The hitchhacker’s guide to iPhone Lightning & JTAG hacking

by stacksmashing

About me: stacksmashing

- Security researcher

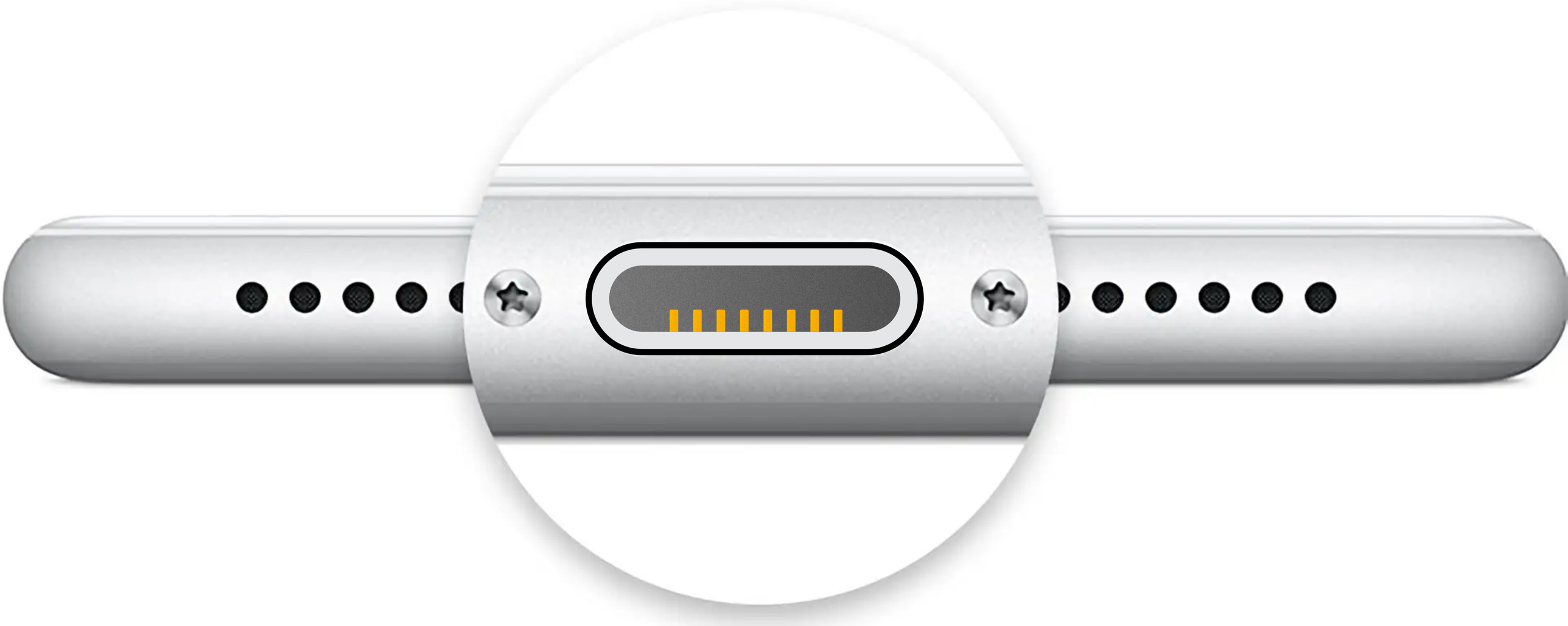
- youtube.com/stacksmashing
- @ghidraninja

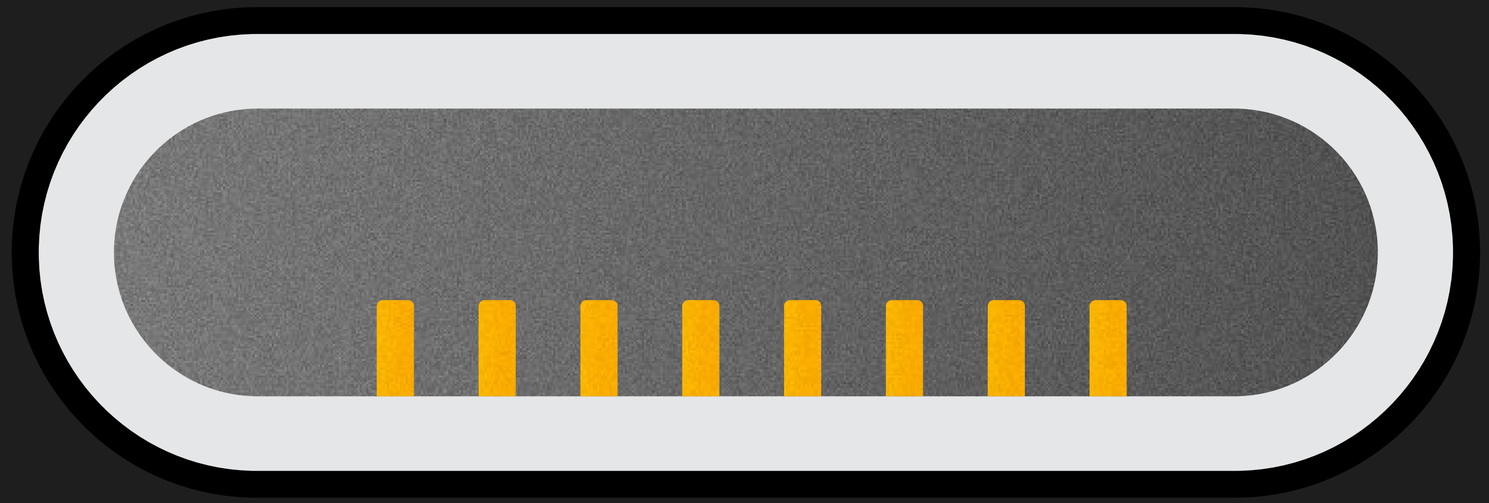
Thanks!

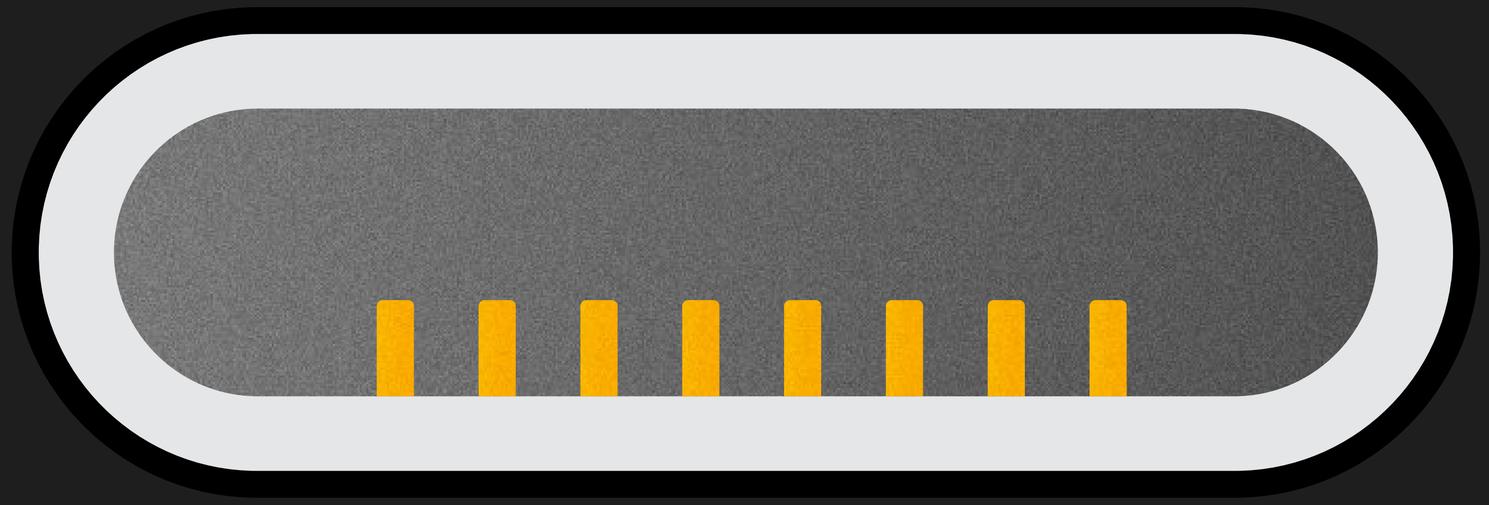
As always: Standing on the shoulders of giants

- Carlo Maragno - @CarloMara1
- Jiska Classen
- Fabian Freyer
- Caro Gross
- Lily - @bendycatus
- John - @nyan_satan
- LambdaConcept
- Elliot

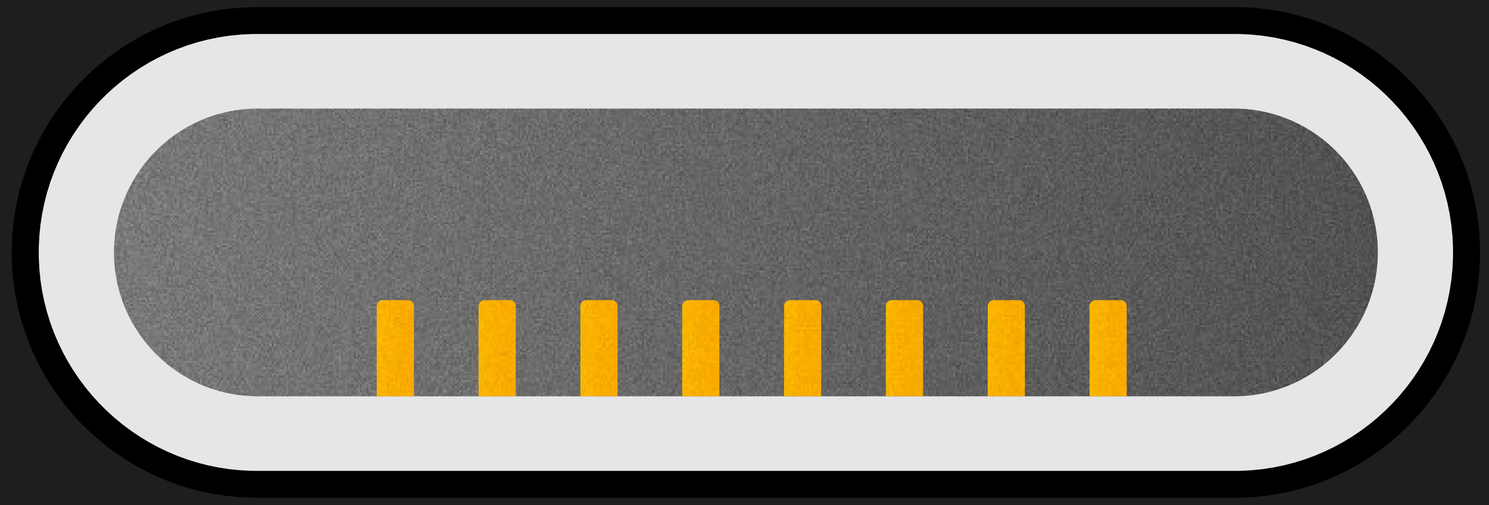
Lightning?





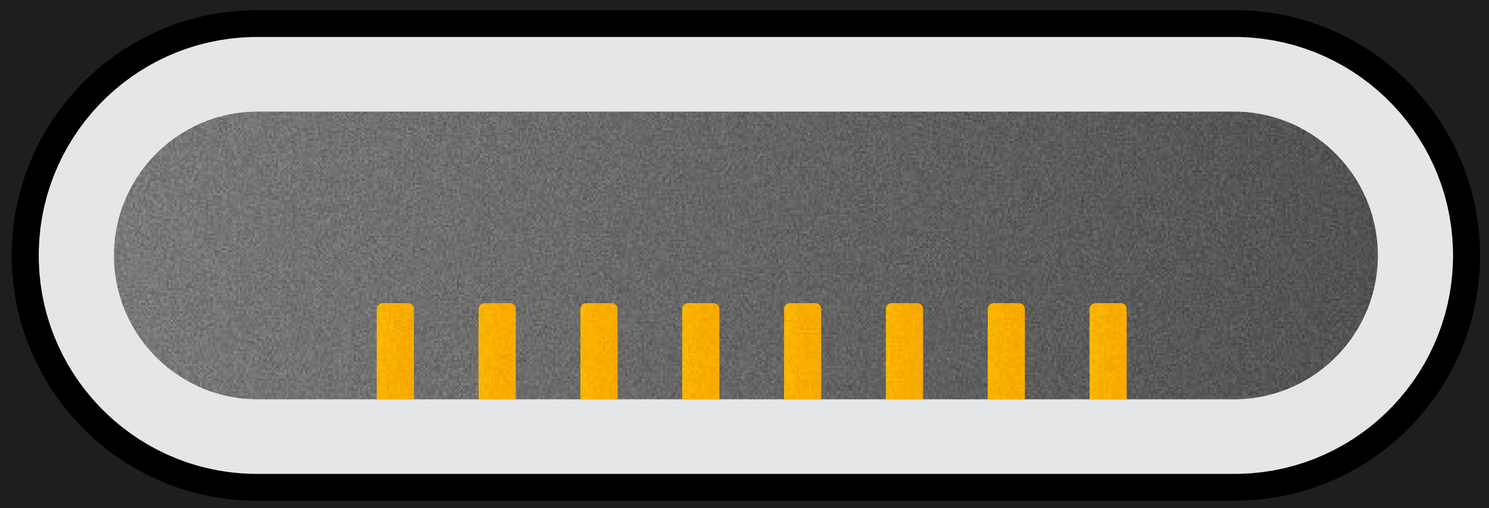


Charging



1 2 3 4 5 6 7 8

Charging

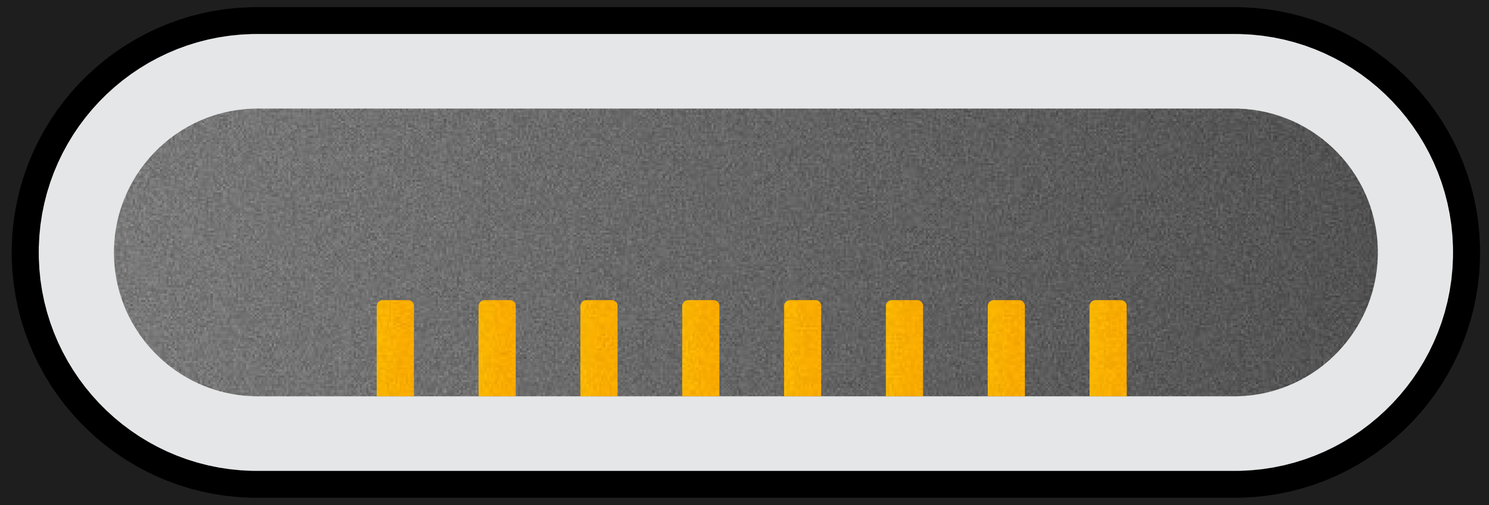


1 2 3 4 5 6 7 8

Data transfer

Audio

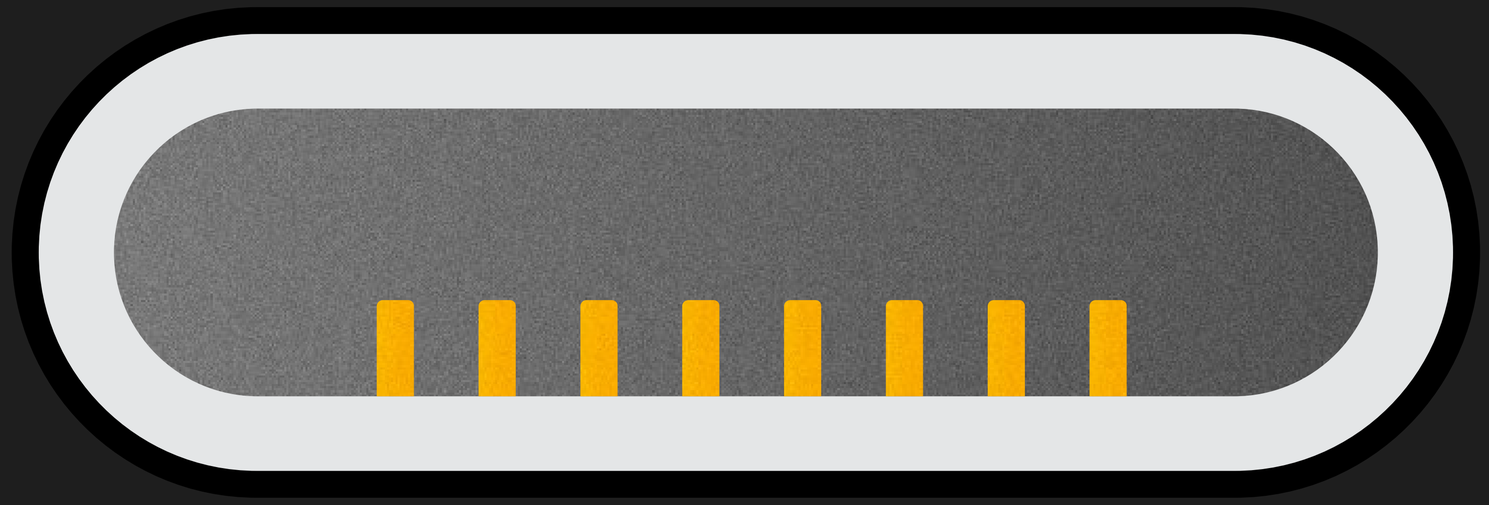
Charging



Data transfer

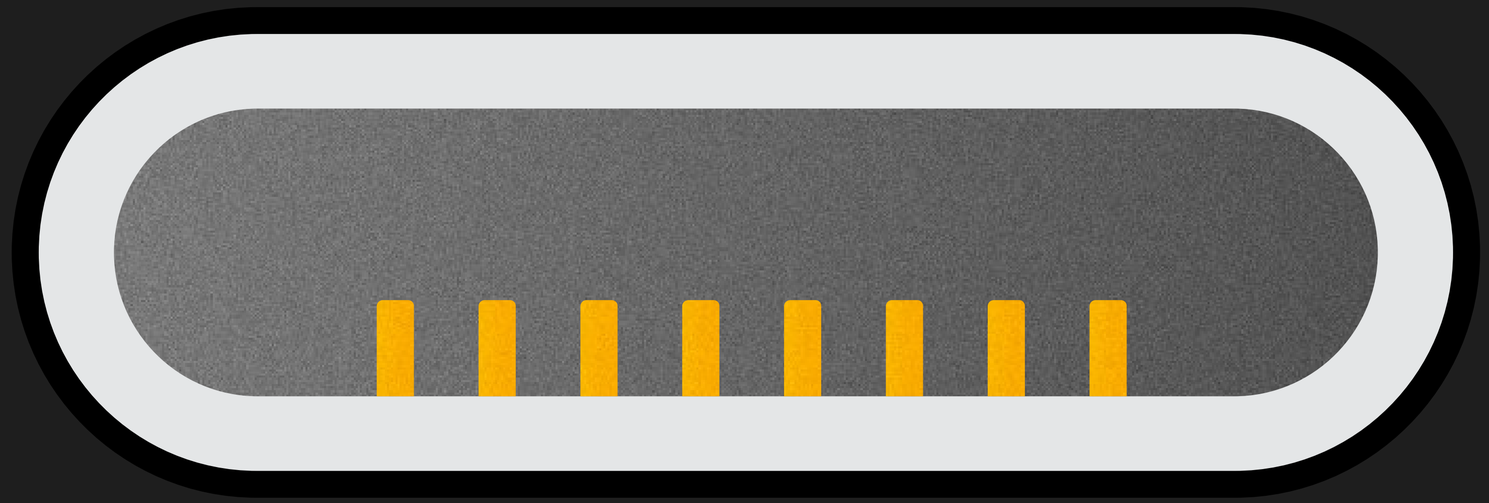
Audio

Charging



Data transfer

Video



Private

aliexpress.com

AliExpress

China PhoneFIX Tool... + Follow

95.5% Positive feedback 11798 Followers

I'm shopping for... On AliExpress In this store

0

Store Home Products Sale Items Top Selling New Arrivals Feedback

DCSD Cable for iPhone/iPad/iPod Engineering & Exploit DCSD USB Cable for WL 64Bit Mijing HDD Test Fixture Engineering Cable

