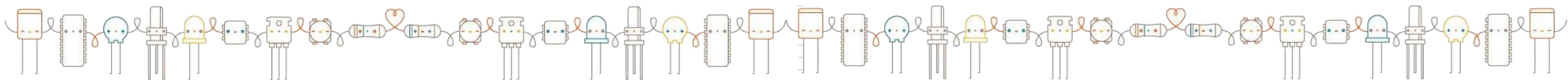


ABRIL
1

Seguridad Informática con Arduino

Utilizando la plataforma Arduino como herramienta para Hacking

Humberto Keymur Landeros

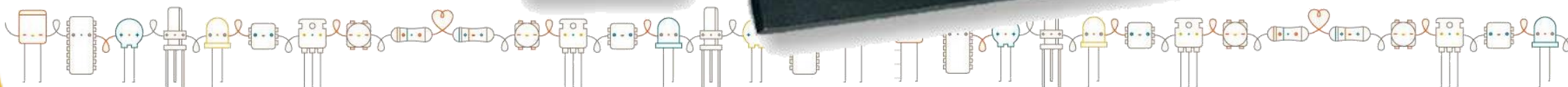
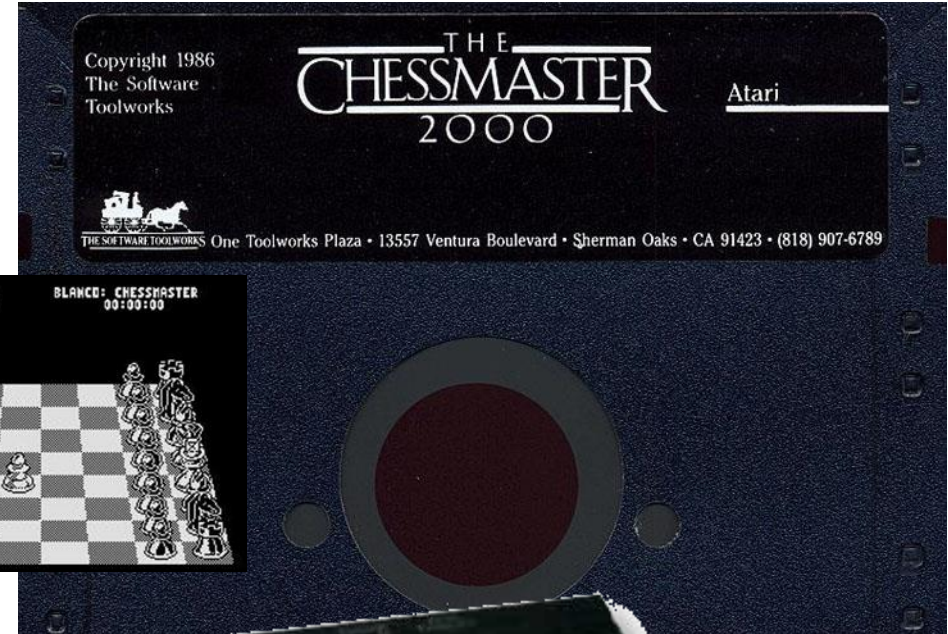
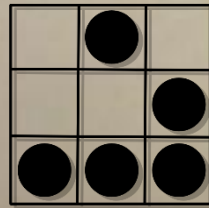
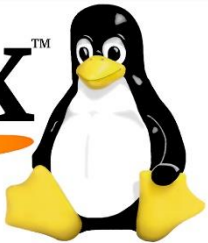


I0



redhat.
CERTIFIED
SYSTEM
ADMINISTRATOR

Linux™



Historia

PIC16F877A

Not Recommended for new designs

Please consider this device **PIC16F18877**

[View Side By Side Comparison](#)

This powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) CMOS FLASH-based 8-bit microcontroller packs Microchip's powerful PIC® architecture into an 40- or 44-pin package and is upwards compatible with the PIC16C5X, PIC12CXXX and PIC16C7X devices. The PIC16F877A features 256 bytes of EEPROM data memory, self programming, an ICD, 2 Comparators, 8 channels of 10-bit Analog-to-Digital (A/D) converter, 2 capture/compare/PWM functions, the synchronous serial port can be configured as either 3-wire Serial Peripheral Interface (SPI™) or the 2-wire Inter-Integrated Circuit (I²C™) bus and a Universal Asynchronous Receiver Transmitter (USART). All of these features make it ideal for more advanced level A/D applications in automotive, industrial, appliances and consumer applications.

