The hitchhacker’s guide to iPhone Lightning & JTAG hacking

by stacksmashing

About me: stacksmashing

- Security researcher

- youtube.com/stacksmashing
- @ghidraninja



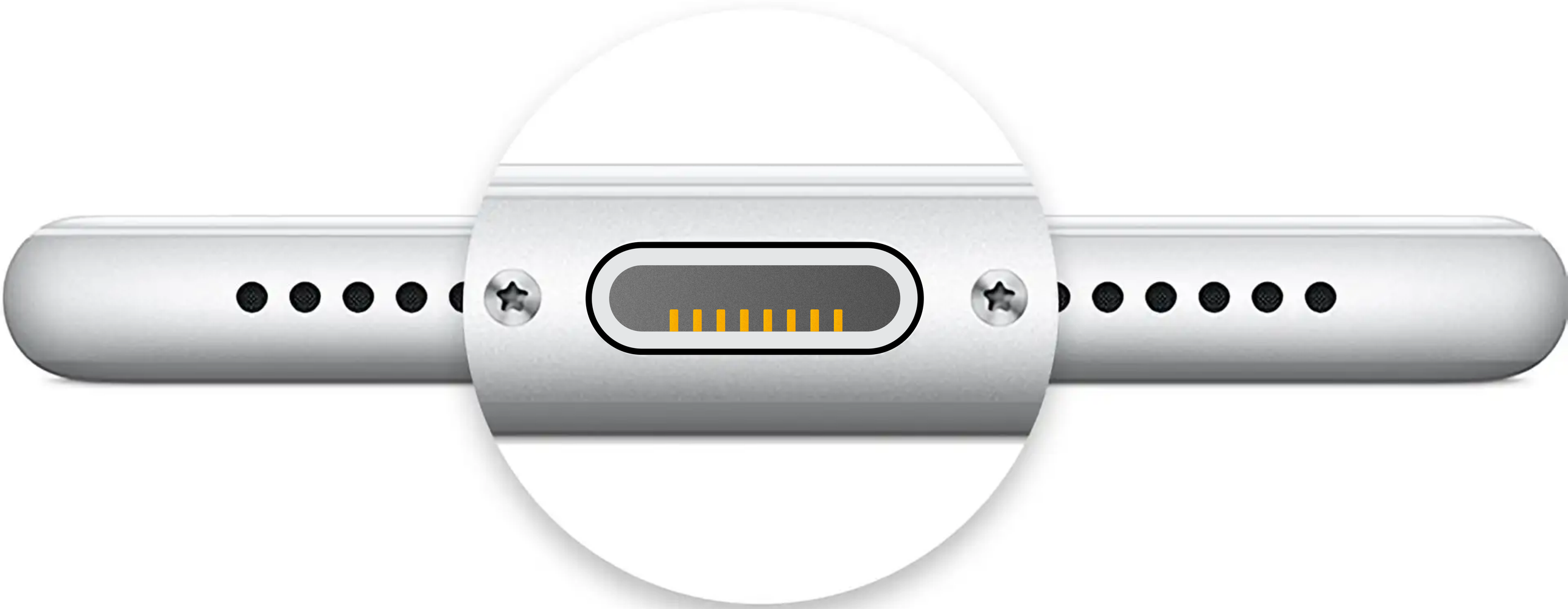
Thanks!

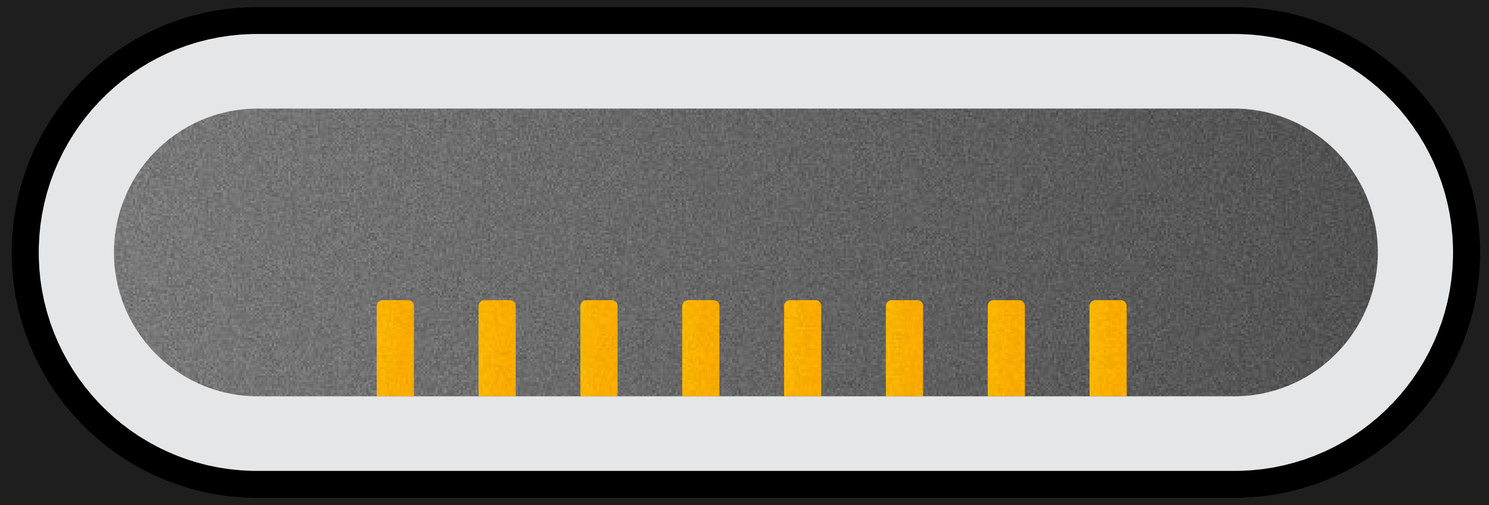
As always: Standing on the shoulders of giants

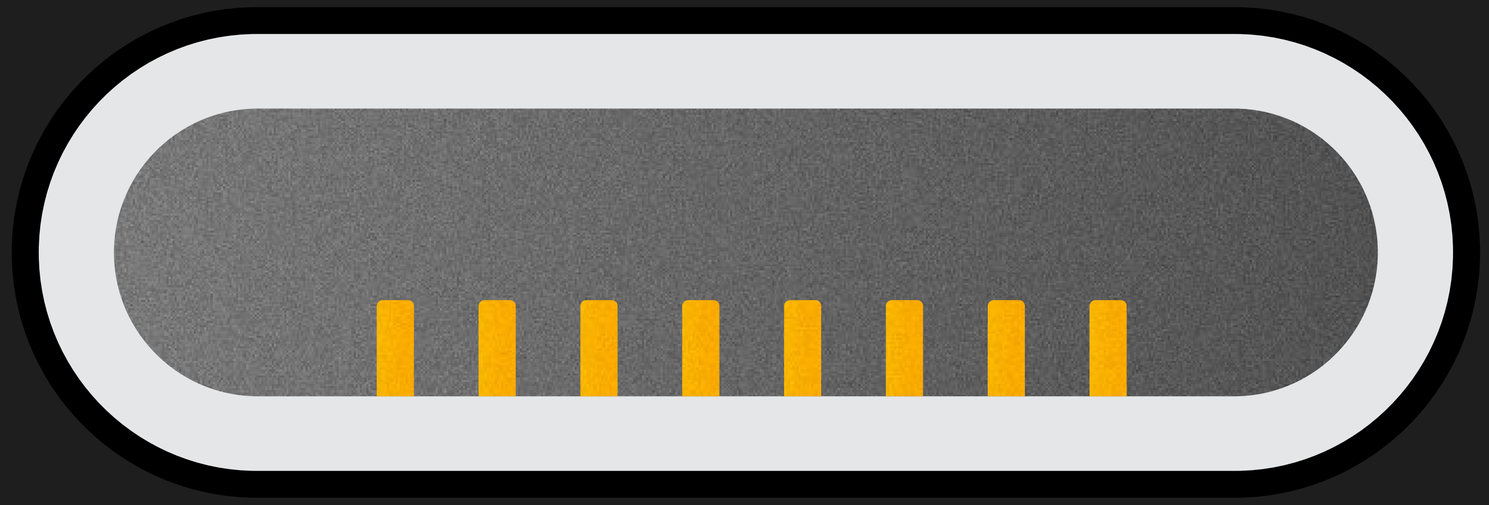
- Carlo Maragno - @CarloMara1
- Jiska Classen
- Fabian Freyer
- Caro Gross
- Lily - @bendycatus
- John - @nyan_satan
- LambdaConcept
- Elliot

Lightning?

