

HARDWARE HACKING Y USO EN BLUE TEAM Y RED TEAM

/Rooted®



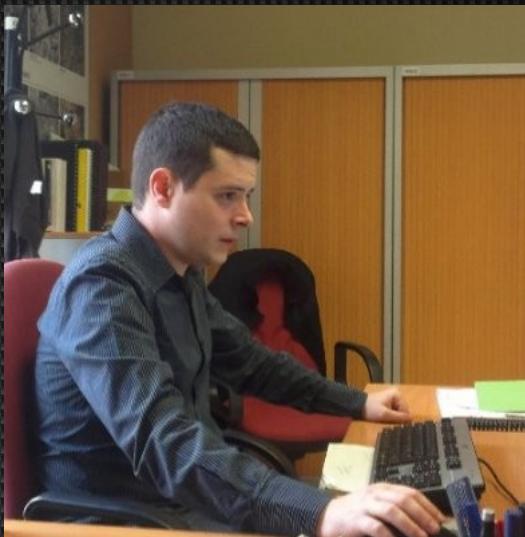
DISCLAIMER

Toda la información aquí presentada es meramente informativa y orientada al pentesting y hacking ético.



Image courtesy: Mikhail Romanenko

ACERCA DE NOSOTROS



Joel Serna Moreno
Ernesto Sánchez Pano

 @JoelSerna 
 @ernesto_xload 

- Interesados en: ciberseguridad, radio, DIY, hacking ...

RESUMEN

Parte I: ¿de dónde venimos y a donde vamos?

- ¿De dónde viene éste proyecto?
- ¿Por qué hackear una videoconsola openhardware?
- Sobre el hardware hacking

Parte II: Con las manos en la masa

- Identificando el hardware y el conexionado
- Haciéndonos la vida más fácil: el bootloader y el IDE
- Hola mundo y primeras pruebas

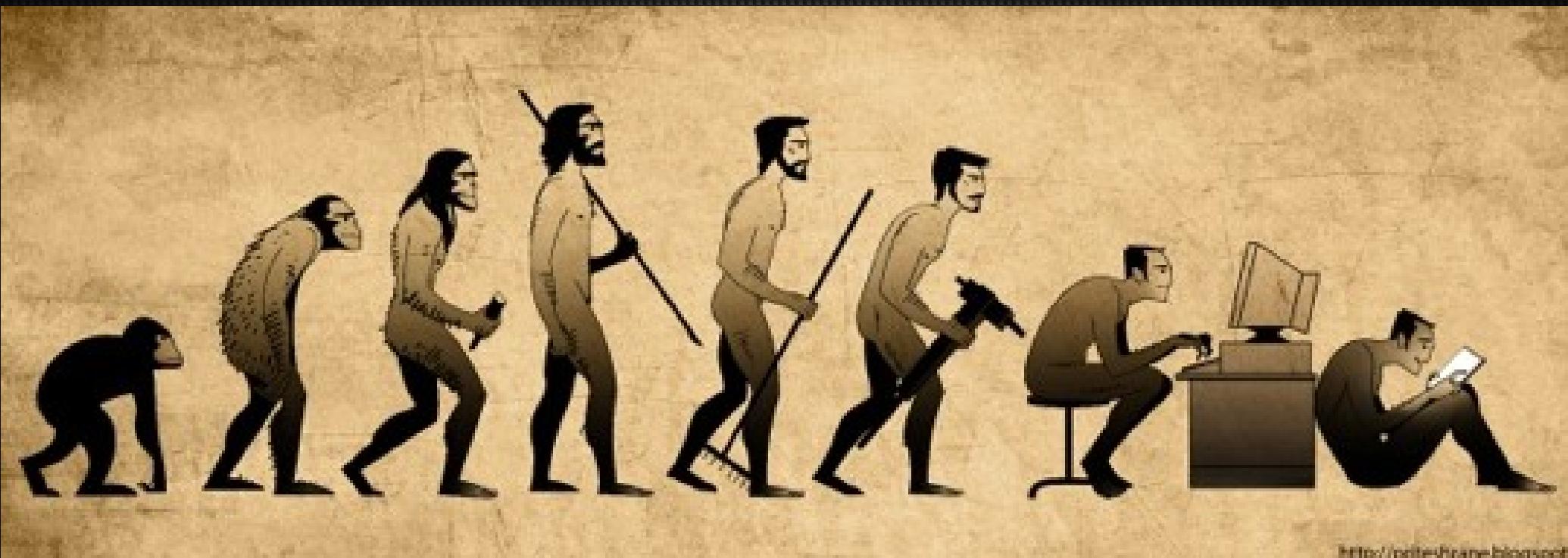
Parte III: ¿Y ahora que?

- Gestor contraseñas por hardware (BlueTeam)
 - Protección del hardware contra lectura
 - Explicación del código
- Haciendo el mal (RedTeam): badUSB con menús
 - Explicación del código
- Posibles mejoras futuras
 - Librería de menús

Despedida, contacto y preguntas

PARTE I

¿DE DÓNDE VENIMOS Y A DONDE VAMOS?



