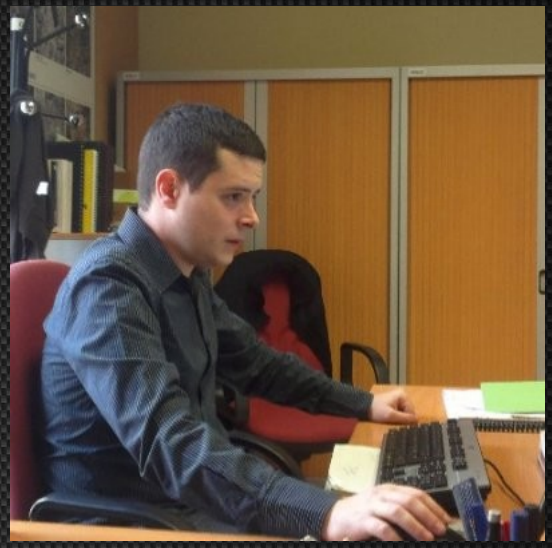
HARDWARE HACKING
Y
USO EN BLUE TEAM Y RED TEAM

DISCLAIMER

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

ACERCA DE NOSOTROS



Joel Serna Moreno @JoelSerna

Ernesto Sánchez Pano @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

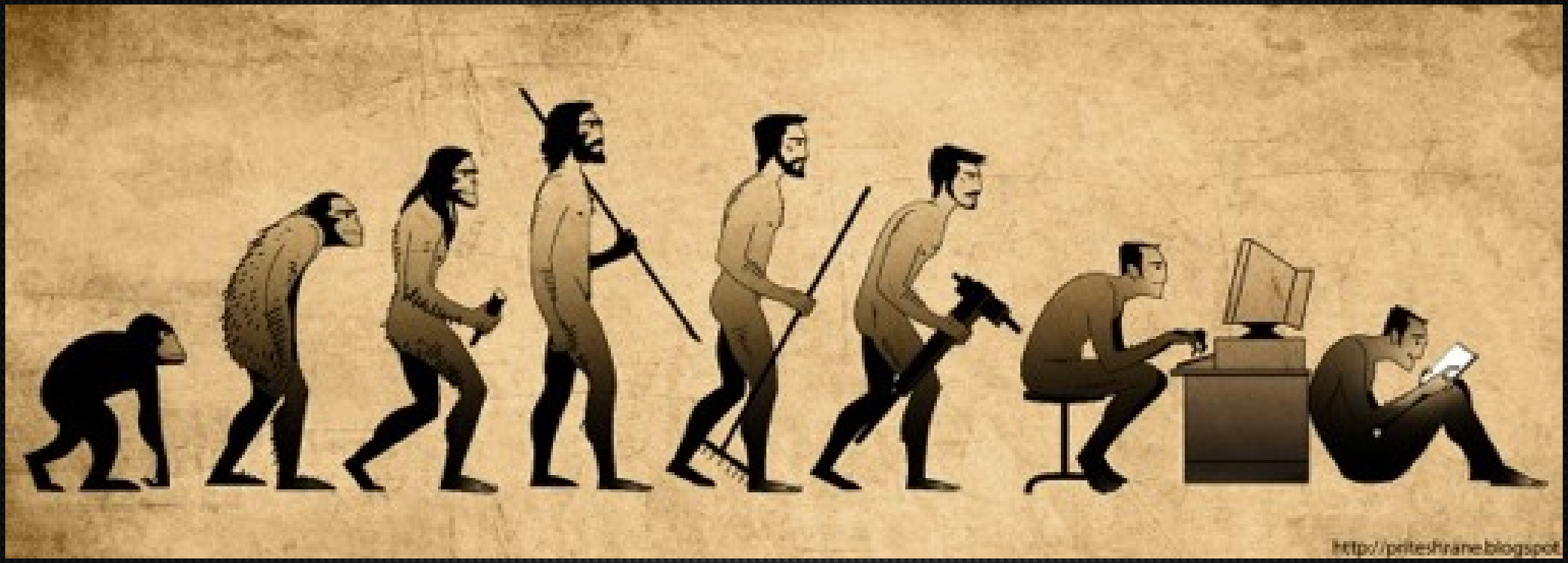
- Identificando el hardware y el conexionado
- Haciéndonos la vida más fácil: el bootloader y el IDE
- Hola mundo y primeras pruebas

