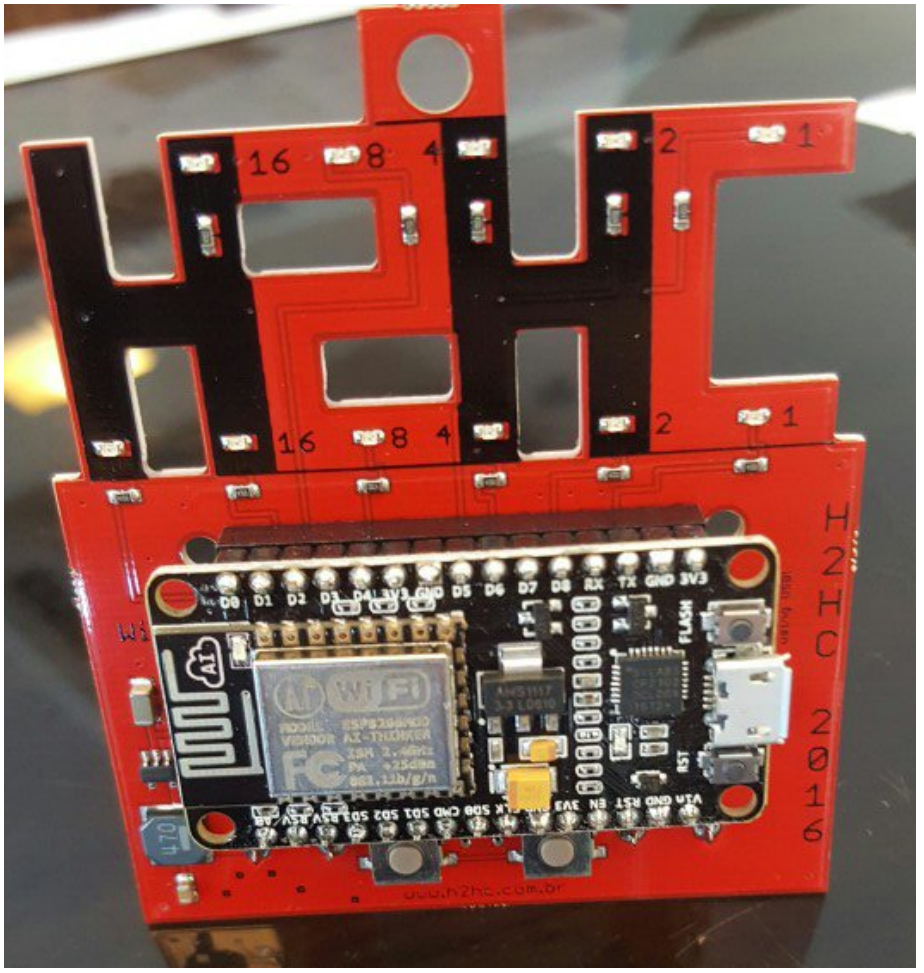
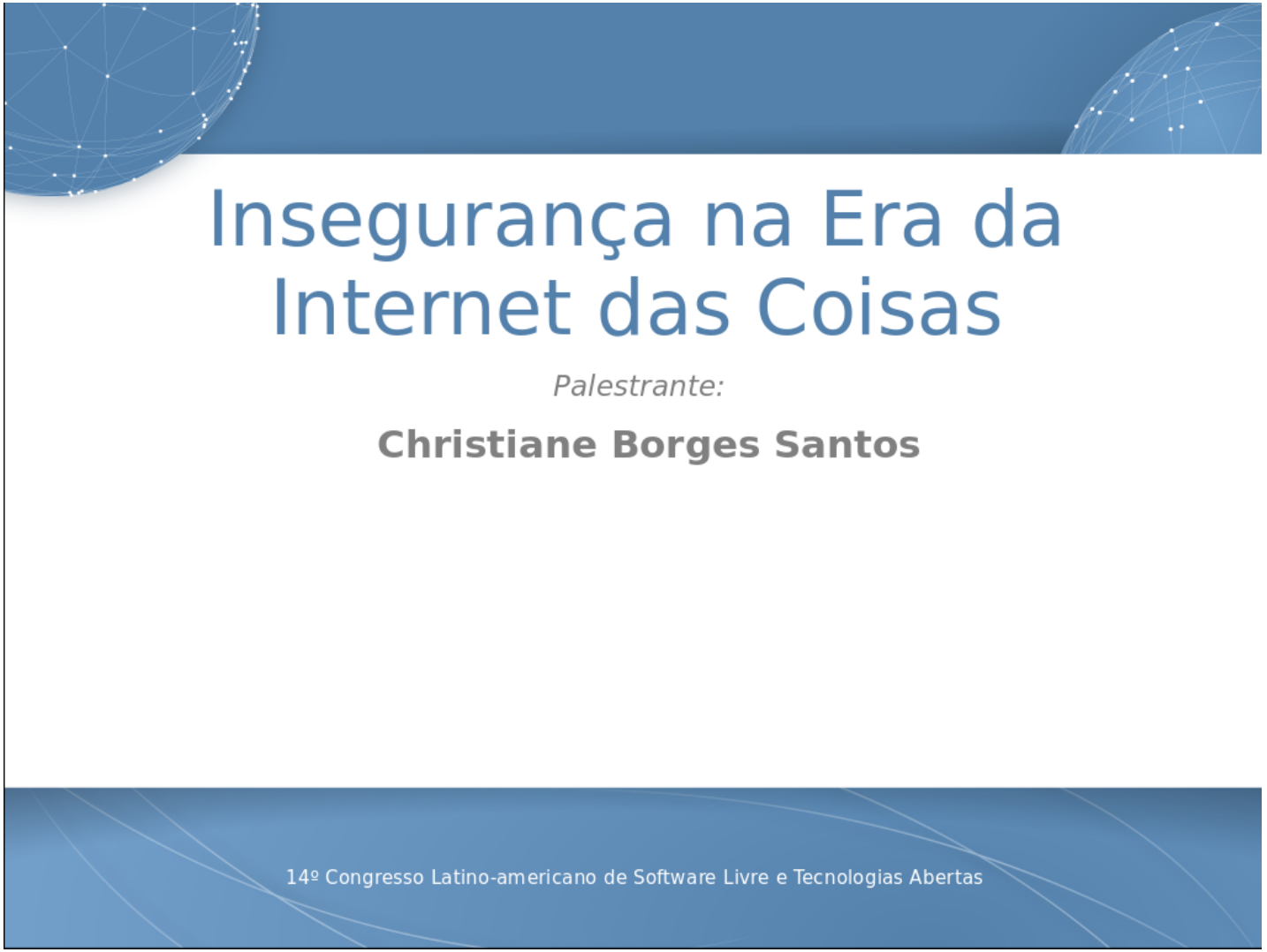
Badge H2HC 2016



Inspiração

Conhecer as limitações do esp8266 para explorar falhas em implementações alheias, através de uma POC que explore os limites do hardware.