4.0 1 Review 2 orders

US $17.99 - 30.29

US $3.00 off Orders over US $4.00 Get coupons

Color:

Number of Pieces:

1pcs

Quantity:

1 540 Pieces available

Ships to United States

Kanzi Cable

The **Kanzi Cable** is a JTAG/SWD Cable capable of debugging CPFM 00 or 01 devices (EVT and DVT devices) which have the Lightning port, using software called Astris. It can be connected to another SWD debugger, using the SWD port, and it can also do UART/Serial. They can be purchased from obscure markets. There are two known types of the Kanzi cable. The normal version and a prototype version with PROTO etched to it.

A Normal Kanzi Cable

Uses

Dumping the SecureROM

One use of the cable is dumping the SecureROM from devices. This can be done using commands such as this one.

This hardware article is a "stub", an incomplete page. Please add more content to this article and remove this tag.

Categories: Article stubs | Cables

Main page
Community portal
Current events
Recent changes
Random page
Help

Miscellaneous
Ground rules
Timeline

Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information

Private

shop.lambdaconcept.com

LambdaConcept

Search our catalog

Home / Bonobo JTAG/SWD Debug Cable

OUT-OF-STOCK

BONOBO JTAG/SWD DEBUG CABLE

€749.00

Tax excluded

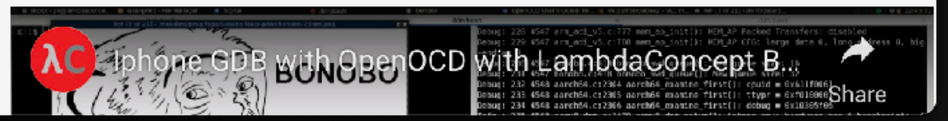
iPhone debugging requires proper tools.

The Bonobo cable connects to your target through Lightning and allows CPU debugging through JTAG/SWD using OpenOCD + AArch64 GDB. Among others, you can: access all CPUs and registers, single step, put hardware breakpoints, dump memory, etc... Perfect for security research.

The target serial console can be accessed on the control PC through Minicom (iBoot prompt), as well as Lightning USB (For DFU, USB exploitation, demote, etc.)

More Here

Demonstration:



Private

shop.lambdaconcept.com

LambdaConcept

Search our catalog

Home / Bonobo JTAG/SWD Debug Cable

OUT-OF-STOCK

BONOBO JTAG/SWD DEBUG CABLE

€749.00

Tax excluded

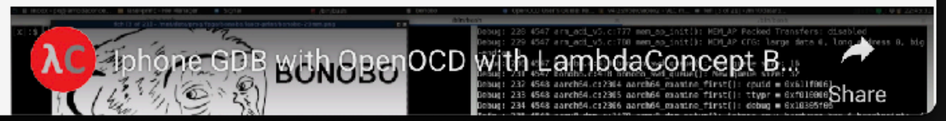
iPhone debugging requires proper tools.

The Bonobo cable connects to your target through Lightning and allows CPU debugging through JTAG/SWD using OpenOCD + AArch64 GDB. Among others, you can: access all CPUs and registers, single step, put hardware breakpoints, dump memory, etc... Perfect for security research.

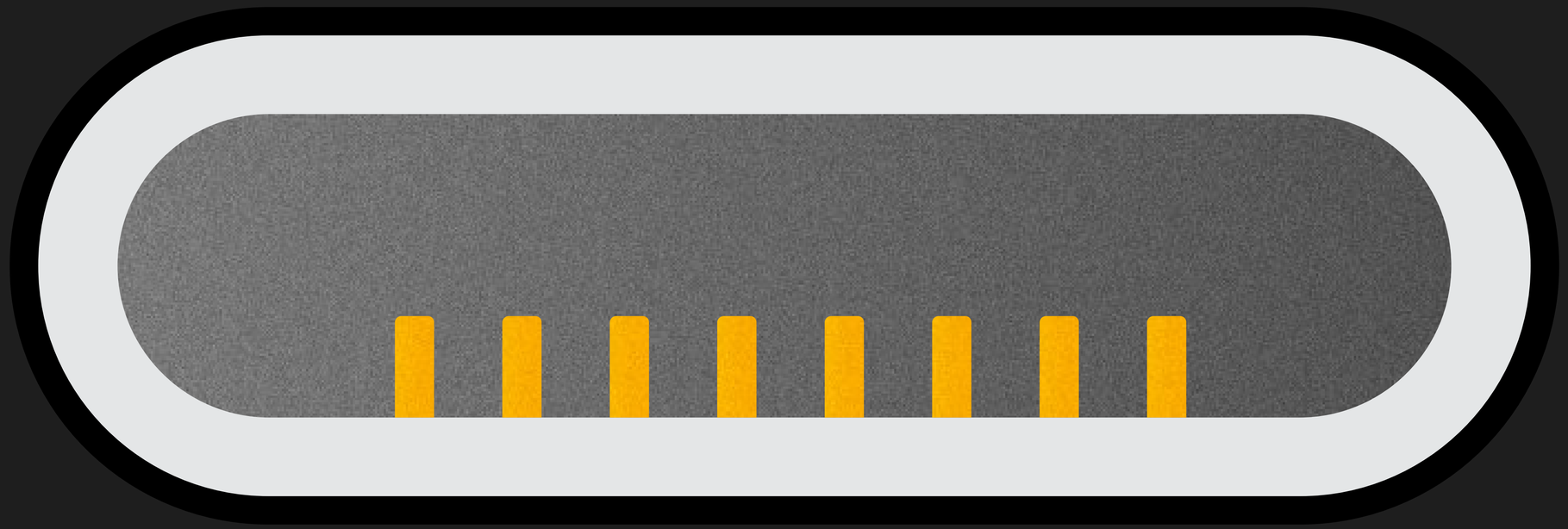
The target serial console can be accessed on the control PC through Minicom (iBoot prompt), as well as Lightning USB (For DFU, USB exploitation, demote, etc.)

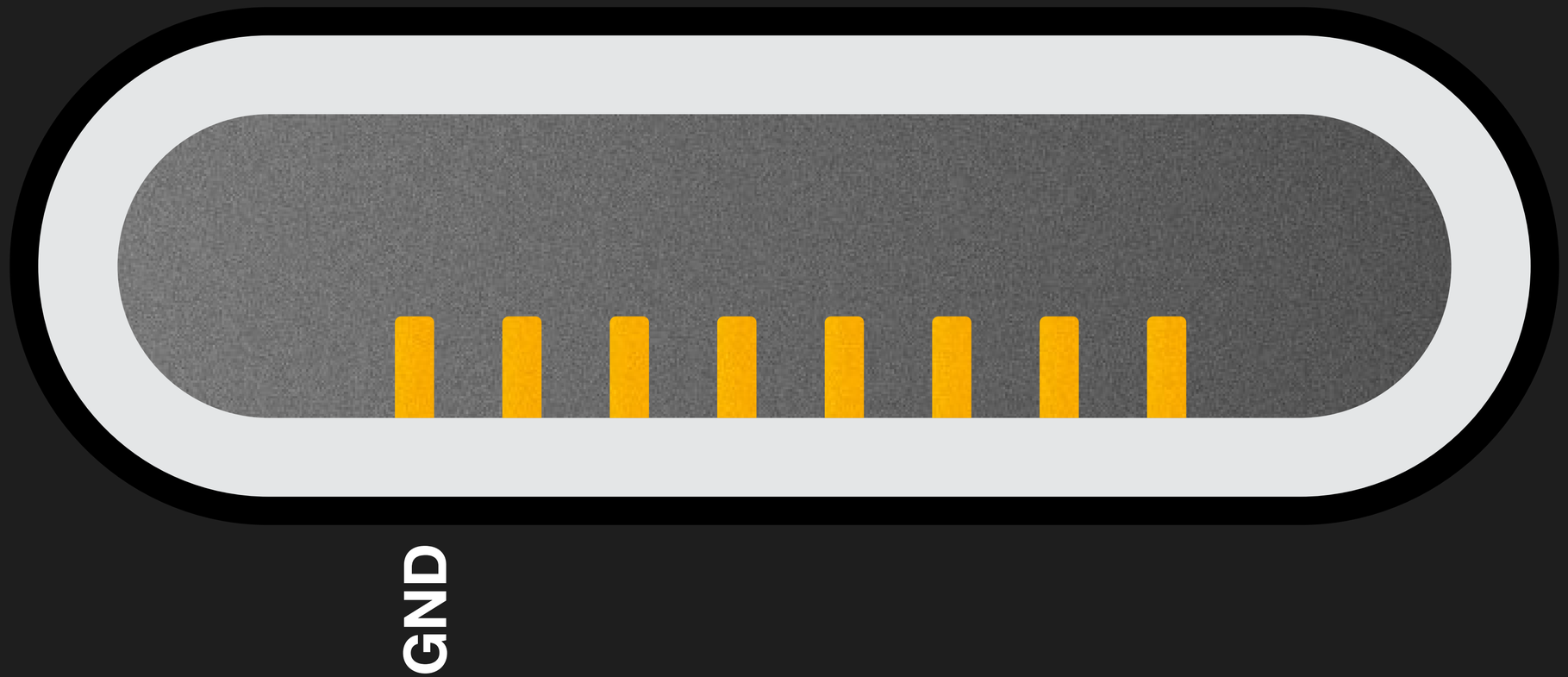
More Here

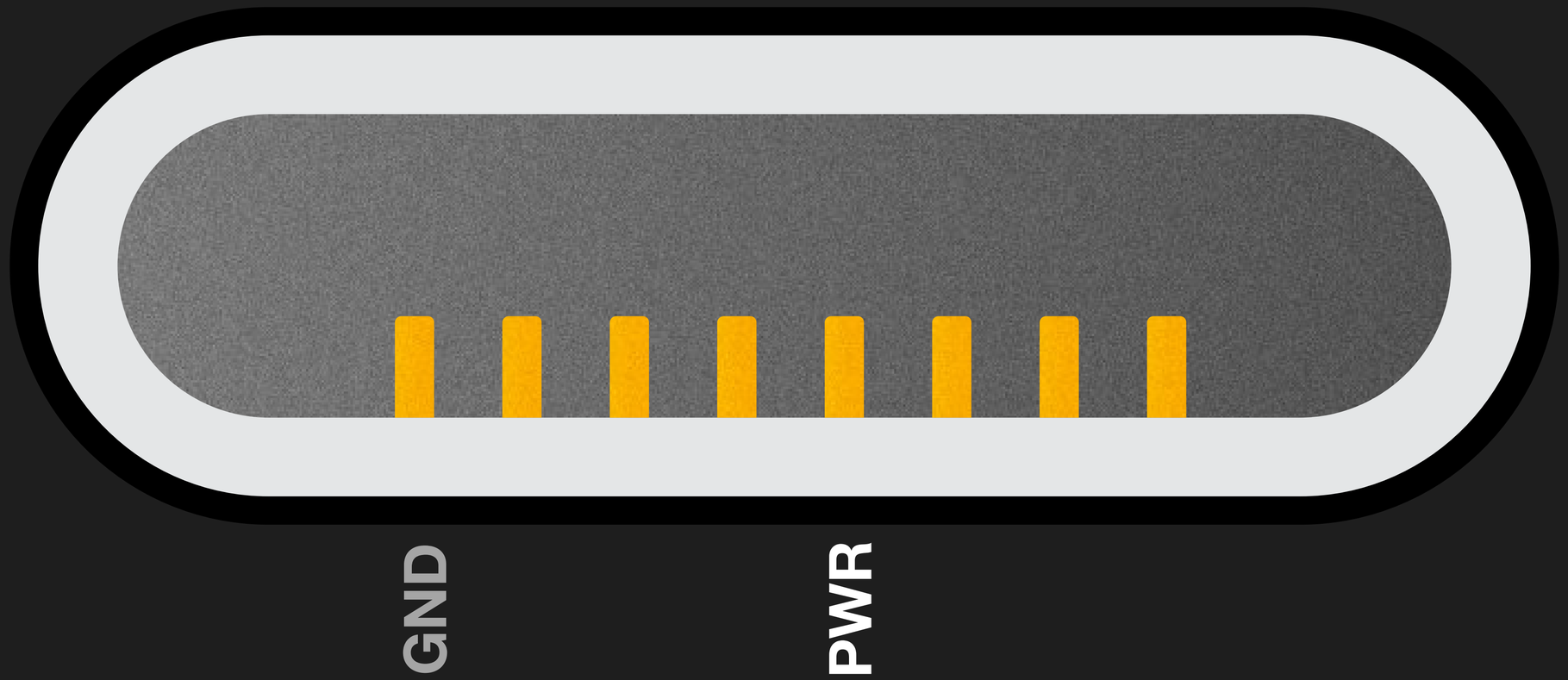
Demonstration:

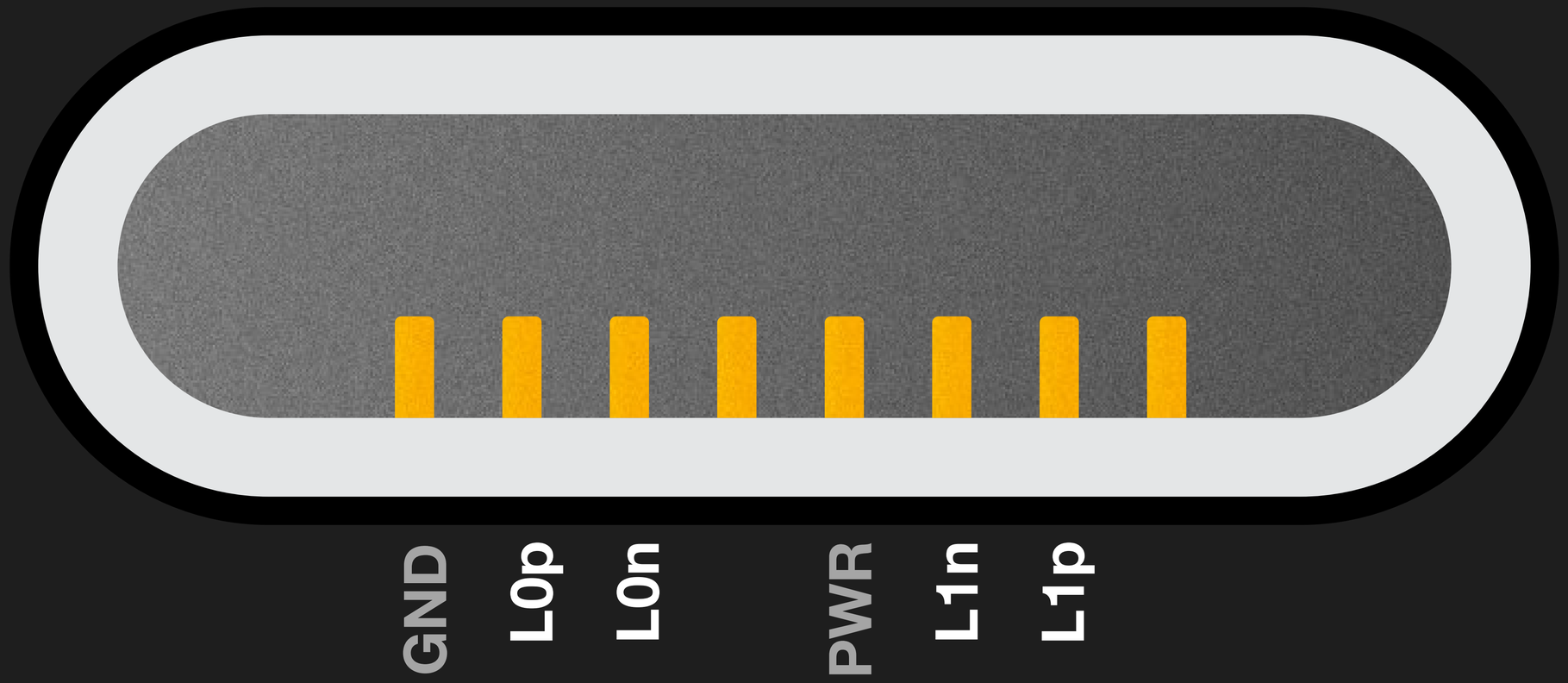


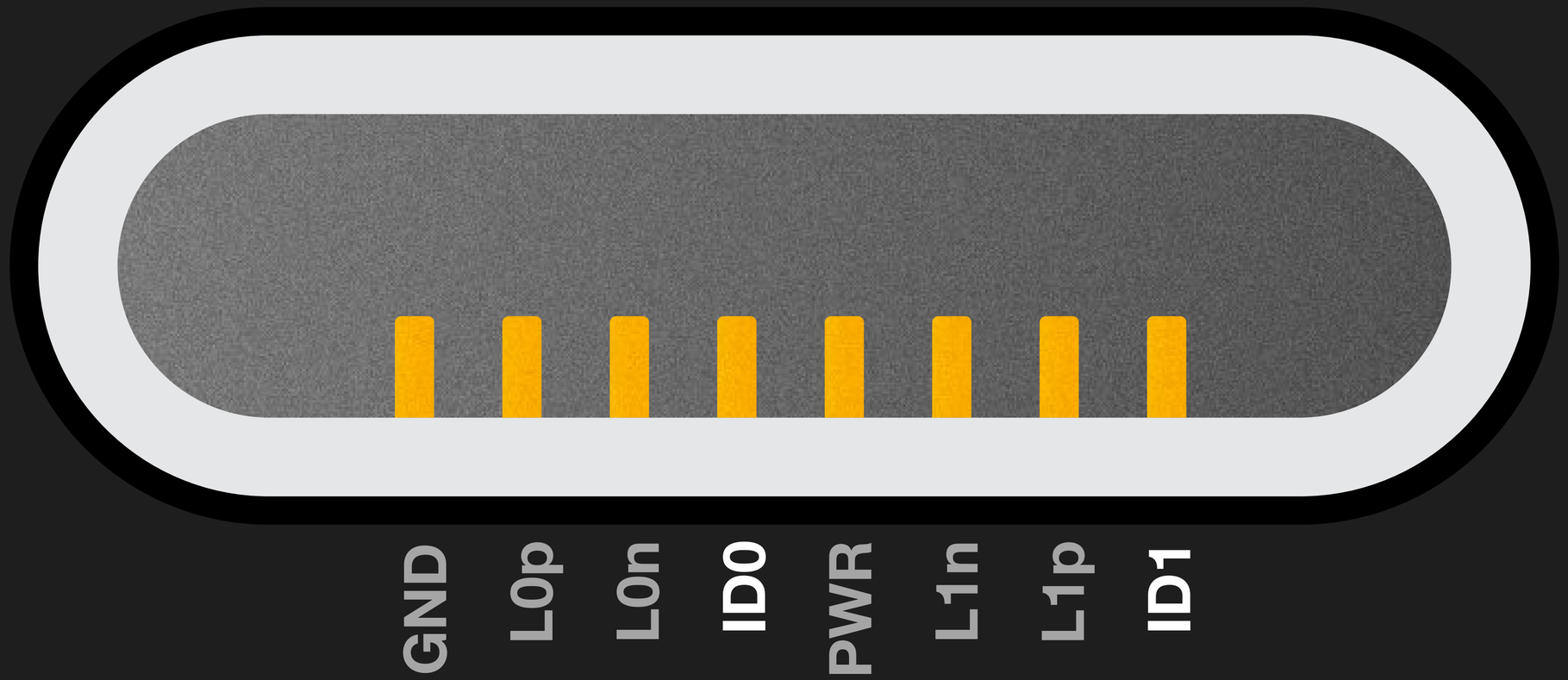
Let’s build our own!

