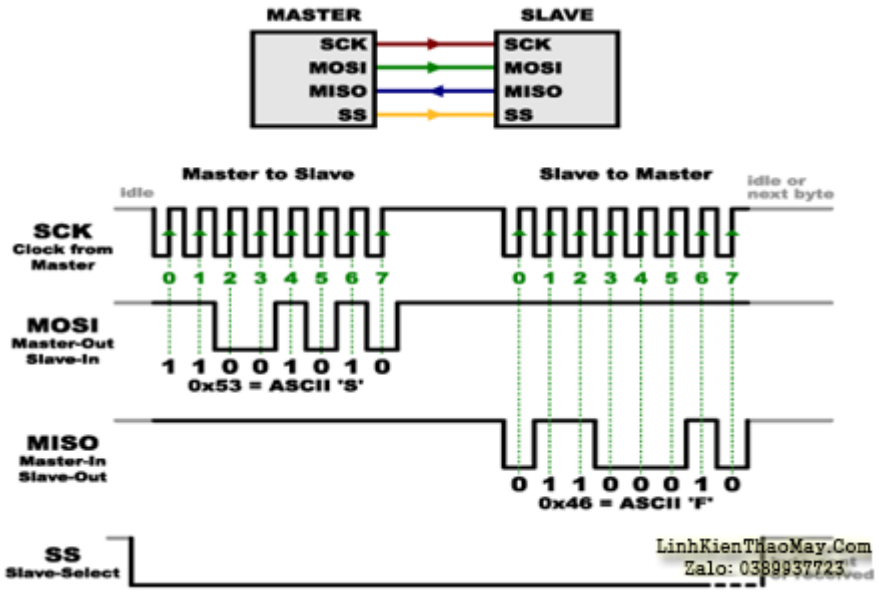
- Ý Tưởng
  - Ghi đè phân vùng `env` với `/bin/sh` để có thể truy cập System OS.
  - Reverse Bootloader `bld` để tìm secret key để decrypt Firmware.

SPI Flash

Tên FCCID flash mình là : W25N01GV theo thông tin gg được là CHIP Flash giao tiếp theo chuẩn SPI và mình biết có công tụ dump firmware là flashrom.
Lúc này mình sẽ tìm hiểu về giao thức SPI về nguyên lý và cách đấu nối.