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

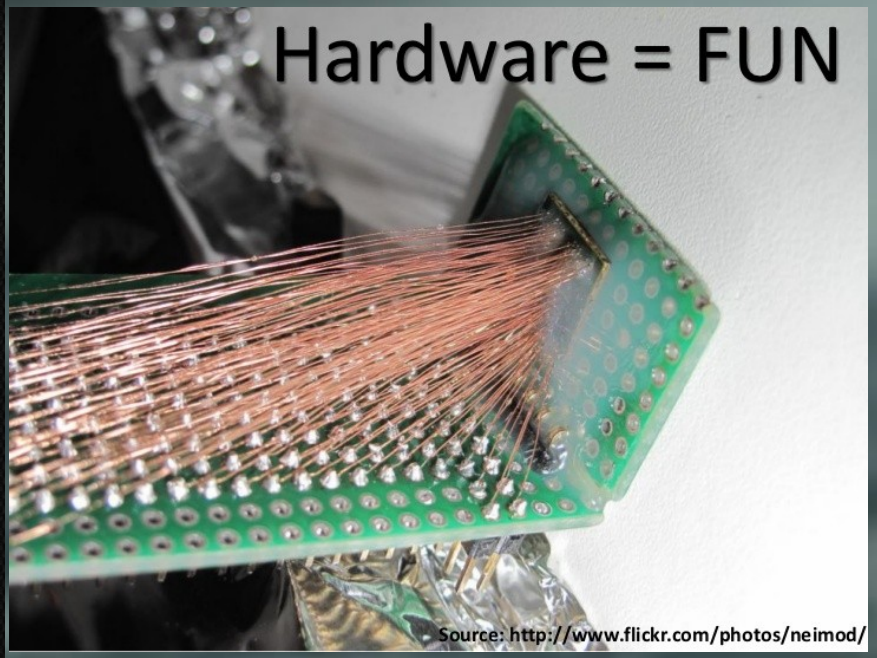
Despedida, contacto y preguntas

PARTE I
¿DE DÓNDE VENIMOS Y A DONDE VAMOS?



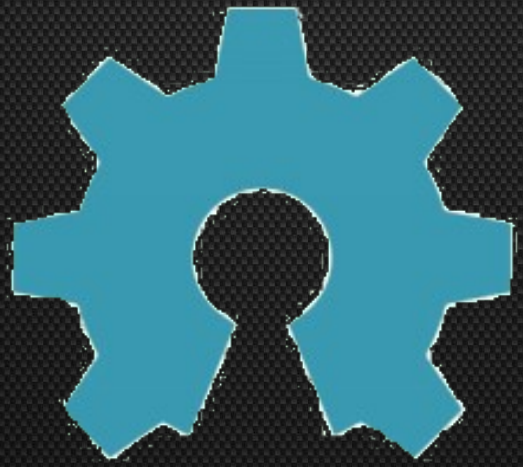
ARDUBOY

¿DE DÓNDE VIENE ESTE PROYECTO?



PORQUÉ HACKEAR UNA CONSOLA LIBRE

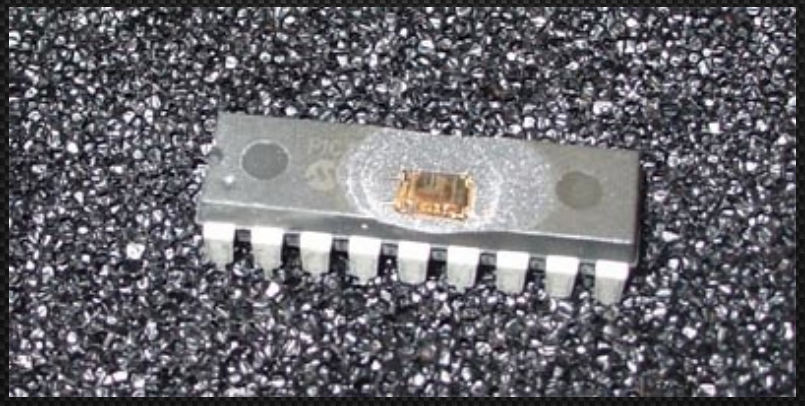
- Como entrenamiento y entreteniemiento.
- Es una forma fácil y sencilla de comprobar nuestros resultados.
- Tiene una amplia documentación y comunidad, tanto de Arduboy como de Arduino



