Bsides 2017 badge programming

$whoami

- Filsy - I designed the hardware
- Silvio did codes
- Kylie did all the hard work yelling at suppliers!

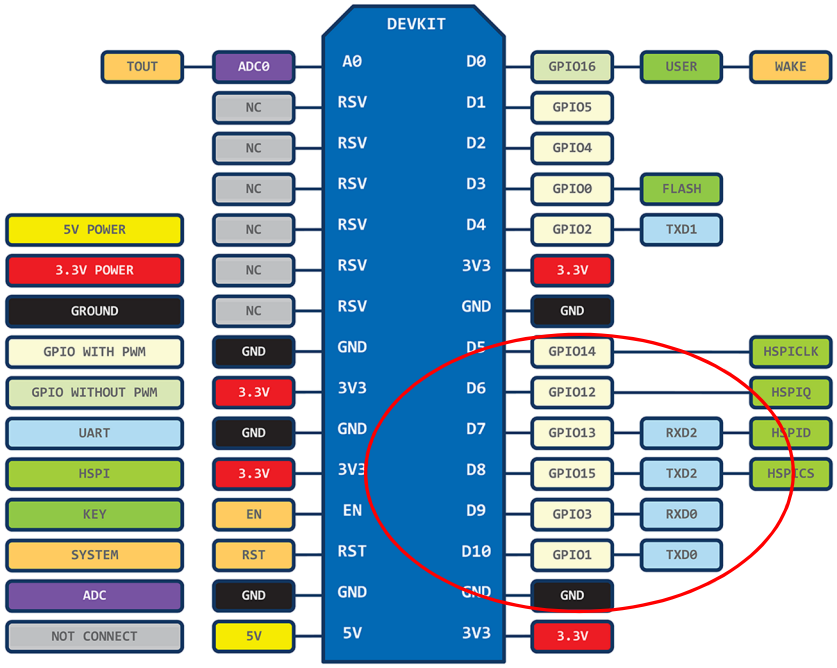
A quick overview of your fancy bird badge

- NodeMCU using an ESP8266 wifi module and CP2102? USB to serial converter
- A 1.8” TFT screen with a ST7735? Controller
- A RC 522 “mifare” rfid reader

What do I need to get started?

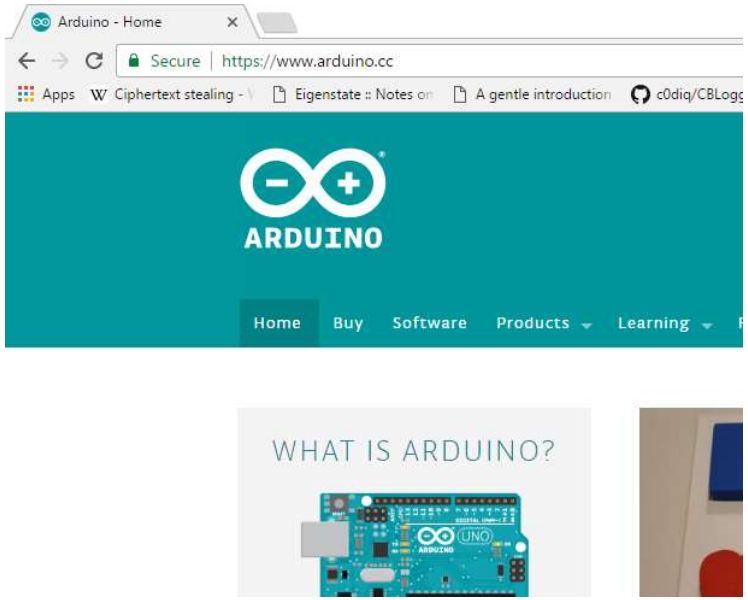
- Mini USB cable.
- Arduino IDE
- Computer.
- (optional) lots of alcohol.
- I have a virtual box image for those wanting to just plug in and go.

Schematics


DEVKIT
TOUT
ADC0
A0
D0
GPIO16
USER
WAKE
NC
RSV
D1
GPIO5
NC
RSV
D2
GPIO4
NC
RSV
D3
GPIO0
FLASH
5V POWER
NC
RSV
D4
GPIO2
TXD1
3.3V POWER
NC
RSV
3V3
3.3V
GROUND
NC
RSV
GND
GND
GPIO WITH PWM
GND
GND
D5
GPIO14
HSPICLK
GPIO WITHOUT PWM
3.3V
3V3
D6
GPIO12
HSPIQ
UART
GND
GND
D7
GPIO13
RXD2
HSPID
HSPI
3.3V
3V3
D8
GPIO15
TXD2
HSPICS
KEY
EN
EN
D9
GPIO3
RXD0
SYSTEM
RST
RST
D10
GPIO1
TXD0
ADC
GND
GND
GND
GND
NOT CONNECT
5V
5V
3V3
3.3V