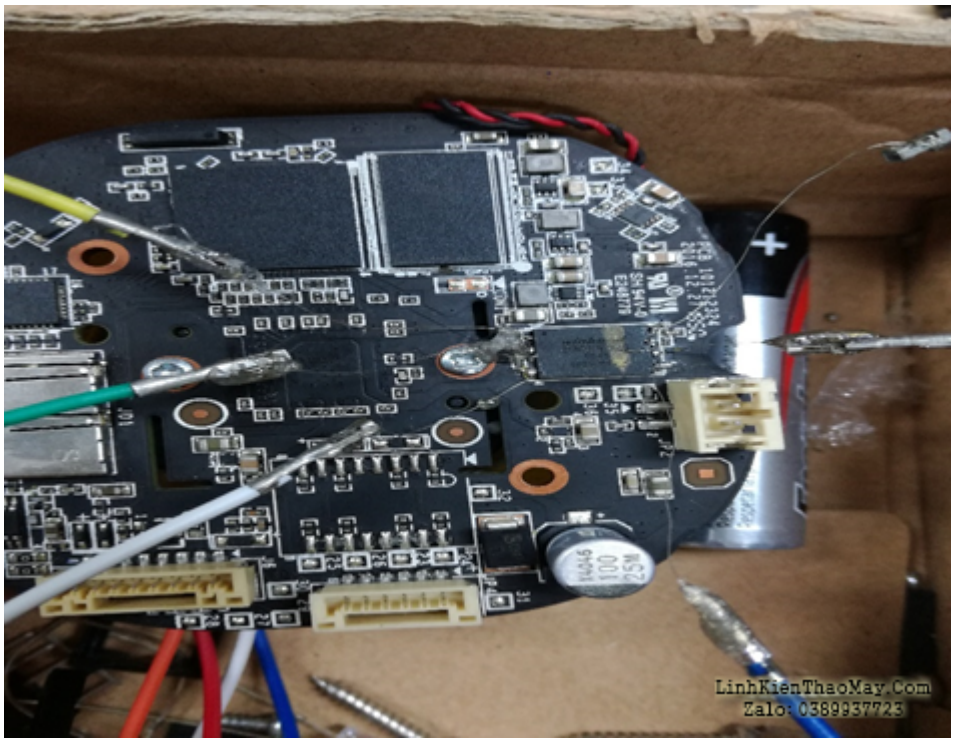
Nguyên lý SPI và Cách Đấu Nối Chân

Bạn tham khảo thông tin nguyên lý và cách đấu nối đây nhé



Ra Chân CHIP Flash

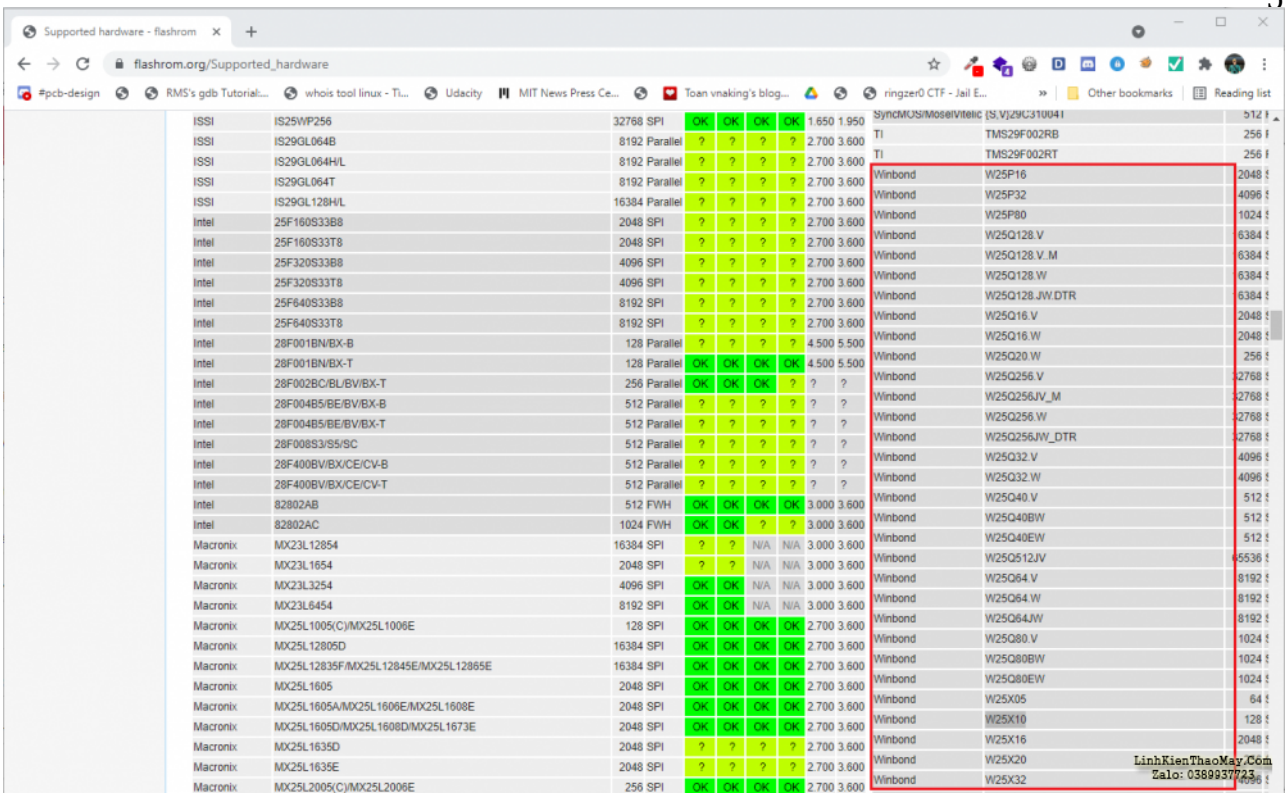
- Việc tiếp theo mình cần phải ra chân bao gồm: SCK, MOSI, MISO,SS
  Vì chip sử dụng chân ngầm nên việc injection là hơi tốn sức sử dụng dây mỏng.



- Thực hiện kết nối SPI với thiết bị PI3
  Mạch định PI disable SPI cần vào `raspi-config` enable SPI protocol.

