



# Dept of Mathematics

## Hi-jack any IoT device Using Lua scripting language

**WARNING**

Transmitting death 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 integrated with Wi-Fi SoC.

# Using driver

CP210x USB to UART Bridge  
VCP Drivers



## **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

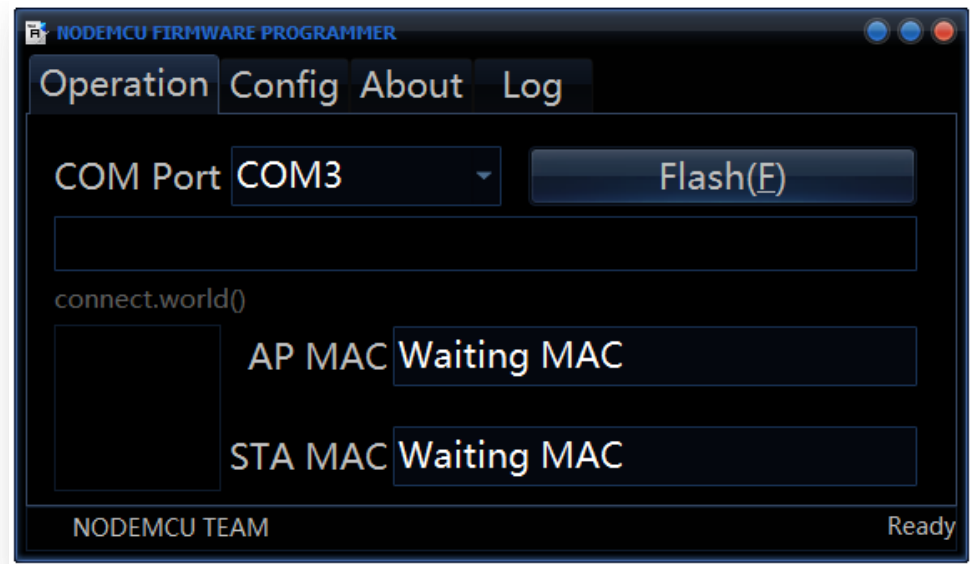
# NODEMCU flashing tool

## 🔗 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

The screenshot shows a web browser window displaying a GitHub repository page. The repository is named "MuhammadOsamaBinJafar / Hi-Jack-any-IoT-Device" and is public. The page includes a navigation bar with links for "Code", "Issues", "Pull requests", "Actions", "Projects", "Wiki", "Security", "Insights", and "Settings". The "Code" dropdown menu is open, showing options to "Clone" (via HTTPS, SSH, or GitHub CLI), "Open with GitHub Desktop", and "Download ZIP". The "Download ZIP" option is highlighted. The repository's main branch is "main", and it has 1 branch and 0 tags. The repository's description states: "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". The repository's files list includes ".gitattributes", "Hi-Jack any IoT Device.rar", and "code.lua". The repository's releases section shows "No releases published" and a link to "Create a new release". The repository's URL is "https://github.com/MuhammadOsamaBinJafar/Hi-Jack-any-IoT-Device/archive/refs/heads/main.zip". The browser's address bar shows the URL, and the taskbar at the bottom displays various application icons and the system clock showing 6:47 AM on 11/28/2021.

MuhammadOsamaBinJafar / Hi-Jack-any-IoT-Device Public

Unwatch 1 Unstar 1 Fork 0

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

main 1 branch 0 tags

MuhammadOsamaBinJafar Create code.lua

.gitattributes Update .gitattributes

Hi-Jack any IoT Device.rar Add files via upload

code.lua Create code.lua

Help people interested in this repository understand your project by adding a README file.

Go to file Add file Code

Clone ?

HTTPS SSH GitHub CLI

https://github.com/MuhammadOsamaBinJafar/Hi-Jack-any-IoT-Device/archive/refs/heads/main.zip