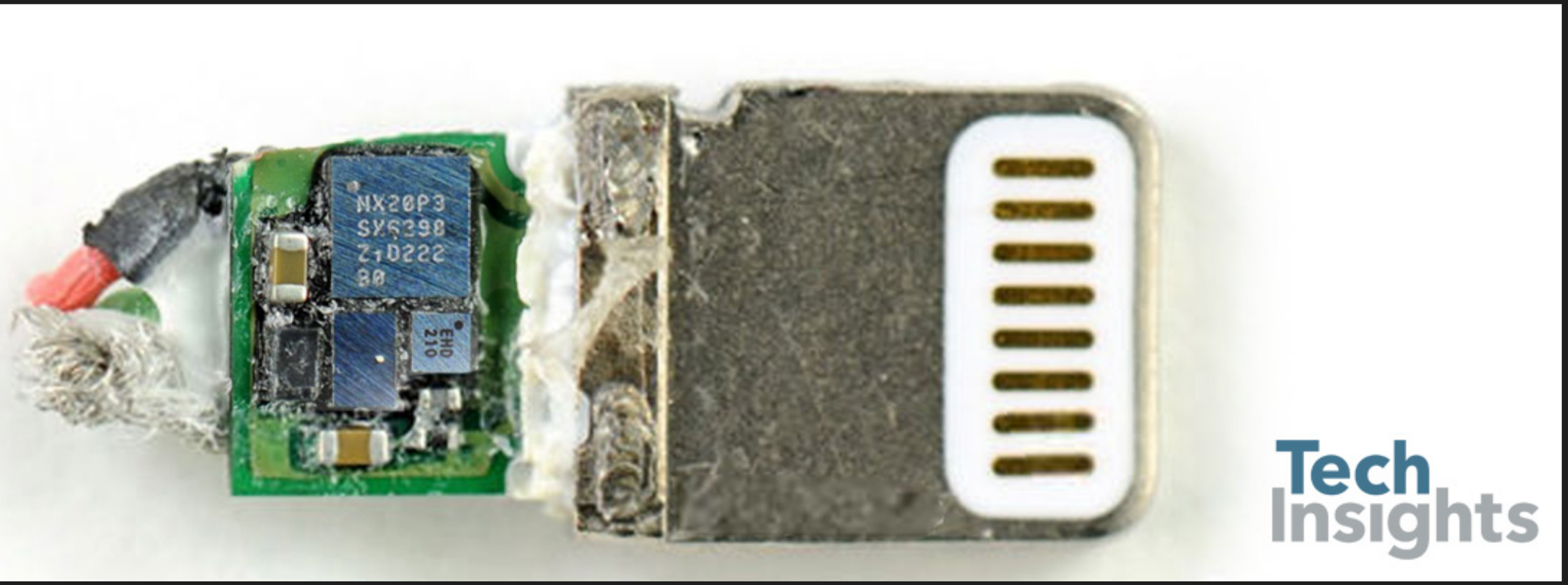


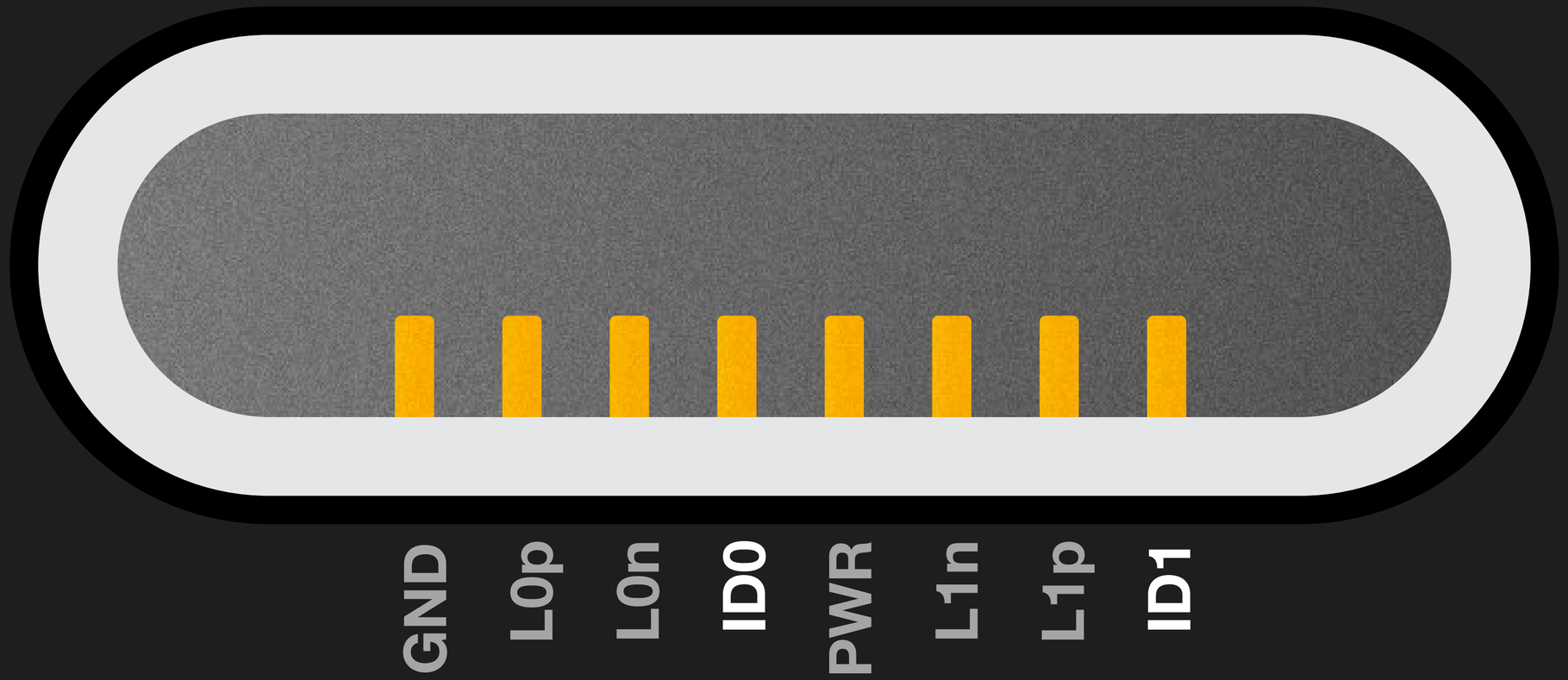




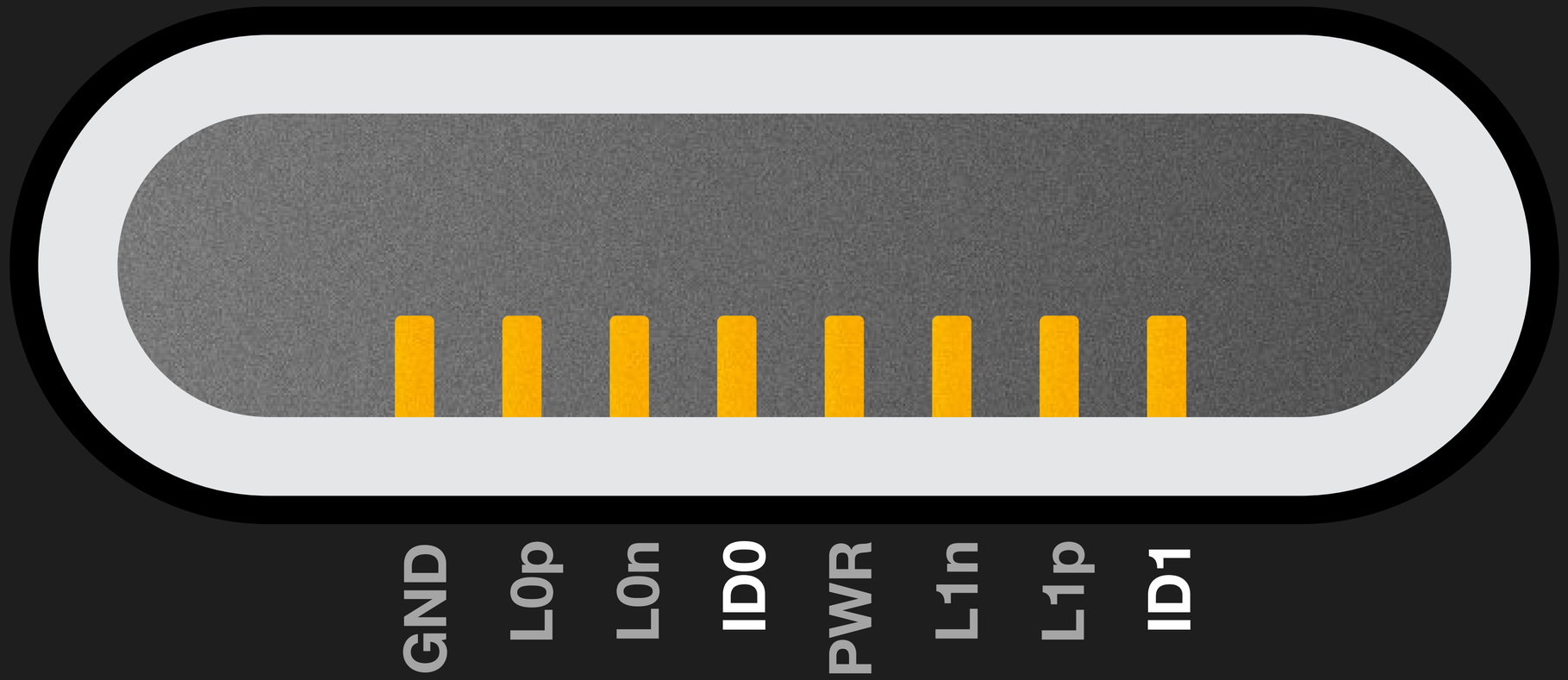




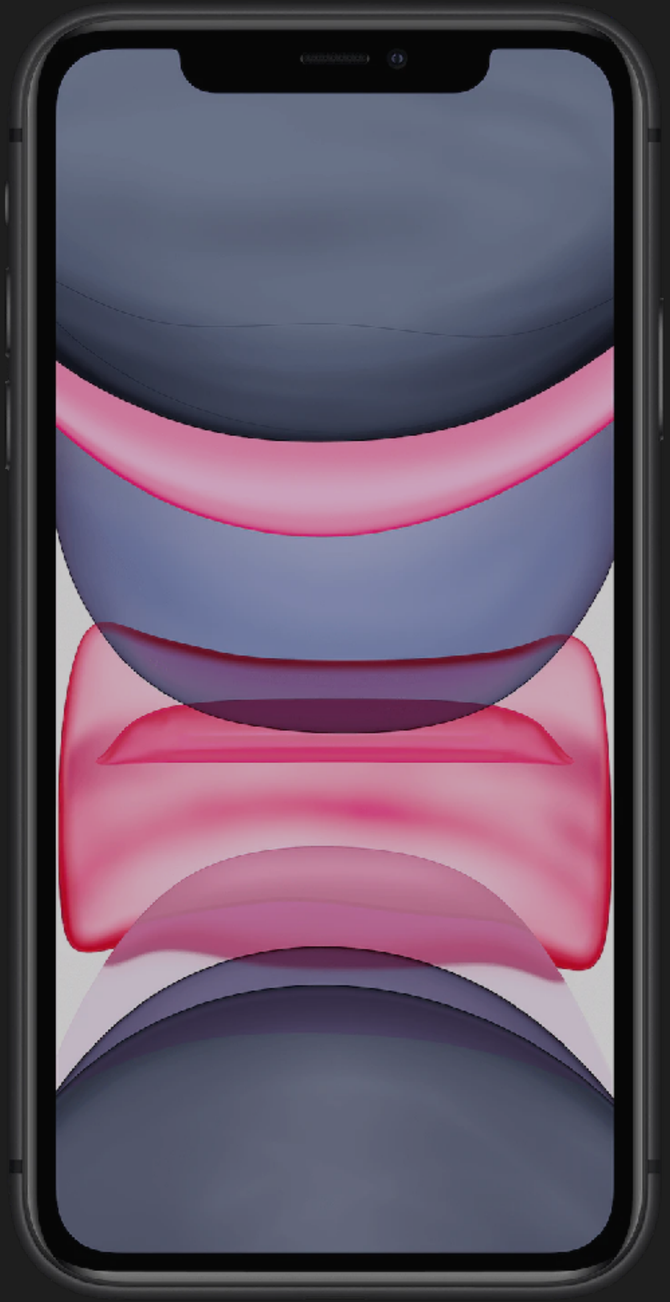


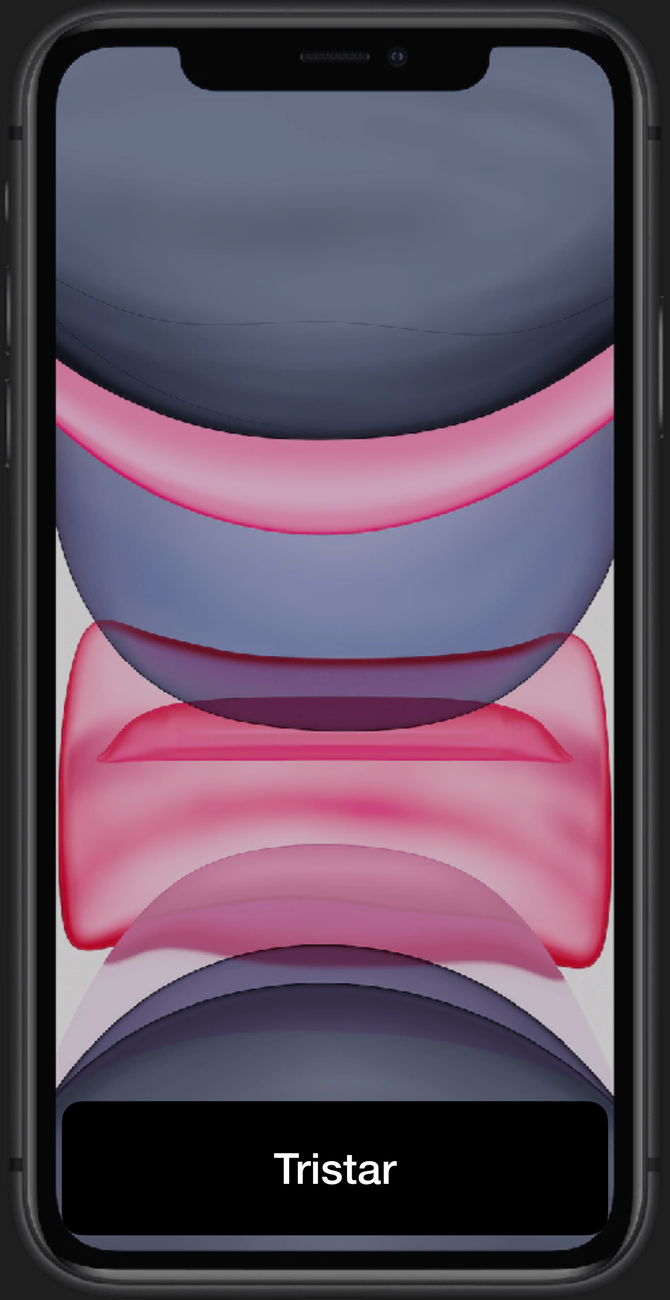


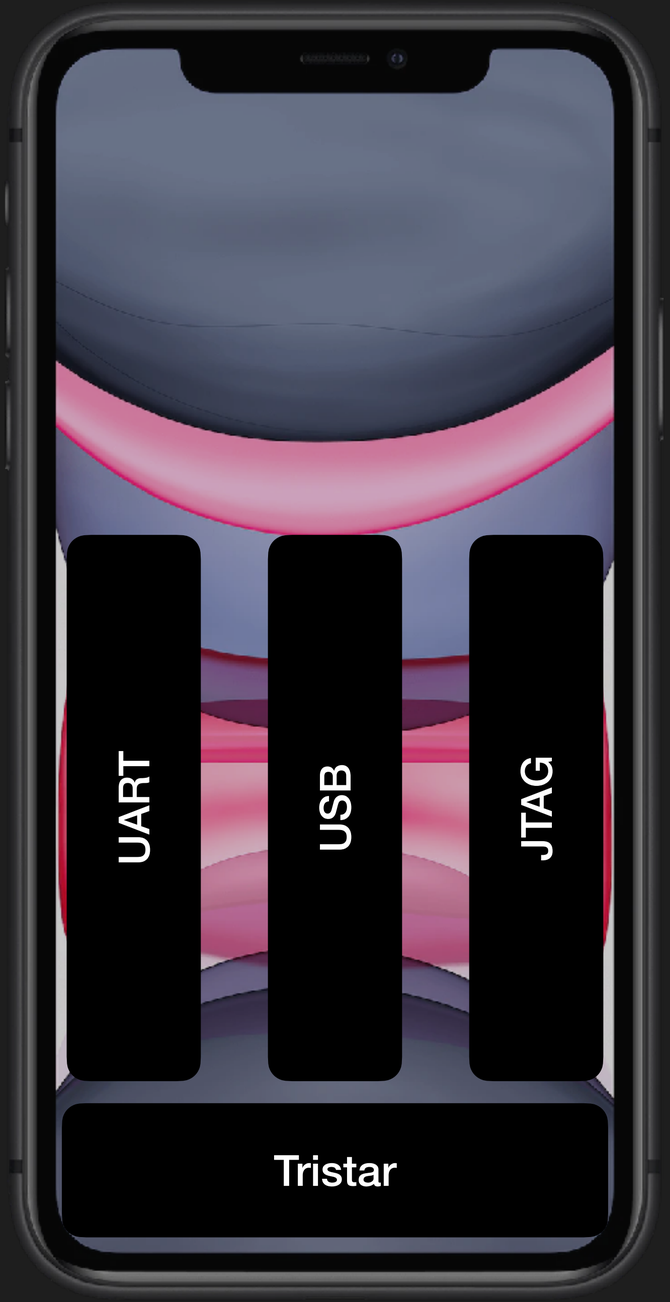
SDQ or IDBUS

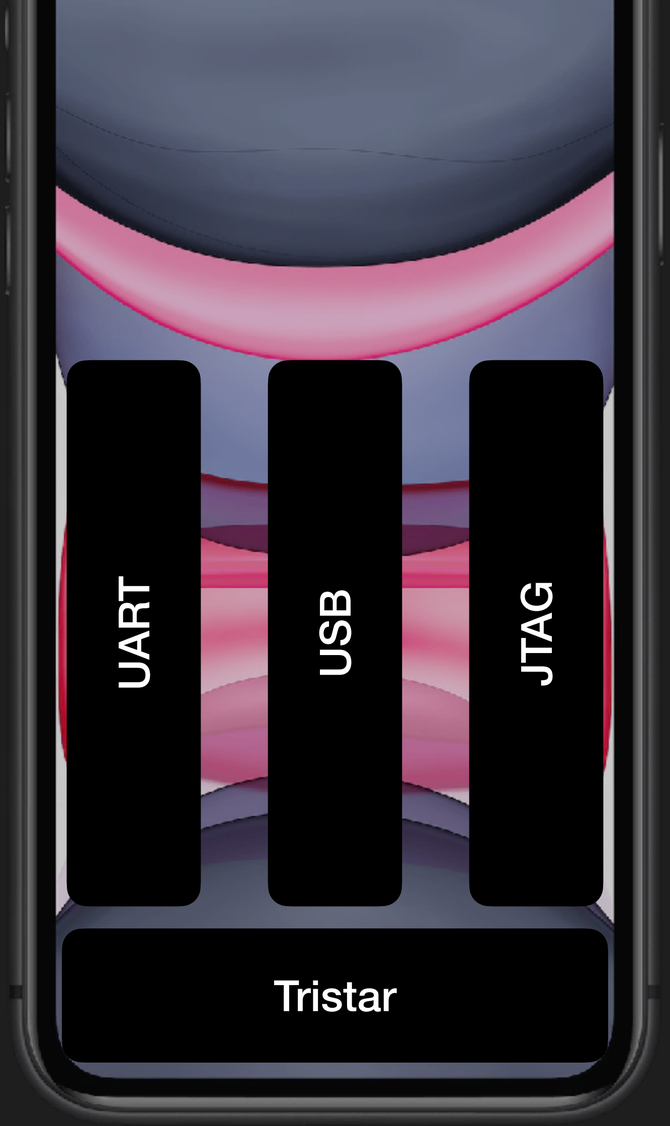


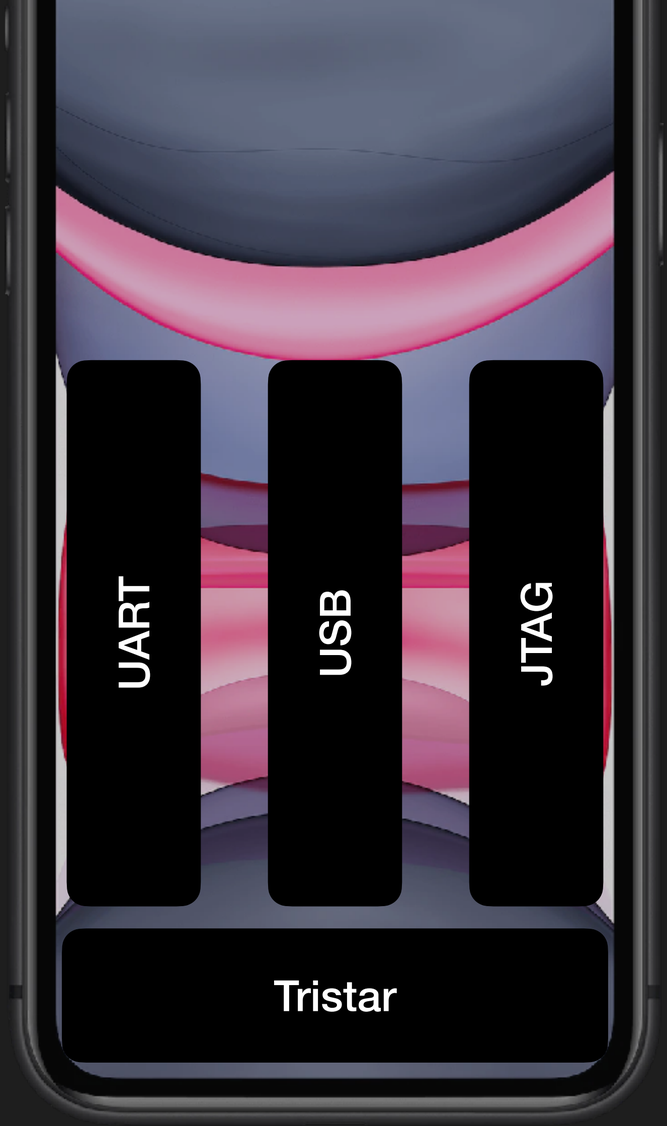
SDQ or IDBUS



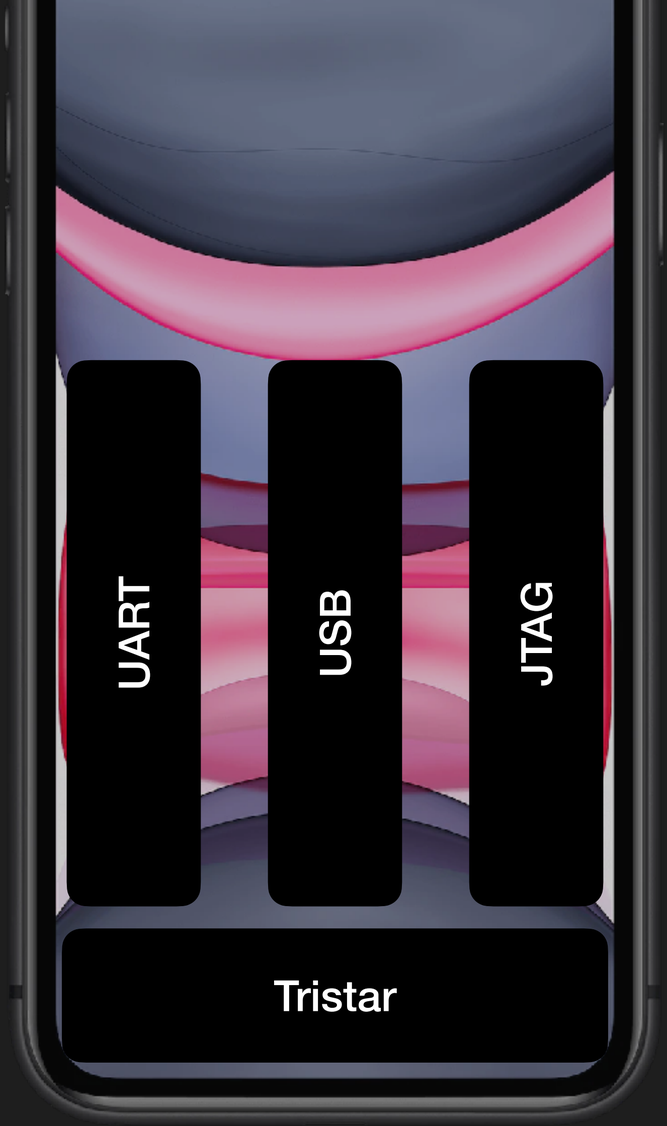






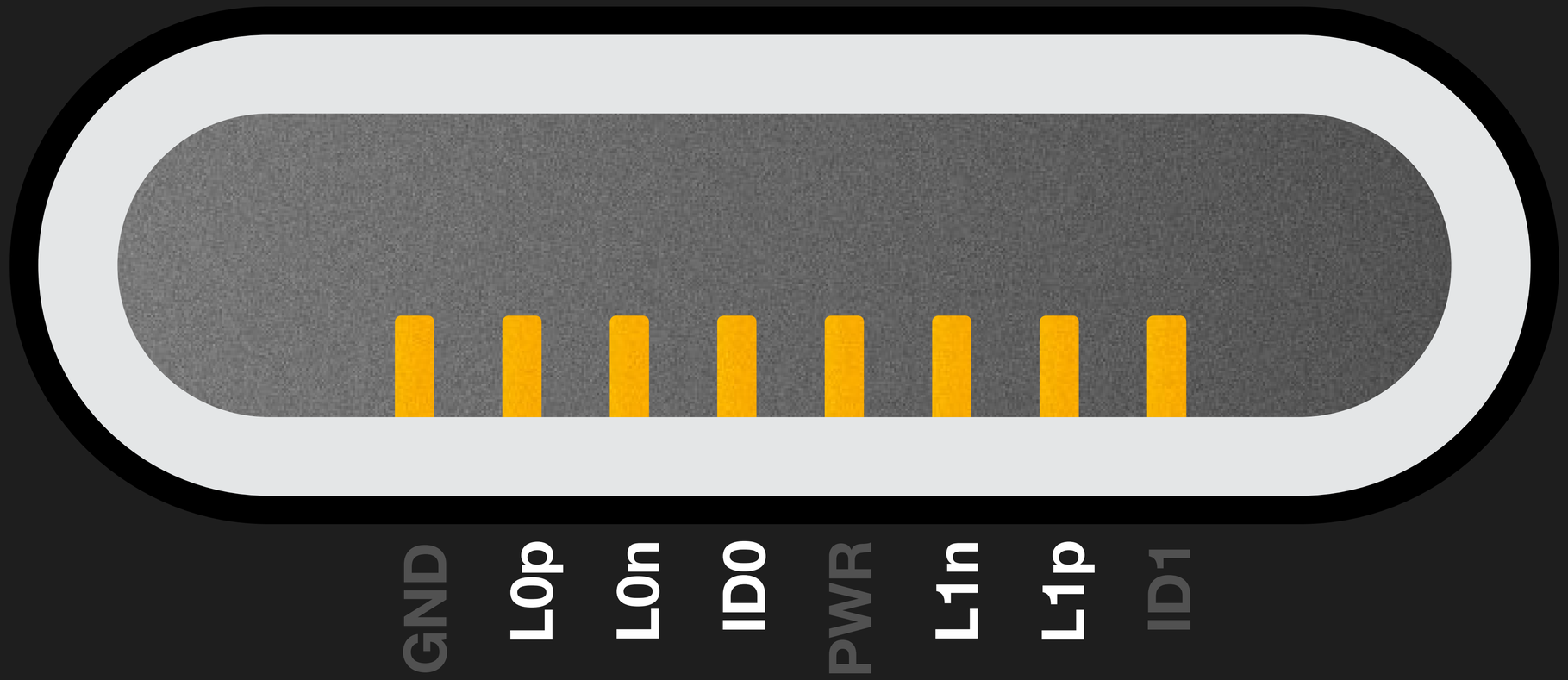


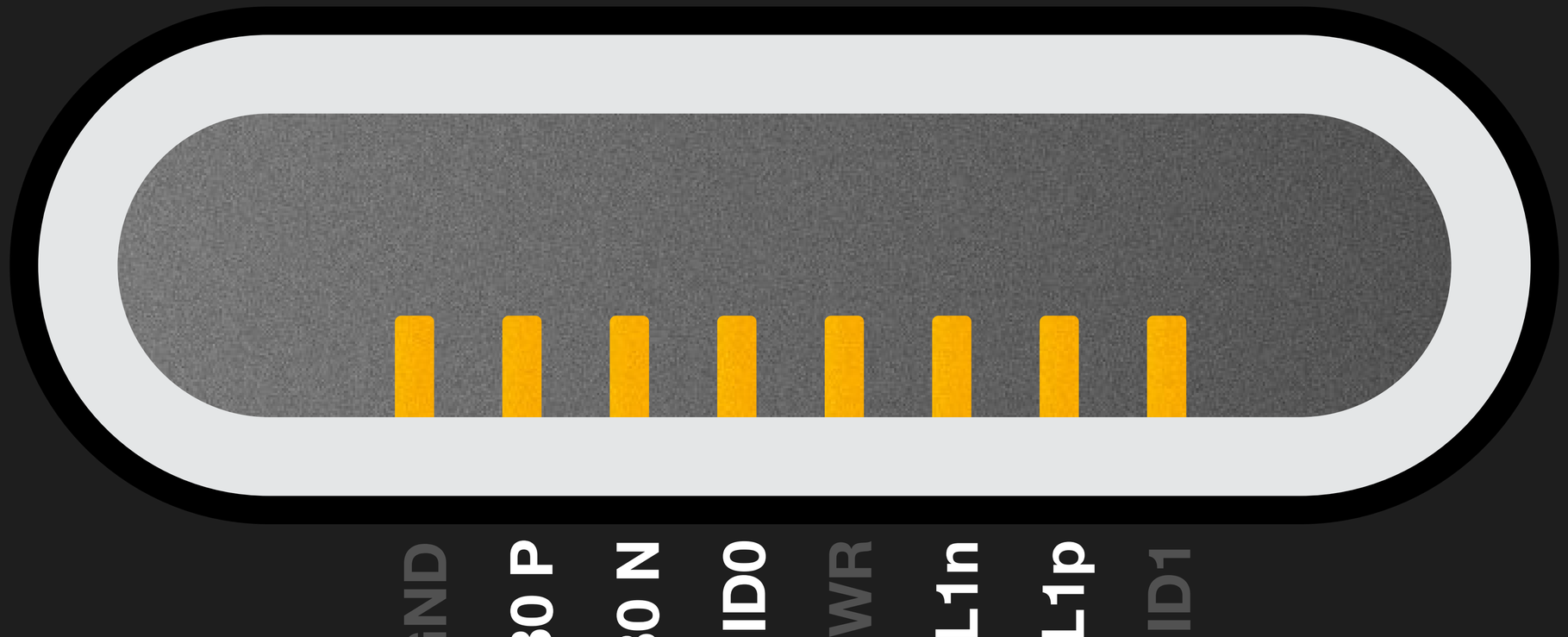
What do you want?

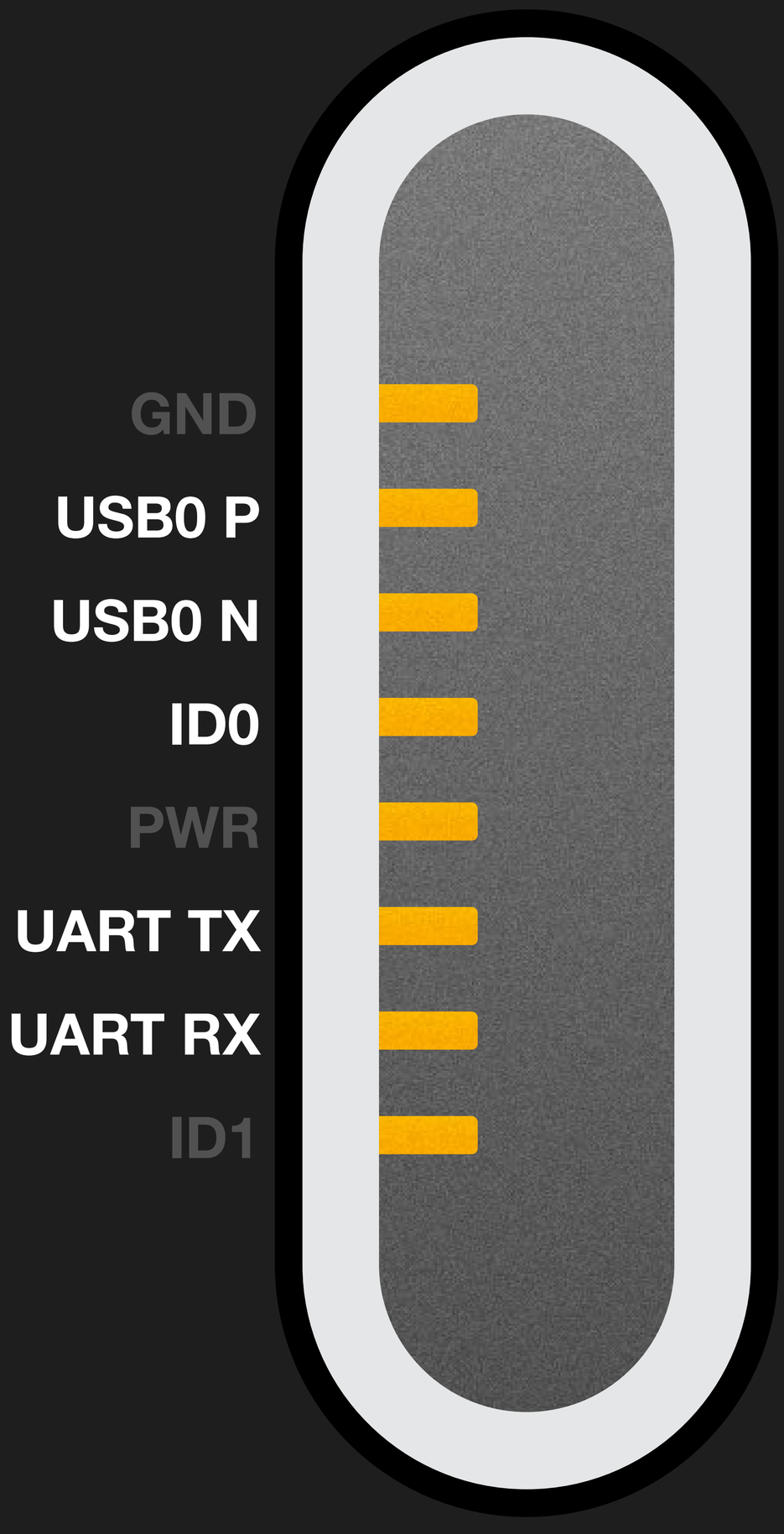


What do you want?

