

# ESP8266 钓鱼 软件使用说明

---

其实关于 **esp8266** 网上有许多教程，好多前辈玩这个已经好多年了，但为了给像我这样的小白系统的解决制作过程中的一些问题，我还是写出来。



## 1. **eps8266** 模块

首先当然你要有一块 **eps8266** 模块，像这样的，最好是有底板的，带 Micro 口的，这些淘宝上都可以搜到的，我的就是淘宝上买的，大概 10-20RMB 左右。



## 2. 如何将固件下载到 esp8266 中

在这里你需要下载两个东西，就是 Flash 下载工具和固件

Flash 下载工

具：<http://espressif.com/zh-hans/support/download/other-tools>

固件我这里用的是：./固件/DNS.ino.ino.nodemcu.bin

将自己的 esp8266 插到电脑上，确定连接没问题的话打开设备管理器看下自己的串口是多少，我这边是 COM6



将下载的 Flash 下载工具解压，打开 ESPFlashDownloadTool\_v3.4.9.2.exe，打开是这样的，选择 esp8266 DownloadTool



在这里需要注意的几点是：

(1) 固件选择之前下载的固件  
DNS.ino.ino.nodemcu  
.bin。

## (2) 地址输入

0×00000 (可能地址这一栏会出现红色的状况，导致无法烧入固件，此时把下载器关了重启下，然后把地址那栏清空再自己手动输入就好了)。

## (3) 这边需要将

DoNotChgBin 勾选起来，否则烧入固件后可能没有wifi，当然不同的板子可能不太一样，这个请大家自行测试。


(4) 这边串口按照自己之前查的选择就行了，波特率 115200 就可以了。

其他设置按照红框里面的选择就行



```
D:\Python27>cd Scripts
D:\Python27\Scripts>nuptool.py --port COM6 erase_flash
nuptool.py v2.1
Connecting....
Detecting chip type... ESP8266
Chip is ESP8266
Uploading stub...
Running stub...
Stub running...
Erasing flash (this may take a while)...
Chip erase completed successfully in 6.0s
Hard resetting...

D:\Python27\Scripts>
```



### 3. 用 arduino 上传 web 到 esp8266

到 arduino 官网下载适合你自己系统的软

件：<https://www.arduino.cc/en/Main/Software>

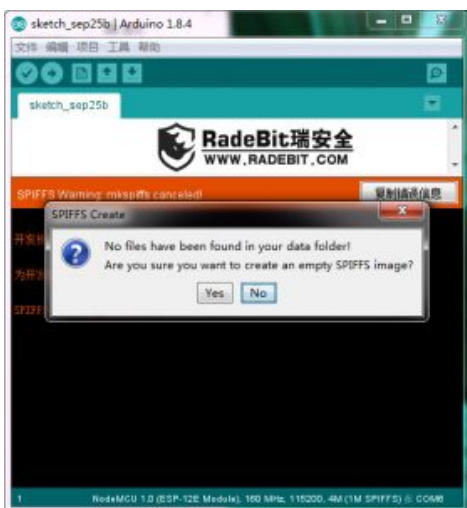
web 源码：./data/\*.html

web 源码上传工具：./tools

我的是 Windows 系统，arduino 版本是 1.8.4，安装完后打开工具——开发板——开发板管理器，此时会自动更新，过个数分钟更新完毕后（当然，如果用外网的话可能几秒钟就能解决），搜索 esp8266，选择第二个，版本选 2.2.0，然后安装。



将上面解压后的 web 源码上传工具的 tools 放到 Arduino 根目录里合并，然后返回以下界面，点击文件——新建，新建一个项目，将里面的代码清空，然后点击文件——保存，将项目保存到一个你能找到的位置，点击工具——esp8266 sketch data upload，会出现以下的提示，选择 No，会发现新建的项目中多出来一个 data 文件夹，里面是空的，然后将上面下载的 web 源码 data 里面的三个文件复制到这个文件夹里面。



然后再返回 arduino，点击工具，开发板按照自己买的选  
择，端口选择自己的端口，  
其他设置如下图红框里面的。  
的。





设置完后点击 esp8266 sketch data upload，这时不会出现提醒，开始上传 web 页面，等个 1 分钟左右 esp8266 上的蓝灯不闪烁了，就表示上传完了。

然后电脑连接 HH 的 wifi，浏览器输入 192.168.1.1/backdoor.html 就能进入 web 页面了，如下图，路由器型号选择通用型，然后输入你测试的 wifi 编号，点确定，电脑提示 SSID 伪造成功，手机就会发现出现了个和你测试的 wifi 一样的没有加密的 wifi，原来的 HH 会不见了，8266 的蓝灯常亮，手机连接那个 wifi 后过几秒会自动弹出路由器升级的页面，然后输入管理员密码，点击开始升级，此时你的 esp8266 会将管理员密码保存，升级完后，8266 的灯就会灭掉。



电脑重新连接 HH，进入 web 页面后管理员密码会在下面的红框这一块显示，这时，就表示获取密码成功了。



到此，整个 esp8266 制作 wifi 的教程到此结束，祝大家玩的开心！！！！