Inspiração


Insegurança na Era da Internet das Coisas
Palestrante:
Christiane Borges Santos
14º Congresso Latino-americano de Software Livre e Tecnologias Abertas

Insegurança na Era da Internet das Coisas

MENU | techtudo VIDA DIGITAL

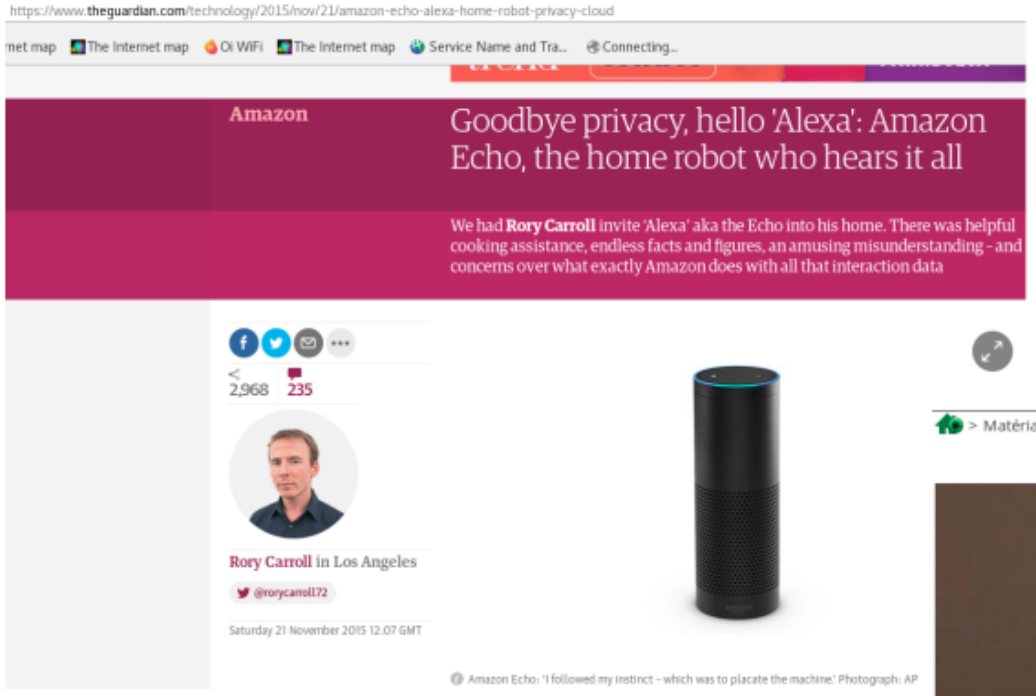
INTERNET

20/01/2014 15h42 - Atualizado em 20/01/2014 15h50

Botnet envia spam na web com ajuda de Smart TVs e geladeira conectada

A empresa de segurança virtual Proofpoint identificou um grande ataque de botnets que vitimizou cerca de 100 mil aparelhos 'smart' entre os dias 23 de dezembro e 6 de janeiro de 2014.

Insegurança na Era da Internet das Coisas


https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud

net map | The Internet map | Oi WiFi | The Internet map | Service Name and Tra... | Connecting...

Amazon

Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all

We had **Rory Carroll** invite 'Alexa' aka the Echo into his home. There was helpful cooking assistance, endless facts and figures, an amusing misunderstanding – and concerns over what exactly Amazon does with all that interaction data

2,968 235

Rory Carroll in Los Angeles

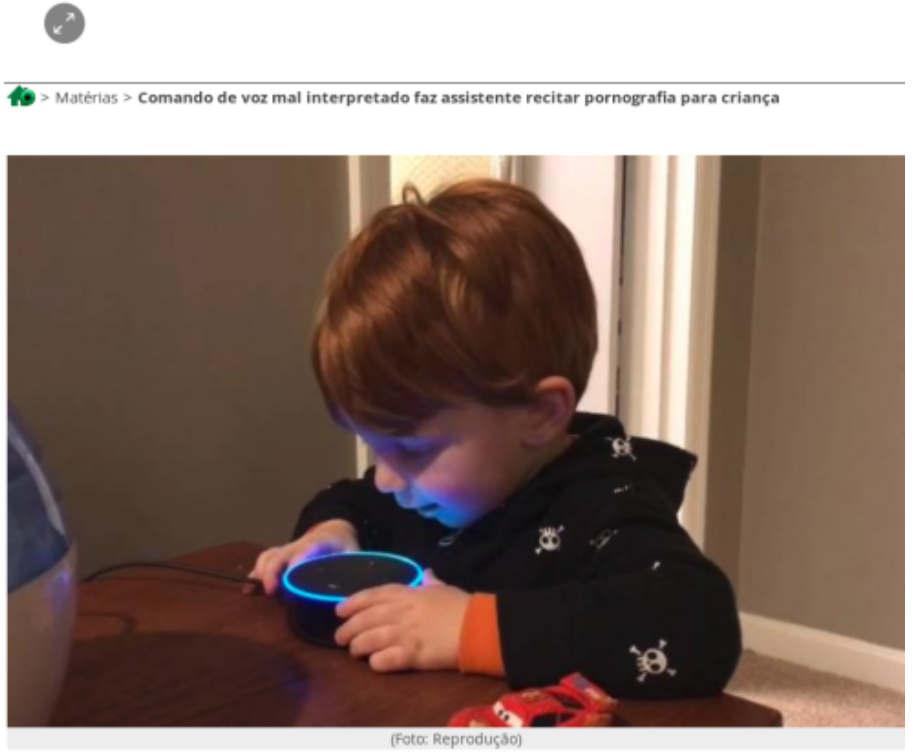
@rorycarroll72

Saturday 21 November 2015 12.07 GMT

Amazon Echo: 'I followed my instinct – which was to placate the machine.' Photograph: AP

Is Alexa working for the CIA? Video shows owner asking Amazon's smart assistant if it is connected to the intelligence agency - causing it to shut down repeatedly

https://goo.gl/Vx5hQh


> Matérias > **Comando de voz mal interpretado faz assistente recitar pornografia para criança**

(Foto: Reprodução)

Comando de voz mal interpretado faz assistente recitar pornografia para criança

LUCAS CARVALHO 30/12/2016 17H00 AMAZON :: INTELIGÊNCIA ARTIFICIAL

Insegurança na Era da Internet das Coisas

É só um brinquedo...