Speak USB plz





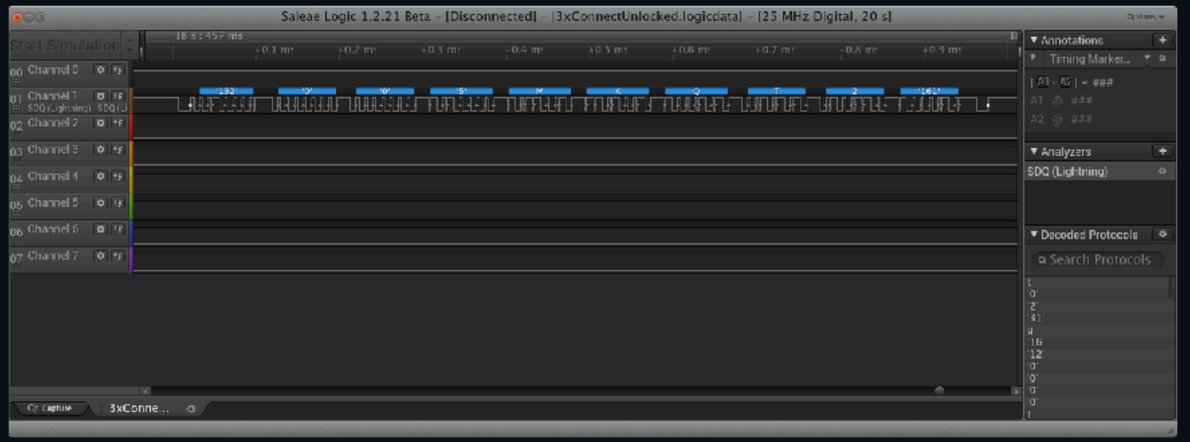


README.md

SDQAnalyzer

This is a simple analyzer for the SDQ protocol that is used on a lot of Apple products, for example:

- Lightning
- MagSafe
- iPhone/iPad battery



Documentation for the Saleae Logic Analyzer SDK can be found here:
https://github.com/saleae/SampleAnalyzer

Packages

No packages published

Contributors 4

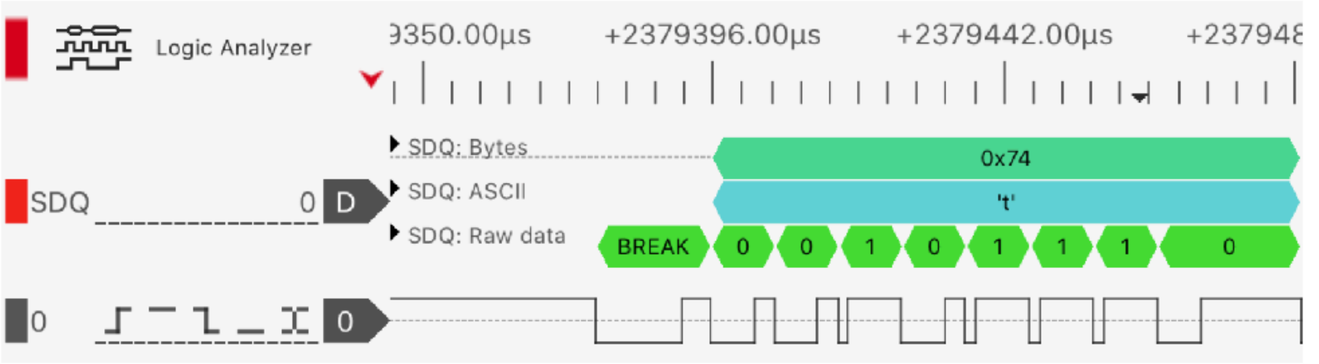
- **Marcus10110** Mark
- **nezza** Thomas Roth
- **ianrrees** Ian
- **nbanerje** Neel Banerjee

Languages

- **C++** 82.8%
- **CMake** 17.2%

Private nyansatan.github.io

What're SDQ and IDBUS?



These 2 terms are often referred as kind of synonyms. For convinience, I'll only use term **IDBUS** from now on, as it seems more correct to me (and that's how this technology called in the THS7383 datasheet)

So, **IDBUS** - is a digital protocol used for negotiations between Tristar and HiFive. Very similar to Onewire protocol

Now we can play

Let's sniff the negotiations between Tristar and HiFive. Take a logic analyzer, a Lightning male-to-female passthrough breakout board, some accessory (normal Lightning to USB cable would fit just fine) and of course some device with Lightning port

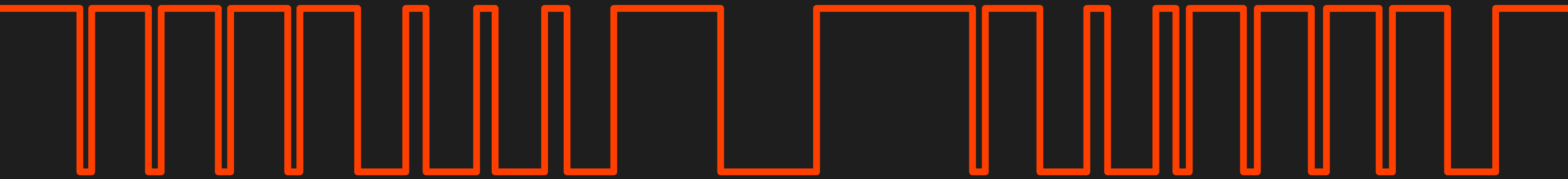
First connect logic analyzer's channels to both **ID** lines of the breakout (pins 4 and 8) and connect the