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Download ZIP

About

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

Releases

No releases published

Create a new release

Activate Windows

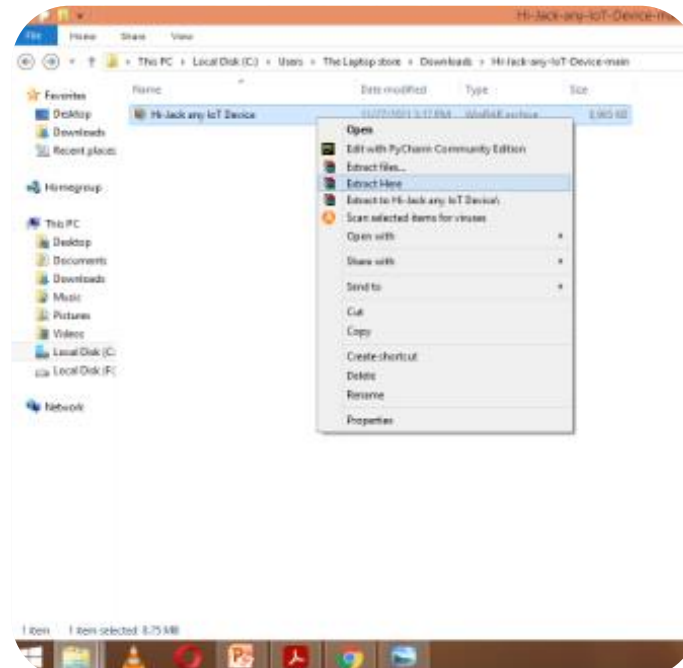
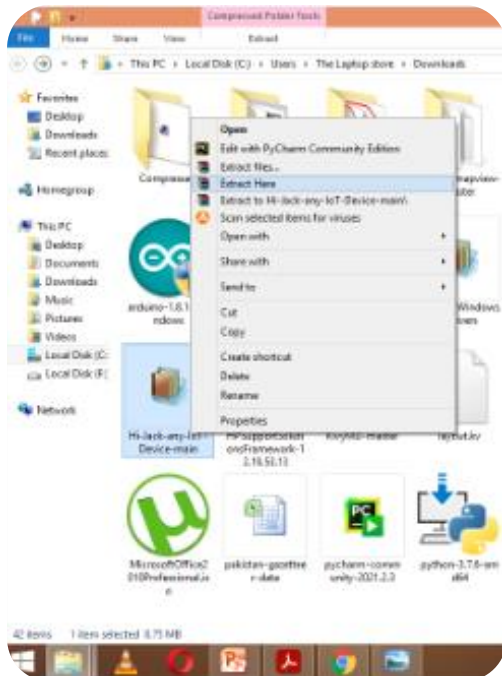
Go to PC settings to activate Windows.