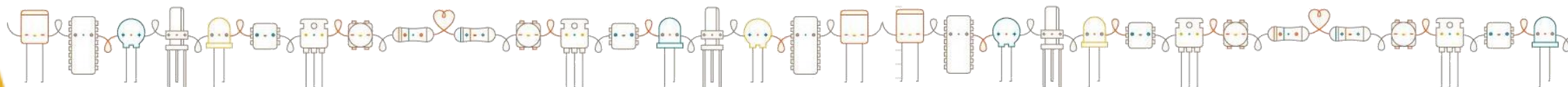


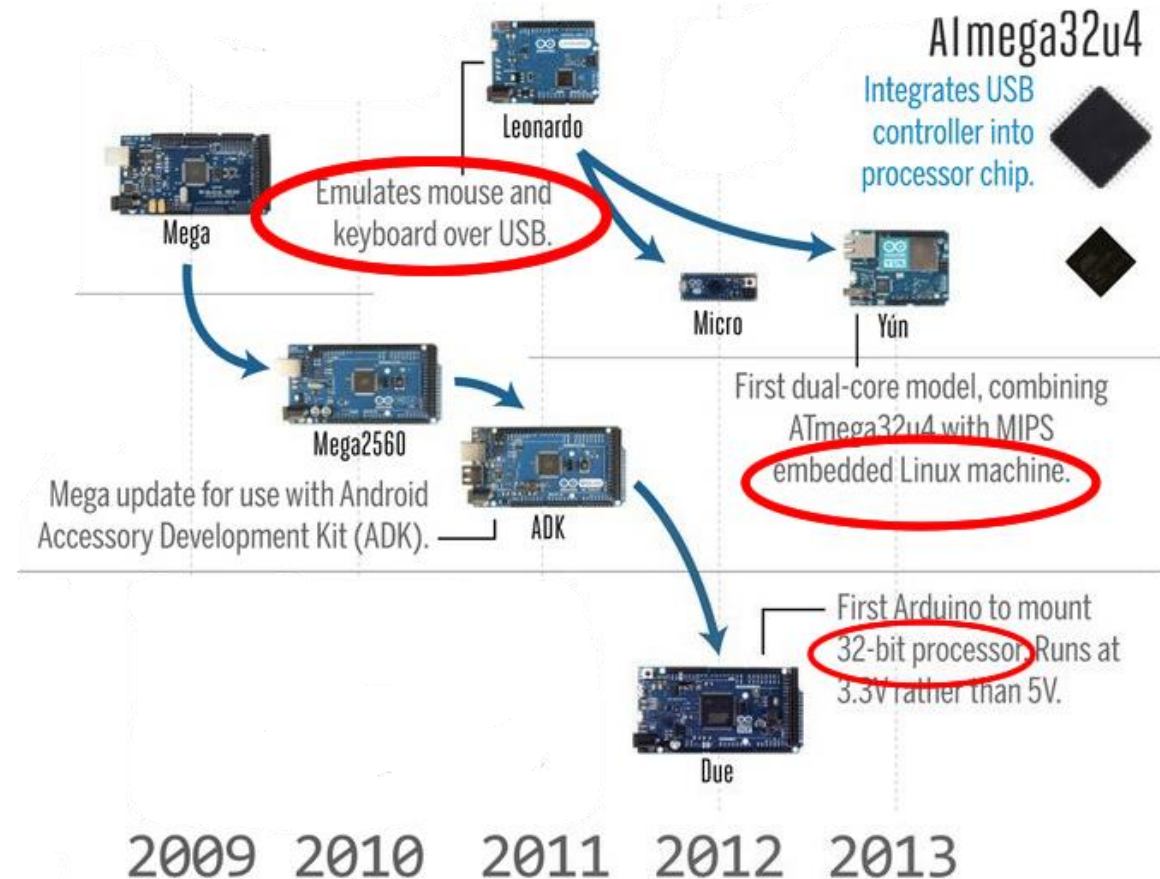
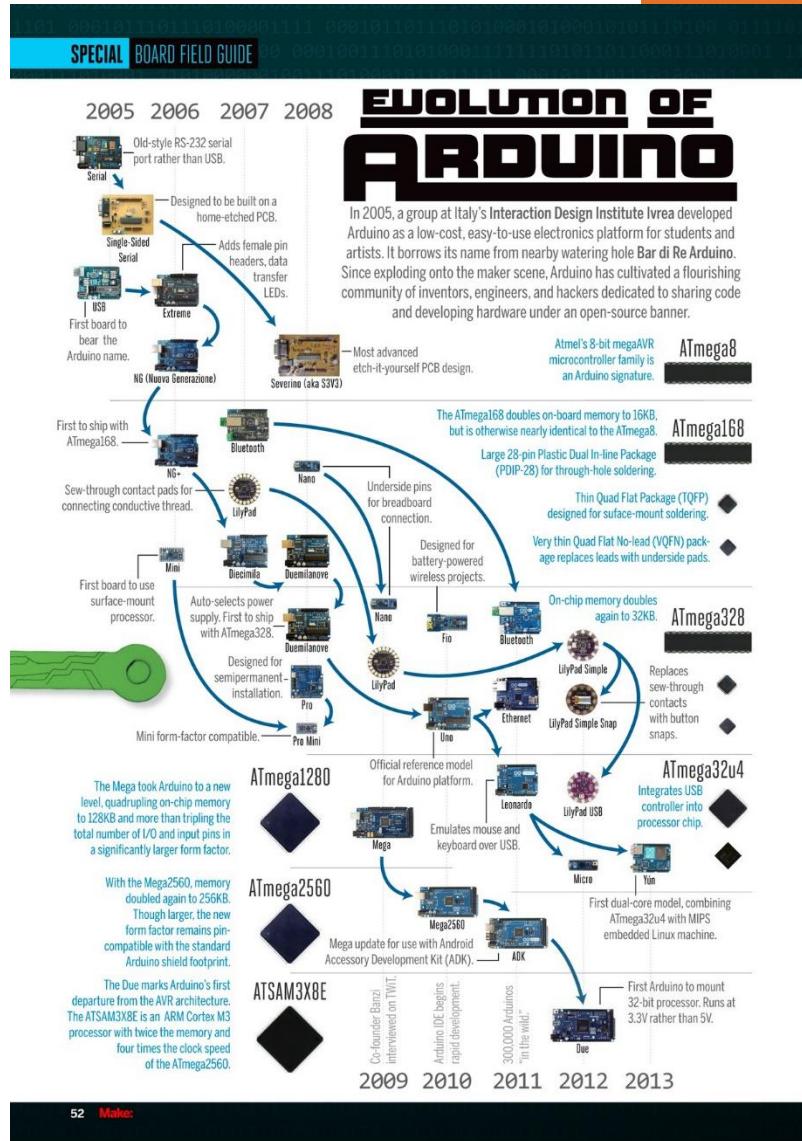
```
C:\Users\k3y1and\AppData\Local\Temp\blink_led.asm - Sublime Text 2 (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

blink_led.asm
1 ;blink_led.asm
2
3 list P = 16F877A
4 include P16F877A.inc
5
6
7 STATUS EQU 0x03
8 PORTB EQU 0x06
9 TRISB EQU 0x86
10 PORTD EQU 0x08
11 TRISD EQU 0x88
12
13 CBLOCK 0x20
14     Kount120us ;Delay count (number of instr cycles
15     for Delay)
16     Kount100us
17     Kount1ms
18     Kount10ms
19     Kount1s
20     Kount10s
21     Kount1m
22 ENDC
23
24 org 0x0000 ;line 1
25     goto START ;line 2 ($0000)
26 org 0x05
27 START
28     banksel TRISD
29
30     movlw 0x00
31     movwf TRISD
32     movwf TRISB
33     banksel PORTB
34     clrf PORTB
35     clrf PORTD
36     call Delay100ms

Line 1, Column 1 Tab Size: 4 Plain Text
```