SDQ or IDBUS

Simple one-wire protocol

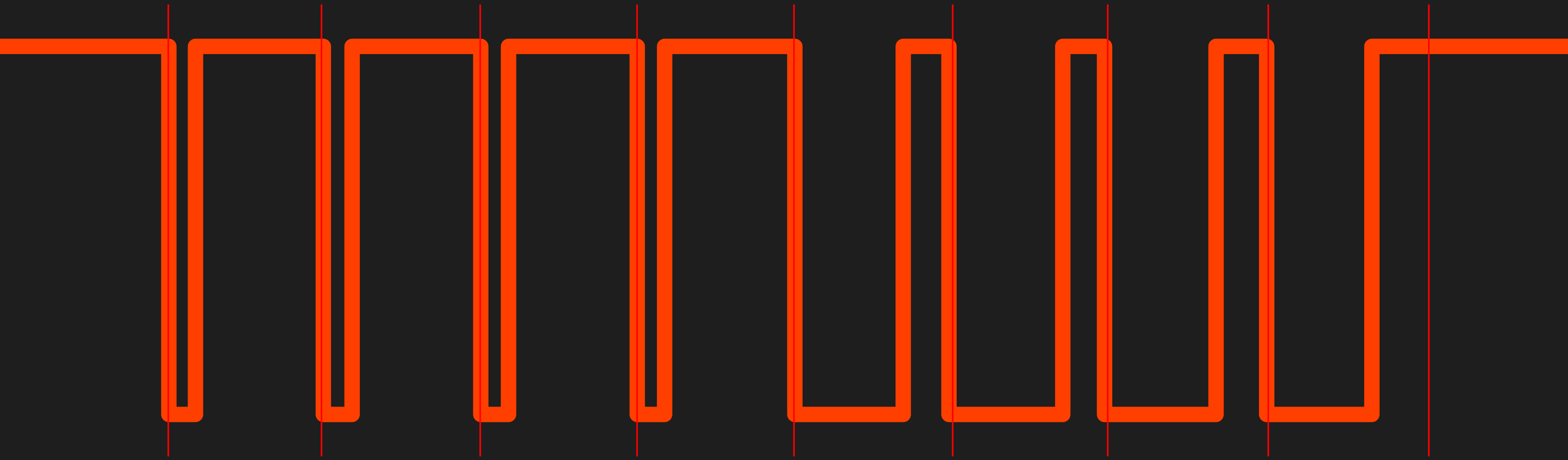
SDQ or IDBUS

Simple one-wire protocol

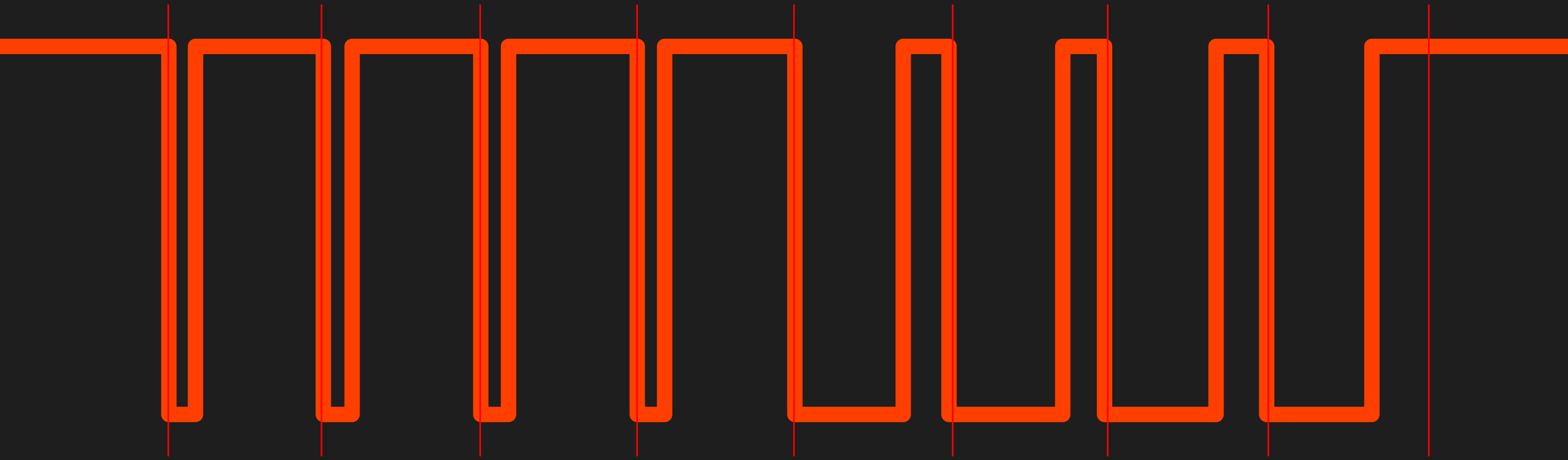


SDQ or IDBUS

SDQ or IDBUS

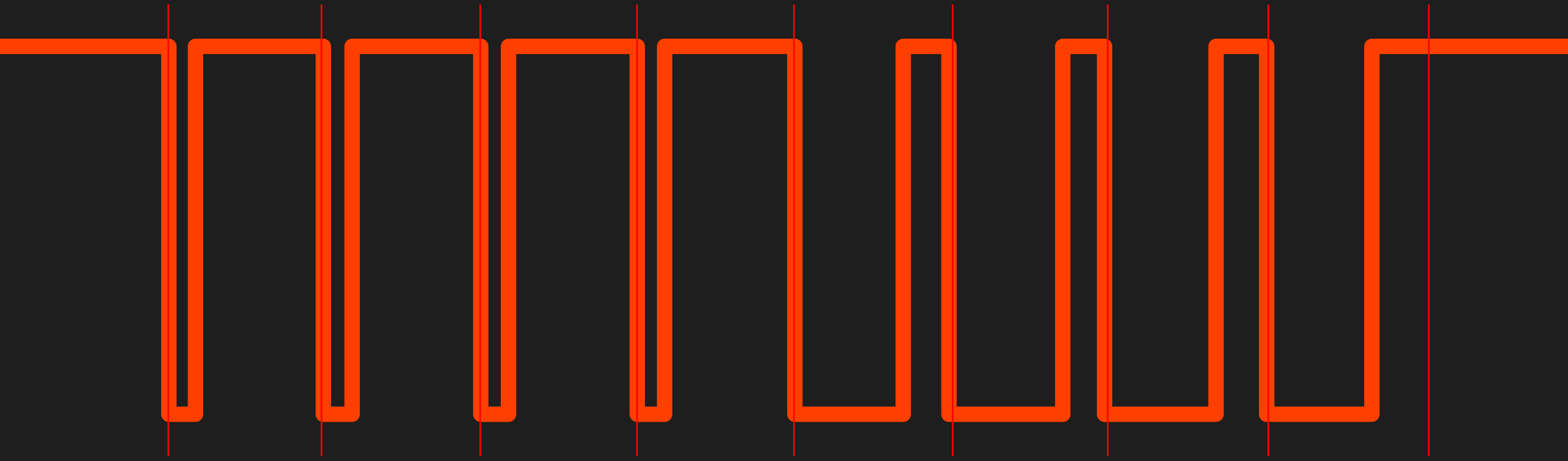


SDQ or IDBUS



1 1 1 1 0 0 0 0

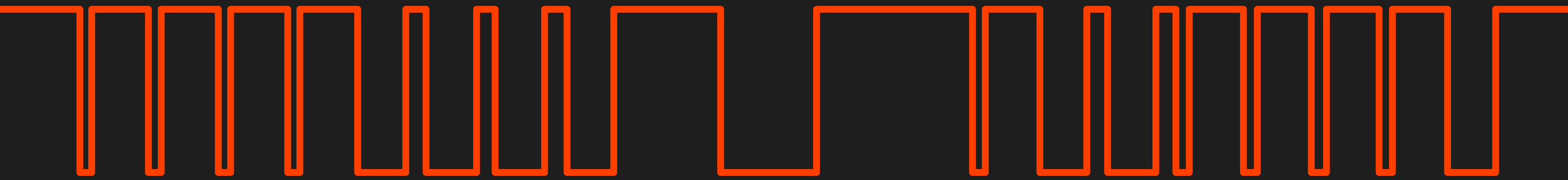
SDQ or IDBUS



1 1 1 1 0 0 0 0

0x0F

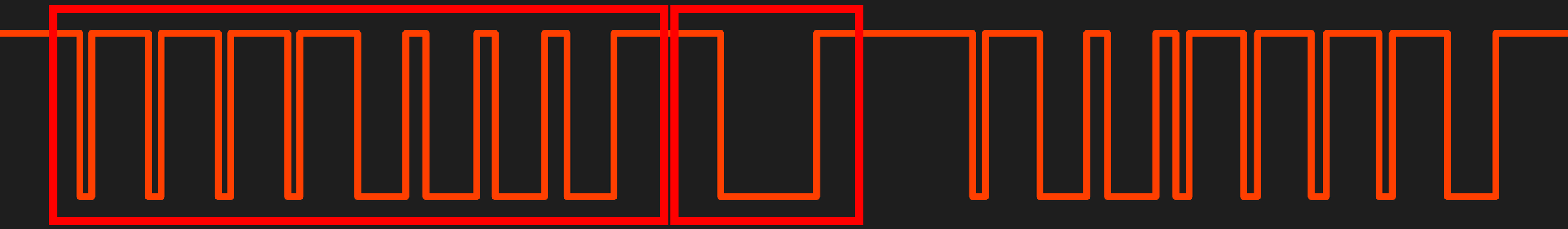
SDQ or IDBUS



SDQ or IDBUS

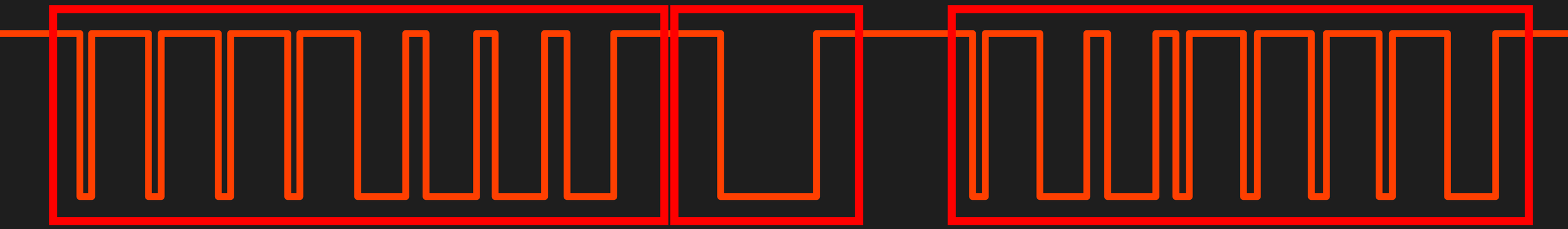
0x0F

SDQ or IDBUS

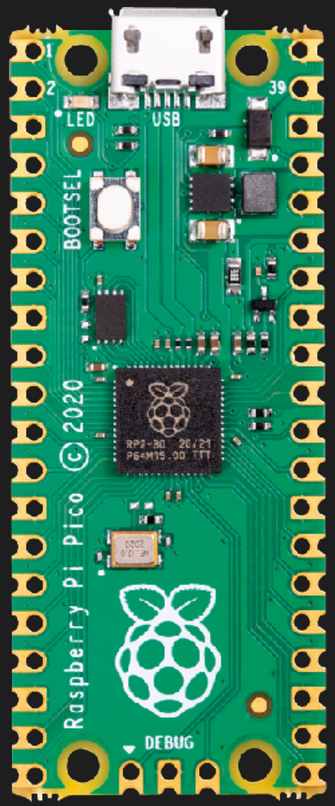


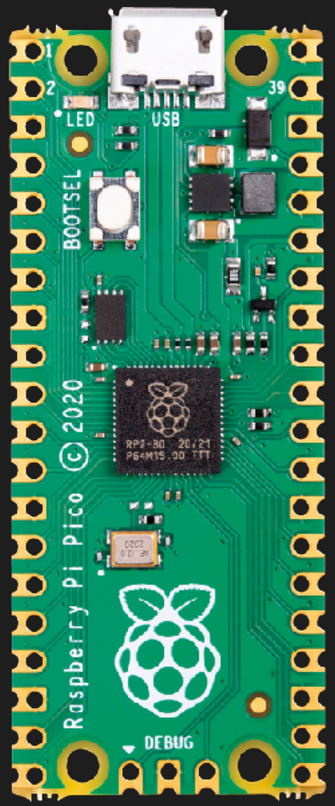
0x0F Break

SDQ or IDBUS

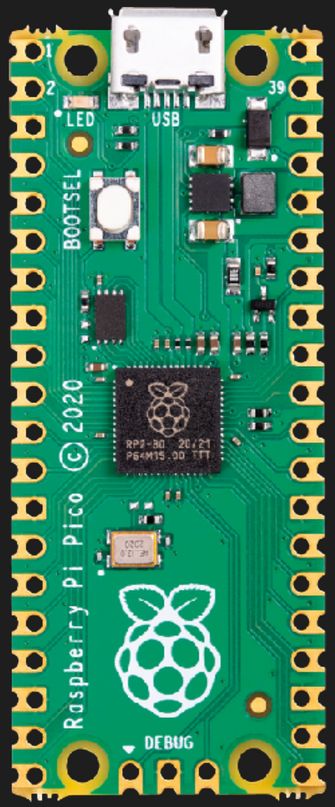


0x0F Break 0x79

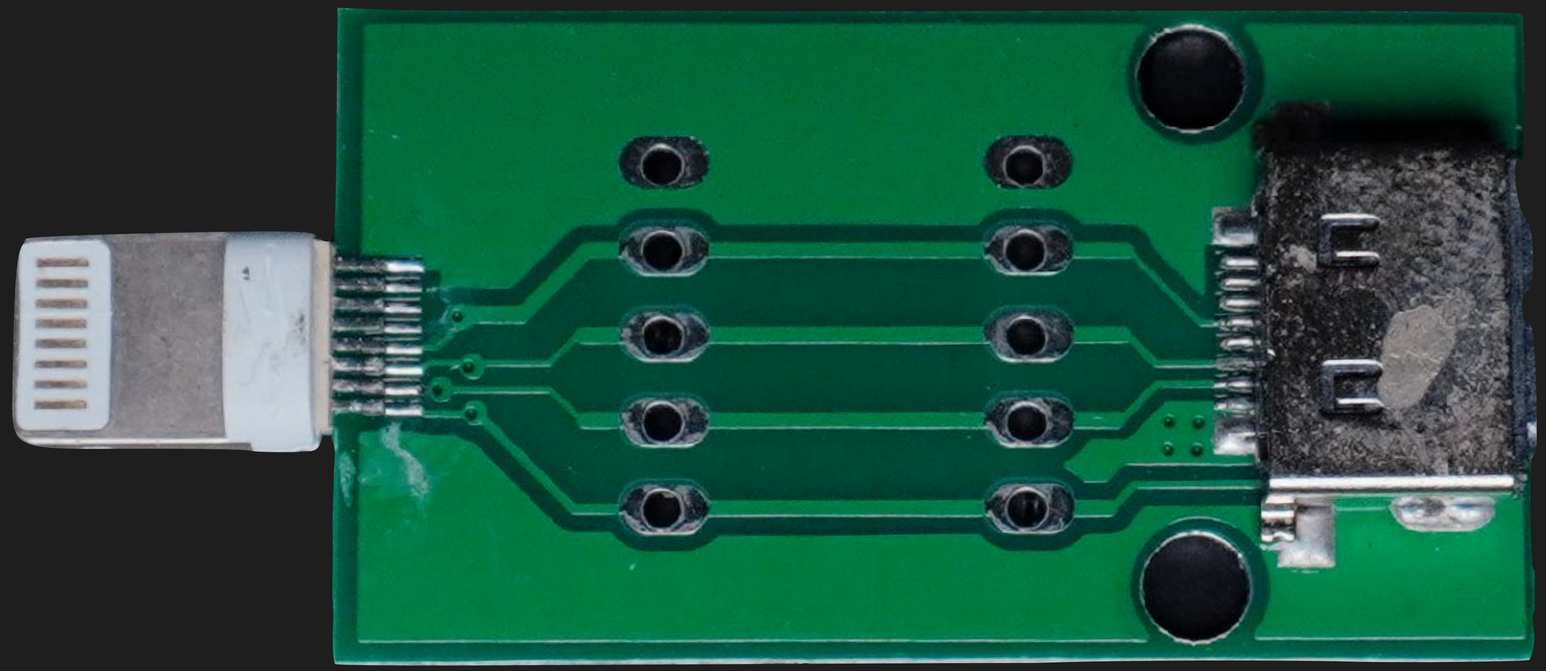




- Runs at 3.3V
- Can easily implement fast protocols using PIO
- Is actually available 🥲



But we need a Lightning connector…



Private

amazon.de

amazon.de

Deliver to United States

All

lightning verlängerung

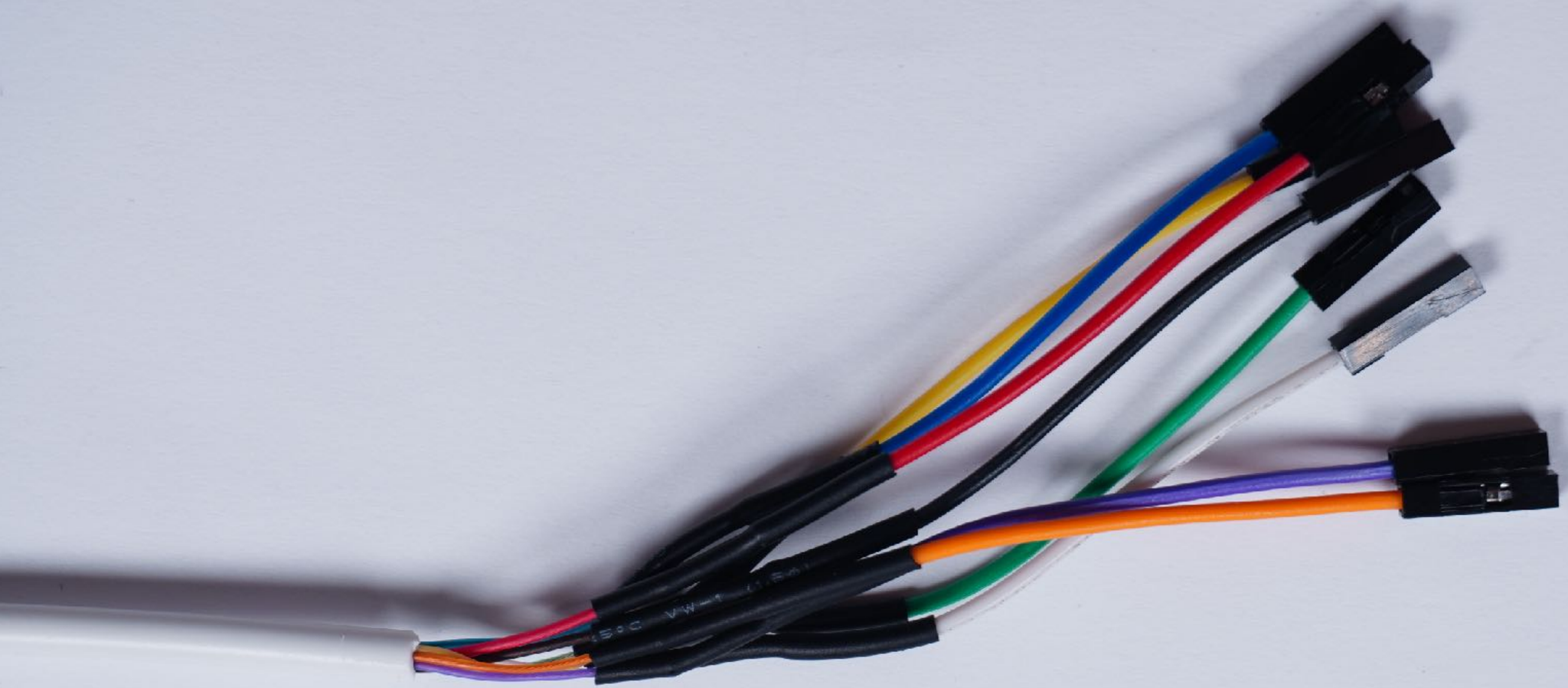
Hello, Sign in Account & Lists

Returns & Orders

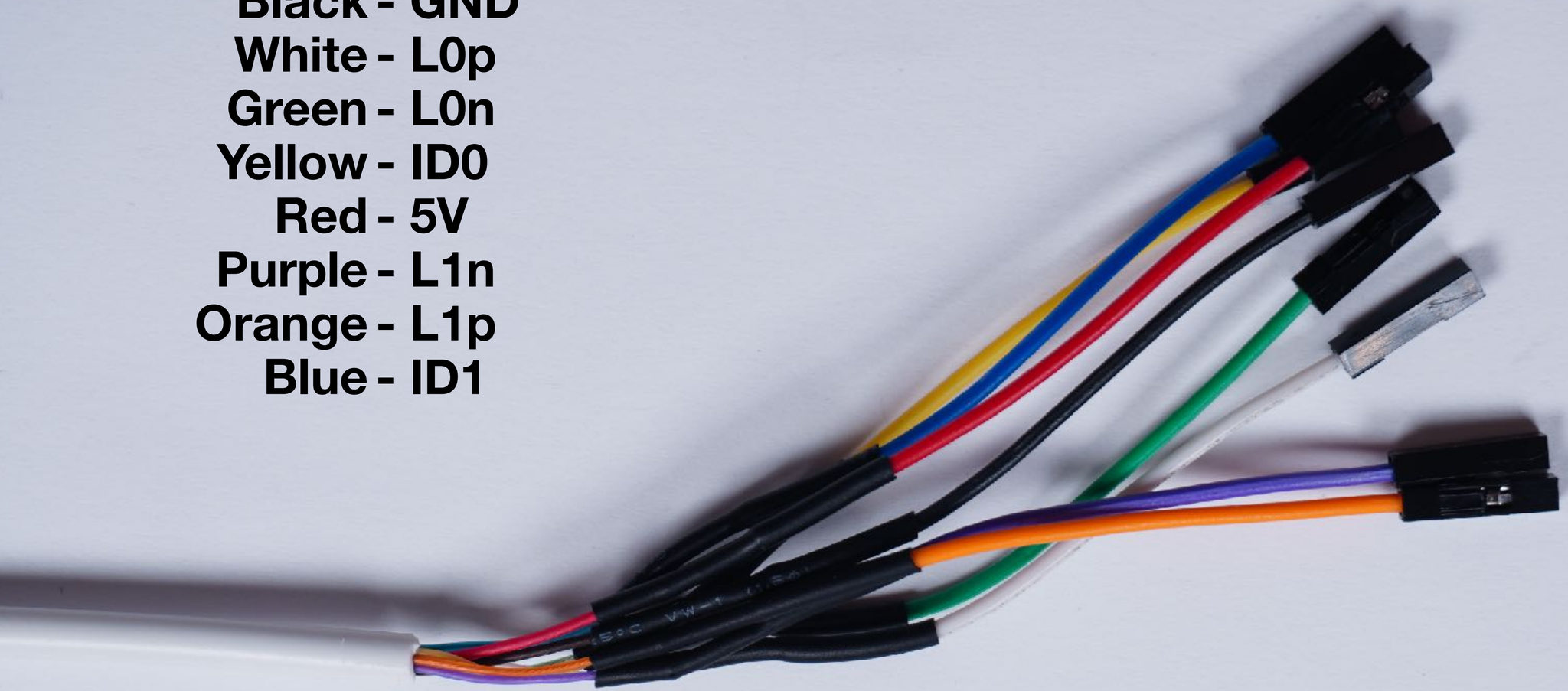
0 Shopping-Basket

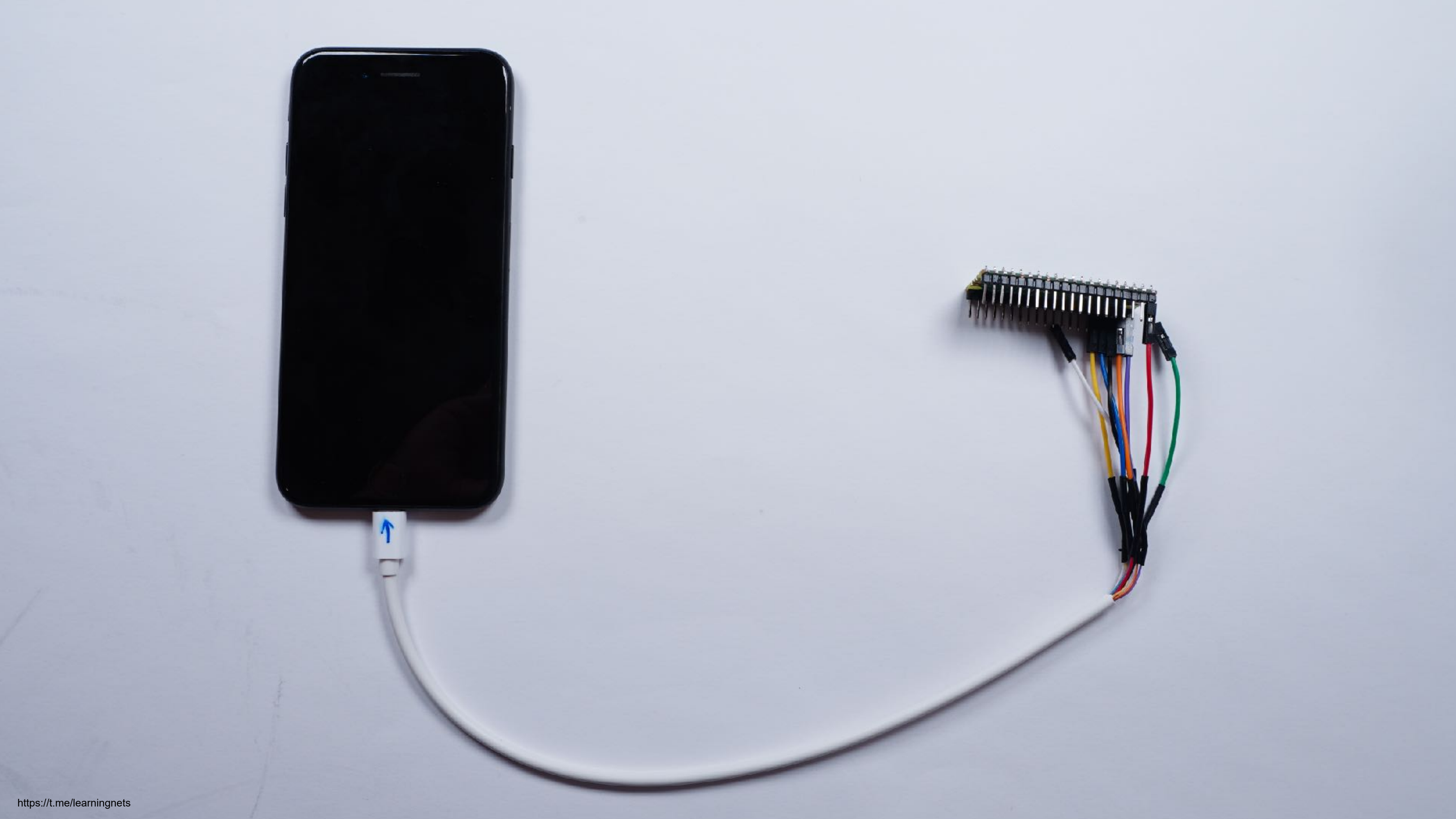
OKCS Originals Extension Cable 1 Metre Compatible with iPhone11, 11 Pro, 11 Max, XR, XS, XS Max, X, 8, 8 Plus, 7, 7 Plus etc. - White

Colour Name:8 pin extender cable.



Black - GND
White - L0p
Green - L0n
Yellow - ID0
Red - 5V
Purple - L1n
Orange - L1p
Blue - ID1





Building a simple DCSD cable

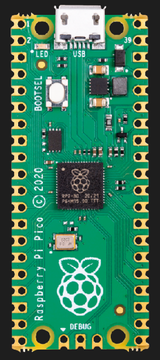
Who’s there?

74 00 07 20

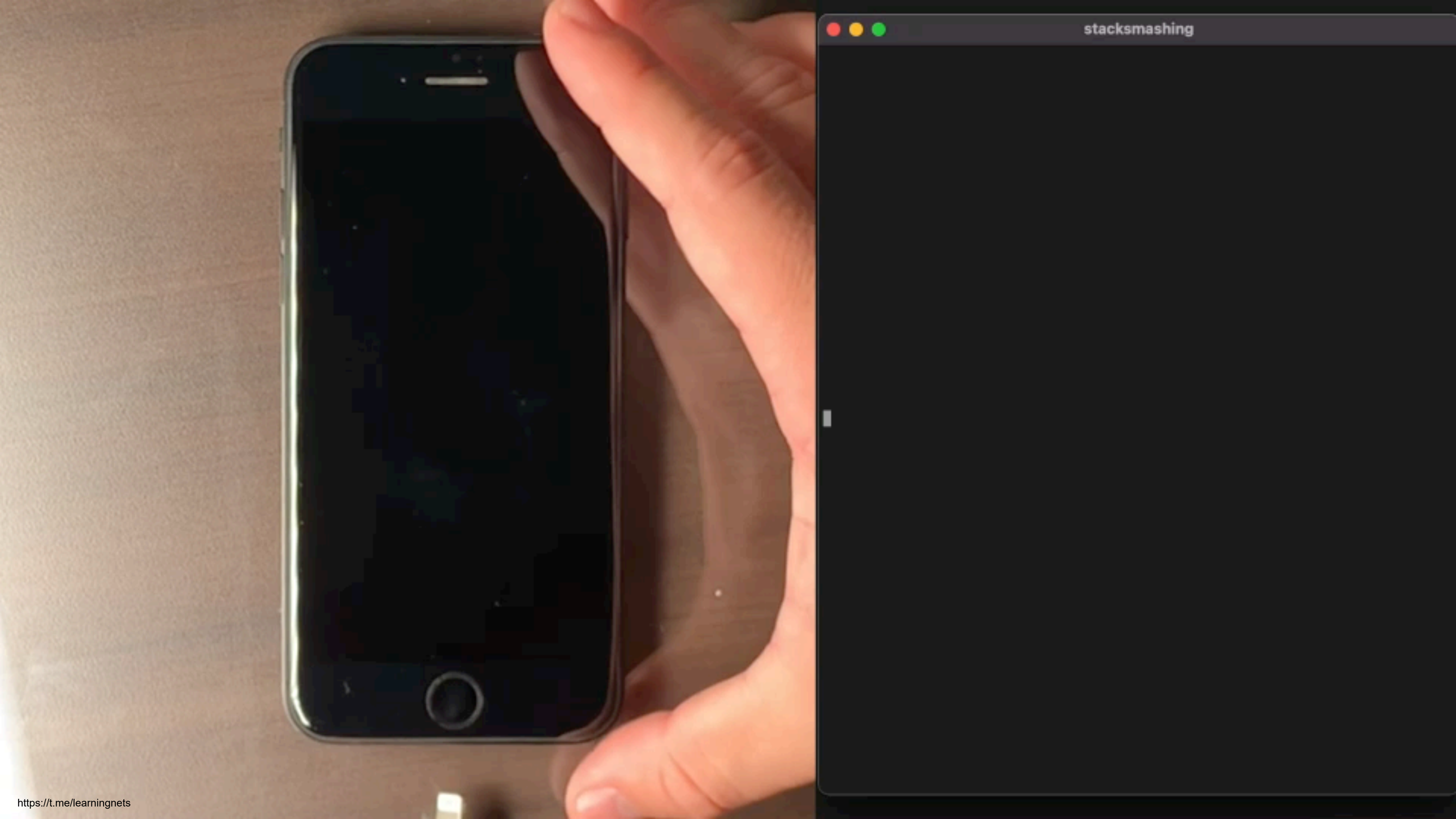
Who’s there?

