# H4X – Lets Hack!

# Microcontrollers (ESP8266)

# whoami

Christo Goosen

# Whoami | grep disclaimer

**I am not a engineer or a embedded/microcontroller expert. I tinker with devices and tech for fun and share what I have learnt through talks. Correct me if I am wrong and ask questions whenever you feel like you are unsure.....**

# Whoami | grep details

## ME

Chief Technology Officer at CTRL Technologies

Studying: MSC Information Security

**Ctrl Tech: Insurance Tech Company**

**Website: takectrl.co.za**

Previous:

- Python Dev
- DevOPS
- Dev/QA in systems performance

## OWASP Cape Town

Open Web Application Security Project.

Non profit for advancing security in web applications and other.

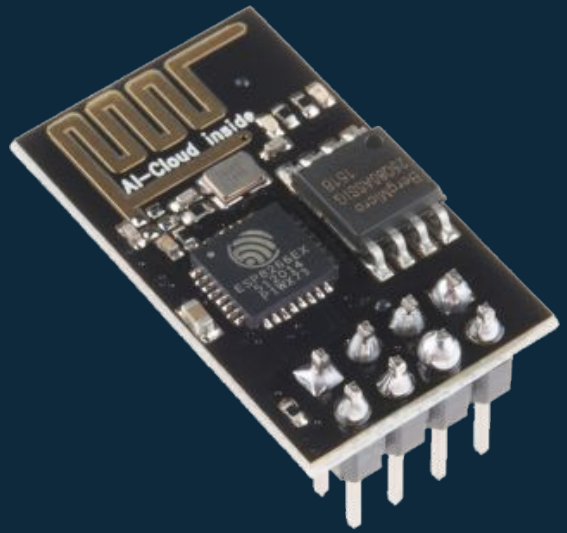
Regular Meetups, all welcome !

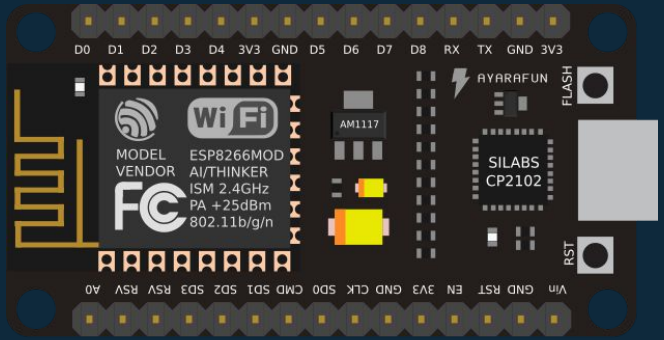
- https://www.owasp.org/index.php/Cape_Town
- http://www.meetup.com/OWASP-Cape-Town-Chapter-Meetup/

