

# BREAKING USB

## WITHOUT BREAKING THE BANK

A LITTLE BIT OF USB HACKING  
FOR A LITTLE BIT OF BUDGET



# THE “STATE OF THE ART”

Extremely useful tools...

## Beagle USB 480 Protocol Analyzer

Part Number: TP320510

Distribution: Physical Shipment

Availability: In-Stock

Price: \$1,200.00

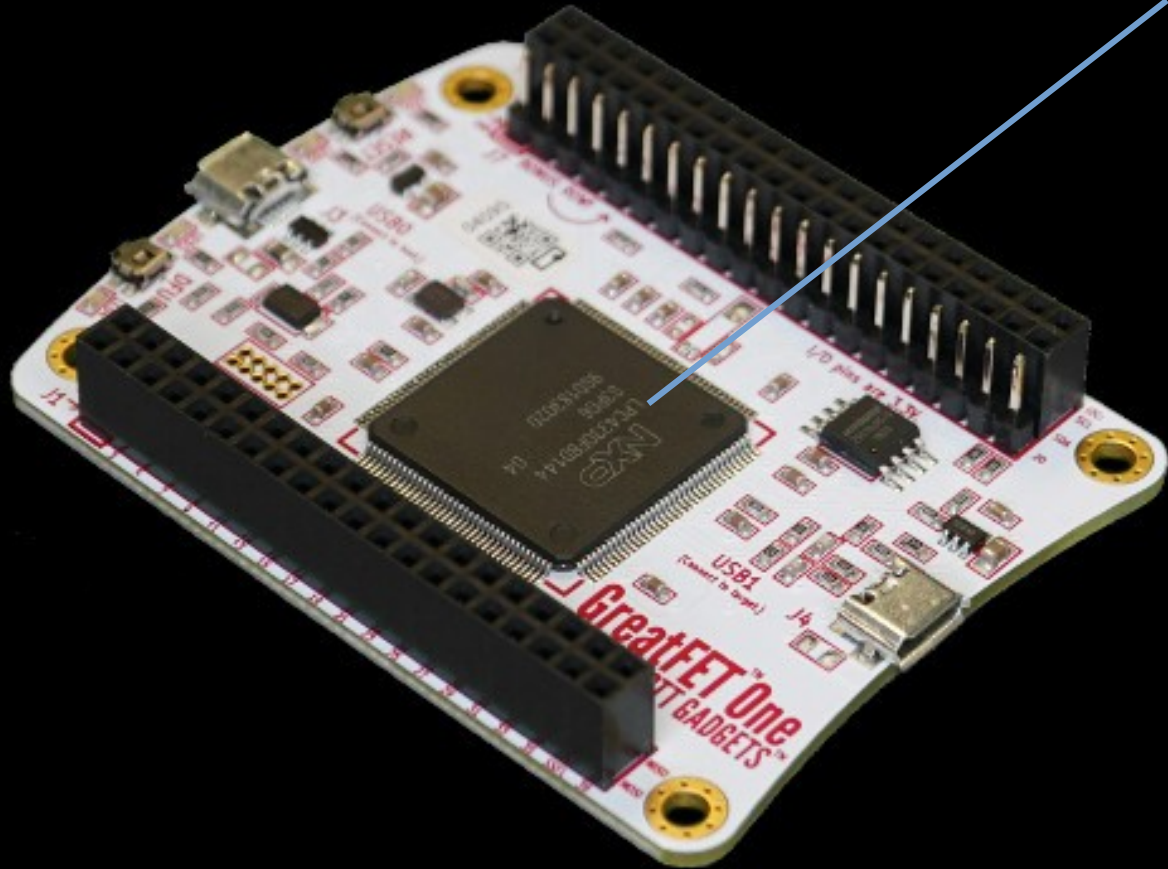
▶ Buy 5 for **\$1,100.00** each and **save 9%**

*Receive 15% off any cable and 20% off any board with purchase of select devices. Discount applied at checkout.*

...with extremely inaccessible price tags.



