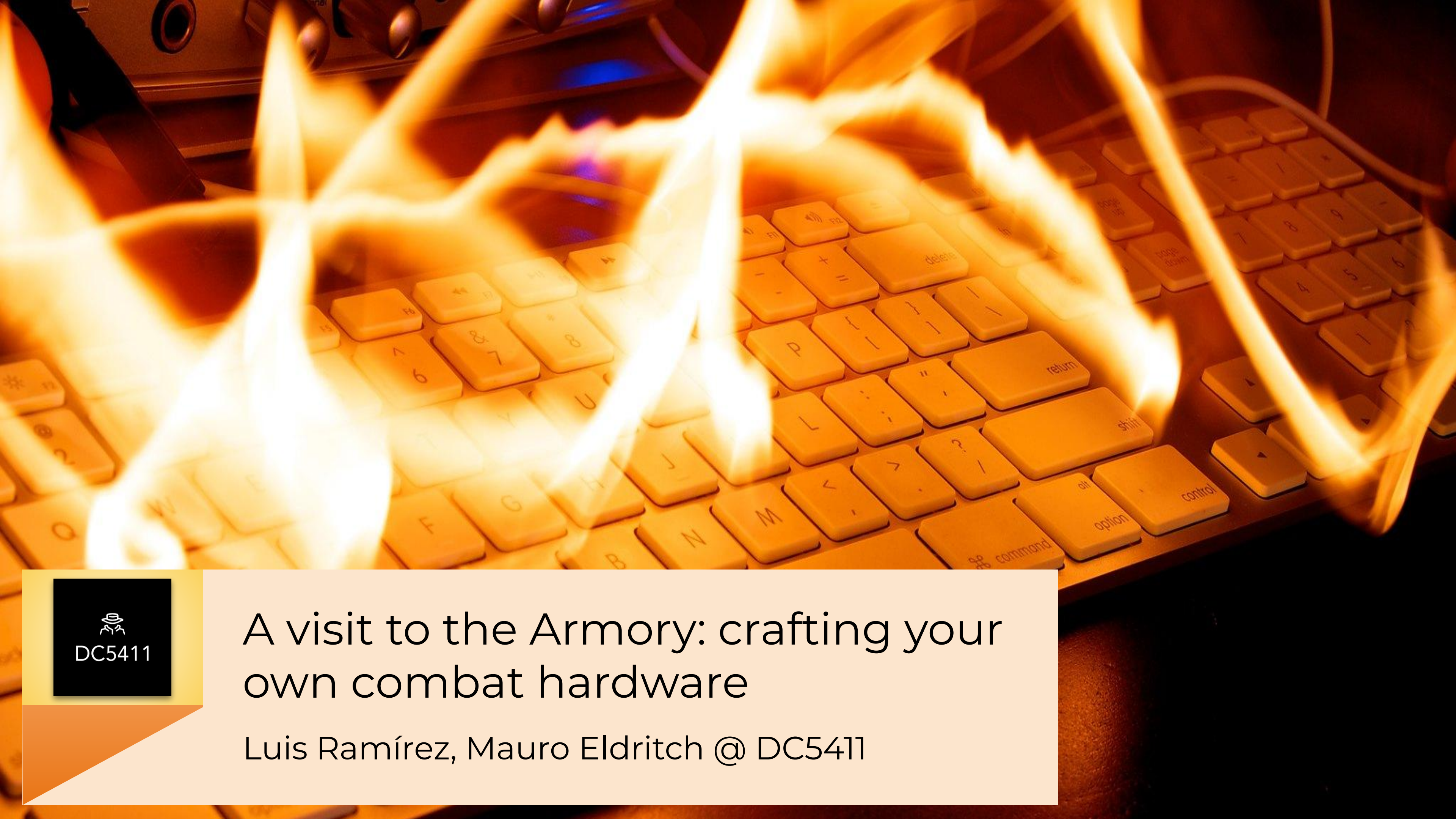


DC5411

A visit to the Armory: crafting your own combat hardware

Luis Ramírez, Mauro Eldritch @ DC5411

Boot

A brief introduction

whoami

🇦🇷 Mauro Eldritch

- Founder @ **BCA** 🇬🇧.
- Founder @ **DC5411** 🇦🇷 🇺🇾.
- Speaker @ **DEFCON** 🇺🇸 (x8: Adversary, Red Team, Hardware Hacking, Data Duplication, & Recon Villages), DevFest Siberia 🇷🇺, DC7831 Nizhny Novgorod 🇷🇺, ROADSEC 🇧🇷, DragonJAR 🇨🇴, P0SCon 🇮🇷, Texas Cyber Summit 🇺🇸, **EC-Council Hacker Halted** 🇺🇸, BSides NCL 🇬🇧, YASCon 🇮🇳, BSides Islamabad 🇵🇰, HoneyCon 🇪🇸, GrayHat 🇺🇸, BSides Panamá 🇵🇦, Conhesi 🇵🇪, Cyberdome Summit 🇮🇳, **Ruby Kaigi** 🇯🇵, BugCON 🇲🇽, ROOTCON 🇵🇭.

whoami

🇨🇴 Luis Ramírez

- Security Hardware Engineer @ **BCA** 🇬🇧.
- Member @ **DC5411** 🇦🇷 🇺🇾.
- Speaker @ **DEFCON** 🇺🇸, DragonJAR 🇨🇴, P0SCon 🇮🇷, Texas Cyber Summit 🇺🇸, GrayHat 🇺🇸, BSides NCL 🇬🇧, YASCon 🇮🇳, BSides Islamabad 🇵🇰, HoneyCon 🇪🇸, Conhesi 🇵🇪, ROOTCON 🇵🇭.

README

Our Armory consists of all sorts of weaponized domestic hardware and infiltration devices (BadUSB power banks, speakers, keyboards, and even an entire BadUSB Framework), which are available as open-source projects

In this talk, we would like to present two of our newest Hardware Hacking experiments:

Smart Movement Sensors 🏃

DeAuther Charges 📴

Surveillance Suite 👁️

README

DC5411
IoT
Eyes Of Ligeia
Eyes Of Ligeia Cam
Eyes Of Ligeia Cam
Eyes Of Ligeia Cam
Eyes Of Ligeia Sensor
Eyes Of Ligeia Sensor
Eyes Of Ligeia Sensor

LICENSE

These projects have open-source versions available at Github.

Pay us a visit at **Github: dc5411/armory** to see all of our open source projects.

Feel free to clone, contribute and build your own tools.

⚙

Sensors

Freeze! Don’t move!

Sensors

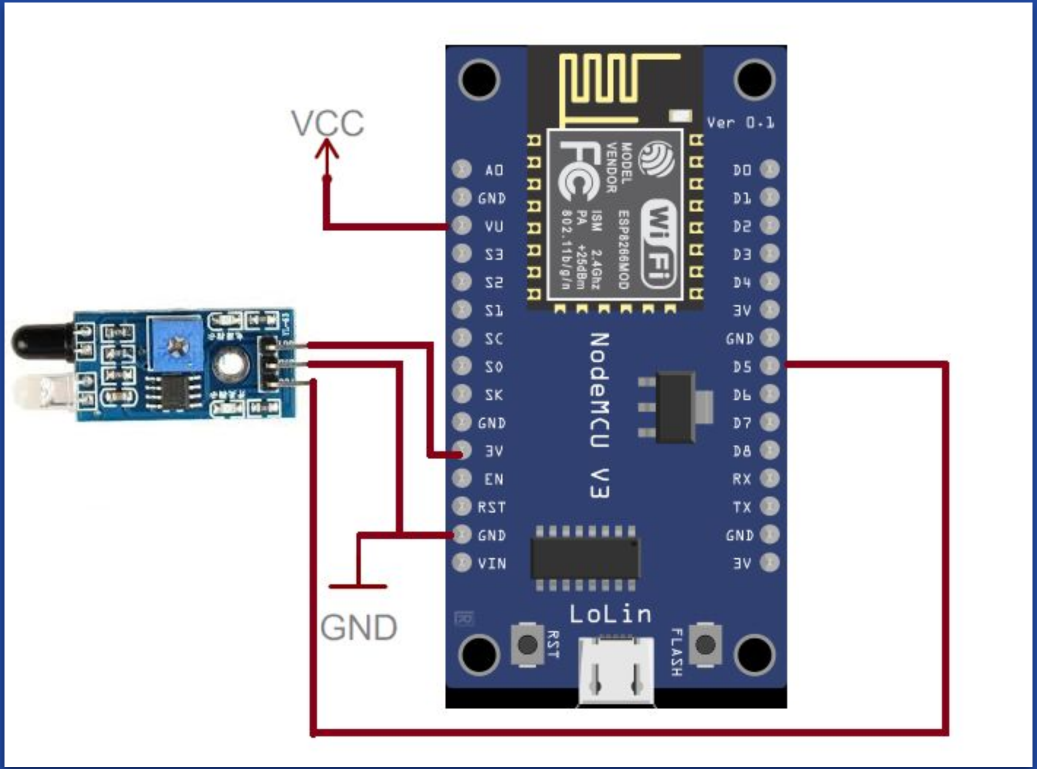
⚙️ Hardware

ESP8266
Infrared Sensor
9v Battery
Power Switch
Disguise Case (3D printed, or an existing object)
Adhesive patch / double-faced tape

💾 Software

BCA’s Firmware
C2 Server: PHP + MySQL + BCA C2 WebApp (Docker-enabled)
Client: BCA Client WebApp or BCA Mobile APK

Sensors


VCC
GND
A0
GND
VU
S3
S2
S1
SC
S0
SK
GND
3V
EN
RST
GND
VIN
D0
D1
D2
D3
D4
3V
GND
D5
D6
D7
D8
RX
TX
GND
3V
Ver 0.1
NodeMCU V3
LoLin
RST
FLASH
ESP8266MOD
ISM 2.4Ghz
PA +25dBm
802.11b/g/n

Sensors

Procedure

🏃 Sensors need a WiFi connection in order to work.