Segurança

Brinquedo conectado à internet vaza dados de crianças

By Jean Prado
3 de março de 2017

BBC Menu

BRASIL Seções

Autoridades alemãs fazem alerta contra boneca que pode ser hackeada para espionar crianças

17 fevereiro 2017

Segundo especialistas, é possível hackear a boneca Minha Amiga Cayla

Insegurança na Era da Internet das Coisas

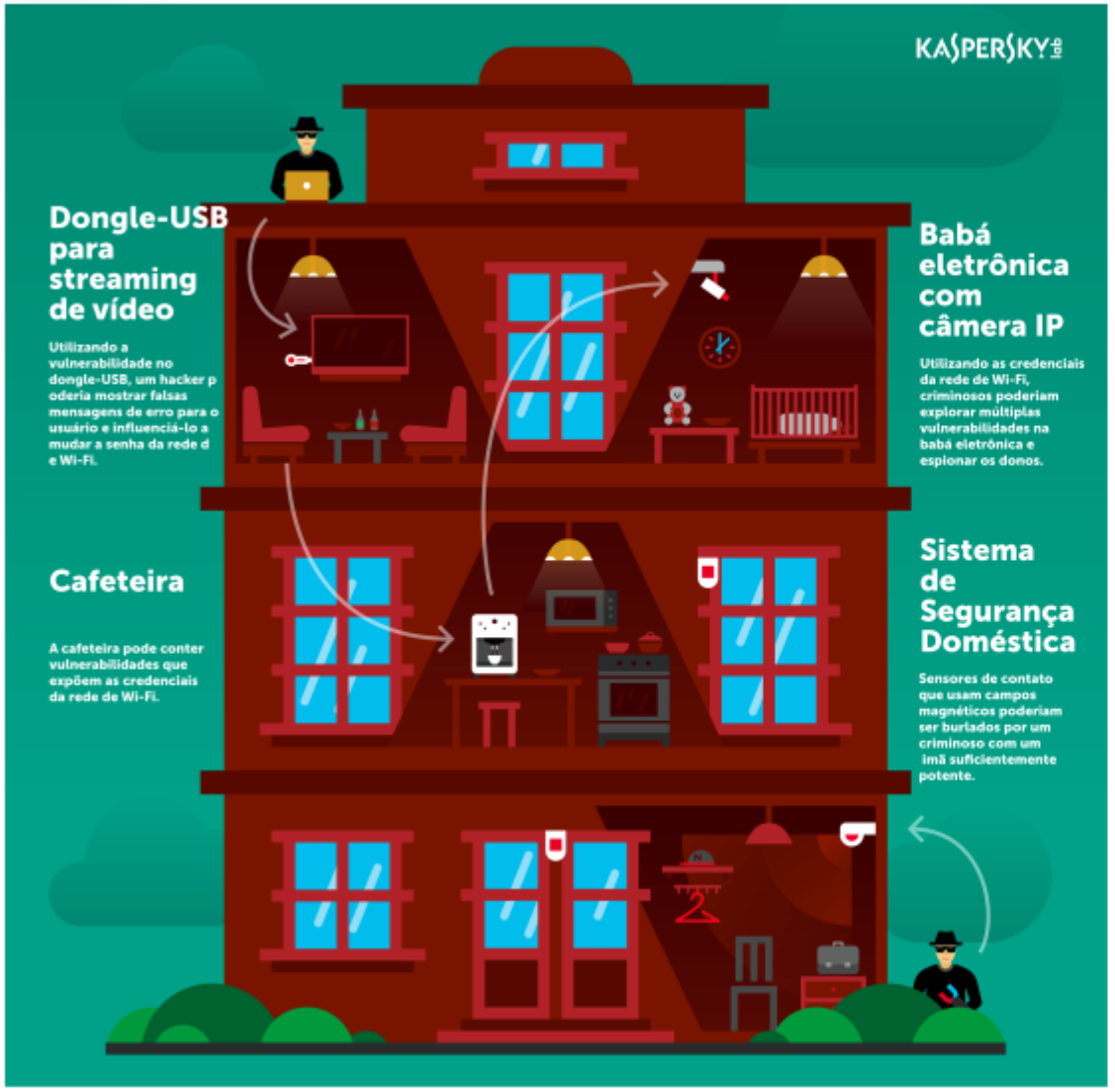
MENU techtudo ELETRÔNICOS

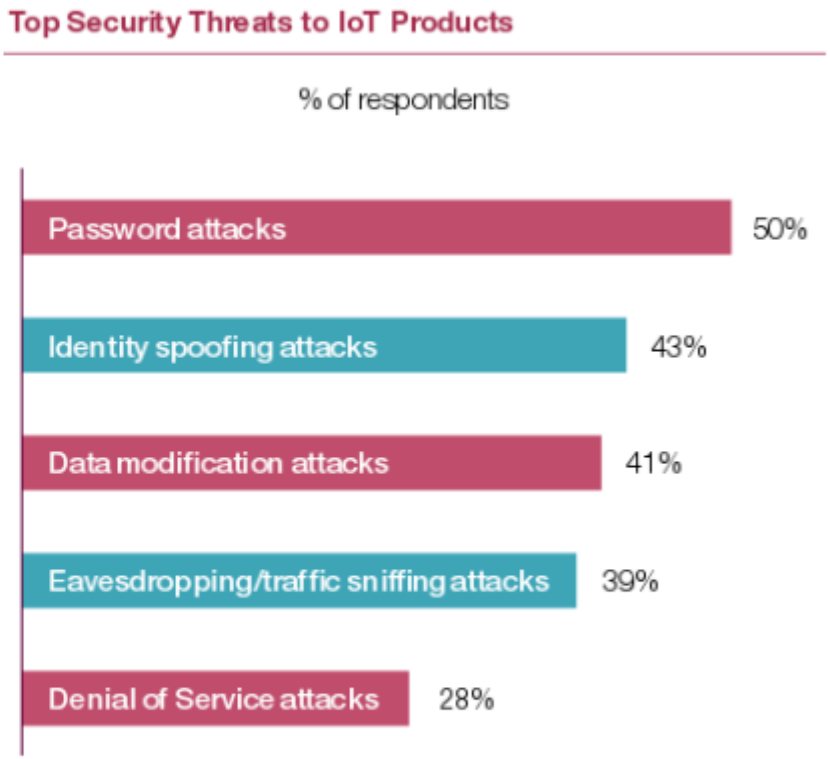
10/07/2014 07h30 - Atualizado em 10/07/2014 07h30

Lâmpadas inteligentes são hackeadas para furto de senhas de Wi-Fi

Lâmpadas inteligentes tem vulnerabilidade grave (Foto: Divulgação/LIFX)