<http://priteshnae.blogspot.com>

ARDUBOY



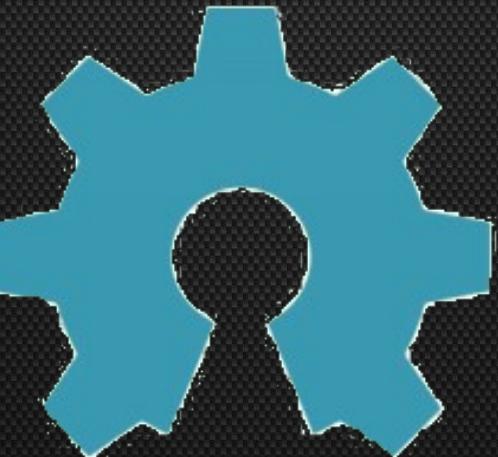
¿DE DÓNDE VIENE ESTE PROYECTO?

Hardware = FUN

Source: <http://www.flickr.com/photos/neimod/>

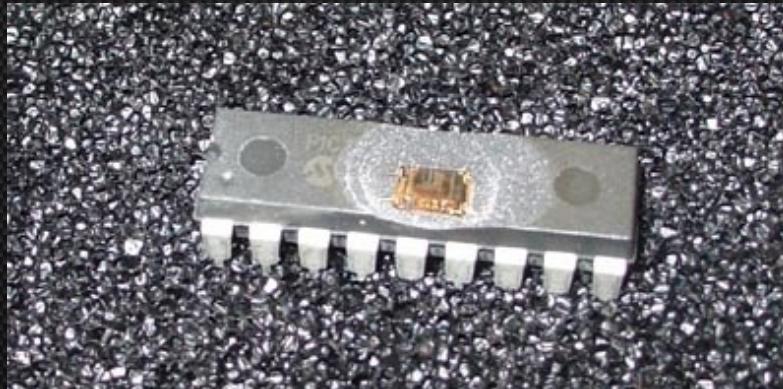
PORQUÉ HACKEAR UNA CONSOLA LIBRE

- Como entrenamiento y entretenimiento.
- Es una forma fácil y sencilla de comprobar nuestros resultados.
- Tiene una amplia documentación y comunidad, tanto de Arduboy como de Arduino