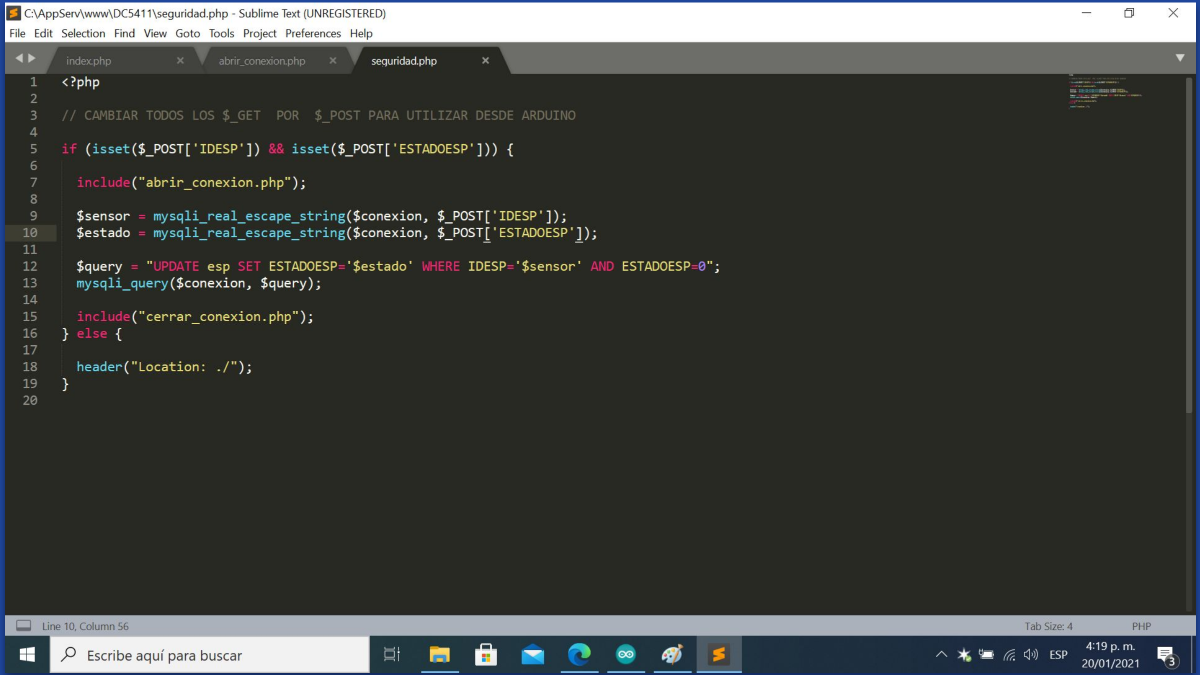
🏃 Depending on the task, Operators can either use a phone as a hotspot to share its LTE connection via WiFi and bind the sensors (short coverage), or use a portable hotspot device for longer coverage.

🏃 Both the sensors and the phone will interact via the Command and Control Server (C2), located outside the premises.

🏃 Whenever something alters a sensor, it will send a push notification to the Operator’s mobile phone, and turn itself red in the WebGUI and/or the App.

Sensors

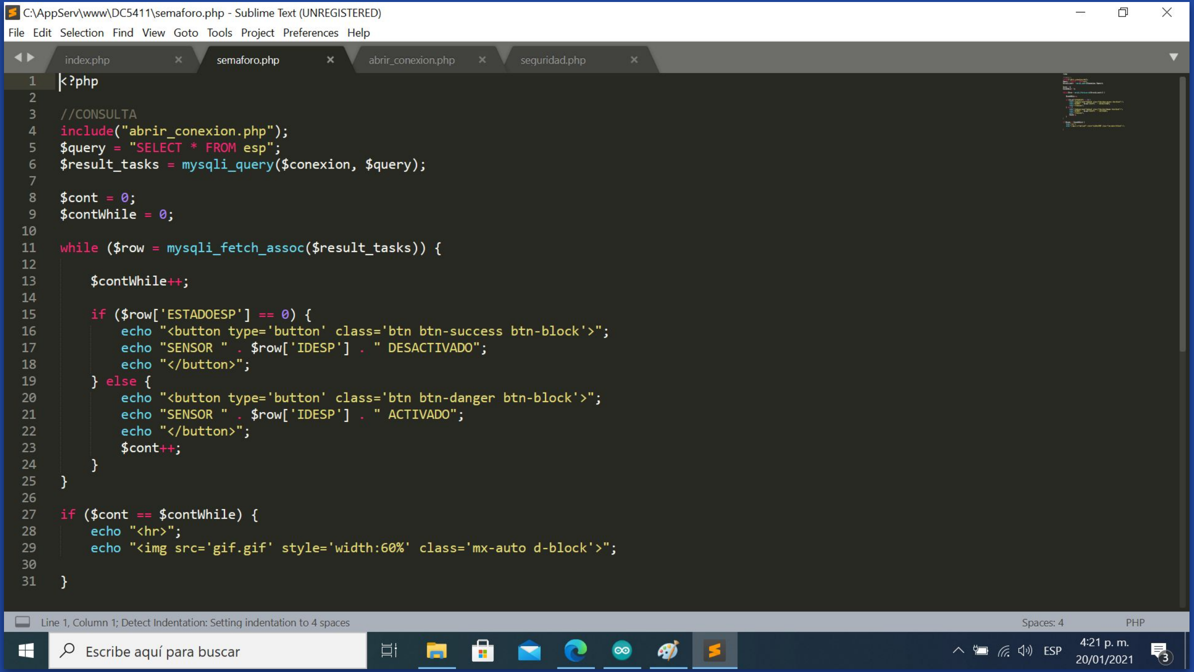
Database connection


C:\AppServ\www\DC5411\seguridad.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
index.php
abrir_conexion.php
seguridad.php
Line 10, Column 56
Tab Size: 4
PHP
Escribe aquí para buscar
ESP
4:19 p. m.
20/01/2021

```php
<?php

// CAMBIAR TODOS LOS $_GET  POR  $_POST PARA UTILIZAR DESDE ARDUINO

if (isset($_POST['IDESP']) && isset($_POST['ESTADOESP'])) {

  include("abrir_conexion.php");

  $sensor = mysqli_real_escape_string($conexion, $_POST['IDESP']);
  $estado = mysqli_real_escape_string($conexion, $_POST['ESTADOESP']);

  $query = "UPDATE esp SET ESTADOESP='$estado' WHERE IDESP='$sensor' AND ESTADOESP=0";
  mysqli_query($conexion, $query);

  include("cerrar_conexion.php");
} else {

  header("Location: ./");
}

```

Sensors

Database connection

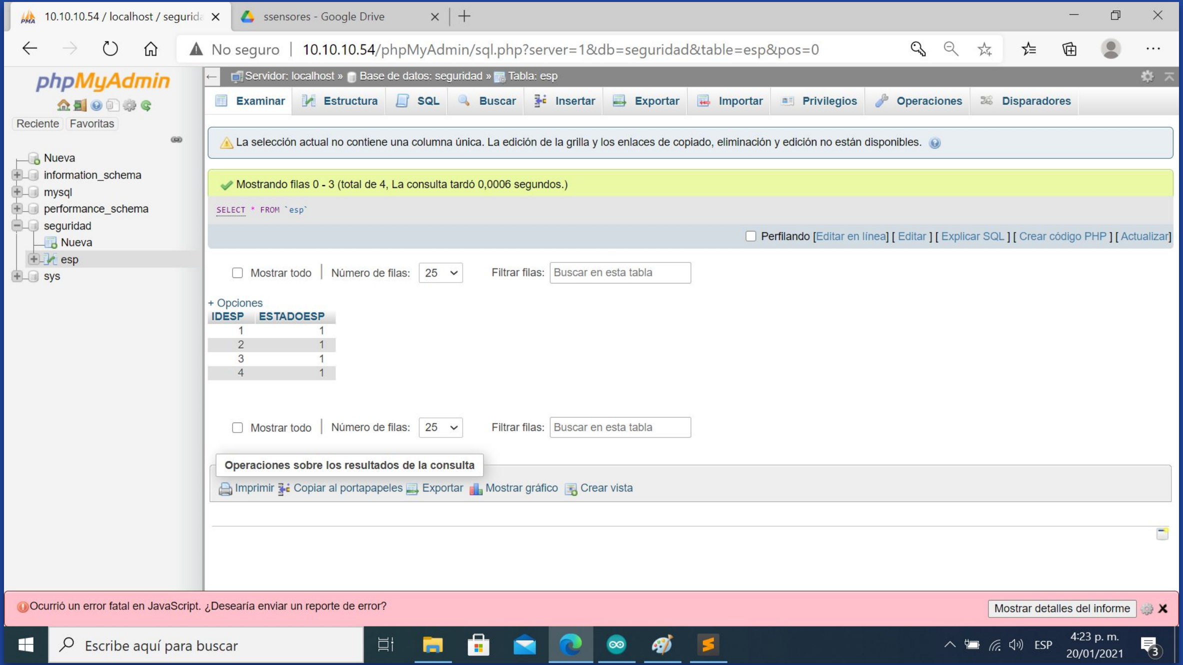

C:\AppServ\www\DC5411\semaforo.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
index.php
semaforo.php
abrir_conexion.php
seguridad.php
Spaces: 4
PHP
Escribe aquí para buscar
ESP
4:21 p. m.
20/01/2021

```php
<?php

//CONSULTA
include("abrir_conexion.php");
$query = "SELECT * FROM esp";
$result_tasks = mysqli_query($conexion, $query);

$cont = 0;
$contWhile = 0;

while ($row = mysqli_fetch_assoc($result_tasks)) {

    $contWhile++;

    if ($row['ESTADOESP'] == 0) {
        echo "<button type='button' class='btn btn-success btn-block'>";
        echo "SENSOR " . $row['IDESP'] . " DESACTIVADO";
        echo "</button>";
    } else {
        echo "<button type='button' class='btn btn-danger btn-block'>";
        echo "SENSOR " . $row['IDESP'] . " ACTIVADO";
        echo "</button>";
        $cont++;
    }
}

if ($cont == $contWhile) {
    echo "<hr>";
    echo "<img src='gif.gif' style='width:60%' class='mx-auto d-block'>";

}
```

Line 1, Column 1; Detect Indentation: Setting indentation to 4 spaces

Sensors

Database backend (phpMyAdmin)



La selección actual no contiene una columna única. La edición de la grilla y los enlaces de copiado, eliminación y edición no están disponibles.