Insegurança na Era da Internet das Coisas





Source: Capgemini Consulting and Sogeti High Tech, “Security in the Internet of Things Survey”, November 2014

Ação

Conhecer as limitações do esp8266 para explorar falhas

https://www.hackster.io/rayburne/warwalking-a9c021

Warwalking with the ESP8266

Made by Ray Burnette - Published in Everything ESP

ABOUT THIS PROJECT

Warwalking is the pedestrian version of wardriving but in this case we are using an ESP8266+OLED powered by a single lithium 3.2V AA cell.

arduino oled wardriving

PROJECT INFO

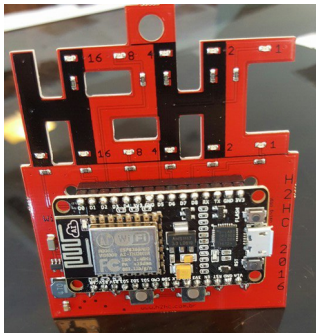
Type	Full instructions provided
Difficulty	Intermediate
Published	July 19, 2015
License	CC BY

Proof of concept

Modelo prático que possa provar o conceito (teórico) estabelecido por uma pesquisa.

- Investigar limites do hardware, com foco na seg.
- Criar um scanner de redes wi-fi com data log
- Permitir geo-localização dos dados
- Backend com ferramentas de extração