Show all

Hi-Jack-any-IoT-De....zip

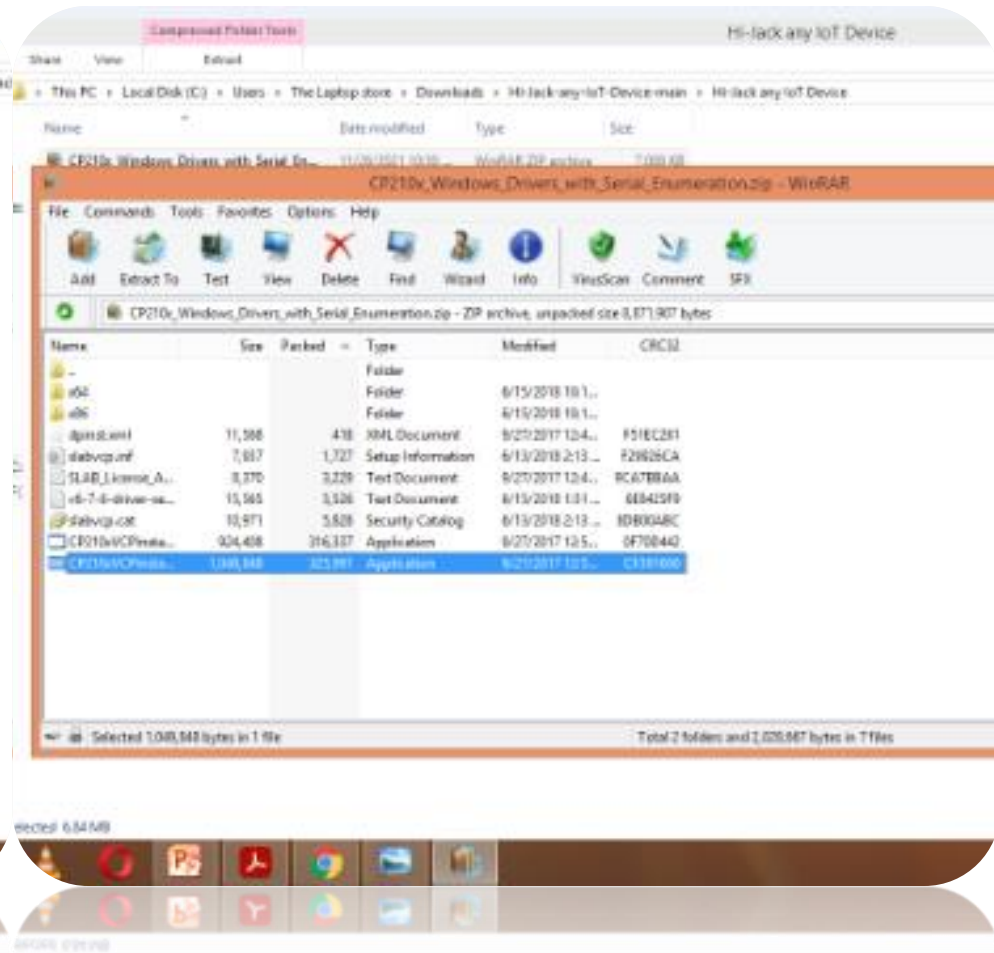
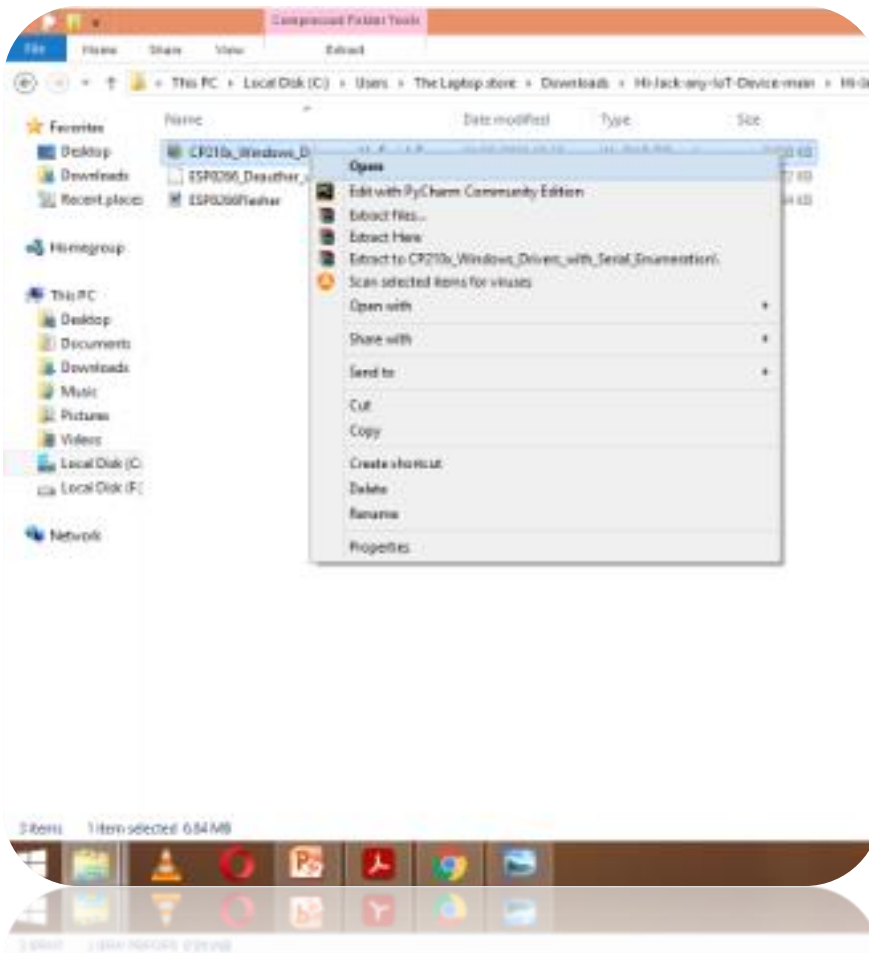
6:47 AM 11/28/2021