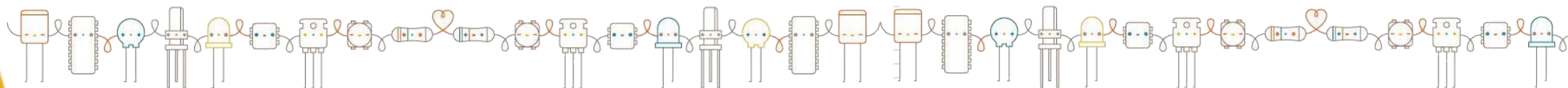
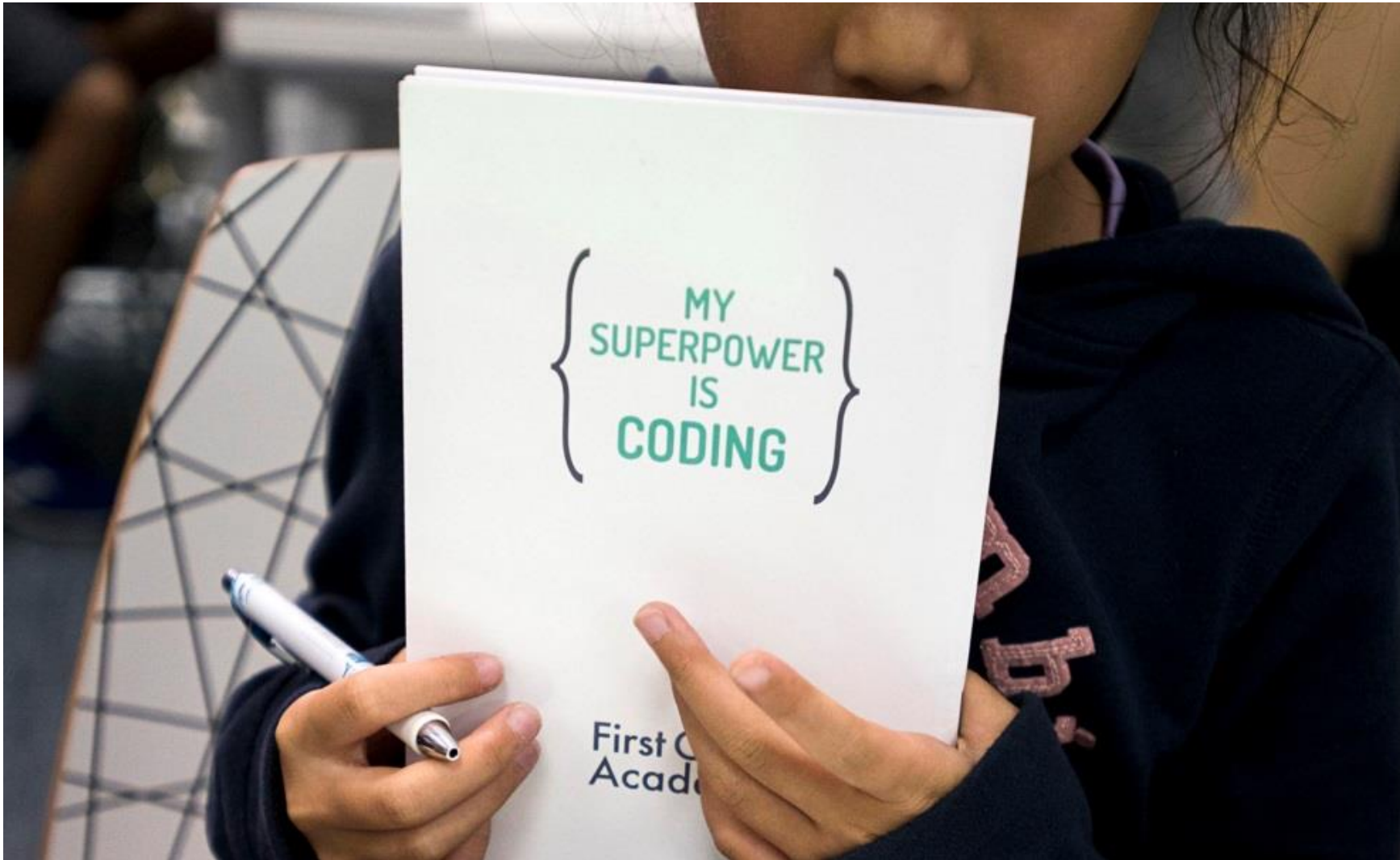
<http://www.ingenieria.unam.mx/crofi/wp-content/uploads/Descargas/Documentos/Cursos/introduccionamicrocontroladorespicconc.pdf>





Seguridad Informática con Arduino

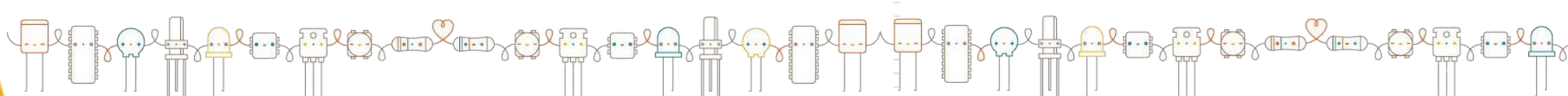
Utilizando la plataforma Arduino como herramienta para Hacking





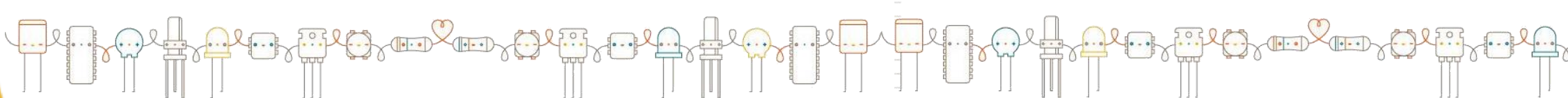
Seguridad Informática

El proceso de métodos y reglas preventivas, correctivas y de detección que se deben seguir para salvaguardar los sistemas y redes informáticas



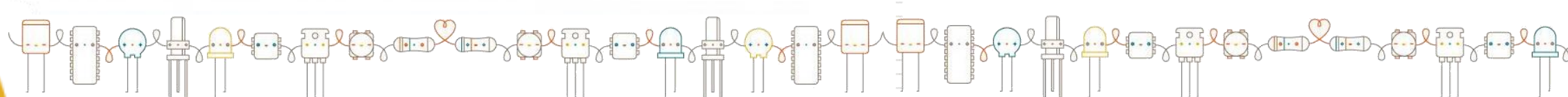
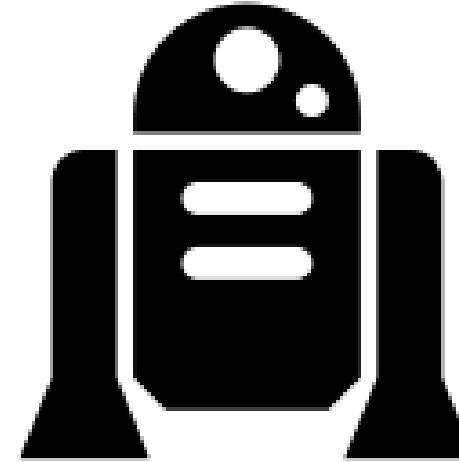
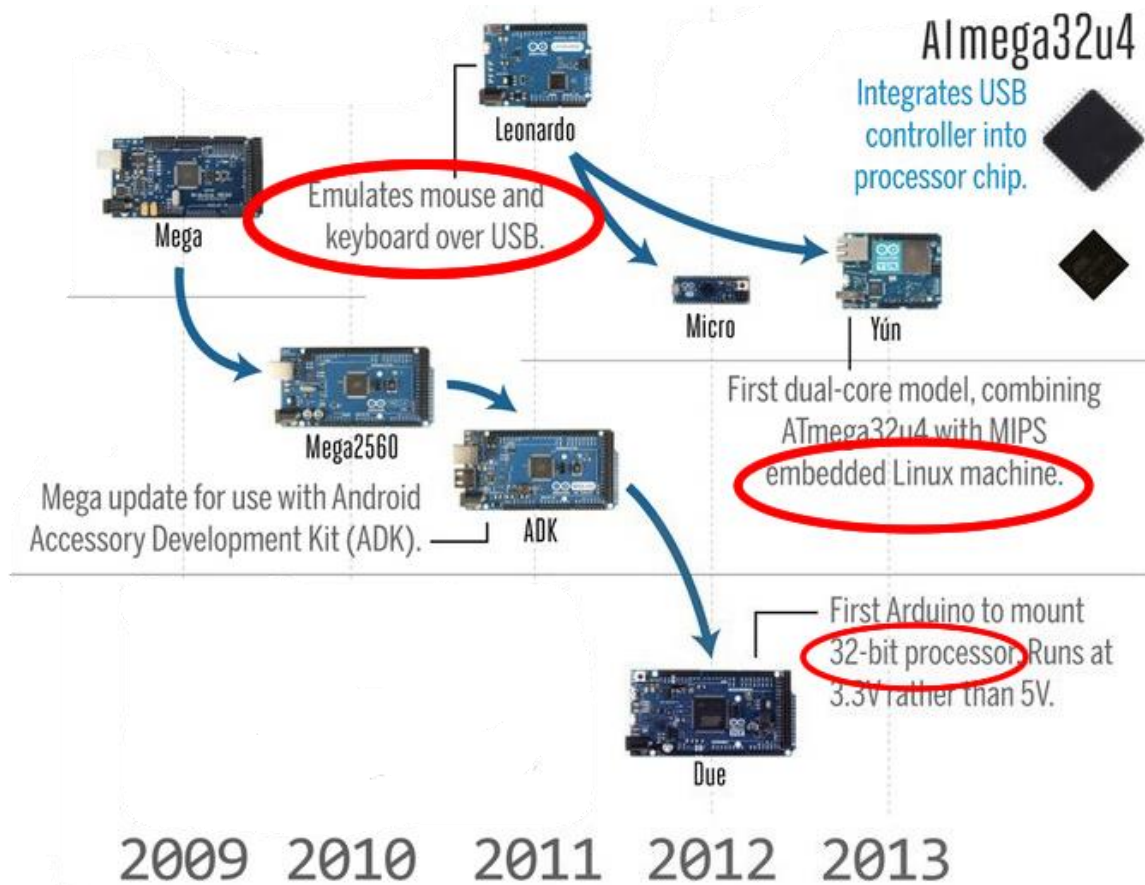