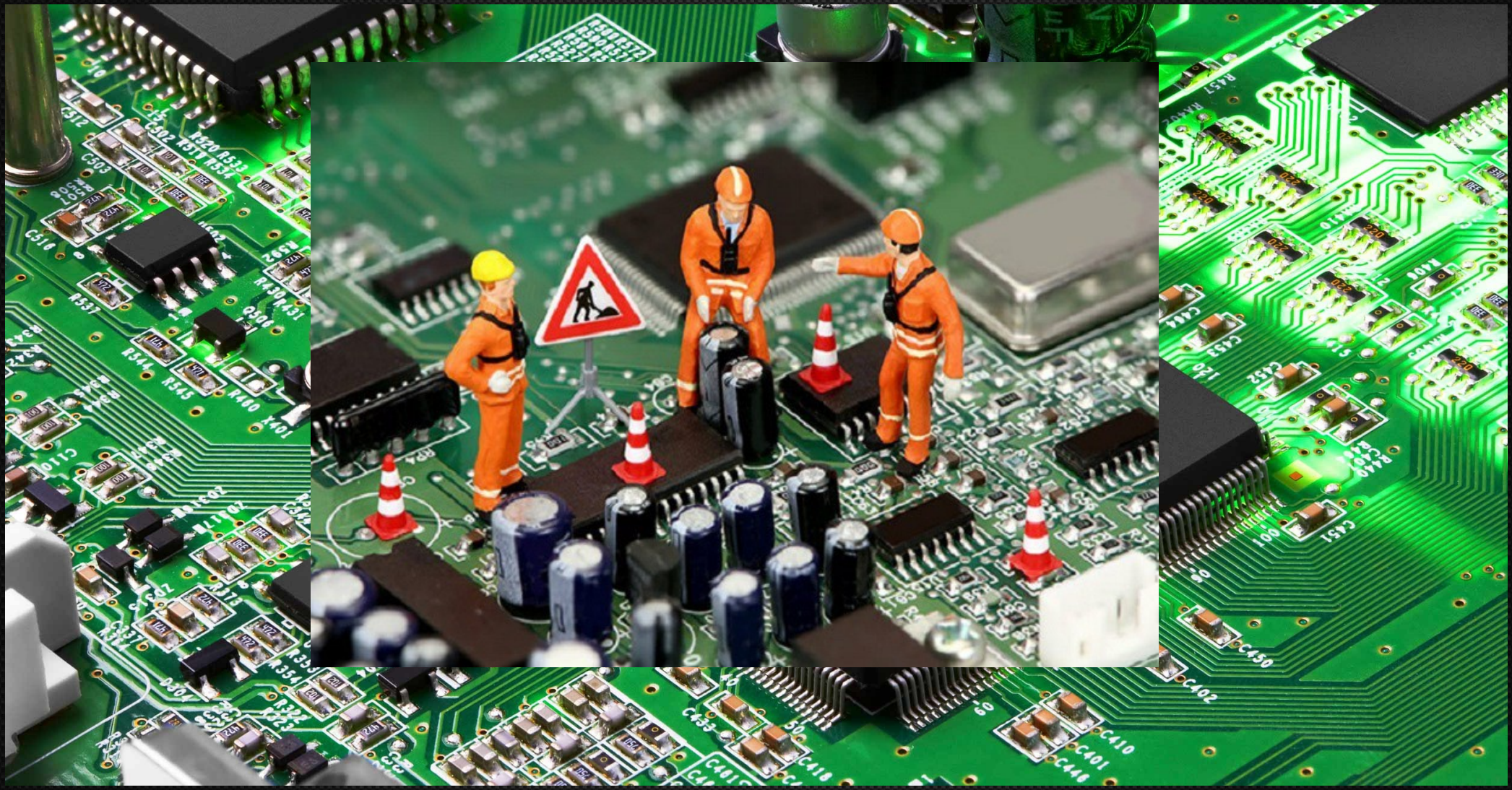
SOBRE HARDWARE HACKING

- Destinamos una videoconsola a otro uso (ciberseguridad)
- Esta es una charla de introducción y motivación

- No se van a tratar sistemas avanzados y complejos.

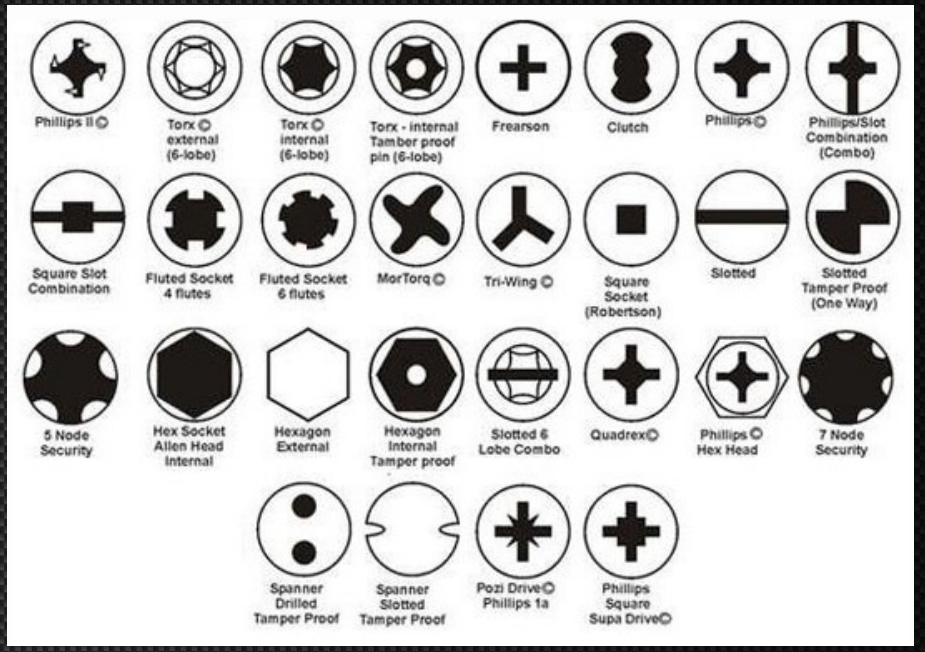


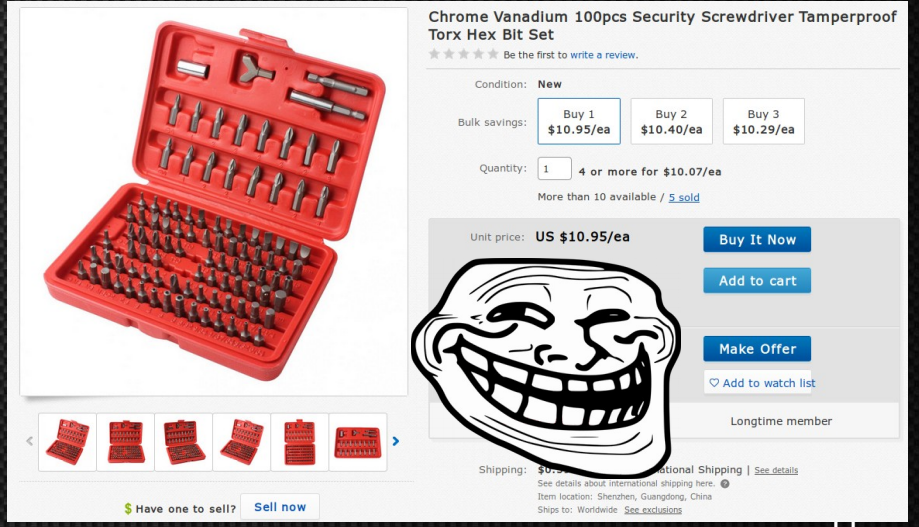
PARTE II
CON LAS MANOS EN LA MASA



ACCEDIENDO AL CIRCUITO (I)