# Extracting zip file



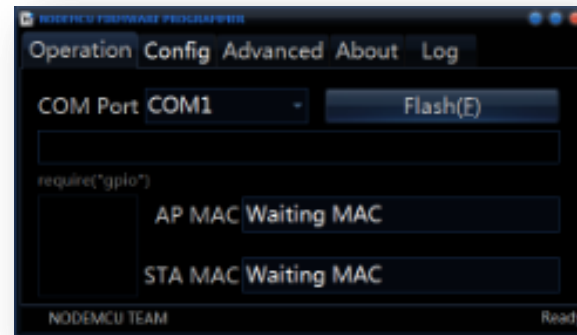
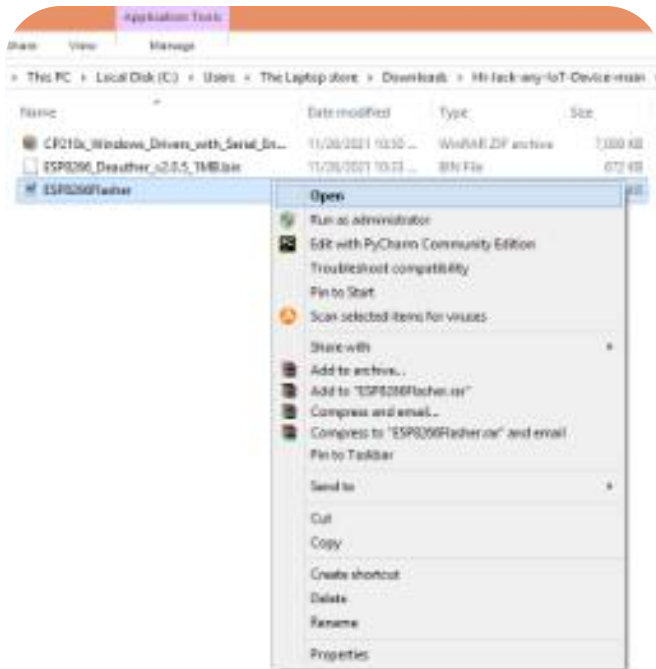


# Installing The CP210x USB to UART Bridge Virtual COM Port (VCP) drivers

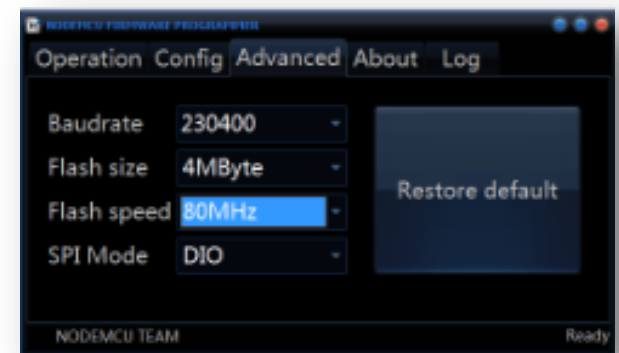




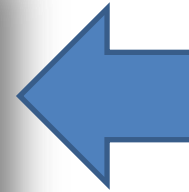
# Installing nodeMCU flasher and configuring it