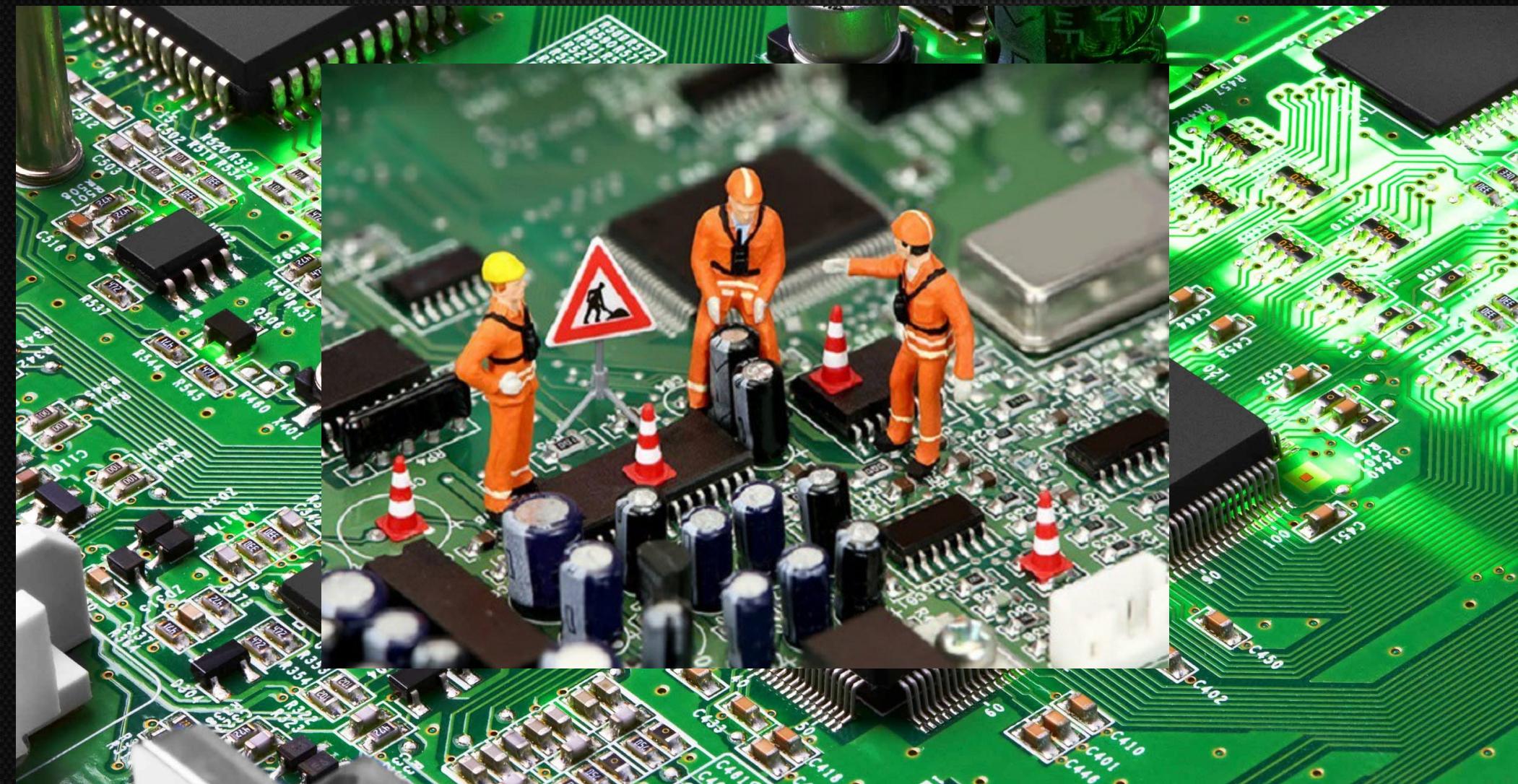
SOBRE HARDWARE HACKING

- Destinamos una videoconsola a otro uso (ciberseguridad)
- Esta es una charla de introducción y motivación
- No se van a tratar sistemas avanzados y complejos.



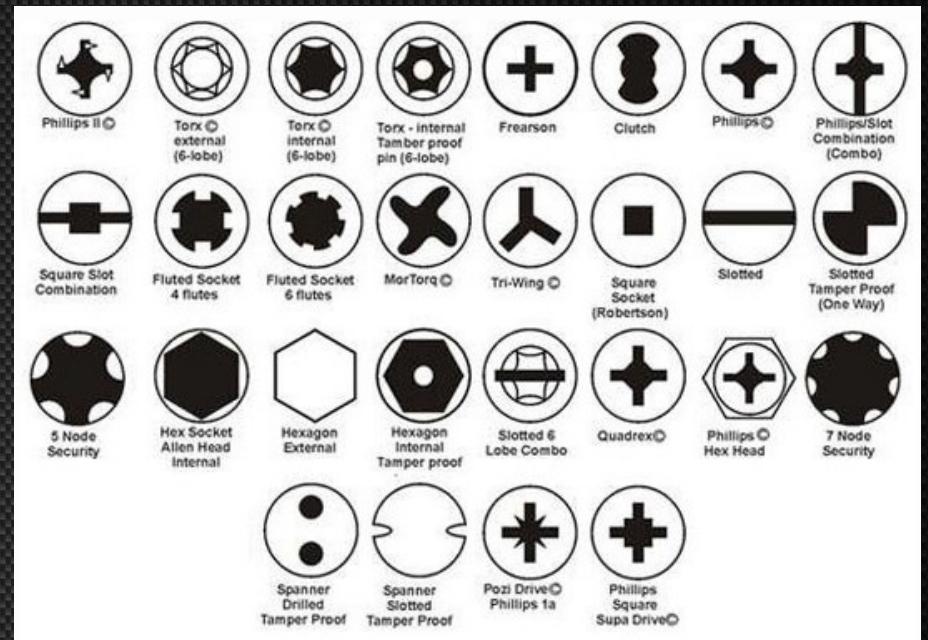
PARTE II

CON LAS MANOS EN LA MASA



ACCEDIENDO AL CIRCUITO (I)

- Protecciones:
 - Tornillos de seguridad
 - Remaches
 - Carcasas selladas
 - Sistemas anti-tamper
 - Precintos



Chrome Vanadium 100pcs Security Screwdriver Tamperproof Torx Hex Bit Set

★ ★ ★ ★ ★ Be the first to write a review.

Condition: New

Bulk savings: Buy 1 \$10.95/ea Buy 2 \$10.40/ea Buy 3 \$10.29/ea

Quantity: 1 4 or more for \$10.07/ea

More than 10 available / [5 sold](#)

Unit price: US \$10.95/ea

[Buy It Now](#) [Add to cart](#) [Make Offer](#) [Add to watch list](#)

Longtime member

Shipping: \$0.00 - International Shipping | See details

See details about international shipping here. Item location: Shenzhen, Guangdong, China Ships to: Worldwide See exclusions