1

# ESP8266

Let’s start with the ESP8266



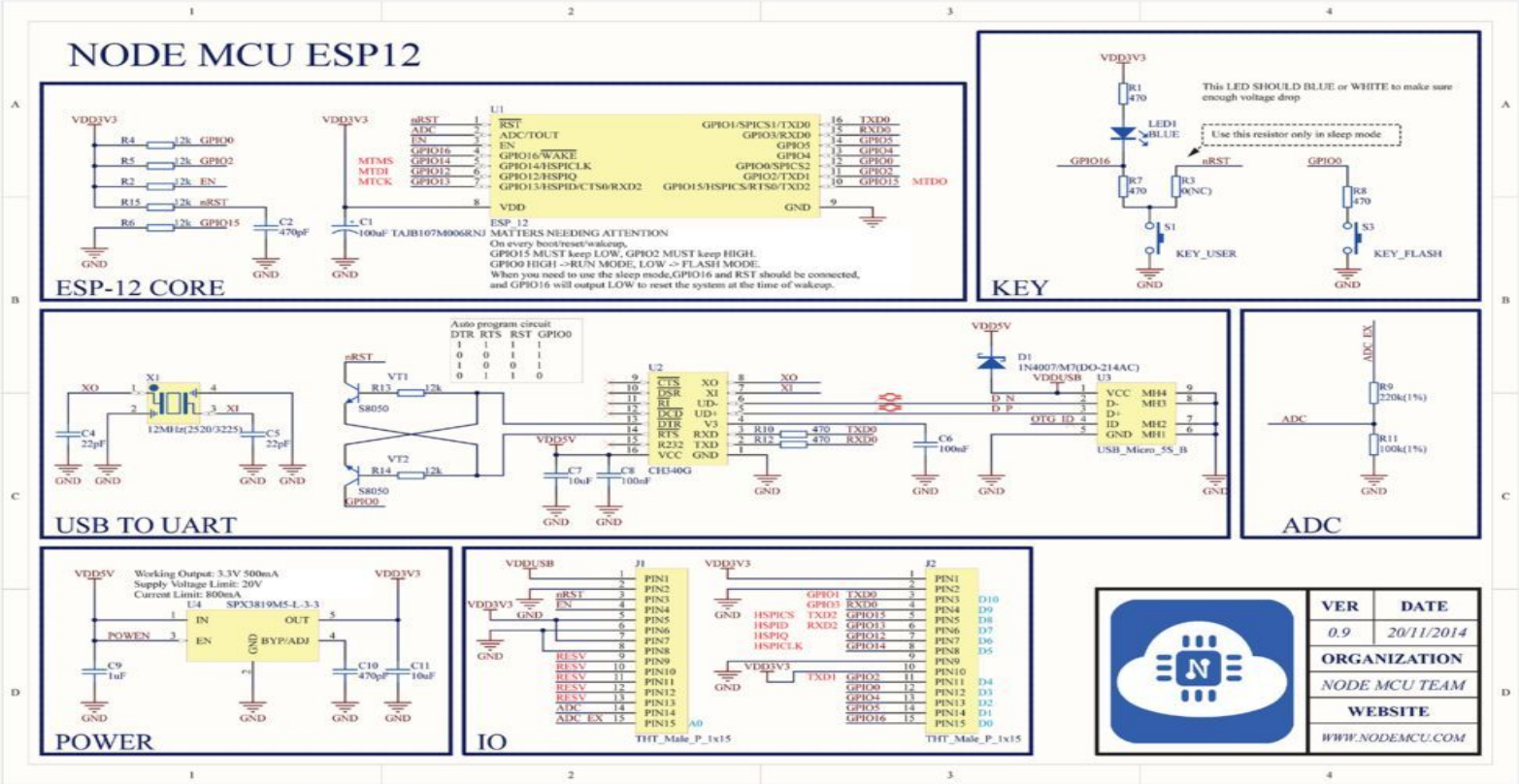
# ESP8266

1

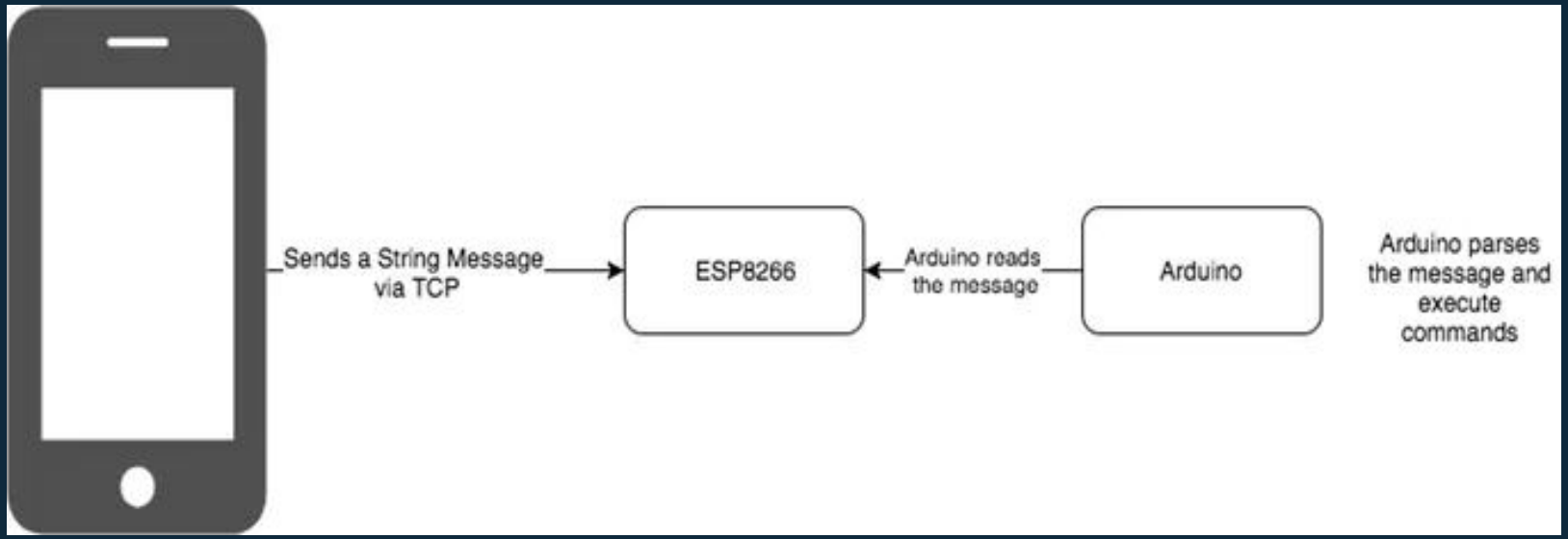
- 32-bit RISC CPU: Tensilica Xtensa LX106 running at 80 MHz*
- 64 KiB of instruction RAM, 96 KiB of data RAM
- External QSPI flash - 512 KiB to 4 MiB* (up to 16 MiB is supported)
- IEEE 802.11 b/g/n Wi-Fi
  - Integrated TR switch, balun, LNA, power amplifier and matching network
  - WEP or WPA/WPA2 authentication, or open networks
- 16 GPIO pins
- SPI, I²C,
- I²S interfaces with DMA (sharing pins with GPIO)
- UART on dedicated pins, plus a transmit-only UART can be enabled on GPIO2
- 1 10-bit ADC