Seguridad Informática





Seguridad Informática





MIRAI BOTNET



En octubre del año pasado, miles de dispositivos infectados realizaron un ataque de denegación de servicio contra los servidores de Dyn, una importante empresa de DNS

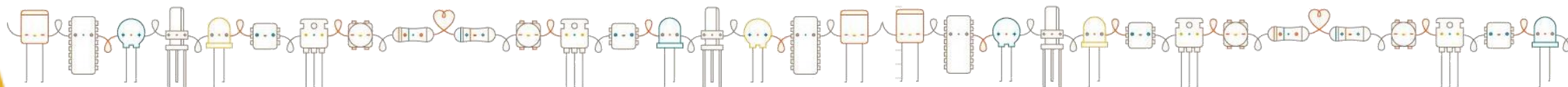
amazon



<http://es.gizmodo.com/el-ataque-de-la-botnet-mirai-le-costo-muy-caro-a-dyn-m-1792035440>

<https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>

| Country | % of Mirai botnet IPs |
|---------------|-----------------------|
| Vietnam | 12.8% |
| Brazil | 11.8% |
| United States | 10.9% |
| China | 8.8% |
| Mexico | 8.4% |





ARDUWORM

Gusano que afecta al Arduino Yun

Se aprovecha de numerosas vulnerabilidades ya que cuenta con un sistema Linux embebido.

<http://www.seg.inf.uc3m.es/~guillermo-suarez-tangil/papers/2016mal-iot.pdf>

<http://hackaday.com/2016/11/11/arduworm-a-malware-for-your-arduino-yun/>

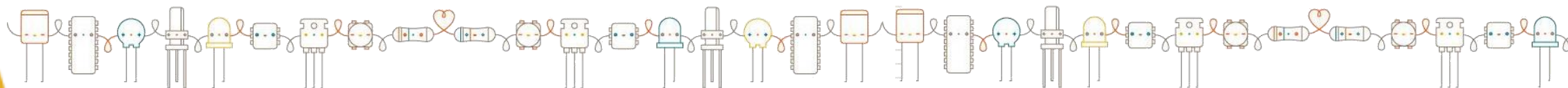
ARDUWORM: A MALWARE FOR YOUR ARDUINO YUN

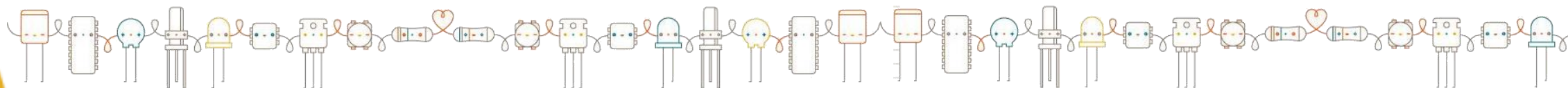
by: Elliot Williams

24 Comments

f t g+

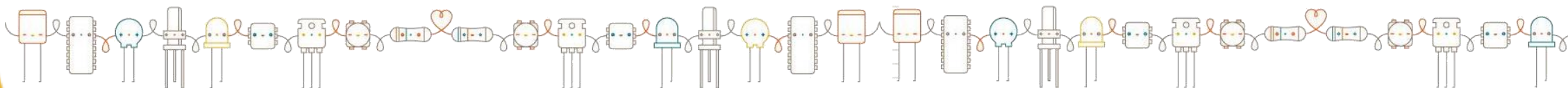
November 11, 2016





Seguridad Informática con Arduino

Utilizando la plataforma Arduino como herramienta para Hacking

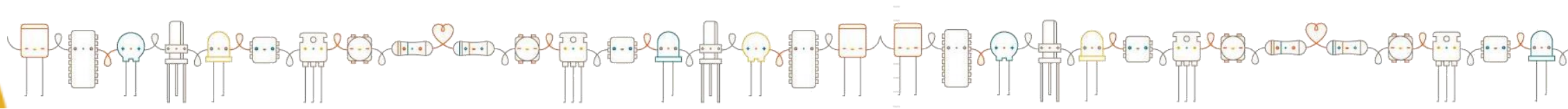




Las herramientas y técnicas mostradas a continuación pueden ser peligrosas u ocasionar daños a terceros y solo son mostradas con fines educativos.

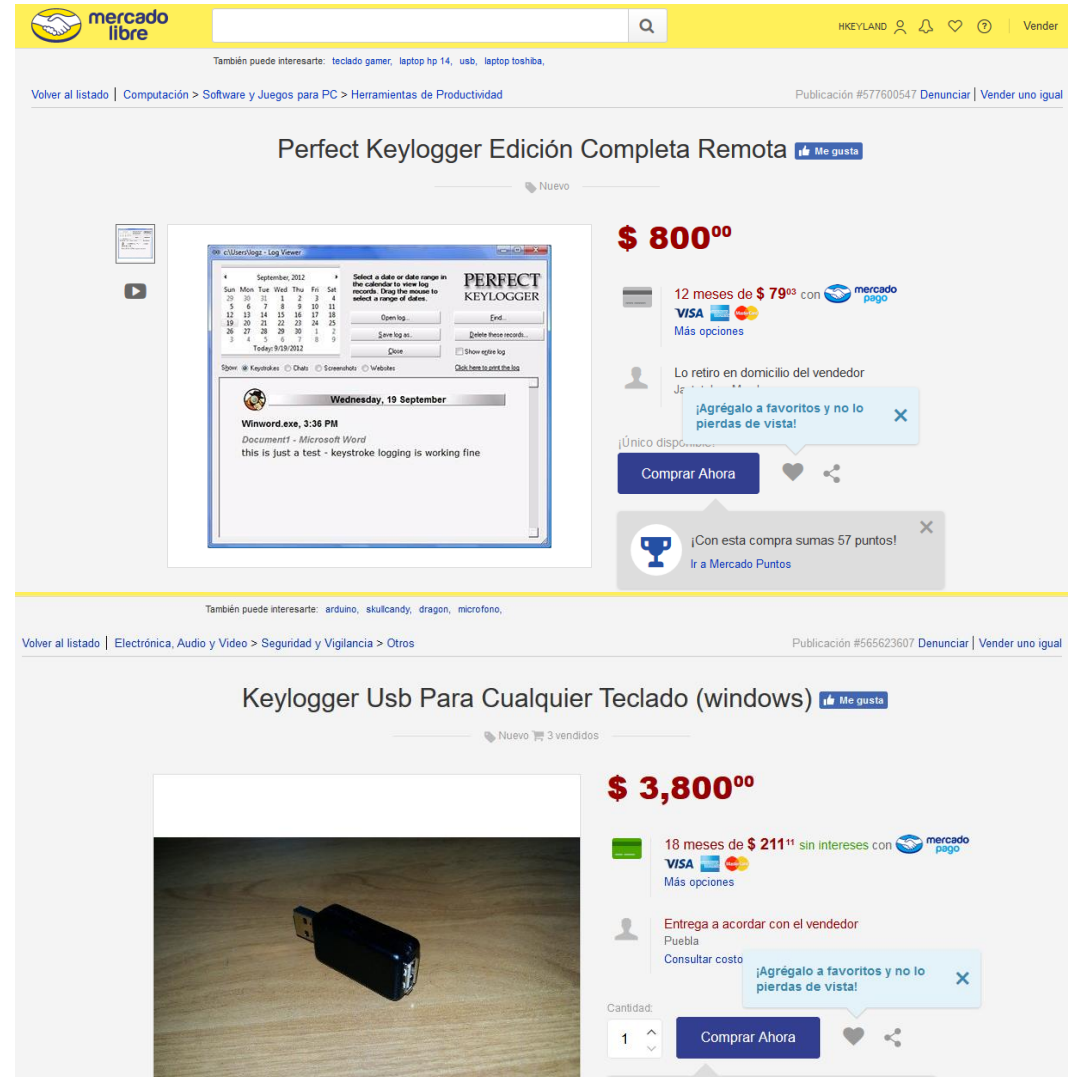
Utilice estas herramientas en sus propios equipos o con un permiso por escrito.