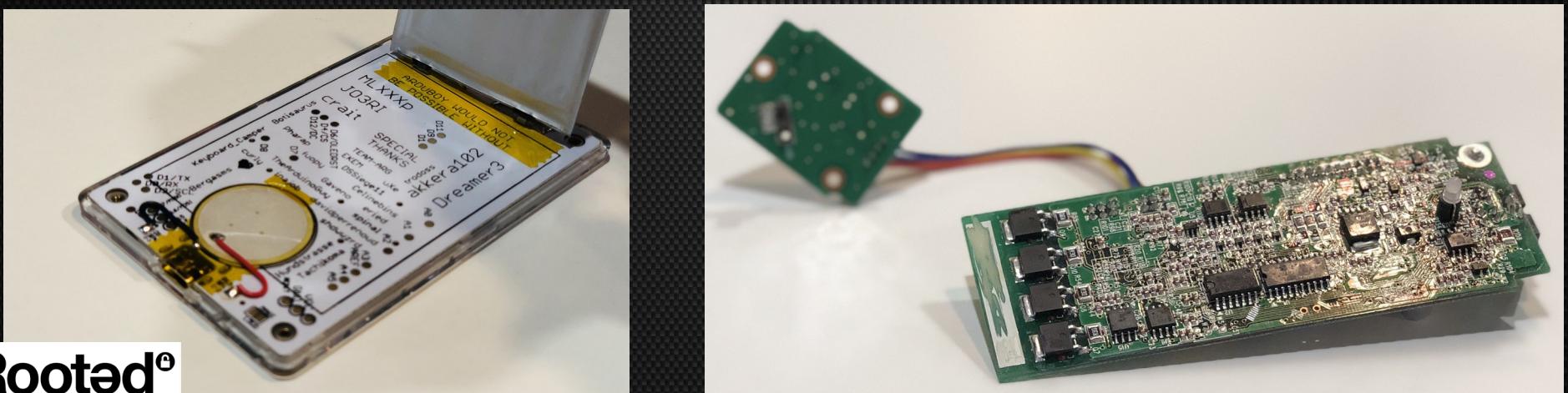
ACCEDIENDO AL CIRCUITO (II)

- Protecciones:
 - Resinas epoxy / siliconas



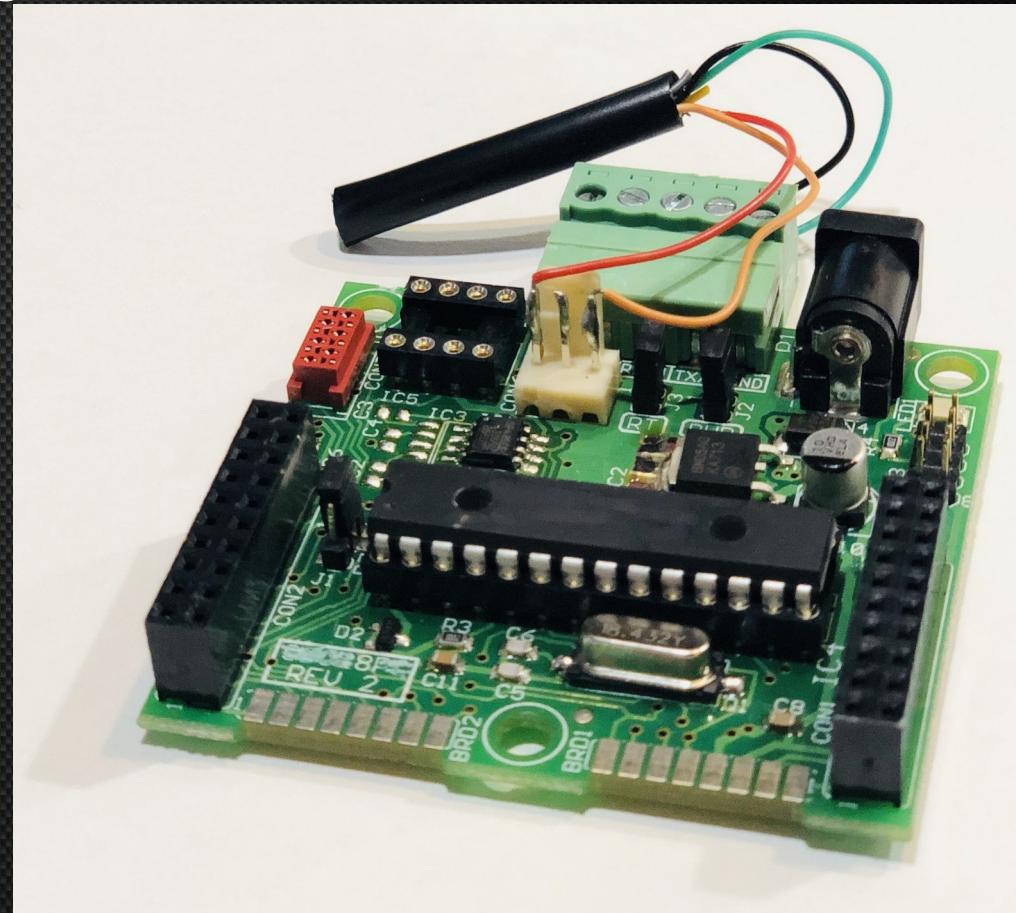
IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (I)

- Integrados
 - Leyendo la referencia
 - ¿Sin referencia o referencia eliminada? (lijados, láser ...)
 - Deduciendo el pinout y buscando el datasheet
 - Si es un microcontrolador o SoC: interfaz de programación
- Pads de testeo, flasheo, uarts ...