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

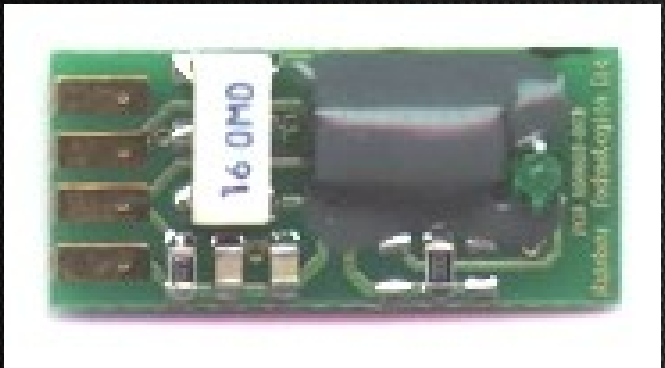


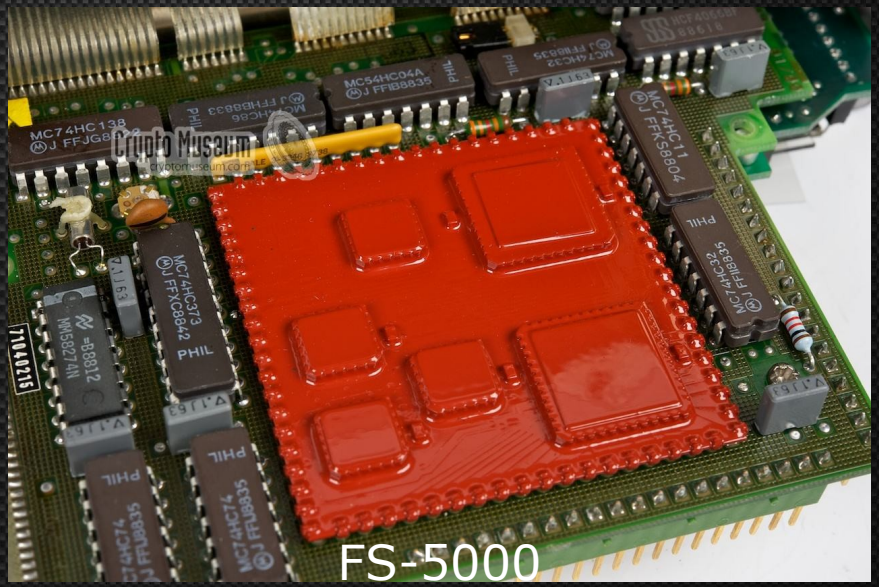


/Rooted©

ACCEDIENDO AL CIRCUITO (II)

- Protecciones:
  - Resinas epoxy / siliconas



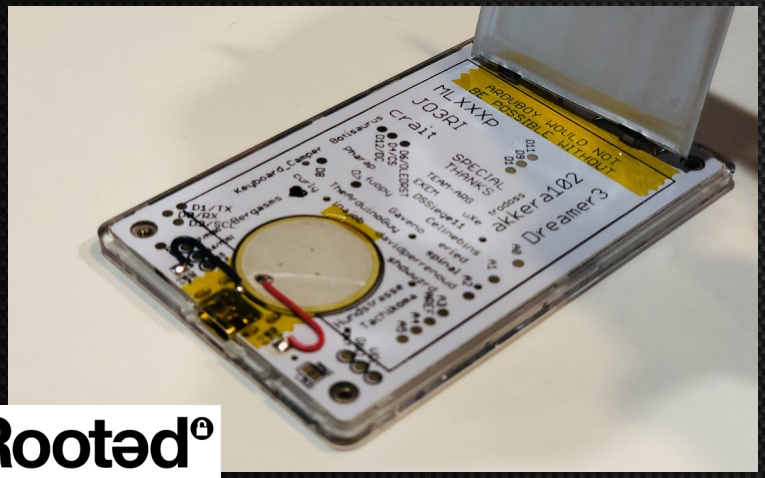


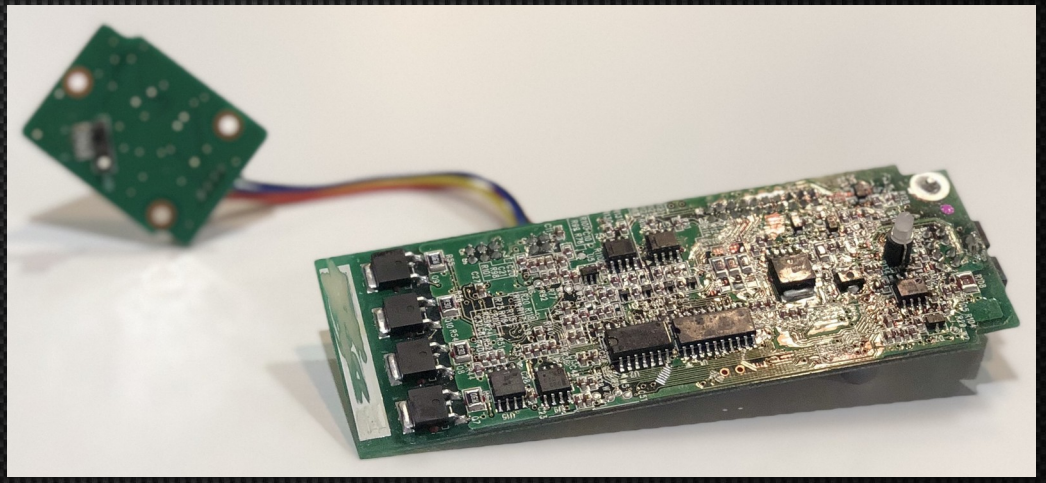
FS-5000

/Rooted

IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (I)