74 00 07 20

Please speak USB & UART



75 20 00 00 00 00 00 AA



JTAG…

JTAG…

… actually SWD

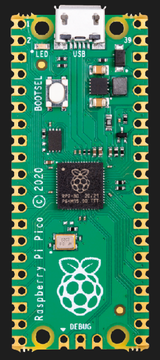
The plan!

The plan!

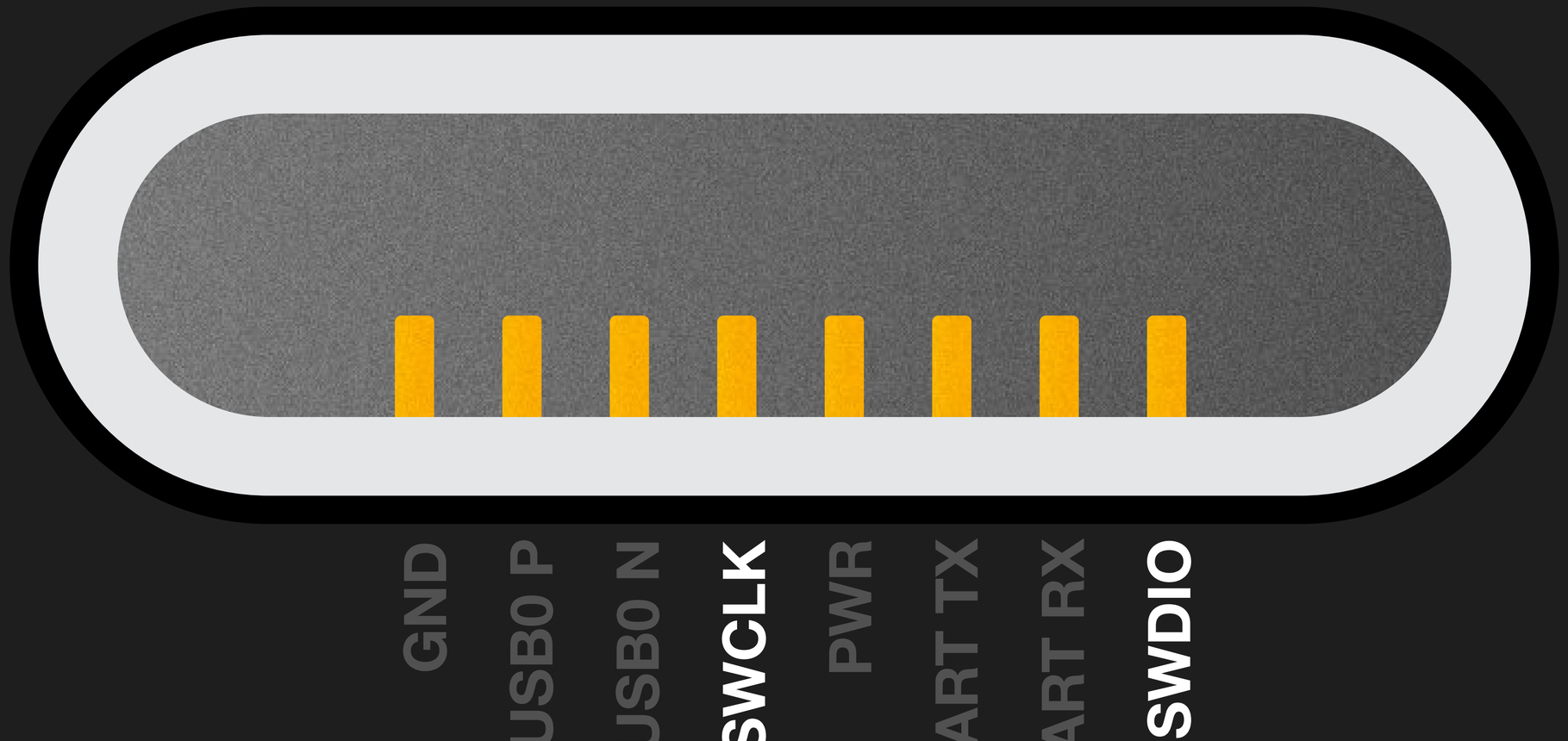
Who’s there?

74 00 07 20

Please speak USB, UART & SWD!

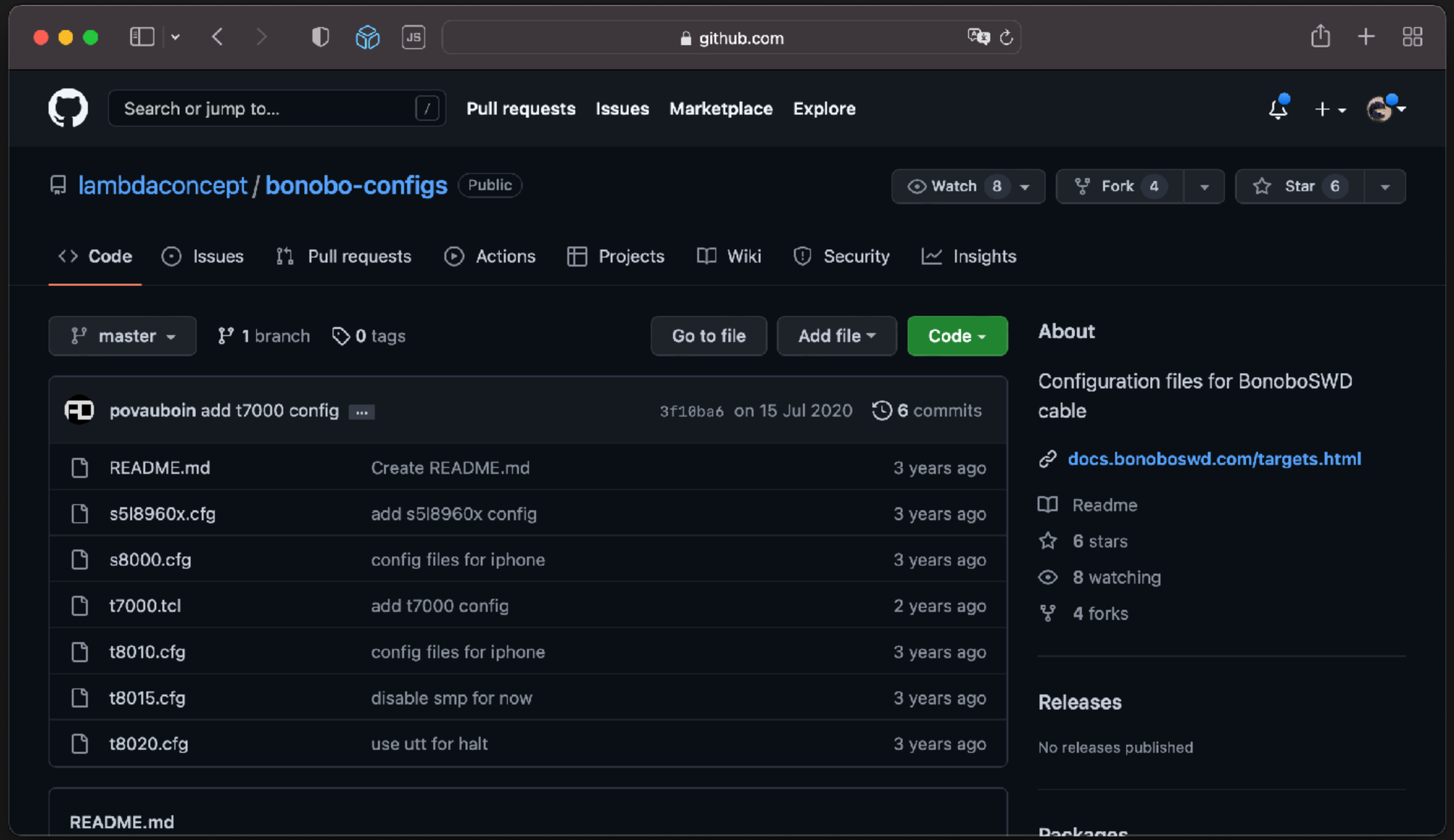


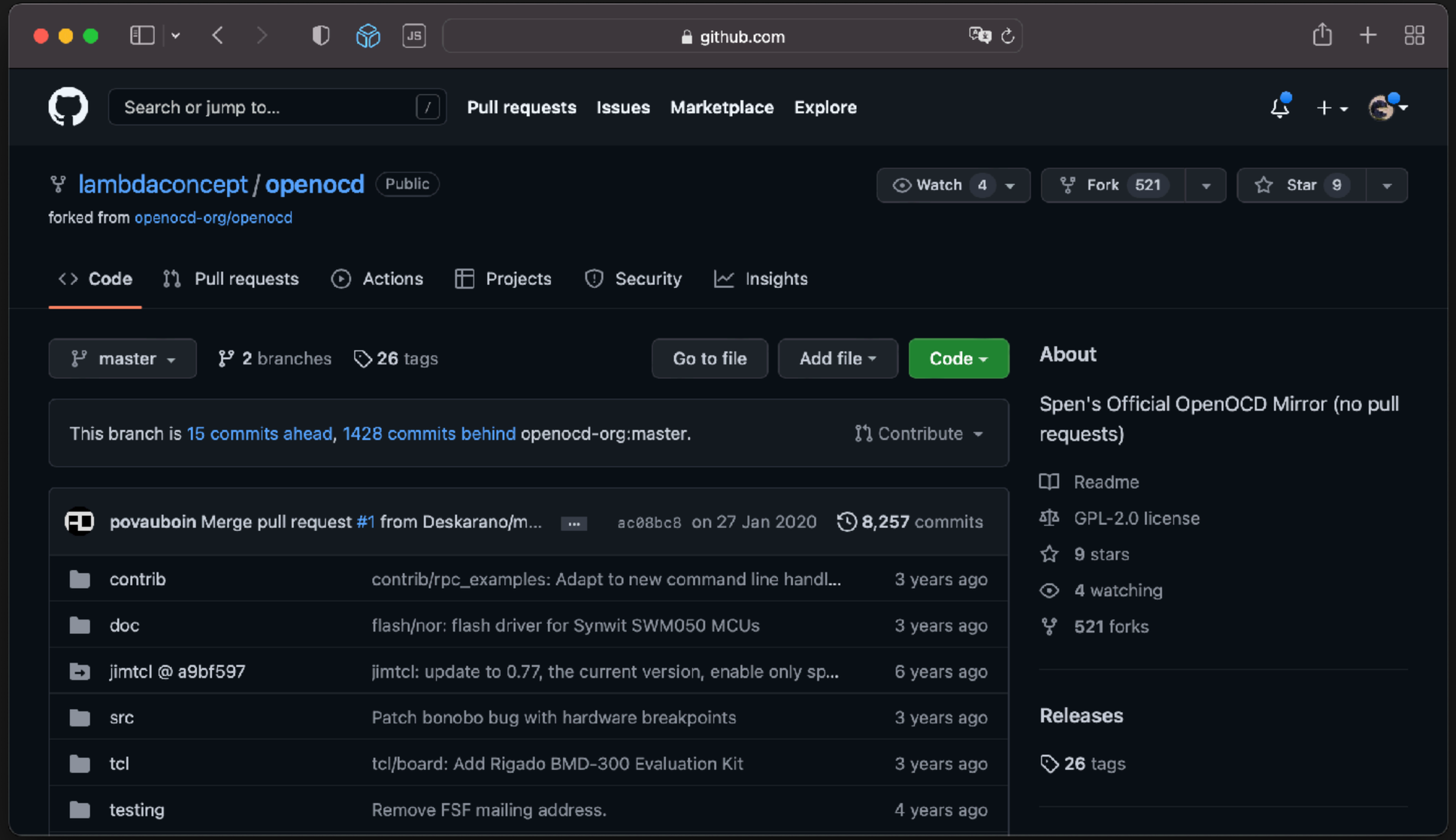
75 A0 00 00 00 00 00 40



The plan!

The plan!





The plan!

The plan!

The plan!

```
J-Link>connect
Device "CORTEX-A12" selected.


Connecting to target via SWD
Found SW-DP with ID 0x4BA02477
```

```
> targets
targets
    TargetName          Type       Endian TapName             State
--  ------------------- ---------- ------ ------------------- ------------
 0  iphone.dbg          mem_ap     little iphone.cpu          running
 1  iphone.mem          mem_ap     little iphone.cpu          running
 2* iphone.ecore0       aarch64    little iphone.cpu          unknown
 3  iphone.ecore1       aarch64    little iphone.cpu          unknown
 4  iphone.ecore2       aarch64    little iphone.cpu          unknown
 5  iphone.ecore3       aarch64    little iphone.cpu          unknown
 6  iphone.pcore0       aarch64    little iphone.cpu          unknown
 7  iphone.pcore1       aarch64    little iphone.cpu          unknown
 8  iphone.sep          aarch64    little iphone.cpu          unknown
```

How do you debug this?

You read the SWD spec

You logic analyze it

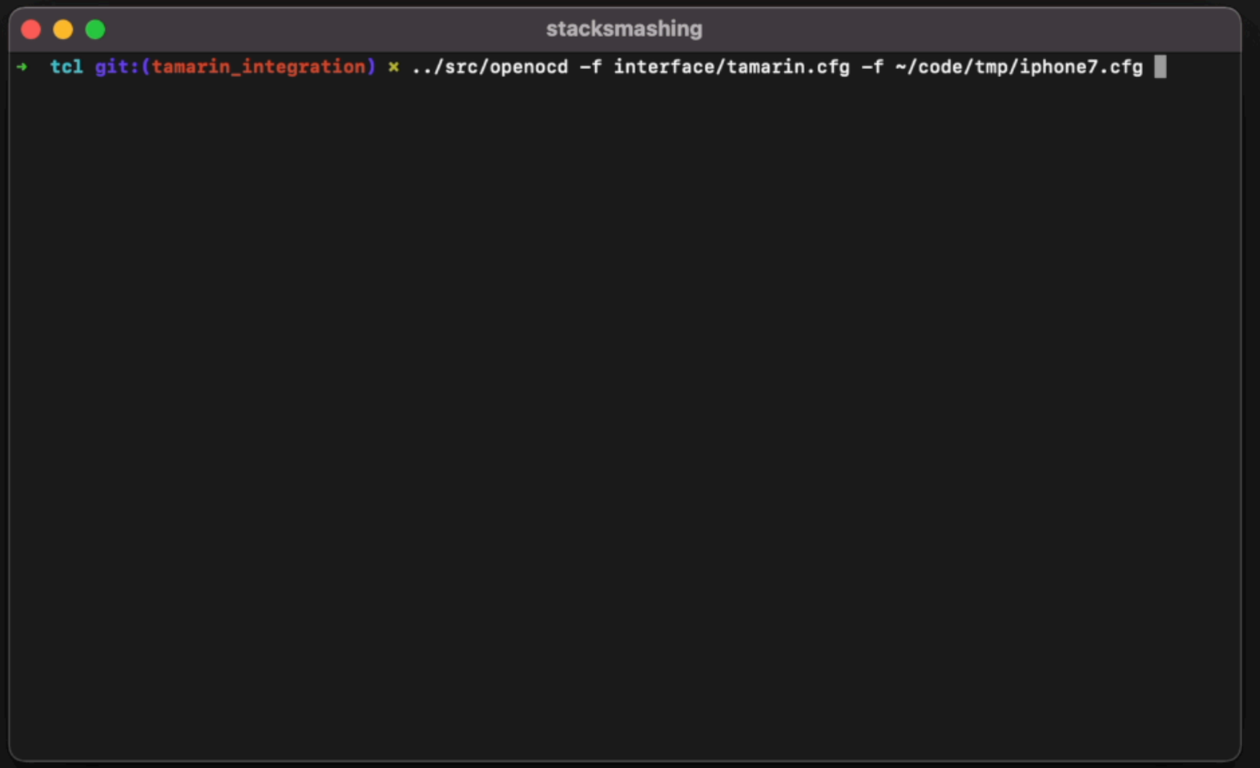
You fix the logic analyzer

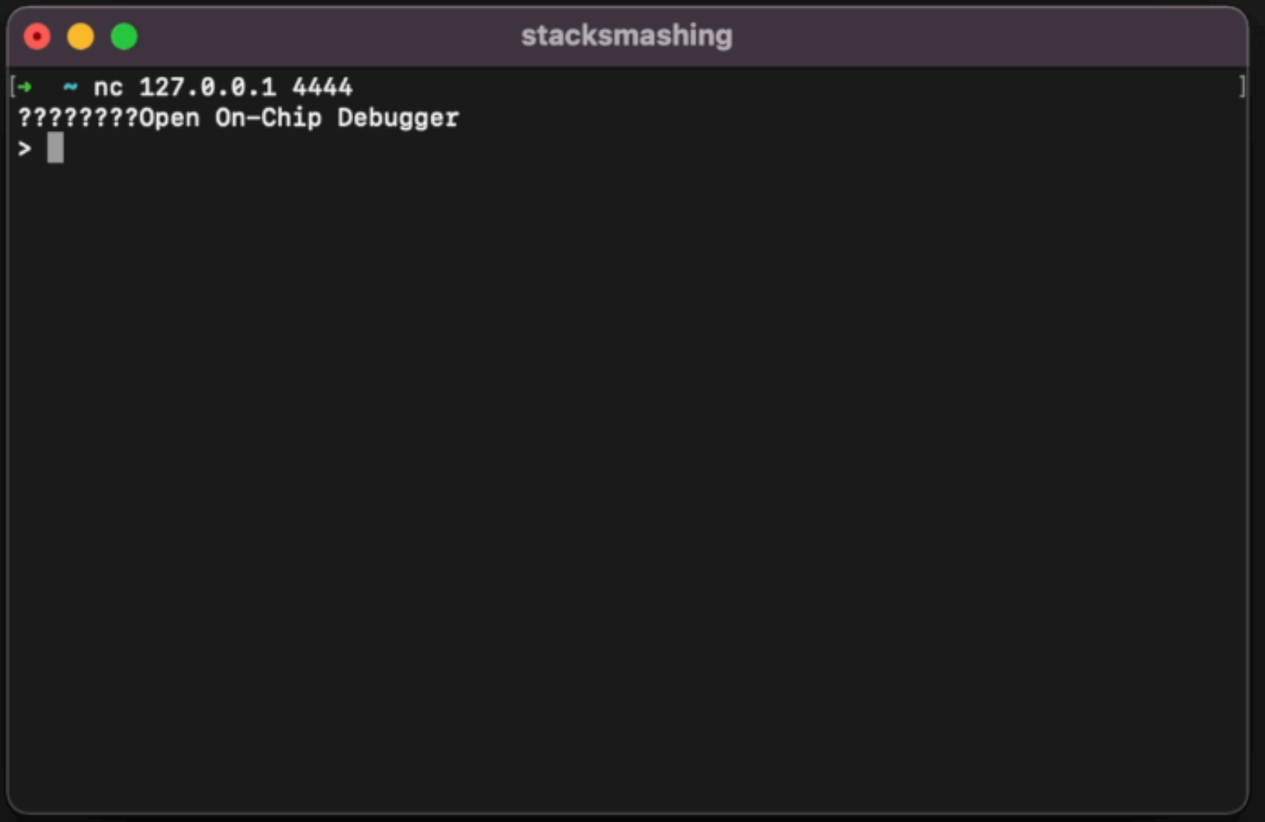
You find OpenOCD does not handle SWD WAITs