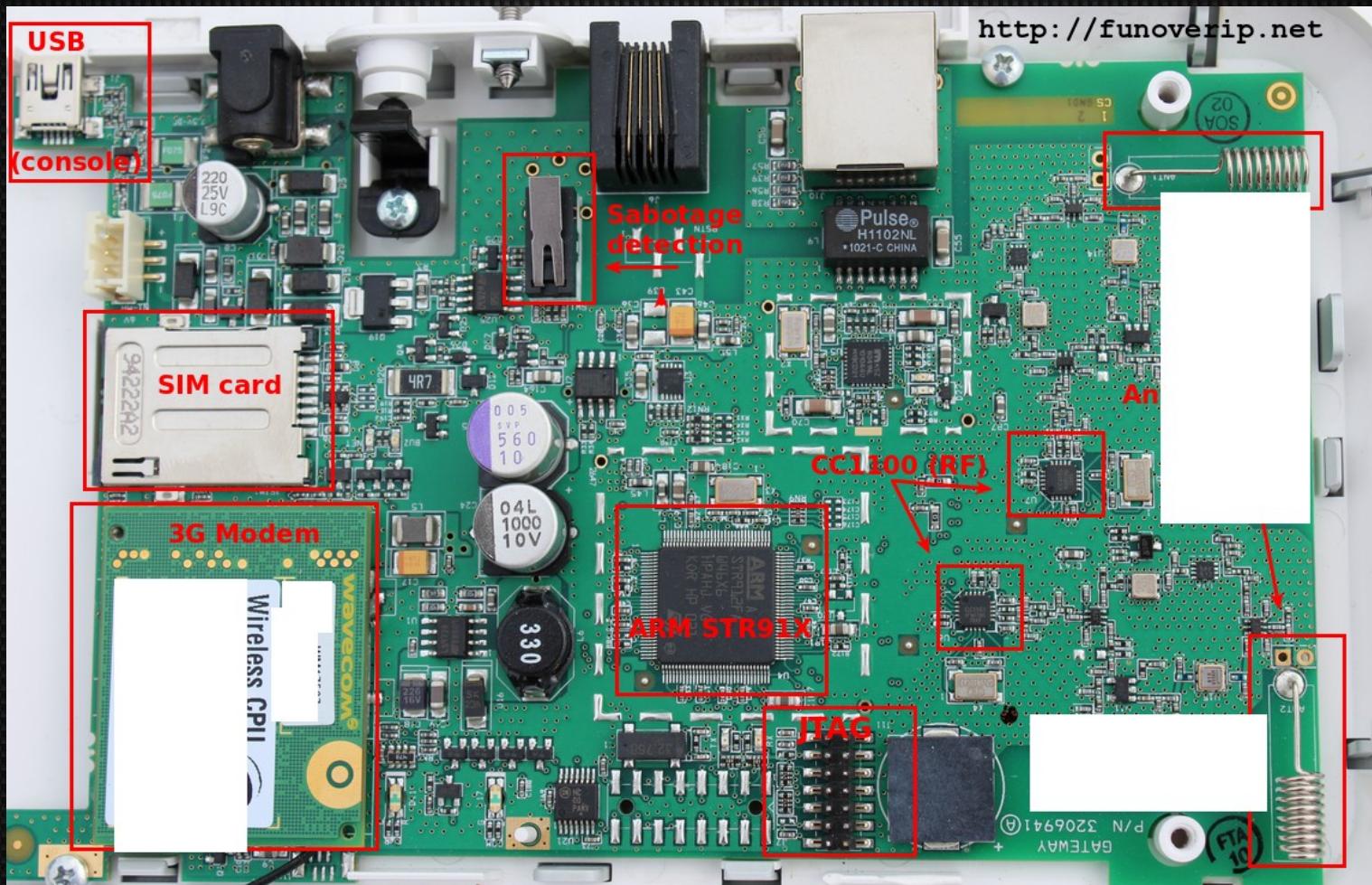


IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (II)

- Componentes interesantes
 - Antenas
 - Circuitos de alimentación / regulación
 - Cristales de cuarzo
 - Conectores
 - ...
- Conexionado entre componentes
 - Polímetro, papel, boli
 - Trabajo metódico