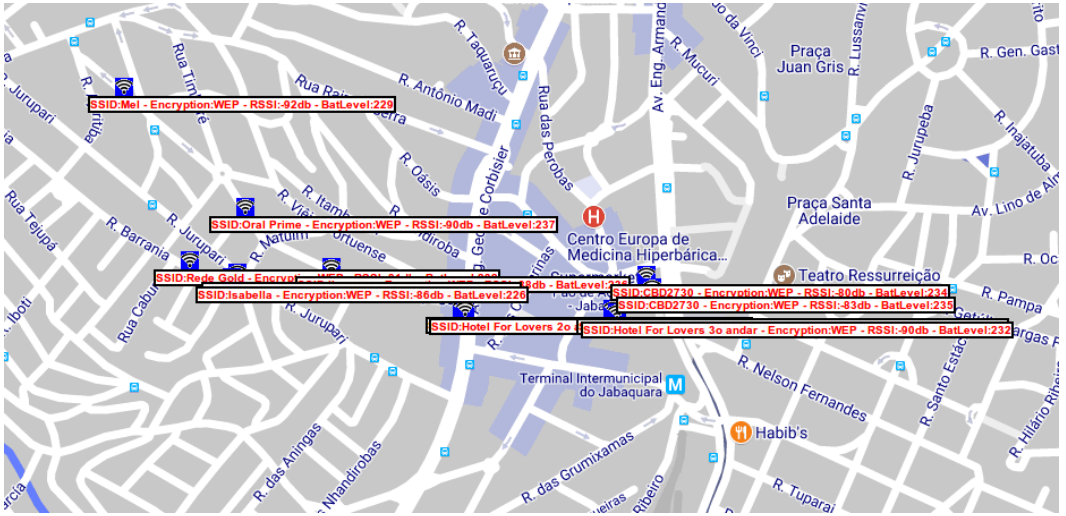
Diagrama



LOG DADOS

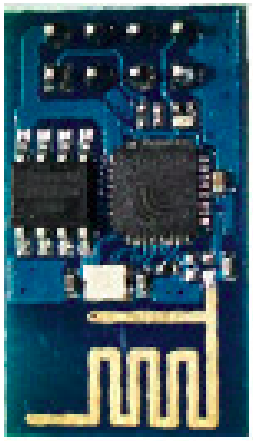
DB

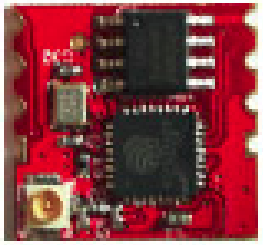
MAPA

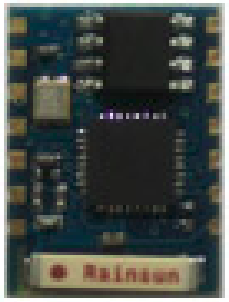


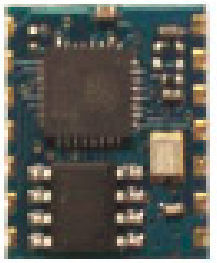
BACKEND

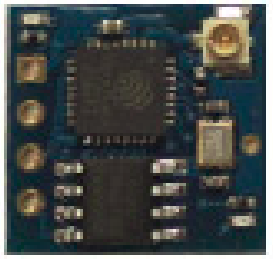
ESP8266


ESP-01

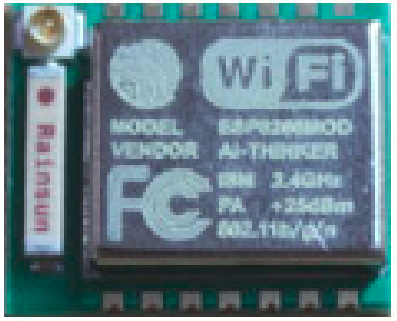

ESP-02


ESP-03


ESP-04

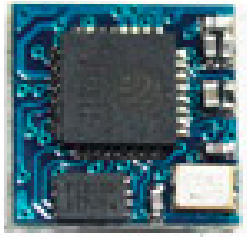

ESP-05

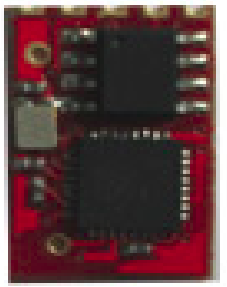