El presentador no se hace responsable del uso ilegal de estas herramientas.

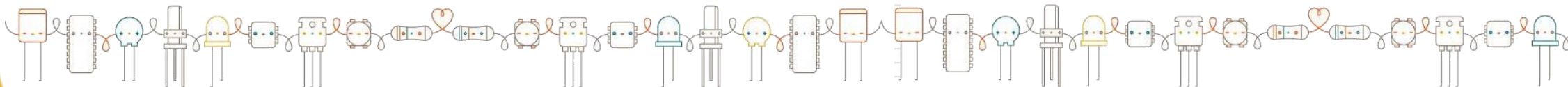


Keylogger

Programa o dispositivo que se encarga de almacenar las pulsaciones que se realizan en el teclado.



The image displays two screenshots of Mercado Libre listings. The top listing is for 'Perfect Keylogger Edición Completa Remota' priced at \$800.00. It features a screenshot of the software's interface, which includes a calendar for selecting a date range and a log viewer showing a sample entry for 'Winword.exe' at 3:36 PM. The bottom listing is for 'Keylogger Usb Para Cualquier Teclado (windows)' priced at \$3,800.00. It features a photograph of a black USB keylogger device. Both listings show payment options like VISA and Mercado Pago, and a 'Comprar Ahora' button.

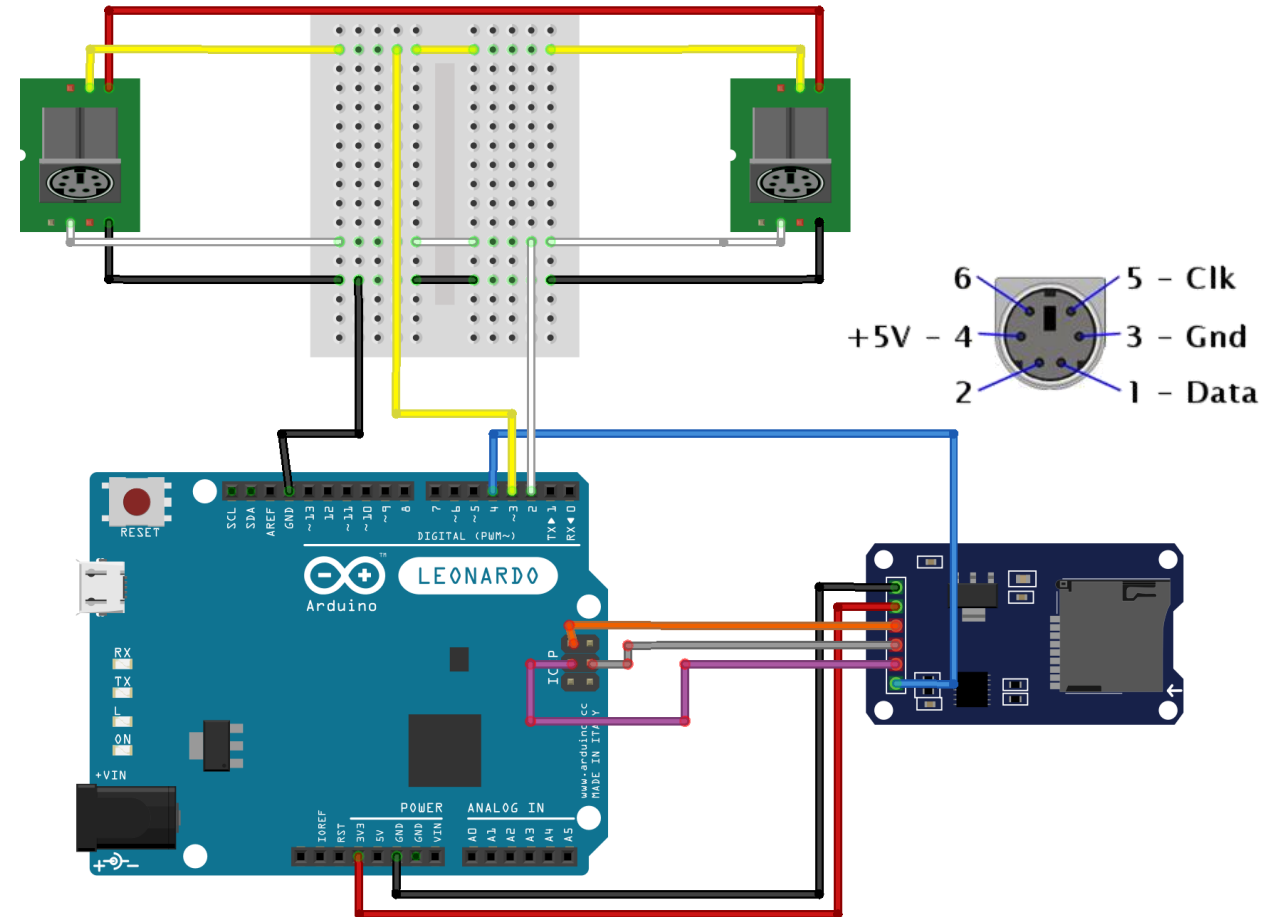




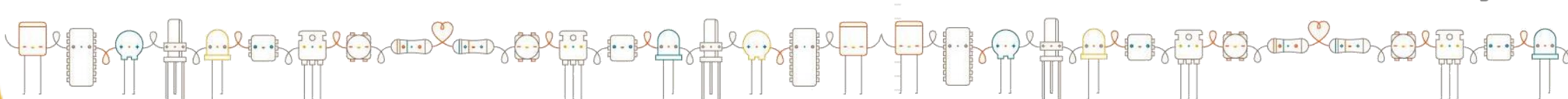
Keylogger

- Teclado PS2 (\$100)
- Arduino Leonardo o Uno (\$250)
- Protoboard (\$50)
- Módulo SD (\$40)
- MicroSD (\$50)

