

Duck Hunt (jugando a cazar patos)



@CONPilarZgz

www.conpilar.es

@HackAndBeers

#CONPilar® **HACK
&BEERS**

#CONPilar19

Let's tweet !!

#HBZaragoza19



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CØNPIlär®

**HACK
&BEERS**



@CONPilarZgz



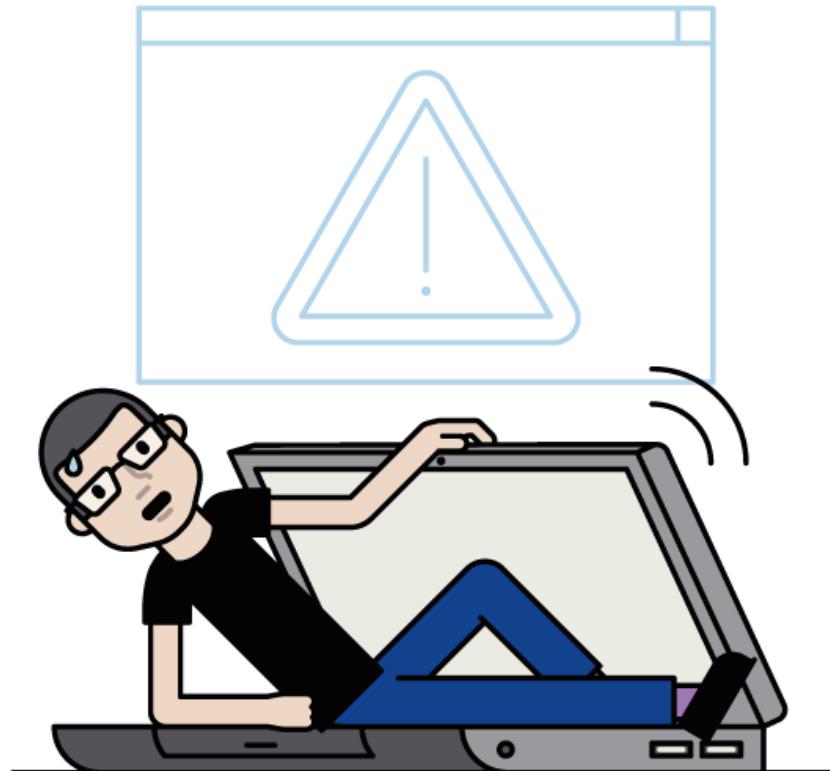
www.conpilar.es

@HackAndBeers

#CONPilar[®]

**HACK
&BEERS**

DISCLAIMER !!!



- La finalidad de esta charla es poner en su sitio los Bad USB
- Lo mostrado aquí a continuación es para “romper” patos
- Me hago responsable de los patos que bloqueéis
- HAZLO en tu casa

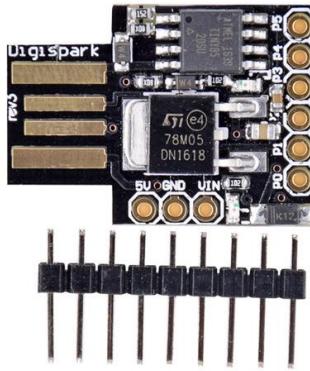


@CONPilarZgz



www.conpilar.es

@HackAndBeers



ATTiny85 – 2€

ATTINY85 Development board

USB Black Blue

Q Sitúa el cursor encima para hacer zoom

1 piezas azul negro TINY85 Digispark Kickstarter Micro placa de desarrollo ATTINY85 módulo Arduino C1 I2C USB

[Ver nombre original del producto en inglés](#)

★★★★★ 4.9 (236 votos) | 638 vendidos

Precio: **€ 1,18 - 1,22** / unidad



Envío: **€ 0,67 a Spain vía AliExpress Saver Shipping**

Tiempo de entrega: 17 días

Cantidad: **1** unidad (4842 unidades disponibles)

[Comprar ahora](#)

[Añadir a la cesta](#)

428

Cupón de nuevo usuario: **€ 2,71** PILLAR

Política de devoluciones: [Se aceptan devoluciones si el producto es muy distinto de su descripción. El comprador puede devolver el producto \(haciéndose cargo de los gastos de envío de vuelta\) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles](#)

Garantías del vendedor: [Entrega Puntual 60 días](#)

Pago:



@CONPilarZgz

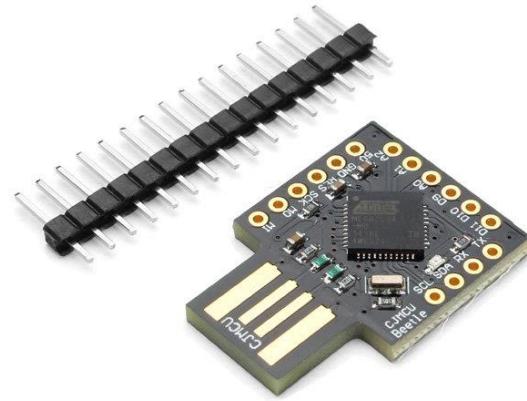


www.conpilar.es

@HackAndBeers

#CONPilar®

HACK
& BEERS



ATMEGA32U4 Mini – 4,70€

Portada de la Tienda Productos ▾ Artículos en oferta ▾ Más Vendidos Novedades Valoraciones

Inicio > Portada de la Tienda > Productos > Micro Mini ATmega32U4

Electronictfans

Pro Micro escarabajo teclado BadUSB USB ATMEGA32U4 Mini desarrollo placa de expansión para 16 Mhz DC 5 V para Arduino

Añadir nombre original del producto en inglés

★★★★★ 4,9 (80 votos) 272 vendidos

Precio: € 3,78 / unidad

Oferta: **€ 3,40** / unidad -10% 09h:28m:09s

Añadir más descuentos en la app | Precio al por mayor: ▾

Envío: € 1,28 a Spain vía AliExpress Saver Shipping ▾
Tiempo de entrega: 17 días

Cantidad: unidad (2422 unidades disponibles)

Comprar ahora **Añadir a la cesta** 316

Cupón de nuevo usuario: **€ 2,71 PILLAR**

Cupones de vendedor: **Recibir cupones de vendedor** ▾ **€ 2,71 dto. por cada € 80,24** ▾

Política de devoluciones: Se aceptan devoluciones si el producto es muy distinto de su descripción. El comprador puede devolver el producto (haciéndose cargo de los gastos de envío de vuelta) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles ▾

Garantías del vendedor: **Entrega Puntual**
60 días

Pago: **VISA** **MasterCard** **PayPal** **WESTERN UNION** **Bank Transfer** Ver más ▾

Protección del comprador



@CONPilarZgz

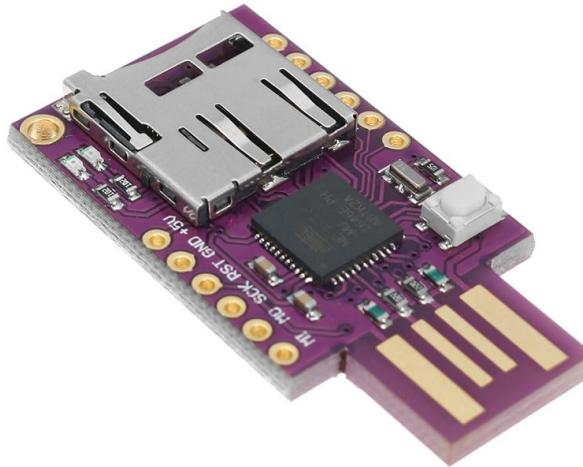


www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
&BEERS**



ATMEGA32U4 para Leonardo R3 – 6€

[Inicio](#) > [Portada de la Tienda](#) > [Productos](#) > [CJMCU series](#)

Q Sitúa el cursor encima para hacer zoom

TF tarjeta MicroSD USB TTF memoria teclado Virtual Badusb ATMEGA32U4 para Leonardo R3

[Ver nombre original del producto en inglés](#)

1 vendido

Precio: **€ 4,67** / unidad

Precio al por mayor: ▾

Envío: **€ 2,00 a Spain vía AliExpress Saver Shipping** ▾

Tiempo de entrega: 17 días

Cantidad: unidad (9991 unidades disponible)

[Comprar ahora](#) [Añadir a la cesta](#) 2

Cupón de nuevo usuario: **PILLAR**

Política de devoluciones: [Se aceptan devoluciones si el producto es muy distinto de su descripción.](#) El comprador puede devolver el producto (haciéndose cargo de los gastos de envío de vuelta) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles ▾

Garantías del vendedor: [Entrega Puntual 60 días](#)

Pago:

Protección del comprador

Devolución íntegra del dinero si no recibes tu pedido

Reembolso íntegro o parcial si el artículo es distinto de su descripción

Saber más ▾



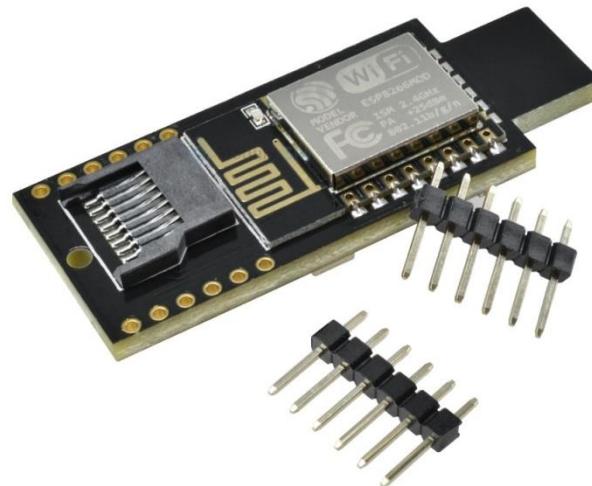
@CONPilarZgz

@HackAndBeers

www.conpilar.es

#CONPilar®

**HACK
&BEERS**



ESP8266 WiFi inalámbrico ATMEGA32U4 – 13€

[Inicio](#) > [Portada de la Tienda](#) > [Productos](#) > [Wifi Modules](#)



ESP8266 WiFi inalámbrico teclado Virtual módulo de memoria de tarjeta de memoria TF 802.11b/g/n ATMEGA32U4 Placa de desarrollo ESP-8266

[Ver nombre original del producto en inglés](#)

1 vendido

Precio: €15,01 / unidad

Oferta: € 10,51 / unidad -30% 09h:21m:55s

[Aún más descuentos en la app](#)

Envío: € 2,68 a Spain vía AliExpress Standard Shipping

Tiempo de entrega: 14 días

Cantidad: unidad (624 unidades disponible)

[Comprar ahora](#)

[Añadir a la cesta](#)



Cupón de nuevo usuario:

€ 2,71 PILLAR

Cupones de vendedor:

[Recibir cupones de vendedor](#) € 0,91 dto. por cada € 26,15

Política de devoluciones

Se aceptan devoluciones si el producto es muy distinto de su descripción. El comprador puede devolver el producto (haciéndose cargo de los gastos de envío de vuelta) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles

Garantías del vendedor:

Entrega Puntual 60 días

Pago:

Ver más

[Protección del comprador](#)



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CØNPIlär®

HACK
&BEERS



BAD USB ATMEGA32U4 – 5,20€

Inicio > Portada de la Tienda > Productos > Others


MODULE FANS



Q. Sitúa el cursor encima para hacer zoom

Microcontrolador USB BadUsb Bad ATMEGA32U4 Placa de desarrollo teclado virtual para Arduino 5 V DC 16 MHz 5 CANALES

[Ver nombre original del producto en inglés](#)

★★★★★ 5.0 (21 votos) | 79 vendidos

Precio: € 4,23 /unidad

Oferta: **€ 3,81** / unidad -10% 09h:12m:43s

[Aún más descuentos en la app](#) | Precio al por mayor: ▾

Envío: € 1,41 a Spain vía AliExpress Saver Shipping ▾
Tiempo de entrega: 17 días ?

