Power Supply

- VCC Positive Voltage
- VSS/GND Ground/Negative Voltage
- Common Voltage: 5V/3.3V/1.7V/1.2V
- · All components should have a same ground reference.
- Laptop/PC is not a common GND

UART/Serial Port

Usually 3 or 4 pin header

Serial Adapter	Target
TX	RX
RX	TX
GND	GND
It is <u>never</u> TX-TX or	RX-RX.

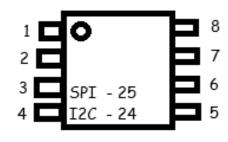


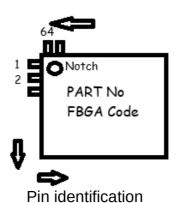
Voltage level and Common ground is important

Common Baudrate: 115200.9600.57600.38400

Flash/EEPROM

EEPROM – SPI(25Lxx) I2C(24Lxx) - SPI(25Qxx) Flash





FT232H Pin Mapping						
FTDI	UART	SPI				
۸۵۸	TV	SCK				

· · = • = · · · · · · · · · · · · · · ·									
FTDI	UART	SPI	I2C	JTAG	SWD				
AD0	TX	SCK	SCK	TCK	SCK				
AD1	RX	MOSI	SDA	TDI	SDIO				
AD2	RTS	MISO	SDA	TDO	SDIO				
AD3	CTS	CS		TMS					
AD4	DTR								

Connect AD1/AD2 for SDIO/SDA

20-Pin Debug Connection

VCC	TRST	TDI		•	RTCK	•	RESET	NC	NC
VCC	GND	GND	GND	GND	GND	GND	GND	GND	GND

10-Pin ST-Link Connection

RST	SWIM	GND	3.3V	5V
SCK	SWD	GND	3.3V	5V

10-pin Debug Connection

VCC	GND	GND	KEY	GND
SWD/ TMS	SCK/ TCK	SWO/ TDO	TDI	nRESET

Hardware Hacking Cheatsheet V2 @marunmagesh

Active Low: Enable by GND Active High: Enable by VCC

Upperscore in pin label means it is active low

Multimeter:

- Voltage: Measured between two point
- · Current: Measured in series between source and device
- Continuity: To see if two points are electrically connected
- Power = Voltage X Current

Memory-FTDI Mapping

Pin	SPI	I2C	FTDI /SPI	FTDI /I2C	Pin	SPI	I2C	FTDI /SPI	FTDI /I2C
1	CS	A0	AD3	GND	8	VCC	VCC	VCC	VCC
2	SO	A1	AD2	GND	7	HOL D	WP	VCC	VCC
3	WP	A2	VCC	GND	6	SCK	SCK	AD0	AD0
4	GND	GND	GND	GND	5	SI	SDA	AD1	AD1 / AD2

- General tips:
- Typical Temperature: 250-350C
- · Always Tin your iron after done
- Heat the pad and not the pin/solder
- If it smells like barbecue, you're doing it wrong
- · Don't touch PCB with bare hand
- Double check connections twice before powering

Useful Commands

Serial:

screen /dev/ttyUSBx (COMx - win) <baudrate> close screen: CTRL+A - K-Y log: -L -Logfile <Log file name> (before /dev)

flashrom

flashrom -p ft2232_spi:type=<232H/2232H> -r <filename> - Read flash -w <filename> - Write flash -c <chipname> - To use flash chip name

openocd

openocd -f interface/<dev.cfg> -f target/<target.cfg> In linux it is in usr\local\share\openocd\scripts\

Open session: telnet localhost:4444

Halt the CPU: halt Reset the CPU: reset Init the CPU: init

Flash info: flash info bank <id>

Flash dump: flash dump image <file> <address><size>

GDB

Start gdb: gdb-multiarch Select arch: set arch <arm/mips> Connect to target: target remote

<localhost>:3333

Breakpoint: break <address>

Register: info register Print memory: x/<nf>

n- no of byte f – format character(a/c/x/s/o)

I2C:

I2cdetect -y 1

File:

vbindiff <file1> <file2> hexdump -C <file> <target>-objdump -D -b binary -marm <file>