\$490 -> \$500

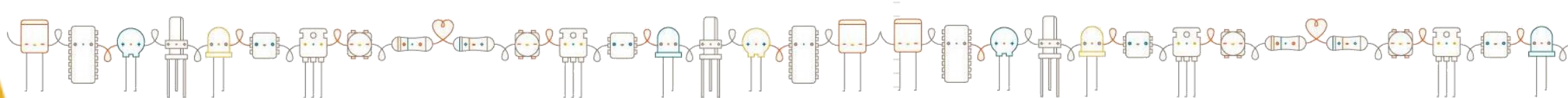


fritzing





Keylogger





RFID – NFC

Radio Frequency Identification
Unidireccional
Near field communication
Bidireccional

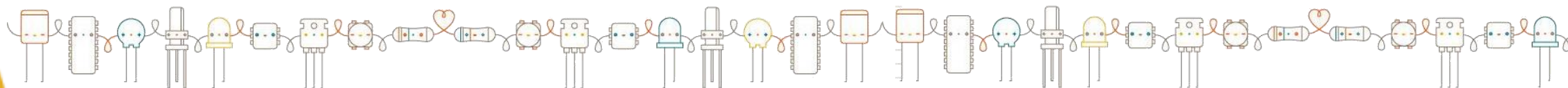
- Control de acceso (empleados)
- Transportes
- Pagos con tarjeta
- Identificación de cualquier tipo

RFID HACKING TOOLS

Tastic RFID Thief

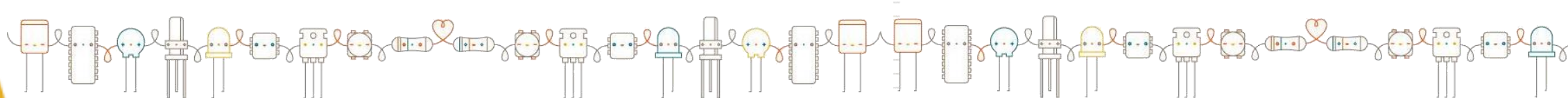


<http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/>





RFID – NFC

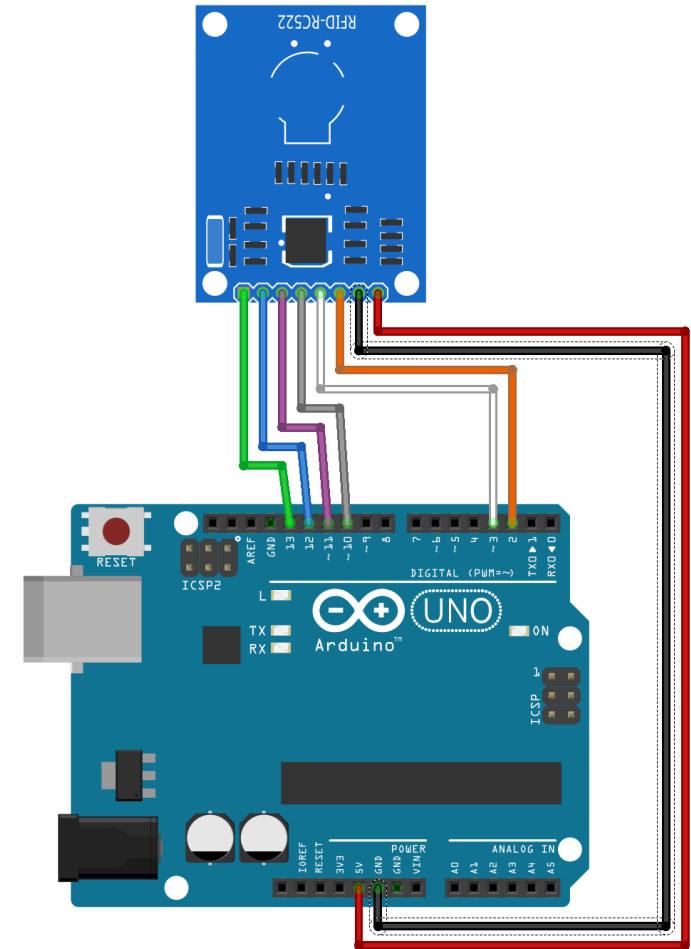


PN532

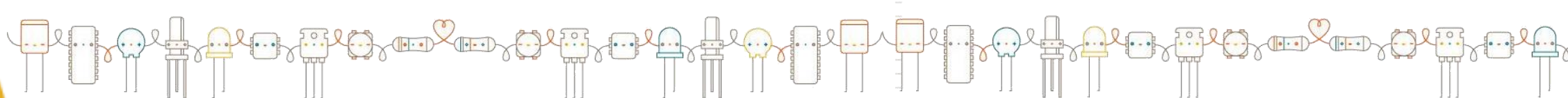
Este módulo permite leer tarjetas de identificación de acceso **Mifare**, como las utilizadas en el metro, gobierno y tarjetas de crédito.

Para la lectura de información se utiliza una clave de 6 valores de 0 hasta 255

[0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF]

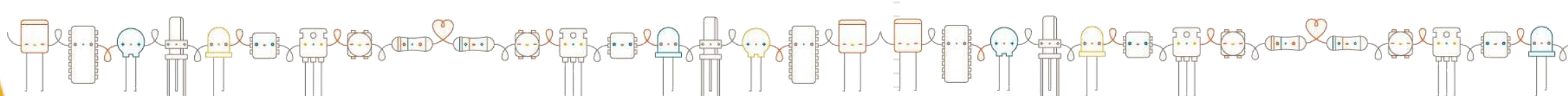


fritzing





readAllMemoryBlocks



Tarjeta Metro

Una vez conocida la llave es posible rellenar la tarjeta con la cantidad de dinero que se quiera.

```
COM3 (Arduino/Genuino Uno)
Enviar

0 0 49 20 49 20 49 20 49 20 49 20 49 20 49 20 | Block 1 | Data Block
49 20 49 20 49 20 49 20 49 20 49 20 49 20 49 20 | Block 2 | Data Block
0 0 0 0 0 0 69 67 89 0 0 0 0 0 0 0 | Block 3 | Sector Trailer
Found 1 tags
Sens Response: 0x4
Sel Response: 0x8
0x3E 0x57 0x2B 0x73
-----
Leyendo tarjeta id #1045900147
-----

3E 57 2B 73 31 88 4 0 46 4D 94 10 4D 10 27 8 | Block 0 | Manufacturer Block
0 0 49 20 49 20 49 20 49 20 49 20 49 20 49 20 | Block 1 | Data Block
49 20 49 20 49 20 49 20 49 20 49 20 49 20 49 20 | Block 2 | Data Block
0 0 0 0 0 0 69 67 89 0 0 0 0 0 0 0 | Block 3 | Sector Trailer
```