Setting up the Arduino workspace

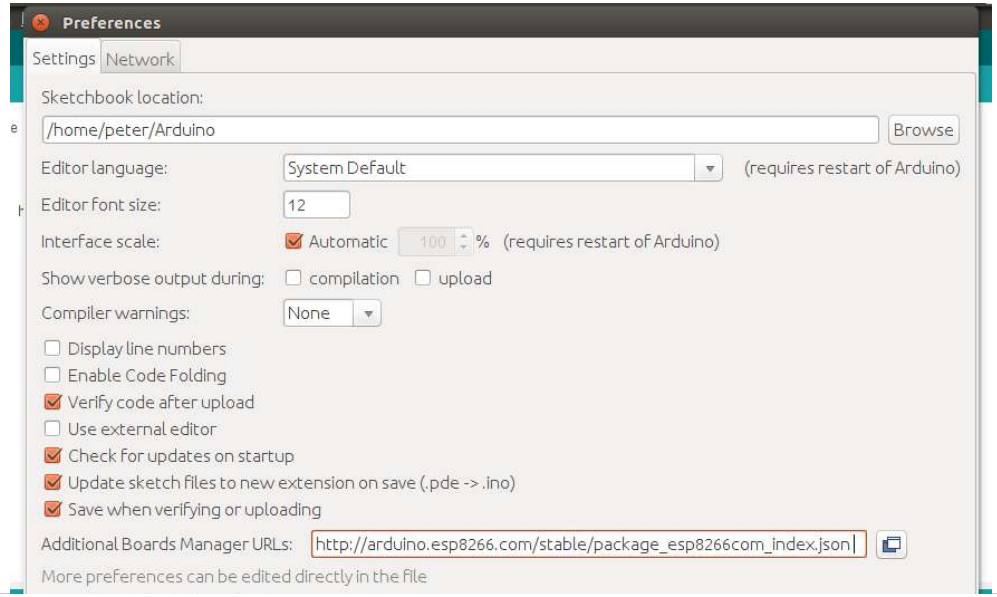
https://www.arduino.cc

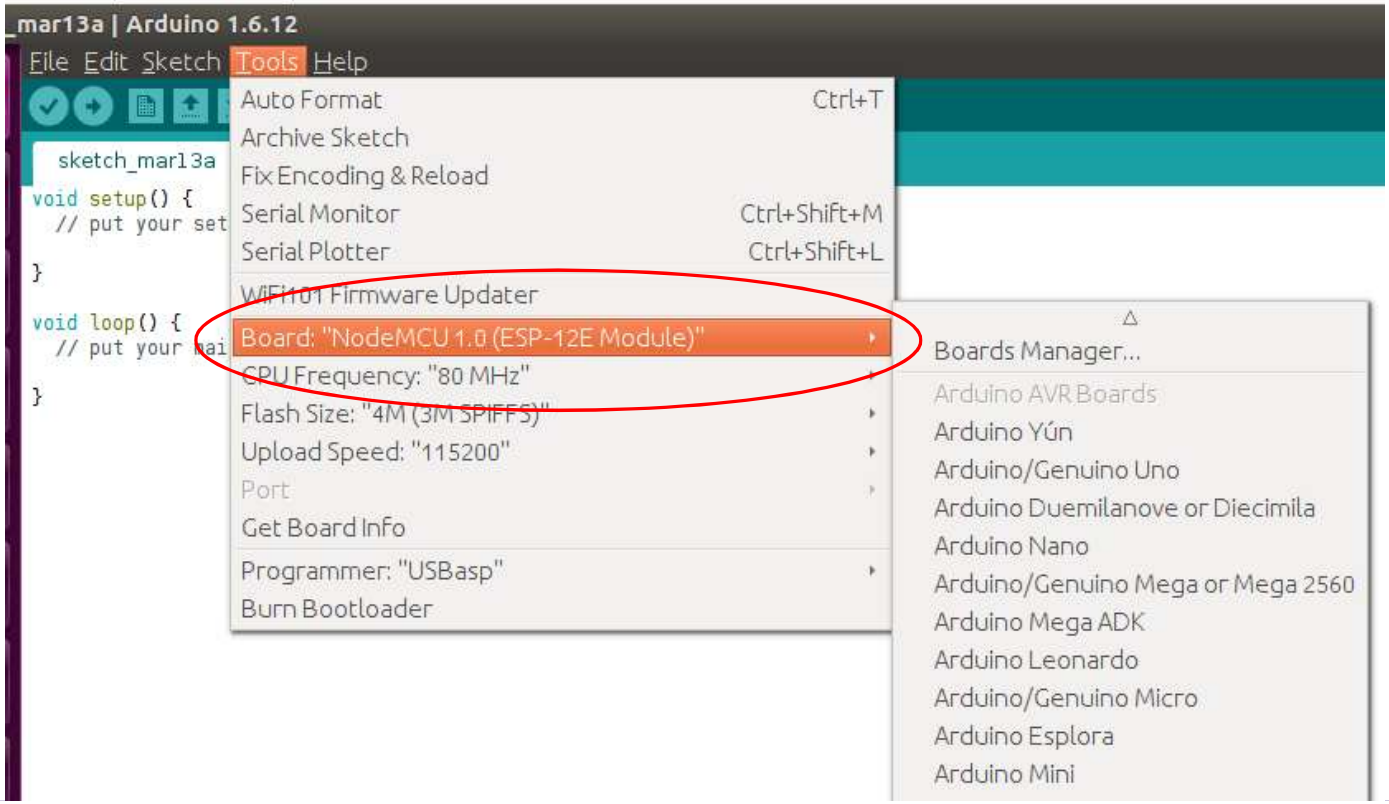


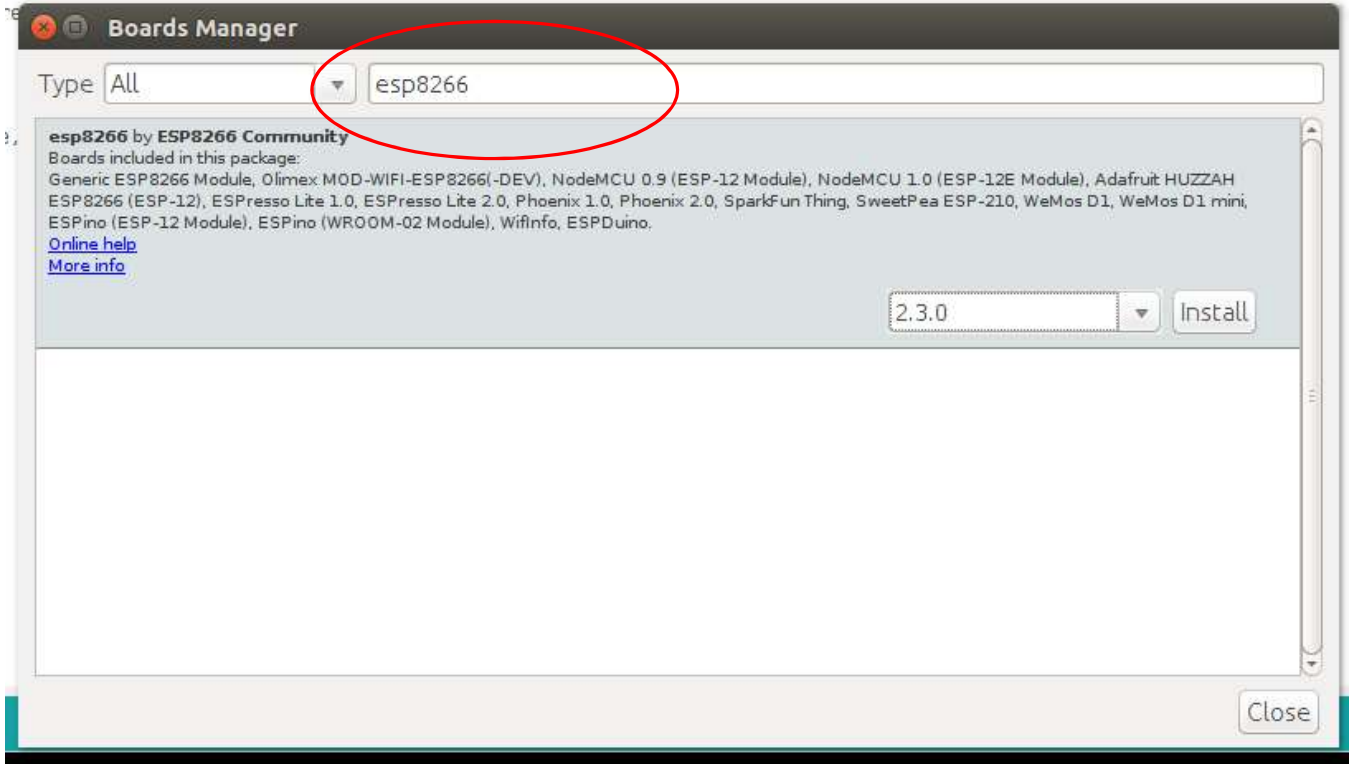
Download the Arduino IDE

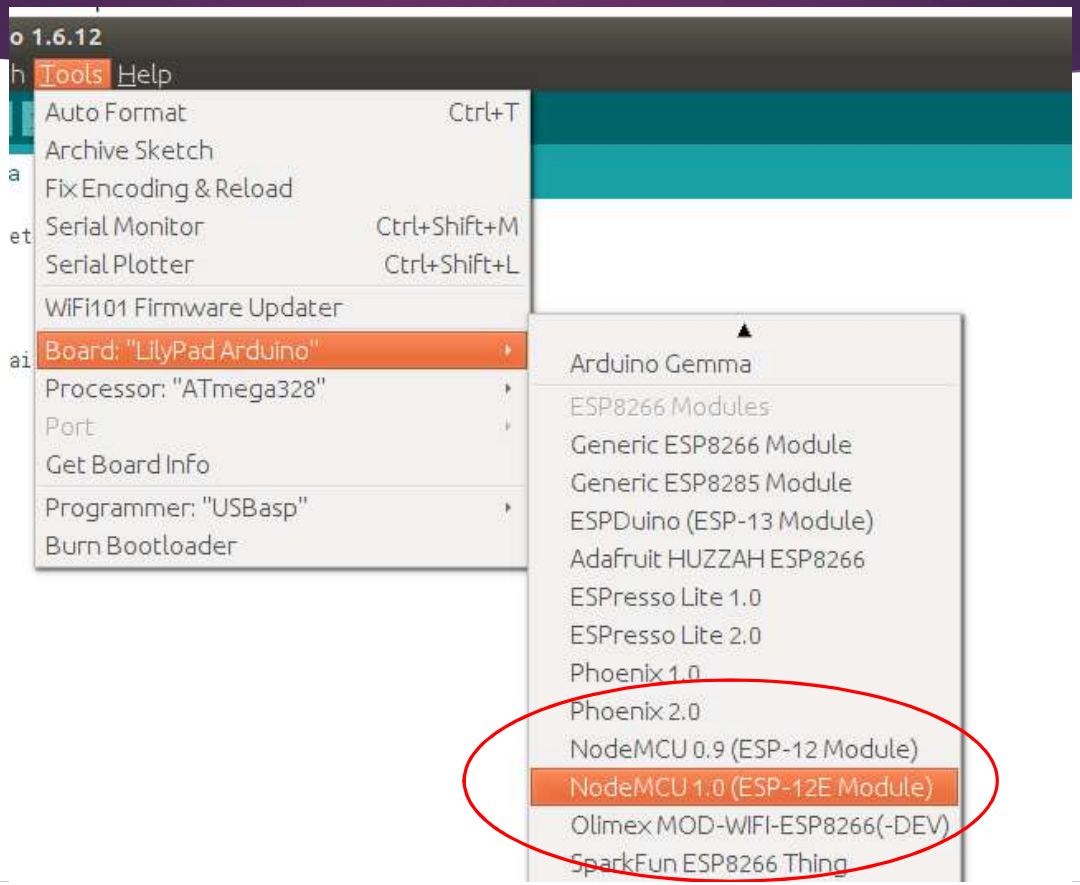
Add the NodeMCU libraries

- http://arduino.esp8266.com/stable/package_esp8266com_index.json




mar13a | Arduino 1.6.12
File Edit Sketch Tools Help
sketch_mar13a
void setup() {
// put your set
}
void loop() {
// put your mai
}
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 Firmware Updater
Board: "NodeMCU 1.0 (ESP-12E Module)"
CPU Frequency: "80 MHz"
Flash Size: "4M (3M SPIFFS)"
Upload Speed: "115200"
