Dept of Mathematics

Hi-jack any IoT device Using Lua scripting language

WARNING

Transmitting deauth packets is unlawful creation of interference within radio channels it's **illegal** according to the law and attracts significant penalties. However**, studying such techniques** should provide a **useful edge** in the **electronic wars** to come you can also use it **to prevent** communication of IP CCTVs, alarms & **almost all IoT devices** within **wireless security system**

By : Muhammad Osama Bin Jafar

Micro controller ESP8266 (NODE MCU)

Overview

NodeMCU is an open source firmware based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua scripting language The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna and integerated with WI-FI SoC

Using driver

VCP Drivers Features and Benefits

The CP210x USB to UART Bridge Virtual COM Port (VCP) drivers are required for device operation as a Virtual COM Port to facilitate host communication with CP210x products. These devices can also interface to a host using the direct access drive

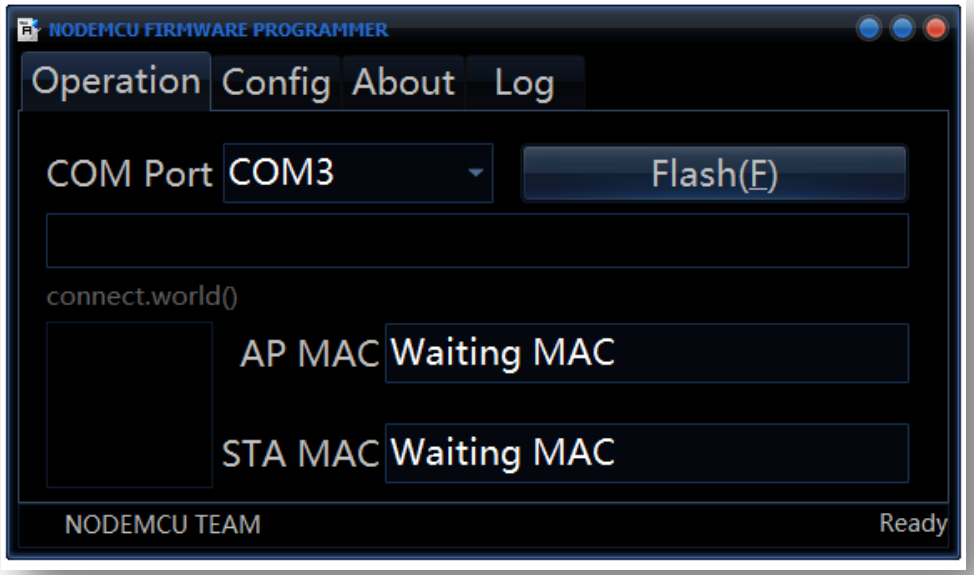
NODEMCU flashing tool

NodeMCU Flasher

NodeMCU flasher is a firmware programmer for NodeMCU DEVKIT V0.9.

You can use it to program NodeMCU DEVKIT or your own ESP8266 board.

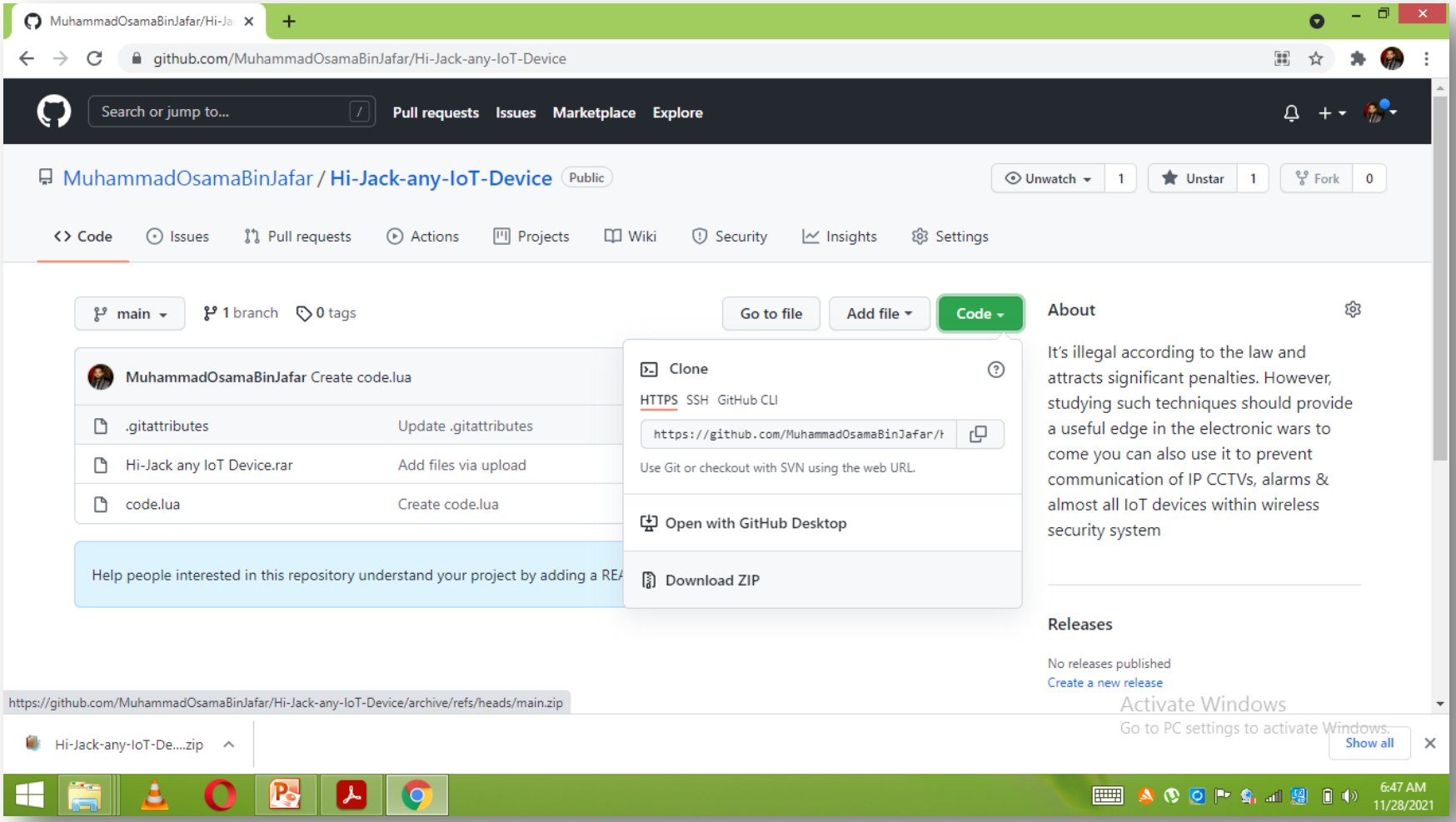
You MUST set GPIO0 to LOW before programming, and NodeMCU DEVKIT V0.9 will do it automatically.