<http://mxhack.blogspot.mx/2011/01/tarjetas-rfid-metro-ciudad-de-mexico.html>

EXCELSIOR

IMAGEN
DIGITAL

TELE

PORTADA NACIONAL GLOBAL DINERO **COMUNIDAD** ADRENALINA FUNCIÓN HACKER

DELEGACIONES GOBIERNO SEGURIDAD

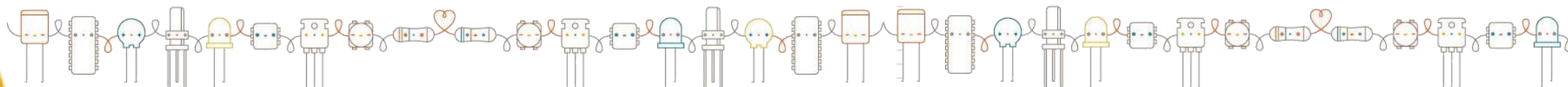
Defraudan 'piratas' con tarjetas TDF; transporte público capitalino

Venden en 350 pesos micas cargadas con 500 pesos para el Metro; ofrecen que es multimodal

29/08/2014 10:28 FILIBERTO CRUZ MONROY



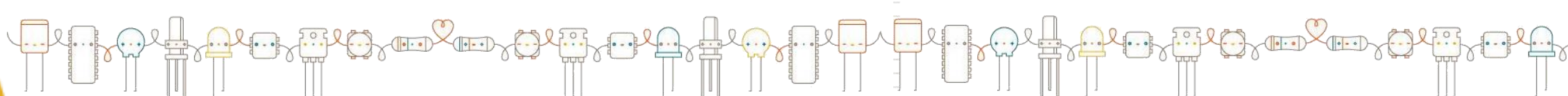
Descubren venta de tarjetas clonadas de transporte 'multi...





readMetroCard

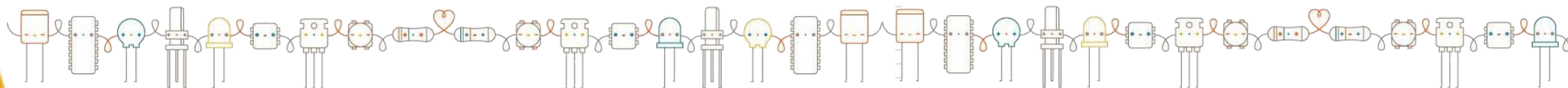
únicamente en Metro



Tarjeta Metro

EL Metro actualizo su sistema para que esto no ocurra (validación de saldo)

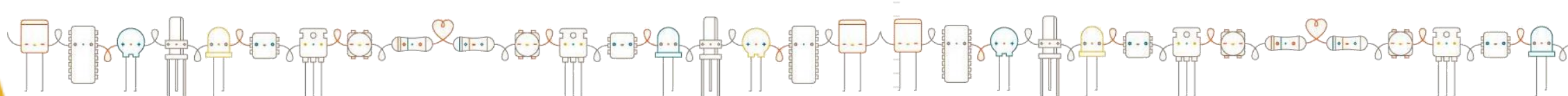
¿Cuánto durará?





Tarjetas bancarias

Esta misma tecnología se utiliza para la aprobación de pagos con acercar nuestra tarjeta.

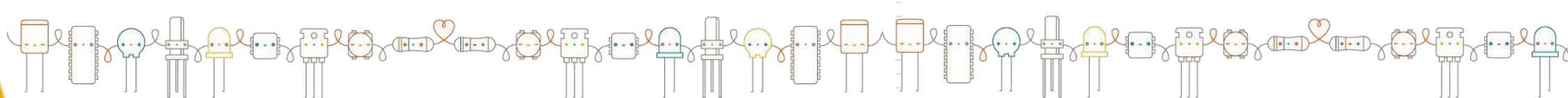


Contramedida

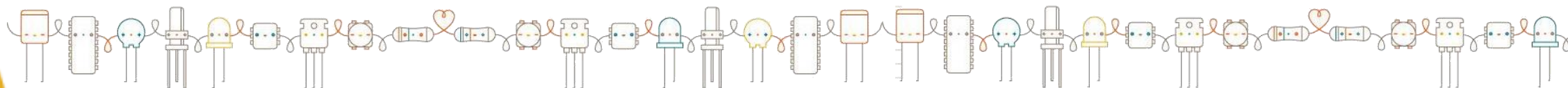
JINBAOLAI



**RFID
BLOCKING
WALLET**



Otros usos

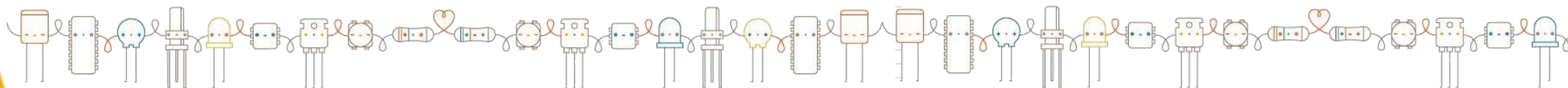
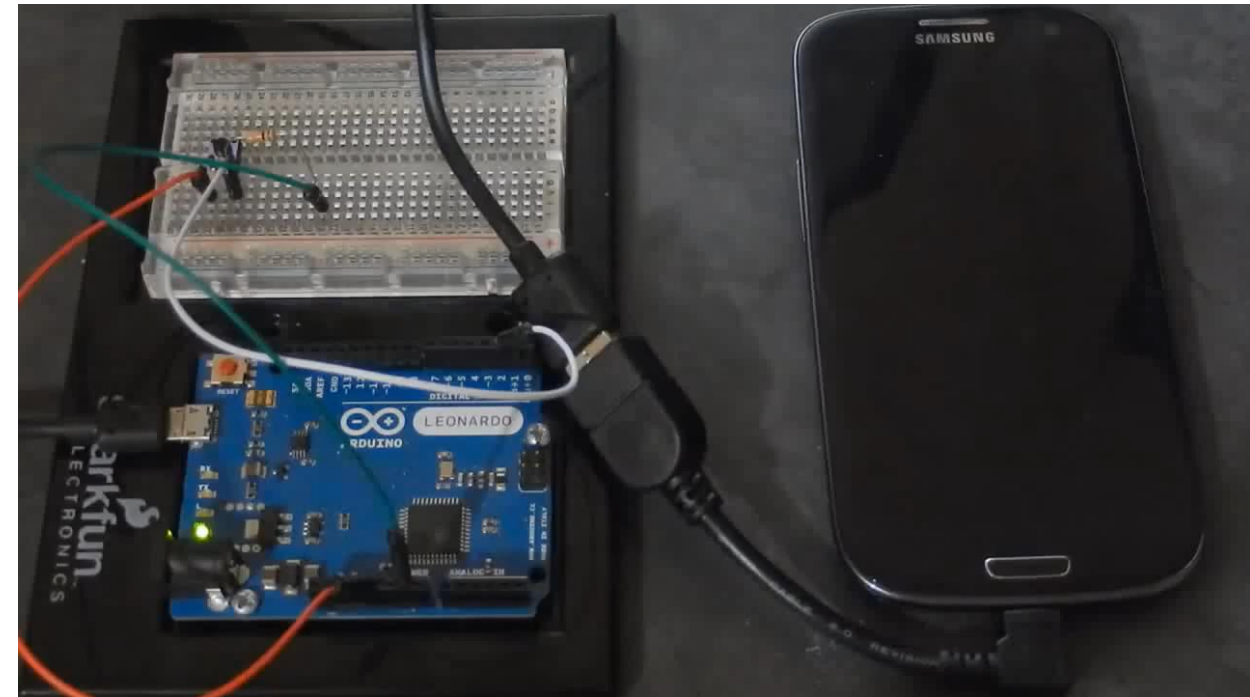


Android – Código de desbloqueo

Los dispositivos Android bloquean su uso mediante patrón o código de desbloqueo.