Flashrom

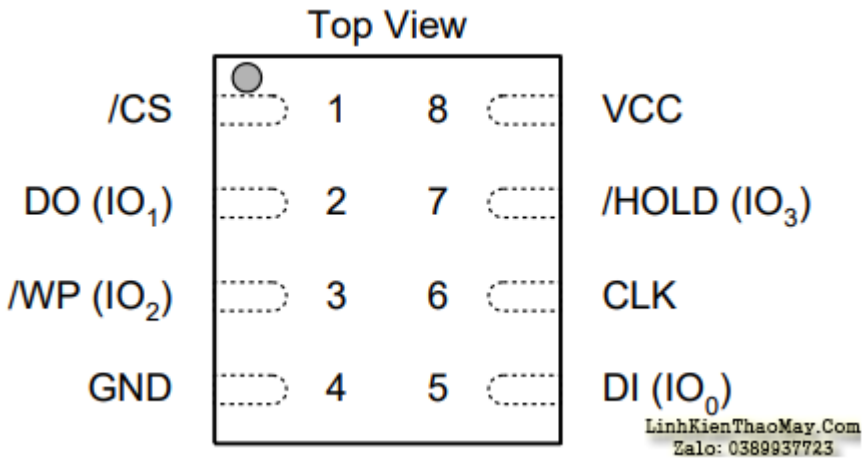
- Cài đặt `flashrom` xem hướng dẫn tại đây
- Nếu bạn không biết tên chip flash của mình cung cụ sẽ tự động detect bằng việc lấy `Manufacturer Id` thông qua SPI rồi so khớp trong CSDL của flashrom.
- Sử dụng command sau để hiểu hơn
  `Flashrom –p linux_spi:dev=/dev/spidev0.0,spispeed=[speed][k|m] –V`
- Lại một lần nữa rất tiếc công cụ chưa hỗ trợ `flash` của mình `Winbond W25N01GV`. Công cụ được tích hợp sử dụng vào thiết bị Attify Badge với giá 44$.
- Bạn có thể kiểm tra các loại `flash` mà flashrom hỗ trợ.



Cấu Tạo Flash

Bài viết thực hiện trên `flash W25N01GV 128M` có datasheet
Các bạn cũng có thể thực hành và áp dụng tương tự với những loại flash khác.