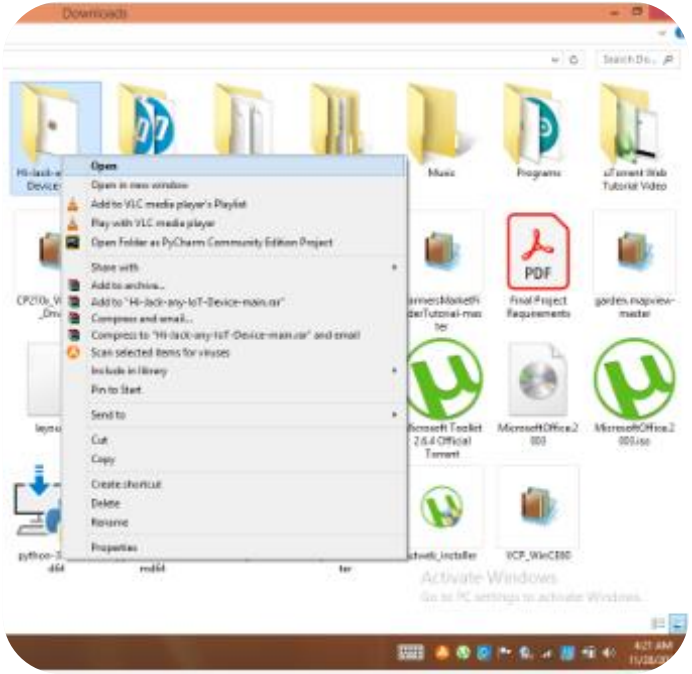
Procedure

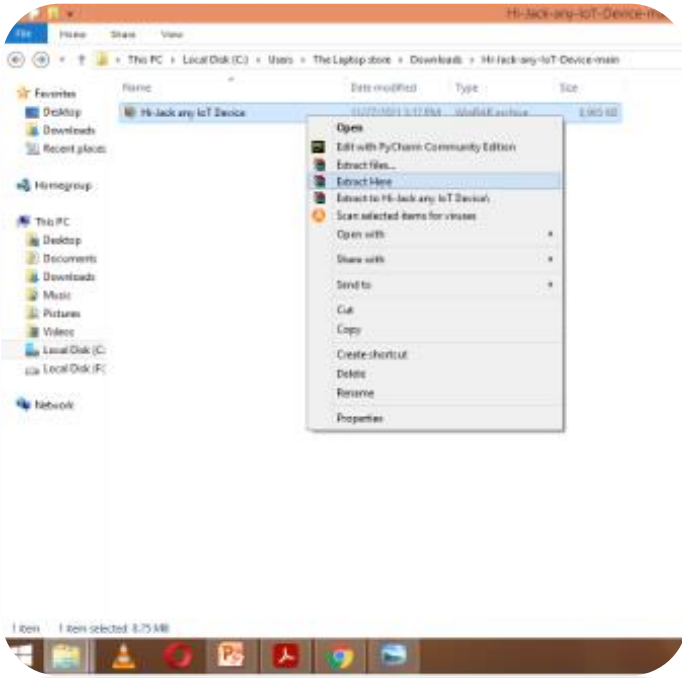
- Download zip file from https://github.com/MuhammadOsamaBinJafar/Hi-Jack-any-IoT-Device
- Extract it , install The CP210x USB to UART Bridge Virtual COM Port (VCP) drivers then install nodeMCU flasher.
- for simplicity Lua code is compiled in a binary file.
- Configure nodeMCU flasher connect your nodeMCU and upload ESP8266_Deauther_v2.0.5_1MB.bin in it by using odd number COM (1,3,5,7..).
- When code is successfully uploaded then disconnect your nodeMCU and power it by any external source.
- Now you find a new wi-fi network named pwned , forget your home network and connect with it by using password **deauther**
- Now open browser and go to iP address **192.168.4.1**