ESP-06

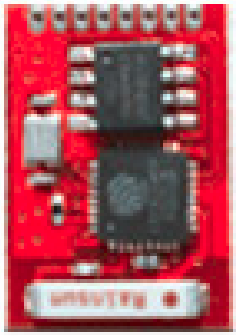


ESP-07

ESP-08


ESP-09

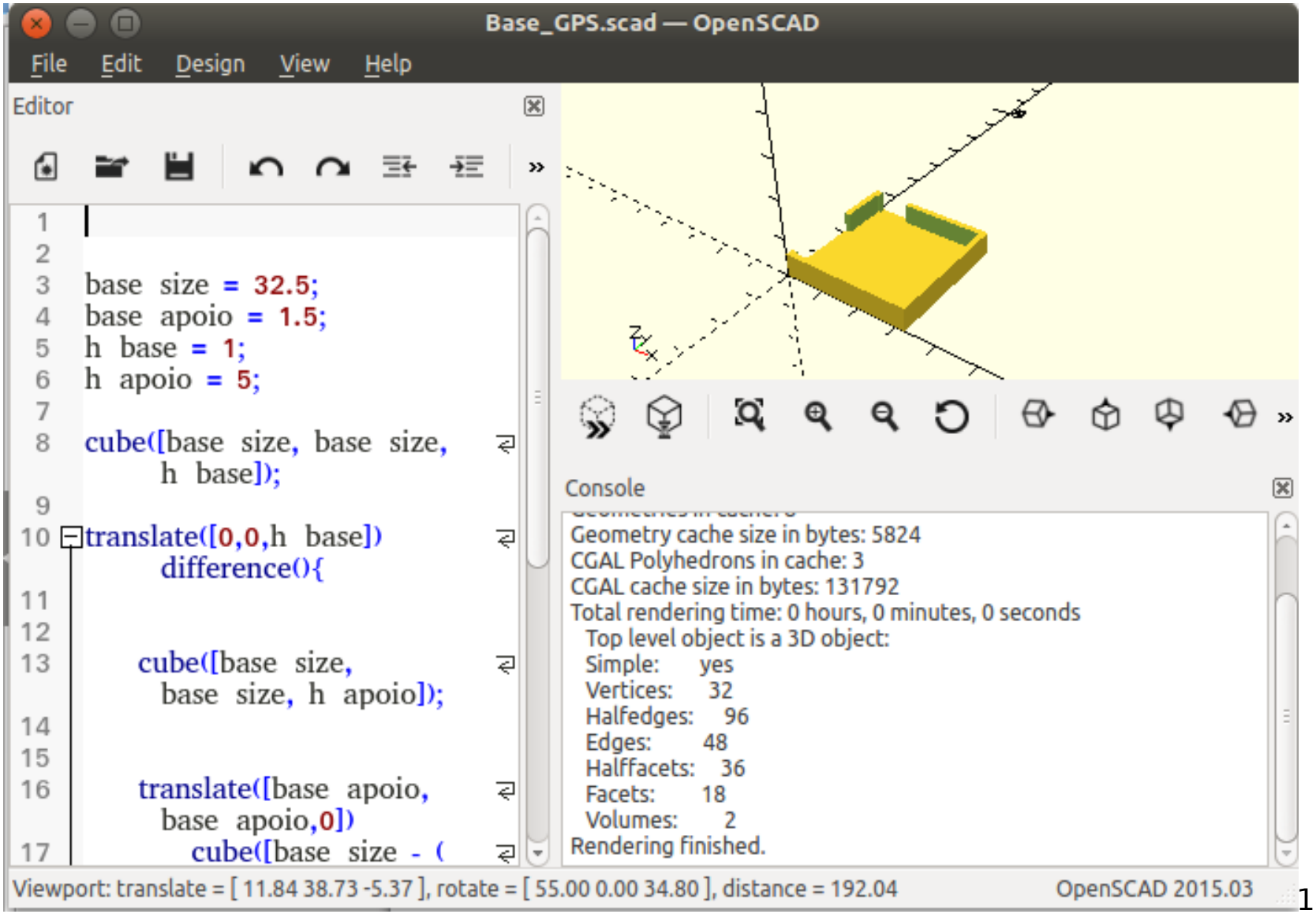

ESP-10


ESP-11

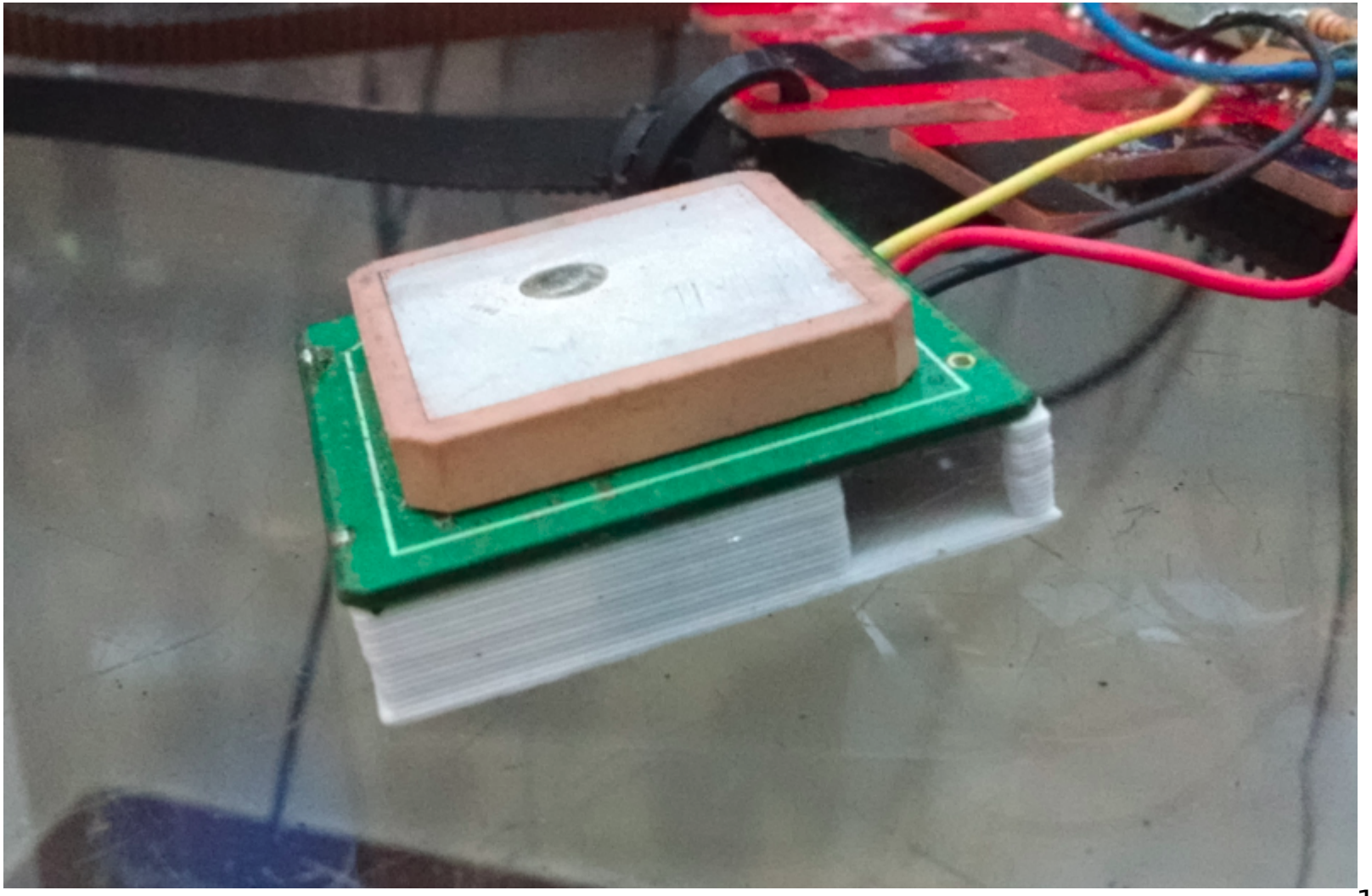
NODE MCU


VIN GND RST EN 3V3 GND CLK SD0 CMD SD1 SD2 SD3 RSV RSV
D0 D1 D2 D3 D4 3V3 GND D5 D6 D7 D8
3V3 GND TX RX

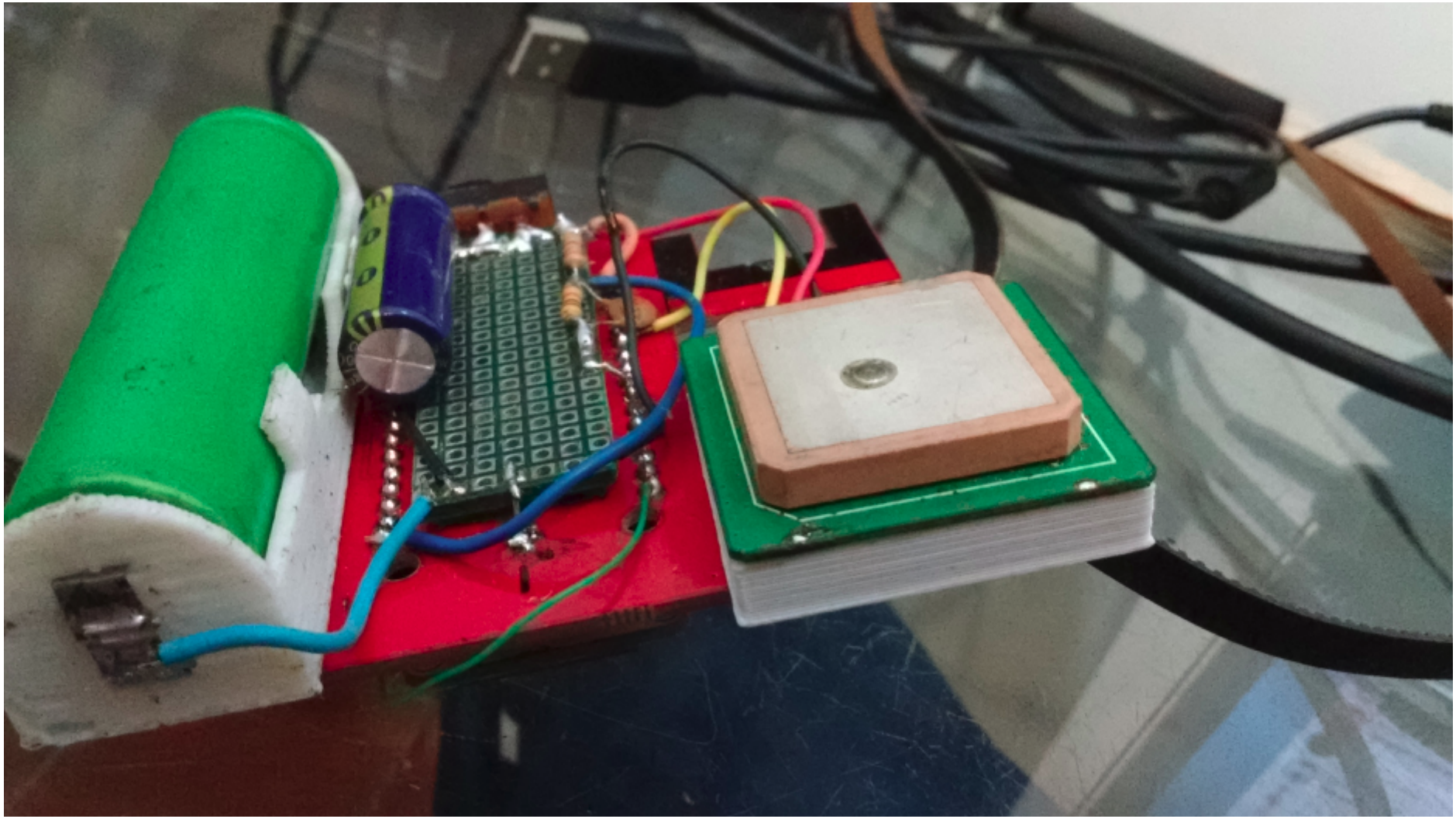
Eletrônica e Mods - 3D



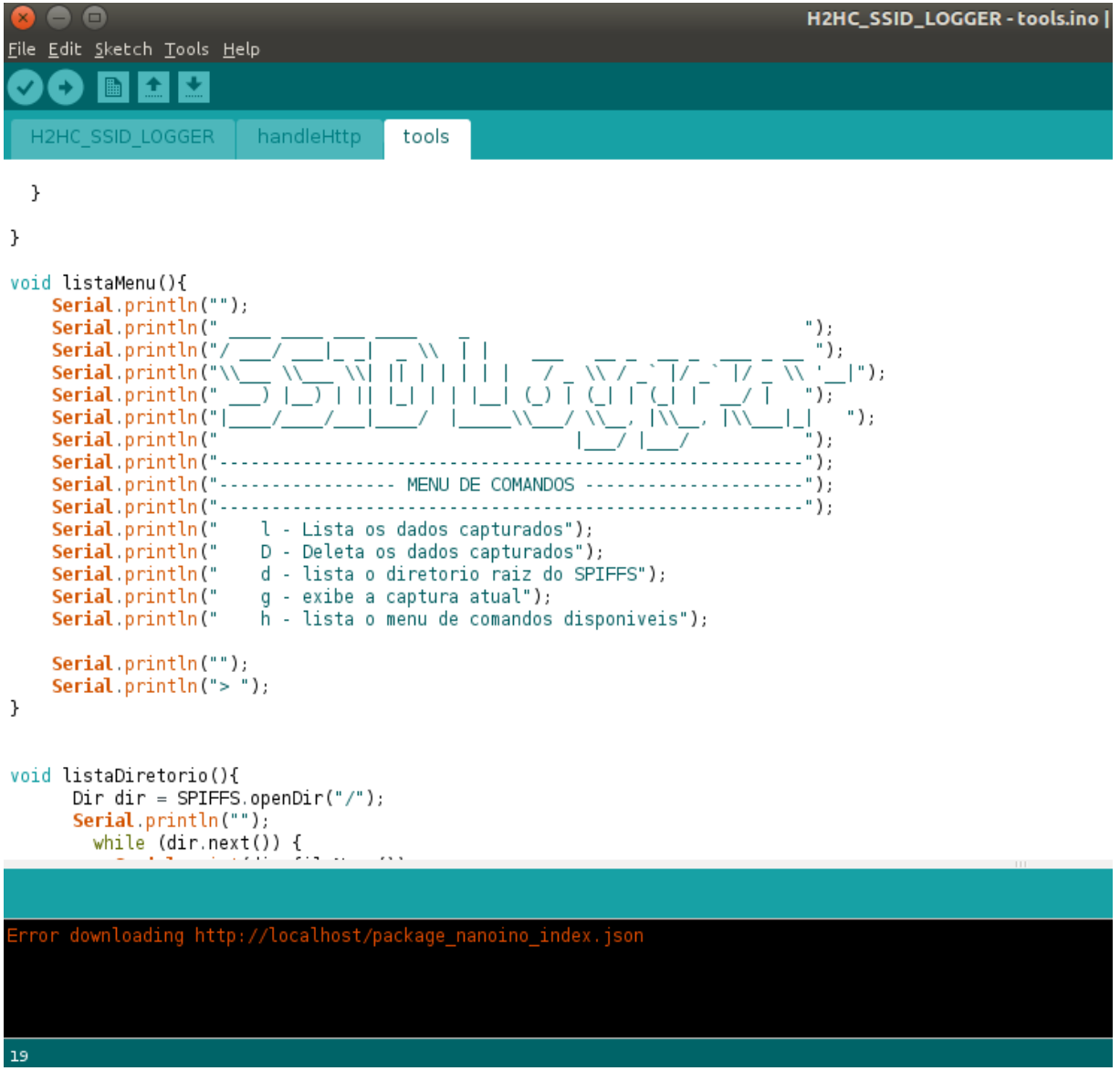
Eletrônica e Mods - GPS



Eletrônica e Mods - Supply



FIRMWARE - Arduino



FIRMWARE - Considerações

```
const char *softAP_ssid = "HACKUDO_CUIDADO";
const char *softAP_password = "12345678";

/* hostname for mDNS. Should work at least on windows. Try http://esp8266.local */
const char *myHostname = "esp8266.local";

/* Don't set this wifi credentials. They are configurated at runtime and stored on EEPROM */
char ssid[32] = "";
char password[32] = "";

// DNS server
const byte DNS_PORT = 53;
DNSServer dnsServer;
```