Sơ đồ PAD WSON 8×6-mm



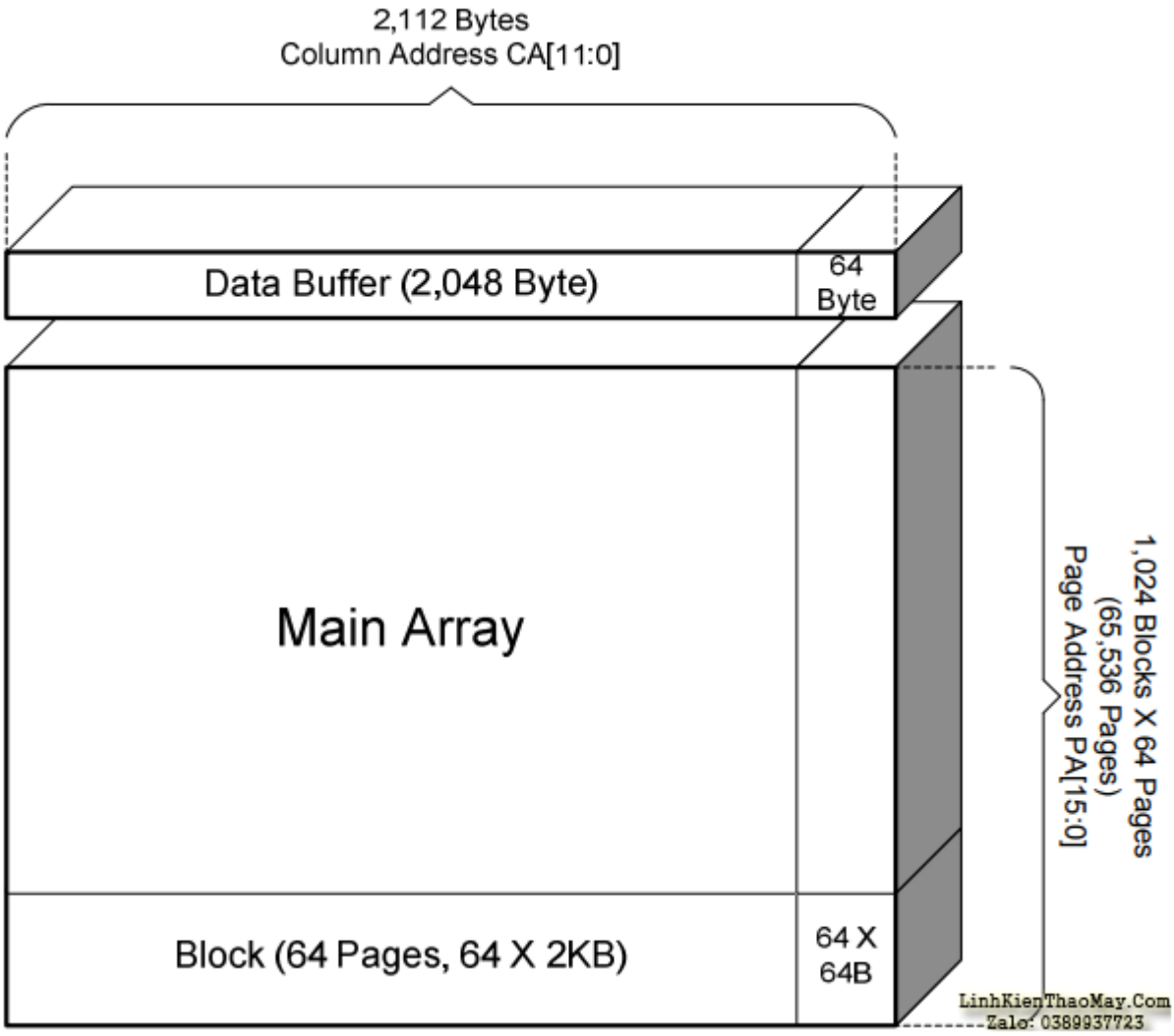
Kiến Trúc Flash Memory và Address

Bộ nhớ Flash W25N01GV chia làm các đơn vị nhỏ như pages, blocks.

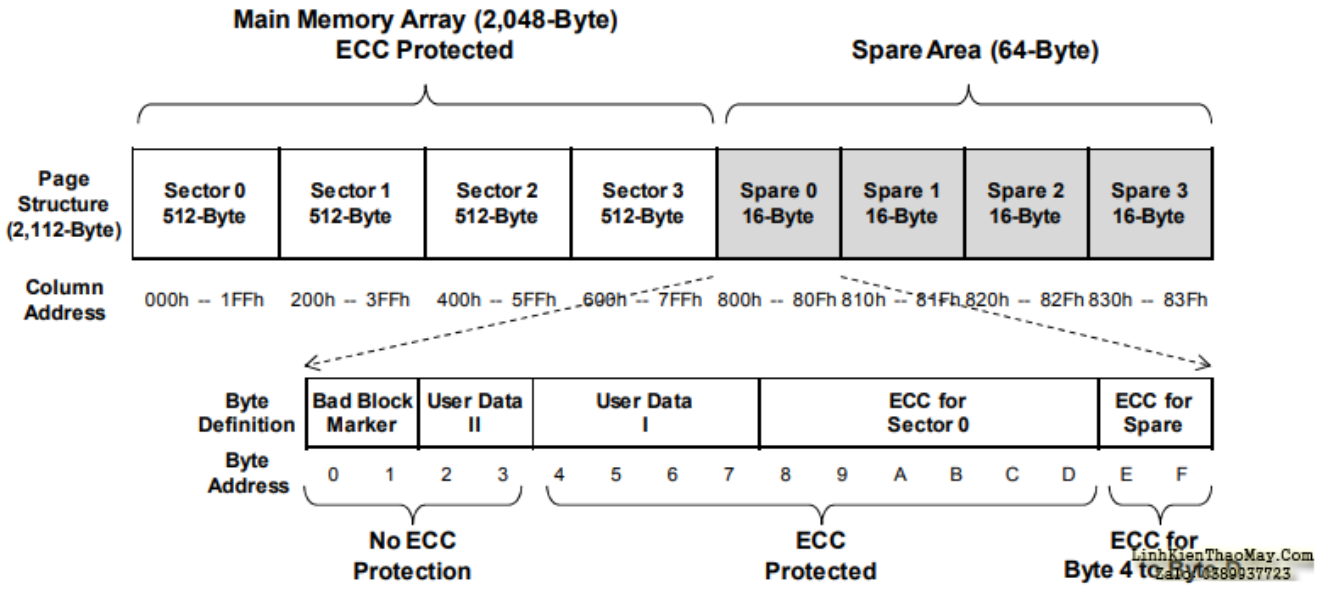
- 1024 Blocks: Mỗi Block có 64 pages.
- 65,536 Pages:
  - Mỗi Pages có 2048 byte