Mostrando filas 0 - 3 (total de 4, La consulta tardó 0,0006 segundos.)

```
SELECT * FROM `esp`
```

□ Mostrar todo | Número de filas: 25 Filtrar filas: Buscar en esta tabla

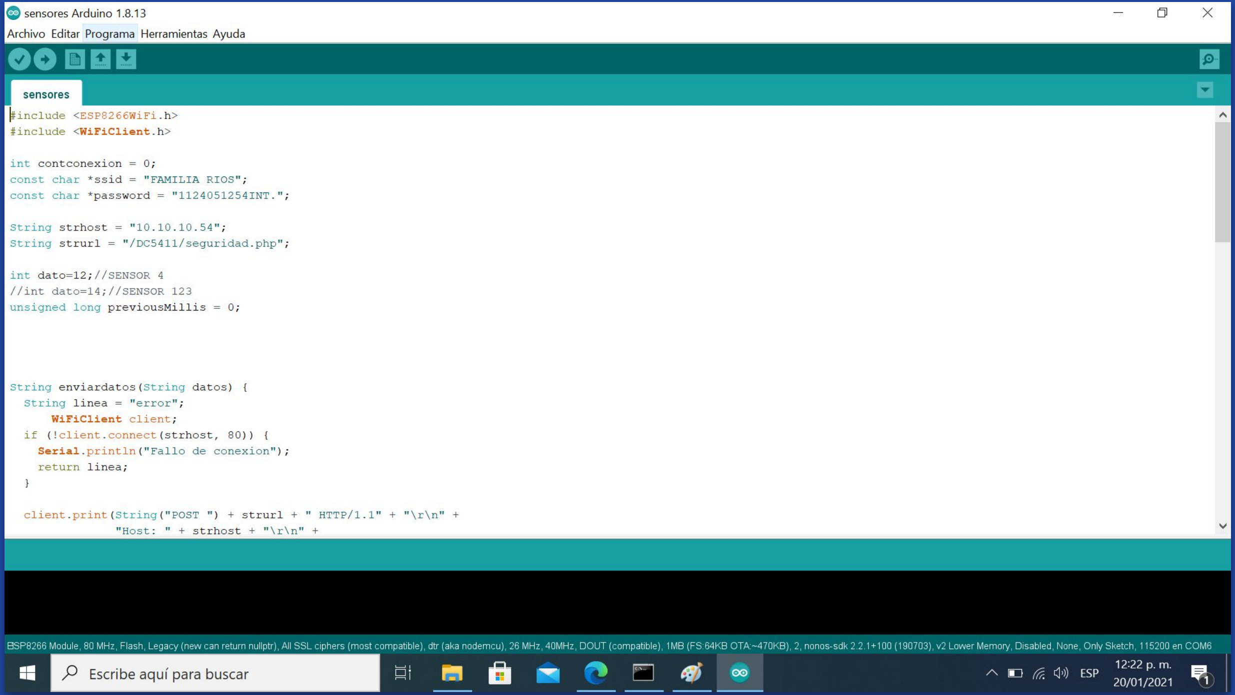
IDESP	ESTADOESP
1	1
2	1
3	1
4	1

□ Mostrar todo | Número de filas: 25 Filtrar filas: Buscar en esta tabla

Ocurrió un error fatal en JavaScript. ¿Desearía enviar un reporte de error?

Sensors

BCA’s firmware

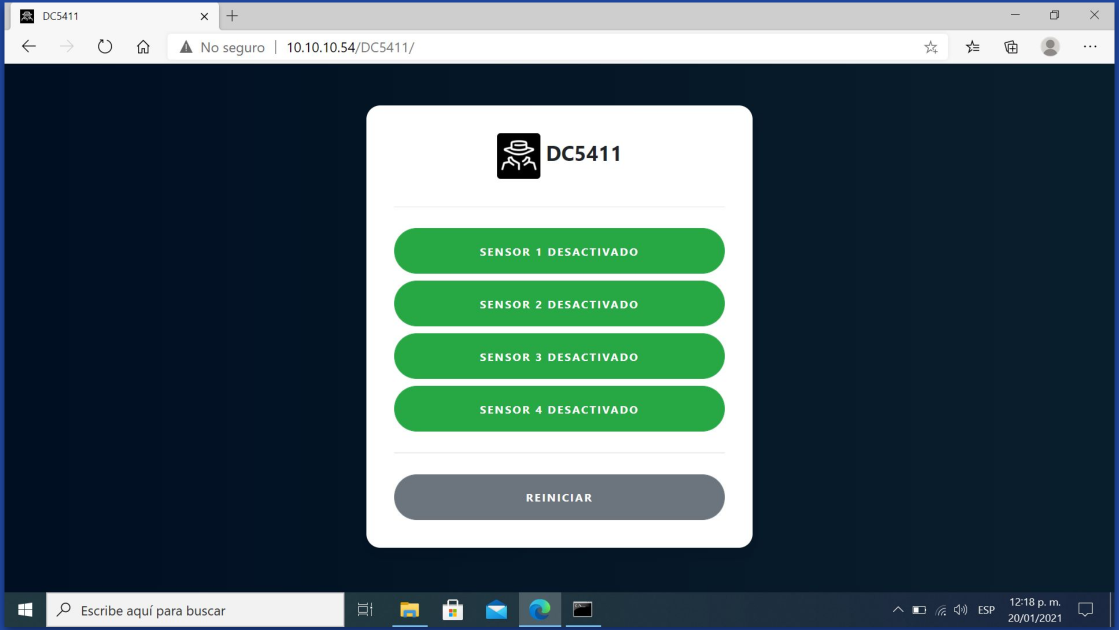


```
#include <ESP8266WiFi.h>
#include <WiFiClient.h>

int contconexion = 0;
const char *ssid = "FAMILIA RIOS";
const char *password = "1124051254INT.";

String strhost = "10.10.10.54";
String strurl = "/DC5411/seguridad.php";

int dato=12;//SENSOR 4
//int dato=14;//SENSOR 123
unsigned long previousMillis = 0;




String enviardatos(String datos) {
  String linea = "error";
      WiFiClient client;
  if (!client.connect(strhost, 80)) {
    Serial.println("Fallo de conexion");
    return linea;
  }

  client.print(String("POST ") + strurl + " HTTP/1.1" + "\r\n" +
               "Host: " + strhost + "\r\n" +
```

ESP8266 Module, 80 MHz, Flash, Legacy (new can return nullptr), All SSL ciphers (most compatible), dtr (aka nodemcu), 26 MHz, 40MHz, DOUT (compatible), 1MB (FS:64KB OTA:~470KB), 2, nonos-sdk 2.2.1+100 (190703), v2 Lower Memory, Disabled, None, Only Sketch, 115200 en COM6

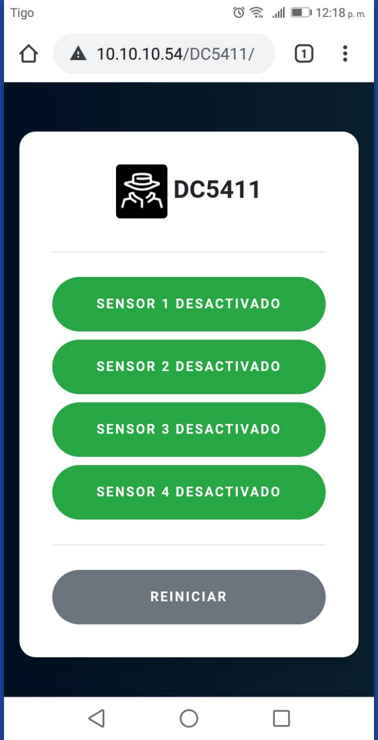
Sensors

webGUI (Thin Client / Desktop)



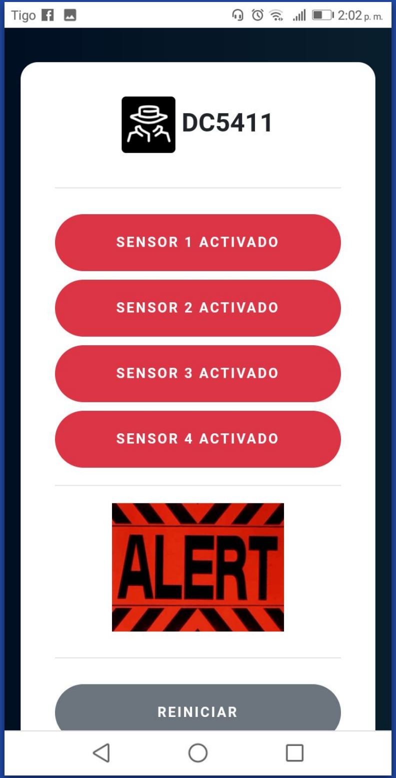
Sensors

webGUI (Thin Client / Mobile)



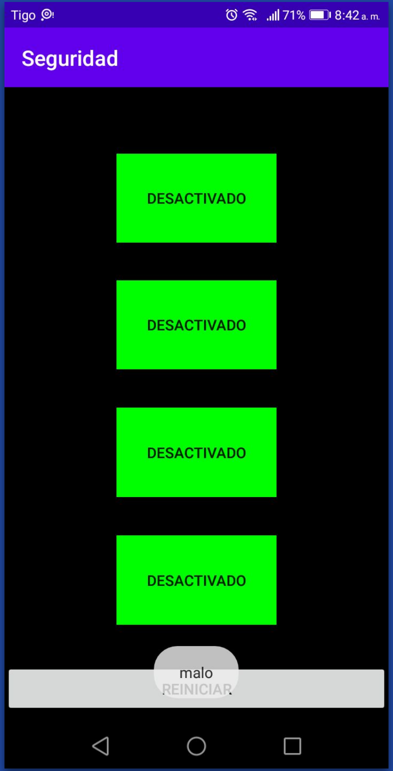
Sensors

webGUI (Thin Client / Mobile)