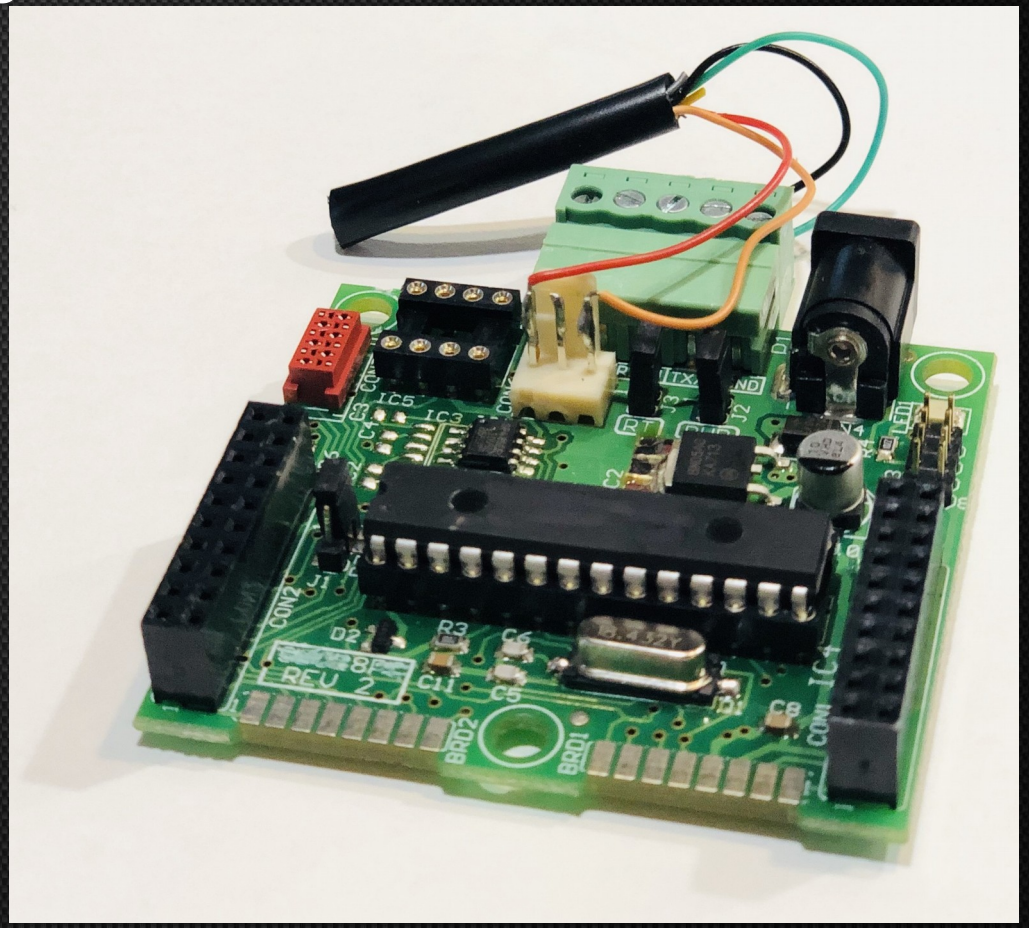
- Integrados
  - Leyendo la referencia
    - ¿Sin referencia o referencia eliminada? (lijados, láser …)
  - Deduciendo el pinout y buscando el datasheet
  - Si es un microcontrolador o SoC: interfaz de programación
- Pads de testeo, flasheo, uarts ...