Port
Get Board Info
Programmer: "USBasp"
Burn Bootloader
Boards Manager...
Arduino AVR Boards
Arduino Yún
Arduino/Genuino Uno
Arduino Duemilanove or Diecimila
Arduino Nano
Arduino/Genuino Mega or Mega 2560
Arduino Mega ADK
Arduino Leonardo
Arduino/Genuino Micro
Arduino Esplora
Arduino Mini

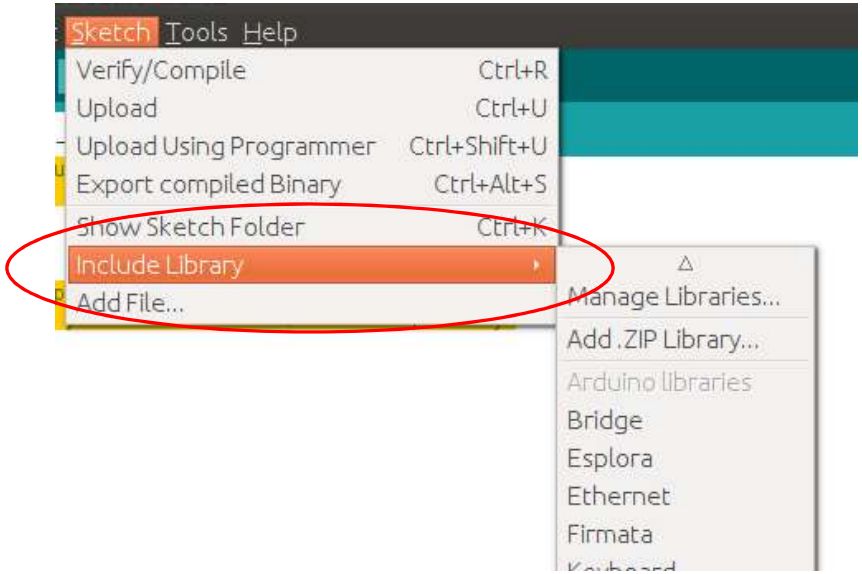

Boards Manager
Type
All
esp8266
esp8266 by ESP8266 Community
Boards included in this package:
Generic ESP8266 Module, Olimex MOD-WIFI-ESP8266(-DEV), NodeMCU 0.9 (ESP-12 Module), NodeMCU 1.0 (ESP-12E Module), Adafruit HUZZAH ESP8266 (ESP-12), ESPresso Lite 1.0, ESPresso Lite 2.0, Phoenix 1.0, Phoenix 2.0, SparkFun Thing, SweetPea ESP-210, WeMos D1, WeMos D1 mini, ESPino (ESP-12 Module), ESPino (WROOM-02 Module), WifInfo, ESPDuino.
Online help
More info
2.3.0
Install
Close


o 1.6.12
h Tools Help
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 Firmware Updater
Board: "LilyPad Arduino"
Processor: "ATmega328"
Port
Get Board Info
Programmer: "USBasp"
Burn Bootloader
Arduino Gemma
ESP8266 Modules
Generic ESP8266 Module
Generic ESP8285 Module
ESPDuino (ESP-13 Module)
Adafruit HUZZAH ESP8266
ESPresso Lite 1.0
ESPresso Lite 2.0
Phoenix 1.0
Phoenix 2.0
NodeMCU 0.9 (ESP-12 Module)
NodeMCU 1.0 (ESP-12E Module)
Olimex MOD-WIFI-ESP8266(-DEV)
SparkFun ESP8266 Thing