Downloading zip file

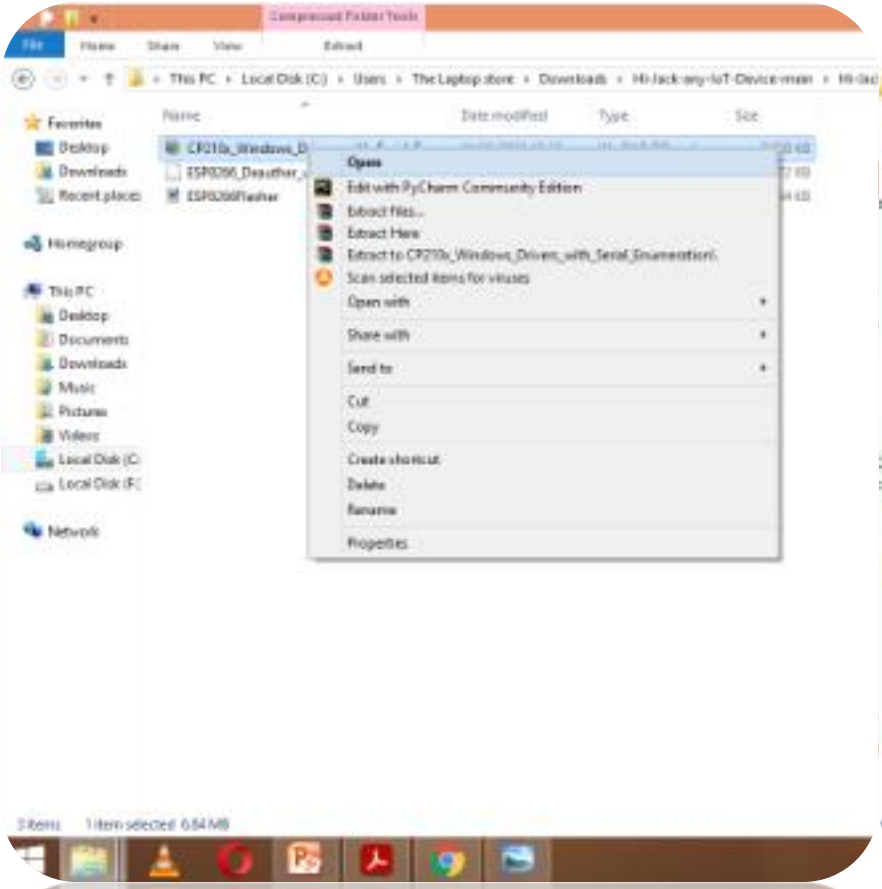


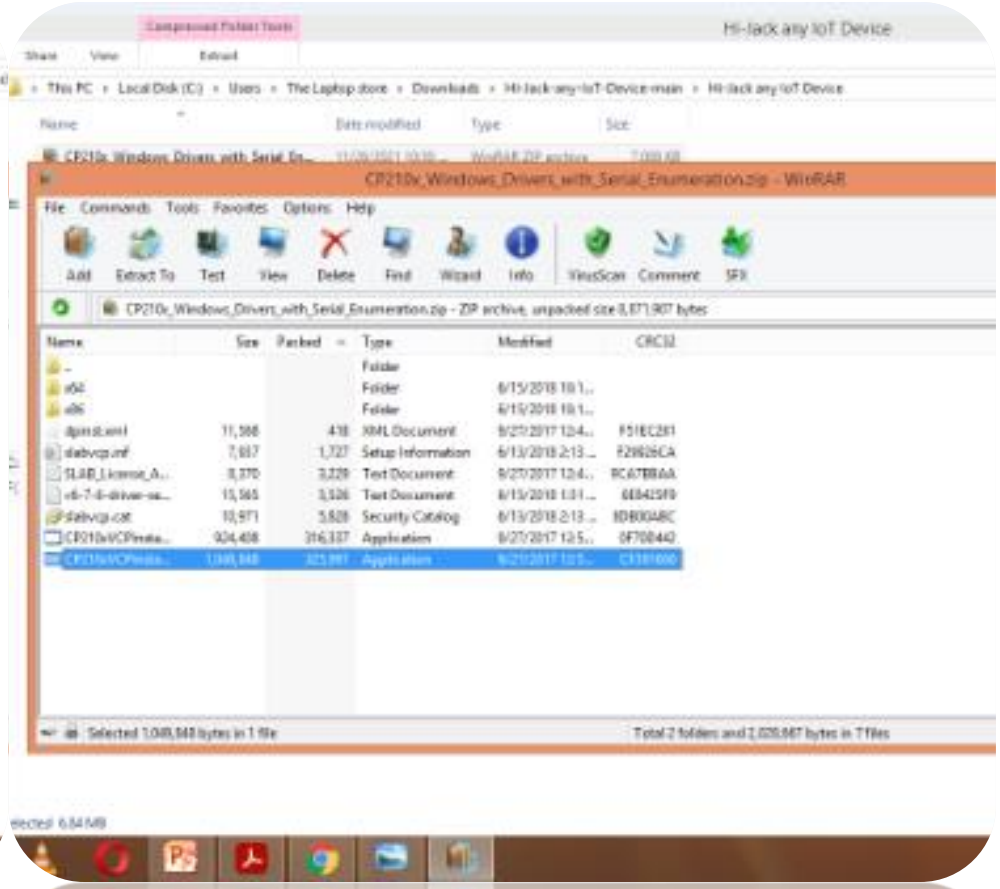
Extracting zip file



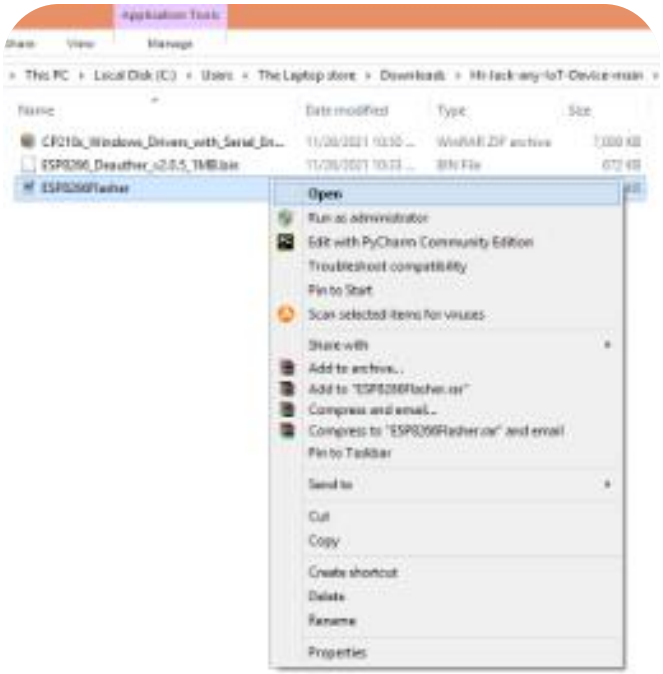


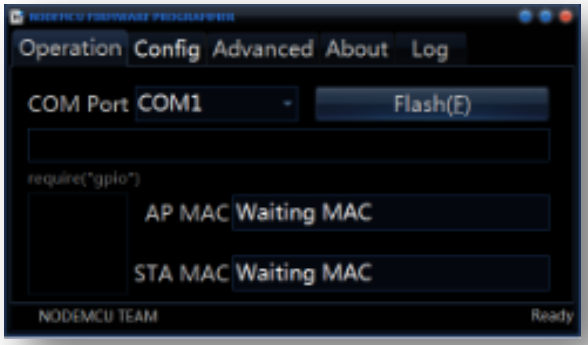
Installing The CP210x USB to UART Bridge Virtual COM Port (VCP) drivers