Cantidad: unidad (11465 unidades disponibles)

[Comprar ahora](#) [Añadir a la cesta](#)

477

Cupón de nuevo usuario:

Cupones de vendedor: € 1,81 dto. por cada € 59,50

Política de devoluciones: Se aceptan devoluciones si el producto es muy distinto de su descripción. El comprador puede devolver el producto (haciéndose cargo de los gastos de envío de vuelta) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles ▶

Garantías del vendedor: Entrega Puntual 60 días

Pago:       Ver más ▶

Protección del comprador

Devolución íntegra del dinero si no recibes tu pedido
 Reembolso íntegro o parcial si el artículo es distinto de su descripción

Saber más ▶



@CONPilarZgz

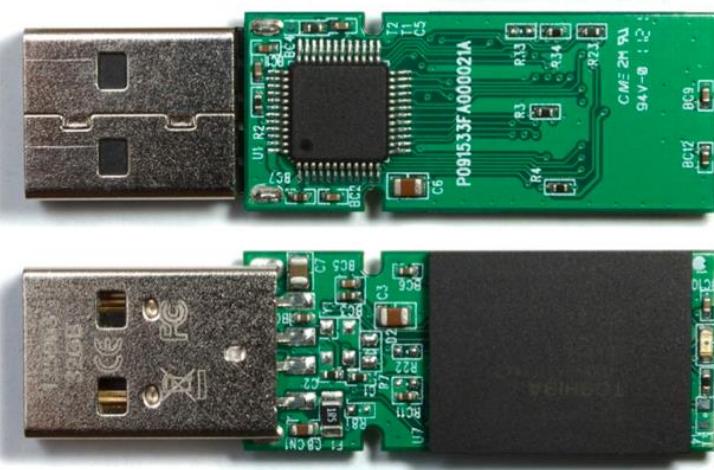


www.conpilar.es

@HackAndBeers

#CØNPIlår®

HACK & BEERS



PENDRIVE – PHISON 2251-03 (2303) – 5€

<https://www.quora.com/Which-USB-drives-contain-Phison-2251-03-2303-controller-type>



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

HACK
& BEERS



BADUSB Cable Harpoon – ¿?€



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

**HACK
&BEERS**

The screenshot shows a web browser window with the URL <https://sneaktechnology.com/product/usbninja-basic/>. The page title is "USBNinja Basic". It features a product image of a white USB cable connected to a laptop, with a small circuit board (the USBNinja) visible. Below the image, there is a "Buy now" button and an "Add to cart" button. The price is listed as \$99.00 USD. The page also includes a "Type" dropdown set to "Type - C" and a quantity selector with a value of 1.

BADUSB Cable

USB NINJA

<https://sneaktechnology.com/>
89\$ - 99\$



@CONPilarZgz

@HackAndBeers



www.conpilar.es

The screenshot shows a campaign page for "USBNinja" on Crowd Supply. The page header includes "CROWD SUPPLY", "BROWSE", "LAUNCH", and "ABOUT US". The main title is "USBNinja" by RFID Research Group. A sub-header states "BadUSB embedded into a USB cable". On the right, there is a summary box with "\$34,848 raised of \$10,000 goal" and "348% Funded!". It also shows the date "Nov 03 funded on Nov 04, 2018" and the number of backers "163". Below this, there is a video player showing a video titled "03:06" and a "Recent Updates" section. The main content area shows four different colored USBNinja modules (white, green, blue, red) and a laptop connected to one of them via a USB cable.



#CONPilar®

HACK
& BEERS



Phoenix Ovipositor ATmega32U4 – ¿?€

Ovipositor

[¿QUÉ ES?](#) [CAPACIDADES](#) [CARACTERÍSTICAS](#) [CONTACTO](#)

English Espanol

introducidos por teclado, independientemente del sistema operativo anfitrión, incluso sin que éste haya arrancado todavía

(Windows - Linux - MacOS - Android)

forma desatendida y transparente: se pueden emular pulsaciones de teclado mediante un sencillo sistema de scripting.

puede usarse para controlar otros dispositivos (módulos WiFi, Bluetooth, ZigBee...).

Envío de los datos obtenidos a otros dispositivos móviles.

CARACTERÍSTICAS TÉCNICAS

- ☞ Dimensiones de la placa
Sin conectores: 38 x 17 mm
Con conectores USB macho y hembra: 62 x 17 mm
- ☞ Microcontrolador ATmega32U4 a 16 MHz.
- ☞ Zócalo para tarjeta microSD, admite 32 GB.
- ☞ Puerto serie y pines de VCC (3,3V) y GND disponibles.
- ☞ Posibilidad de desarrollar firmwares personalizados.

[Ver hoja de producto](#)



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CØNPIl
r®

HACK
&BEERS



Rubber Ducky HAK5 – \$44.99

PRODUCTS ▾ PODCASTS ▾

HAK5

COMMUNITY SUPPORT

USB RUBBER DUCKY

\$44.99

Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among hackers, pentesters and IT pros. With its debut, keystroke injection attacks were invented – and since it has captured the imagination with its simple scripting language, formidable hardware, and covert design.

QTY

— 1 +

ADD TO CART



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
& BEERS**

#CONPilar19

Let's tweet !!

#HBZaragoza19



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CØNPIlår®

**HACK
&BEERS**

#CONPilar19

Let's tweet !!

#HBZaragoza19



RED TEAM



BLUE TEAM



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CØNPlilr®

**HACK
&BEERS**

PROTECCIONES

- Patito Hunter de Miguel Ángel Arroyo
- Condom USB
- Políticas de Windows
- USBDevview
- Shielducky de Álex Torrecrack



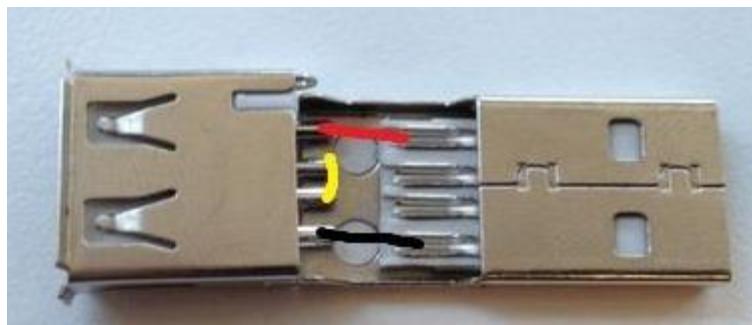
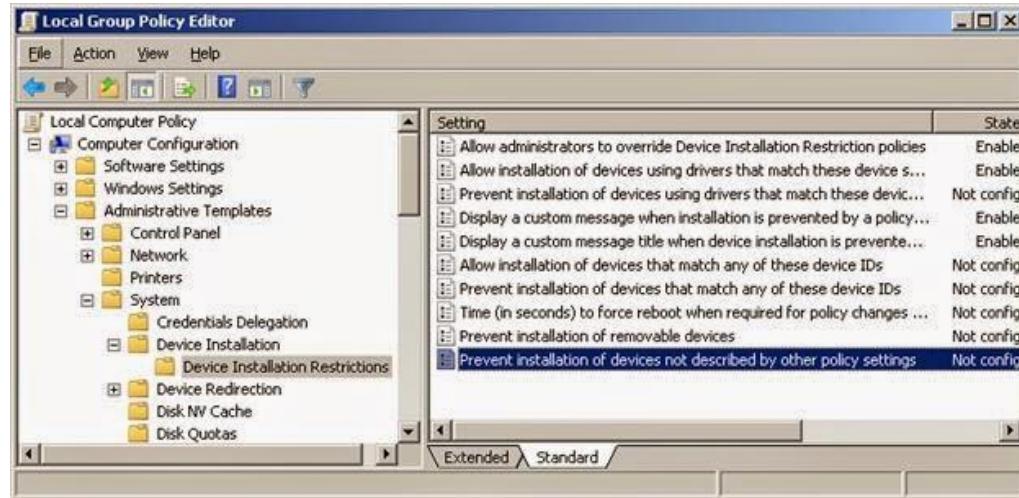
@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CØNPIlär® **HACK
&BEERS**



Device N...	Description	Device Type	Connected	Safe To Un...	Disabled	USB H...
USB Device	USB Mass Storage ...	Mass Storage	No	No	No	No
USB Device	Generic Bluetooth ...	Bluetooth Device	No	Yes	No	No
USB Device	Generic Bluetooth ...	Bluetooth Device	No	Yes	No	No
USB Device	VirtualBox USB	Vendor Specific	No	No	No	No
USB2.0 WLAN	3Com OfficeConne...	Vendor Specific	No	No	No	No
USB2.0 WLAN	3Com OfficeConne...	Vendor Specific	No	No	No	No
USB2.0 WLAN	3Com OfficeConne...	Vendor Specific	No	No	No	No

Fuentes:

<http://www.elladodelmal.com/2014/05/usb-rubber-ducky-un-teclado-malicioso.html>
<https://hacking-etico.com/2016/03/14/patito-hunter/>



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

HACK
&BEERS



@CONPilarZgz

www.conpilar.es

@HackAndBeers

#CØNPIlär®

**HACK
&BEERS**



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CØNPIlår®

**HACK
&BEERS**

OPCIÓN 1



AMAZON - 8€



AMAZON 21€



@CONPilarZgz



www.conpilar.es

@HackAndBeers

OPCIÓN 2



Tesis - HyperTerminal

Archivo Edición Ver Llamar Transferir Ayuda

AT
OK
AT+CMGF?
+CMGF: 0

OK
AT+CMGF=?
+CMGF: (0,1)

OK
AT+CMGF=0
OK
AT+CMGF=1
OK

0:00:36 conectado Autodetect. 9600 8-N-1 DESPLAZAR MAY NUM Capturar



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CØNPIlär®

**HACK
&BEERS**

EMAIL - KINGSTON

Kingston Technology #3294899 ► VIEJO FEB-19 x

Kingston Customer Service <customerservice@kingston.eu>
para informática ▾ mar., 23 oct. 2018 16:28 ★ ↗

Traducir mensaje Desactivar para: inglés ▾

Estimado Eloy,

Le agradecemos el interés mostrado por Kingston Technology y sus productos.

Con referencia a su solicitud, la información sobre los comandos AT que ha solicitado es una información solamente interna y no es una función que ofrezca Kingston. Estas unidades se han diseñado como dispositivos de almacenamiento. Lamentamos comunicarle que no vamos a poder ayudarles en esta ocasión.

No dude en contactarnos para cualquier otro tipo de información.