Sensors

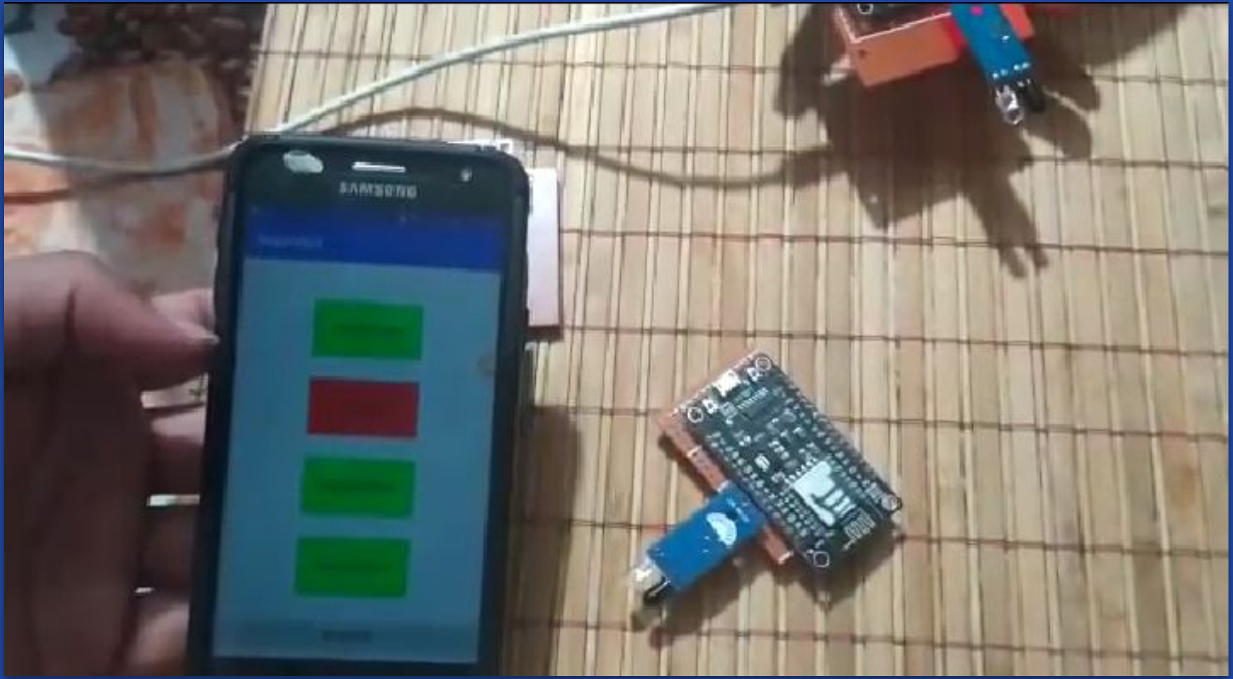
webGUI (Thick Client / Mobile)



malo

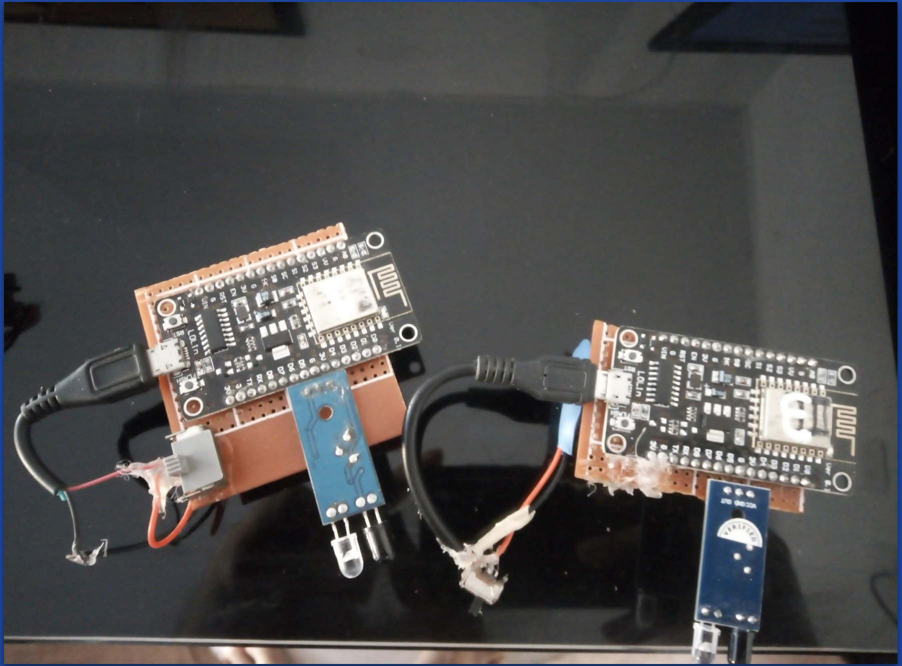
Sensors

Final product (without case)



Sensors

Final product (without case)



Sensors

Advantages over common sensors

🏃 Open Source and affordable.

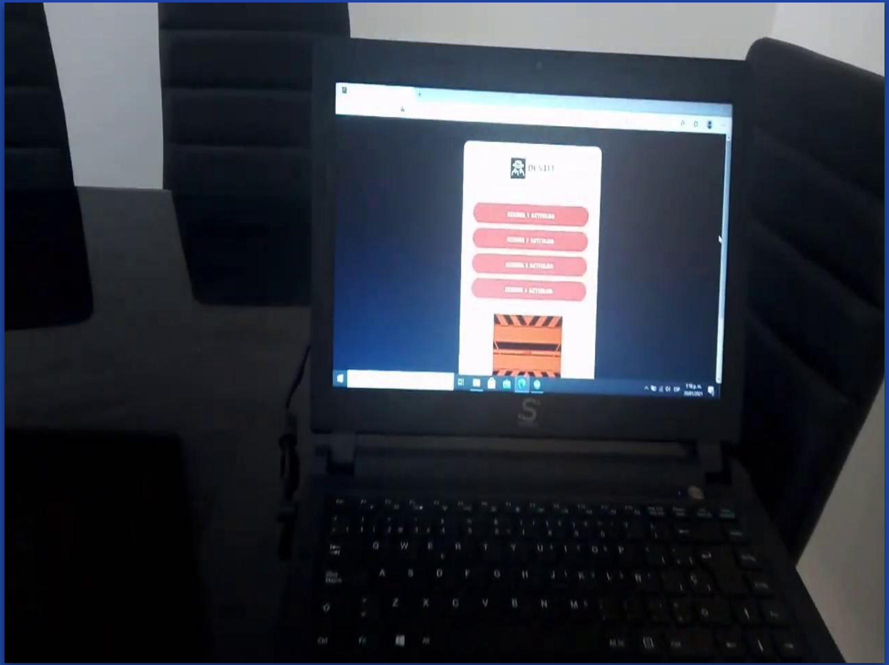
🏃 Scalable and extensible.

🏃 Smart, simple and intuitive User Interface.

🏃 Not tied to a single vendor-locked response (ring a bell, sound an alarm, etc). You can trigger any response, and extend the sensors capabilities by either adding custom affordable hardware (Arduino, for instance) or custom software.

Sensors

Demo



Charges

host is unreachable

Charges

⚙️ Hardware

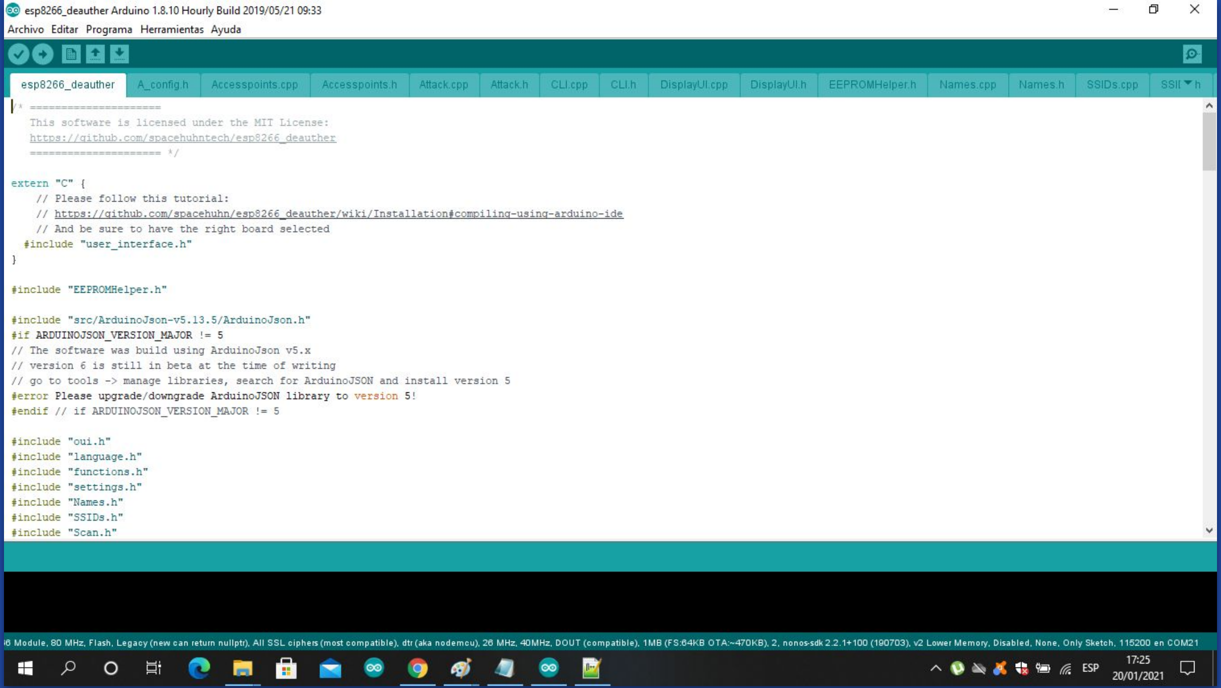
ESP8266
USB Power Bank
Power Switch
Case (3D Printed)
Adhesive patch