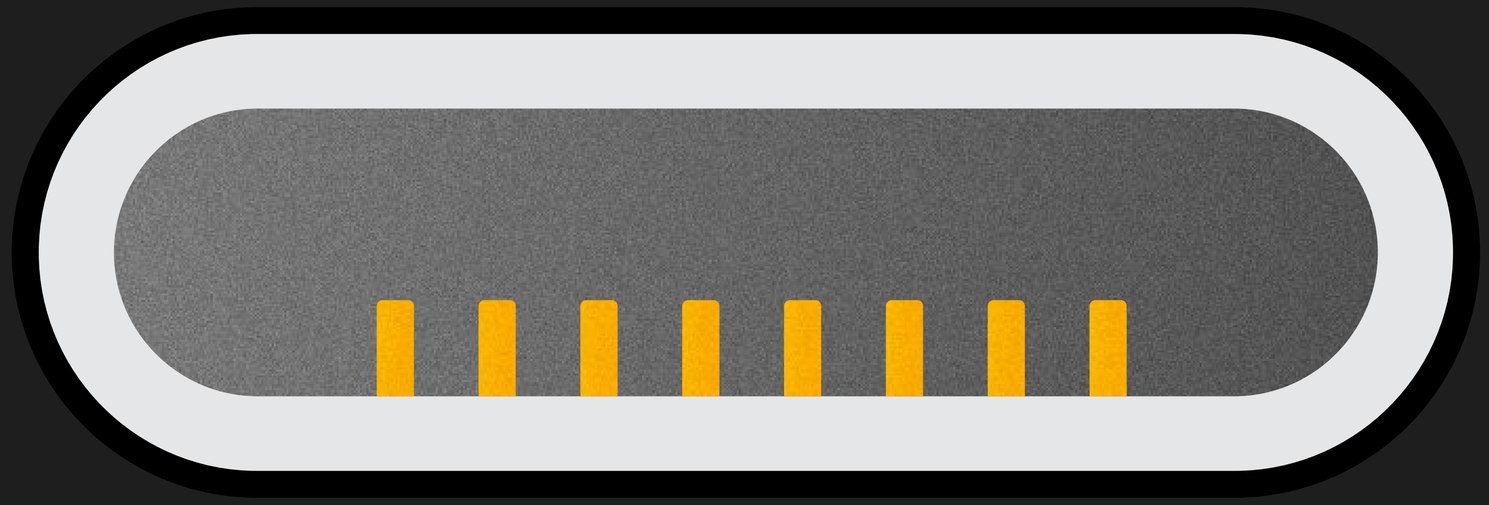






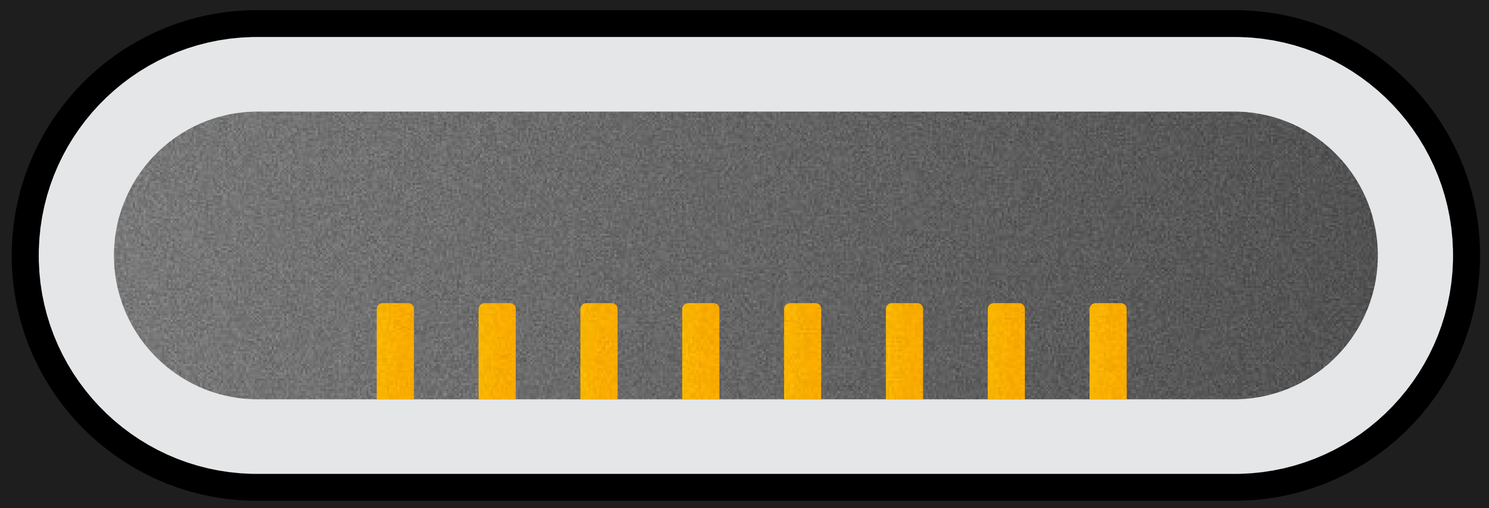

1 2 3 4 5 6 7 8

Charging



1 2 3 4 5 6 7 8

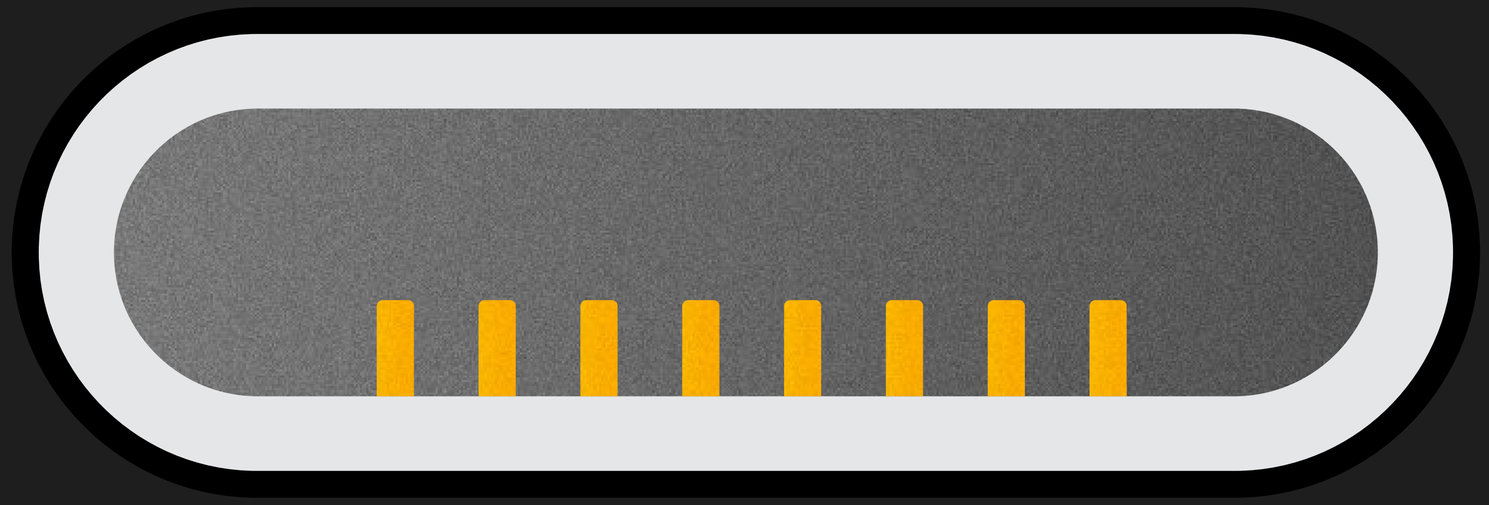
Charging



Data transfer

Audio

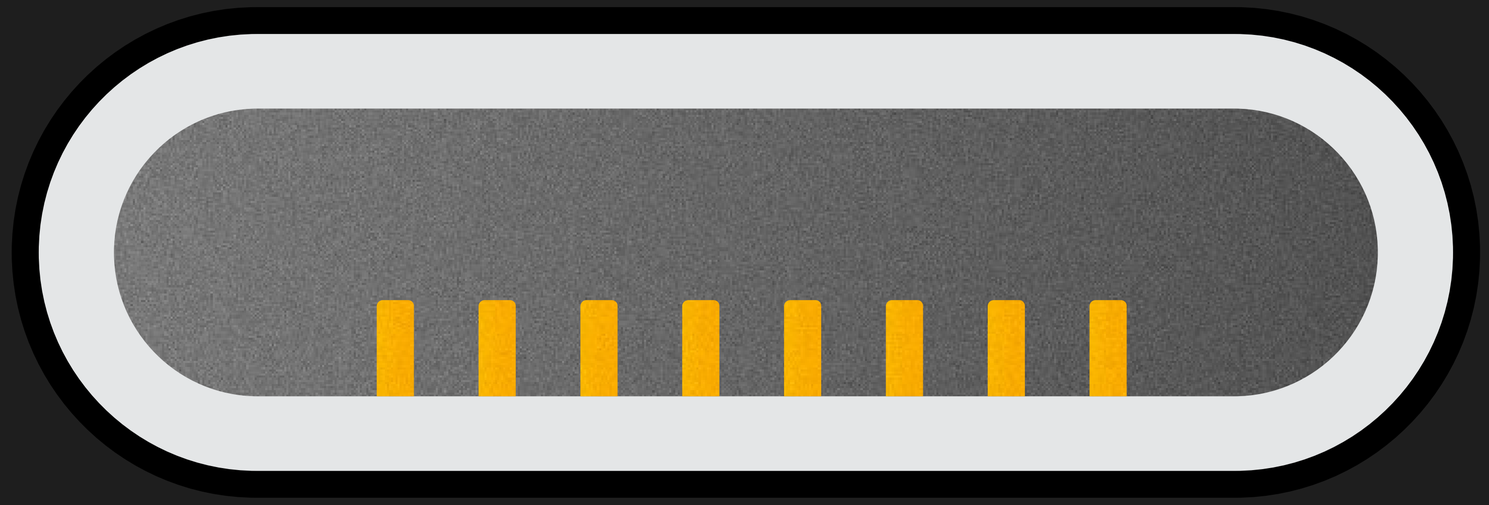
Charging



Data transfer

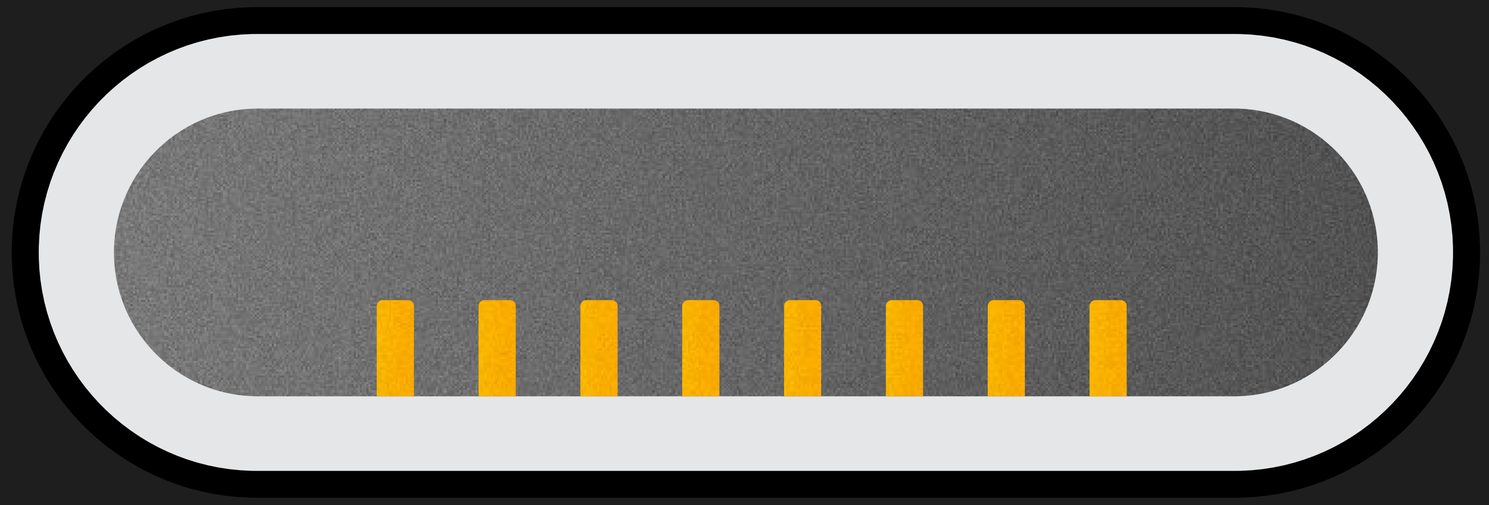
Audio

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

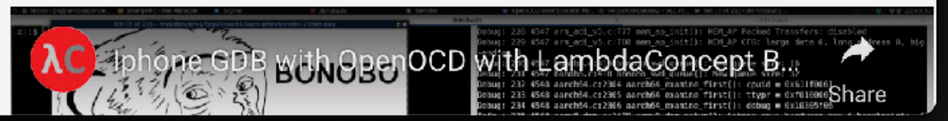
iPhone debugging requires proper tools.

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

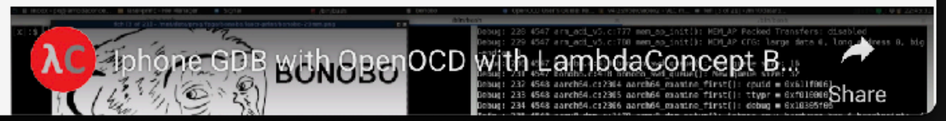
iPhone debugging requires proper tools.

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.

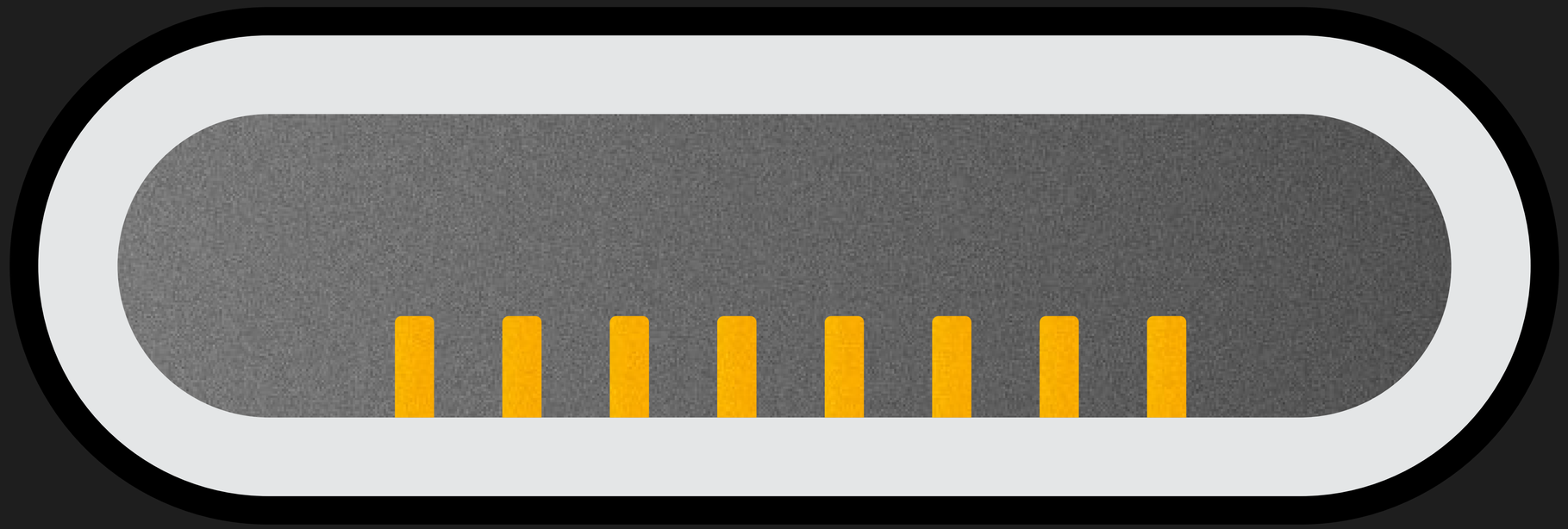
The target serial console can be accessed on the control PC through Minicom (iBoot prompt), as well as Lightning USB (For DFU, USB exploitation, demote, etc.)

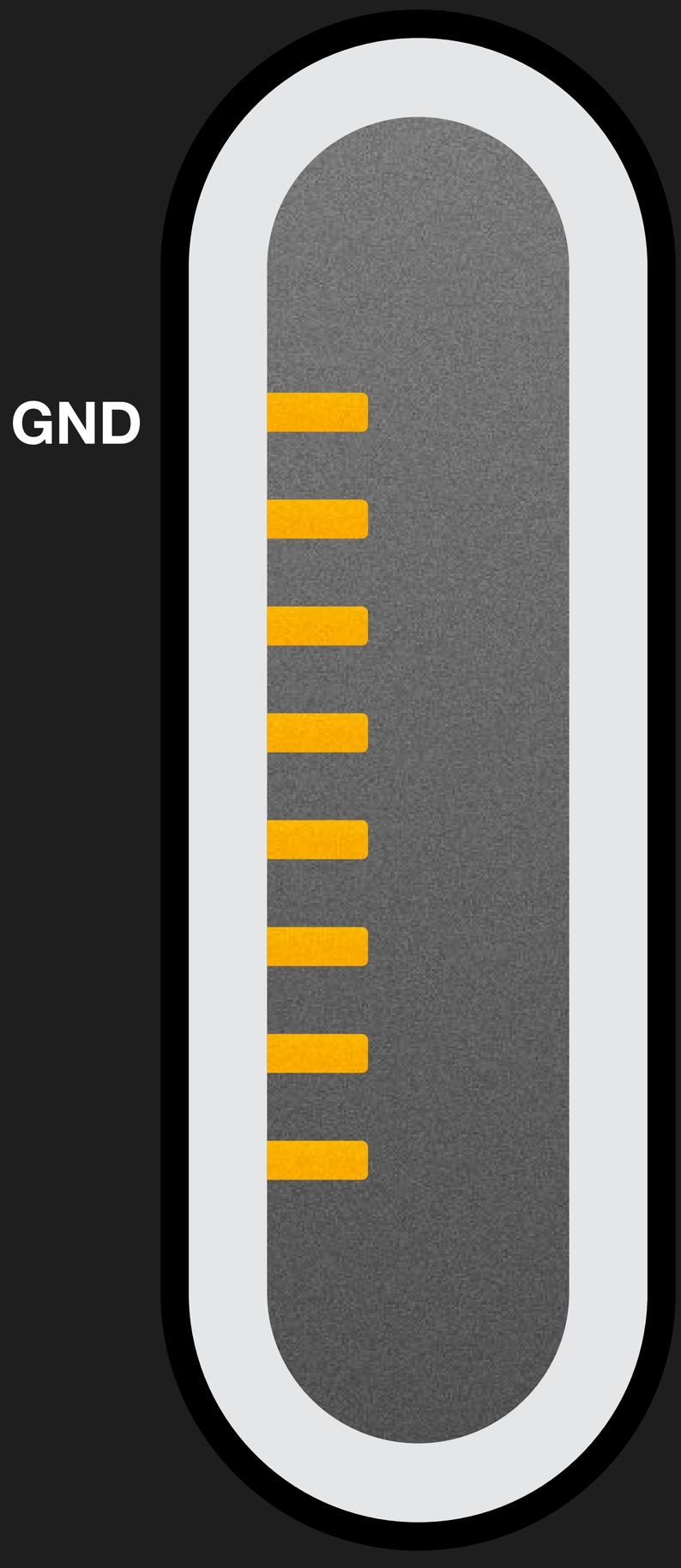
More Here

Demonstration:

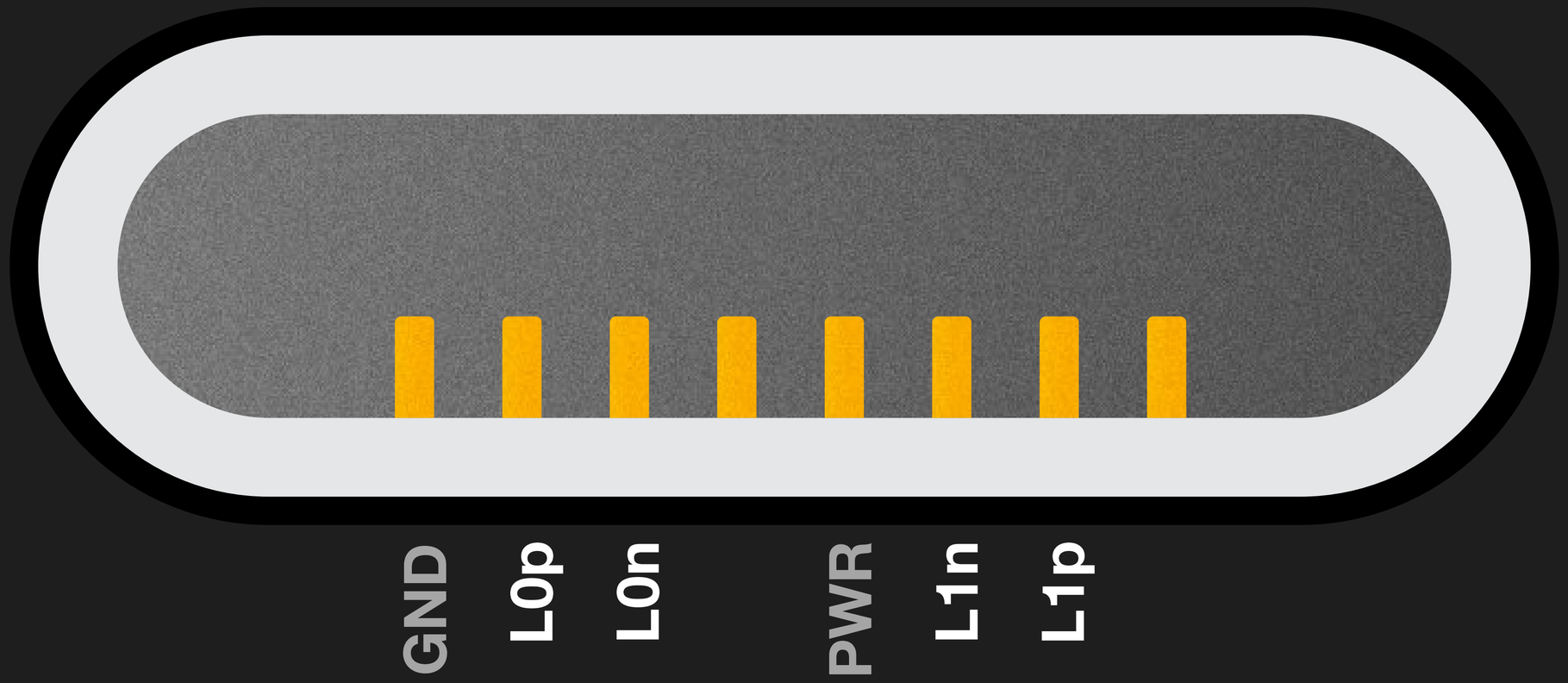


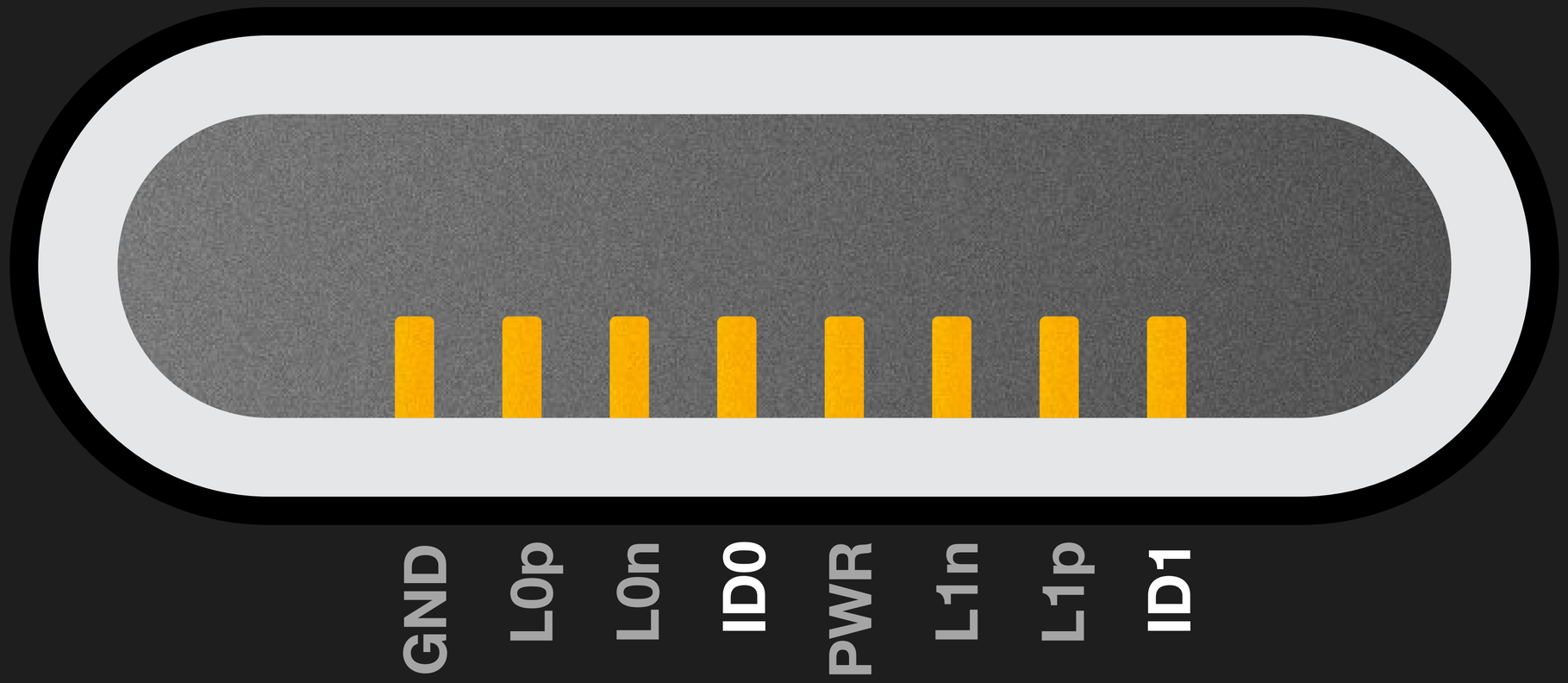
Let’s build our own!