Un cordial saludo,
Jonathas Soares

Trataremos sus datos con respeto y sus detalles serán guardados y protegidos de forma segura. Puede encontrar más detalles en nuestra [política de privacidad](#)



@CONPilarZgz



www.conpilar.es

@HackAndBeers

**HACK
&BEERS**

EMAIL - TOSHIBA

Re: [TOSHIBA#2018102249006391] Contact form

Toshiba Memory Europe GmbH <support@toshiba-memory.com>
para contacto ▾

No se muestran las imágenes. Mostrar las imágenes a continuación - Mostrar siempre

inglés ▾ > español ▾ Traducir mensaje

Dear valued customer,

Thank you for contacting the Toshiba Memory Europe GmbH.

We apologize for the long processing time. We had technical issues.

Our service is offered in english or german language only.

Please send your request in either one of those languages and we will be glad to be of ass

Thank you.

Best regards,

Percy König
Support Engineer



@CONPilarZgz

@HackAndBeers



www.conpilar.es

informática eloy <contacto@informaticaeloy.com>
para support ▾

Hello Goodnight. I'm developing a study for the university, and I would like to know the AT commands to communicate with a Toshiba pendrive through UART. Thank you, your help will be very necessary.

Remitente notificado con
[Mailtrack](#)

Toshiba Memory Europe GmbH <support@toshiba-memory.com>
para informática ▾

No se muestran las imágenes. Mostrar las imágenes a continuación - Mostrar siempre imágenes de support@toshiba-memory.com

inglés ▾ > español ▾ Traducir mensaje

Dear valued customer,

thank you for contacting the Toshiba Memory Europe GmbH.

For our consumer products,we can only provide the technical details provided on our website:

<https://www.toshiba-memory.com/>

Thank you for your understanding.

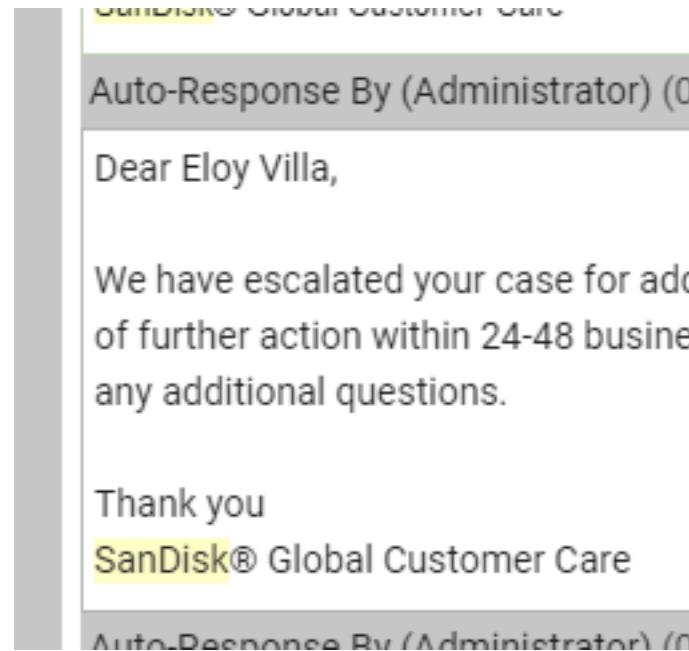
Best regards

Thorsten Freimann



HACK
&BEERS

EMAIL - SANDISK



Response By Email (Sarah K.) (03/01/2019 05:23 PM)

Dear Mr. Villa,

I would like to thank you for contacting us.

I understand you would like to know some details about the Ultra USB 3.0 16GB as the AT Commands to communicate with a USB through UART.

I have to inform you that this information is not published for our retail products, this is considered engineering level information, and it is not available for sharing.

I want to inform you also that I had escalated your case to the higher level team in order to see if I can get this information for you, but unfortunately this information can be shared.

This is the page support in case you want to take a look to our articles:

[USB page support](#)

[Click here](#) to register your product online.

Para su información: Si lo prefiere, Ud. también puede comunicarse con nosotros en Español.

Date Created: 02/27/2019 12:22 PM



@CONPilarZgz

@HackAndBeers

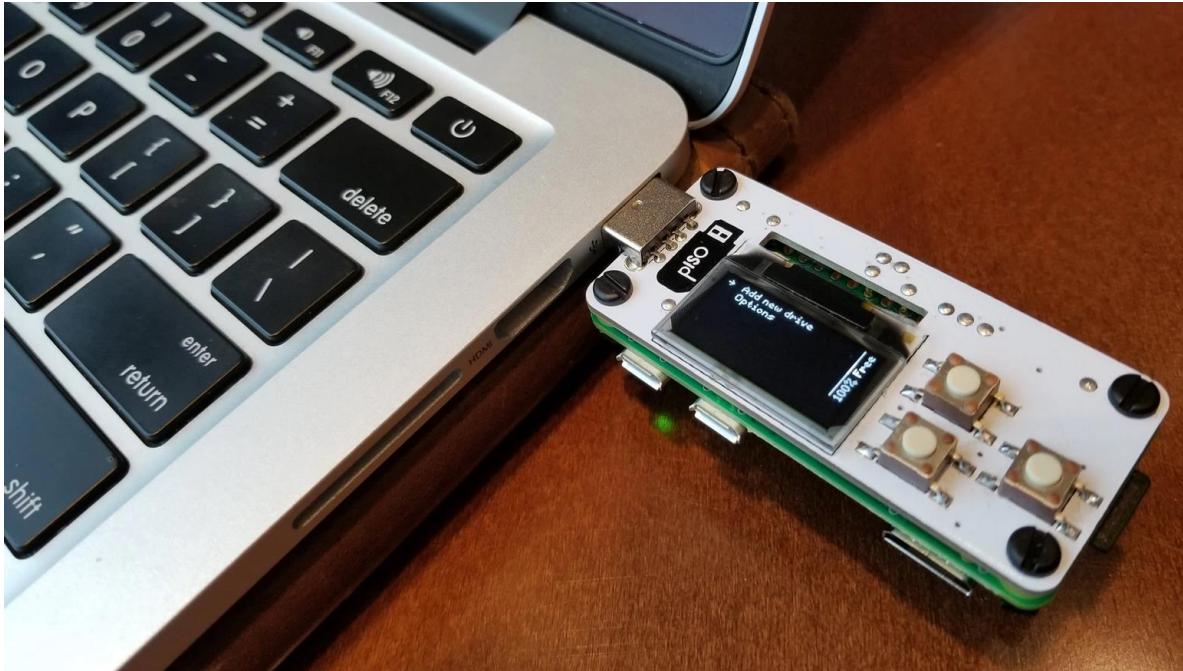


www.conpilar.es

#CØNPIlår®

HACK
&BEERS

OPCIÓN 3



<https://www.kickstarter.com/projects/178023282/piso-the-most-versatile-flash-drive-yet/posts?page=3>



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

HACK
& BEERS

OPCIÓN 4



<https://www.tme.eu>

1070€ + IMPUESTOS



<https://www.meilhaus.de>

745€ + IMPUESTOS



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CØNPIlär®

HACK
&BEERS

OPCIÓN 4.2



Adafruit Beagle USB 12

<https://thepihut.com>

£370€ (430€) + IMPUESTOS



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CØNPIlär®

HACK
& BEERS

OPCIÓN 4.3

Aliexpress
140€

The image shows a screenshot of an AliExpress product page for a "USBCAN-I Bas" USB-CAN interface. The product is a black rectangular device with a green header labeled "USBCAN". It has several pins labeled "USB", "RX", "SYS", "TX", and "PWR". The page features Chinese text at the top: "广成科技" (Guangcheng Technology), "USBCAN-I Bas", and "包邮" (Free shipping). Below the device, there is more Chinese text: "高性能工业CAN卡, 性价比高" (High-performance industrial CAN card, high price-to-value ratio), "支持J1939 DBC分析" (Supports J1939 DBC analysis), and "兼容周立功USBCAN" (Compatible with ZLW USBCAN). To the right of the product image, the product details are listed: "Guangcheng tecnología USB-CAN autobús analizador USB puede tarjeta usbcn convertidor J1939 protocolo de análisis", "Precio: € 117,19 / unidad", "Envío: € 21,84 a Spain vía AliExpress Standard Shipping", "Cantidad: 1", "Comprar ahora", "Añadir a la cesta", and a "Cupón de nuevo usuario: € 2,71 PILLAR". At the bottom, there is a note about returns: "Se aceptan devoluciones si el producto es muy distinto de su descripción. El comprador puede devolver el producto (haciéndose cargo de los gastos de envío de vuelta) o quedarse con el producto y acordar con el vendedor la devolución del dinero. Ver detalles ▶".



@CONPilarZgz
www.conpilar.es

@HackAndBeers

#CONPilar®

HACK
& BEERS

OPCIÓN 4.3.1

Amazon
13€

Compraste este producto el 7 feb 2019.
Tamaño: 1x Logic Analyzer | Ver este pedido



AZDelivery ★★★★★ Logic Analyzer analizador logico con ebook Gratis!
de AZDelivery
★★★★★ 6 opiniones de clientes

Precio: EUR 10,74 IVA no incluido
EUR 12,99 IVA incluido
Envío gratis (2 días) para clientes Prime
Precio final del producto

Entrega GRATIS el lunes
si haces el pedido en 21 hrs y 25 mins. Ver detalles

Tiempo de envío superior a lo normal en artículos de Prime. Más información ▾
En stock.

Factura con IVA descargable ▾ | Vendido por AZDelivery-Shop y gestionado por Amazon. Se puede envolver para regalo

Nuevo desde EUR 12,99

Tamaño: 1x Logic Analyzer

1x Charger Doctor EUR 6,29 prime	1x Logic Analyzer EUR 12,99 prime	1x Voltímetro Amperímetro EUR 7,09 prime	3x Charger Doctor EUR 12,99 prime
3x Logic Level EUR 7,49 prime	6x Logic Level EUR 9,99 prime		

- ✓ Compatible con software de análisis Logic y programas de código abierto como sigrok (análisis de protocolo de RS232)
- ✓ 9 entradas de señal mensurables paralelas (0-5V) con hasta 24 millones de pasos de medición por segundo!
- ✓ Dimensiones (LxAnxAl): 55 x 28 x 14 mm
- ✓ Incluye cable de conexión de aprox. 100cm mini USB y cable plano de 10 polos (20cm).
- ✓ ¡En cualquier caso usted recibirá una factura con IVA incluido según las normas alemanas, así como productos de alta calidad de España por compra de ★★★★ AZDelivery! Con el eBook gratuito de AZDelivery, usted puede comenzar directamente sin tener que dedicar mucho tiempo a configurar el producto.