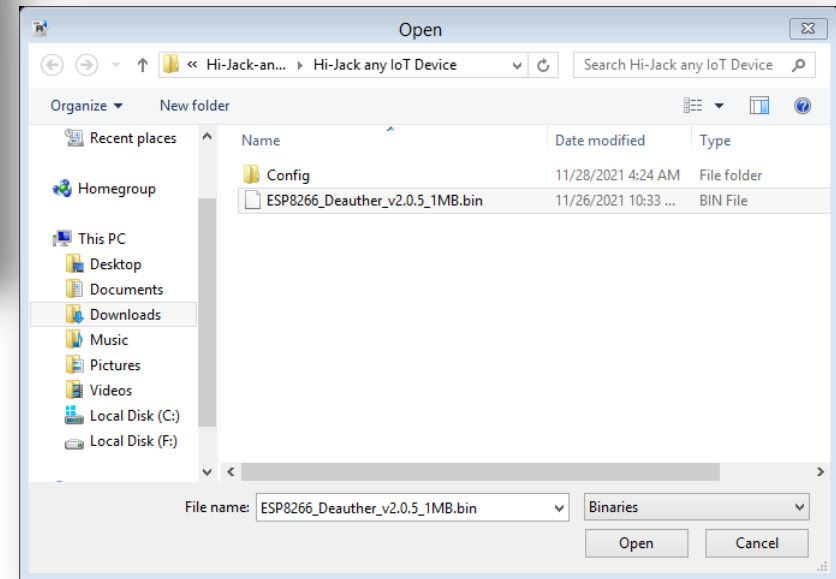
Then configure it to



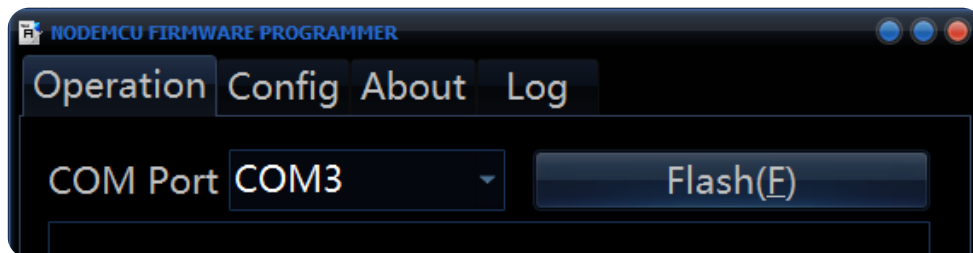
Connect your nodeMCU by using good quality cable  
and upload code in it



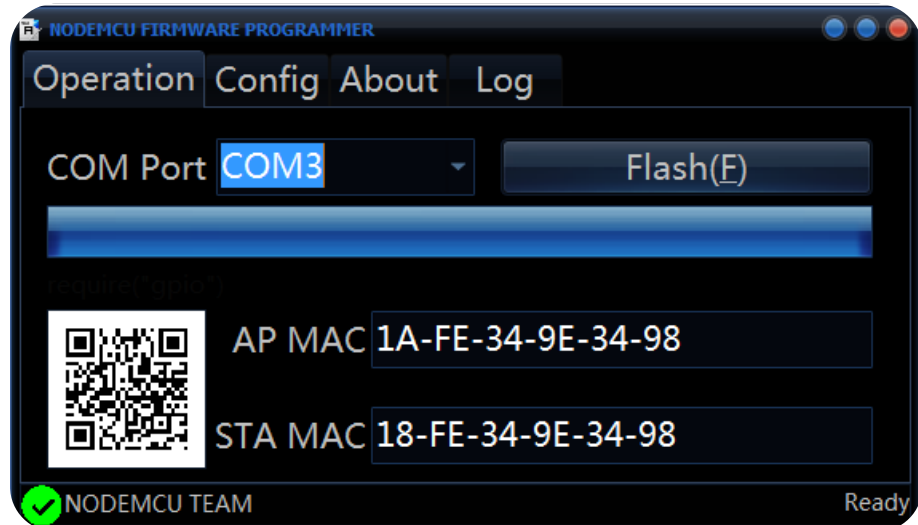
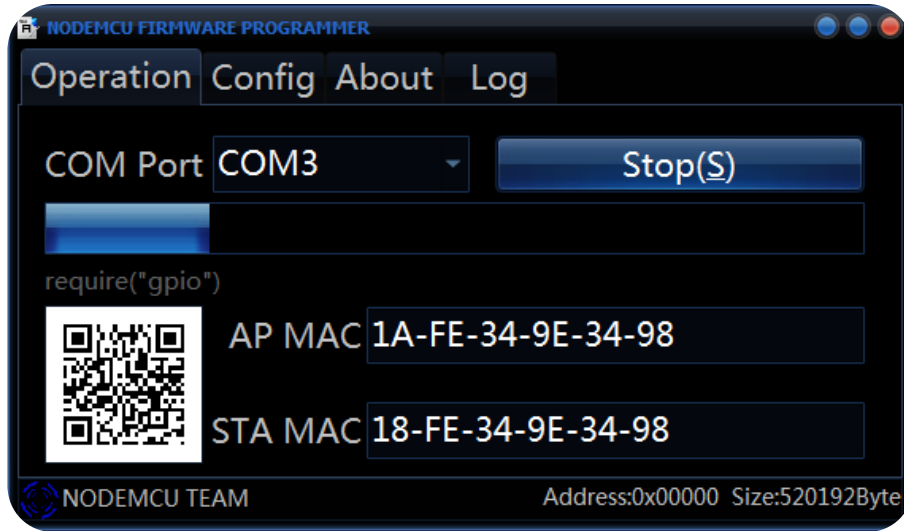
Click ot it and Select binary file  
ESP8266\_Deauther\_v2.0.5\_1MB.bin