# ESP8266 Internals (ESP-12)

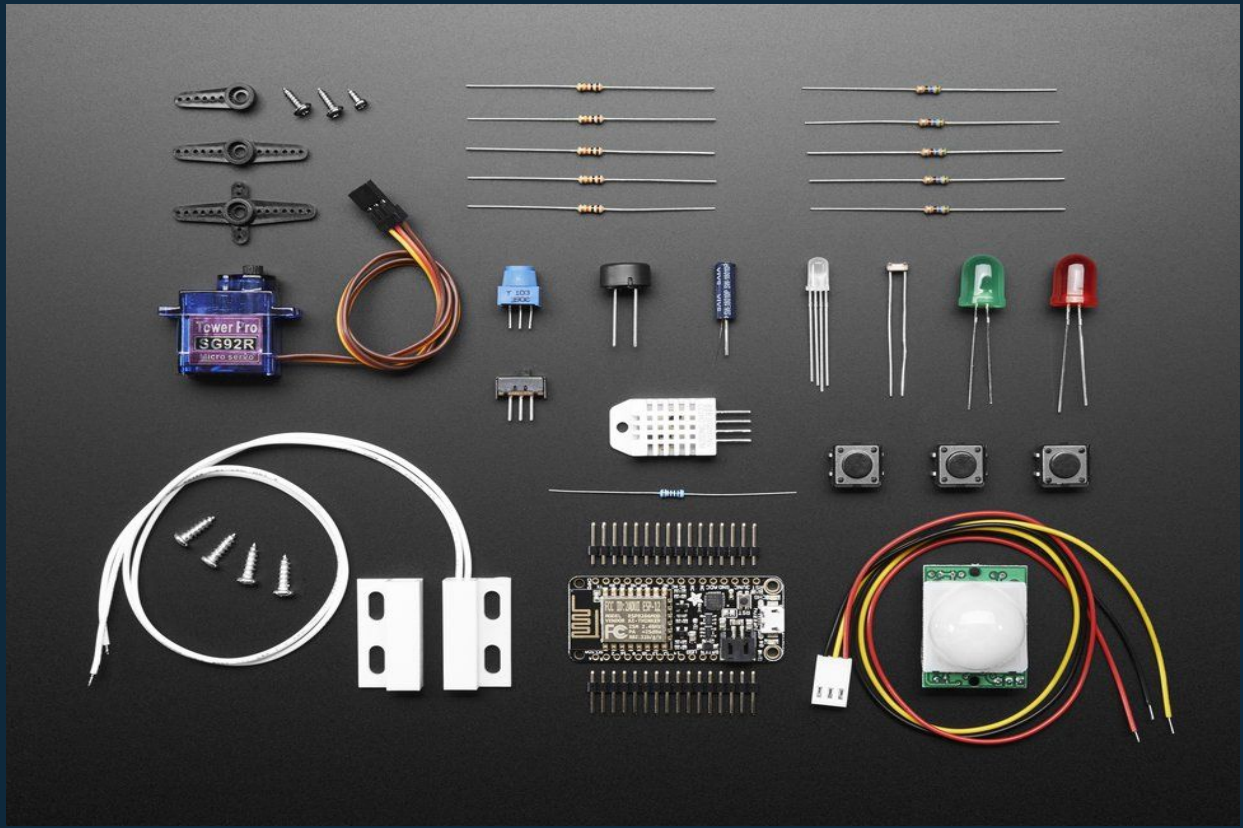
# ESP8266 Internals (ESP-12)



# ESP8266 & Arduino



# ESP8266 & sensors/devices




https://www.adafruit.com/product/2680

2

# Programming the ESP8266

Programming languages, toolchains, etc.

