Deloitte.
CyberSOC Academy

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

“El internet de los huevos”

EuskalHack Security Congress

Pedro Candel aka @NN2ed_s4ur0n – 23 de junio de 2017

Ponente

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

Whoami

Deloitte.
CyberSOC Academy

```
class PedroC:
    def __init__(self):
        self.name = 'Pedro Candel'
        self.email1 = 'pcandel@cybersoc.deloitte.es'
        self.email2 = 's4ur0n@s4ur0n.com'
        self.website = 'https://www.s4ur0n.com'
        self.nickname = '@NN2ed_s4ur0n'
        self.role = 'Security Researcher'
        self.interest = [ 'Reversing', 'Malware',
                          'Offensive Security', '…' ]
        self.member_of = [ 'mlw.re', 'OWASP',
                           'NetXploit', 'CiberTroll', '…' ]
```

Disclaimer

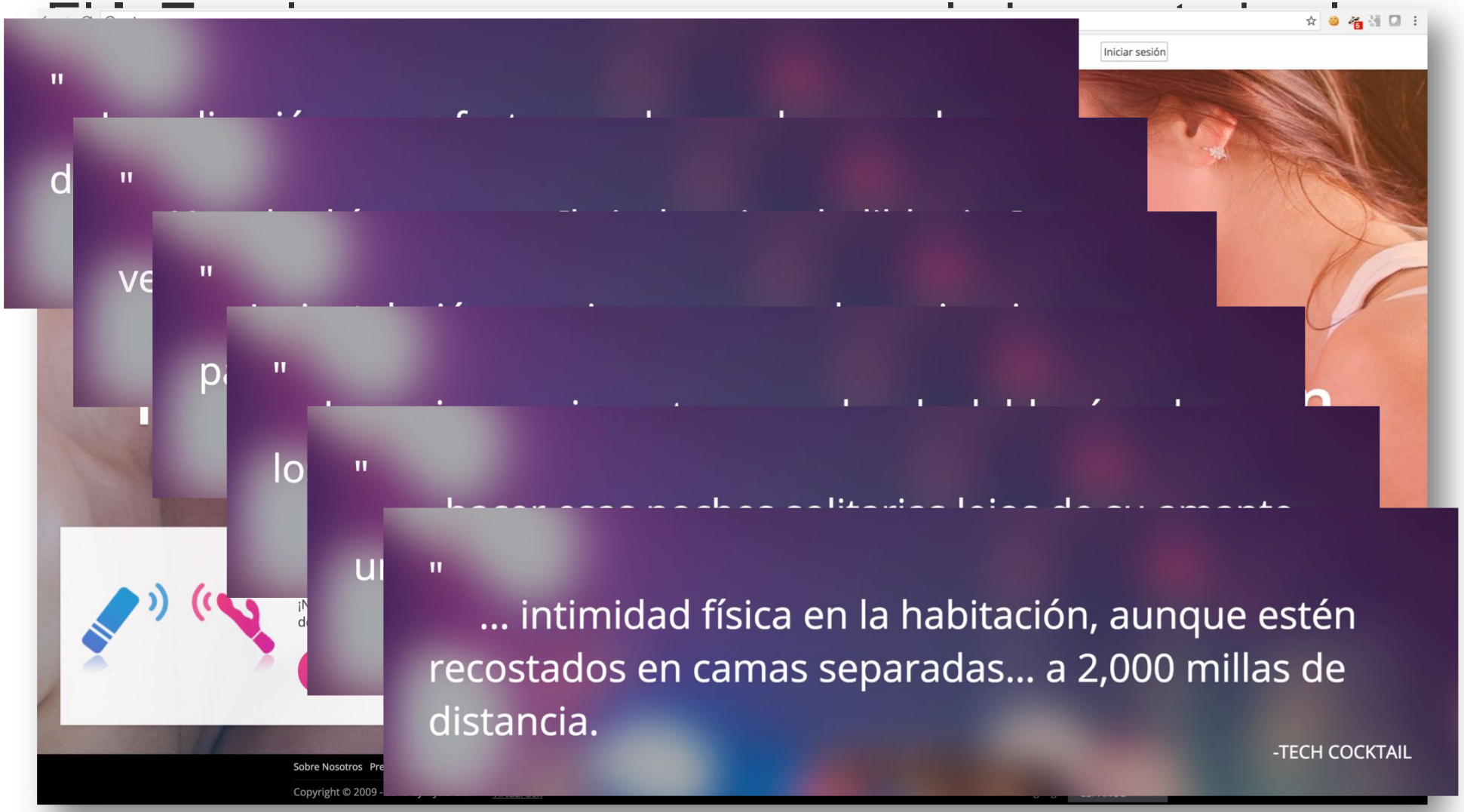
El autor **NO se hace responsable** del uso que se realice de la presentación, código(s), hardware empleado o forma de almacenamiento y/o transporte de los “huevos”

En ningún momento de la investigación, se han visto dañados personas, animales o cosas

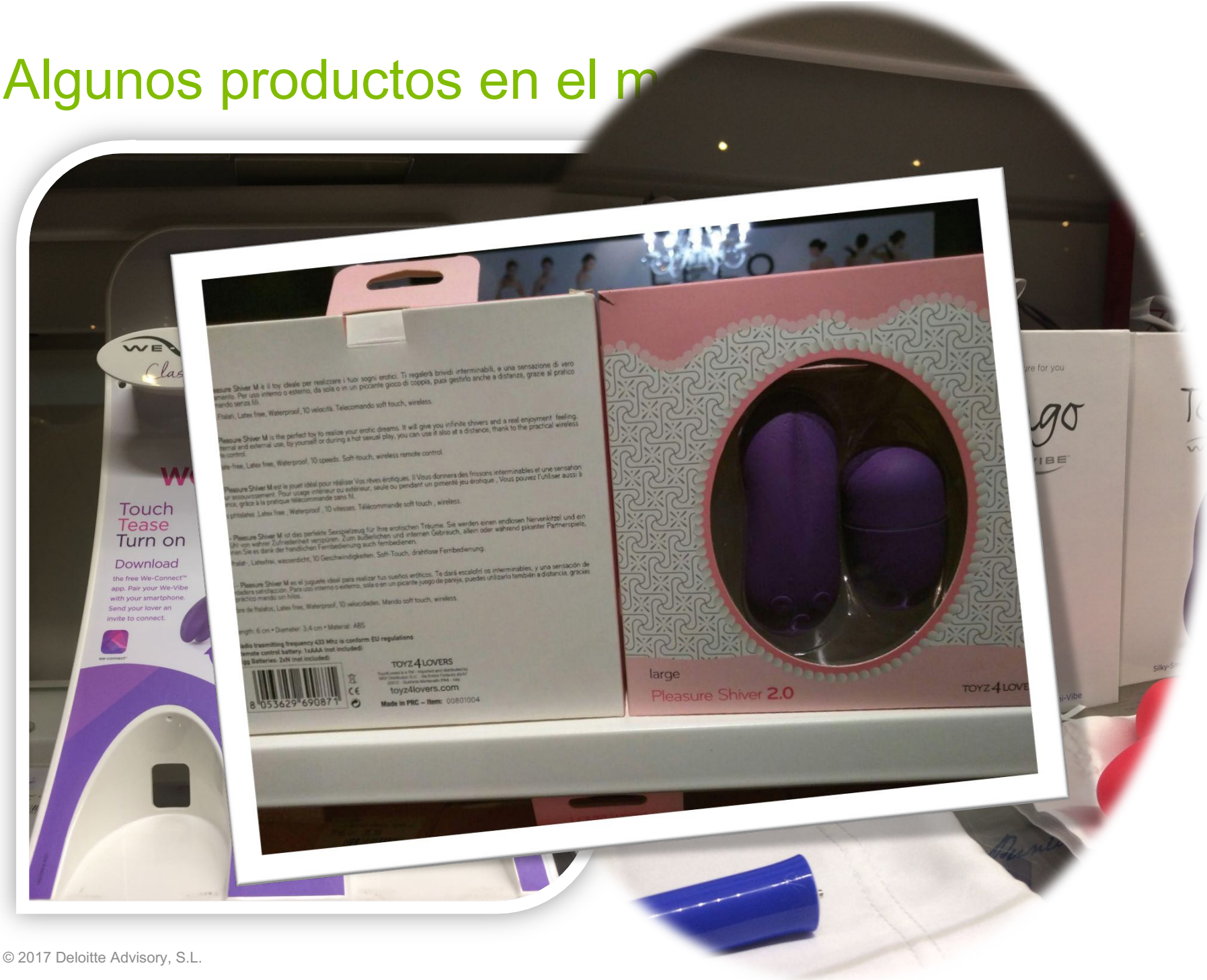
Introducción
IoT(L;DR;)