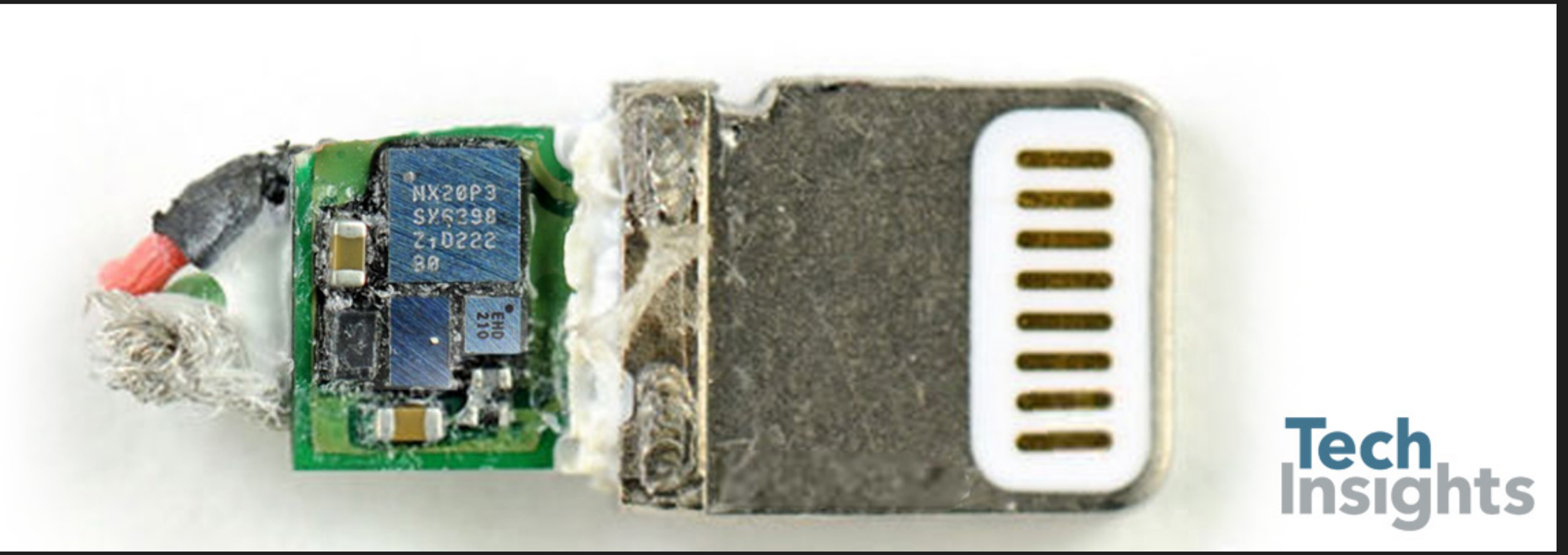


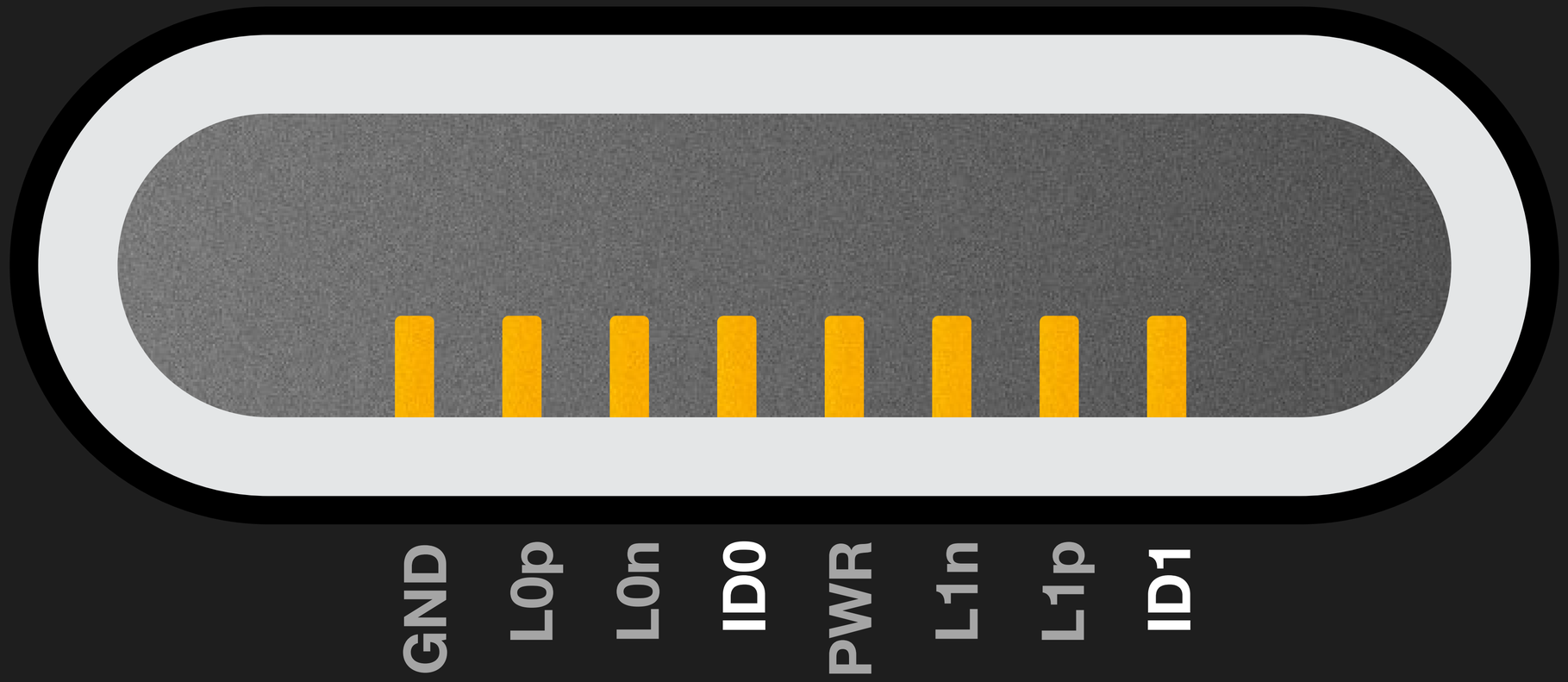

GND


GND
PWR

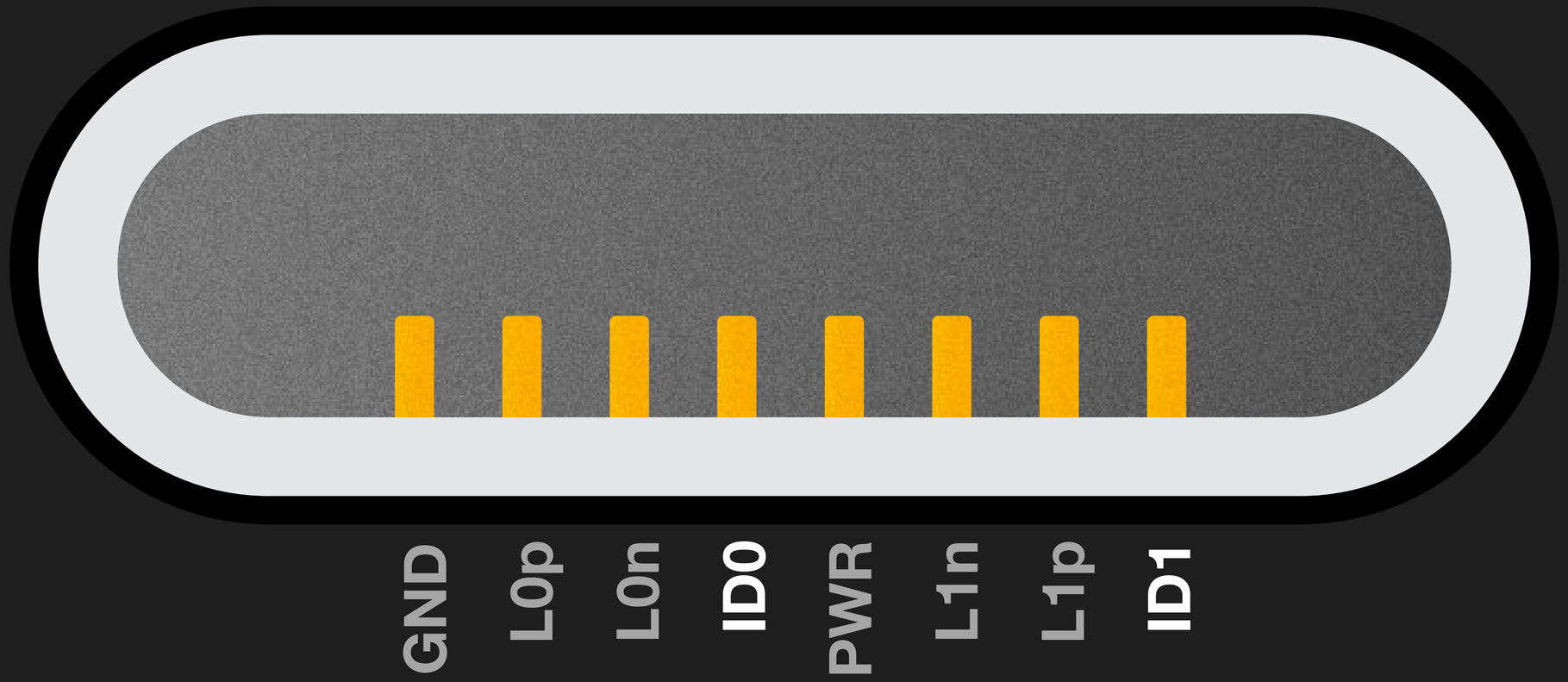

GND
L0p
L0n
PWR
L1n
L1p


GND
L0p
L0n
ID0
PWR
L1n
L1p
ID1

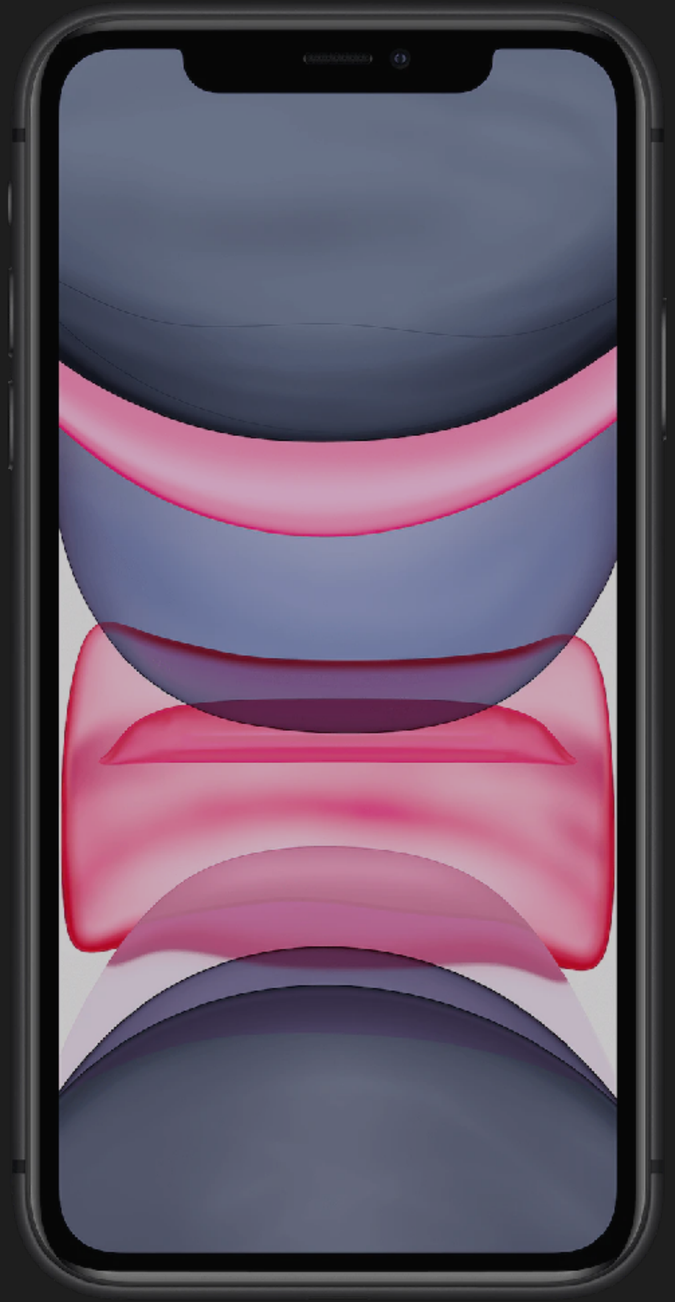

NX20P3
SX6298
Z1D222
B0
EHD
210
Tech
Insights

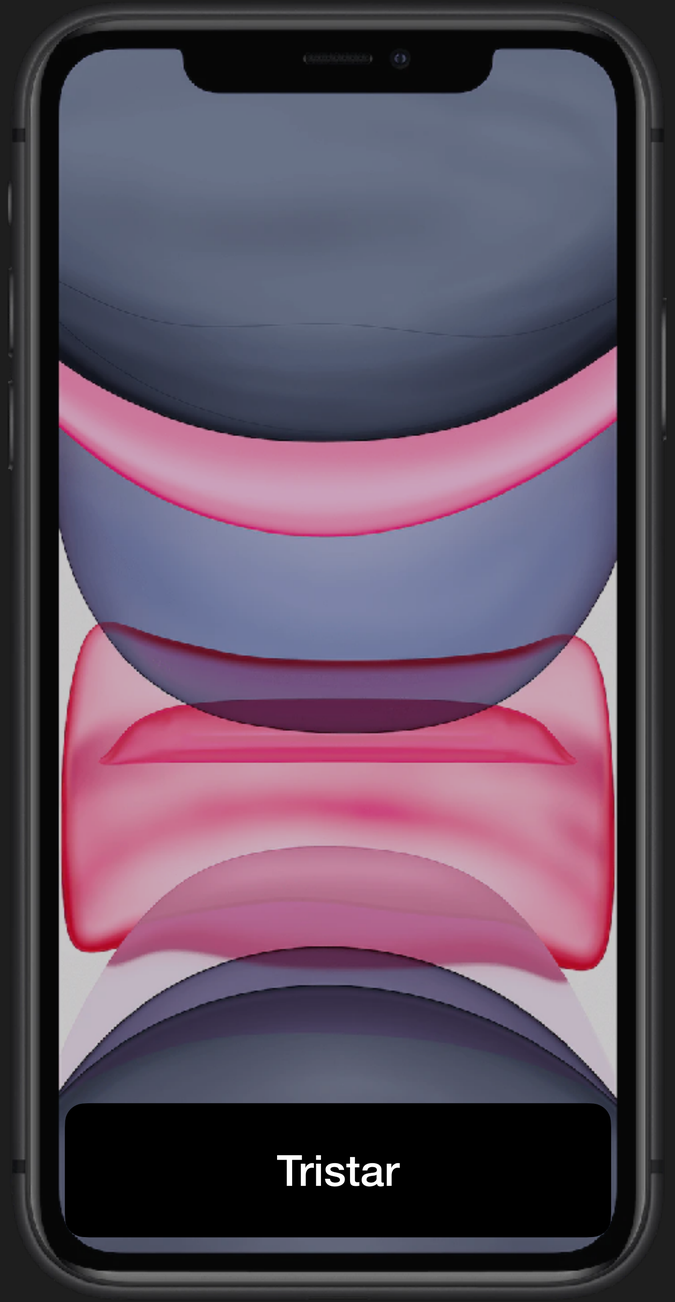


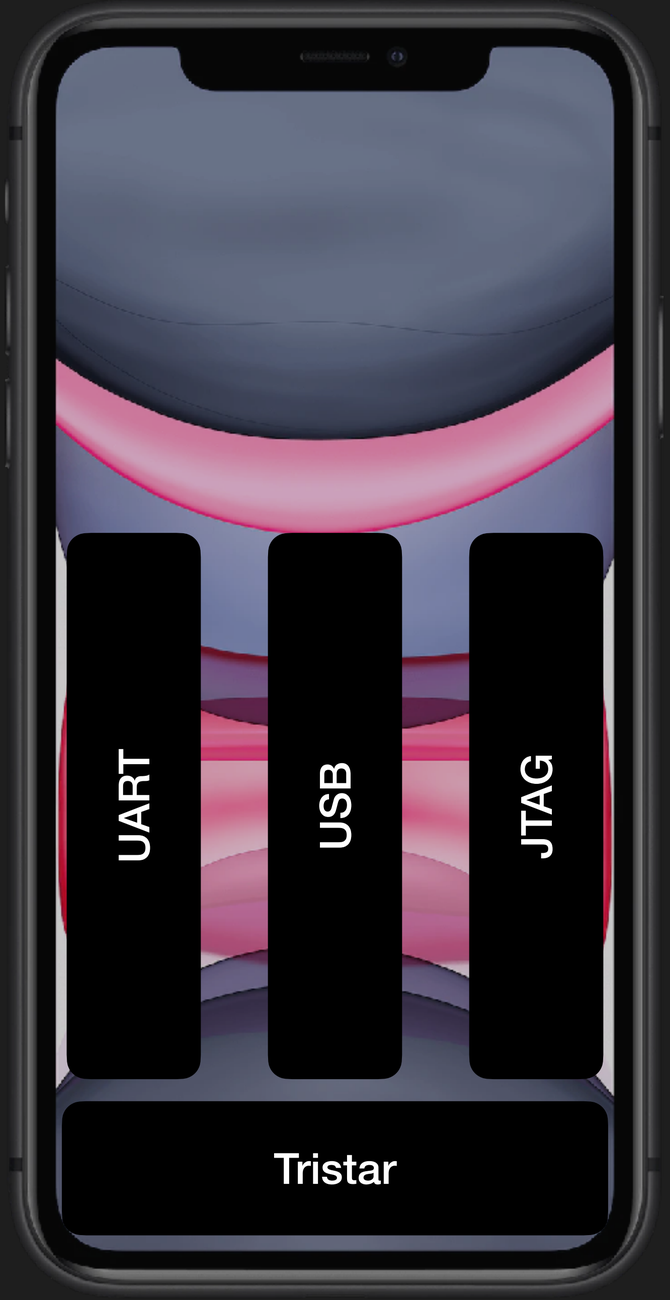