💾 Software

SpaceHuhn’s Firmware
BCA’s Firmware Patch

Charges

Spacehuhn’s firmware

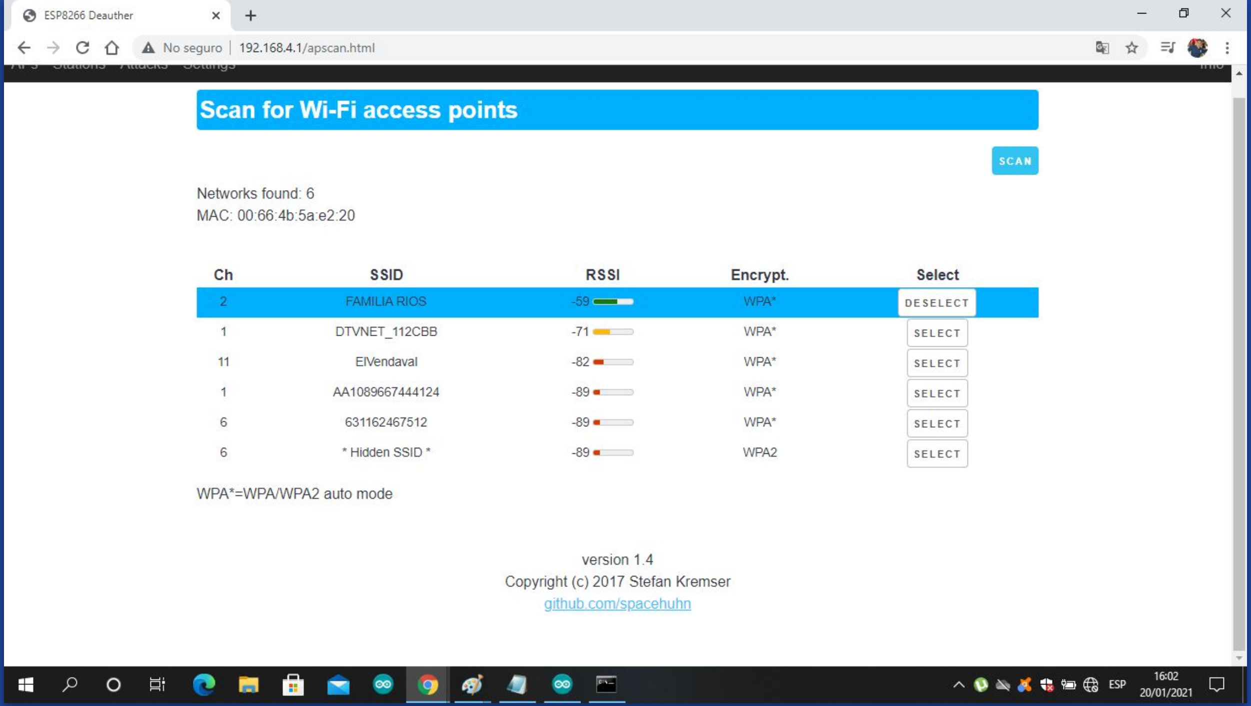


```
/* =====================
   This software is licensed under the MIT License:
   https://github.com/spacehuhntech/esp8266_deauther
   ===================== */

extern "C" {
    // Please follow this tutorial:
    // https://github.com/spacehuhn/esp8266_deauther/wiki/Installation#compiling-using-arduino-ide
    // And be sure to have the right board selected
  #include "user_interface.h"
}

#include "EEPROMHelper.h"

#include "src/ArduinoJson-v5.13.5/ArduinoJson.h"
#if ARDUINOJSON_VERSION_MAJOR != 5
// The software was build using ArduinoJson v5.x
// version 6 is still in beta at the time of writing
// go to tools -> manage libraries, search for ArduinoJSON and install version 5
#error Please upgrade/downgrade ArduinoJSON library to version 5!
#endif // if ARDUINOJSON_VERSION_MAJOR != 5

#include "oui.h"
#include "language.h"
#include "functions.h"
#include "settings.h"
#include "Names.h"
#include "SSIDs.h"
#include "Scan.h"
```

```
6 Module, 80 MHz, Flash, Legacy (new can return nullptr), All SSL ciphers (most compatible), dtr (aka nodemcu), 26 MHz, 40MHz, DOUT (compatible), 1MB (FS:64KB OTA:~470KB), 2, nonos-sdk 2.2.1+100 (190703), v2 Lower Memory, Disabled, None, Only Sketch, 115200 en COM21
```

Charges

Scans dashboard


ESP8266 Deauther
No seguro | 192.168.4.1/apscan.html
APs Stations Attacks Settings
Info
ESP
16:02
20/01/2021

Scan for Wi-Fi access points

SCAN

Networks found: 6
MAC: 00:66:4b:5a:e2:20

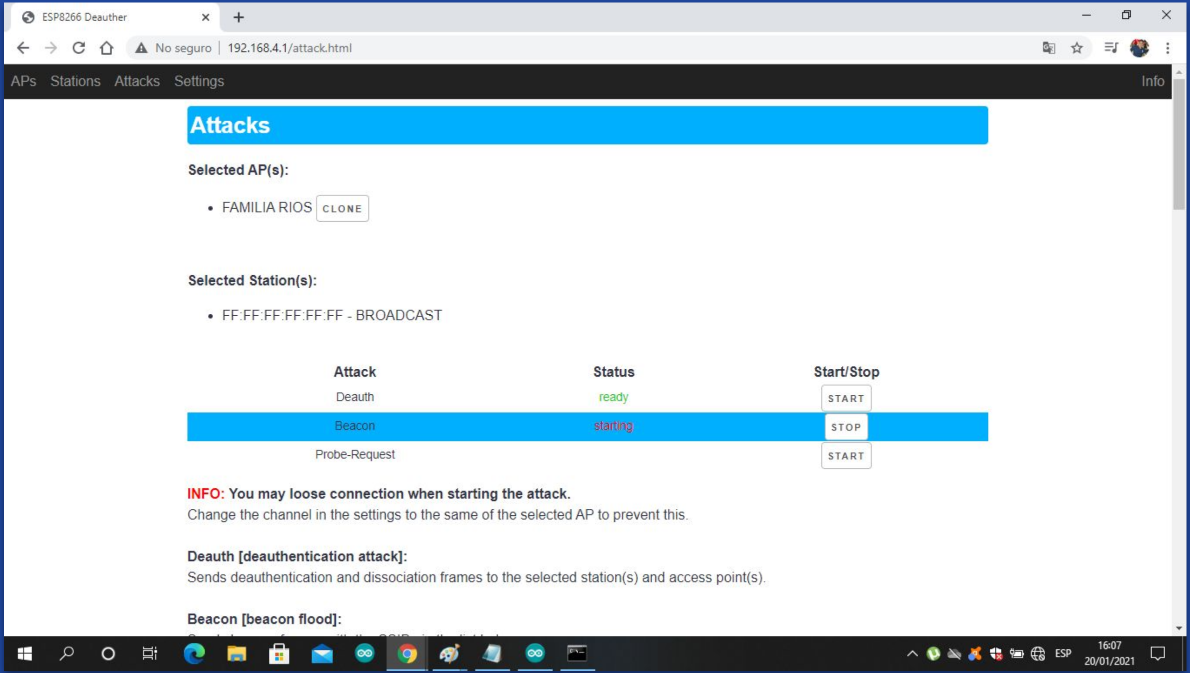
Ch	SSID	RSSI	Encrypt.	Select
2	FAMILIA RIOS	-59	WPA*	DESELECT
1	DTVNET_112CBB	-71	WPA*	SELECT
11	ElVendaval	-82	WPA*	SELECT
1	AA1089667444124	-89	WPA*	SELECT
6	631162467512	-89	WPA*	SELECT
6	* Hidden SSID *	-89	WPA2	SELECT

WPA*=WPA/WPA2 auto mode

version 1.4
Copyright (c) 2017 Stefan Kremser
github.com/spacehuhn

Charges

Attacks dashboard



Attacks

Selected AP(s):

- FAMILIA RIOS CLONE

Selected Station(s):

- FF:FF:FF:FF:FF:FF - BROADCAST

Attack	Status	Start/Stop
Deauth	ready	START
Beacon	starting	STOP
Probe-Request		START

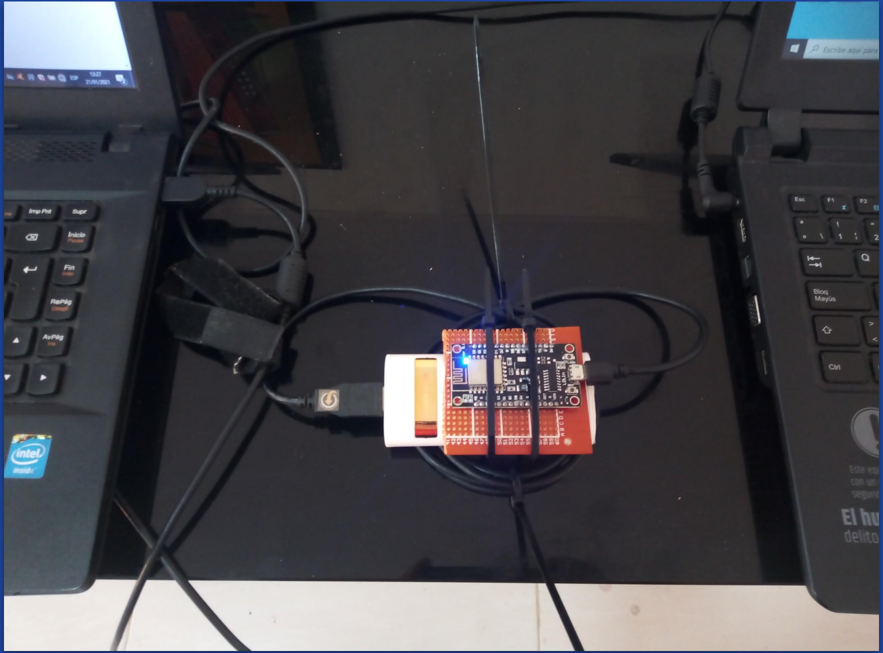
INFO: You may loose connection when starting the attack.
Change the channel in the settings to the same of the selected AP to prevent this.

Deauth [deauthentication attack]:
Sends deauthentication and dissociation frames to the selected station(s) and access point(s).

Beacon [beacon flood]:

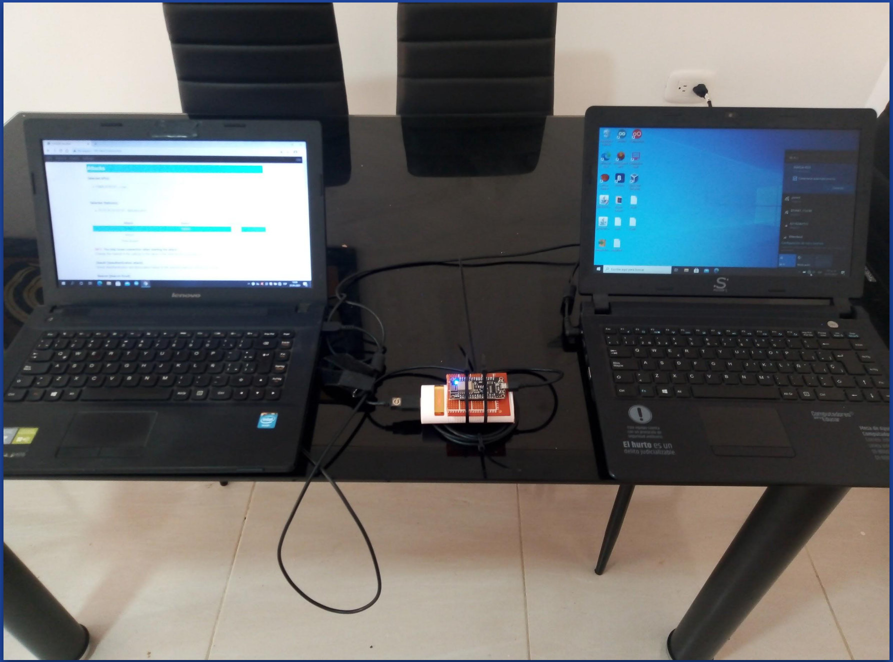
Charges

Final product without case



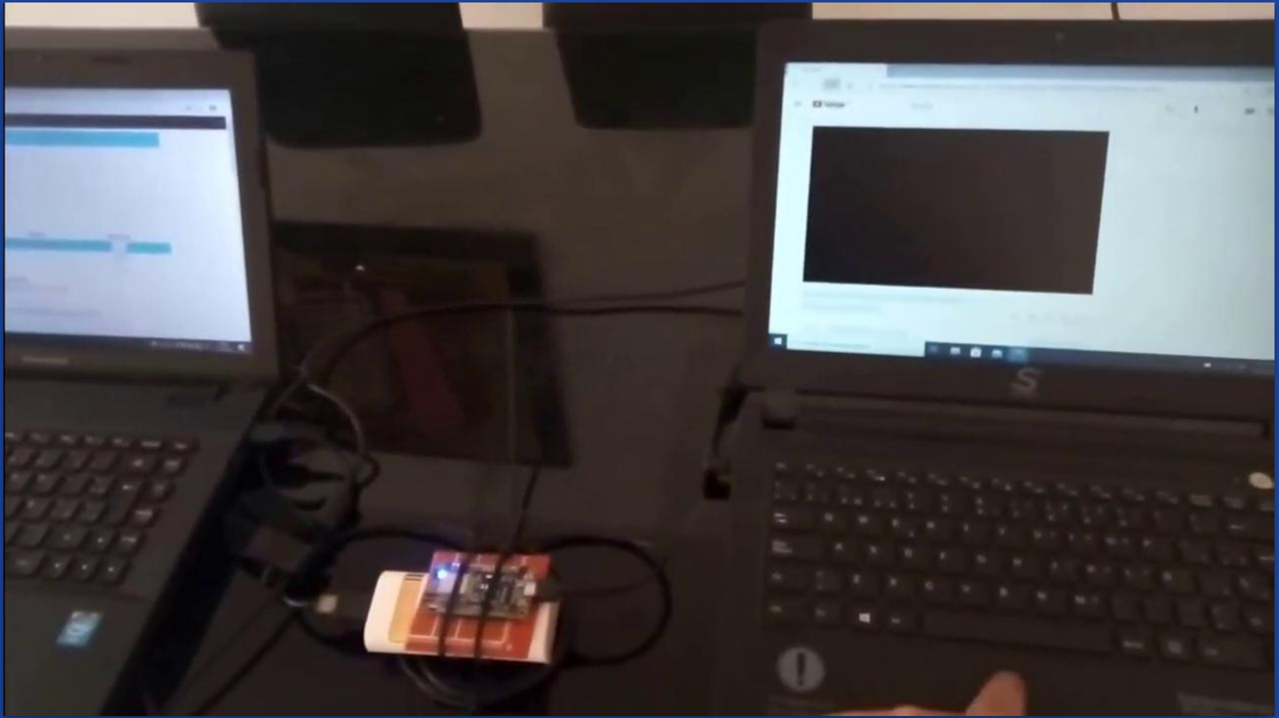
Charges

Size comparison with laptops



Charges

Demo



Charges

Advantages over classic deployment model

📴 Battery-Powered, making it portable.

📴 Custom firmware adds translations, common local SSID names (for faking local ISPs) and simplifies certain operations.

📴 Custom discreet case allows easy and free deployment (adhesive patch allows sticking the charge to different surfaces like windows, walls, doors, furniture and more).

📴 Also, its standard size allows all sorts of cases to be used to disguise the charge, from wall sockets and electrical boxes to air fresheners, or vents.

Surveillance

This meeting is being recorded

Surveillance

⚙️ Hardware

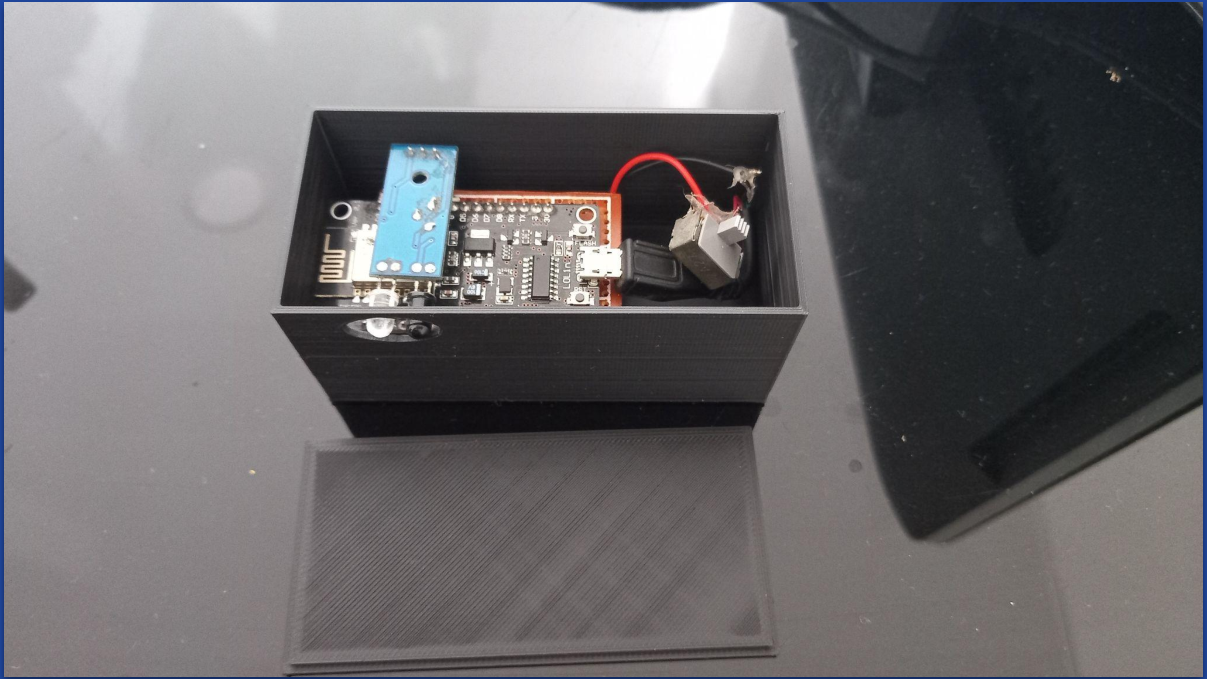
ESP32-CAM
USB Power Bank or 9v Battery
Infrared Sensor
Power Switch
Case (3D Printed)
Adhesive patch