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

    - Mỗi page có thêm 64 byte SpareArea
- Tổng dung lượng: 65536 * 2KB = 128M



- Cấu tạo Page
    - 4 sector mỗi sector là 512 byte
    - 4 spare mỗi space là 16 byte và đại diện cho 4 sector. ECC được xây dựng trên thuật toán để bảo toàn tính toàn vẹn của các sector. Trong quá trình đọc ghi dữ liệu, ECC engine sẽ xác minh data đọc ghi thông qua các bít trạng thái ECC



Manufacturer ID và Device Identification

Các hãng sẽ phân loại với nhau bằng `Manufacturer ID`. Các chip cùng một hãng phân loại với nhau bằng `Device ID`.

MANUFACTURER ID	**(MF7 - MF0)**
Winbond Serial Flash	EFh
Device ID	**(ID15 - ID0)**
W25N01GV	AA21h

LinhKienThaoMay.Com
Zalo: 0389937723

Bảng Tập Lệnh (Instrution Set Table)

Mỗi hãng sẽ quy định các tập lệnh riêng đối với thiết bị.

Commands	OpCode	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7	Byte8	Byte9
Device RESET	FFh								
JEDEC ID	9Fh	Dummy	EFh	AAh	21h				
Read Status Register	0Fh / 05h	SR Addr	S7-0	S7-0	S7-0	S7-0	S7-0	S7-0	S7-0
Write Status Register	1Fh / 01h	SR Addr	S7-0						
Write Enable	06h								
Write Disable	04h								
BB Management (Swap Blocks)	A1h	LBA	LBA	PBA	PBA				
Read BBM LUT	A5h	Dummy	LBA0	LBA0	PBA0	PBA0	LBA1	LBA1	PBA1
Last ECC failure Page Address	A9h	Dummy	PA15-8	PA7-0					
Block Erase	D8h	Dummy	PA15-8	PA7-0					
Program Data Load (Reset Buffer)	02h	CA15-8	CA7-0	Data-0	Data-1	Data-2	Data-3	Data-4	Data-5
Random Program Data Load	84h	CA15-8	CA7-0	Data-0	Data-1	Data-2	Data-3	Data-4	Data-5
Quad Program Data Load (Reset Buffer)	32h	CA15-8	CA7-0	Data-0 / 4	Data-1 / 4	Data-2 / 4	Data-3 / 4	Data-4 / 4	Data-5 / 4
Random Quad Program Data Load	34h	CA15-8	CA7-0	Data-0 / 4	Data-1 / 4	Data-2 / 4	Data-3 / 4	Data-4 / 4	Data-5 / 4
Program Execute	10h	Dummy	PA15-8	PA7-0					
Page Data Read	13h	Dummy	PA15-8	PA7-0					
Read	03h	CA15-8	CA7-0	Dummy	D7-0	D7-0	D7-0	D7-0	D7-0
Fast Read	0Bh	CA15-8	CA7-0	Dummy	D7-0	D7-0	D7-0	D7-0	