SDQ or IDBUS

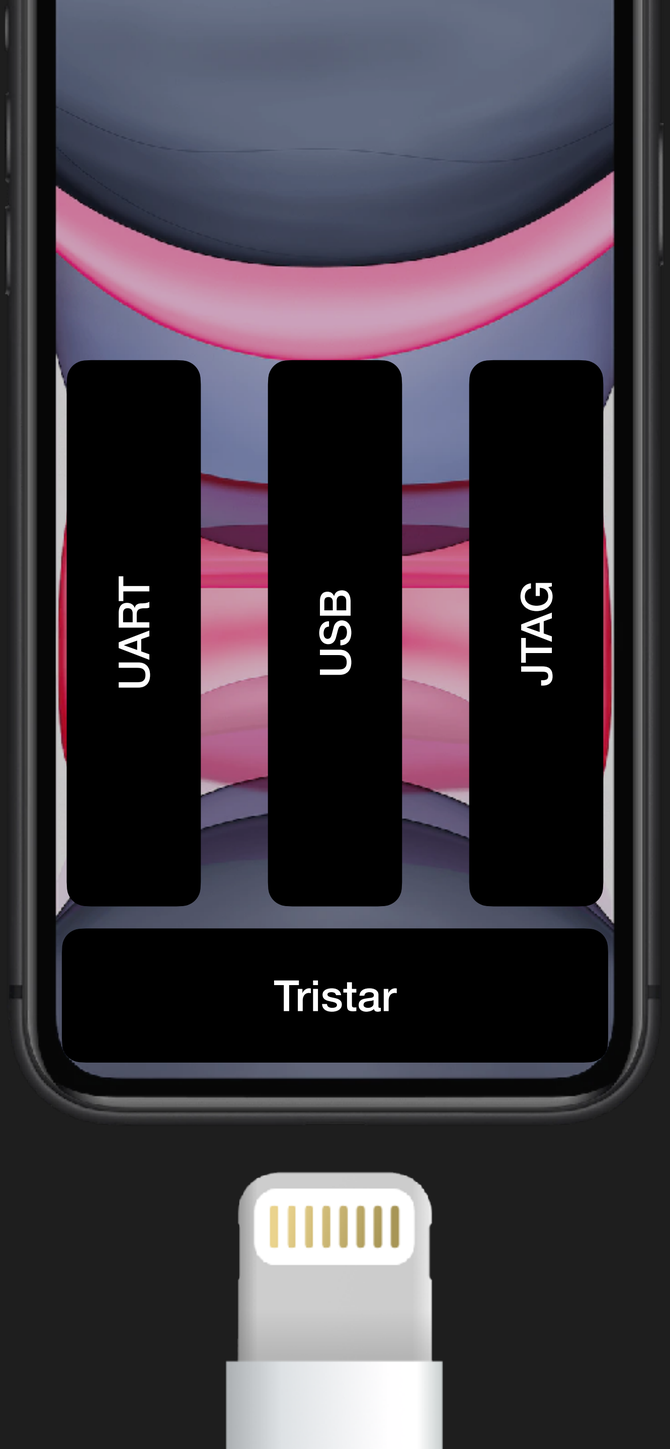


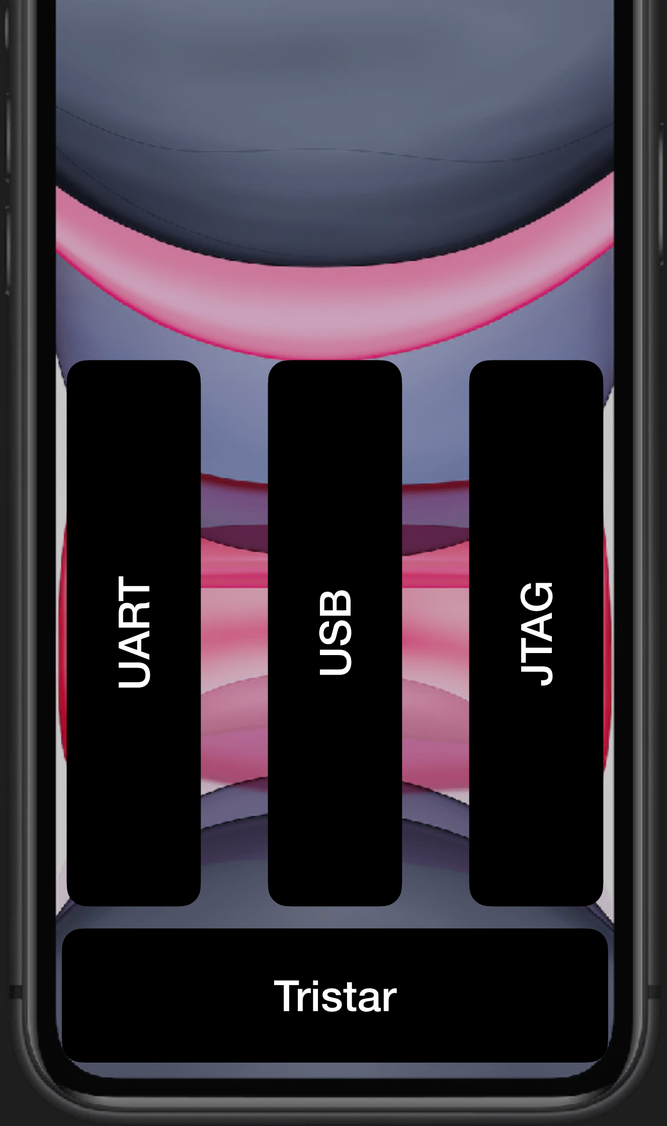
SDQ or IDBUS




Tristar

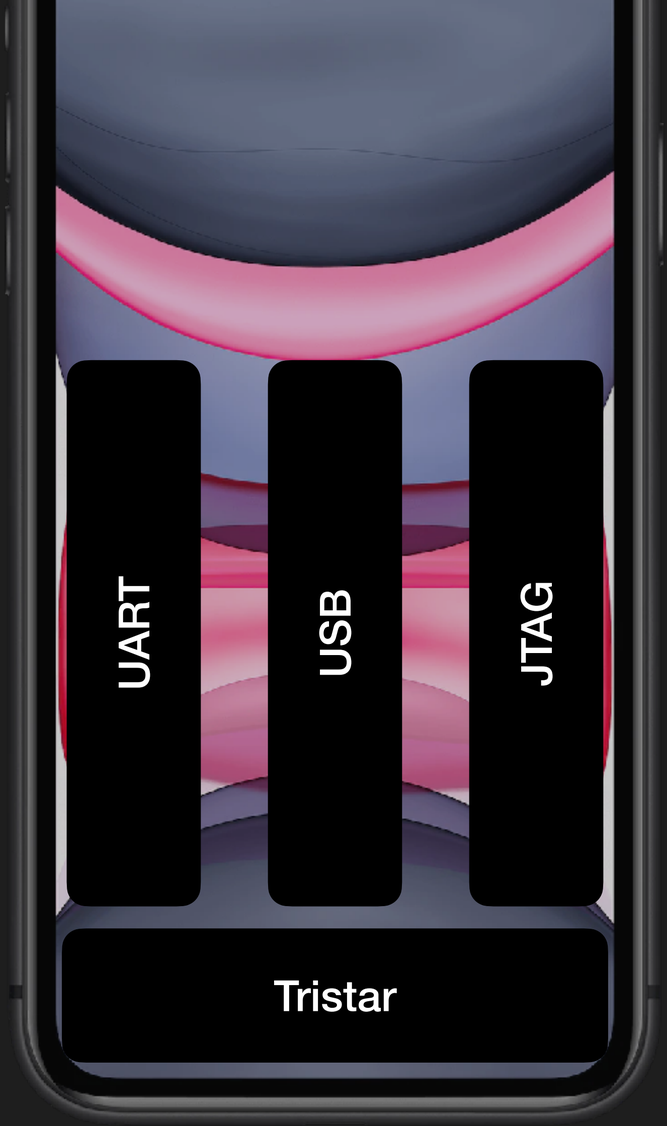

UART
USB
JTAG
Tristar


UART
USB
JTAG
Tristar





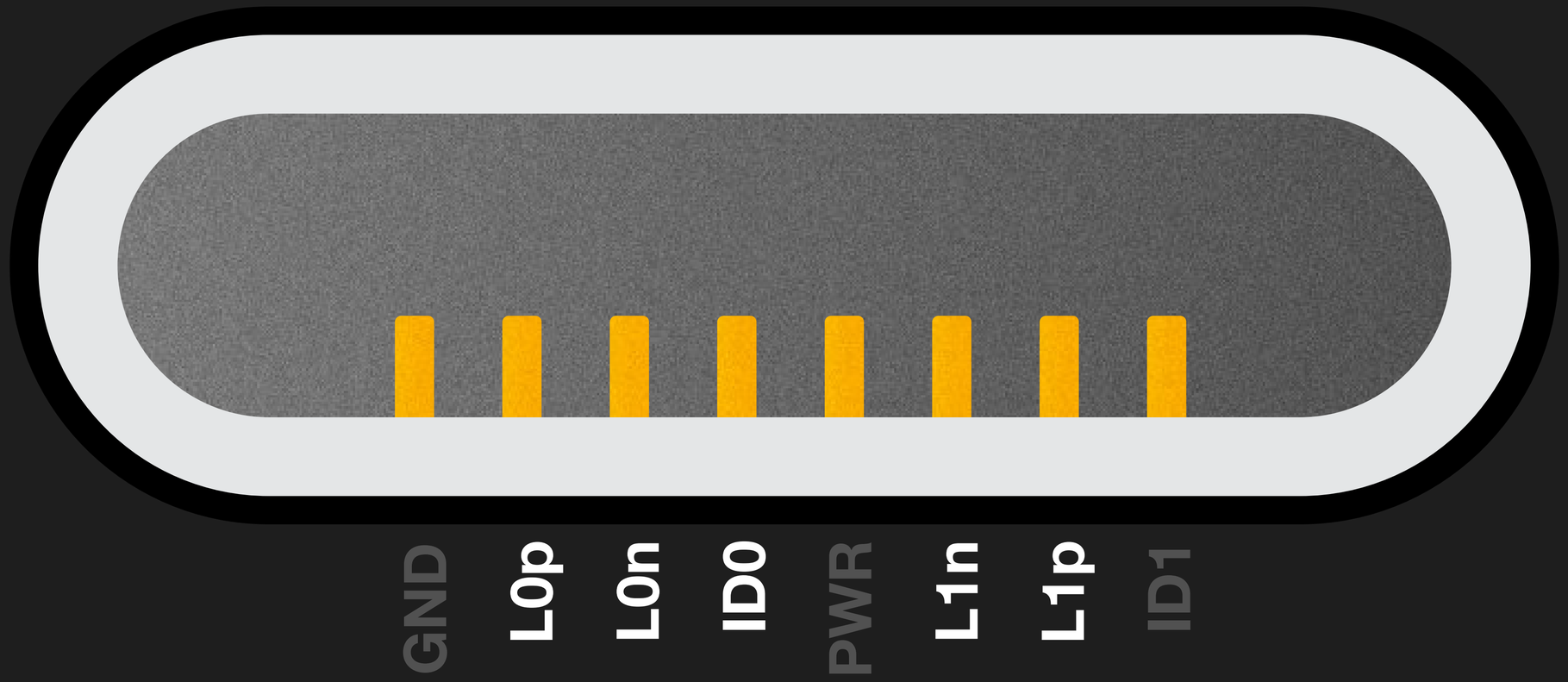
What do you want?

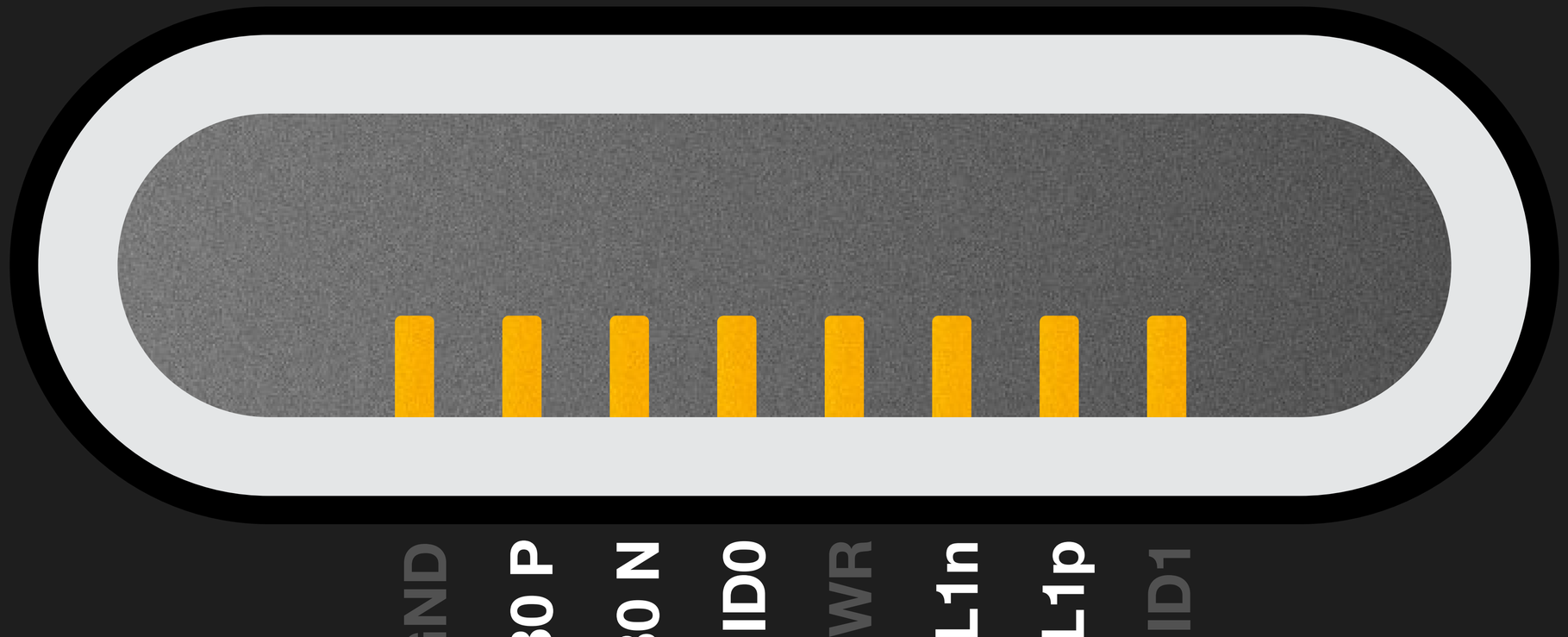


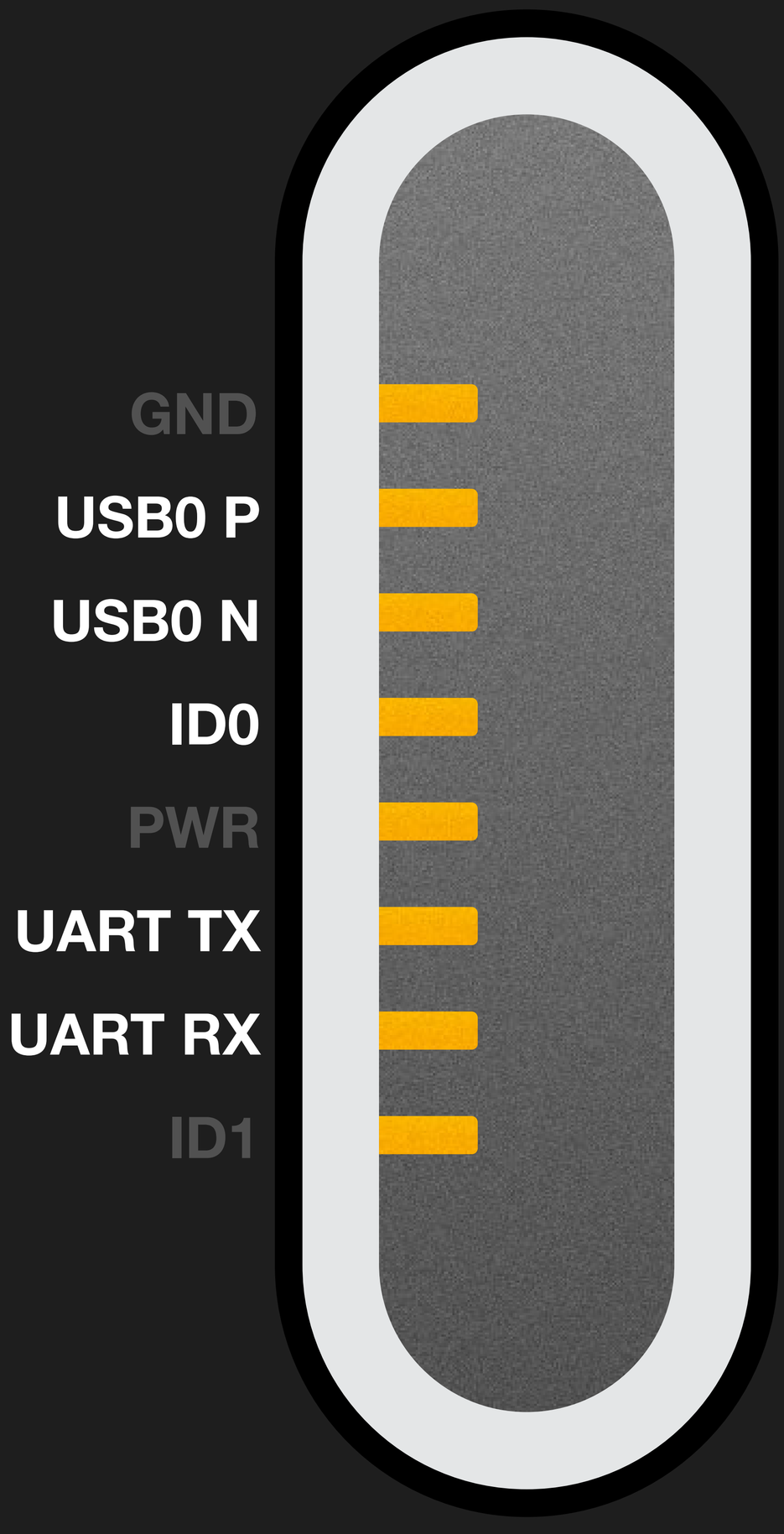


What do you want?