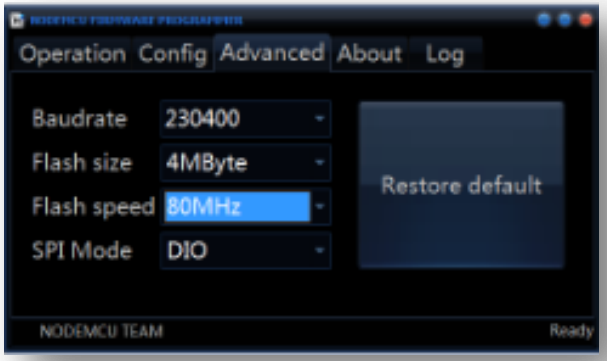


Installing nodeMCU flasher and configuring it



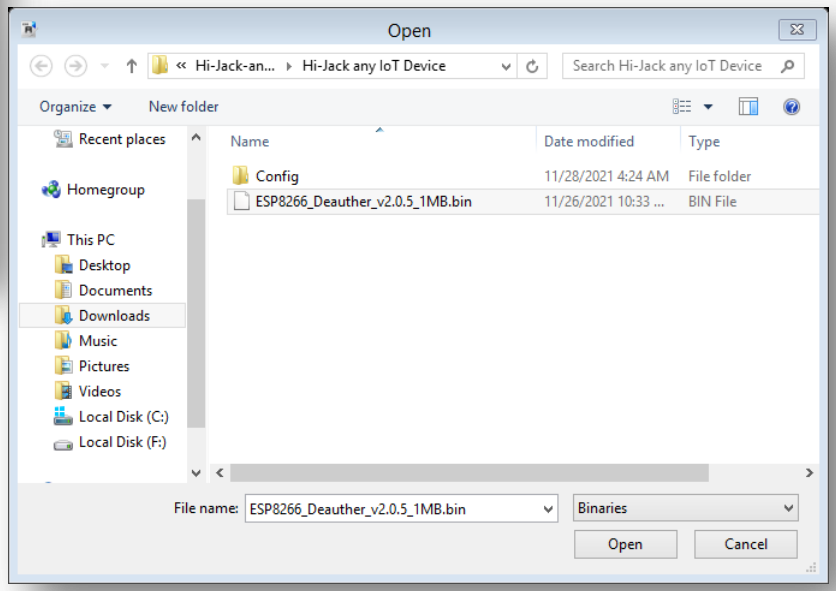


Then configure it to

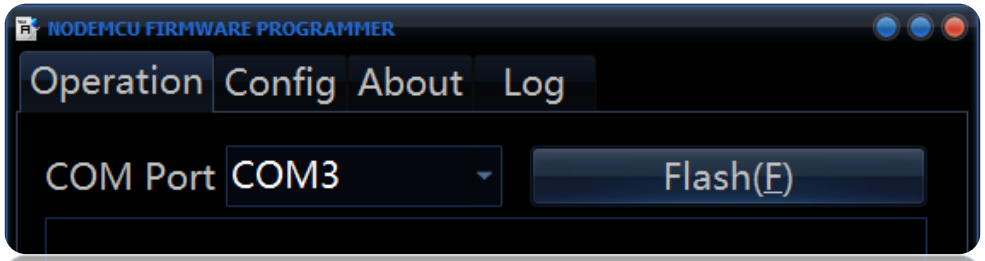


Connect your nodeMCU by using good quality cable and upload code in it

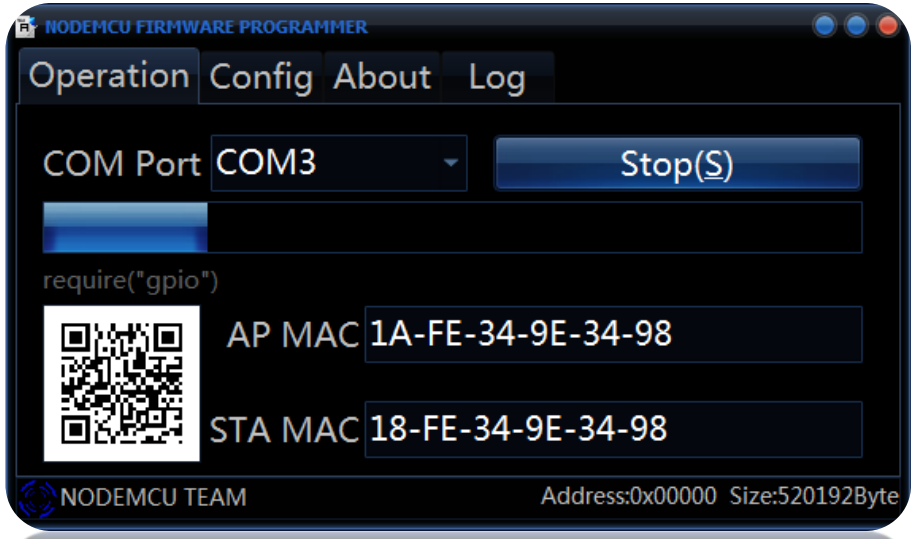
Click ot it and Select binary file ESP8266_Deauther_v2.0.5_1MB.bin