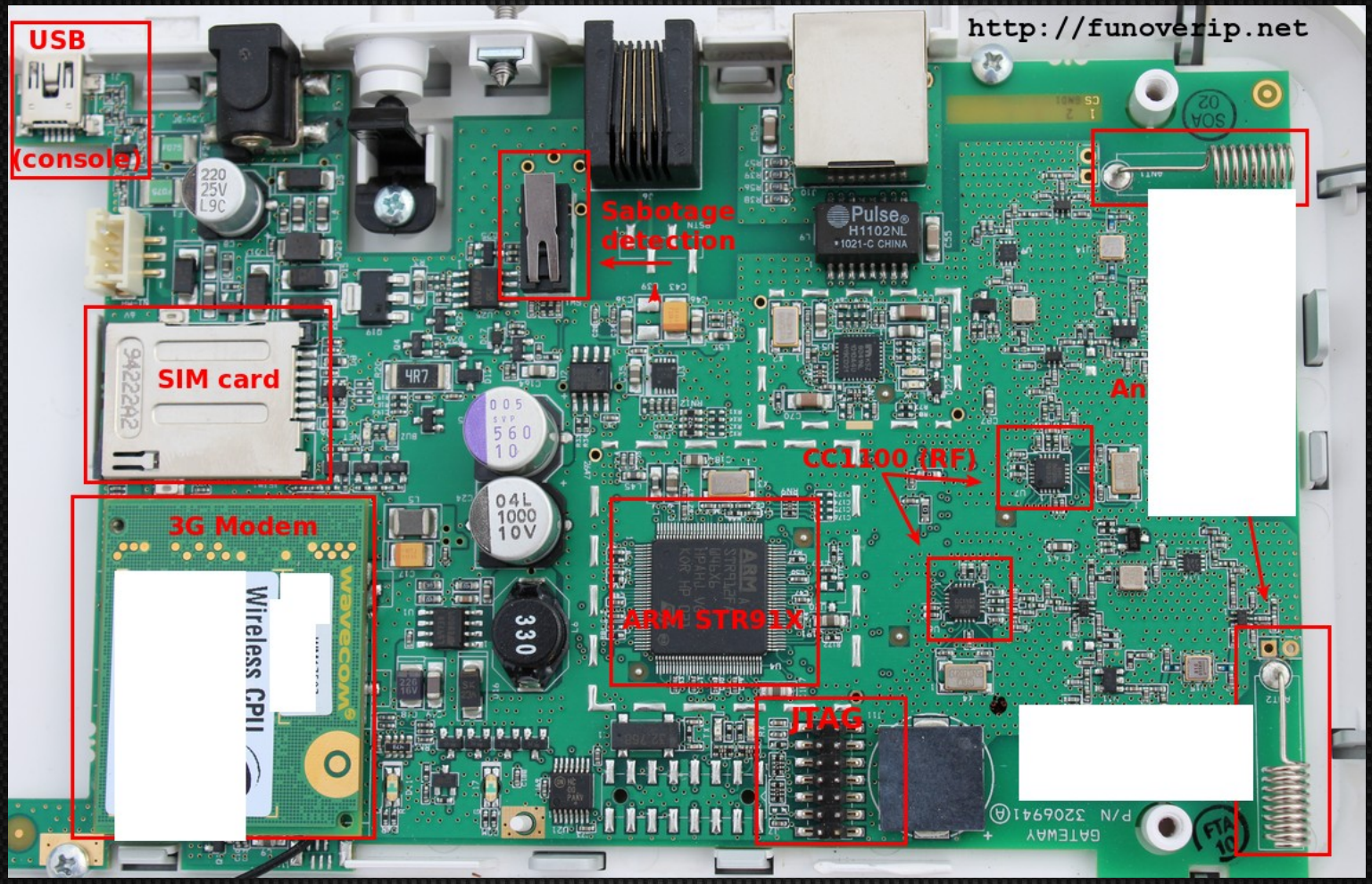


IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (II)

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



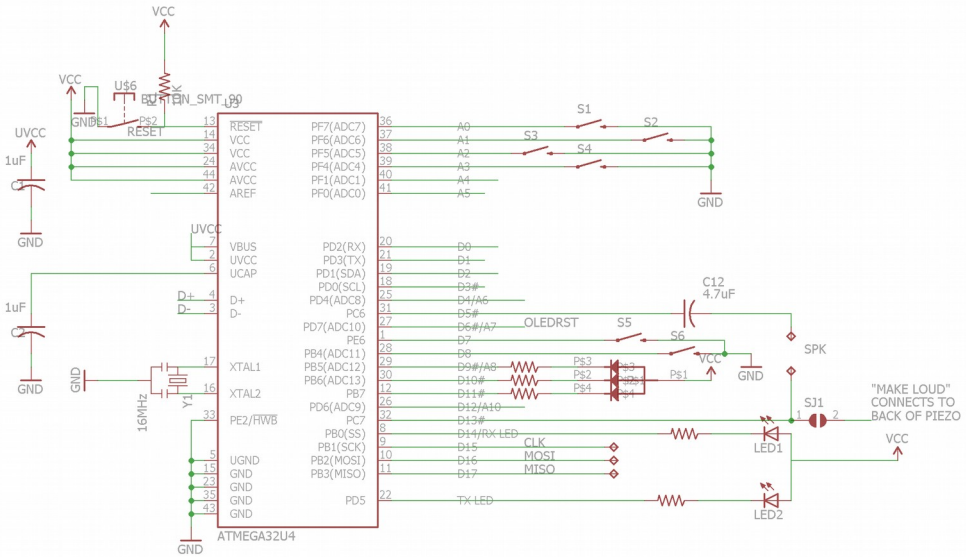
IDENTIFICANDO EL HARDWARE Y EL CONEXIONADO (III)