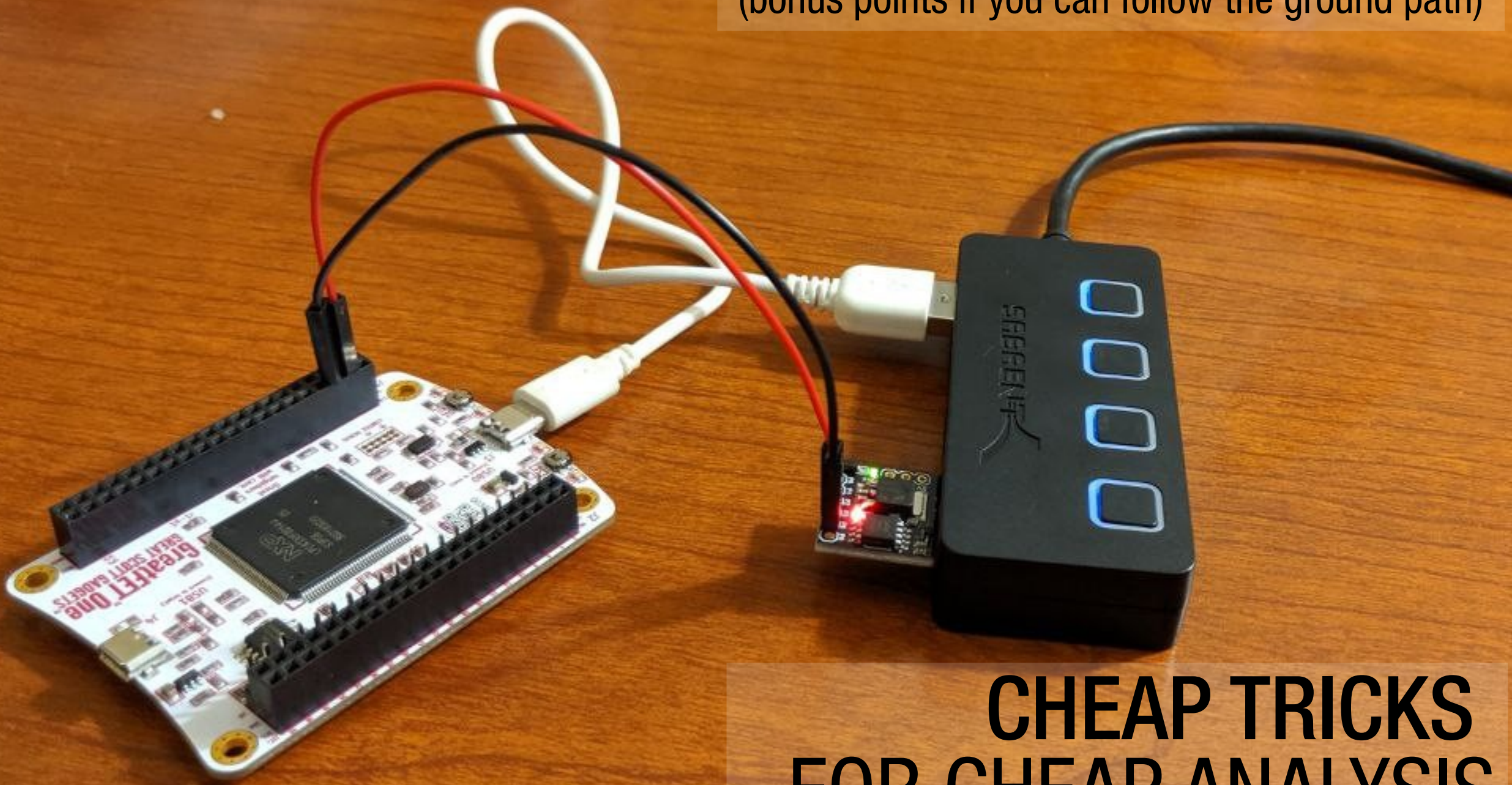
# WE CAN GO CHEAPER!