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

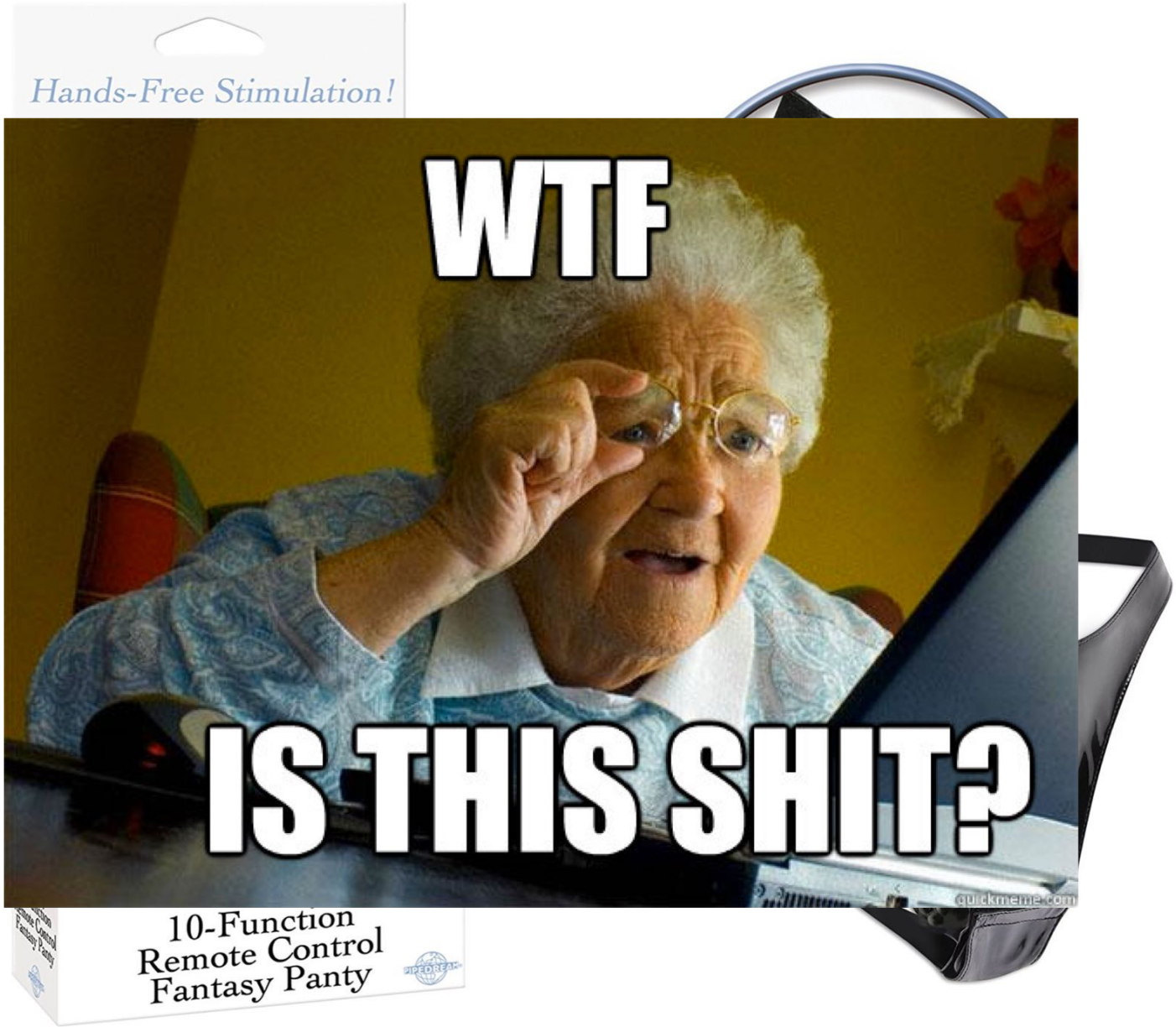
Introducción



Algunos productos en el m



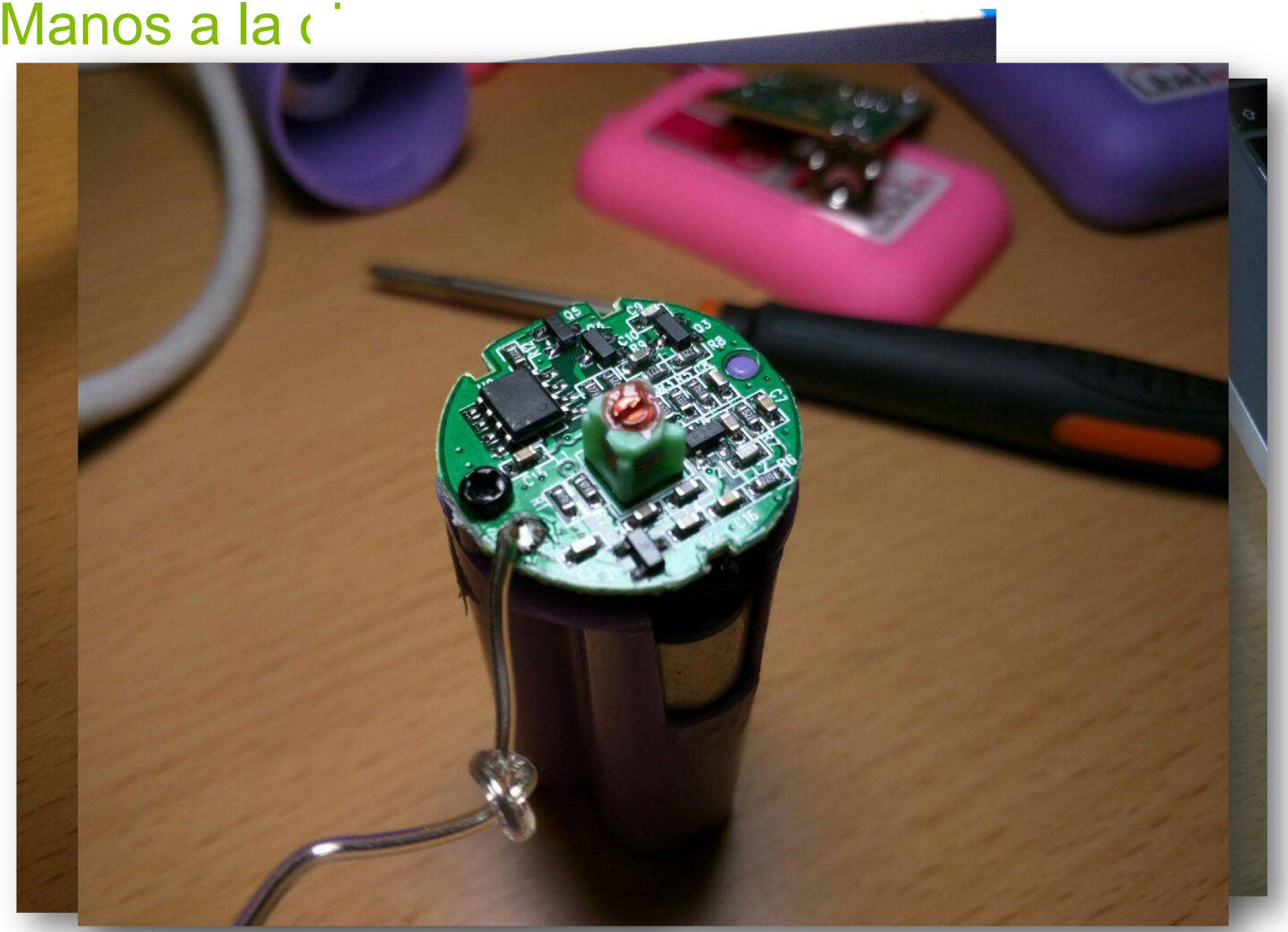
Evolución 2.0 de los productos



Materiales necesarios

- Echarle un poco de caradura
- Por supuesto un huevo o un par de huevos
- Las pilas!!! (Que nunca las incluyen)
- Destornillador de estrella
- Destornillador plano
- SDR (TDT USB stick)
- Arduino Uno o Mini
- Módulo emisor/receptor 433 MHz para Arduino
- Cableado diverso, resistencias, pulsadores
- Recipiente con arroz o convencer a la pareja para que te deje hacer el **eggtesting**
- Vivienda alternativa si el PoC no es satisfactorio

Manos a la



Identificación de componentes

LR4

- 4

Photos



SMD crystal oscillator resonant R433A R315A LR433T2 LR315T2 three-legged 433.92 315M saw 3*7

Unit Price: **$2.10**

Wholesale Price:

Quantity	Price (Per lot)
1 - 3	$2.10
4 - 6	$0.61
7 - 10	$0.40
11 - 15	$0.29

Item#: 18695641445

Location: Huzhou (Zhejiang)

Selected: **"433T2"**

Color classification: 433T2

Quantity: 1 (310190 available)

Shipping Cost: $ 8.13 to US Via China Post Air Mail [Small]

Total price: **$ 2.10 x 1 + $ 8.13 = $ 10.23**

Buy It Now | Add to Cart

Add to My Favorite Item

Radiofrecuencia y terminología

Una **señal** puede ***ser transportada*** en una onda AM o FM

AM (Amplitude Modulation): funciona mediante la variación de la amplitud de la señal transmitida en relación con la información que se envía

Radiofrecuencia y terminología

PWM (Pulse Width Modulation): En el caso de transmitir una clave (p.e. los mandos remotos) puede emplearse este tipo de modulación. La ***duración*** de un pulso determina el bit que se transmite. Un pulso **largo** es un **cero** y un pulso **corto** es un **uno**

OOK (On-Off Keying): Es una forma de codificación por **desplazamiento en amplitud** en la que se representa un valor binario ***basado en la duración*** de la **presencia de una señal portadora** (o simplemente una señal de amplitud alta)

Ingeniería Inversa de llaves estáticas remotas

Captura de la señal

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

Identificación de la señal

Lo primero será **identificar la señal** mediante el SDR en la frecuencia que se encuentre

Se emp
Alexan

En ocas a que
funcion un
barrido o
buscando en la web del fabricante o incluso en las ***especificaciones "declaradas"***