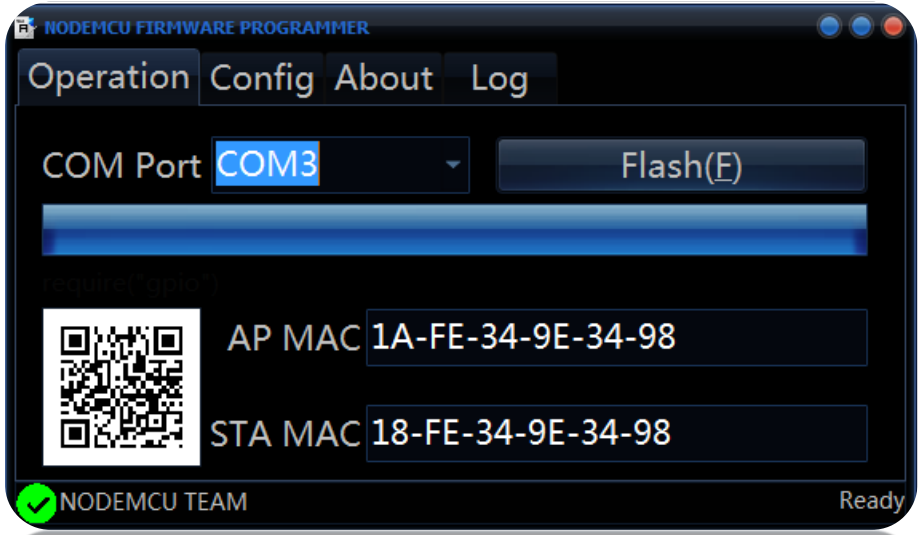


Then click on flash f



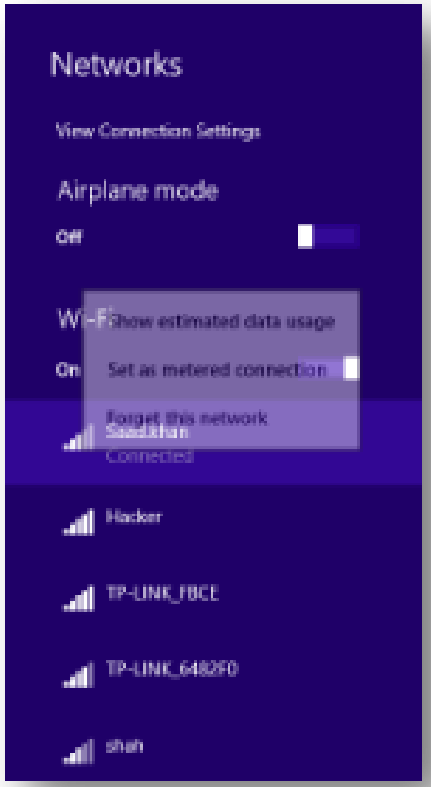
Uploading code in nodeMCU is successful

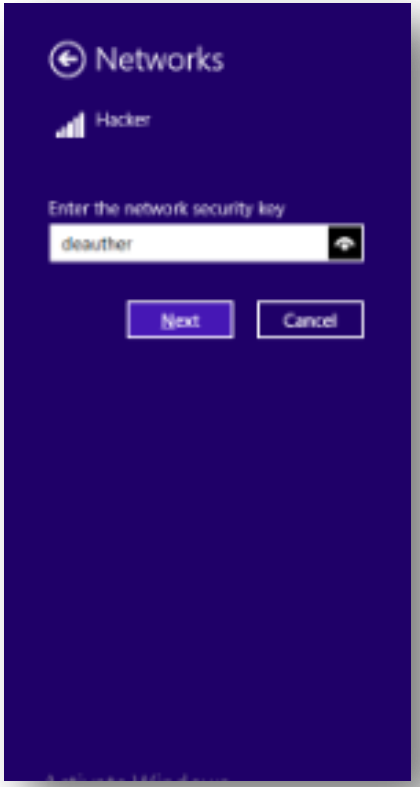




Now connect with pwned, new WI-FI network and go to ip address **192.168.4.1**

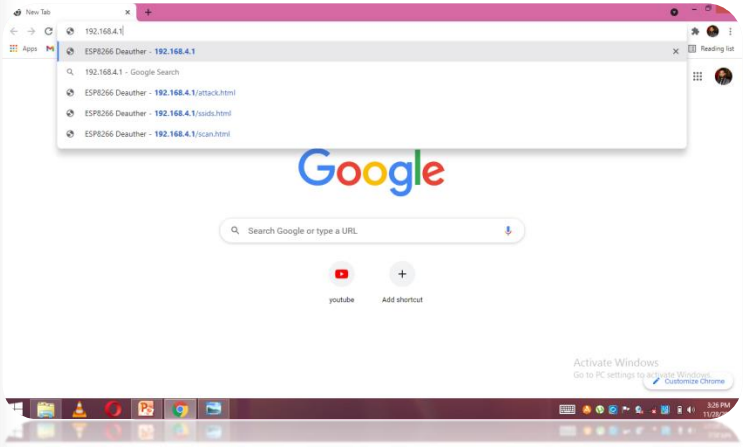
- Forget your home network
- Connect with pwned , new wifi network transmited by nodeMCU