💾 Software

BCA’s Firmware
C2 Server: Flask

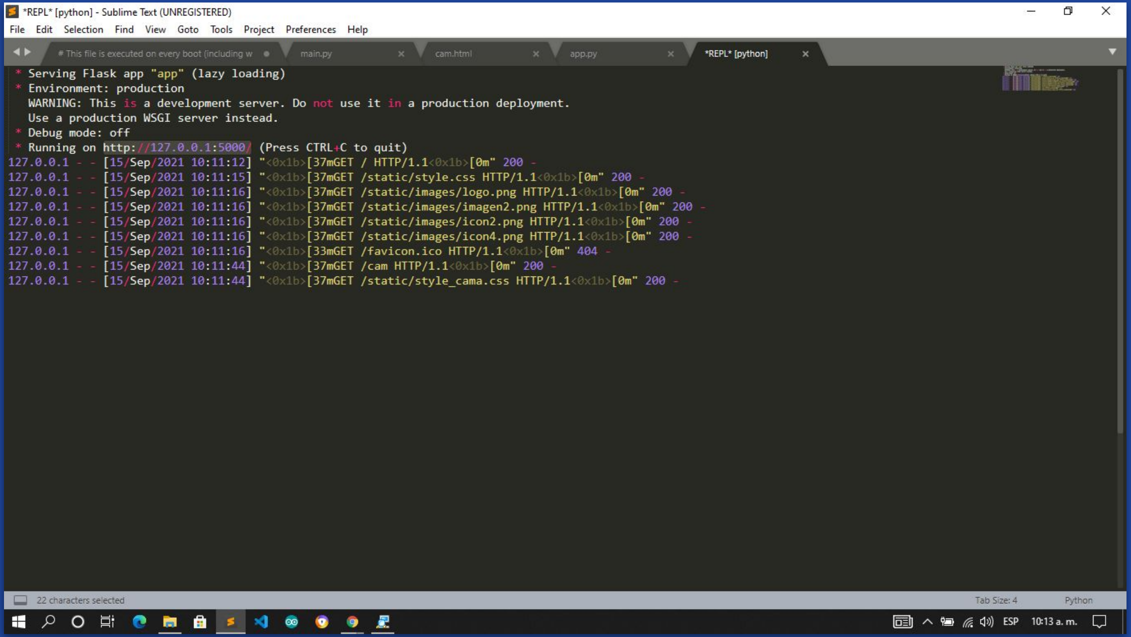
Surveillance

Product outline



Surveillance

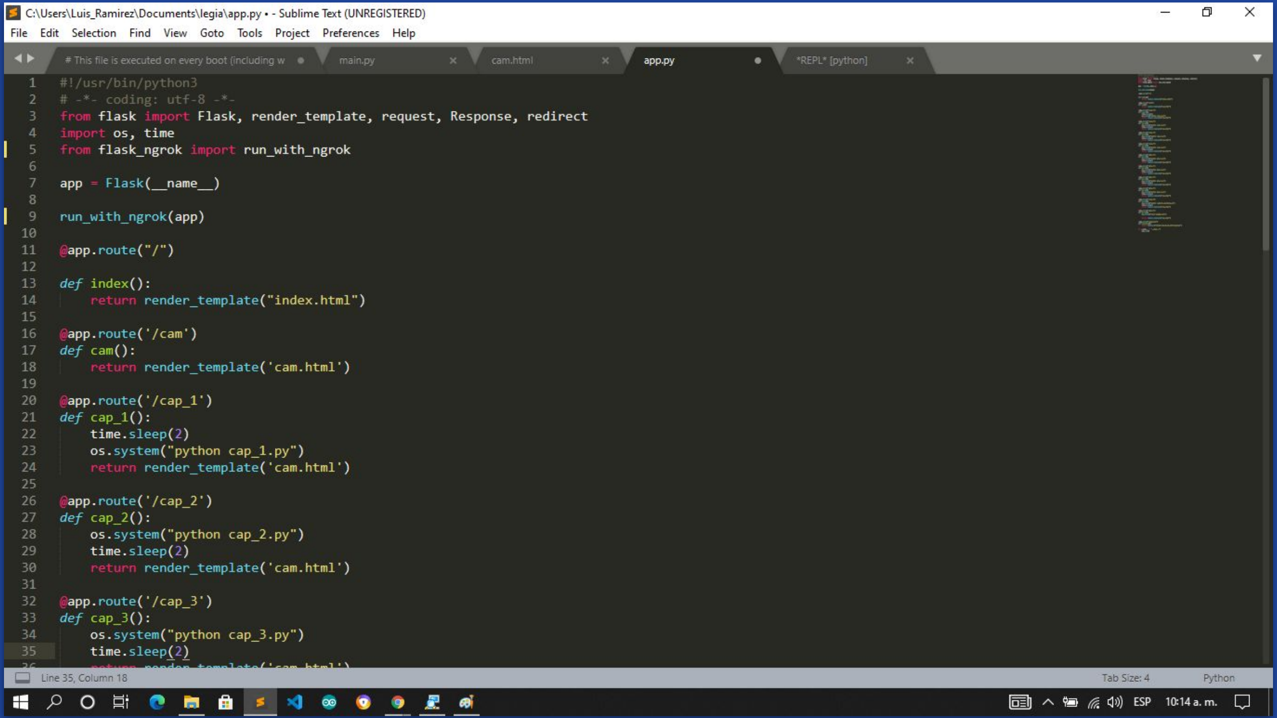
C2 Server


REPL [python] - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
# This file is executed on every boot (including w
main.py
cam.html
app.py
REPL [python]
22 characters selected
Tab Size: 4
Python
ESP
10:13 a. m.

```
 * Serving Flask app "app" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [15/Sep/2021 10:11:12] "<0x1b>[37mGET / HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:15] "<0x1b>[37mGET /static/style.css HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:16] "<0x1b>[37mGET /static/images/logo.png HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:16] "<0x1b>[37mGET /static/images/imagen2.png HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:16] "<0x1b>[37mGET /static/images/icon2.png HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:16] "<0x1b>[37mGET /static/images/icon4.png HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:16] "<0x1b>[33mGET /favicon.ico HTTP/1.1<0x1b>[0m" 404 -
127.0.0.1 - - [15/Sep/2021 10:11:44] "<0x1b>[37mGET /cam HTTP/1.1<0x1b>[0m" 200 -
127.0.0.1 - - [15/Sep/2021 10:11:44] "<0x1b>[37mGET /static/style_cama.css HTTP/1.1<0x1b>[0m" 200 -
```

Surveillance

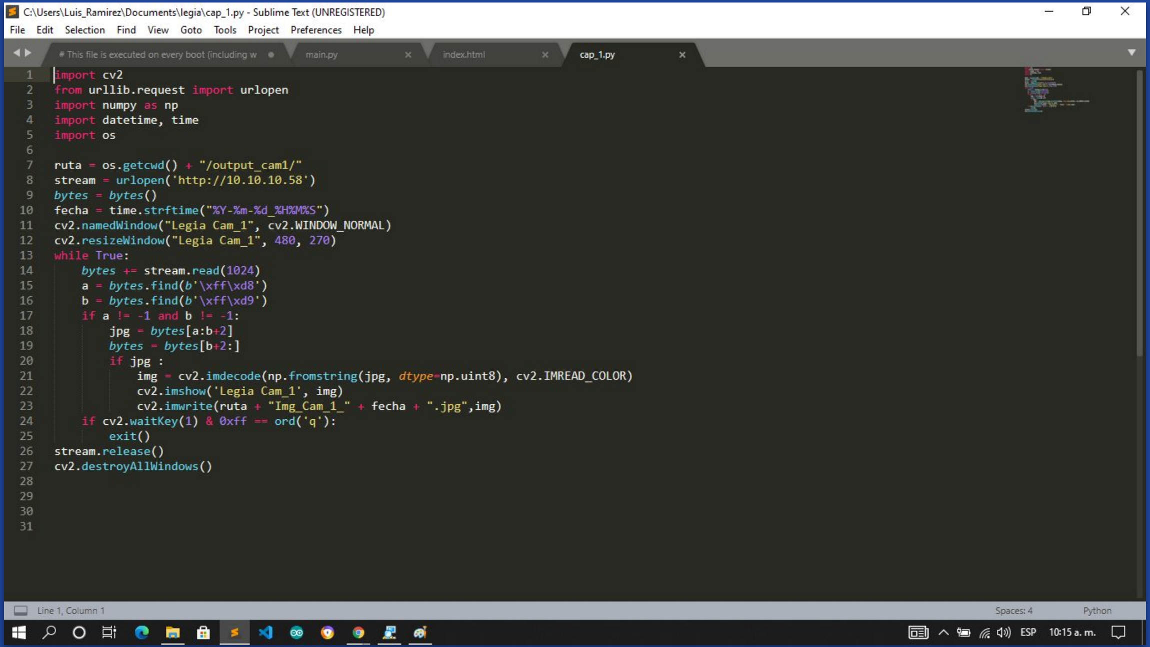
C2 Server


C:\Users\Luis_Ramirez\Documents\legia\app.py • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
# This file is executed on every boot (including w
main.py
cam.html
app.py
REPL [python]
Line 35, Column 18
Tab Size: 4
Python
ESP
10:14 a. m.

```python
#!/usr/bin/python3
# -*- coding: utf-8 -*-
from flask import Flask, render_template, request, Response, redirect
import os, time
from flask_ngrok import run_with_ngrok

app = Flask(__name__)

run_with_ngrok(app)

@app.route("/")

def index():
    return render_template("index.html")

@app.route('/cam')
def cam():
    return render_template('cam.html')

@app.route('/cap_1')
def cap_1():
    time.sleep(2)
    os.system("python cap_1.py")
    return render_template('cam.html')

@app.route('/cap_2')
def cap_2():
    os.system("python cap_2.py")
    time.sleep(2)
    return render_template('cam.html')

@app.route('/cap_3')
def cap_3():
    os.system("python cap_3.py")
    time.sleep(2)
    return render_template('cam.html')
```

Surveillance

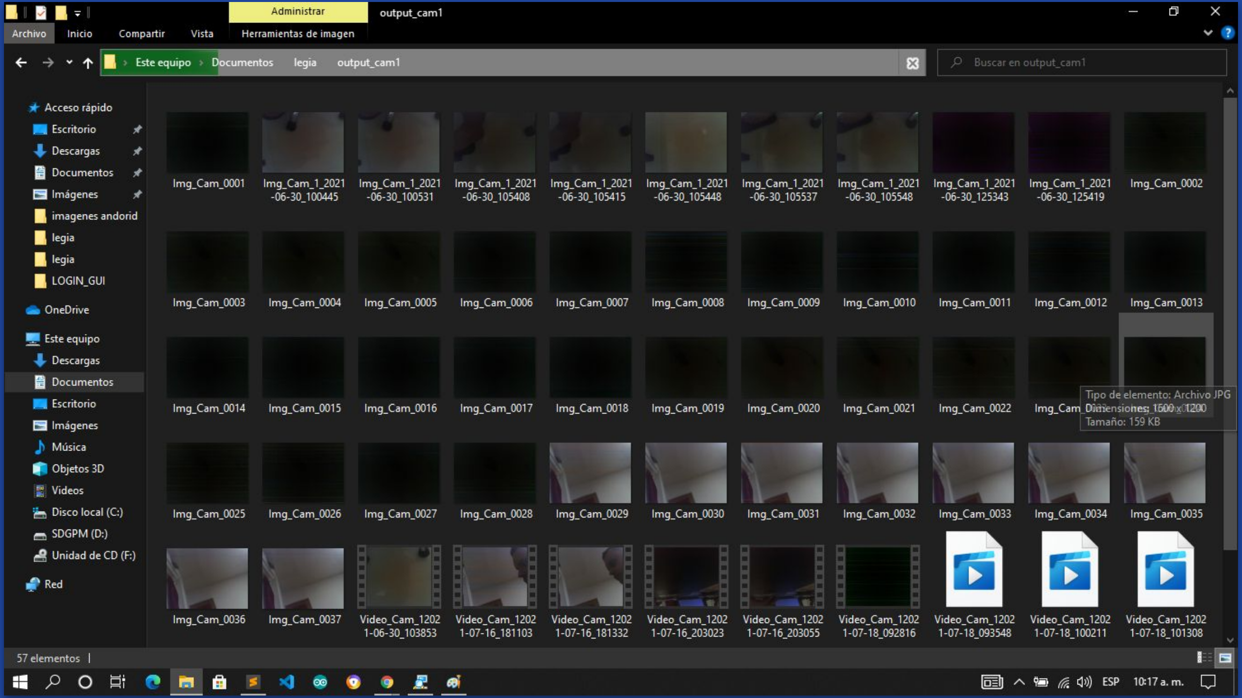
Recording script


C:\Users\Luis_Ramirez\Documents\legia\cap_1.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
# This file is executed on every boot (including w
main.py
index.html
cap_1.py
Line 1, Column 1
Spaces: 4
Python
ESP
10:15 a. m.

```python
import cv2
from urllib.request import urlopen
import numpy as np
import datetime, time
import os

ruta = os.getcwd() + "/output_cam1/"
stream = urlopen('http://10.10.10.58')
bytes = bytes()
fecha = time.strftime("%Y-%m-%d_%H%M%S")
cv2.namedWindow("Legia Cam_1", cv2.WINDOW_NORMAL)
cv2.resizeWindow("Legia Cam_1", 480, 270)
while True:
    bytes += stream.read(1024)
    a = bytes.find(b'\xff\xd8')
    b = bytes.find(b'\xff\xd9')
    if a != -1 and b != -1:
        jpg = bytes[a:b+2]
        bytes = bytes[b+2:]
        if jpg :
            img = cv2.imdecode(np.fromstring(jpg, dtype=np.uint8), cv2.IMREAD_COLOR)
            cv2.imshow('Legia Cam_1', img)
            cv2.imwrite(ruta + "Img_Cam_1_" + fecha + ".jpg",img)
    if cv2.waitKey(1) & 0xff == ord('q'):
        exit()
stream.release()
cv2.destroyAllWindows()
```