## GreatFET One (codename Azalea)

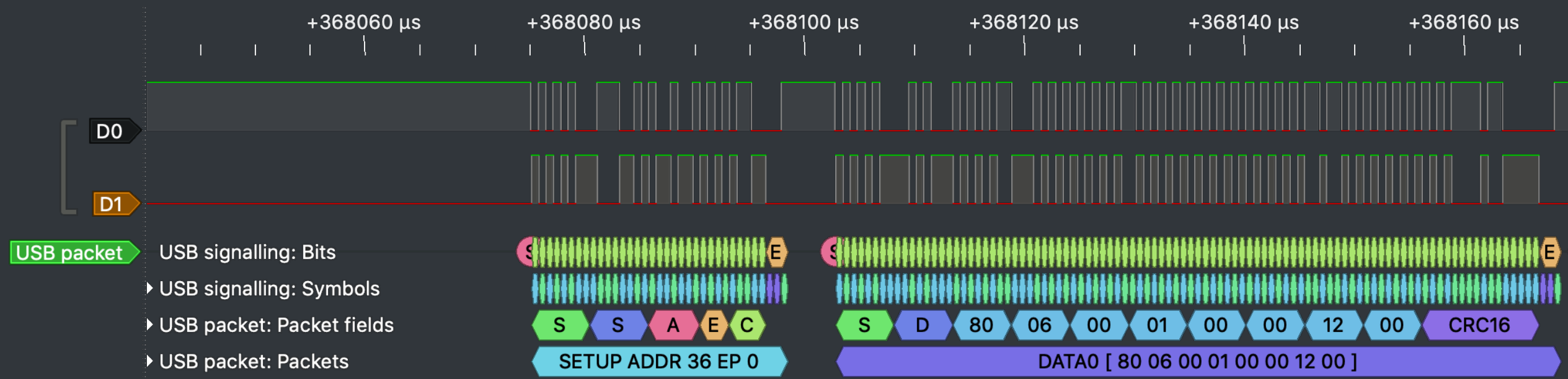
- Multi-tool for hardware hacking – including lots of USB functionality.
- USB LS / FS analysis built-in; will be able to do HS analysis with an inexpensive add-on.
- FaceDancer functionality! We'll see this in a bit.
- Build them yourselves! Design files at <https://github.com/greatfet-hardware>

(bonus points if you can follow the ground path)