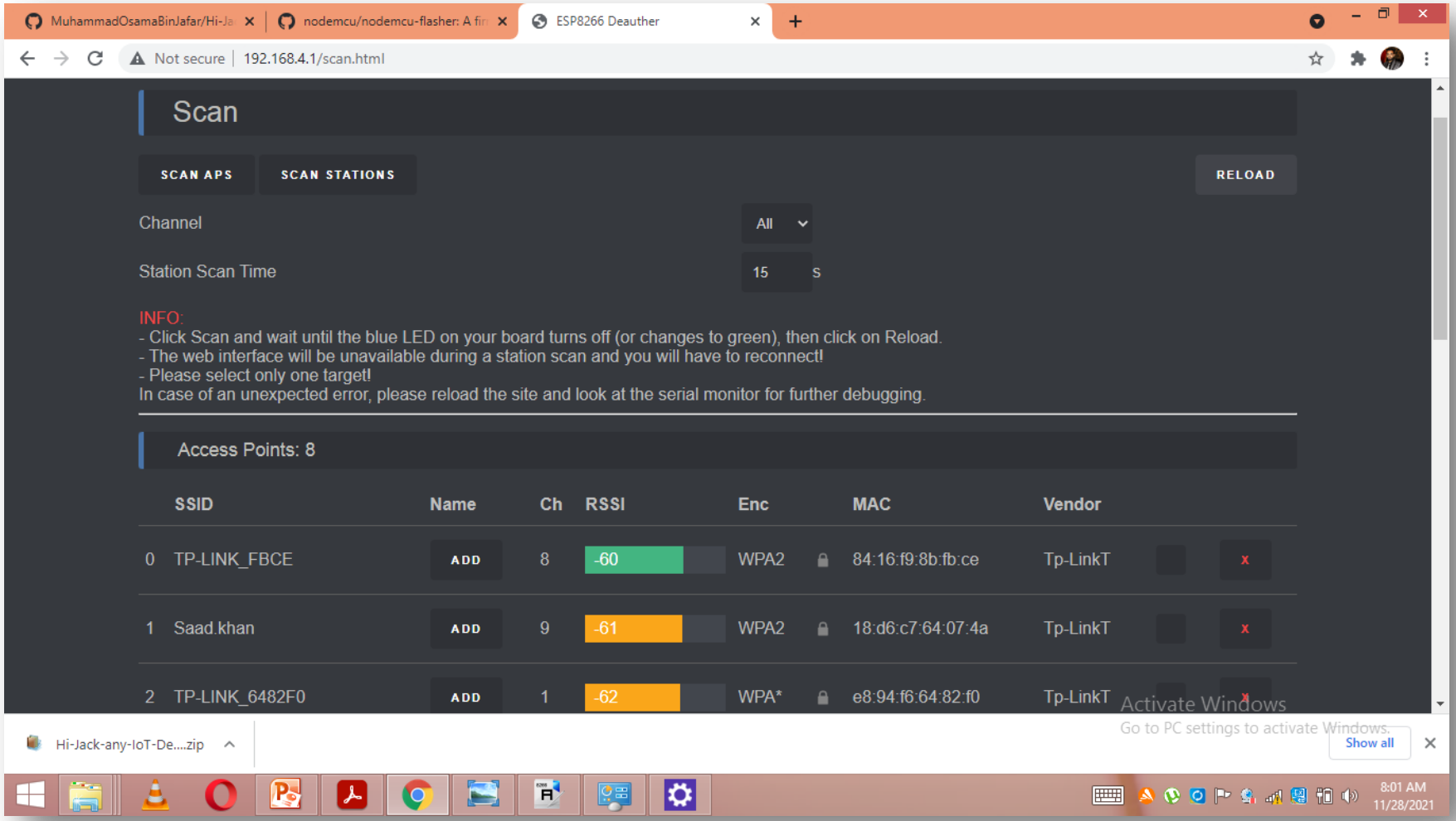
then open this ip address

192.168.4.1



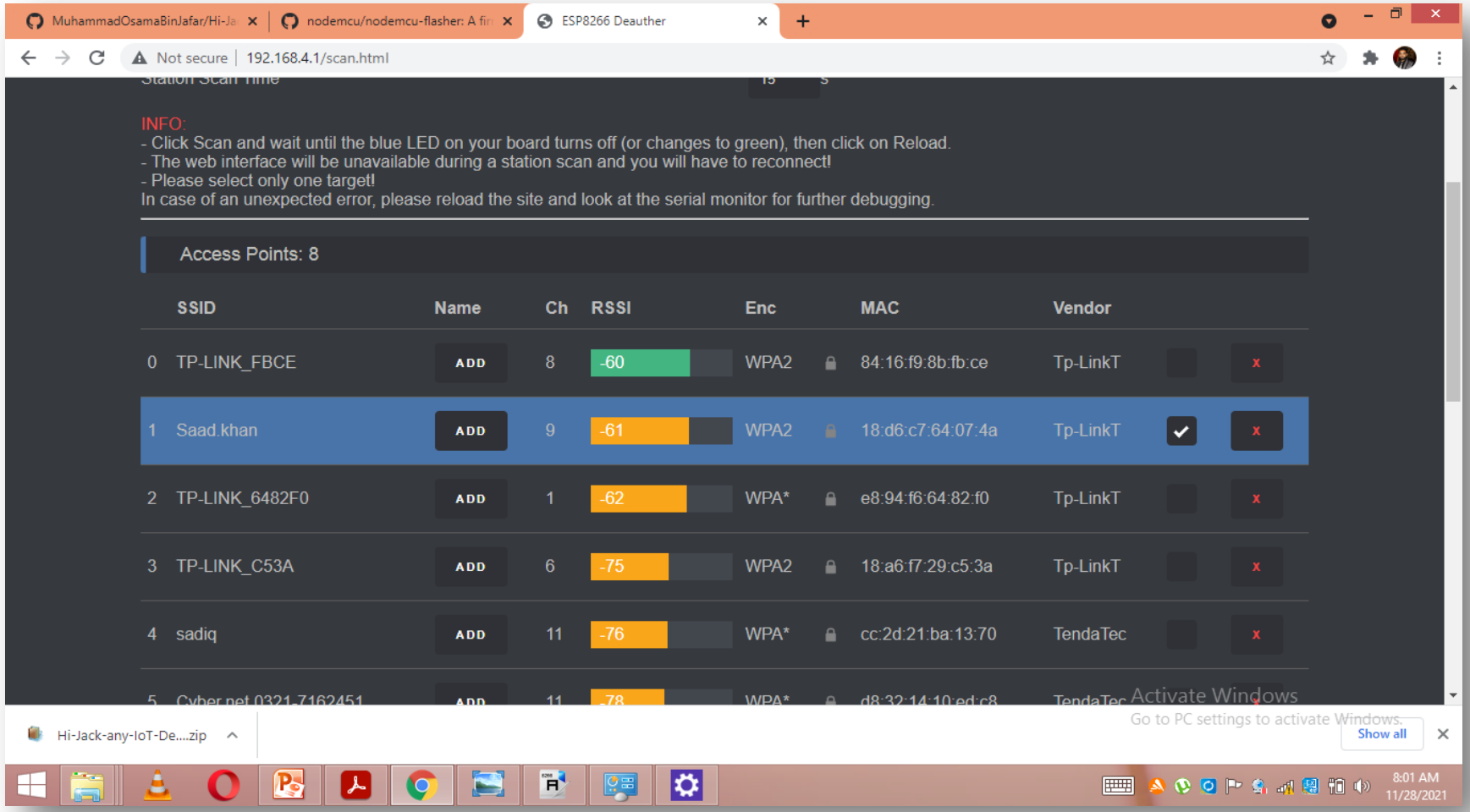
scan IoT devices

Scan all IoT Devices within range of your nodeMCU by cliciking on scan and then press reload in html of **192.168.4.1**



Target device

- In my case I target my home network , Use it only against your own networks and devices



Attack on target

Deauth

Closes the connection of WiFi devices by sending deauthentication frames to access points and client devices you selected.
This is only possible because a lot of devices don't use the 802.11w-2009 standard that offers a protection against this attack.
Please only select one target! When you select multiple targets that run on different channels and start the attack, it will quickly switch between those channels and you have no chance to reconnect to the access point that hosts this web interface.