Then click on flash f

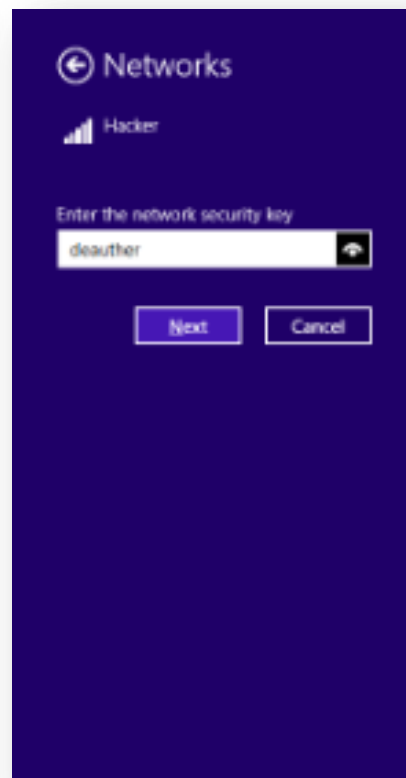
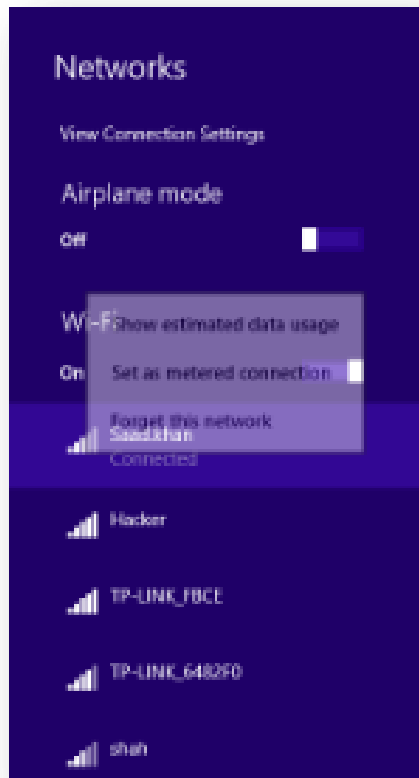


# Uploading code in nodeMCU is successful



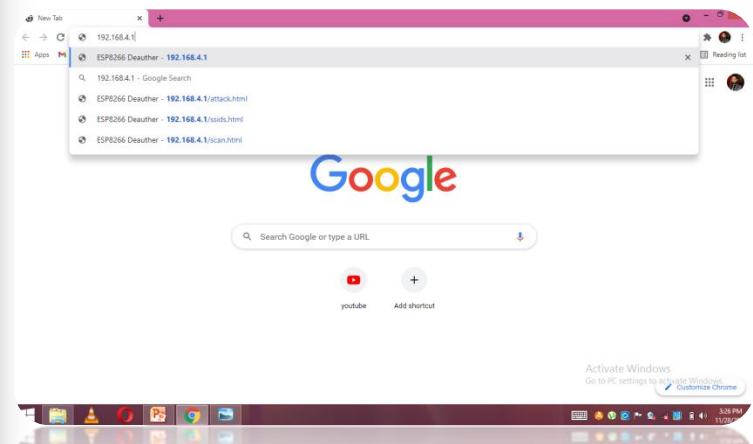
Now connect with pwned, new WI-FI network  
and go to ip address **192.168.4.1**

- 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 clicking on scan and then press reload in html of [192.168.4.1](http://192.168.4.1)

Scan

SCAN APS SCAN STATIONS RELOAD

Channel All

Station Scan Time 15 s

**INFO:**

- Click Scan and wait until the blue LED on your board turns off (or changes to green), then click on Reload.
- The web interface will be unavailable during a station scan and you will have to reconnect!
- Please select only one target!

In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

Access Points: 8

	SSID	Name	Ch	RSSI	Enc	MAC	Vendor		
0	TP-LINK_FBCE	ADD	8	-60	WPA2	84:16:f9:8b:fb:ce	Tp-LinkT		x
1	Saad.khan	ADD	9	-61	WPA2	18:d6:c7:64:07:4a	Tp-LinkT		x
2	TP-LINK_6482F0	ADD	1	-62	WPA*	e8:94:f6:64:82:f0	Tp-LinkT		x