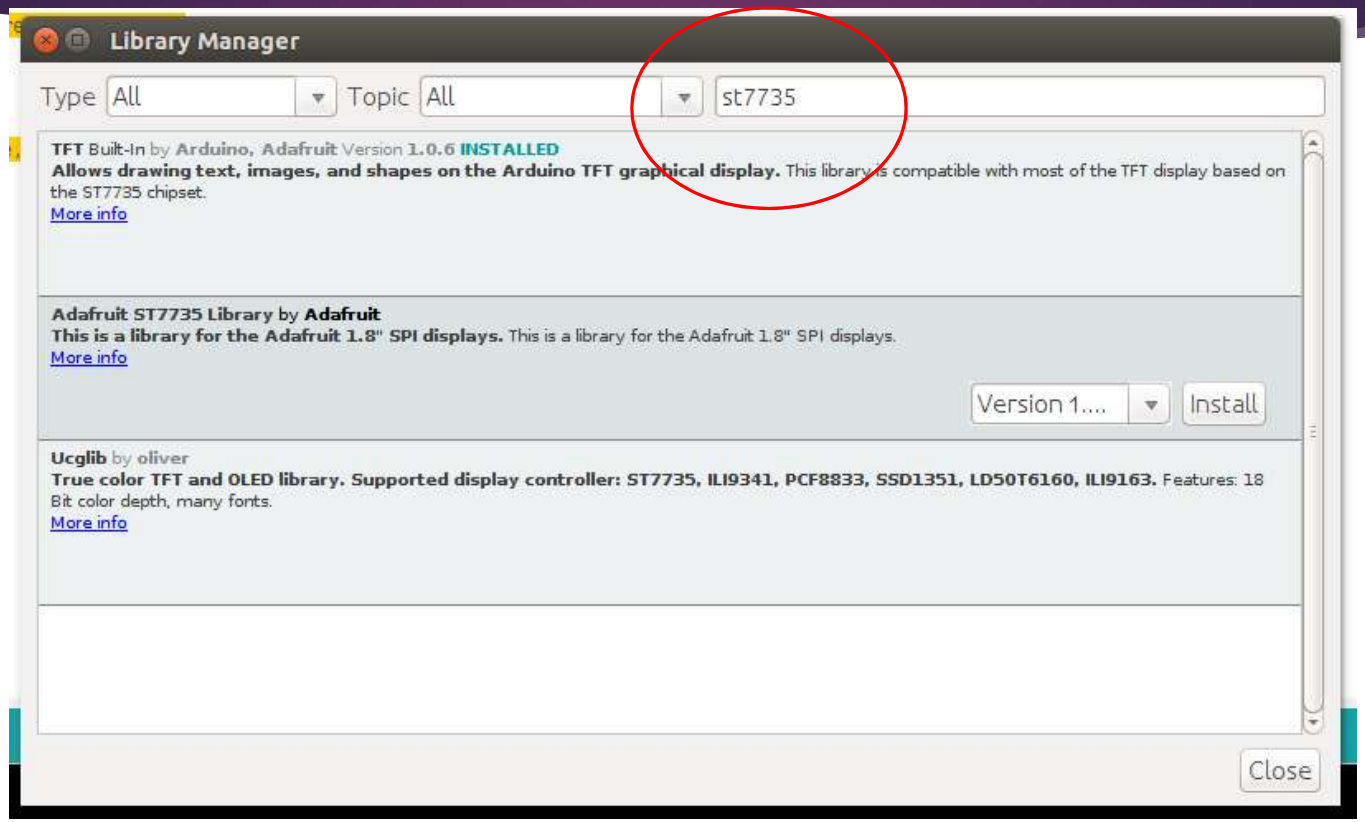
Skip the next few steps

- Libraries are at
- Git pull https://github.com/peterfillmore/BSides2017_Template
- I found the “default” libraries are “a bit” broken.
- The ones in the git repo at least work.