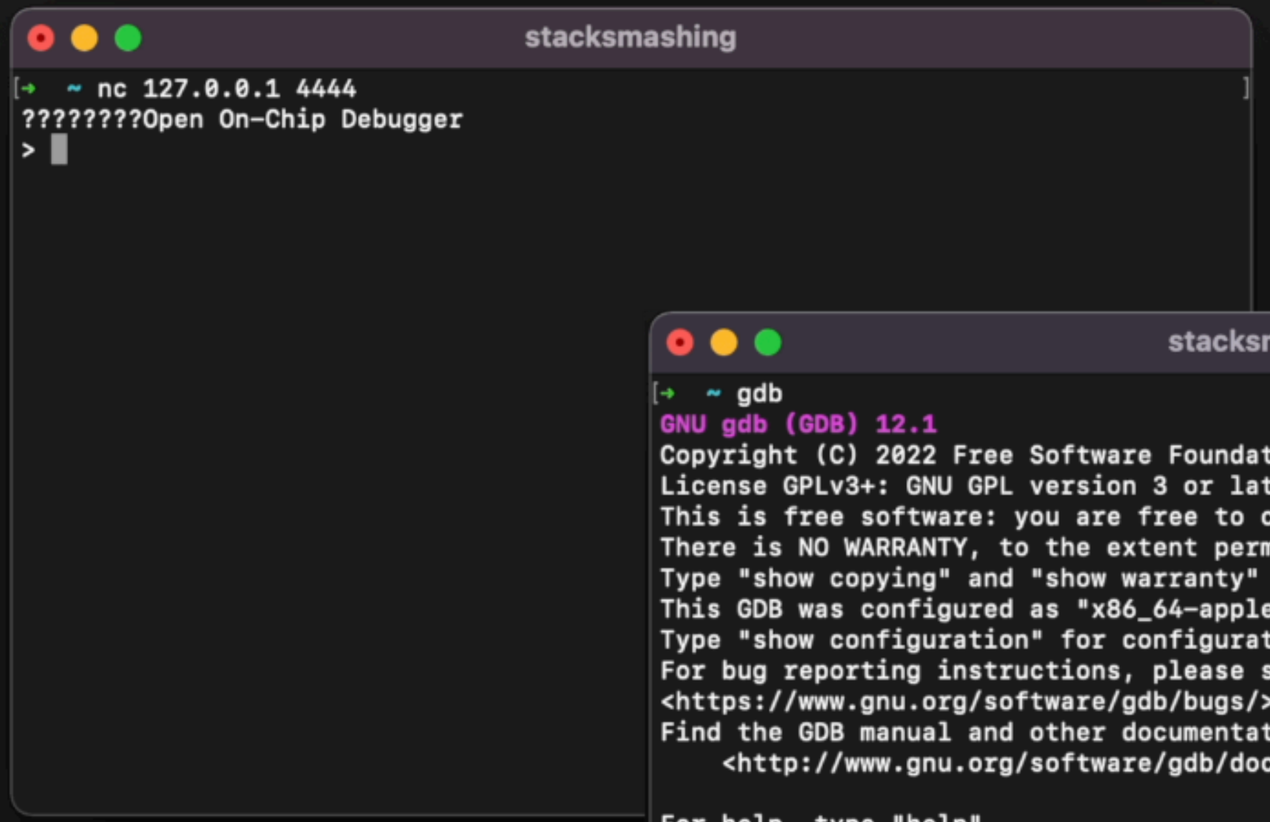
You implement SWD by hand

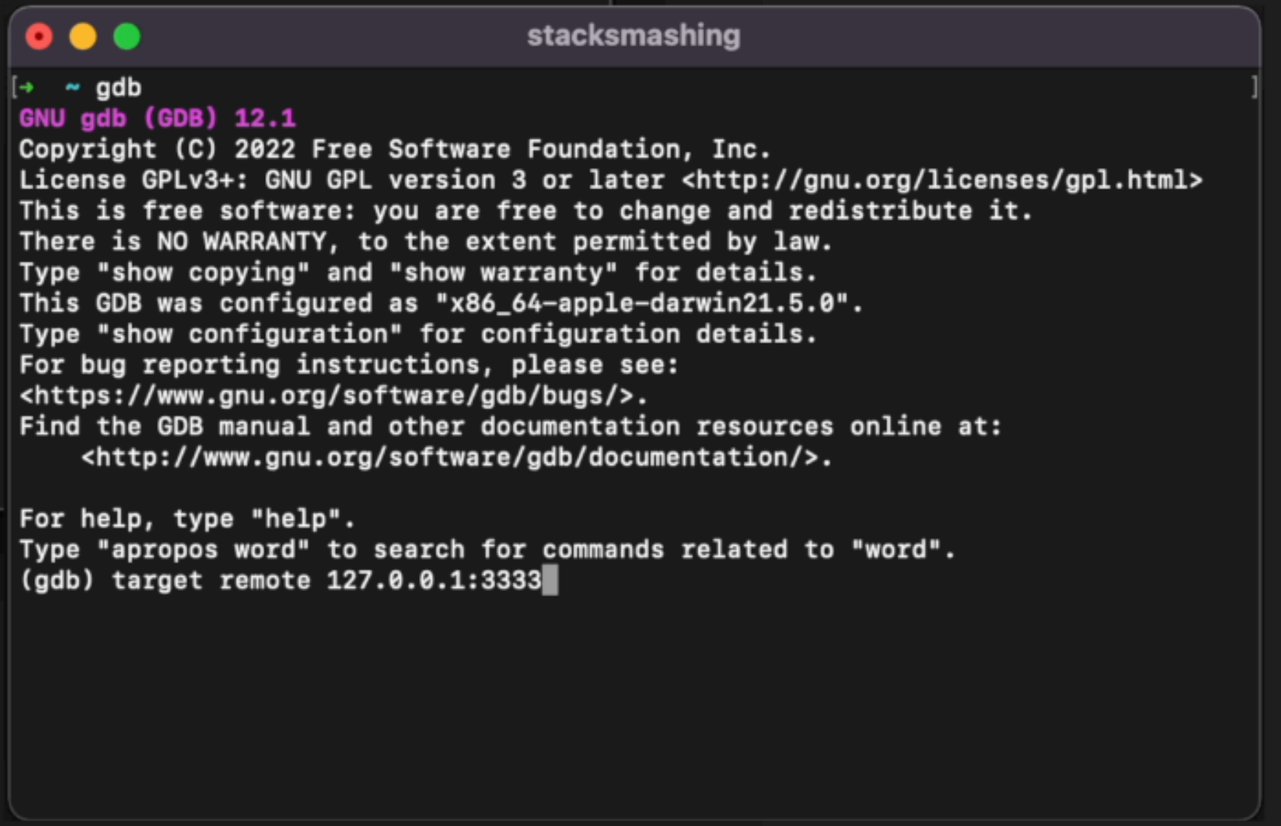
You find a single SWD bit was wrong

You find a single SWD bit was wrong









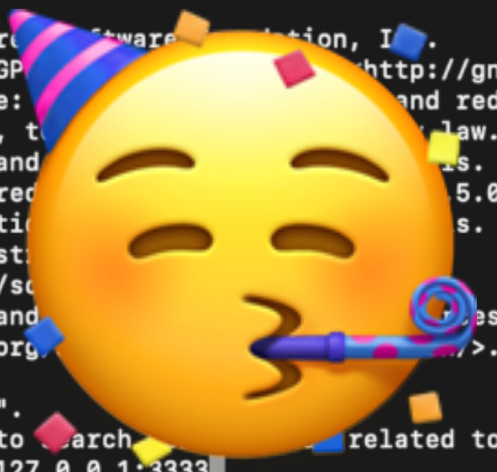
stacksmashing

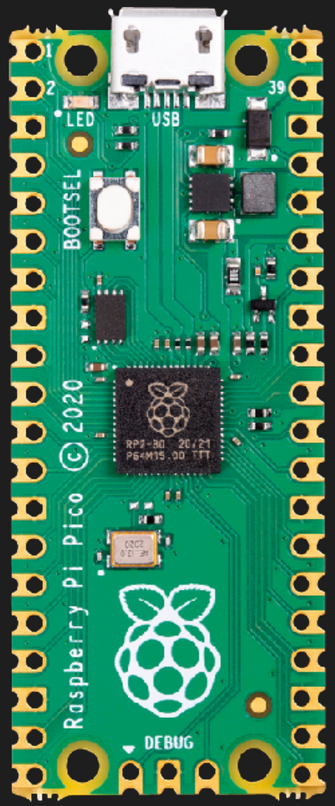
```
[➜  ~ nc 127.0.0.1 4444                                                    ]
????????Open On-Chip Debugger
>
```

stacksmashing

```
[➜  ~ gdb                                                                  ]
GNU gdb (GDB) 12.1
Copyright (C) 2022 Fr                                tion, I .
License GPLv3+: GNU GP                              <http://gnu.org/licenses/gpl.html>
This is free software:                                and redistribute it.
There is NO WARRANTY, t                               law.
Type "show copying" and                               s.
This GDB was configured                               5.0".
Type "show configurati                                s.
For bug reporting inst
<https://www.gnu.org/s
Find the GDB manual and                               es online at:
    <http://www.gnu.org                                >.

For help, type "help".
Type "apropos word" to search                         related to "word".
(gdb) target remote 127.0.0.1:3333
```





- SDQ bridge
  - Supporting DCSD & JTAG
- iPhone compatible debug probe
- Fully open-source

Kanzi

Kanzi

Bonobo

Kanzi

Chimp

Bonobo

Kanzi

Kong

Chimp

Bonobo

Kanzi

Kong

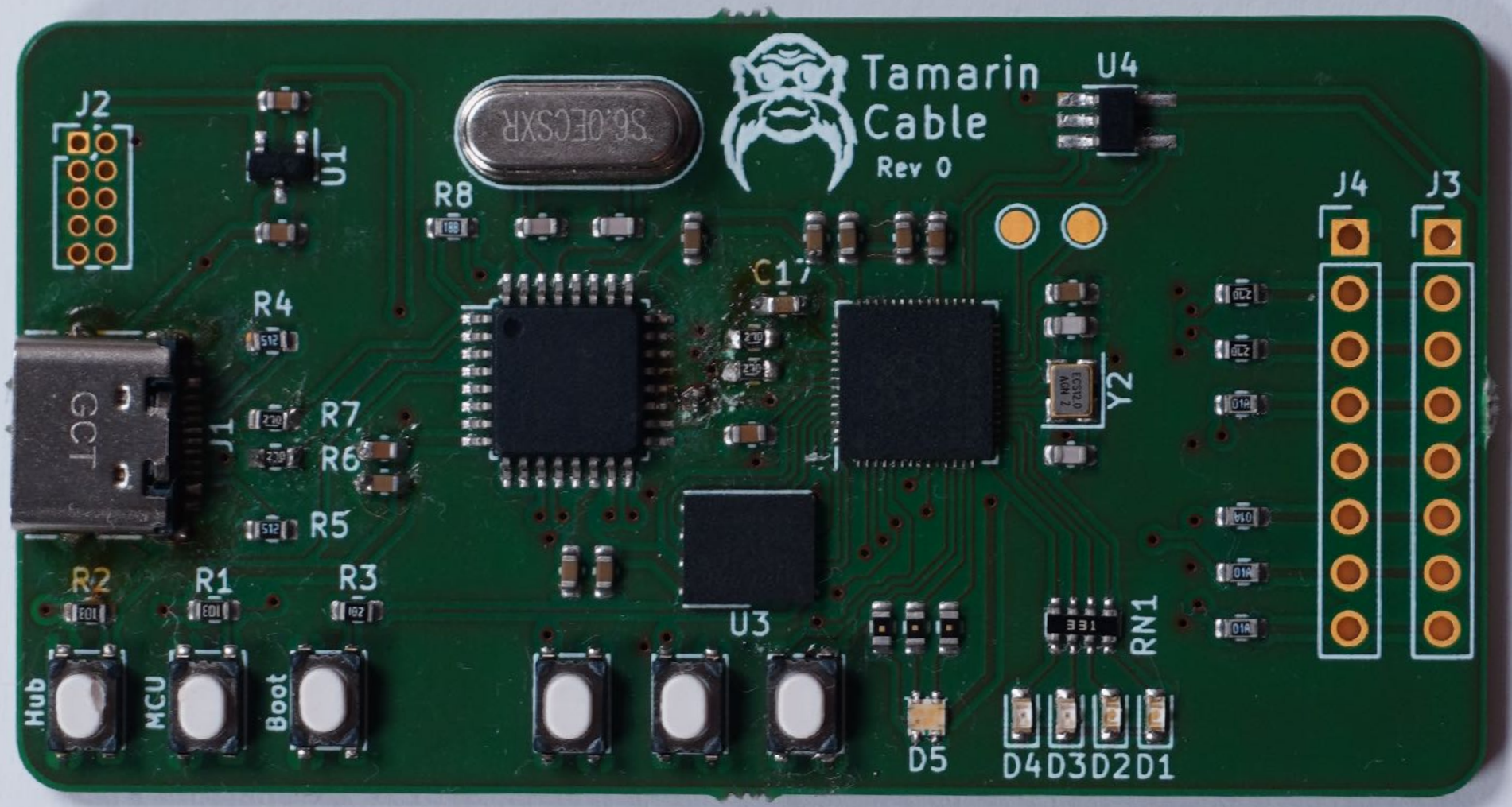
Chimp

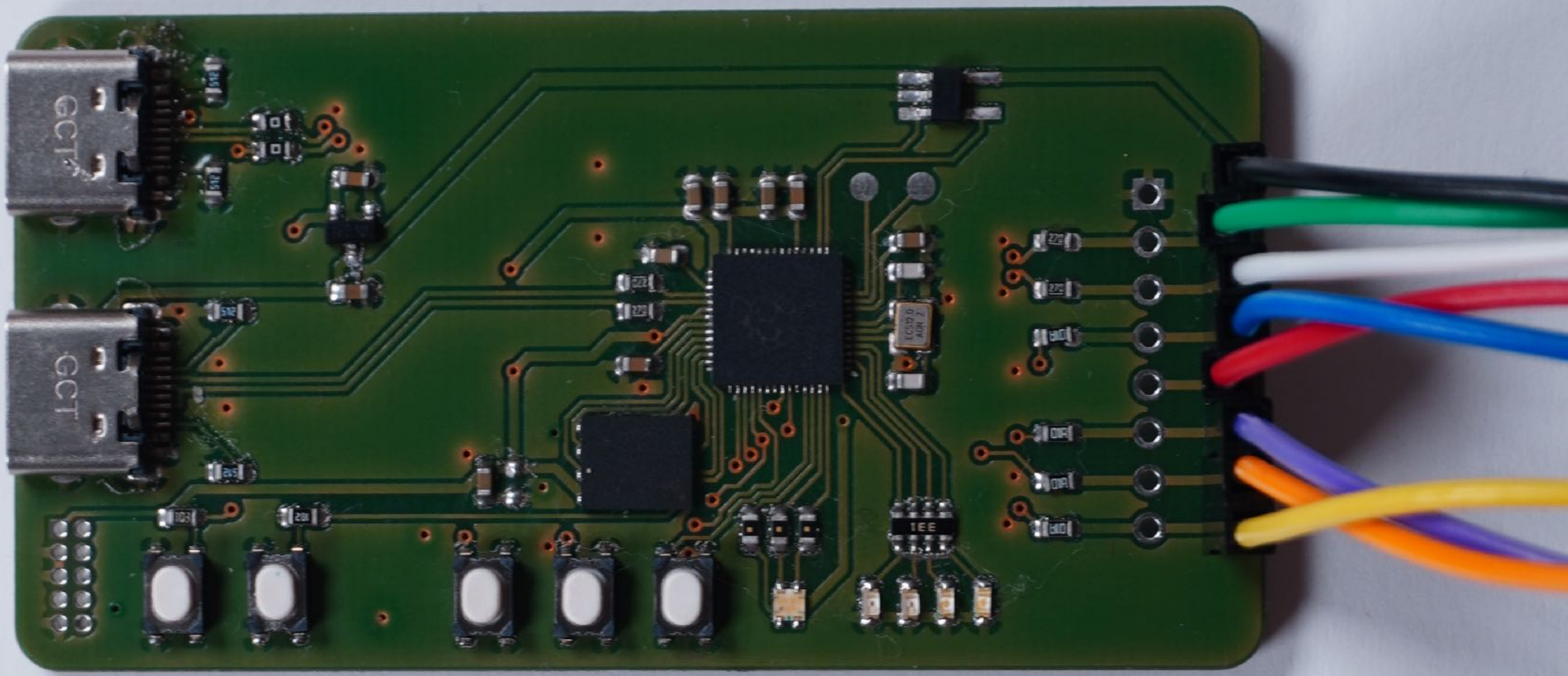
Tamarin Cable

Bonobo

Tamarin Cable

github.com/stacksmashing/tamarin-firmware





Releases

- You can find everything on github.com/stacksmashing
  - Tamarin Cable Firmware
  - Forked OpenOCD
  - Forked swd-analyzer
  - SDQAnalyzer

Thank you!

- youtube.com/stacksmashing
- @ghidraninja
- contact@stacksmashing.net