Ver más detalles



@CONPilarZgz

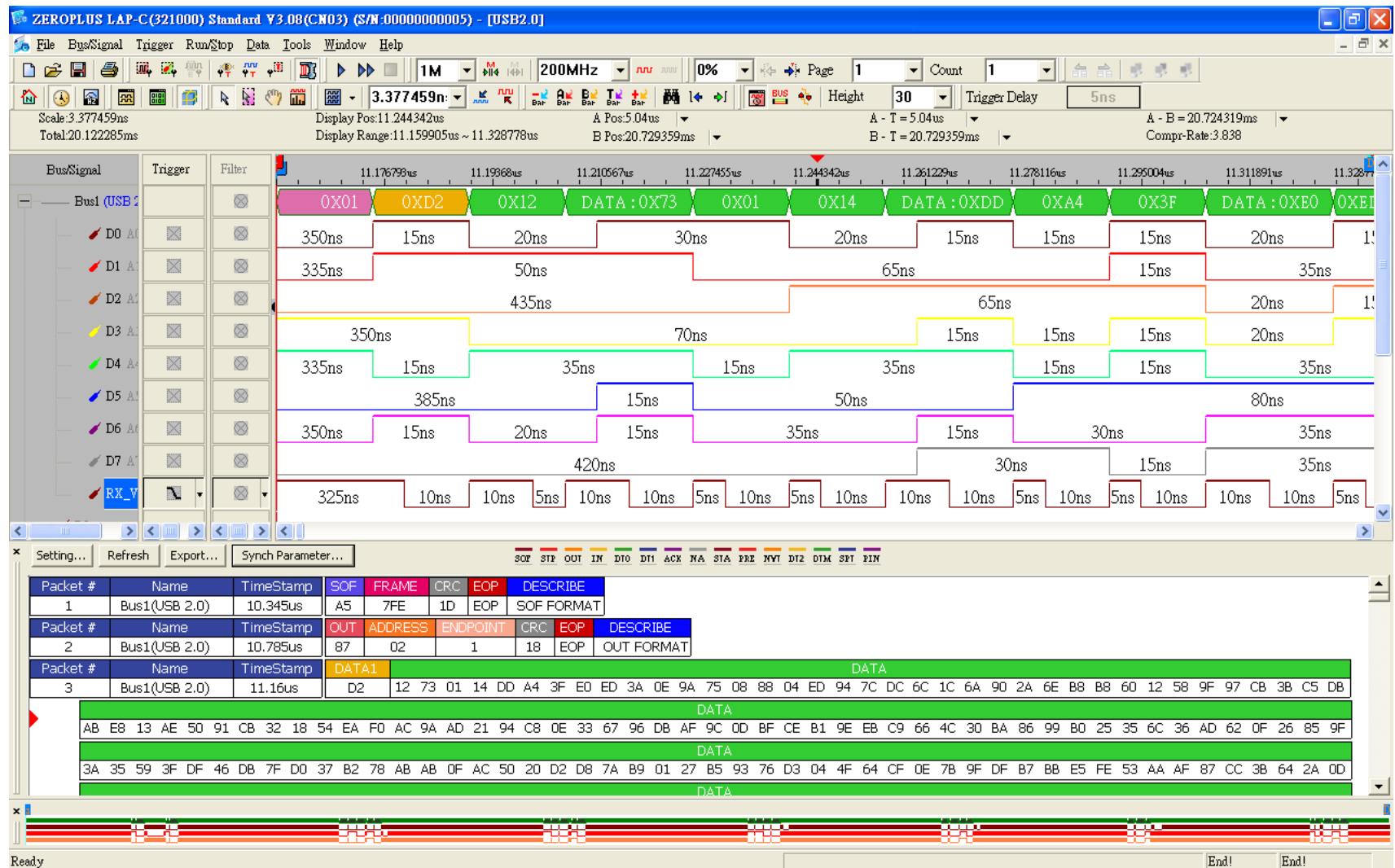


www.conpilar.es

@HackAndBeers

#CONPilar®

HACK & BEERS



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
&BEERS**

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
1	+0 =0	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
2	+94870 =94870	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 30	0x000B570C2BAA	02 01 06 02 0A 08 09 03 03 18 02 18 04 18 09 18 07 09 42 47 4D 31 31 31	0x22D91B	-47	OK
3	+16376 =111246	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
4	+110622 =221868	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
5	+119995 =341863	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
6	+02005 =423868	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 21	0x0069CD40DE94	02 01 1A 08 FE 4C 00 09 06 03 02 C0 AB 1D C3	0xC9B2FF	-67	OK
7	+35492 =459360	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
8	+113121 =572481	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
9	+33890 =606371	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 21	0x0069CD40DE94	02 01 1A 08 FF 4C 00 09 06 03 02 C0 AB 1D C3	0xC9B2FF	-66	OK
10	+70482 =676853	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
11	+101871 =778724	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
12	+108747 =887471	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 36	0x0007802FAA29	02 01 06 1A FF 4C 00 02 15 E2 C5 6D B5 DF FB 45 D2 B0 60 D0 F5 A7 10 96 E0 00 00 00 00 C6	0xB7E630	-34	OK
13	+87650 =975121	0x25	0xEE89BED6	ADV_IND	Type TxAdd1 RxAdd1 PDU-Length 0 0 0 21	0x0069CD40DA94	02 01 1A 08 FF 4C 00 09 06 03 02 C0 AB 1D C3	0xC9B2FF	-65	OK
P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
Capturing device Radio Configuration Select fields Packet details Address book Display filter Time line										
Field Name: <input type="text"/> Template: <input type="text"/>										
Filter condition: <input type="text"/>										
Filter management:										
First And										
<input type="button" value="Add"/>										
<input type="button" value="Remove"/>										
<input type="button" value="Open"/>										
<input type="button" value="Save"/>										
<input type="button" value="Merge"/>										
<input type="button" value="Turn off filter"/>										



@CONPilarZgz

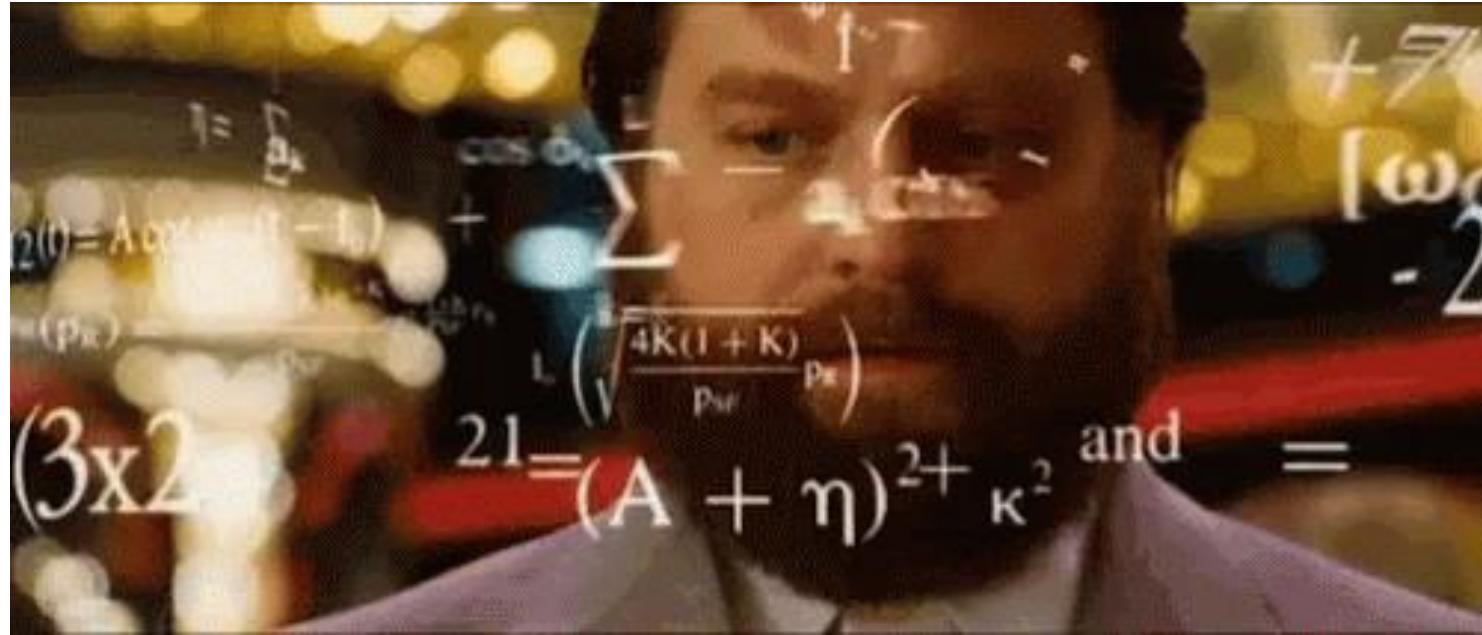
@HackAndBeers



www.conpilar.es

#CONPilar®

HACK
&BEERS



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPil r® **HACK
&BEERS**

OPCIÓN 5 (beta)

¿Qué me falta? ¿En que fallo?

- Blockchain
- IA
- Cloud Computing
- Machine Learning
- Tor
- Deep Web
- 6G
- Fuga de talento



@CONPilarZgz

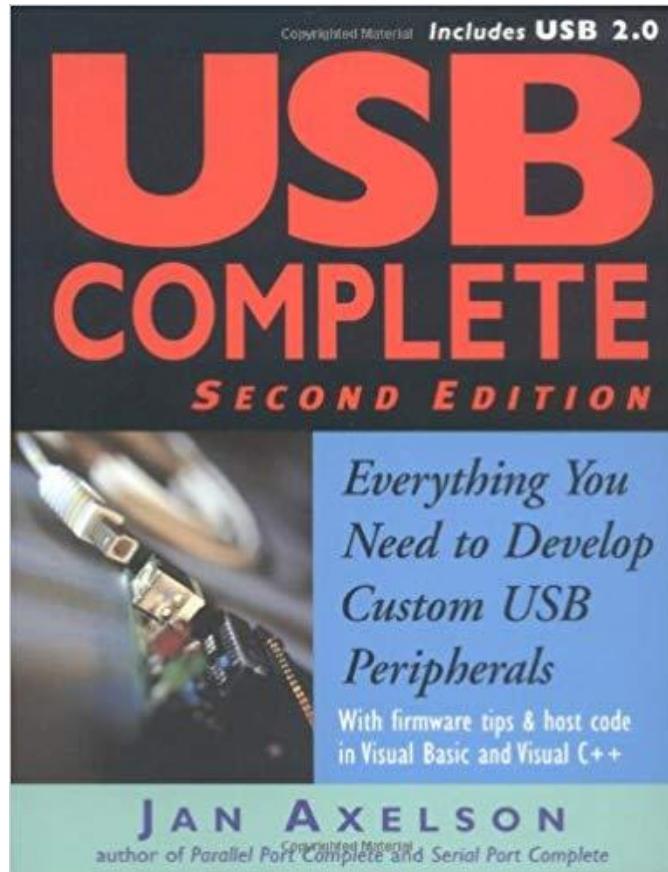


www.conpilar.es

@HackAndBeers

#C0NPIlarr® **HACK
&BEERS**

OPCIÓN 6



AMAZON
2ª mano
8€

business Libros en idiomas extranjeros ▾

Enviar a ELOY
Ejea De L... 50600 Departamentos ▾ Volver a comprar Las ofertas de hoy Características Vender en Amazon B

Libros en idiomas extranjeros Búsqueda avanzada Todos los géneros Preventa Los más vendidos Todos los Libros Catalán Galle USB Complete: The Developer's Guide (Complete Guides series) y más

Libros > Informática, internet y medios digitales > Hardware y dispositivos portátiles

i Compraste este producto el 12 nov 2018.
[Ver este pedido](#)

Echa un vistazo ↓

USB Complete: Everything You Need to Develop Custom US
1 jun 2005
de Jan Axelson ▾ (Autor)
★★★★★ 78 opiniones de EE. UU.