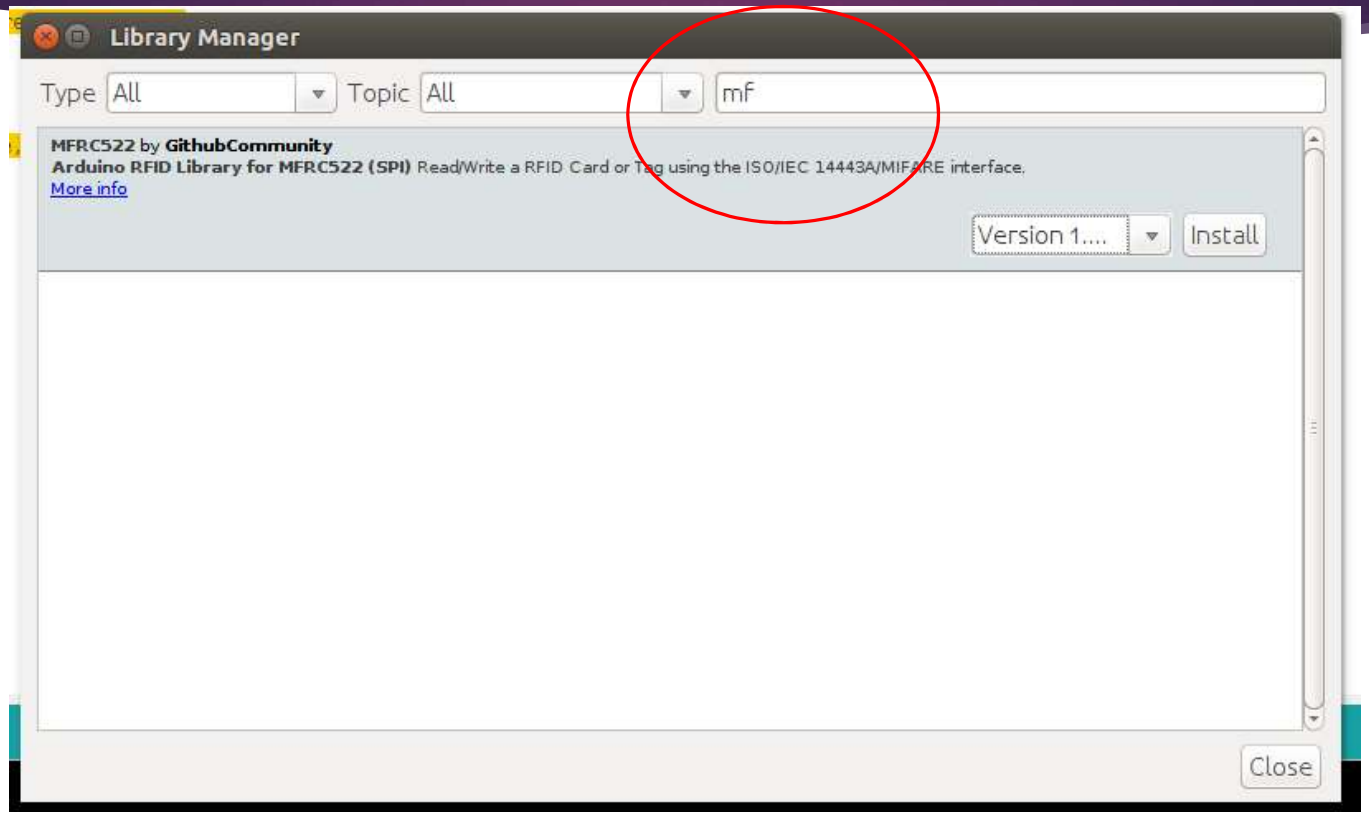
Installing libraries through the IDE



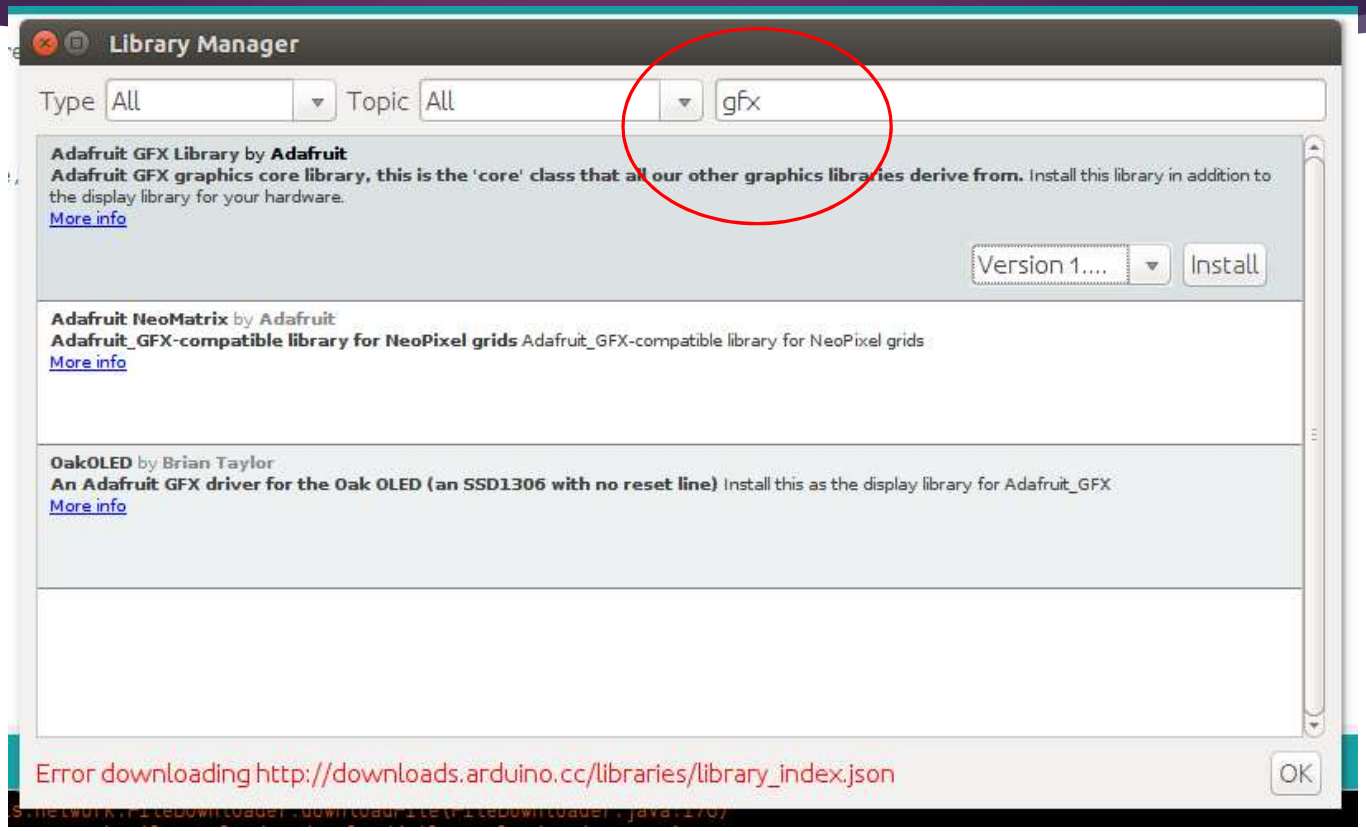
Display library



RFID Reader


Library Manager
Type
All
Topic
All
mf
MFRC522 by GithubCommunity
Arduino RFID Library for MFRC522 (SPI) Read/Write a RFID Card or Tag using the ISO/IEC 14443A/MIFARE interface.
More info
Version 1....
Install
Close

GFX Library


Library Manager
Type All
Topic All
gfx
Adafruit GFX Library by Adafruit
Adafruit GFX graphics core library, this is the 'core' class that all our other graphics libraries derive from. Install this library in addition to the display library for your hardware.
More info
Version 1....
Install
Adafruit NeoMatrix by Adafruit
Adafruit_GFX-compatible library for NeoPixel grids Adafruit_GFX-compatible library for NeoPixel grids
More info
OakOLED by Brian Taylor
An Adafruit GFX driver for the Oak OLED (an SSD1306 with no reset line) Install this as the display library for Adafruit_GFX
More info
Error downloading http://downloads.arduino.cc/libraries/library_index.json
OK

For those with the ILI board.

- git clone https://github.com/sumotoy/TFT_ILI9163C

```
peter@peter-VirtualBox:~$ cd Arduino/
peter@peter-VirtualBox:~/Arduino$ ls
BSides_Test  libraries
peter@peter-VirtualBox:~/Arduino$ cd libraries/
peter@peter-VirtualBox:~/Arduino/libraries$ ls
Adafruit_ST7735_Library  MFRC522  readme.txt
peter@peter-VirtualBox:~/Arduino/libraries$ cat readme.txt
For information on installing libraries, see: http://www.arduino.cc/en/Guide/Lib
raries
peter@peter-VirtualBox:~/Arduino/libraries$ git clone https://github.com/sumotoy
/TFT_ILI9163C
```

Optional – The SD Card driver