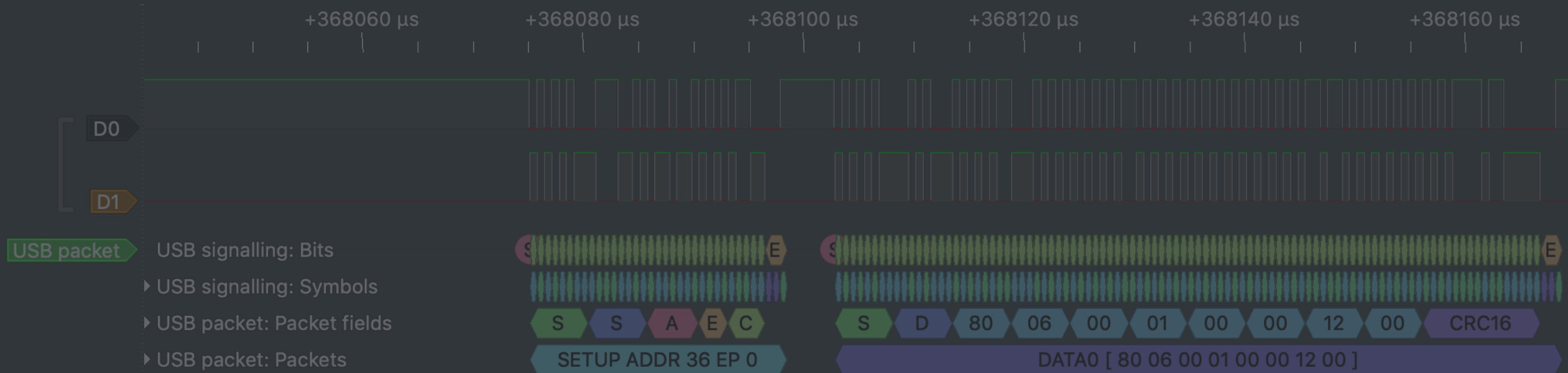


# CHEAP TRICKS FOR CHEAP ANALYSIS

# SIMPLE ANALYSIS WITH SIGROK



```
22] <, standard request to device (GET_DESCRIPTOR: value=DEVICE descriptor (index=0x00), index=0, length=18
22] <: b'\x12\x01\x00\x02\x00\x00\x00@\r\x0f\xc1\x00r\x05\x01\x02\x00\x01' [collapsed]
22] <, standard request to device (GET_DESCRIPTOR: value=CONFIGURATION descriptor (index=0x00), index=0, le
22] <: b'\t\x02)\x00\x01\x01\x00\x80\xfa' [collapsed]
22] <, standard request to device (GET_DESCRIPTOR: value=CONFIGURATION descriptor (index=0x00), index=0, le
22] <: b'\t\x02)\x00\x01\x01\x00\x80\xfa\t\x04\x00\x00\x02\x03\x00\x00\x00\t!\x11\x01\x00\x01"P\x00\x07\x05
22] >, standard request to device (SET_CONFIGURATION: value=1, index=0, length=0)
```



```

22] <, standard request to device (GET_DESCRIPTOR: value=DEVICE descriptor (index=0x00), index=0, length=18
22] <: b'\x12\x01\x00\x02\x00\x00\x00@\r\x0f\xc1\x00r\x05\x01\x02\x00\x01' [collapsed]
22] <, standard request to device (GET_DESCRIPTOR: value=CONFIGURATION descriptor (index=0x00), index=0, le
22] <: b'\t\x02)\x00\x01\x01\x00\x80\xfa' [collapsed]
22] <, standard request to device (GET_DESCRIPTOR: value=CONFIGURATION descriptor (index=0x00), index=0, le
22] <: b'\t\x02)\x00\x01\x01\x00\x80\xfa\t\x04\x00\x00\x02\x03\x00\x00\x00\t!\x11\x01\x00\x01"P\x00\x07\x05
22] >, standard request to device (SET_CONFIGURATION: value=1, index=0, length=0)

```

<https://www.github.com/usb-tools> (FaceDancer/USBProxy/prototype-ViewSB shown)

# COMPLEX ANALYSES WITH USB-TOOLS

# WE CAN STILL GO CHEAPER?



ModuleLive

1Pcs EZ-USB FX2LP CY7C68013A USB Core Board Development Board Logic Analyzer With I2C Serial SPI Interface

★★★★★ 5.0 (3 votes) | 8 orders

Price: ~~US \$3.51~~ / piece

Discount Price: **US \$3.16** / piece -10% 23h:22m:36s

Shipping: US \$0.64 to United States via SunYou Economic Air Mail

Estimated Delivery Time: 45 days

Quantity:  piece (9974 pieces available)

[Buy Now](#) [Add to Cart](#) ♥ 8

New User Coupon: **201,84 py6.** [GET IT NOW](#)



Comidox 1Set USB Logic Analyzer Channel UART IIC SPI Debug for A

by Comidox

★★★★☆ 4.0 (1 customer review)


Price: **\$6.99** ✓prime

- This item is an inexpensive logic analyzer designed to capture data from a USB device. It is not an official Saleae product. This item is also supported by Saleae.
- Sampling rate up to: 24 MHz, can be 24MHz, 16MHz, 100KHz, 50KHz, 25KHz.
- The logic for each channel sampling rate of 24M/s. On some occasions.
- A total of 8 digital channels, the voltage range is 0V to 5V. 0V is considered low, above 1.5V is considered high.
- UART, SPI, IIC and other communication debugging, can automatically analyze UART, IIC, SPI and many other protocols.