Speak USB plz


GND
L0p
L0n
ID0
PWR
L1n
L1p
ID1


GND
USB0 P
USB0 N
ID0
PWR
L1n
L1p
ID1

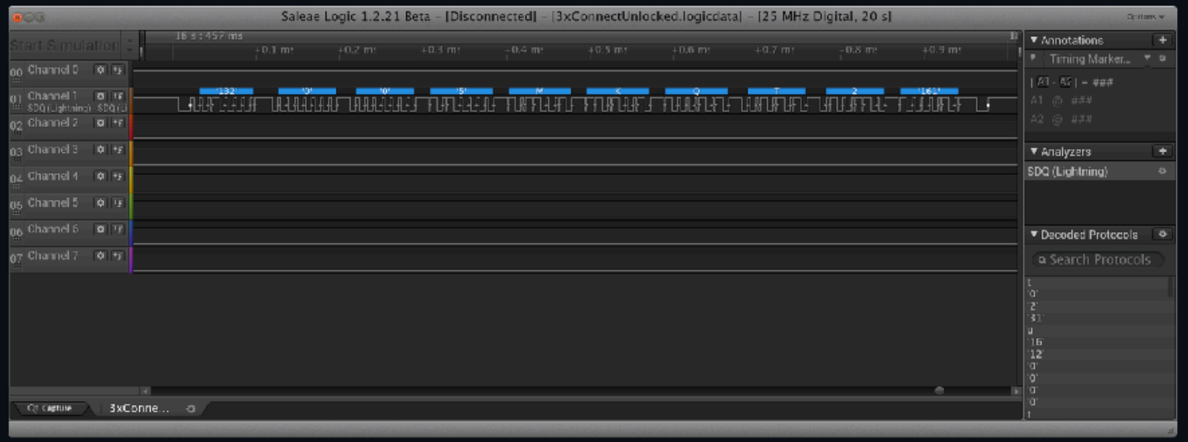

GND
USB0 P
USB0 N
ID0
PWR
UART TX
UART RX
ID1

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

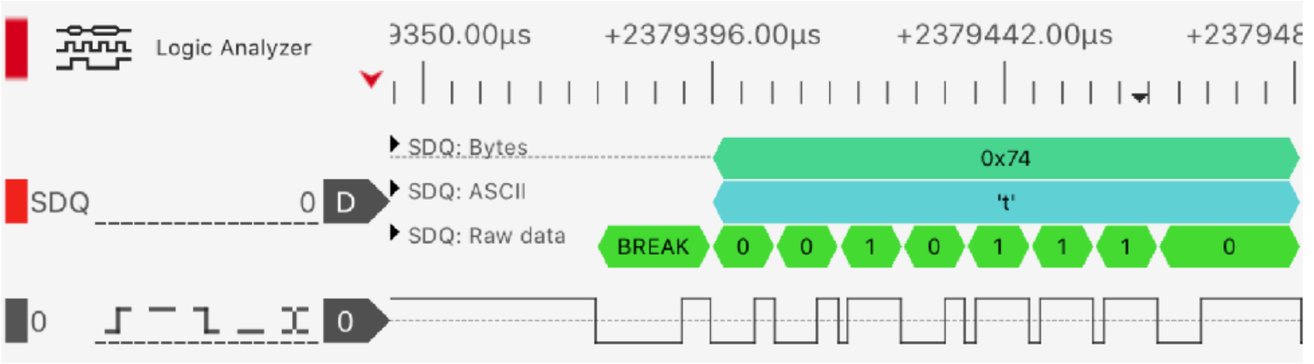
- **Marcus10110** Mark
- **nezza** Thomas Roth
- **ianrrees** Ian
- **nbanerje** Neel Banerjee

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

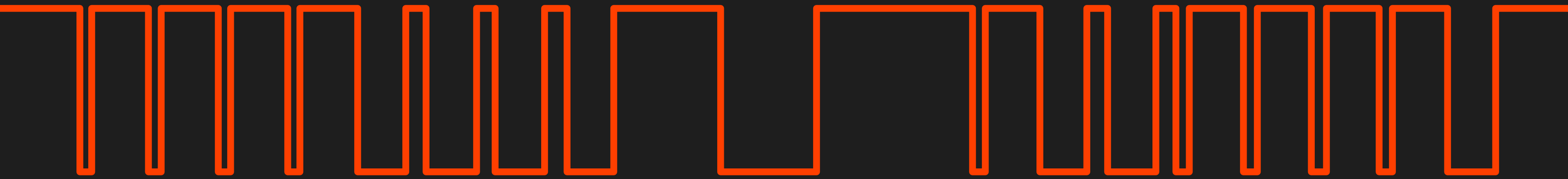
First connect logic analyzer's channels to both **ID** lines of the breakout (pins 4 and 8) and connect the