- You have an SD card?
- Well you can use it!
- (we didn't use this in the normal board)

Add these headers

- #include <pins_arduino.h> //sane PIN numbering
- #include <SPI.h> // SPI support
- #include <Adafruit_GFX.h> // Core graphics library
- #include <Adafruit_ST7735.h> // Hardware-specific library
- #include <WiFiServer.h> //using wifi?
- #include <ESP8266WiFiMulti.h>
- #include <WiFiUdp.h>
- #include <WiFiClient.h>
- #include <ESP8266WiFi.h>
- #include <WiFiClientSecure.h>
- #include "MFRC522.h"//RFID reader
- #include <SD.h> //SD Card

TFT Initialisation Code

```
#define TFTDC   D2  // D/C select line to TFT
#define TFTCS   D8 // Active LOW to TFT
#define TFTBL   D1 // Active HIGH to turn on TFT backlight
#define TFTRST  D0
Adafruit_ST7735 tft = Adafruit_ST7735(TFTCS, TFTDC, TFTRST);
pinMode(TFTDC, OUTPUT);
pinMode(TFTCS, OUTPUT);
pinMode(TFTBL, OUTPUT);
pinMode(TFTRST, OUTPUT);
tft.initR(INITR_GREENTAB); // initialize a ST7735S chip, black tab
analogWrite(TFTBL, 2048);  // TFT backlight 50%
```

RFID Initialisation Code

- #define RFID_RST_PIN D4 // Configurable, see typical pin layout above
- #define RFID_SS_PIN D3 // Configurable, see typical pin layout above
- MFRC522 mfrc522(RFID_SS_PIN, RFID_RST_PIN); // Create MFRC522 instance
- pinMode(RFID_SS_PIN, OUTPUT);
- pinMode(RFID_RST_PIN, OUTPUT);
- mfrc522.PCD_Init(); // Init MFRC52
- mfrc522.PCD_DumpVersionToSerial(); // Show details of PCD - MFRC522 Card Reader details

SD Initialisation Code

```
#define SDCARD_CS_PIN D9
 pinMode(SDCARD_CS_PIN, OUTPUT);
if (!SD.begin(SDCARD_CS_PIN)) {
   Serial.println("SD initialization failed!");
   return;
 }
 Serial.println("initialization done.");
```