# Languages/Frameworks

- Trusty old C
- Micropython
- Lua (NodeMCU)
- Javascript
- Mongoose OS
- Espruino (Javascript)
- Arduino (C++
- ESP8266 BASIC
- Etc etc etc)

# Micropython

- Micropython:
- WARNING: The port is experimental and many APIs are subject to change.
- 
- Supported features include:
  - REPL (Python prompt) over UART0.
  - Garbage collector, exceptions.
  - Unicode support.
  - Builtin modules: gc, array, collections, io, struct, sys, esp, network, many more.
  - Arbitrary-precision long integers and 30-bit precision floats.
  - WiFi support.

# Micropython

Features continued:

- Sockets using modlwip.
- GPIO and bit-banging I2C, SPI support.
- 1-Wire and WS2812 (aka Neopixel) protocols support.
- Internal filesystem using the flash.
- WebREPL over WiFi from a browser (clients at https://github.com/micropython/webrepl).
- Modules for HTTP, MQTT, many other formats and protocols via https://github.com/micropython/micropython-lib .
- 
- Work-in-progress documentation is available at http://docs.micropython.org/en/latest/esp8266/ .

# Micropython – Docs

https://docs.micropython.org/en/latest/esp8266/esp8266/tutorial/repl.html

https://micropython.org/webrepl/

3

# WIFI/IOT/Smart Devices

Hello world!

5

# Make something smart

# Get Started!

**Adafruit**

https://learn.adafruit.com/category/internet-of-things-iot

**instructables**

http://www.instructables.com/howto/esp8266/

**Hackaday**

https://hackaday.com/tag/esp8266/

**Aliexpress**

https://www.aliexpress.com/wholesale?catId=0&initiative_id=SB_20180406221016&SearchText=esp8266