LinhKienThaoMay.Com
Zalo: 0389937723

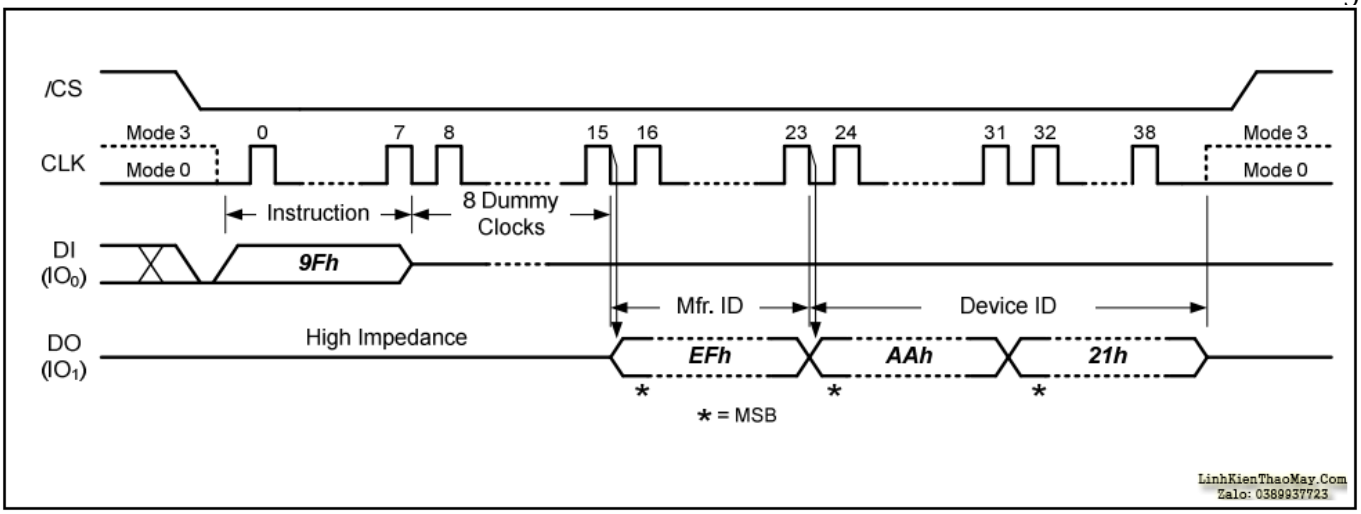
Read JEDEC ID (0x9F) Example

Các bạn cần xác định 2 tham số: command và độ dài Response

- Command: 0x9F
- BUF length: 2 Byte

Để gửi dữ liệu qua SPI

- Chân CS thiết lập trạng thái low
- Chân ID gửi đi dữ liệu 0x9F dưới dạng bit
- Chân DO nhận 2 byte Device ID dưới dạng bit
- CLK đồng bộ với xung của các bít



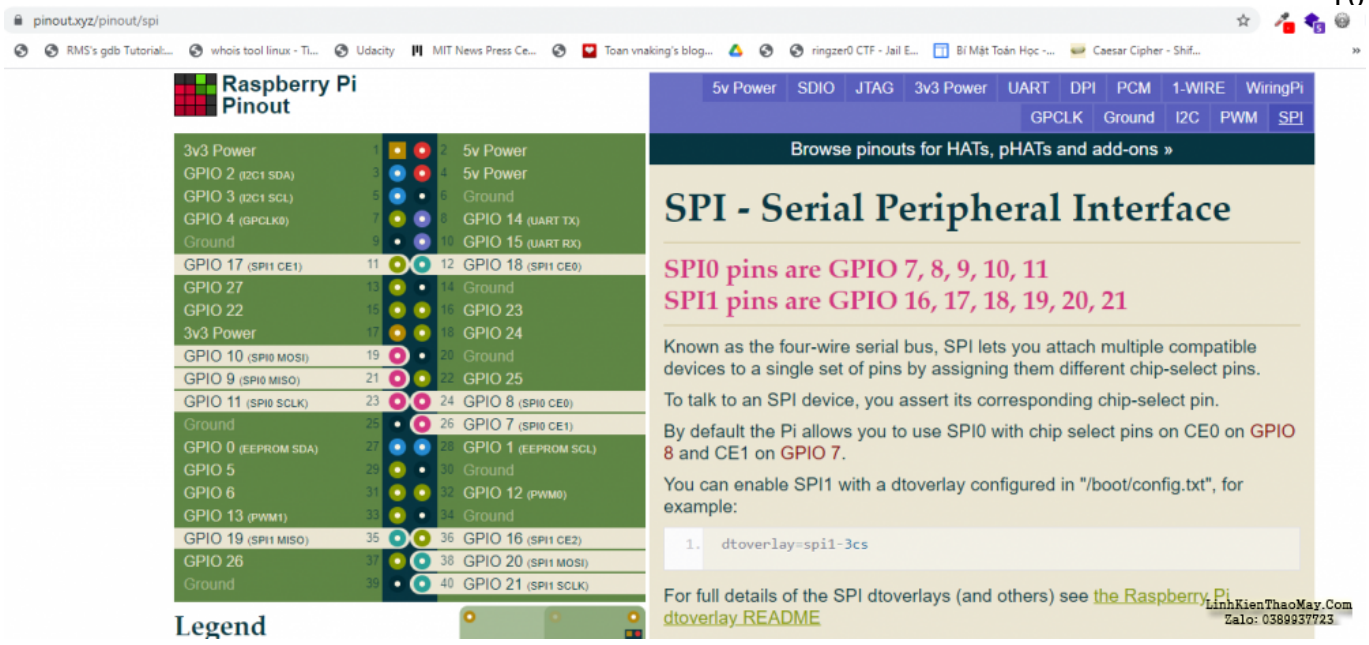
Lý thuyết là vậy hiện tại đã có thư viện hỗ trợ hết rồi rất đơn giản với `wringPi`. Truy cập trang [web để](#) hiểu hơn các hàm API hỗ trợ SPI trên PI.

```
/*
Run command đ load dirver và c p phát bộ đệm lớn hơn 4KB n u c n
gpio load spi
gpio load spi 100
*/
#include <wiringPiSPI.h>

int main(){
    char buf[3];
    wiringPiSPISetup(0, 10000000); // Theo datashet đạt được 50MB/s

    buf[0] = 0x9F // 2 byte còn lại đ chứa device ID
    wiringPiSPIDataRW(0, buf, 3);
    printf("Device ID: %X %X", buf[1], buf[2]);
    return 0;
}
```