Do a lot of googling and copy pasta'ing

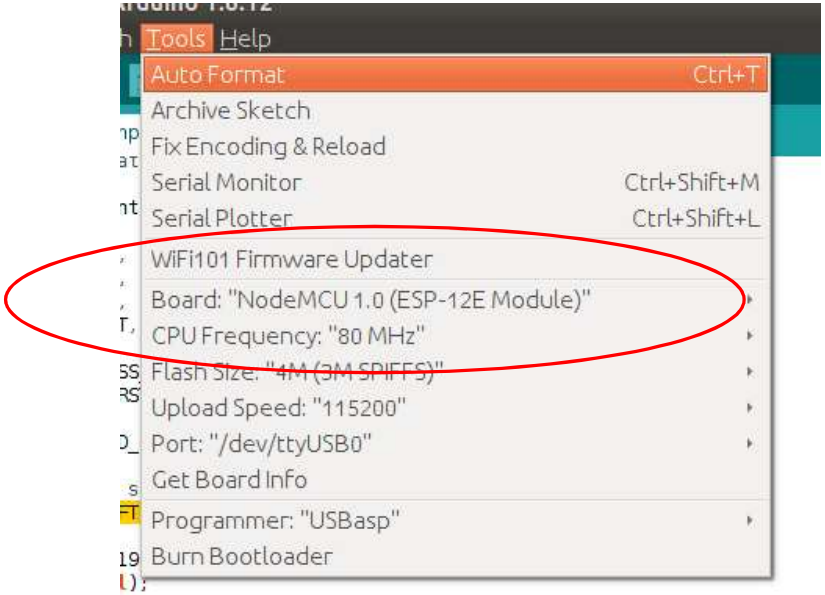
- There's a lot of available Arduino code available to play with.
- Feel free to experiment!
- Its easy to compile, flash and test.

Accessing the USB port (in linux)

- $sudo adduser <you> dialout
- Logout/log back in.
- Or just run under sudo.

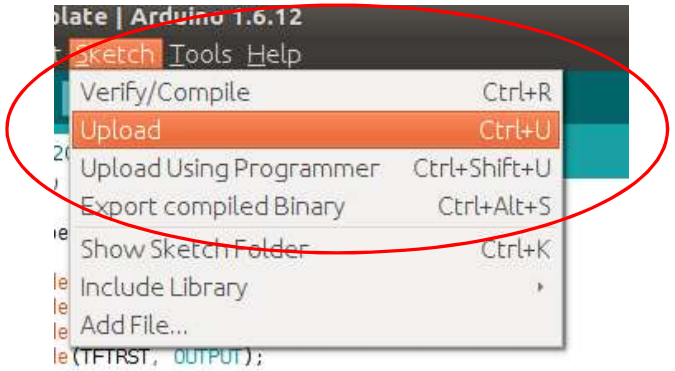
Writing code to the badge

Set the detected port

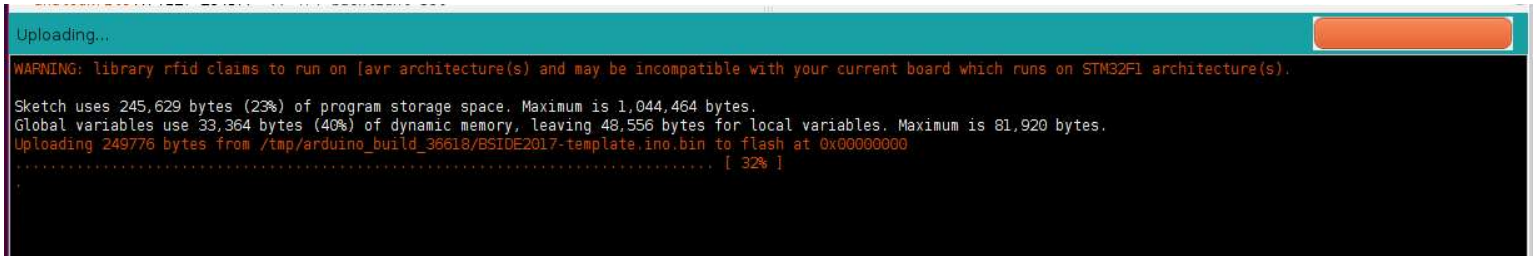


Click upload

Hit “Upload”
This’ll also re-compile your sketch



The upload then starts.



Have Fun!

- Arduino has a huge amount of libraries and boards available.
- The provided schematic shows you the pins.
- Feel free to take of the NodeMCU and use it for other projects!
- Or use this board!

You don't _have_ to use Arduino

- Micropython!
- Bare Metal!

Micropython demo

MicroPython - Python fo ×

ps://micropython.org/download#esp8266

Eigenstate :: Notes on | A gentle introduction | c0diq/CBLogger · Gith | EMV CVM Database | Include Security Blog | tomato42/tlsfuzz

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.

- esp8266-20170108-v1.8.7.bin (elf, map) (latest)
- esp8266-20161110-v1.8.6.bin (elf, map)
- esp8266-20161017-v1.8.5.bin (elf, map)
- esp8266-20160909-v1.8.4.bin (elf, map)
- esp8266-20160809-v1.8.3.bin (elf, map)
- esp8266-20160710-v1.8.2.bin (elf, map)
- esp8266-20160603-v1.8.1.bin (elf, map)
- esp8266-20160503-v1.8.bin (elf, map)

The following are daily builds of the ESP8266 firmware. They have the latest features and bug fixes. WebREPL is

Bare C code!

- http://gnutoolchains.com/esp8266/
- https://github.com/pfalcon/esp-open-sdk

Banned stuff – do not read!

- https://github.com/spacehuhn/esp8266_deauther
- Totally don't run esptool.py –port /dev/ttyUSB0 read_flash and dump the fw off the device.
- No running "strings" on anything you dumped on your badge – especially if you're looking for CTF flags!