SDQ or IDBUS

Simple one-wire protocol

SDQ or IDBUS

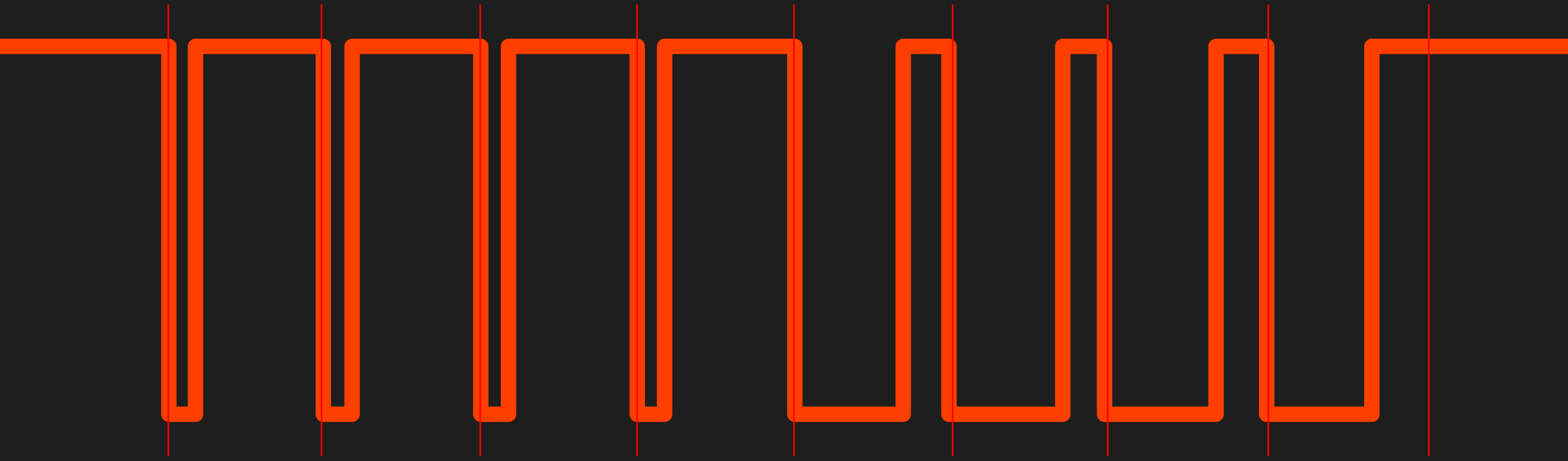
Simple one-wire protocol



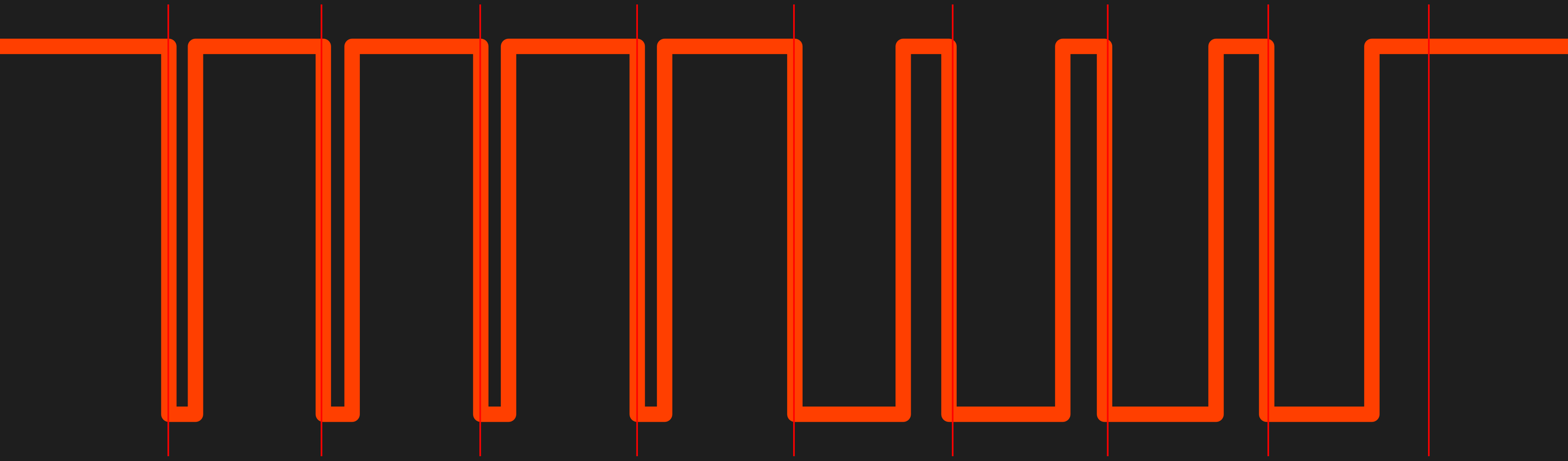
SDQ or IDBUS



SDQ or IDBUS

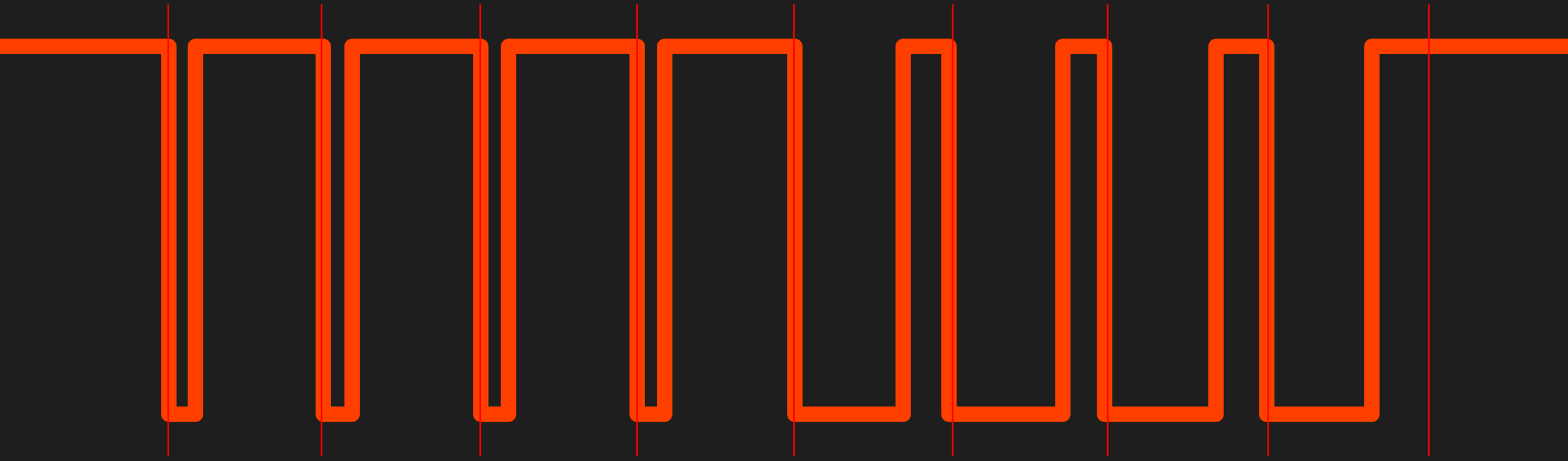


SDQ or IDBUS



1 1 1 1 0 0 0 0

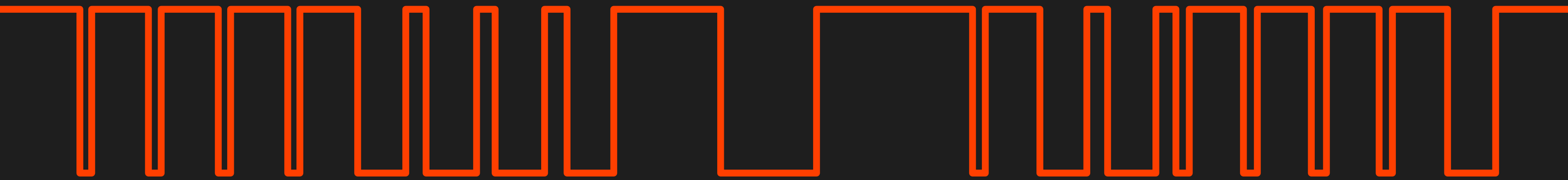
SDQ or IDBUS



1 1 1 1 0 0 0 0

0x0F

SDQ or IDBUS



SDQ or IDBUS

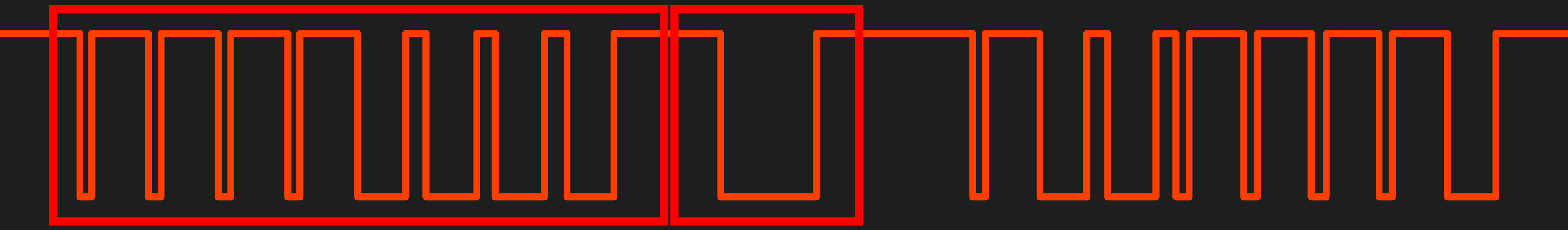




0x0F

SDQ or IDBUS



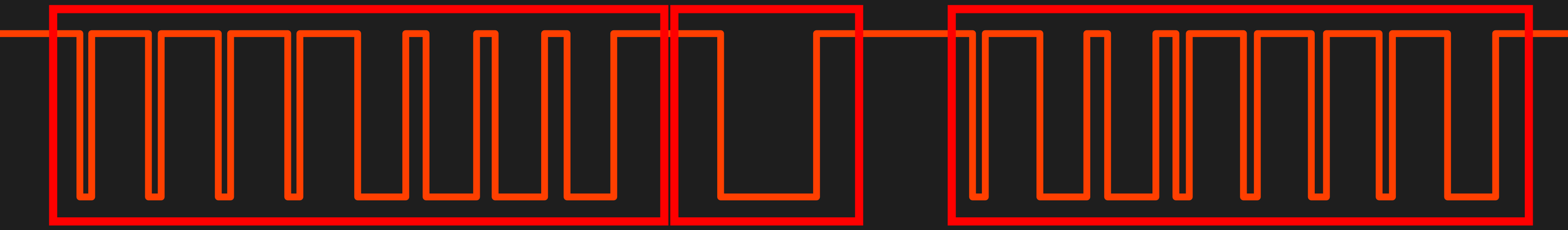


0x0F Break

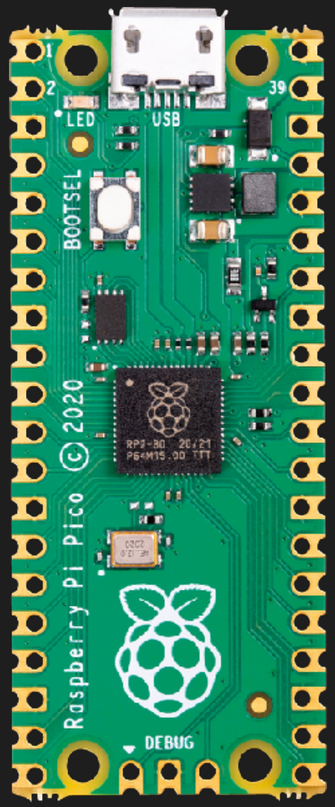
SDQ or IDBUS

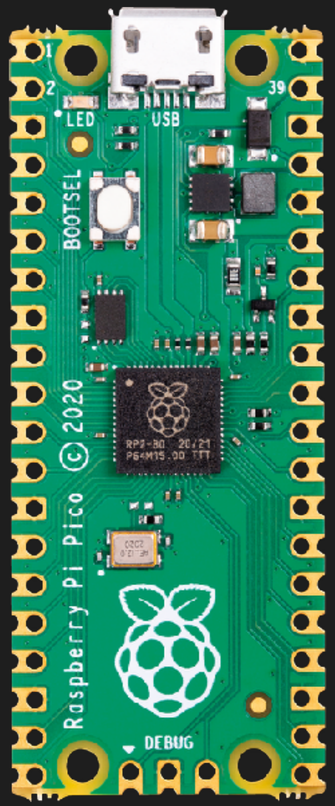






0x0F Break 0x79

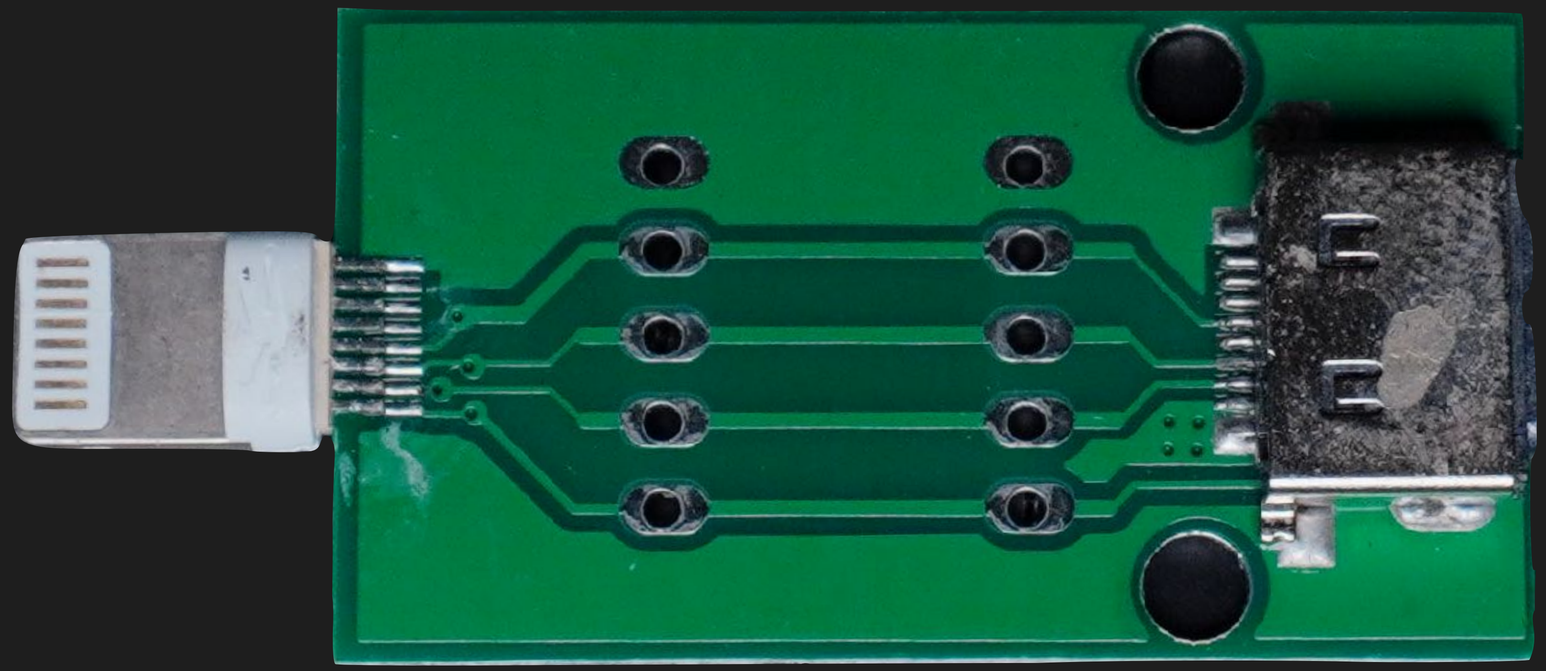

1
2
39
LED
USB
BOOTSEL
Raspberry Pi Pico © 2020
DEBUG



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



But we need a Lightning connector…




saleae
esc
caps lock
shift
fn
control
option

Private

amazon.de

amazon.de Deliver to United States All lightning verlängerung Hello, Sign in Account & Lists Returns & Orders 0 Shopping-Basket

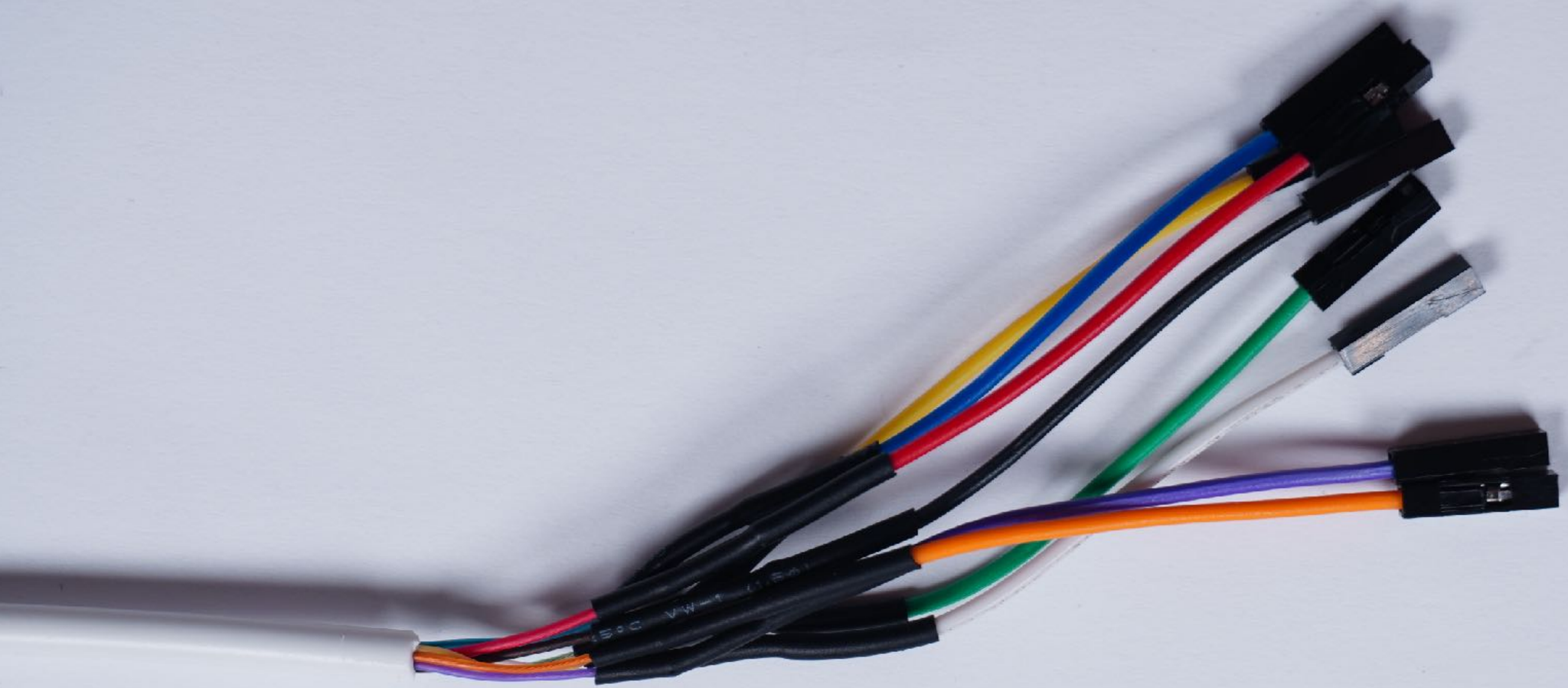


OKCS Originals Extension Cable 1 Metre Compatible with iPhone11, 11 Pro, 11 Max, XR, XS, XS Max, X, 8, 8 Plus, 7, 7 Plus etc. - White

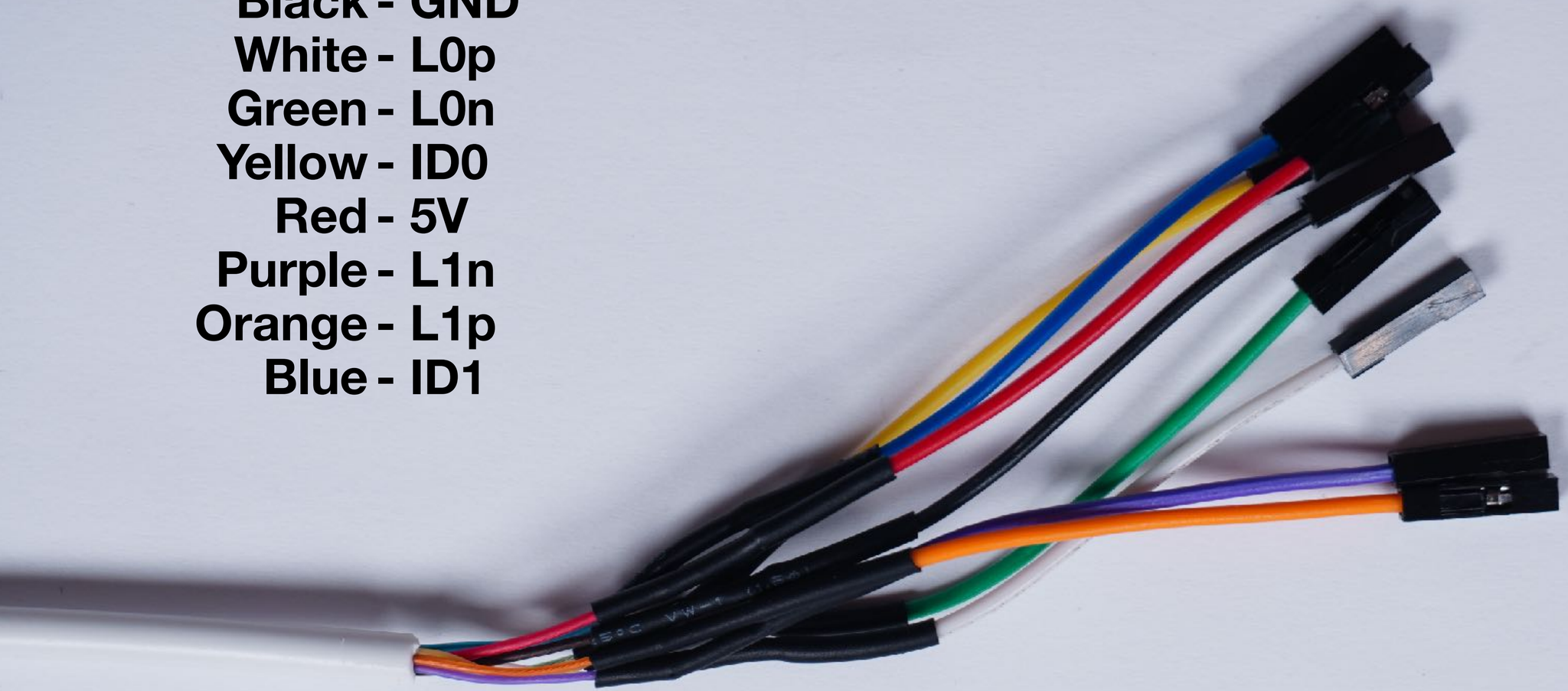
Colour Name:8 pin extender cable.