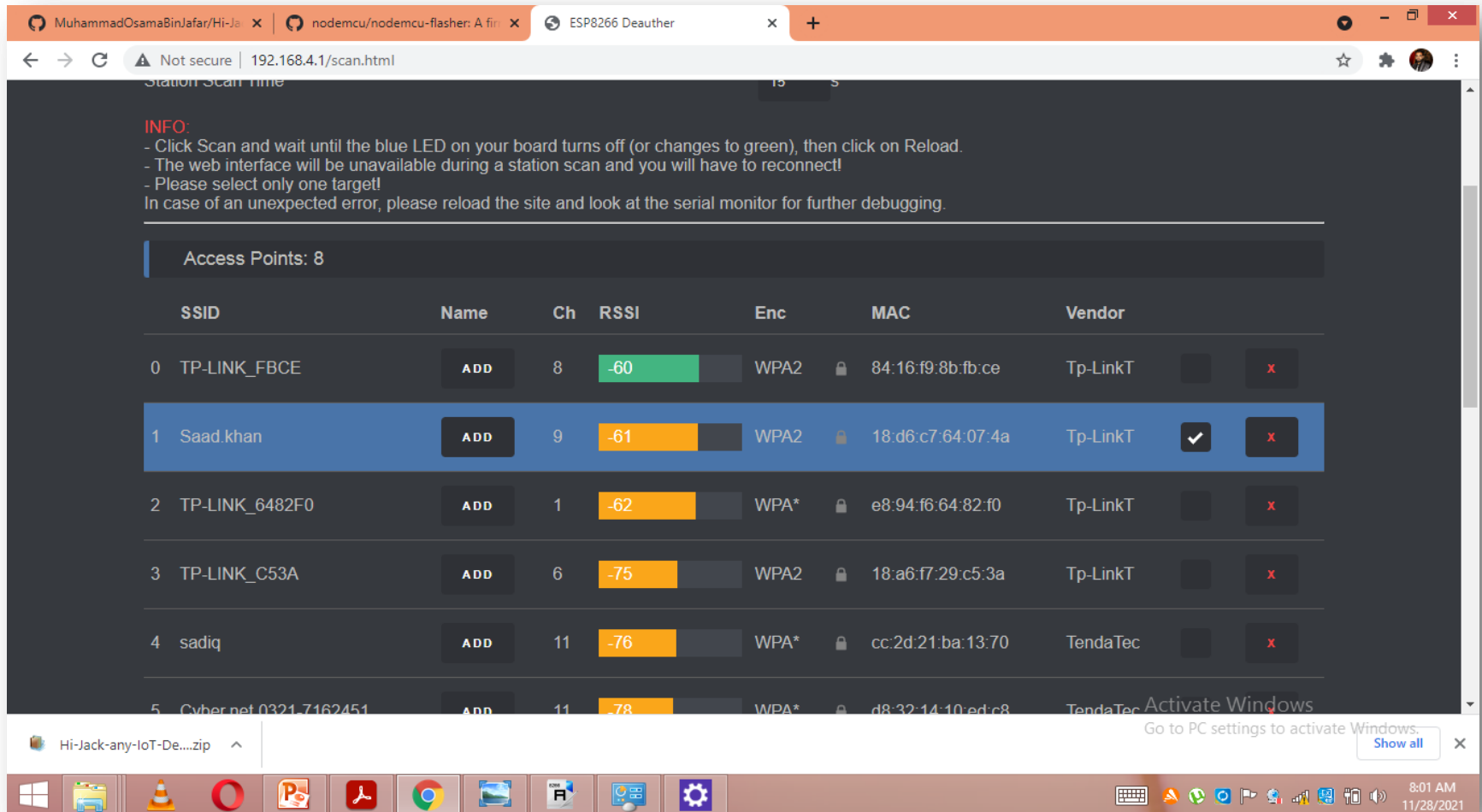
Hi-Jack-any-IoT-De...zip

Activate Windows. Go to PC settings to activate Windows. Show all

8:01 AM 11/28/2021

# Target device

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



Station Scan time

INFO:

- Click Scan and wait until the blue LED on your board turns off (or changes to green), then click on Reload.
- The web interface will be unavailable during a station scan and you will have to reconnect!
- Please select only one target!