> Ver los 7 formatos y ediciones

Versión Kindle EUR 32,68 IVA incluido Tapa blanda desde EUR 7,76

Ler con nuestra App gratuita 6 Usado desde EUR 7,76
3 Nuevo desde EUR 23,38

Nota: Este producto sólo está disponible de otros vendedores (ver todas las ofertas).

Hay una nueva edición de este producto:
USB Complete FIFTH EDITION EUR 34,36 En stock.

Usb Complete 5th Edn: The Developer's Guide (Complete Guides)



@CONPilarZgz

www.conpilar.es

@HackAndBeers

#C0NPIlarr®

**HACK
&BEERS**

- El USB (*Universal Serial Bus*) se creó para unificar la gran variedad de conectores serie que existían
 - Facilmente configurable
 - Permite la conexión en caliente (*plug and play*)
 - El SO detecta la conexión y desconexión de dispositivos
 - El SO identifica los dispositivos conectados y los configura
 - Facilmente ampliable
 - Pueden conectarse tipos muy distintos de dispositivos
 - Síncronos/asíncronos
 - Diferentes velocidades de transferencia
 - Se reduce el número de puertos necesarios
 - Hasta 127 dispositivos pueden conectarse en un mismo puerto
 - El propio puerto puede proporcionar alimentación a los dispositivos

Fuente:

Oliverio J. Santana Jaria
Universidad de Las Palmas de G.C.



@CONPilarZgz



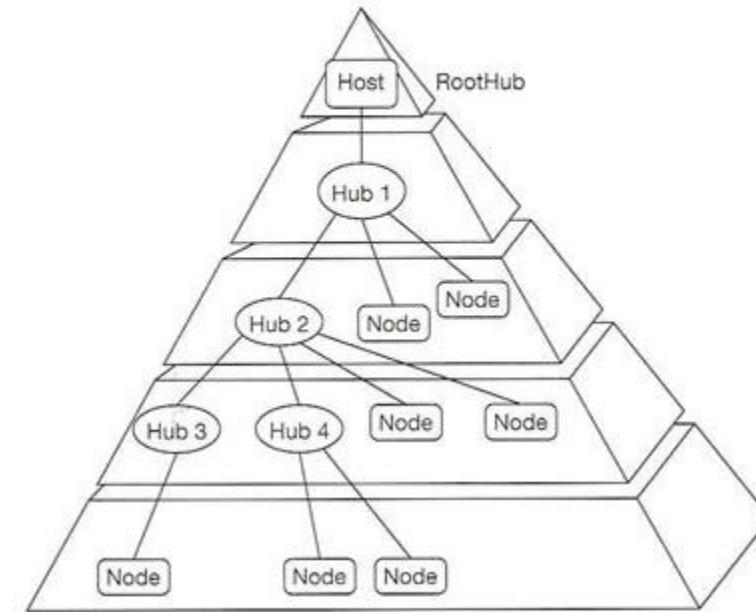
www.conpilar.es

@HackAndBeers



**HACK
& BEERS**

- El bus USB tiene una estructura estratificada con forma de árbol
 - La conexión de los dispositivos sigue un esquema encadenado (*hardware polling*)
 - La gestión del bus es centralizada y se realiza desde el controlador integrado en el computador (*host*)
 - Cada dispositivo USB tiene su propia dirección en el sistema
 - El controlador inicia todas las actividades y se comunica con el computador por medio de interrupciones
 - Ningún dispositivo USB puede iniciar una transacción por sí mismo para evitar sobrescribir datos presentes en el bus



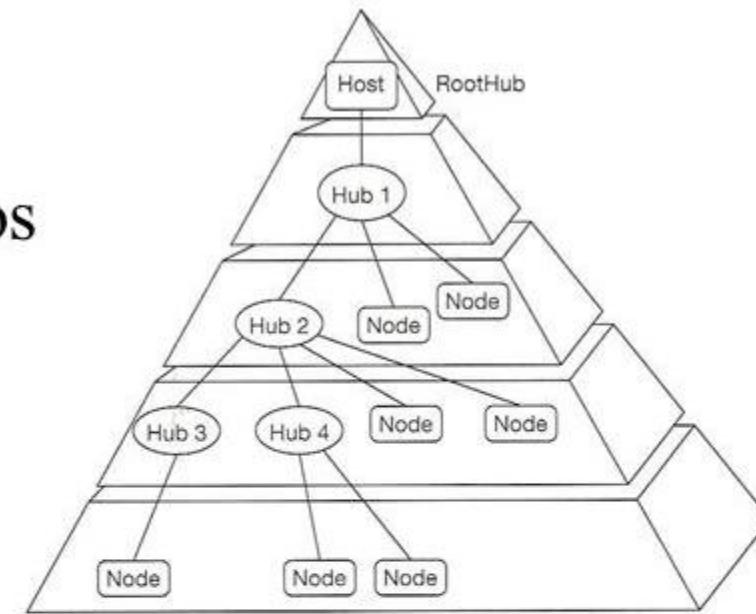
@CONPilarZgz



www.conpilar.es

@HackAndBeers

- El host también actúa como un distribuidor (*hub*) que permite la conexión de varios dispositivos USB (nodos)
 - Se reduce el número de conexiones necesarias
 - Se reduce la cantidad de recursos del computador ocupados (canales E/S, canales DMA, interrupciones...)
- Se pueden añadir hubs adicionales para ampliar la estructura del sistema y permitir la conexión de un mayor número de dispositivos (hasta 127)



@CONPilarZgz

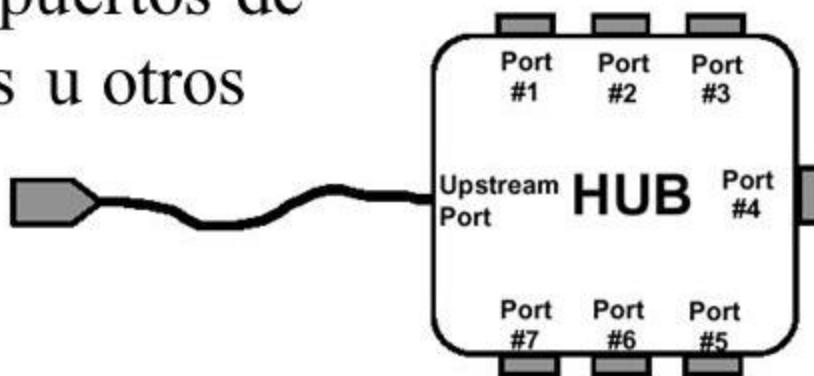
@HackAndBeers



www.conpilar.es

- La principal funcionalidad de un hub es extender el sistema proporcionando nuevos puertos de conexión

- Cada hub proporciona un puerto de conexión con el host (*upstream*) y varios puertos de conexión con dispositivos u otros hubs (*downstream*)



- Al igual que cualquier otro dispositivo USB, un hub debe ser configurado, recibiendo su propia dirección



@CONPilarZgz

@HackAndBeers

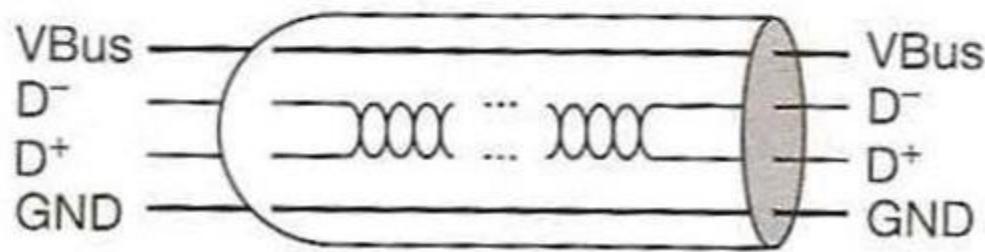


www.conpilar.es

#CONPilar®

**HACK
&BEERS**

- El cable USB contiene solo cuatro líneas
 - GND: tierra
 - VBus: alimentación (no es suficiente para algunos dispositivos)
 - D+ D-: líneas diferenciales de transmisión
- La longitud máxima del cable es de 5 metros y su ancho de banda máximo es 60 Mbytes (USB 2.0)



Pin 1	VBus	rojo
Pin 2	D-	blanco
Pin 3	D+	verde
Pin 4	GND	negro



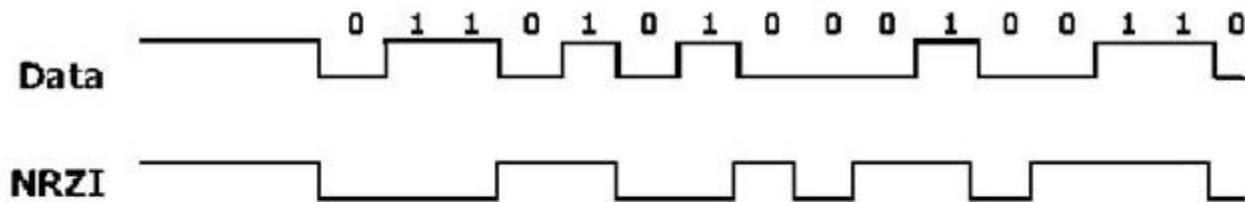
@CONPilarZgz



www.conpilar.es

@HackAndBeers

- Los datos se transmiten en serie por las líneas D+ D-
- No hay una señal de reloj
 - La sincronización se obtiene a partir de los propios datos utilizando condificación NRZI (*Non Return to Zero Inverted*)
 - Un uno se representa manteniendo el nivel de voltaje
 - Cada vez que aparece un cero se cambia la polaridad



- Si aparecen seis unos seguidos se inserta un cero (*bit-stuffing*) para forzar cambios de polaridad frecuentes y evitar, con ello, pérdidas de sincronización



@CONPilarZgz



www.conpilar.es

@HackAndBeers

- Las transferencias de datos se realizan estableciendo canales de comunicación virtuales (*pipes*)
 - Los canales son creados por el host
 - Cada canal ocupa parte del ancho de banda disponible

- Los canales terminan en un punto de final
 - Cada dispositivo puede soportar varios puntos de final y, por tanto, varios canales distintos
 - La prioridad de los dispositivos viene dada por la conexión en cadena



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
&BEERS**

- Cuando se conecta un dispositivo, el canal de control por defecto se establece con el punto de final 0
- Durante la inicialización, el host determina:
 - El formato de datos que soporta el dispositivo conectado
 - El tipo de dispositivo y la dirección de la transferencia
 - Los requerimientos de frecuencia y latencia de bus
 - El ancho de banda necesario
 - El tamaño máximo de los paquetes
- Finalizado este proceso, el host asigna una dirección al dispositivo



@CONPilarZgz

@HackAndBeers



www.conpilar.es

- Las transmisiones se dividen en tramas de tiempo (*frame*)
- Durante las tramas se producen transacciones compuestas por paquetes
 - Existen tres tipos de paquetes:
 - Inicialización (*token*)
 - Datos (*data*)
 - Protocolo (*handshake*)
 - Cada paquete comienza con un campo de sincronización (SYNC) que maximiza el número de transiciones en la línea
 - El tipo de paquete se diferencia con un identificador (*PID*)