Specifications for this item

Brand Name	Comidox
EAN	0661083100000
Part Number	CP317
UPC	661083100000

Roll over image to zoom in



Condition: **New**

Quantity:  More than 10 available [22 sold / See feedback](#)

Was: ~~US \$4.30~~

You save: **\$0.22 (5% off)**

Price: **US \$4.08**

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

**eBay Money Back Guarantee**  
We'll make sure you get this item or get your money back. [Learn more](#)

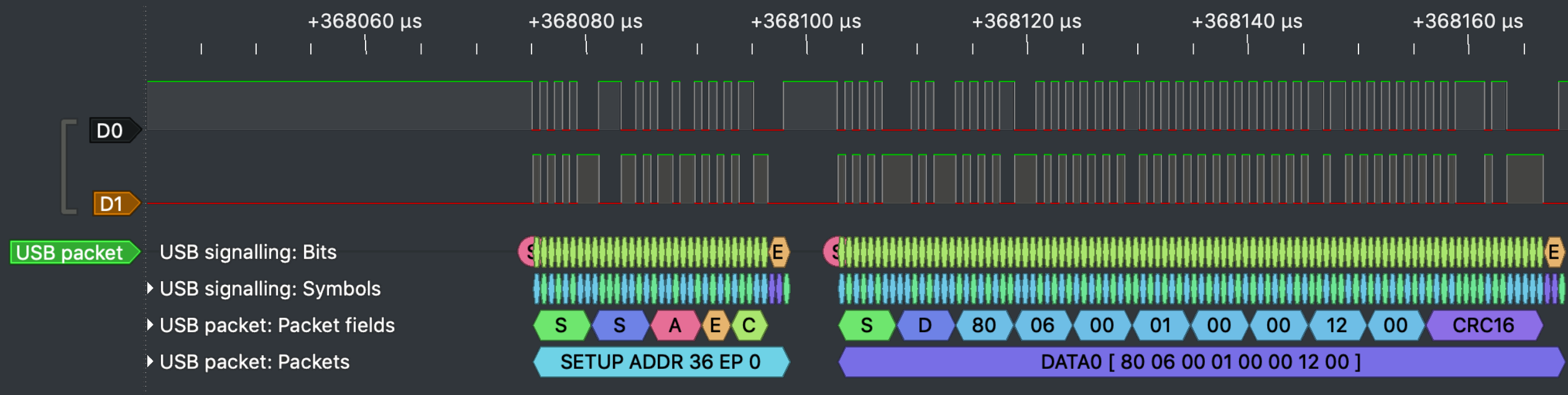
**100% buyer satisfaction** 22 sold Free shipping

**Bucks** You'll earn **\$0.04** in eBay Bucks. [See conditions](#)

Super-cheap FX2 “LA” boards are really freaking cheap, and can capture up to 24MHz via Sigrok.

That’s enough for LS/FS USB!

# ANALYSIS WITH SIGROK? **YEP**



ANALYSES WITH USB-TOOLS? **WELL, NOT YET**



**EVEN CHEAPER?!?**

# EVEN CHEAPER

It's easy to forget one of the **cheapest tools** we have for USB hacking:

# EVEN CHEAPER

It's easy to forget one of the **cheapest tools** we have for USB hacking:

~~our own imaginations~~  
**free software and the computer you already have\*!**

\*If you don't already have a computer, substitute a line here about the Raspberry Pi Zero, or similar. (Sorry for assuming.)

# SO:

**LET'S GET OUR ENVIRONMENTS SET UP,  
AND LET'S HACK SOME USB!**

instructions on the website: <https://mini.usbc.tf>