Arquivo de dados

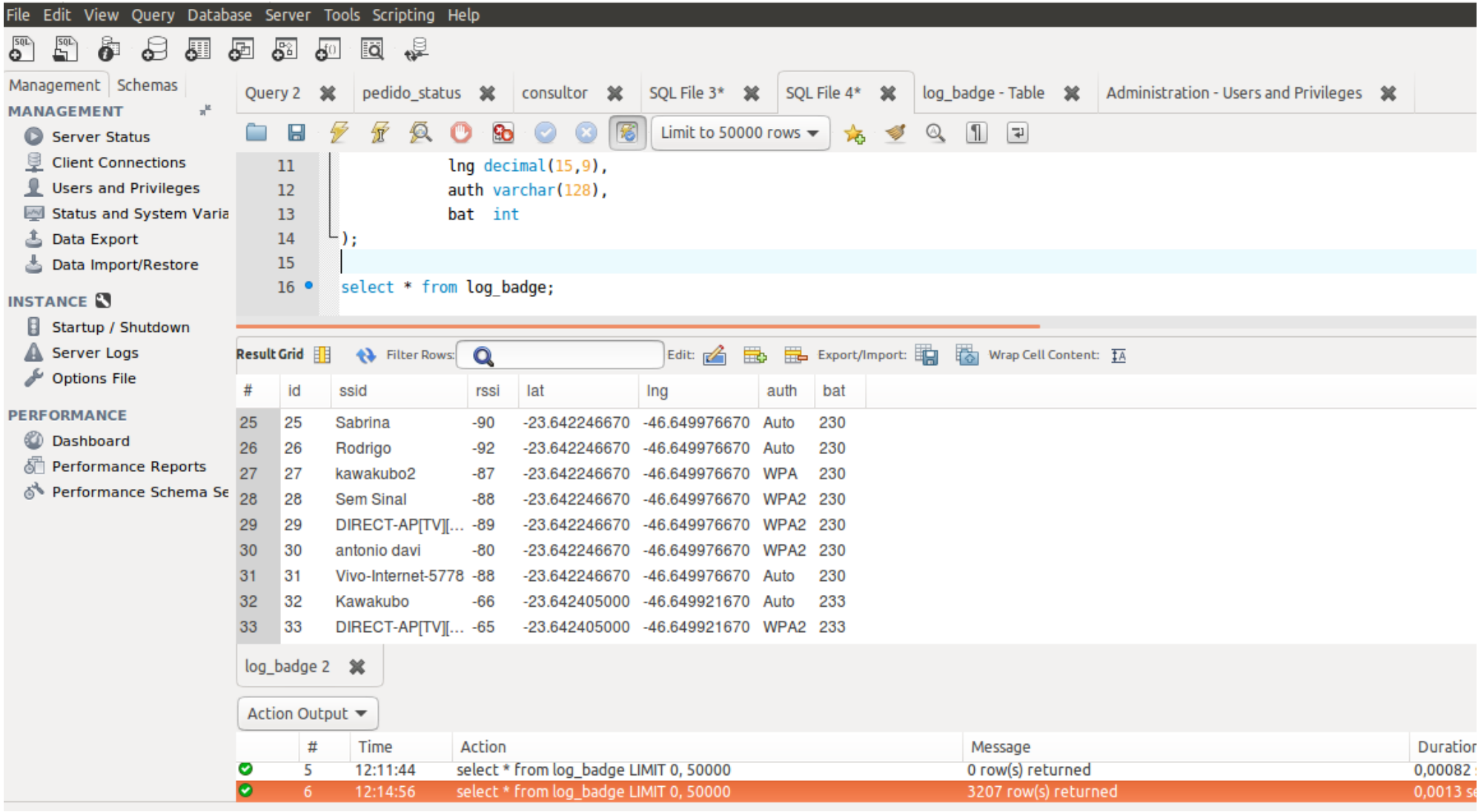
SSID – RSSI – Lat – Lng – Battery level

Rodrigo|Auto|-72|-23.64202000|-46.64996500|235|
dobmoto|Auto|-72|-23.64202000|-46.64996500|235|
JMS-JOMASI|WPA2|-84|-23.64202000|-46.64996500|235|
CBD2730|WEP|-80|-23.64490333|-46.64160000|234|
dobm_spare|Auto|-92|-23.64202000|-46.64996500|235|
RedeDaSilva2|Auto|-91|-23.64202000|-46.64996500|235|
lkreuser|WEP|-88|-23.64475500|-46.64756500|236|
Oral Prime|WEP|-90|-23.64371000|-46.64920167|237|
dobmoto_porteira|WPA2|-48|-23.64202000|-46.64996500|235|
Rodrigo|Auto|-77|-23.64198833|-46.64997500|229|
dobmoto|Auto|-76|-23.64198833|-46.64997500|229|
kawakubo2|WPA|-90|-23.64198833|-46.64997500|229|
Hotel For Lovers 2o andar|WEP|-92|-23.64549500|-46.64504167|235|
JMS-JOMASI|WPA2|-82|-23.64198833|-46.64997500|229|
dobm_spare|Auto|-88|-23.64198833|-46.64997500|229|
dobmoto_porteira|WPA2|-50|-23.64198833|-46.64997500|229|
NANA63|Auto|-89|-23.64198833|-46.64997500|229|

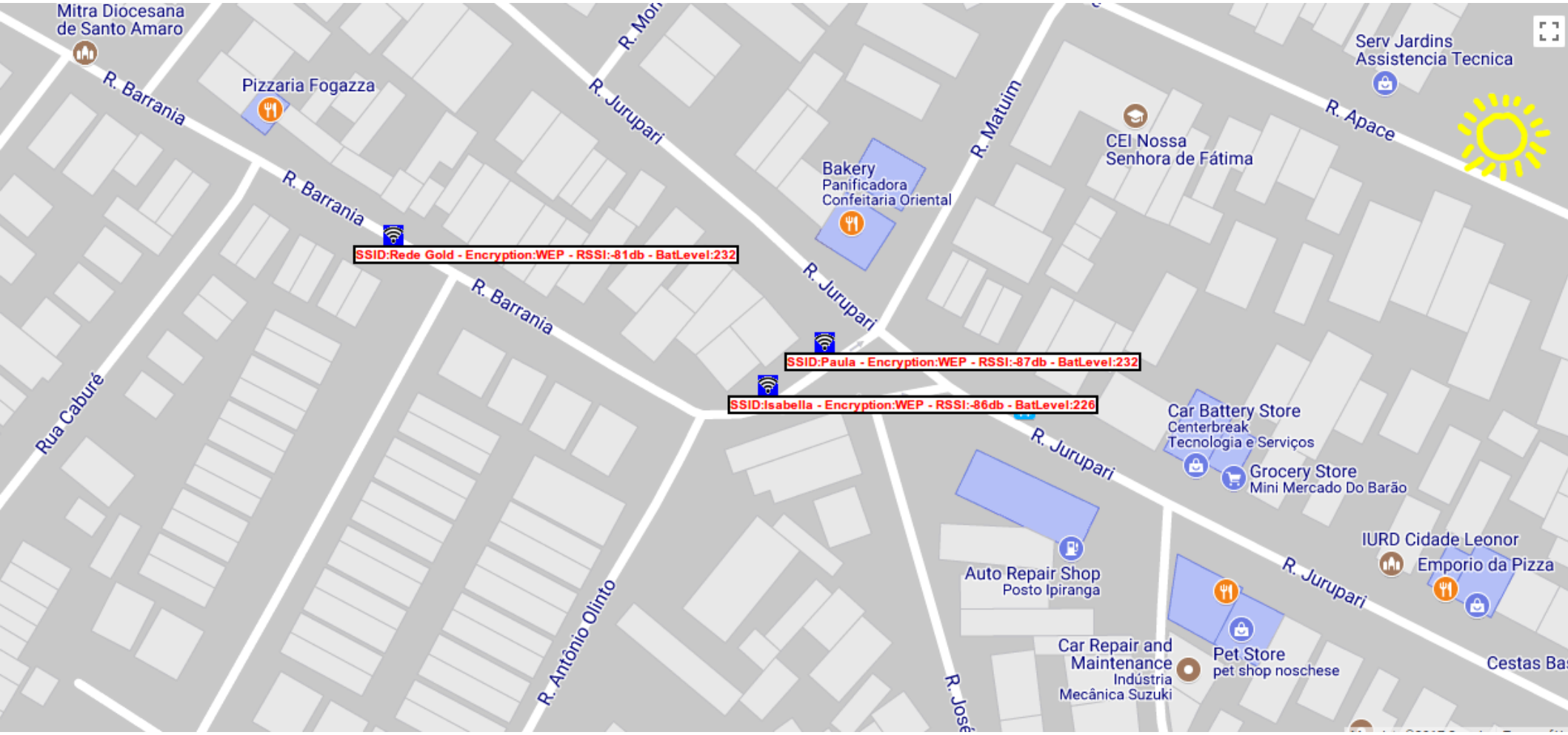
Backend


h2hc_badge
JavaScript Resources
PHP Language Library [PHP 7.1]
PHP Include Path
css
fonts
imagens
include
config.php
database.php
js
ole
utilidades
index.js
index.php
mapa.php
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
var customMapTy
var customMapTy
map.mapTypes.s
map.mapTypes.s
// Create the DI
// passing in thi
var homeControl
var homeControl
homeControlDiv.
map.controls[go
var diaNoiteCont

Banco de dados e analise



Geoposicionamento de dados



Conclusão

Além do warwalking, percebe-se que todo contexto de desenvolvimento de código do ESP8266 pode ser explorado em busca de leaks, pois o foco dos exemplos é na facilidade de implementação e não na segurança.

Conclusão

Explorar as limitações do hardware permite saber mais sobre como hackea-lo

Conhecendo os limites de cada ferramenta, é possivel utilizar um hardware extremamente barato para coleta de dados, Armazenamento e posterior analise

Perguntas?

Ano que vem tem mais!

Obrigado!!

Daniel Basconcello Filho
daniel@robotizando.com.br

Christiane Borges Santos
christiane.santos@ifg.edu.br

Bibliografias:
Warwalking with ESP8266 - https://www.hackster.io/rayburne/warwalking-a9c021
Wikipedia Proof of concept: https://en.wikipedia.org/wiki/Proof_of_concept
Node MCU: http://www.nodemcu.com/index_en.html
Arduino Board for ESP8266: http://arduino.esp8266.com/stable/package_esp8266com_index.json
Google maps API for DEVS: https://developers.google.com/maps/?hl=pt-br
OpenSCAD: http://www.openscad.org/
Projeto REPRAP: www.reprap.org