Token:

PID								8 bit	3 bit	5 bit
0	1	x	x	1	0	x	x	ADDR	ENDP	CRC5

Data:

PID								0- n bit	16 bit
0	0	x	x	1	1	x	x	DATA	CRC16

Handshake:

PID							
1	0	x	x	0	1	x	x

PID	Meaning	PID (Hex)	Type
STALL	Error	0x1e	Handshake packet
SETUP	Initialization	0x2d	Token packet
PRE	Preamble	x	Special packet, only for low-speed devices
DATA1	Data packet 1	0x4b	Data packet
NACK	Not Acknowledge	0x5a	Handshake packet
IN	Receive	x	Token packet
SOF	Start of Frame	0x5a	Token packet
DATA0	Data packet 0	0xc3	Data packet
ACK	Acknowledge	0xd2	Handshake packet
OUT	Send	0x1e	Token packet



- Podemos distinguir dos tipos distintos de canales
- Los canales de mensaje tienen un formato concreto
 - El esquema que siguen es: Petición – Dato – Estado
 - Cada petición debe ser completamente resuelta antes de pasar a la siguiente
 - Implican un movimiento de datos bidireccional
- Los canales de flujo (*stream*) no tienen un formato
 - Los datos se envían de forma secuencial
 - El movimiento de datos es unidireccional



@CONPilarZgz



www.conpilar.es

@HackAndBeers

- Se definen 4 tipos posibles de transferencias
- Control (canal mensaje): utilizadas para configurar los dispositivos que se conectan
 - Se garantiza la correcta emisión/recepción de datos
 - No se garantiza la latencia o el ancho de banda
- Masivas (canal flujo): transferencias esporádicas de grandes cantidades de datos que pueden esperar (impresoras, escáneres...)
 - Se garantiza la correcta emisión/recepción de datos
 - No se garantiza la latencia o el ancho de banda



@CONPilarZgz



www.conpilar.es

@HackAndBeers

- Por interrupciones (canal flujo): transferencias esporádicas de pocos datos que requieren atención inmediata (teclado, ratón...)
 - Se garantiza la correcta emisión/recepción de datos
 - Se garantiza la latencia y el ancho de banda
- Alta velocidad (canal flujo): grandes cantidades de información que se transmiten de forma continua (audio/video en tiempo real...)
 - No se garantiza la correcta emisión/recepción de datos
 - Se garantiza una latencia y un ancho de banda constante



@CONPilarZgz



www.conpilar.es

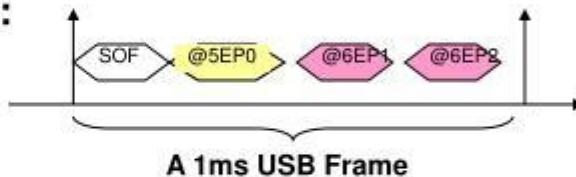
@HackAndBeers



USB transfer

- A device has several endpoints
- Each endpoint is assigned to a logical pipe with the host
- Each pipe is characterized by:
 - Device address
 - Endpoint number
 - Transfer type
- Transfer type:

Type	Direction	Packets per frame	Max Packet Size
Control	Bidir	Several	64 Bytes
Bulk	Unidir	Several	64 Bytes
Isochronous	Unidir	One	1024 Bytes
Interrupt	Unidir	One max	64 Bytes



- Control: configuration/command/status type communication
- Bulk: large amounts of data at highly variable times
- Isochronous: constant-rate, error tolerant transfers
- Interrupt: send or receive data infrequently but with bounded service periods

6



@CONPilarZgz



www.conpilar.es

@HackAndBeers

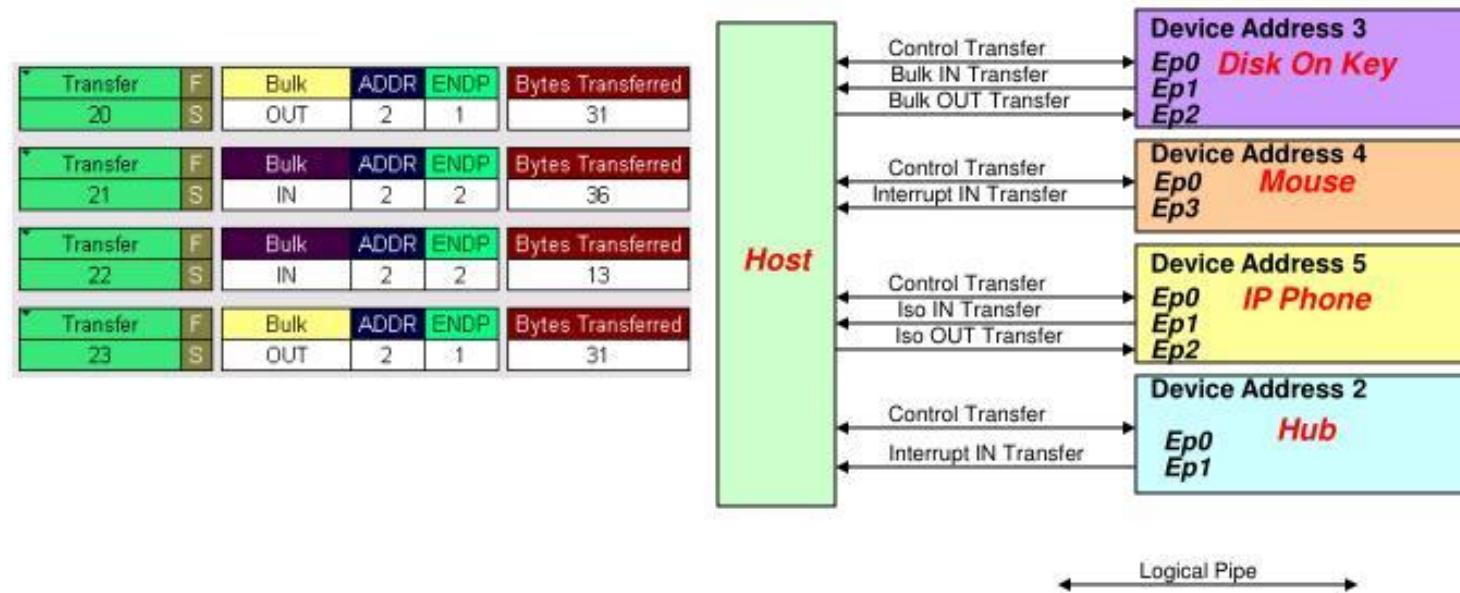
#CONPilar®

**HACK
& BEERS**



USB pipes

- Device address is affected by the host
- Endpoint configuration depends on the device implementation
- Time multiplexing of transfer is under host control





USB transactions

- A transfer is composed of one or several transactions
- Example of control transfer (several transactions)

Transfer	F	Control	ADDR	ENDP	bRequest	wValue	wIndex	Data	Time Stamp
19	S	GET	2	0	0xFE	0x0000	0x0000	1 byte	00003.6908 7345
		Transaction	F	SETUP	ADDR	ENDP	T	D	Time Stamp
		67	S	0xB4	2	0	0	D->H C I 0xFE 0x0000 0x0000 1 0x4B	24.417 µs 00003.6908 7345
		Transaction	F	IN	ADDR	ENDP	T	Data	Time Stamp
		68	S	0x96	2	0	I	1 byte 0x4B	20.417 µs 00003.6909 1310
		Transaction	F	OUT	ADDR	ENDP	T	Data	Time Stamp
		69	S	0x87	2	0	I	0 bytes 0x4B	234.250 µs 00003.6909 2535

Setup Stage
Data Stage
Status Stage

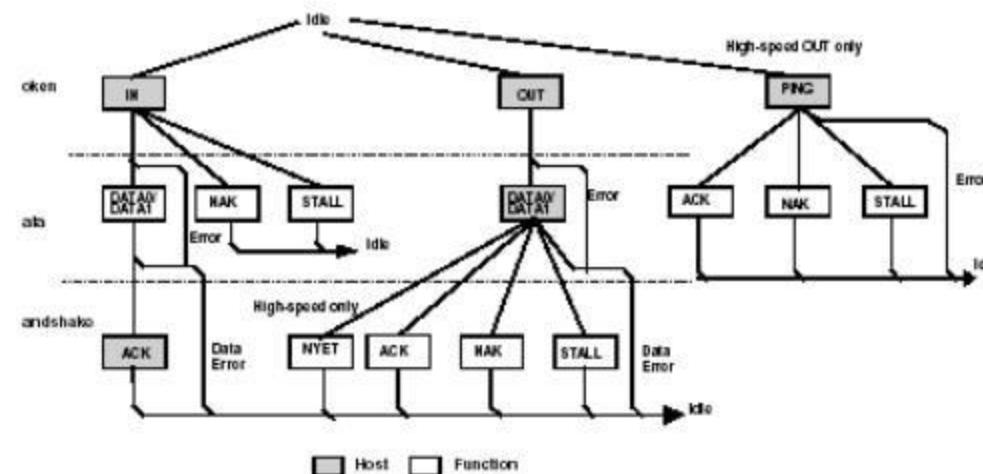
- Example of bulk transfer (one transaction)

Transfer	F	Bulk	ADDR	ENDP	Bytes Transferred	Time Stamp					
20	S	OUT	2	1	31	00003.6911 1590					
		Transaction	F	OUT	ADDR	ENDP	T	Data	ACK	Time	Time Stamp
		70	S	0x87	2	1	O	31 bytes 0x4B		192.083 µs	00003.6911 1590



USB Transactions (1)

- A transaction is made of 3 packets
 - Token: device address, endpoint number, transfer type
 - Data : data to be sent
 - Handshake: acknowledge
- Example of bulk transaction:



10



@CONPilarZgz

@HackAndBeers



www.conpilar.es

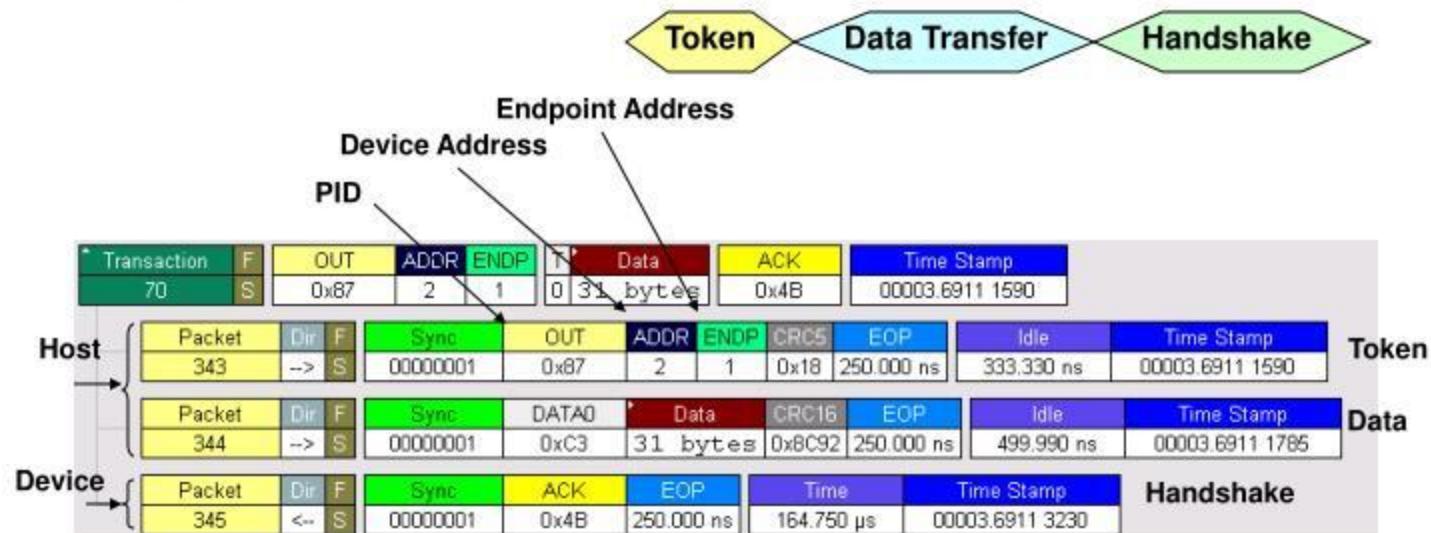
#C0NPIlarr®

**HACK
&BEERS**



USB Transactions (2)