Demo

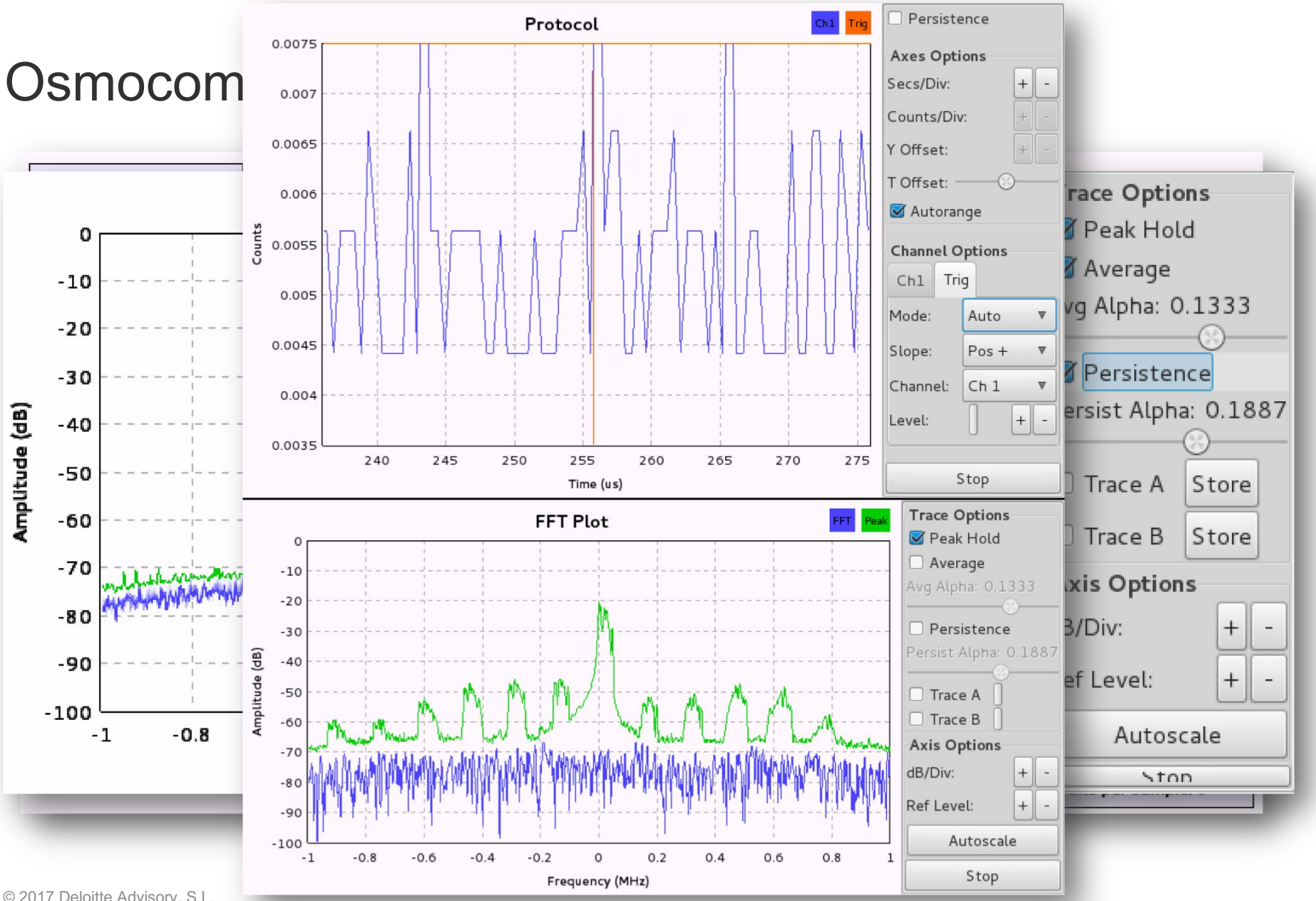
Captura de la señal

Emplearemos el software libre **GNURadio** disponible en (http://gnuradio.org/) y **Audacity** (http://www.audacityteam.org/) o bien mediante un gestor de paquetes.

```
$ sudo apt-get install gnu-radio
$ sudo apt-get install rfcat
$ sudo apt-get install gr-osmosdr
$ sudo apt-get install audacity
$ systemctl --user enable pulseaudio
$ systemctl --user start pulseaudio
$ gnuradio-companion
```

Diagrama de flujos para aislar la señal

Osmocom



Demo

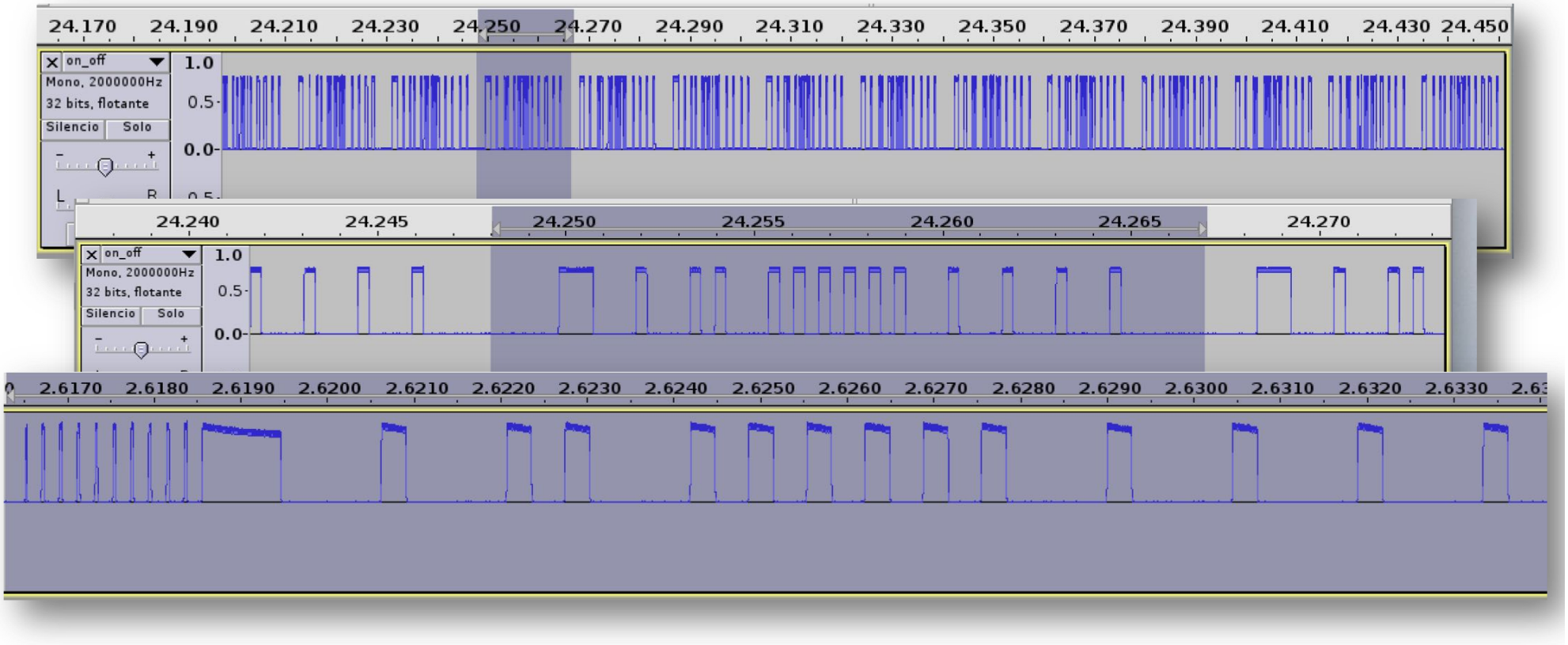
Ingeniería Inversa de llaves estáticas remotas

Análisis de la señal

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

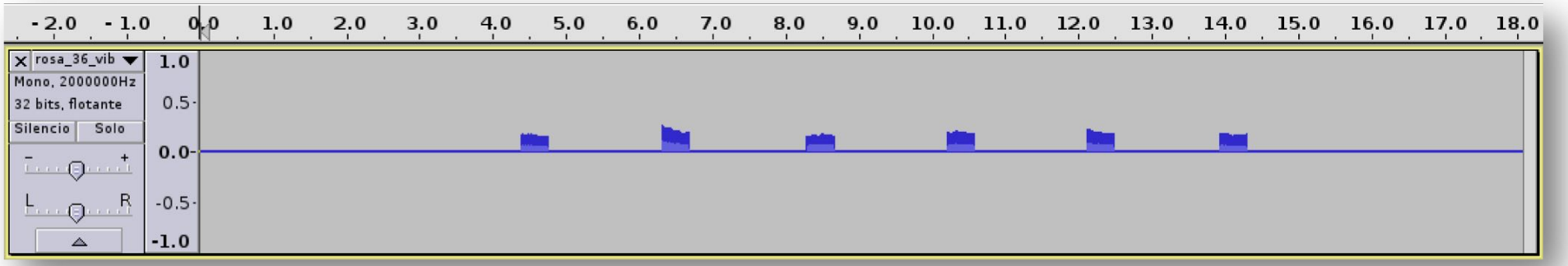
Análisis de la señal

Función “Encendido / Apagado”:



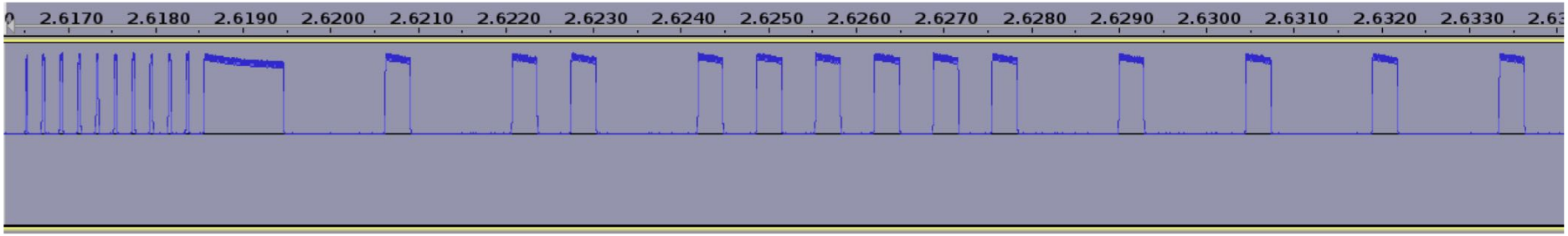
Análisis de la señal

Función “Cambiar Vibración”:



Análisis de la señal

Secuencia **encender** en el IoT de color **rosa**:



Sync:

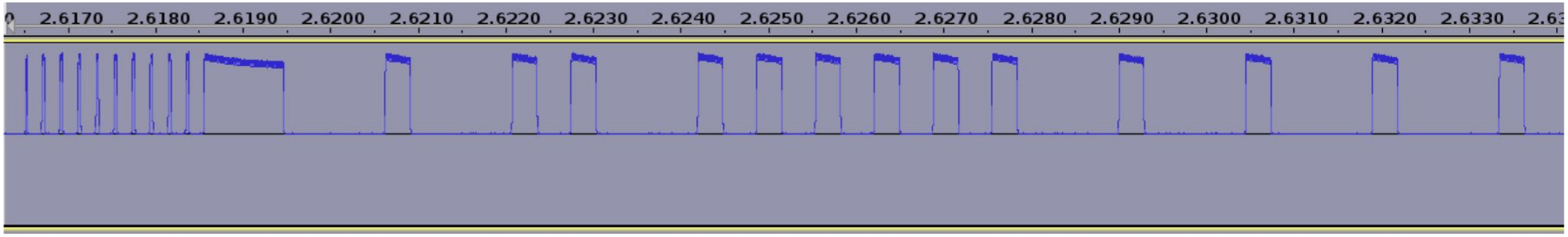
1.1.1.1.1.1.1.1.1.1. (10 veces)

Data (on):

Preamble	Databits	Dec
1-1 ligado (2)	01011011111101010101 (20)	376661

Análisis de la señal

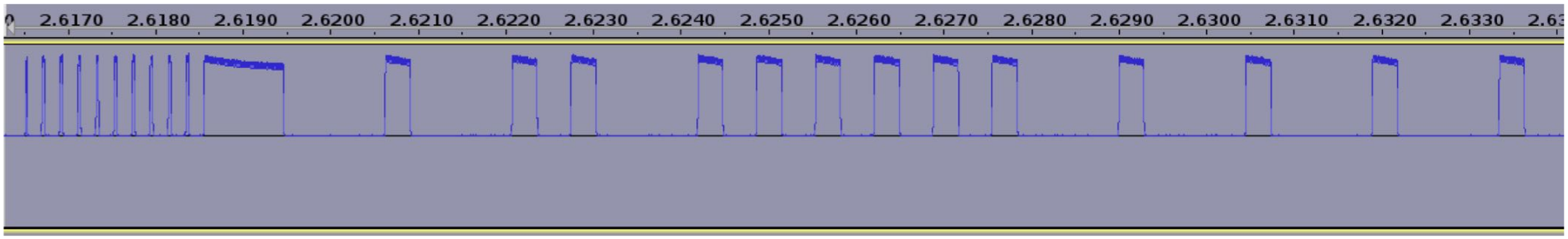
Secuencia **encender** en el IoT de color **rosa**:



1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Análisis de la señal

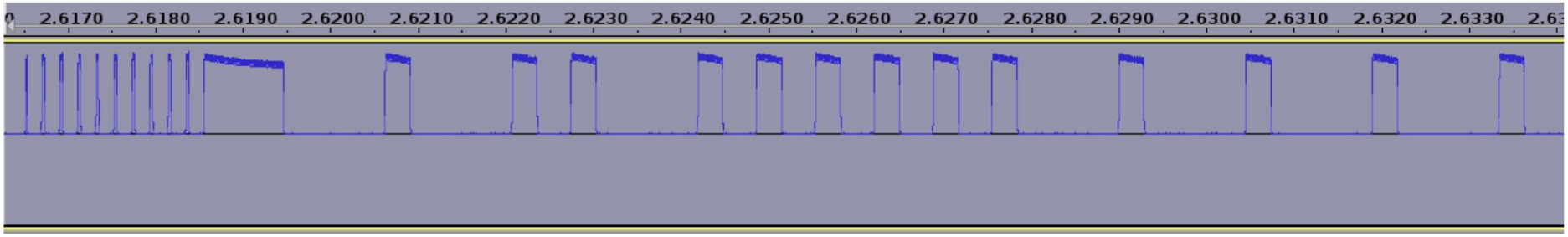
Secuencia **encender** en el IoT de color **rosa**:



1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Análisis de la señal

Secuencia **encender** en el IoT de color **rosa**:

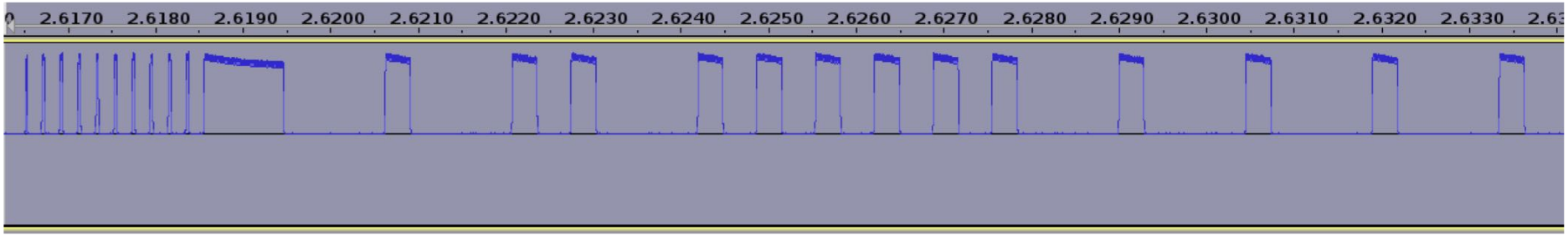


1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Total: **20 veces** cada vez que se pulsa el botón

Análisis de la señal

Secuencia **encender** en el IoT de color **morado**:



Sync:

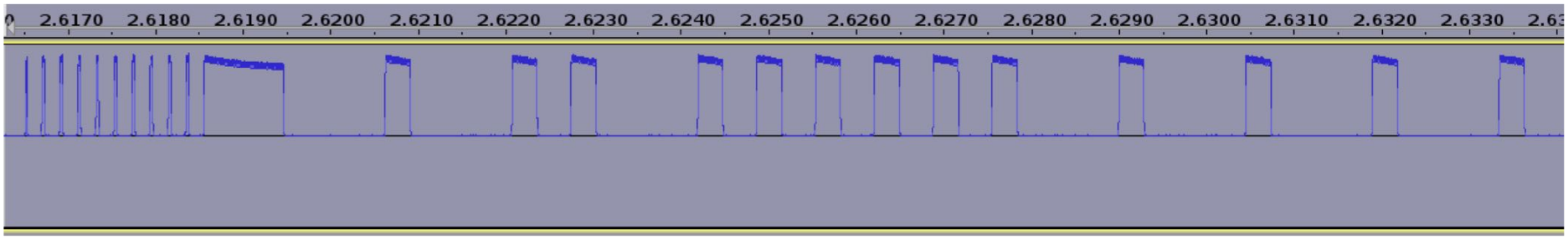
1.1.1.1.1.1.1.1.1.1. (10 veces)

Data (on):

Preamble	Databits	Dec
1-1 ligado (2)	01011011111101010101 (20)	376661

Análisis de la señal

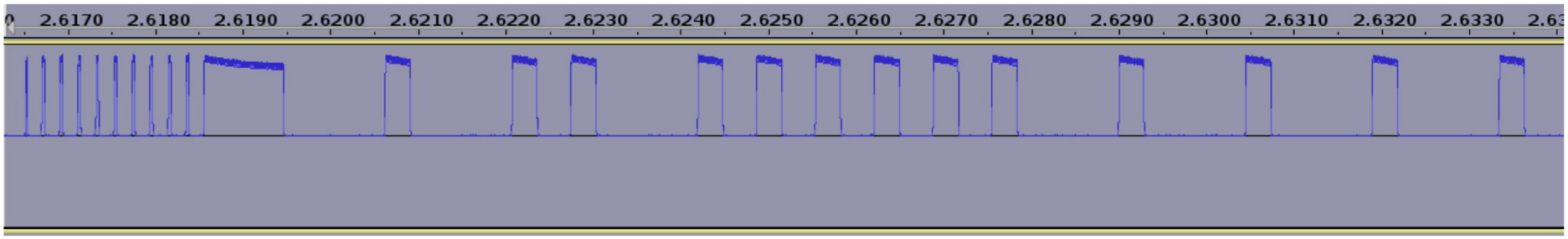
Secuencia **encender** en el IoT de color **morado**:



1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Análisis de la señal

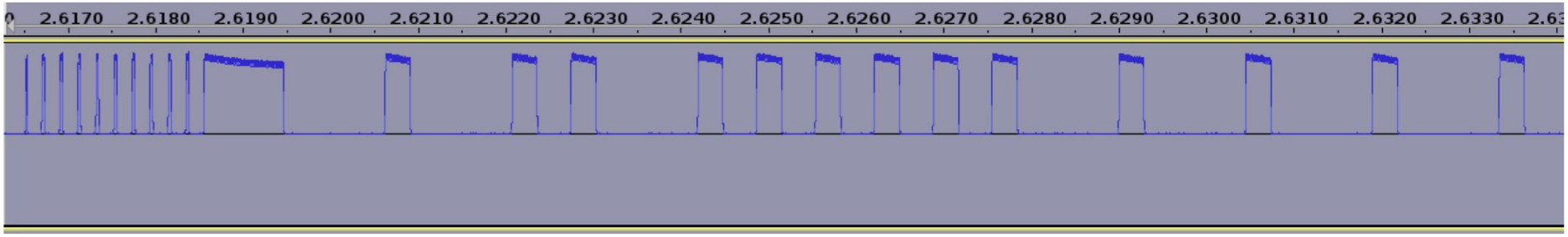
Secuencia **encender** en el IoT de color **morado**:



1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Análisis de la señal

Secuencia **encender** en el IoT de color **morado**:



1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)
1-1 ligado (2) 01011011111101010101 (20)

Total: **20 veces** cada vez que se pulsa el botón

Análisis de la señal

Diferencia(s) **encender** en los IoT color **rosa/morado**:

Sync en **rosa**
1.1.1.1.1.1.1.1.1.1. (10 veces)

Sync en **morado:**
1.1.1.1.1.1.1.1.1.1. (10 veces)

Conclusión: se emplea la misma sincronización de trama en ambos

Análisis de la señal

Diferencia(s) **encender** en los IoT color **rosa/morado**:

Preamble en **rosa**
1-1 ligado

Preamble en **morado:**
1-1 ligado

Conclusión: se emplea el mismo preámbulo en ambos

Análisis de la señal

Diferencia(s) **encender** en los IoT color **rosa/morado**:

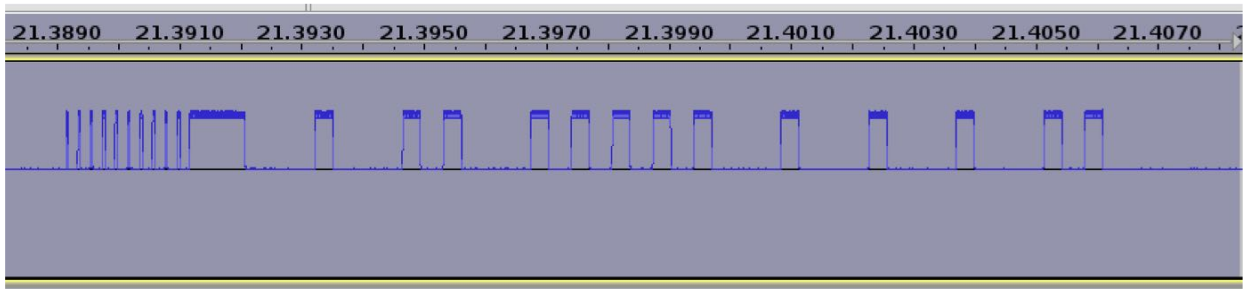
Datos en **rosa**
01011011111101010101 (20) 376661 (Dec)