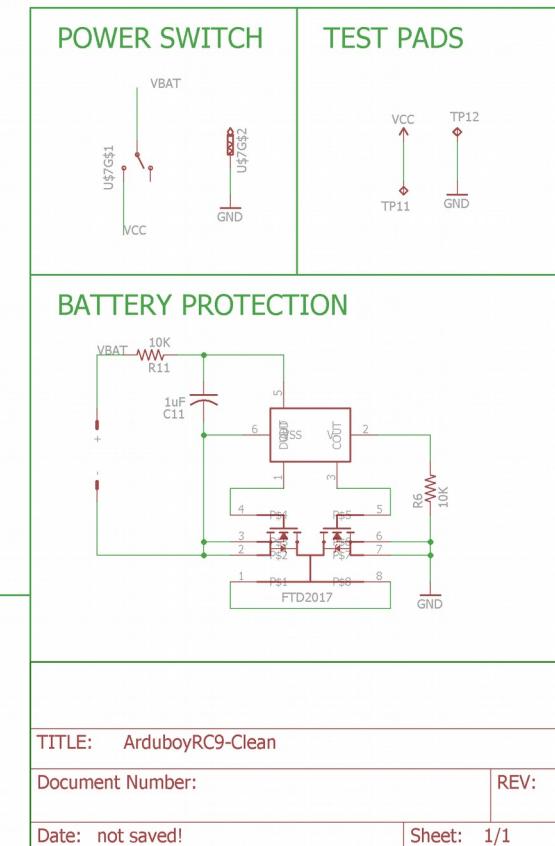
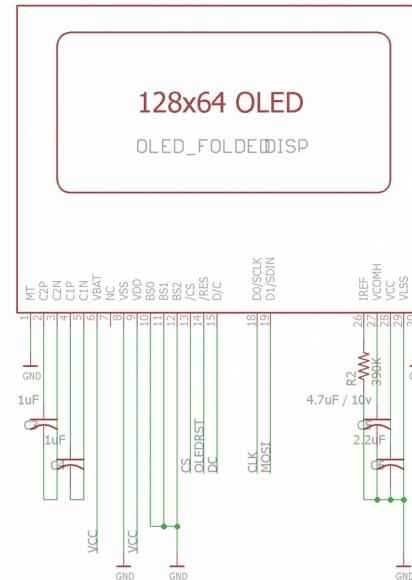
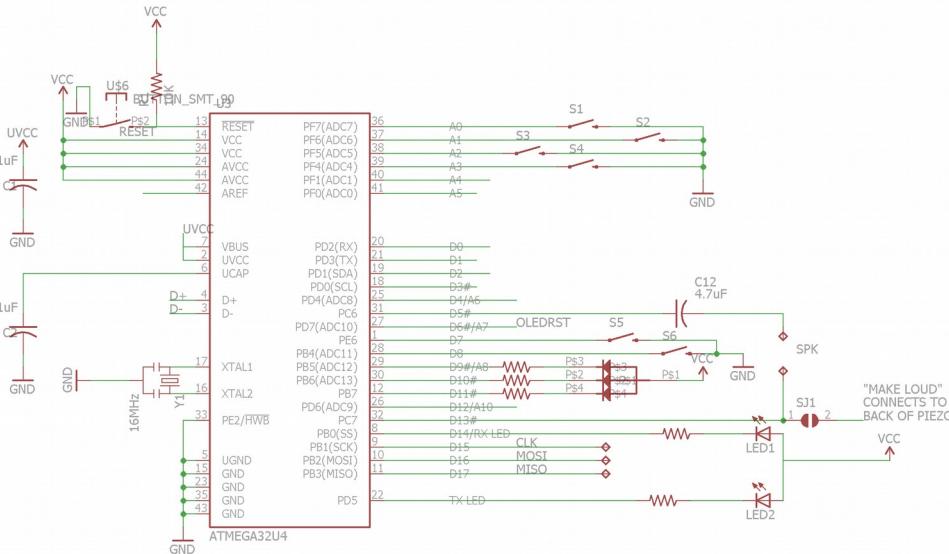


IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (III)