- Example of bulk OUT transaction:



11



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

HACK
&BEERS



Control transfer

Transfer	F	Control	ADDR	ENDP	bRequest	wValue	wIndex	Descriptors	Time Stamp		
2	S	GET	2	0	GET_DESCRIPTOR	DEVICE type	0x0000	DEVICE descriptor	00003.6507 1660		
Transaction	F	SETUP	ADDR	ENDP	T D Tp R	bRequest	wValue	wIndex	wLength	ACK	Time Stamp
6	S	0xB4	2	0	0 D>H S D	GET_DESCRIPTOR	DEVICE type	0x0000	18	0x4B	00003.6507 1660
		Packet	Dir F	Sync	SETUP	ADDR	ENDP	CRC5	EOP	Idle	Time Stamp
		111	-> S	00000001	0xB4	2	0	0x15	260.000 ns	333.330 ns	00003.6507 1660
		Packet	Dir F	Sync	DATA0	Data	CRC16	EOP	Idle	Time Stamp	
		112	-> S	00000001	0xC3	8 bytes	0x072F	216.660 ns	533.330 ns	00003.6507 1665	
		Packet	Dir F	Sync	ACK	EOP	Time	Time	Stamp	Time Stamp	
		113	<- S	00000001	0x4B	216.660 ns	10.667 µs	00003.6507 2380			
Transaction	F	IN	ADDR	ENDP	NAK						
7	S	0x96	2	0	0x5A						
		Packet	Dir F	Sync	IN	ADDR	ENDP	CRC5	EOP	Idle	Time Stamp
		114	-> S	00000001	0x96	2	0	0x15	216.660 ns	533.330 ns	00003.6507 3020
		Packet	Dir F	Sync	NAK	EOP	Time	Time	Stamp	Time Stamp	
		115	<- S	00000001	0x5A	216.660 ns	72.417 µs	00003.6507 3225			
Transaction	F	IN	ADDR	ENDP	T Data		ACK				
8	S	0x96	2	0	1 18 bytes		0x4B				
		Packet	Dir F	Sync	IN	ADDR	ENDP	CRC5	EOP	Idle	Time Stamp
		116	-> S	00000001	0x96	2	0	0x15	216.660 ns	533.330 ns	00003.6508 0070
		Packet	Dir F	Sync	DATA1	Data	CRC16	EOP	Idle	Time Stamp	
		118	<- S	00000001	0xD2	18 bytes	0x6BC9	216.660 ns	533.330 ns	00003.6508 0275	
		Packet	Dir F	Sync	ACK	EOP	Time	Time	Stamp	Time Stamp	
		119	-> S	00000001	0x4B	216.660 ns	9.750 µs	00003.6508 1200			
Transaction	F	OUT	ADDR	ENDP	T Data		ACK				
9	S	0x87	2	0	1 0 bytes		0x4B				

The device is not ready...
The device does not acknowledge the transaction

The host retries...
The device has Acknowledged the transaction

13



@CONPilarZgz



www.conpilar.es

@HackAndBeers

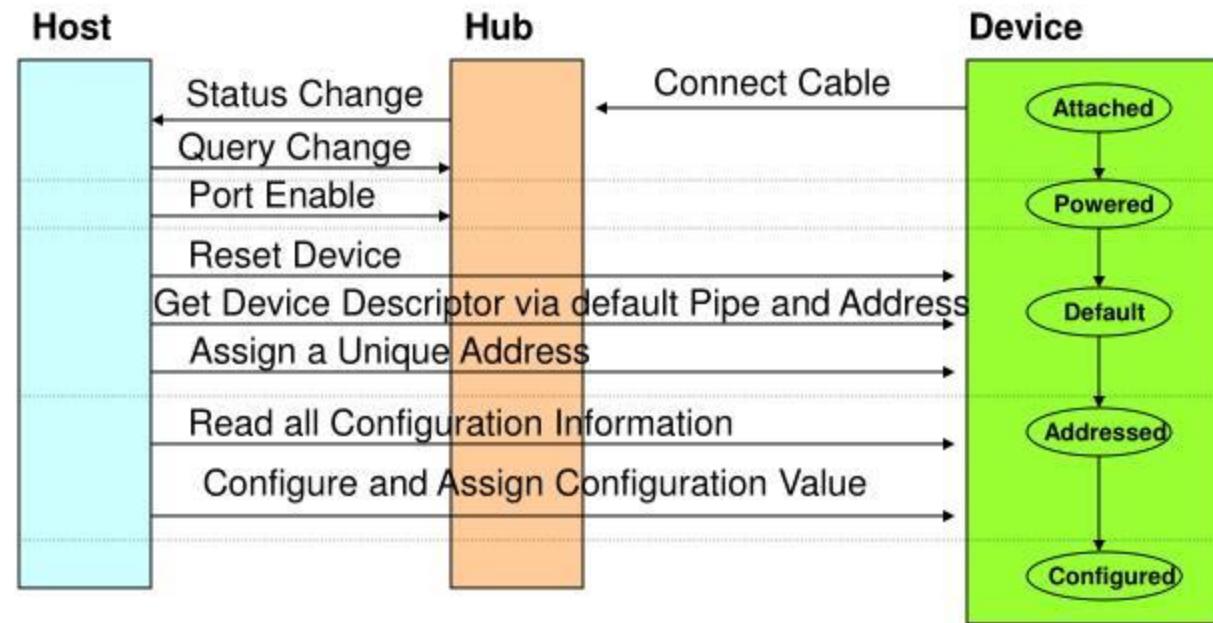
#CONPilar®

HACK & BEERS



Enumeration

- Enumeration is the Process of Assigning Addresses and Setting Configurations



18



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#C0NPIlarr®

**HACK
&BEERS**



Enumeration trace

Reset.				15.036 ms	Idle		1387	Default Address, default control endpoint			
Transfer	L	Control	ADDR ENDP	bRequest	wValue	Time		Enter Address State			
1	S	SET	0 0	SET_ADDRESS	New address 3	0.956 ms					
2	S	GET	3 0	GET_DESCRIPTOR	DEVICE type 0x0000	DEVICE descriptor	5.999 ms				
3	S	GET	3 0	GET_DESCRIPTOR	CONFIGURATION type 0x0000	CONFIGURATION descriptor	4.999 ms				
4	S	GET	3 0	GET_DESCRIPTOR	CONFIGURATION type 0x0000	4 descriptors	10.998 ms				
5	S	GET	3 0	GET_DESCRIPTOR	DEVICE type 0x0000	DEVICE descriptor	6.999 ms				
6	S	GET	3 0	GET_DESCRIPTOR	CONFIGURATION type 0x0000	CONFIGURATION descriptor	5.999 ms				
7	S	GET	3 0	GET_DESCRIPTOR	CONFIGURATION type 0x0000	4 descriptors	9.998 ms				
8	S	SET	3 0	SET_CONFIGURATION	New configuration 1	2.999 ms		Enter Configured State			
9	S	SET	3 0	0x0A	0x0000 0x0000	2.999 ms					
10	S	GET	3 0	GET_DESCRIPTOR	Descriptor type 0x22, Index 0	0x0000 HID Report descriptor	16.997 ms				
57	S	IN	ADDR ENDP	NAK	Time						
		0x96	3 1	0x5A	7.999 ms						