Datos en **morado:**
01011011111101010101 (20) 376661 (Dec)

Conclusión: se emplea la misma secuencia en ambos y posiblemente en todas las series

Análisis de la señal

Secuencia **apagar** en el IoT de color **rosa**:



Sync:

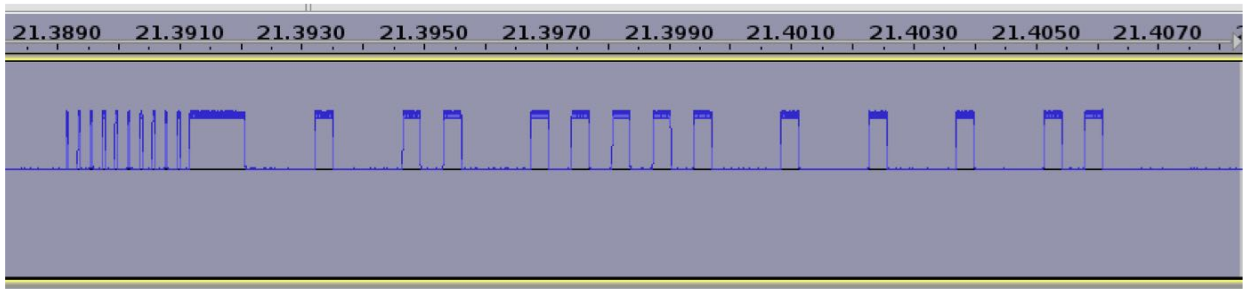
1.1.1.1.1.1.1.1.1.1. (10 veces)

Data (on):

Preamble	Databits	Dec
1-1 ligado (2)	01011011111010101011 (20)	376491

Análisis de la señal

Secuencia **apagar** en el IoT de color **rosa**:



1-1 ligado (2) 01011011111010101011 (20) 376491
1-1 ligado (2) 01011011111010101011 (20) 376491
1-1 ligado (2) 01011011111010101011 (20) 376491

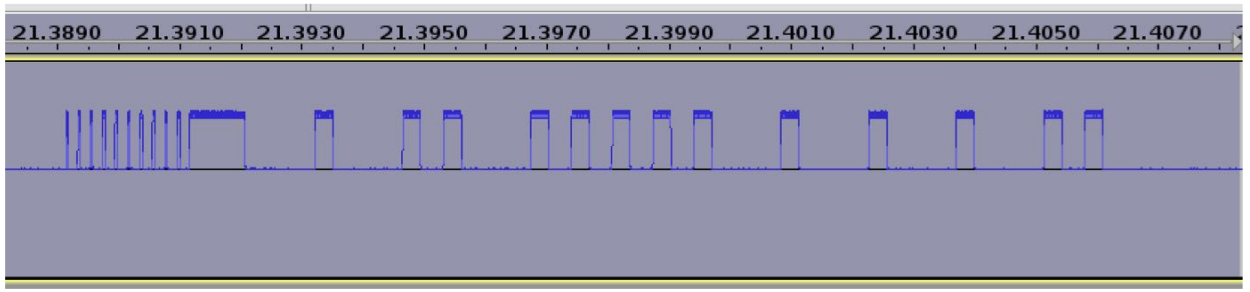
...

1-1 ligado (2) 01011011111010101011 (20) 376491

Total: **20 veces** cada vez que se pulsa el botón

Análisis de la señal

Secuencia **apagar** en el IoT de color **morado**:



Sync:

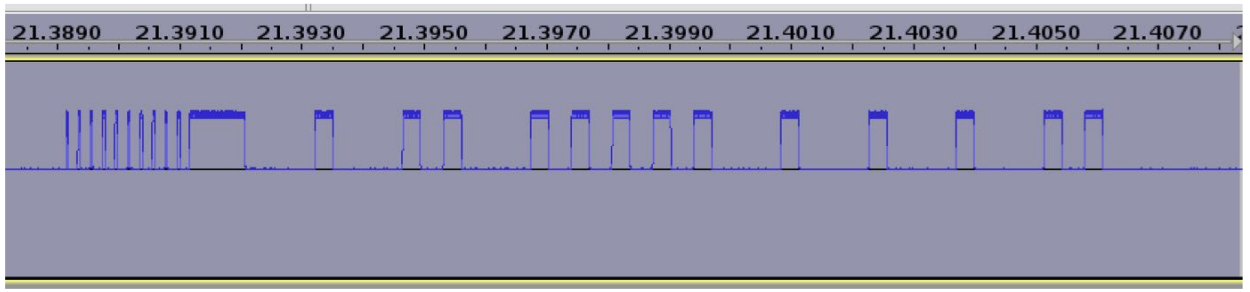
1.1.1.1.1.1.1.1.1.1. (10 veces)

Data (on):

Preamble	Databits	Dec
1-1 ligado (2)	01011011111010101011 (20)	376491

Análisis de la señal

Secuencia **apagar** en el IoT de color **morado**:



1-1 ligado (2) 01011011111010101011 (20) 376491
1-1 ligado (2) 01011011111010101011 (20) 376491
1-1 ligado (2) 01011011111010101011 (20) 376491

...

1-1 ligado (2) 01011011111010101011 (20) 376491

Total: **20 veces** cada vez que se pulsa el botón

Análisis de la señal

Diferencia(s) **apagar** en los IoT color **rosa/morado**:

Sync en **rosa**
1.1.1.1.1.1.1.1.1.1. (10 veces)

Sync en **morado:**
1.1.1.1.1.1.1.1.1.1. (10 veces)

Conclusión: se emplea la misma sincronización de trama en ambos

Análisis de la señal

Diferencia(s) **apagar** en los IoT color **rosa/morado**:

Preamble en **rosa**
1-1 ligado

Preamble en **morado:**
1-1 ligado

Conclusión: se emplea el mismo preámbulo en ambos

Análisis de la señal

Diferencia(s) **apagar** en los IoT color **rosa/morado**:

Datos en **rosa**
01011011111010101011 (20) 376491 (Dec)

Datos en **morado:**
01011011111010101011 (20) 376491 (Dec)

Conclusión: se emplea la misma secuencia en ambos y posiblemente en todas las series

Análisis de la señal

Diferencia(s) **enceder** y **apagar** en los IoT

Datos **encender:**
01011011111101010101 (20) 376661 (Dec)

Datos **apagar:**
01011011111010101011 (20) 376491 (Dec)

0101101111**10101010**1 (8) 170 (Dec)
0101101111**01010101**1 (8) 85 (Dec)

Conclusión: encender = NOT(encender) o bien apagar = NOT(apagar)

Análisis de la señal de vibración

Secuencia **cambiar** en el IoT de color **rosa** y **morado**:

Sync:

1.1.1.1.1.1.1.1.1.1. (10 veces)

Data (first):

Preamble	Databits	Dec
1-1 ligado (2)	01011011011011101101 (20)	374509

…

Total: **20 veces**

Análisis de la señal de vibración

¿Os suena ya la secuencia?

