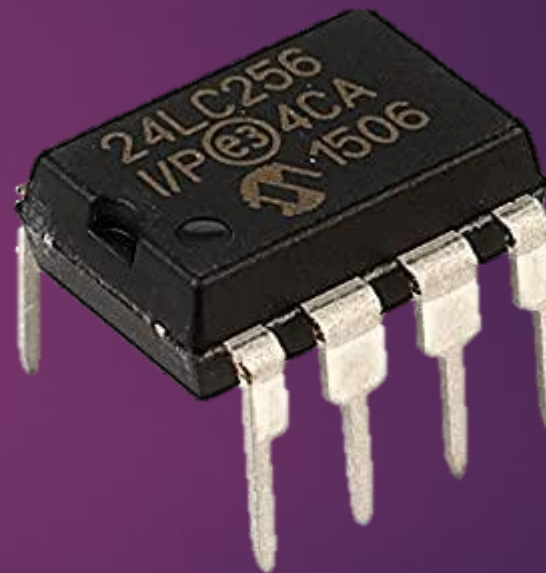


EEPROM

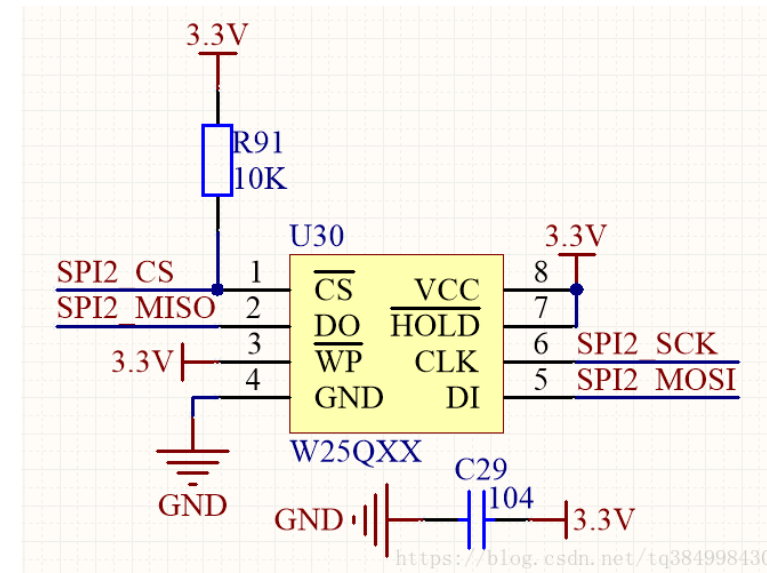
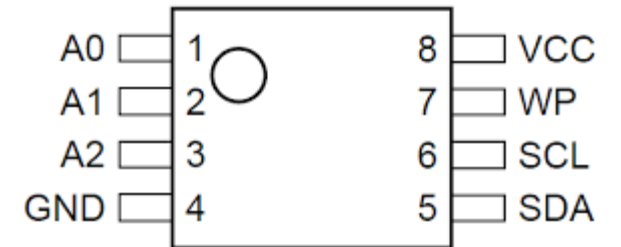
DUMPING AND ANALYSIS



About EEPROM

- ▶ electrically erasable programmable read-only memory
- ▶ It also has a limited life - that is, the number of times it can be reprogrammed is limited to tens or hundreds of thousands of times
- ▶ Contains firmware or configurations
- ▶ Used in : PC , Routers , Embedded and IOT
- ▶ I2C or ISP

8-Pin TSSOP



Dumping

- ▶ Installing flashrom
 - ▶ `sudo apt install flashrom`
- ▶ Configuring Arduino
 - ▶ <https://github.com/urjaman/frser-duino>
- ▶ Connecting Arduino and EEPROM
 - ▶ https://flashrom.org/Arduino_flasher_3.3v
- ▶ Dumping

Arduino pin	Function	Flash chip pin name
D13	CLK (Clock)	CLK
D12	MISO (Master In Slave Out)	MISO or SO
D11	MOSI (Master Out Slave In)	MOSI or SI
D10	CS# (Chip Select)	CS# or CS OR SS
GND	GND (Ground)	GND
5V	3.3V	VCC
5V	3.3V	WP# (Write Protect)
5V	3.3V	HOLD#



***LET'S
START***

analysis

- ▶ Binwalk
 - ▶ binwalk dump.bin, binwalk -e dump.bin , binwalk -E dump.bin
- ▶ Fmk
 - ▶ ./extract-firmware dump.bin
- ▶ Strings
 - ▶ strings dump.bin
- ▶ dd
 - ▶ dd if=dump.bin skip=1000 count=4000 of=part.bin



***LET'S
START***