Beacon

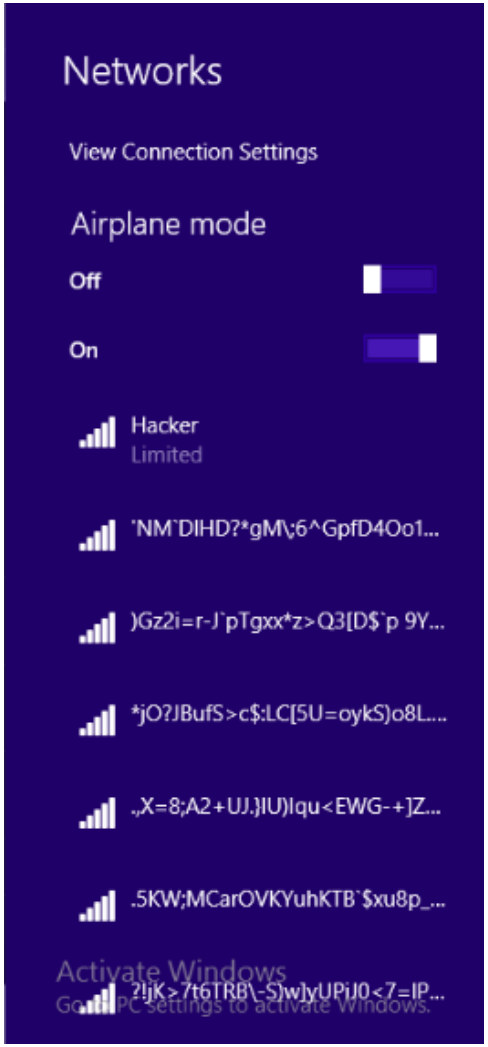
Beacon packets are used to advertise access points. By continuously sending beacon packets out, it will look like you created new WiFi networks.
You can specify the network names under SSIDs.

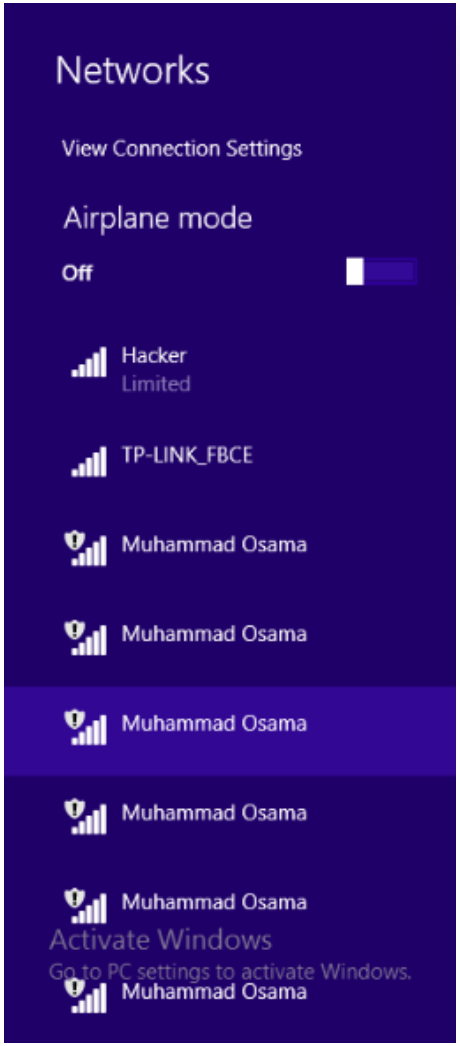
Probe

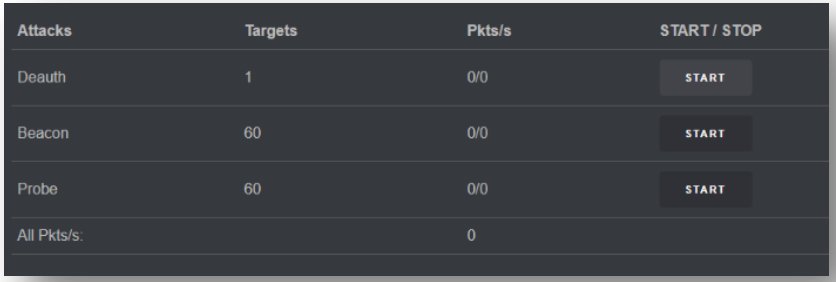
Probe requests are sent by client devices to ask if a known network is nearby.
Use this attack to confuse WiFi trackers by asking for networks that you specified in the SSID list.
It's unlikely you will see any impact by this attack with your home network.

Attacks	Targets	Pkts/s	START / STOP
Deauth	1	0/0	START
Beacon	60	0/0	START
Probe	60	0/0	START
All Pkts/s:		0	

I used deauth to target for disconnect all devices with target and then simulataneoulsy used beacon for 60 new networks and prob to confuse device WiFi trackers by asking for networks that you specified in the SSID list.







Attacks	Targets	Pkts/s	START / STOP
Deauth	1	0/0	START
Beacon	60	0/0	START
Probe	60	0/0	START
All Pkts/s:		0	

This project is only for educational purpose use it only against your own devices It uses valid Wi-Fi frames described in the IEEE 802.11 standard and does not block or disrupt any frequencies.
Please check the legal regulations in your country before using it.

Devoted to all my Teachers
~Muhammad Osama Bin Jafar