Análisis de la señal de vibración

Secuencia **cambiar** en el IoT de color **rosa** y **morado**:

Data (first):

Preamble	Databits	Dec
1-1 ligado (2)	01011011011011101101 (20)	374509

...

Total: **20** repeticiones

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011110101010111 (20)	188075

...

Total: **20** repeticiones

Análisis de la señal de vibración

Secuencia **cambiar** en el IoT de color **rosa** y **morado**:

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011101011011101 (20)	375517

...

Total: **20** repeticiones

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011011011101101 (20)	374509

...

Total: **20** repeticiones

Análisis de la señal de vibración

Secuencia **cambiar** en el IoT de color **rosa** y **morado**:

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011110101010111 (20)	376151

...

Total: **20** repeticiones

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011101011011101 (20)	375517

...

Total: **20** repeticiones

Análisis de la señal de vibración

Secuencia **cambiar** en el IoT de color **rosa** y **morado**:

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011011011101101 (20)	374509

...

Total: **20** repeticiones

Data (next):

Preamble	Databits	Dec
1-1 ligado (2)	01011011110101010111 (20)	376151

...

Total: **20** repeticiones

Análisis de la señal de vibración

Secuencia **cambio de vibración** en el IoT de color **rosa** y **morado**:

Data (next):

Preamble Databits Dec

1-1 ligado (2) …

...

Total: **20** repeticiones

Análisis de la señal de vibración

Diferencias en **cambio de vibración** en los IoT:

Seq. 01: 01011011**0110111011**01 886 (Dec)
Seq. 02: 01011011**1101010101**11 1707 (Dec)
Seq. 03: 01011011**1010110111**01 1390 (Dec)

Seq. 04: 01011011**0110111011**01 **886 (Dec)**
Seq. 05: 01011011**1101010101**11 **1707 (Dec)**
Seq. 06: 01011011**1010110111**01 **1390 (Dec)**

Seq. 07: 01011011**0110111011**01 **886 (Dec)**
Seq. 08: 01011011**1101010101**11 **1707 (Dec)**

…

Análisis de la señal de vibración

Conclusiones:

Los dispositivos IoT disponen de **36 vibraciones**

Vibración(n) = n mod 3

Seq. 01: 01011011**011011101101** (1 mod 3) = **1**
Seq. 02: 01011011**101010101111** (2 mod 3) = **2**
Seq. 03: 01011011**101011011101** (3 mod 3) = **0**

…

Seq. 26: (26 mod 3) = 2 01011011**101010101111**

…

Seq. 36: (36 mod 3) = 0 01011011**101011011101**

Ingeniería Inversa de llaves estáticas remotas

Reproducción de la señal

Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

Reproducción de la señal

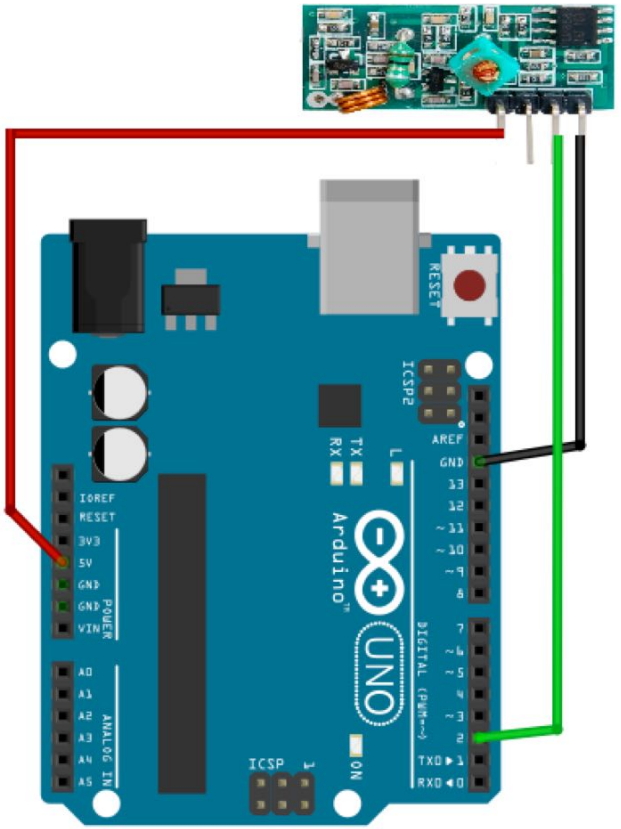
https://www.thehackersgarage.com

Box #2 (Noviembre 2016)

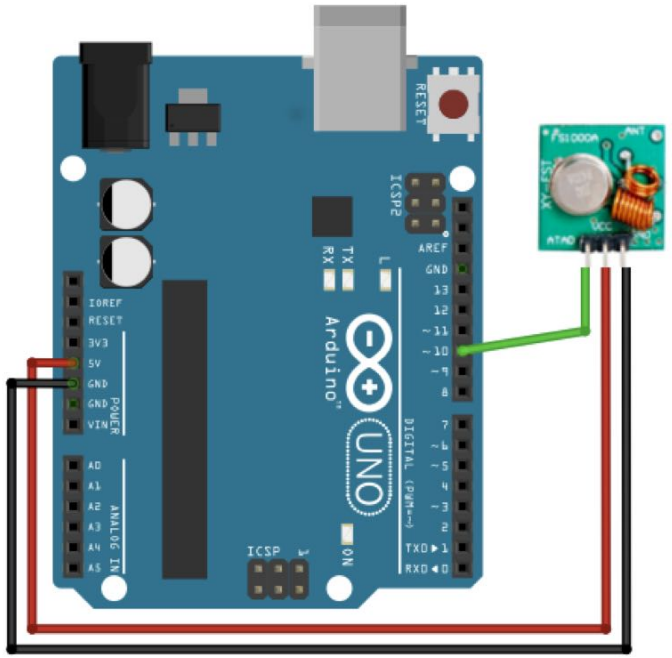
- DVB-T + DAB + FM RTL2832U + R820T2 Digital SDR TV Dongle + Antenna + Remote Control
- 3D printed SDR DVBT DAB Antenna Base
- Arduino UNO
- TFT 2.4 Touch Screen for Arduino
- 433Mhz Receiver Module
- 433Mhz Transmitter Module
- 433Mhz Garage Door Opener
- Transparent Lock
- Transparent box for electronic components storage
- Ninja wallet - 18 tools in 1
- 9V battery snap connector
- 6 Wires - male/female

Reproducción de la señal

Receptor



Emisor



Demo

Preguntas

¿Alg nta?

Muchas gracias

Deloitte.