19



@CONPilarZgz

@HackAndBeers



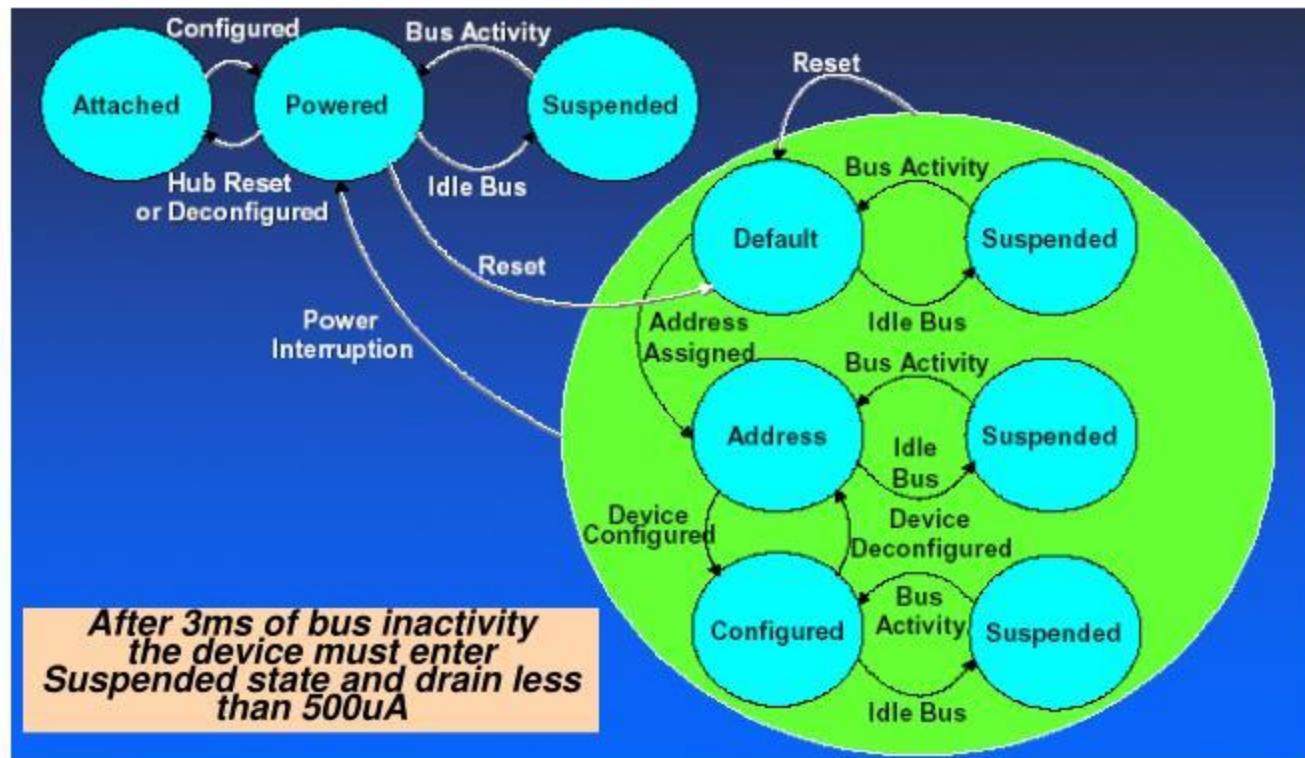
www.conpilar.es

#C0NPl1ar®

**HACK
&BEERS**



USB Device State



20



@CONPilarZgz



www.conpilar.es

@HackAndBeers



Host software architecture

Linux and WIN CE provide

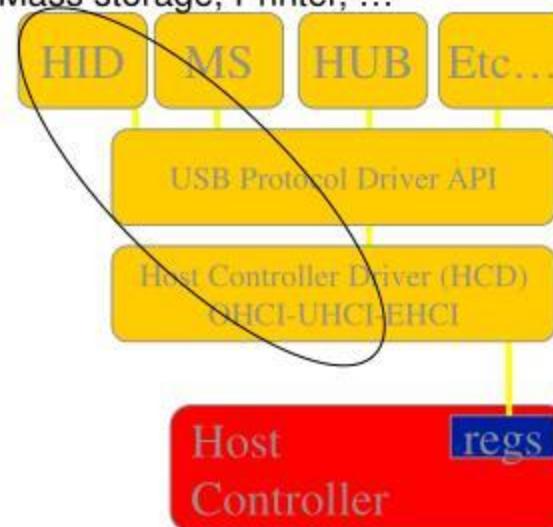
- ✓ OHCI/UHCI/EHCI HCD driver
- ✓ USBD Driver
- ✓ Main class drivers: Hub, HID, Mass storage, Printer, ...

**• Symbian and RTOS does not provide USB host stack driver
• SW IPs providers are able to provide solutions for RTOS**

- ✓ Softconnex, Philog, ...
- ✓ Expensive: (65k\$ for a mass storage solution)

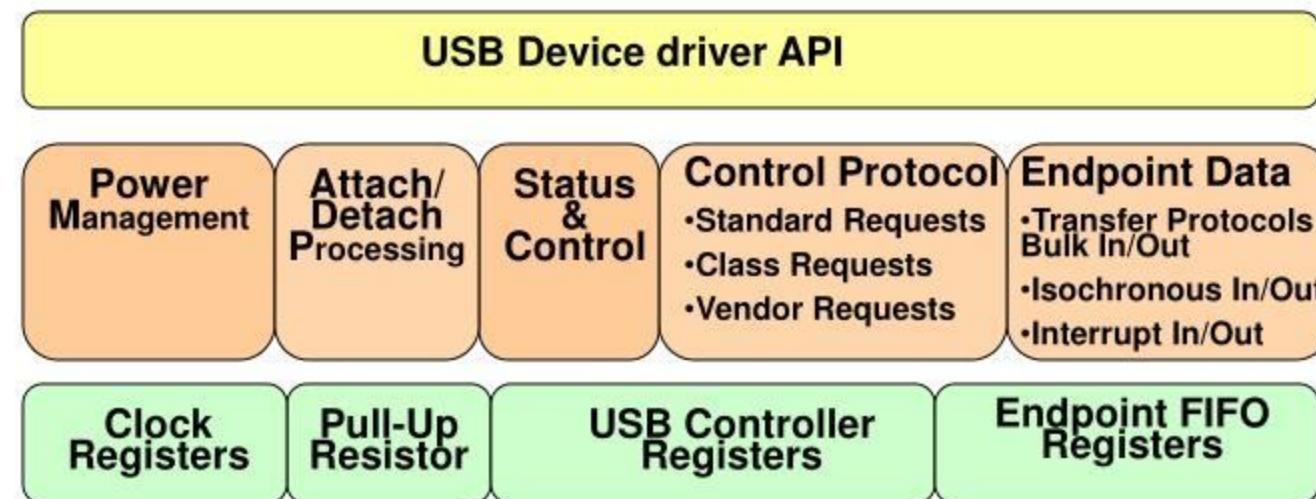
• It is still possible to build a mini host from our full host:

- ✓ the SW is only able to drive some kinds of devices





Device USB driver components



23



@CONPilarZgz

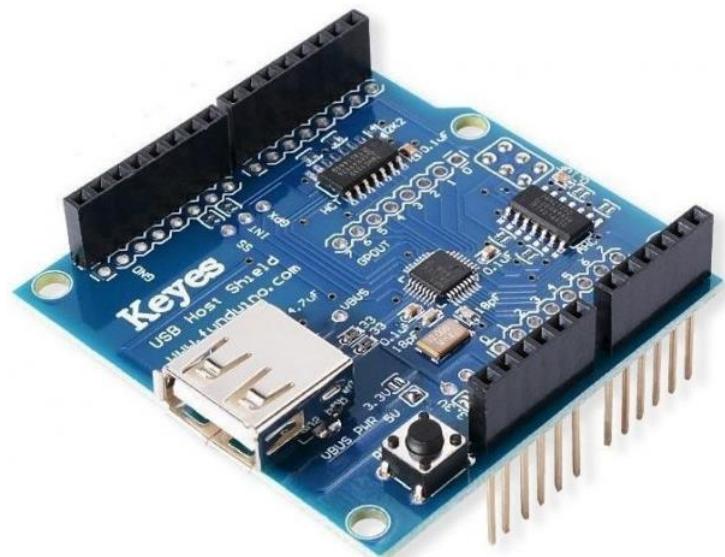
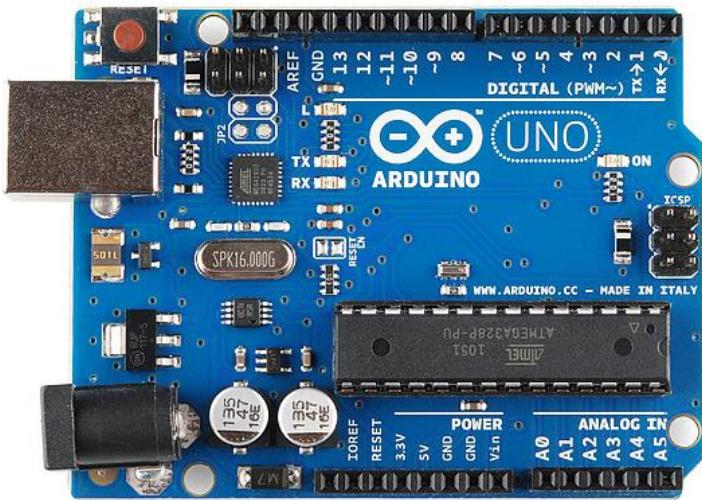
www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
& BEERS**

Arduino UNO



USB Host Shield

Relé Shield Arduino



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPilar®

**HACK
& BEERS**



Host usb Shield mini



ESP8266



Módulo relés SSD



@CONPilarZgz



www.conpilar.es

@HackAndBeers

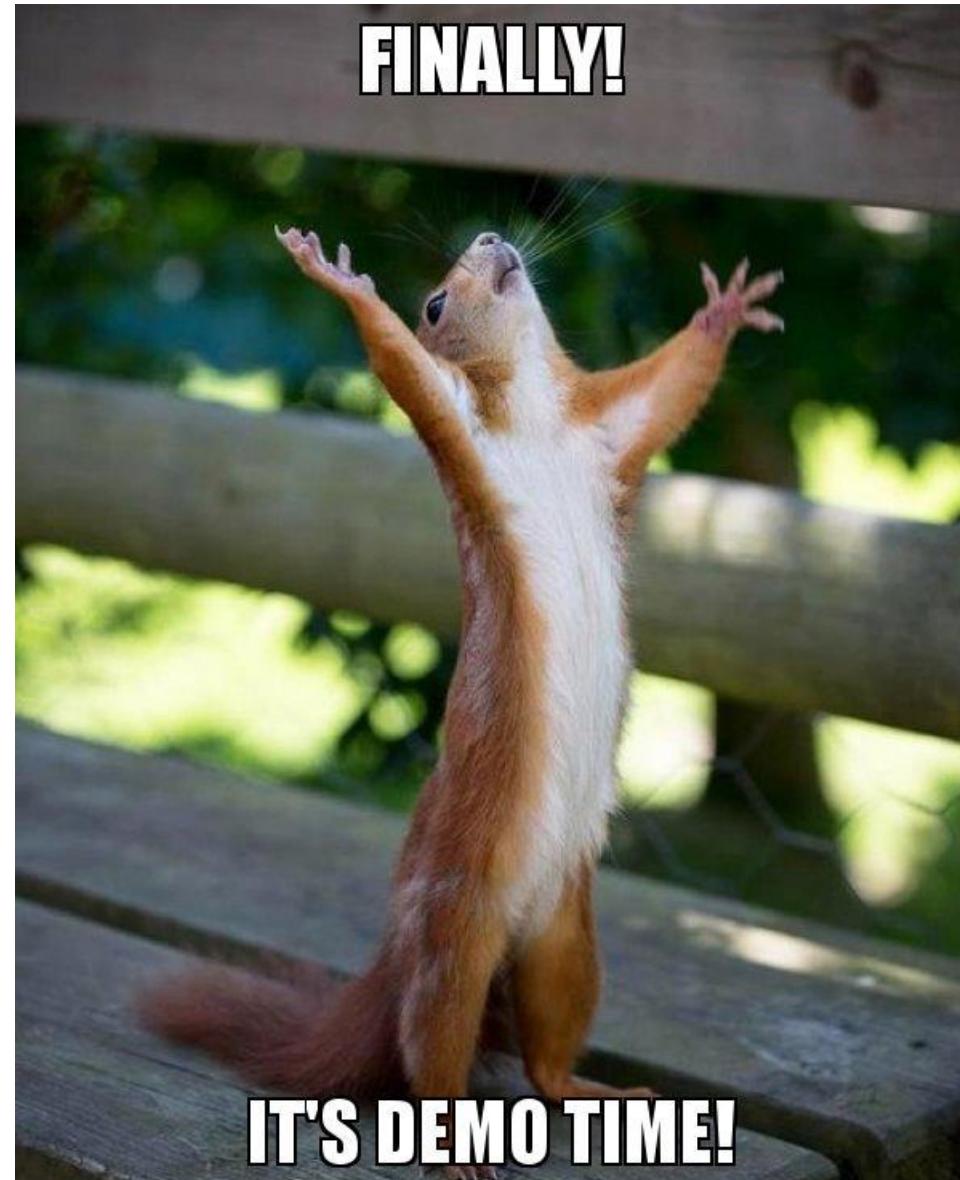
#CONPilar®

**HACK
&BEERS**

#CONPilar19

Let's tweet !!

#HBZaragoza19



@CONPilarZgz

@HackAndBeers



www.conpilar.es

#CONPilar®

**HACK
&BEERS**

Duck Hunt (jugando a cazar patos)

¡ ¡Muchas gracias!!



by #CONPilar[®]



SOPHOS



@CONPilarZgz



www.conpilar.es

@HackAndBeers

#CONPilar[®]