Generalmente el código es de 4 números con un retraso de 30 segundos cada 5 intentos

16 hrs para romper la clave



USB RUBBER DUCKY DELUXE

\$44.99

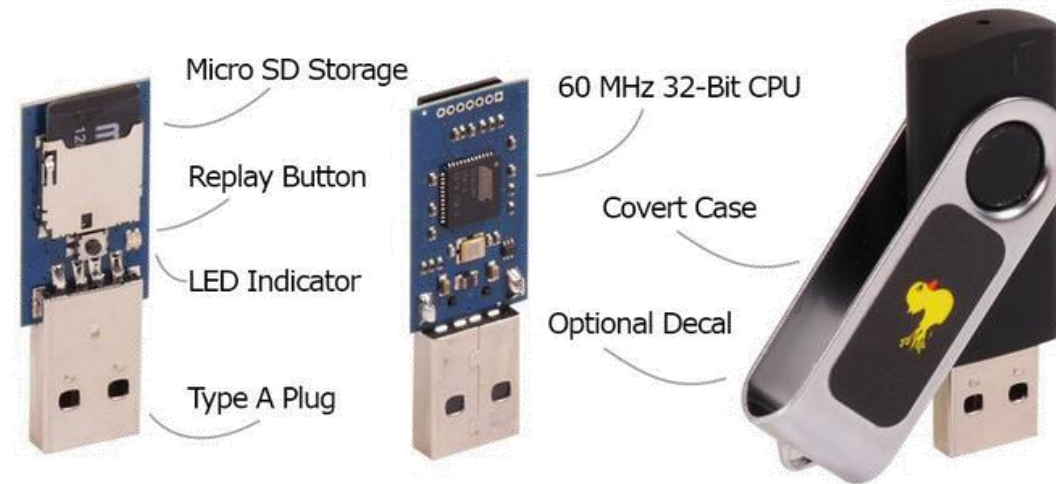
Quantity

1

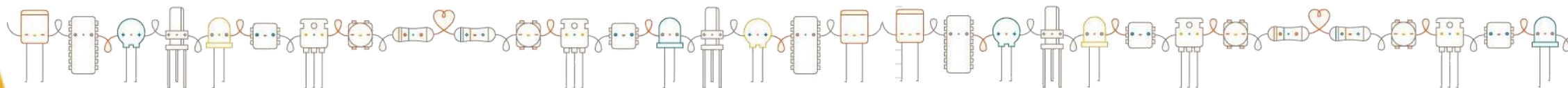
ADD TO CART

[Tweet](#) [Share](#) [Pin It](#) [Add](#) [Email](#)

[Email](#)



MR. ROBOT



Malduino – BAD USB

Emula un teclado para inyectar comandos en el equipo victima

MALDUINO — OPEN SOURCE BADUSB

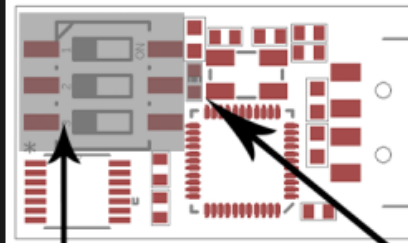
by: **Pedro Umbelino**

28 Comments

f t g+

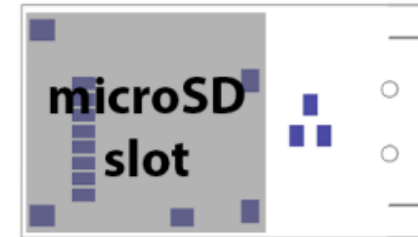
January 24, 2017

Top View

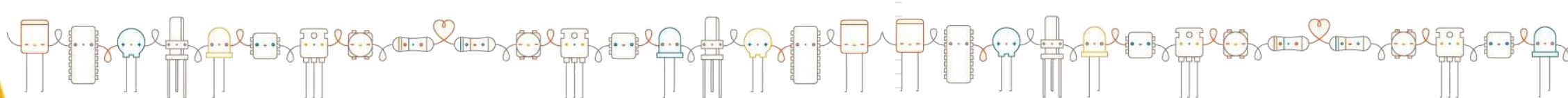


DIP Switches used to select different scripts

Bottom View

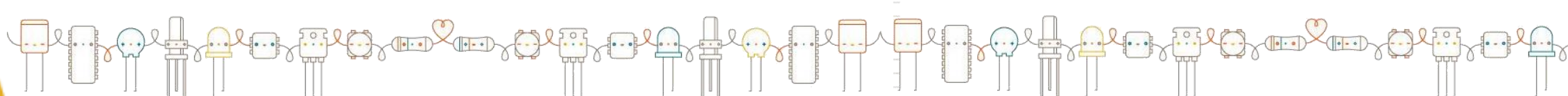


LED indicates when script is running and done





stealData



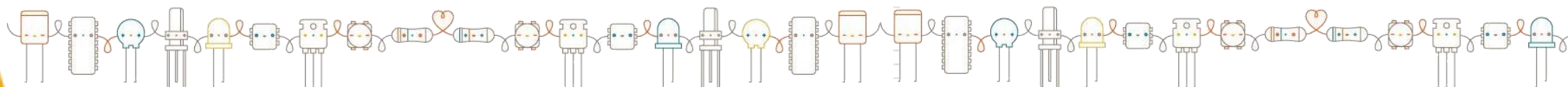


stealData

```
root@DESKTOP-T731MIS: /mnt/c/Users/k3y1and/Downloads/firefox_decrypt
root@DESKTOP-T731MIS:/mnt/c/Users/k3y1and/Downloads/firefox_decrypt# python firefox_decrypt.py pass/
2017-04-01 09:24:39,788 - WARNING - Attempting decryption with no Master Password

Website:  https://accounts.google.com
Username:  'k3y1andhk'
Password:  'hacking#'

Website:  https://es-la.facebook.com
Username:  'k3y1andhk@gmail.com'
Password:  'hacking$'
root@DESKTOP-T731MIS:/mnt/c/Users/k3y1and/Downloads/firefox_decrypt# ls pass/
cert8.db key3.db logins.json profiles.ini
root@DESKTOP-T731MIS:/mnt/c/Users/k3y1and/Downloads/firefox_decrypt#
```

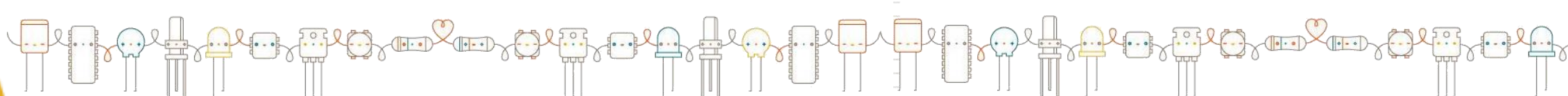




Enlaces Interesantes

<http://hackaday.com/?s=arduino>

<https://www.hackthissite.org/>





Gracias

¿Preguntas?

k31yand

[@hkeyland](http://k3y1and.blogspot.mx/hkeyland@gmail.com)