Rasberry có 2 kênh SPI `/dev/spidev0.0` and `/dev/spidev0.1` tham khảo các pin tại trang pinout.xyz



- Ngoài ra Flash có vài tính năng quản lý như đánh dấu các page lỗi thông qua table BBM LUT

Kết Quả

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

Sử dụng các tập lệnh mình dump được flash `HIK_Winbond_W25.flash`. Khá vui mừng `strings HIK_Winbond_W25.flash | grep key` ra được một số kết quả tích cực

```
%s,%d: Hmac key initial failed!
%s,%d: hash i_key_pad and message start failed!
%s,%d: hash i_key_pad and message update failed!
%s,%d: Hash Final i_key_pad+message failure, ret=%d
,%d: Hash Init o_key_pad+hash_sum_1 failure, ret=%d
%s,%d: Hash Update o_key_pad failure, ret=%d
%s,%d: Hash Final o_key_pad+hash_sum_1 failure, ret=%d
```

```
%s,%d: RSA padding mode error, mode = 0x%x. public key encryption operation, the block type shall be 02.
%s,%d: For a private key decryption operation, the block type shall be 02.
%s,%d: key is null.
%s,%d: For a private- key encryption operation, the block type shall be 00 or 01.
%s,%d: For a public key decryption operation, the block type shall be 00 or 01
```

Hiện các bạn trong phẩn tiếp theo

Các bài viết tương tự:

1. [Phần 2] Sử dụng công cụ Binwalk để phân tích Firmware
2. acnos SK419HDMI – bác có firmware v3.5 không.cho e xin với
3. Chia sẻ Firmware Trạm hàn (mỏ hàn có bộ điều khiển nhiệt độ)
4. Dịch ngược camera yoosee xem có gì =))
5. Extract Firmware thiết bị TP-Link
6. Hướng dẫn dump firmware ESP8266, ESP32 với UART
7. Hướng dẫn Flash firmware Tasmota cho SONOFF một cách đơn giản nhất
8. Mạch nạp ST-Link V2 mini bản clone, lỡ tay nâng cấp firmware
9. Máy chích cá – Có bạn nào trong diễn đàn pro máy chích cá ko chỉ mình với , hôm trước mình thấy 1máy chích cá dùng sò b688 nhưng có mạch dao động dùng 2con d880 với mấy con điện trở và tụ nữa bạn nào biết mạch này thì chỉ mình với
10. Nâng cấp bộ nhớ Flash cho TL-WR841N v8
11. Thử bruteforce camera China và cái kết :D
12. 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 nhung 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 nhung khong ket noi dc voi may in va may tinh khong tim dc thiet bi

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