In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

Access Points: 8

	SSID	Name	Ch	RSSI	Enc	MAC	Vendor		
0	TP-LINK_FBCE	ADD	8	-60	WPA2	84:16:f9:8b:fb:ce	Tp-LinkT		x
1	Saad.khan	ADD	9	-61	WPA2	18:d6:c7:64:07:4a	Tp-LinkT	✓	x
2	TP-LINK_6482F0	ADD	1	-62	WPA*	e8:94:f6:64:82:f0	Tp-LinkT		x
3	TP-LINK_C53A	ADD	6	-75	WPA2	18:a6:f7:29:c5:3a	Tp-LinkT		x
4	sadiq	ADD	11	-76	WPA*	cc:2d:21:ba:13:70	TendaTec		x
5	Cyber.net.0321-7162451	ADD	11	-78	WPA*	d8:32:14:10:ed:c8	TendaTec		x

Hi-Jack-any-IoT-De...zip

Activate Windows. Go to PC settings to activate Windows. Show all

8:01 AM 11/28/2021

# 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

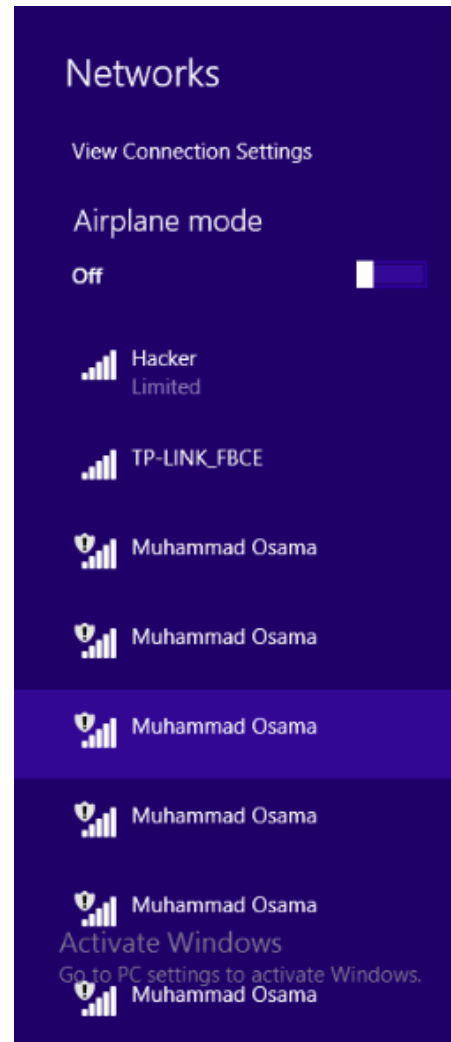
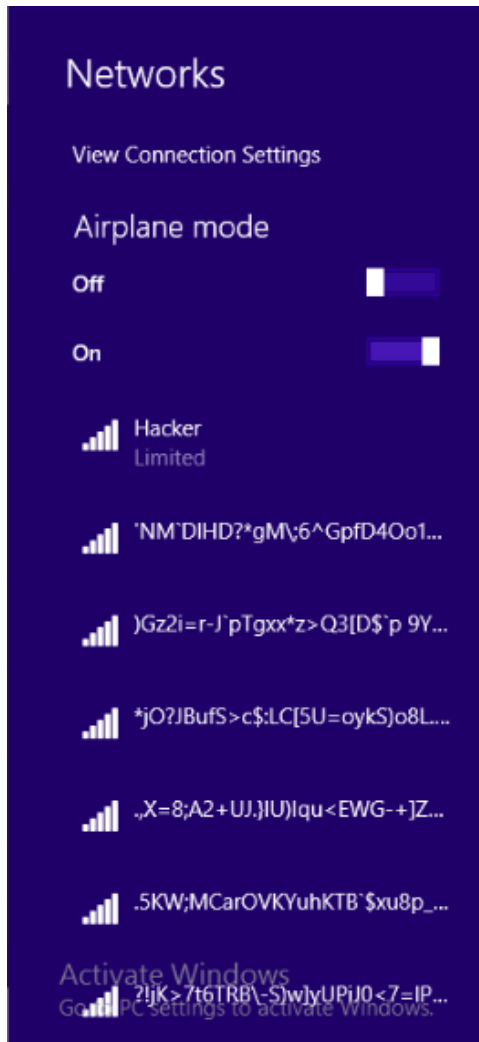
Probe requests are sent by client devices to ask if a known network is nearby. Use this attack to confuse WiFi trackers by asking for networks that you specified in the SSID list. It's unlikely you will see any impact by this attack with your home network.

MAPS ONLINE

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 simultaneously 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**