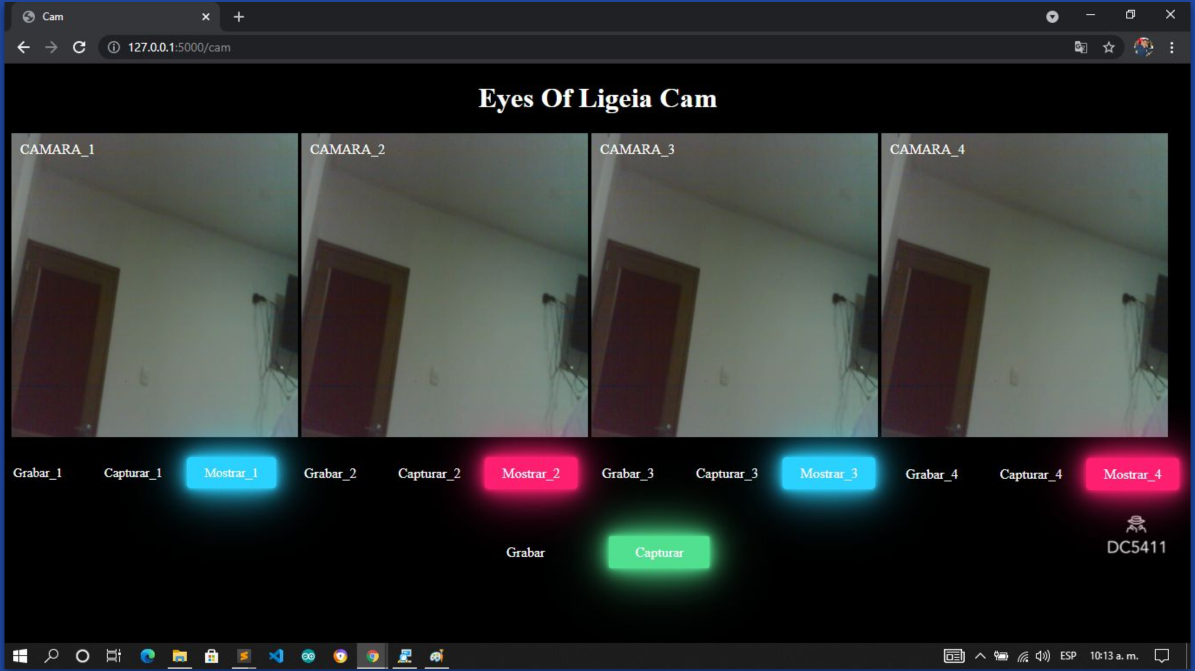
Surveillance

Recordings



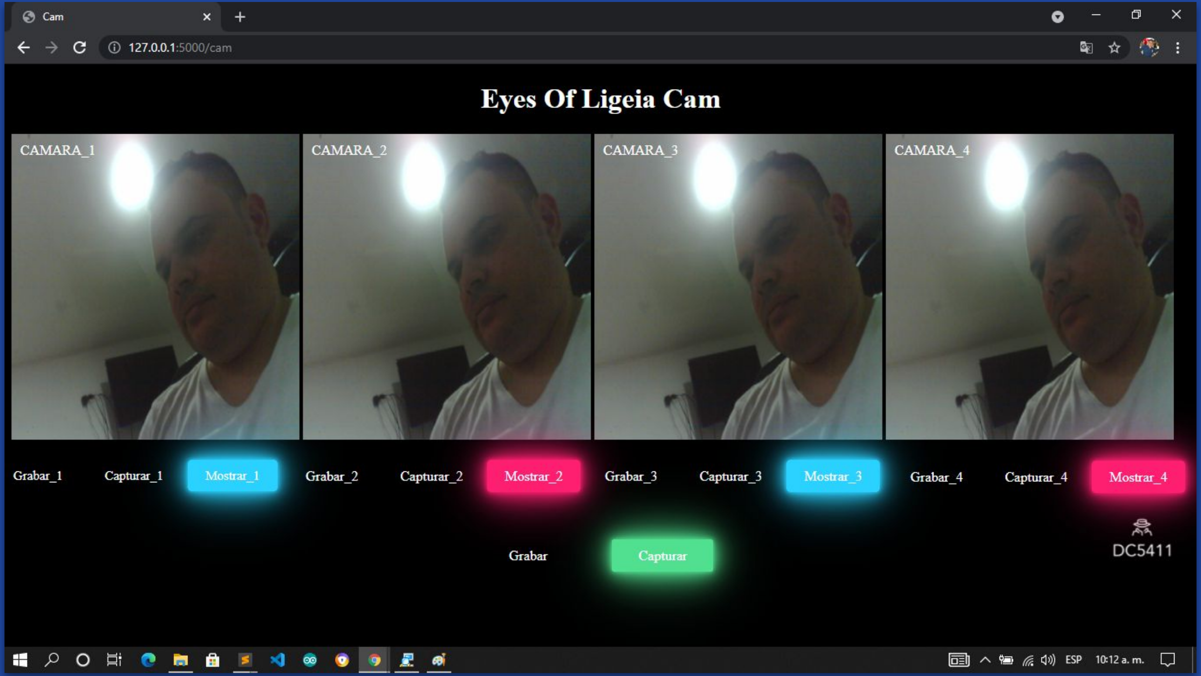
Surveillance

Recording in progress



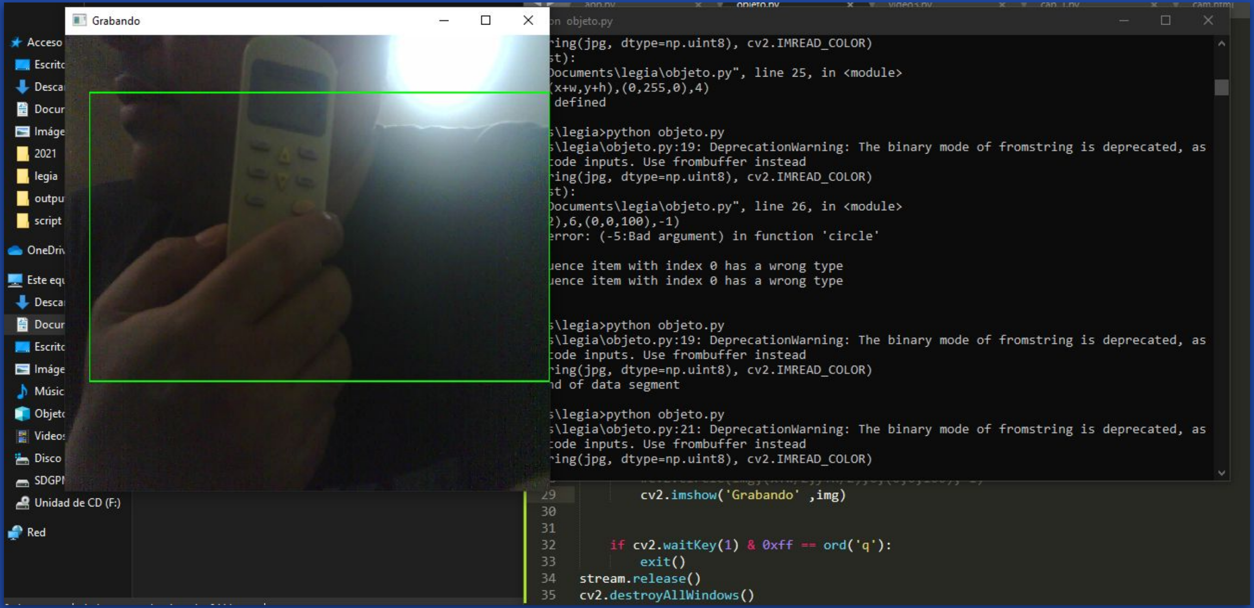
Surveillance

Recording in progress



Surveillance

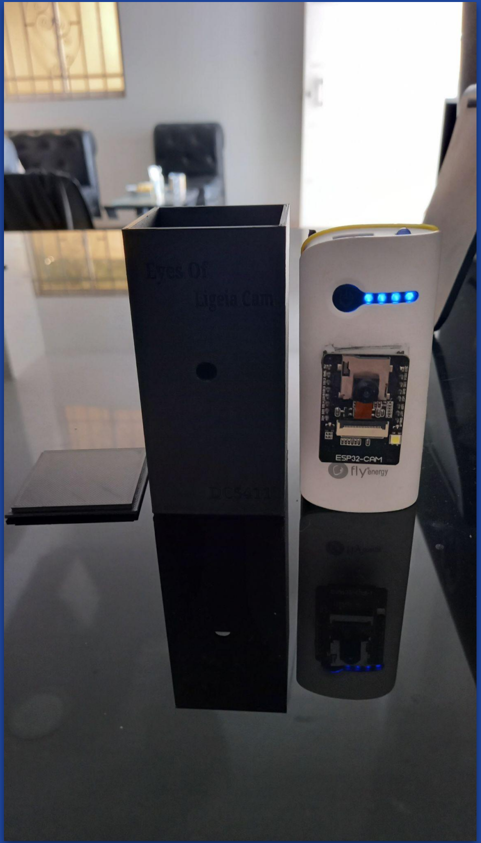
Experimental feature: AI



```
ring(jpg, dtype=np.uint8), cv2.IMREAD_COLOR)
st):
Documents\legia\objeto.py", line 25, in <module>
(x+w,y+h),(0,255,0),4)
 defined

s\legia>python objeto.py
s\legia\objeto.py:19: DeprecationWarning: The binary mode of fromstring is deprecated, as
code inputs. Use frombuffer instead
ring(jpg, dtype=np.uint8), cv2.IMREAD_COLOR)
st):
Documents\legia\objeto.py", line 26, in <module>
2),6,(0,0,100),-1)
error: (-5:Bad argument) in function 'circle'

uence item with index 0 has a wrong type
uence item with index 0 has a wrong type


s\legia>python objeto.py
s\legia\objeto.py:19: DeprecationWarning: The binary mode of fromstring is deprecated, as
code inputs. Use frombuffer instead
ring(jpg, dtype=np.uint8), cv2.IMREAD_COLOR)
nd of data segment

s\legia>python objeto.py
s\legia\objeto.py:21: DeprecationWarning: The binary mode of fromstring is deprecated, as
code inputs. Use frombuffer instead
ring(jpg, dtype=np.uint8), cv2.IMREAD_COLOR)
```

```python
        cv2.imshow('Grabando' ,img)


    if cv2.waitKey(1) & 0xff == ord('q'):
        exit()
stream.release()
cv2.destroyAllWindows()
```

Surveillance



Surveillance

Surveillance

Demo

Surveillance

init 0

Conclusions, Q&A

init 0

Conclusions

🧰 With the arrival of new embedded hardware and its almost infinite combinations, it is increasingly easy to create implements to our liking.

🧰 The use of this technology combined with open source software solutions gives a wide spectrum of movement and flexibility for creators.

🧰 Not only is the final result more economical, but the product's life span can be virtually infinitely extended, receiving updates and upgrades that closed, commercial hardware does not.

init 0

Follow us

Twitter

@larm182luis | @MauroEldritch | @dc54111

Github

@MauroEldritch | @larm182 | @dc5411

This work is published on Github:
github.com/dc5411/armory

Questions?