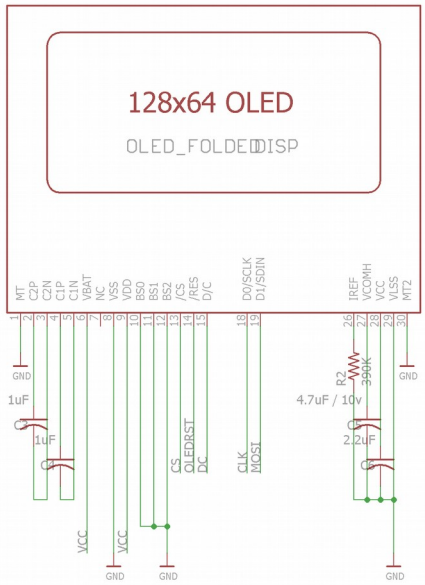


https://funoverip.net/

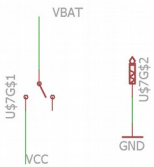
/Rooted

EL HARDWARE: ARDUBOY

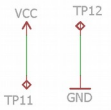




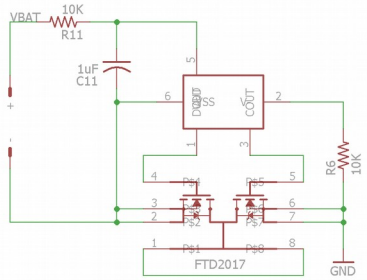
POWER SWITCH



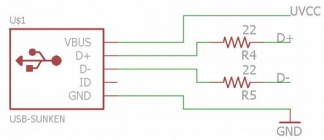
TEST PADS



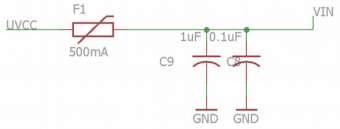
BATTERY PROTECTION



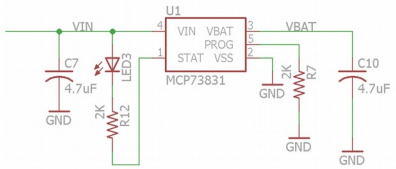
USB INPUT



POWER INPUT



CHARGE CONTROLLER

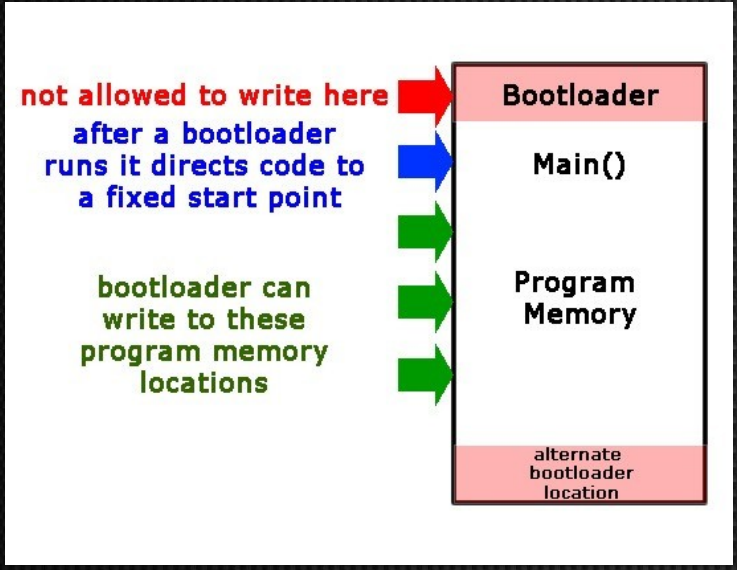


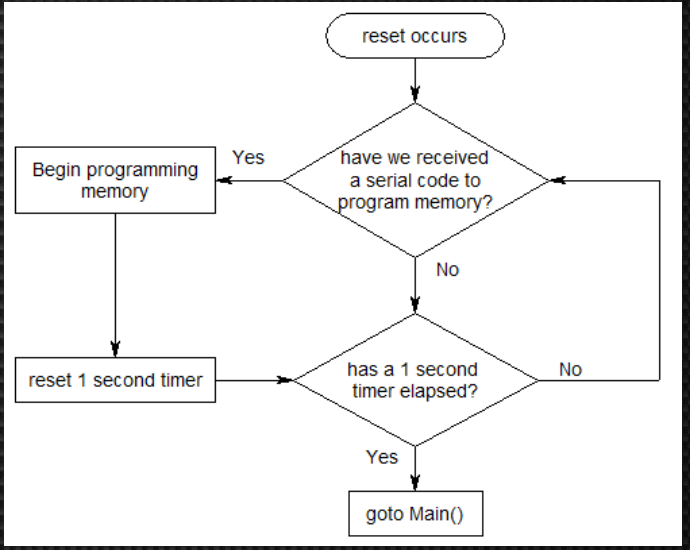
TITLE:	ArduboyRC9-Clean
Document Number:	REV:
Date: not saved!	Sheet: 1/1

/Rooted

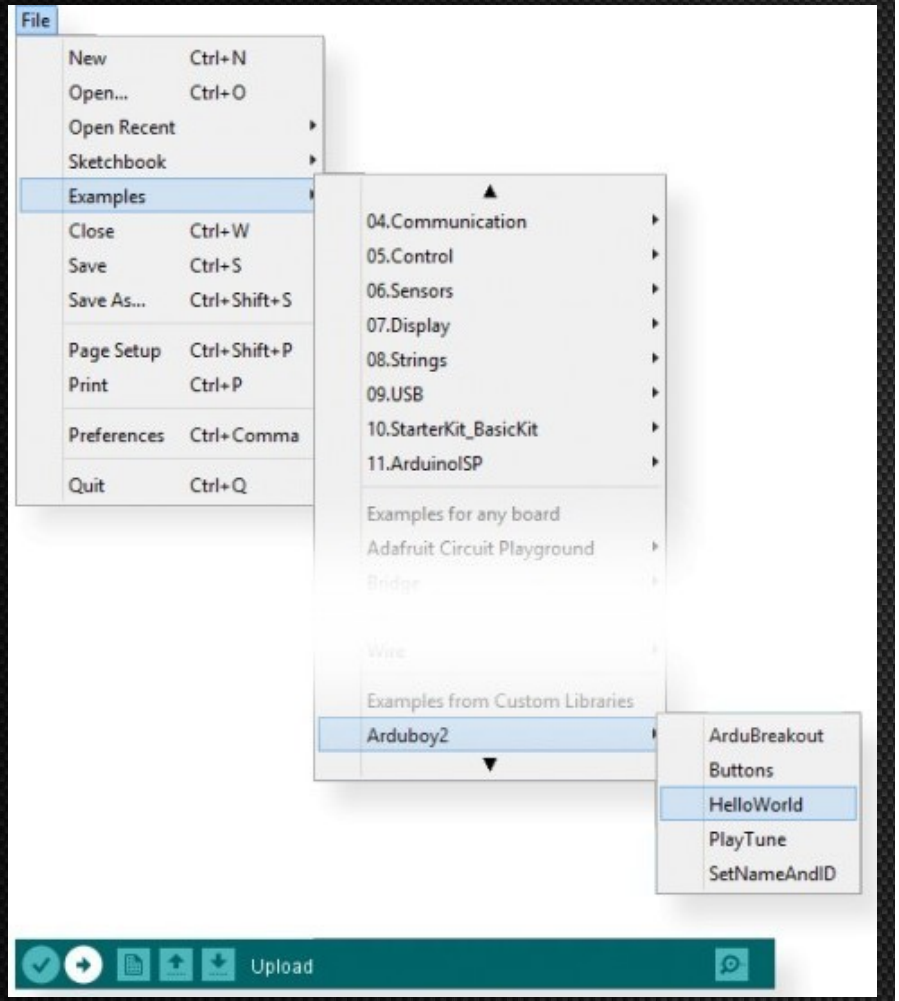
FACILITANDO EL DESARROLLO: EL IDE Y EL BOOTLOADER