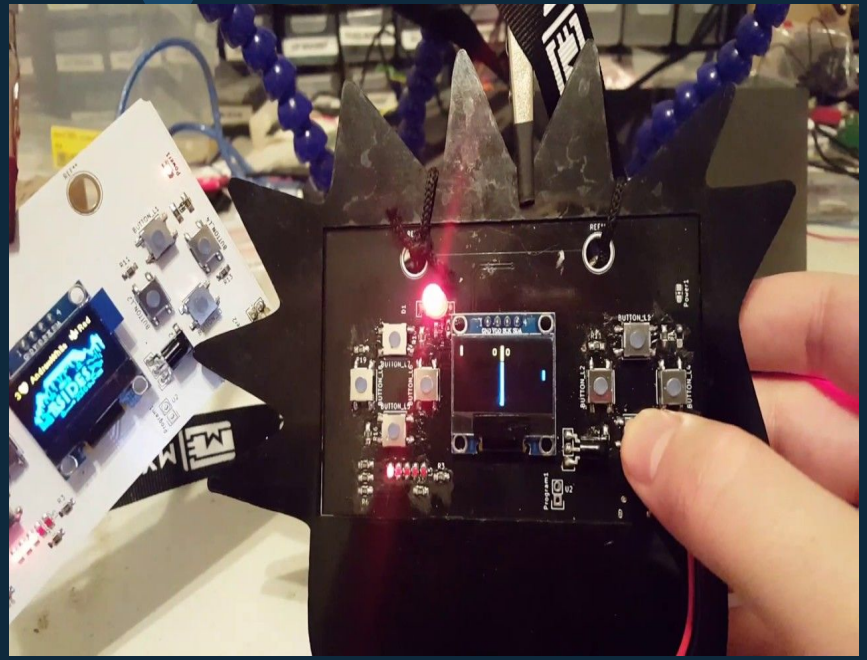
**Intro talk youtube**

https://www.youtube.com/watch?v=srrf-25_Ytw

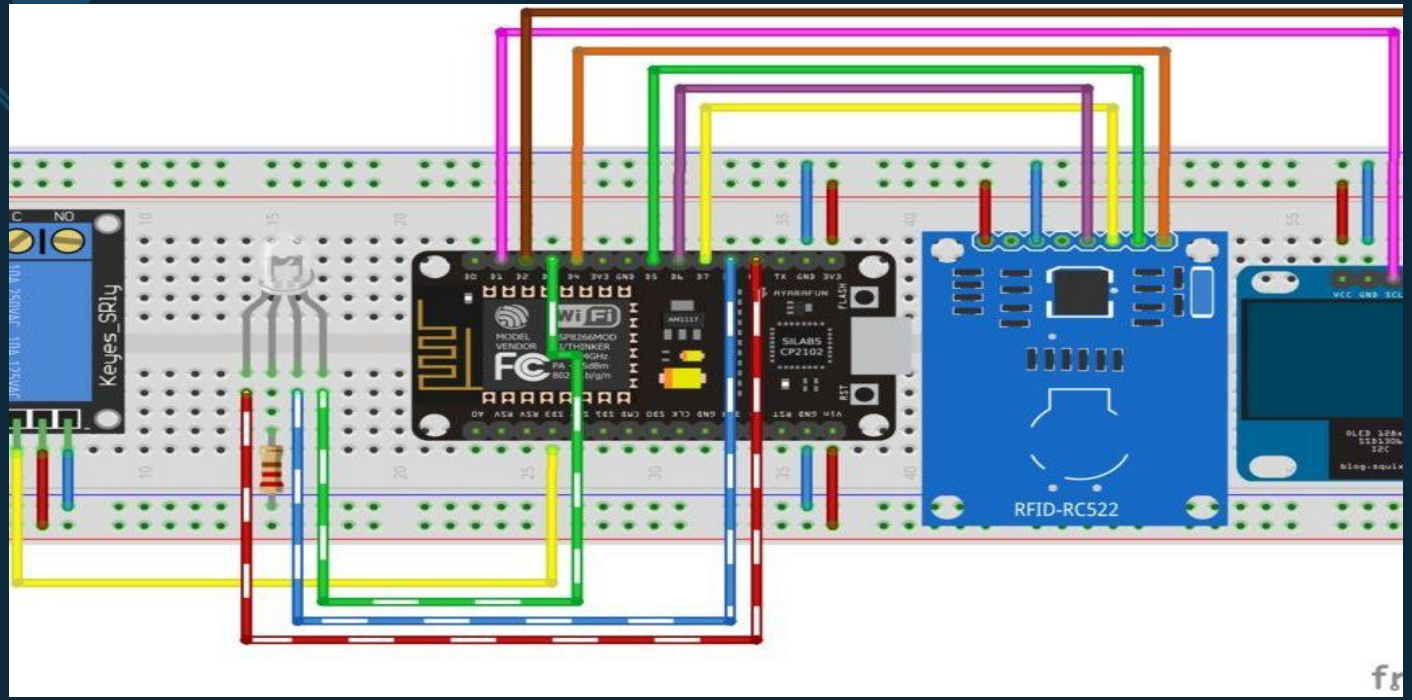
**Follow these geniuses**

- Twitter
  - @elasticninja
  - @AndrewMohawk
- https://robynfarah.com/
- https://www.facebook.com/groups/ArduinoCapeTown/about/

# BSIDES CPT 2016 & 2017



# Access Control
# Wifi + RFID



4

# Security

Insecurity of Things

# Low Level device Access & Wifi

Deauth attacks:

- https://hackernoon.com/deauthentication-attack-and-other-wifi-hacks-using-an-esp8266-module-14f9142b063d
- https://github.com/spacehuhn/esp8266_deauther

Wifi Sniffing:

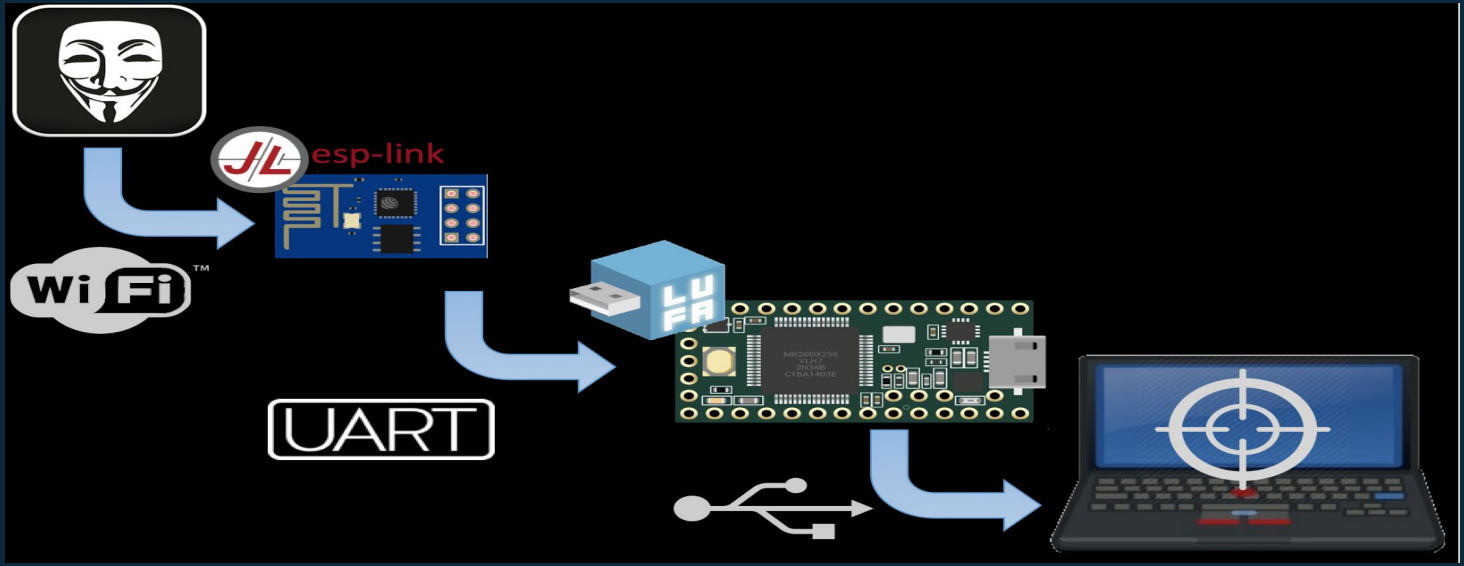
- https://www.hackster.io/rayburne/esp8266-mini-sniff-f6b93a
-

# WIFI KRACK

- Fixing Krack:
  - https://github.com/esp8266/Arduino/issues/3725
  - https://github.com/nodemcu/nodemcu-firmware/issues/2138
- Smoking out KRACK in remote places:
  - http://www.instructables.com/id/ESP8266-OTA-Tutorial-Over-the-Air-Update/
  -

# SensePost badUSB

https://github.com/sensepost/USaBUSe



SHODAN

Explore | Developer Pricing | Enterprise Access | Contact Us

New to Shodan? Login or Register

# The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

## Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

## See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

## Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

## Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

**Balticum TV wireless network (Klaipeda)**
Added on 2018-04-06 19:31:06 GMT
Lithuania, Klaipeda
**Details**

```
<html><title> Test esp8266 </title><meta http-equiv=refresh content=10 /> <h1> Test ESP8266 </h
1><form name='forma1'>Password:<br><input type='password' name='ps' size='20' maxlength='30'></
form><br><br>ds18b20 Temperatura: 5.3125 C
 <br><br>am2320 Temperatura: 2.4 C - RH = 90.2
 <br><br>dth11 T...
```

**OJSC Rostelecom Macroregional Branch South**
Added on 2018-04-06 14:51:04 GMT
Russian Federation, Krasnodar
**Details**

```
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: sw: www.it4it.club, hw: esp8266
Content-Length: 0
Connection: close
```

# Thanks!

## Any questions?

You can find me at:

- @owasp_cpt
- christo<at>christogoosen.co.za
- christo.goosen<at>takectrl.co.za
- christo.goosen<at>owasp.org
- github.com/c-goosen

# Sources

ESP8266:

- https://en.wikipedia.org/wiki/ESP8266
- https://github.com/esp8266/Arduino/blob/master/doc/esp8266wifi/client-secure-examples.rst

IOT Development:

- https://opensource.com/article/17/3/mongoose-os-iot-development
- https://platformio.org/platforms/espressif8266
- https://mongoose-os.com/software.html
- https://mongoose-os.com/docs/reference/api.html

Programming Languages:

- Micropython
  - http://docs.micropython.org/en/latest/pyboard/library/machine.Pin.html
- NodeMCU
  - http://www.nodemcu.com/index_en.html
- Arduino
  - https://github.com/esp8266/Arduino

# Sources

Projects, libraries and examples:

- https://github.com/esp8266/Arduino/blob/master/doc/esp8266wifi/client-secure-examples.rst
- http://www.techparva.com/index.php/2017/09/28/interfacing-mfrc522-rfid-card-esp8266/
- https://github.com/sensepost/USaBUSe
-