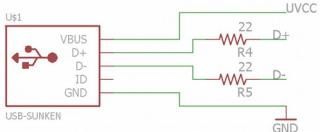


<https://funoverip.net/>

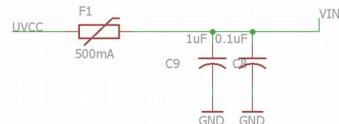
EL HARDWARE: ARDUBOY



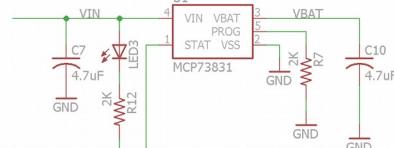
USB INPUT



POWER INPUT

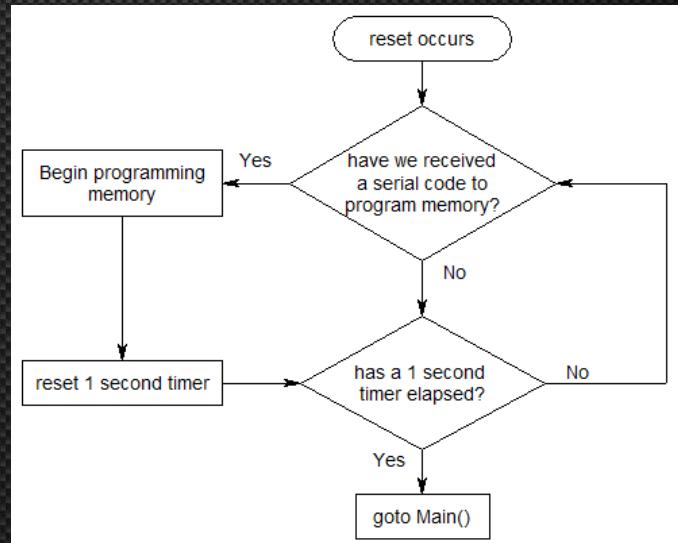
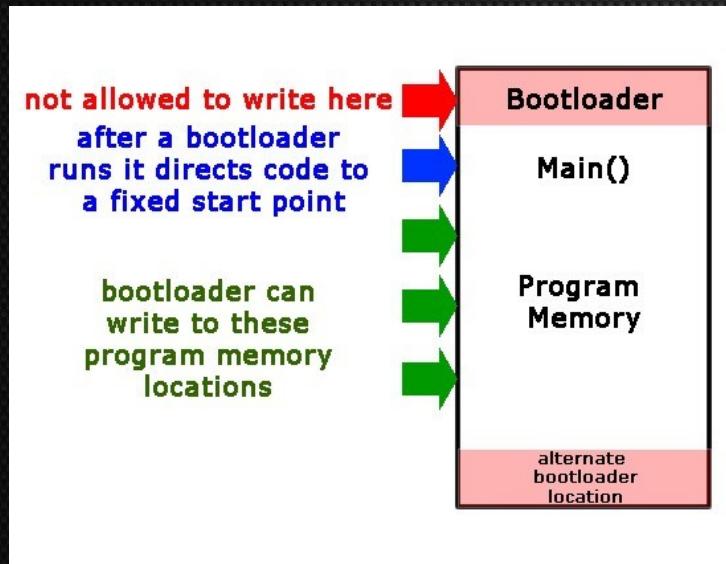


CHARGE CONTROLLER

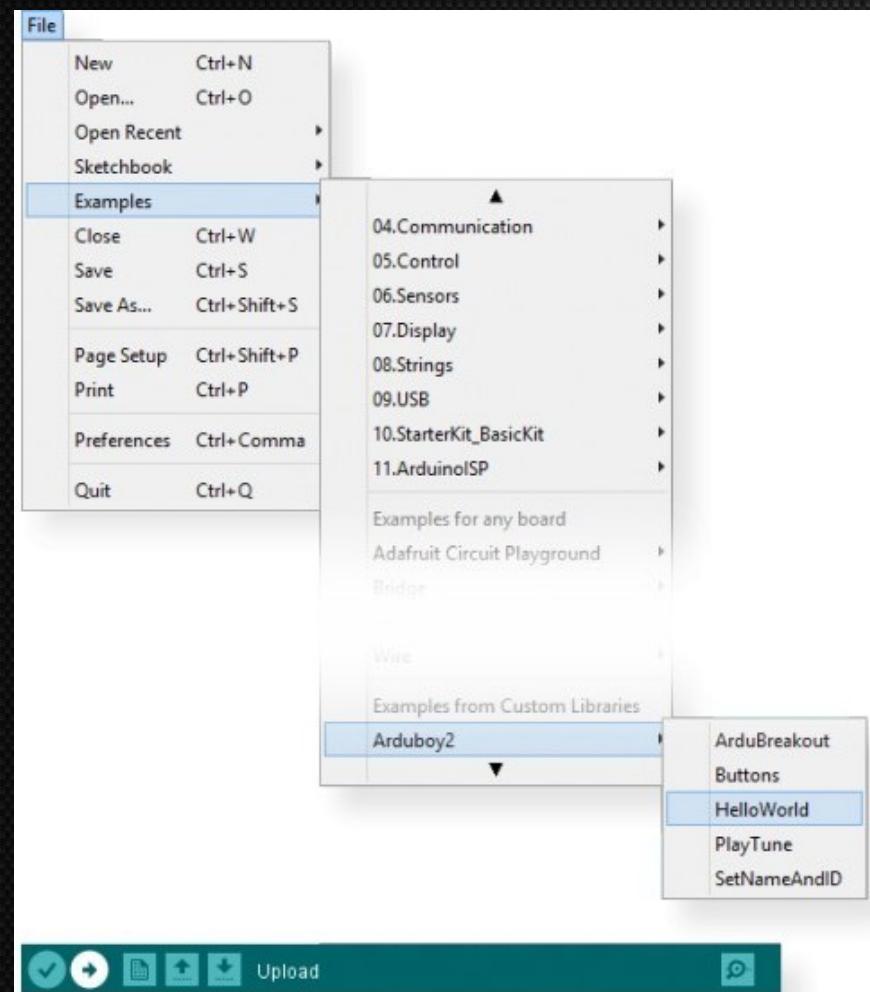


FACILITANDO EL DESARROLLO: EL IDE Y EL BOOTLOADER

- IDE (Arduino)
- Funcionamiento bootloader.
 - ¿Como se graba el bootloader?