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





HOLA MUNDO




```ino
#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 finaly we tell the arduboy to display what we just wrote to the display
  arduboy.display();
}
```

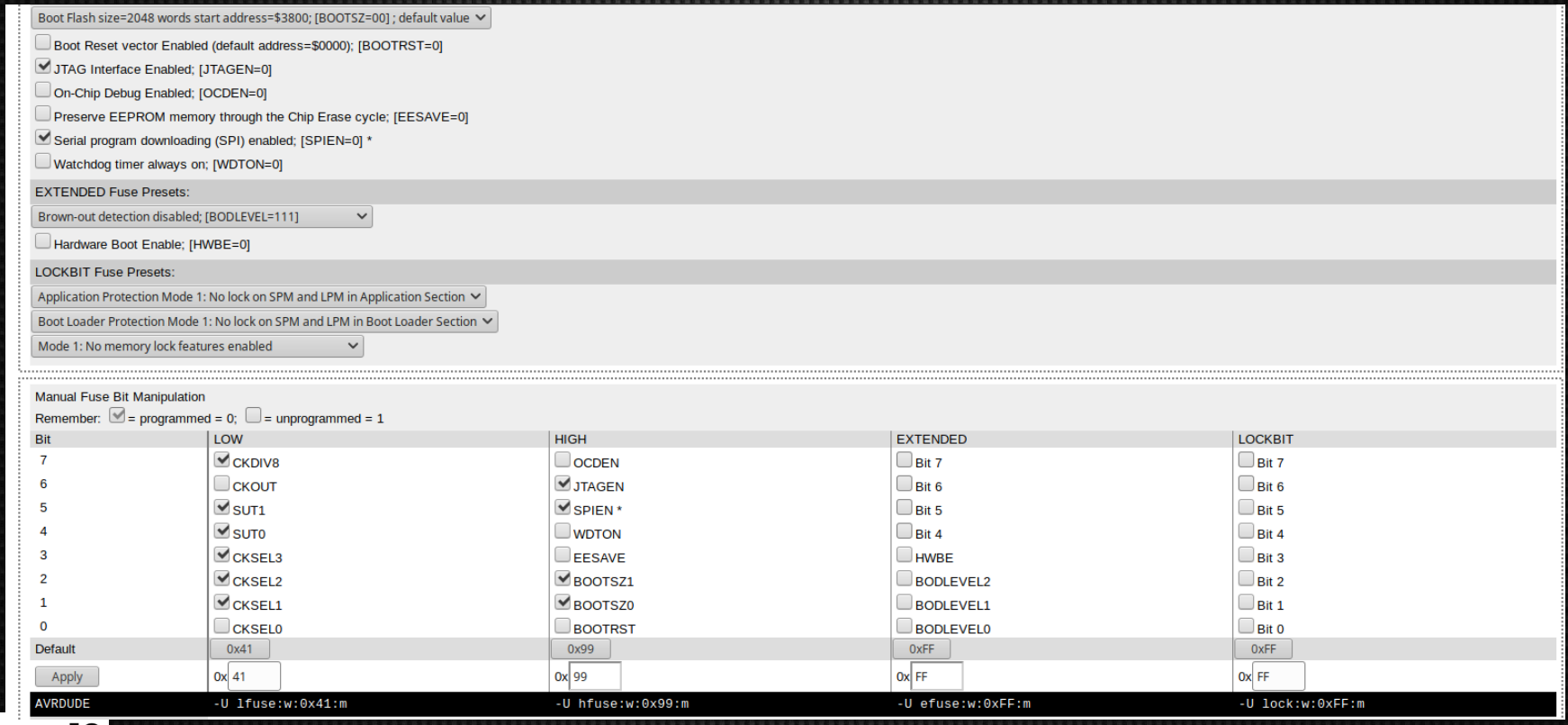

/Rooted

PARTE III
¿Y AHORA QUE HACEMOS?

GESTOR DE CONTRASEÑAS POR HARDWARE (BLUETEAM)

- Protección contra lectura:
  - Fuse calculator:

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

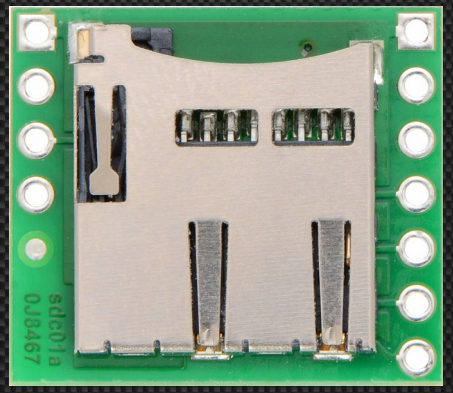


/Rooted

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
- ...

@JoelSerna

@ernesto_xload

/Rooted©