HOLA MUNDO



```
#include <Arduboy2.h>

// make an instance of arduboy used for many functions
Arduboy2 arduboy;

// This function runs once in your game,
// use it for anything that needs to be set only once in your game.
void setup() {
    // initiate arduboy instance
    arduboy.begin();

    // here we set the framerate to 15, we do not need to run at
    // default 60 and it saves us battery life
    arduboy.setFrameRate(15);
}

// our main game loop, this runs once every cycle/frame,
// this is where our game logic goes.
void loop() {
    // pause render until it's time for the next frame
    if (!arduboy.nextFrame())
        return;

    // first we clear our screen to black
    arduboy.clear();

    // we set our cursor 5 pixels to the right and 10 down from the top
    // (positions start at 0, 0)
    arduboy.setCursor(4, 9);

    // then we print to screen what is in the Quotation marks ""
    arduboy.print(F("Hello, world!"));

    // then we finally we tell the arduboy to display what we just wrote to the display
    arduboy.display();
}
```

PARTE III

¿Y AHORA QUE HACEMOS?



www.myconfinedspace.com for unwatermarked image

GESTOR DE CONTRASEÑAS POR HARDWARE (BLUETEAM)

- Protección contra lectura:

- Fuse calculator:

<http://eleccelerator.com/fusecalc/fusecalc.php>

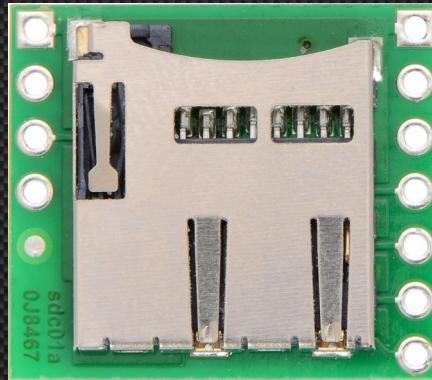
The screenshot shows the AVRDUDE fuse calculator interface. At the top, there are several configuration options and dropdown menus for boot settings. Below these are sections for EXTENDED Fuse Presets and LOCKBIT Fuse Presets, each with dropdown menus for different protection modes. The main area is titled "Manual Fuse Bit Manipulation". It contains a table with four columns: Bit, LOW, HIGH, and LOCKBIT. The Bit column lists bits 7 down to 0. The LOW column shows programmed values (CKDIV8, CKOUT, SUT1, SUTO, CKSEL3, CKSEL2, CKSEL1, CKSEL0) with checkboxes. The HIGH column shows unprogrammed values (OCDEN, JTAGEN, SPIEN*, WDTON, EESAVE, BOOTS1, BOOTS0, BOOTRST) with checkboxes. The LOCKBIT column shows unprogrammed values (Bit 7 to Bit 0) with checkboxes. Below the table, there are input fields for hex values: Default (0x41), Apply (0x41), High fuse (0x99), Low fuse (0x99), Extended fuse (0xFF), and Lock bit (0xFF). At the bottom, command-line arguments are displayed: -U lfuse:w:0x41:m, -U hfuse:w:0x99:m, -U efuse:w:0xFF:m, and -U lock:w:0xFF:m.

BADUSB CON MENÚS (REDTEAM)



MEJORAS FUTURAS

- Librería para menús
- Ampliar hardware Arduboy:
 - Wifi
 - MicroSD
 - ...



AGRADECIMIENTOS Y PREGUNTAS

- Organización de RootedCON 2019
-
- David Marugán  @RadioHaking
- Fernando  @EA4FSV
- Pedro Cabrera  @PCabreraCamara
- Roland Papenfuss  @Santpapen
- Eva Banegas  @bigdata
- ...

GRACIAS **THANK**
ARIGATO **YOU**
SHUKURIA **BOLZİN** **MERCI**
JUSPAXAR

DANKSCHEEN
SPASSIBO
TAVTAPUCH
MEDAWAGSE
BAINKA
YAQHANEYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
MERİ
SPASIBO
DENKAUJA
HENACHALHYA
UNHALCHEESH
NATUR
GÜ
EKOJU
SIKOMO
MARETAI
NINGMONCHAR
MINMONCHAR
TINGKI
BİYAN
SHUKRIA

CHALTU
NUHUN
SNACHALHYA
DHANYABAAD
WABEEJA MAITEKA
HUI
YUSPAGARIATAM
MAAKE
SANCO
MERASTAWHY
GAEJTHO
LAH
KOMAPSUMNIDA
PAKDIES
MEHRBANI

GOZAIMASHITA
EFCHARISTO
AGUYJE
FAKAUE

 @JoelSerna

 @ernesto_xload