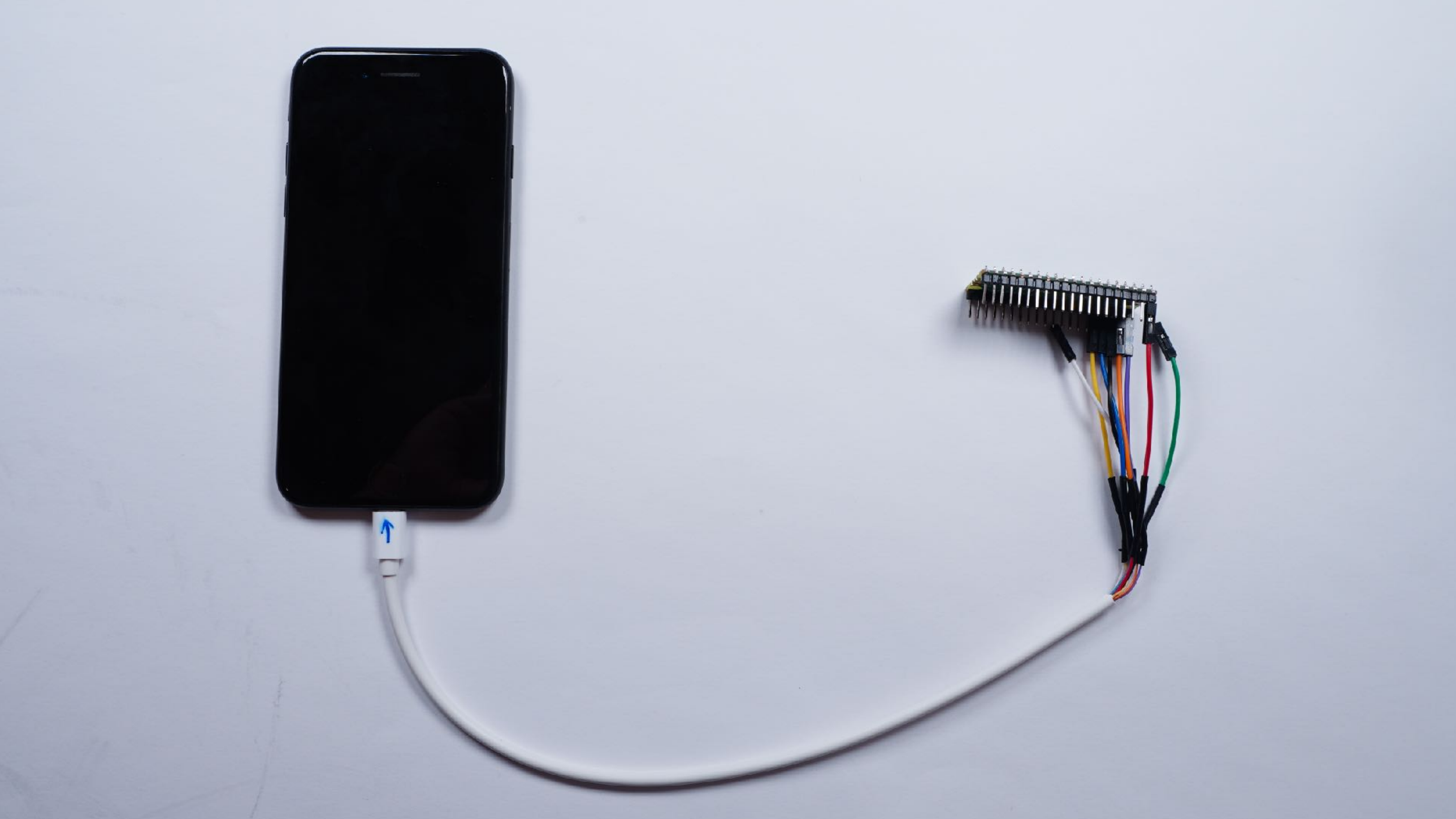






Black - GND
White - L0p
Green - L0n
Yellow - ID0
Red - 5V
Purple - L1n
Orange - L1p
Blue - ID1





Building a simple DCSD cable




LED
USB
BOOTSEL
Raspberry Pi Pico
©2020
DEBUG

Who’s there?



74 00 07 20

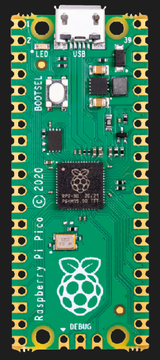


Who’s there?

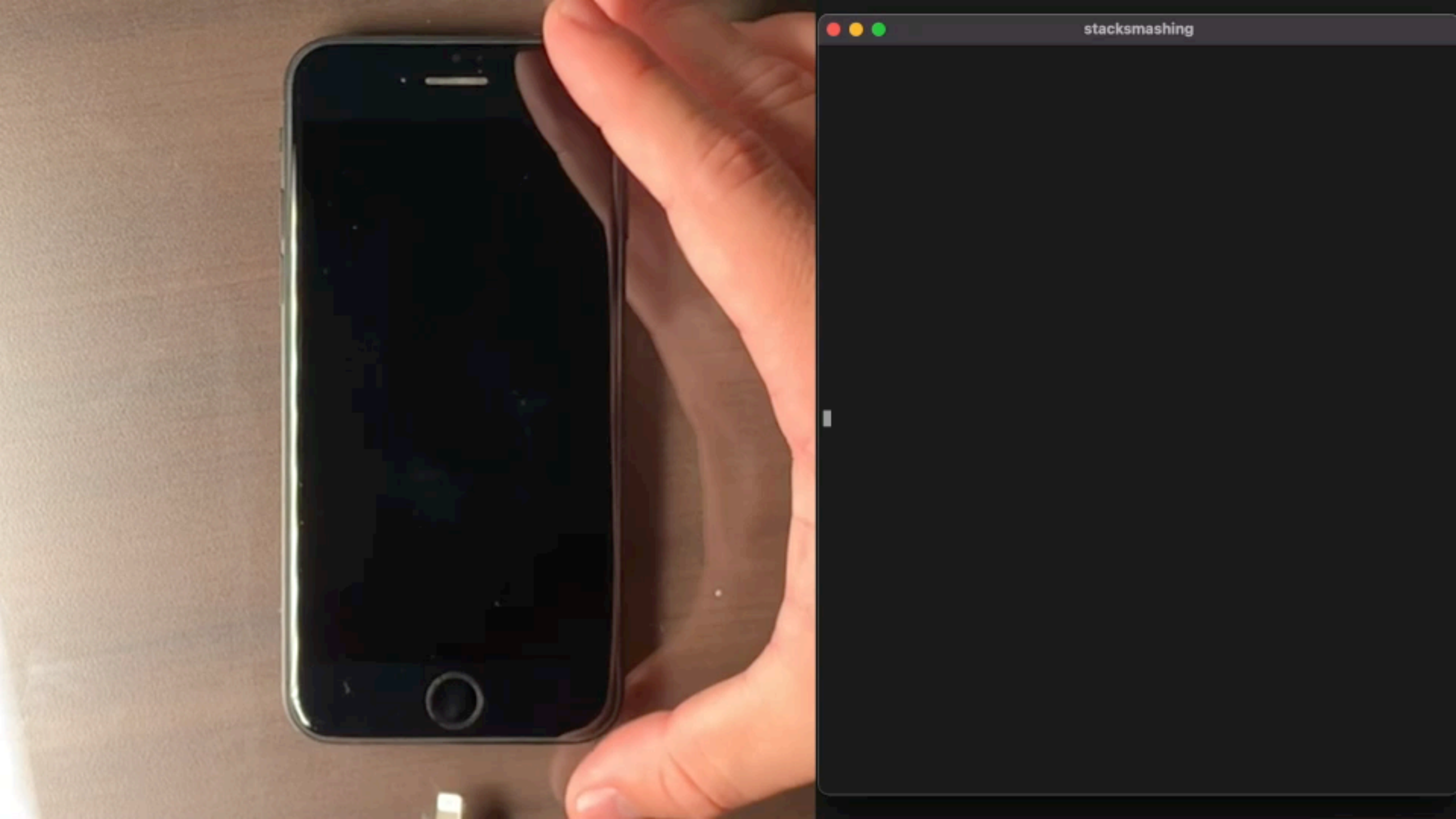


```
74 00 07 20
```

Please speak USB & UART




```
75 20 00 00 00 00 00 AA
```


stacksmashing

JTAG…

JTAG…

… actually SWD

The plan!

The plan!

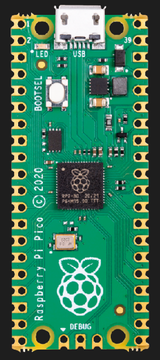


Who’s there?

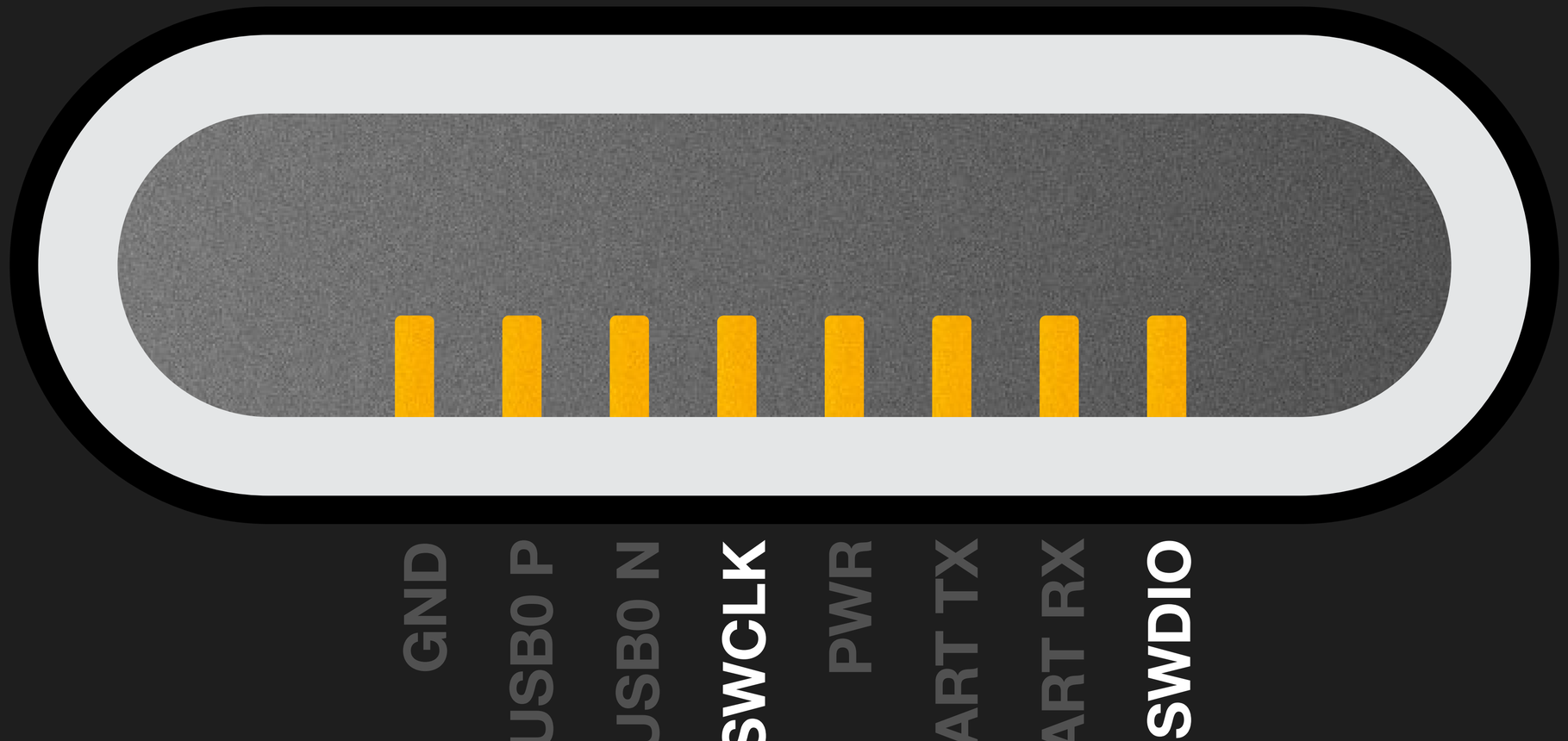


74 00 07 20

Please speak USB, UART & SWD!



75 A0 00 00 00 00 00 40

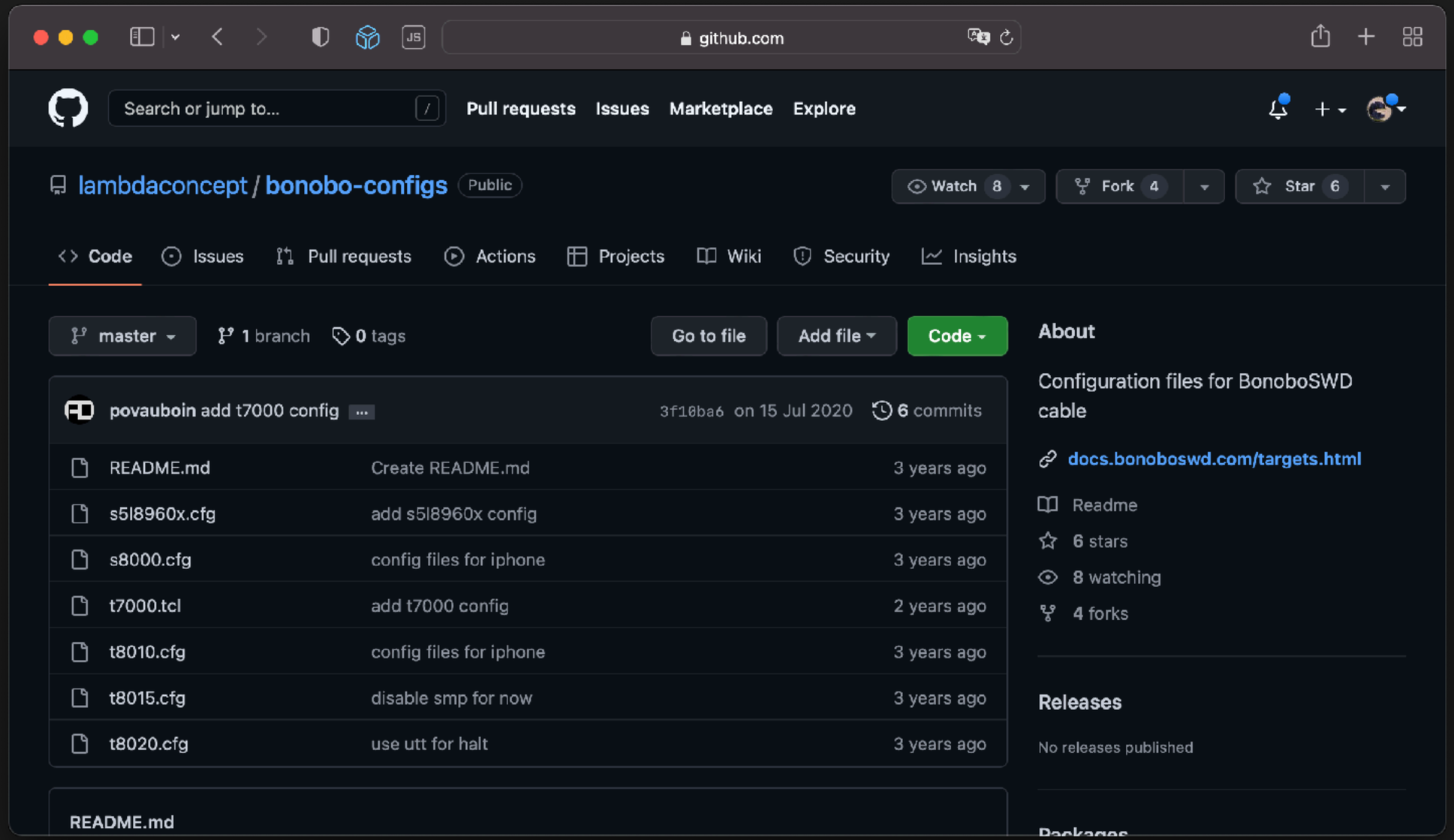

GND
USB0 P
USB0 N
SWCLK
PWR
UART TX
UART RX
SWDIO

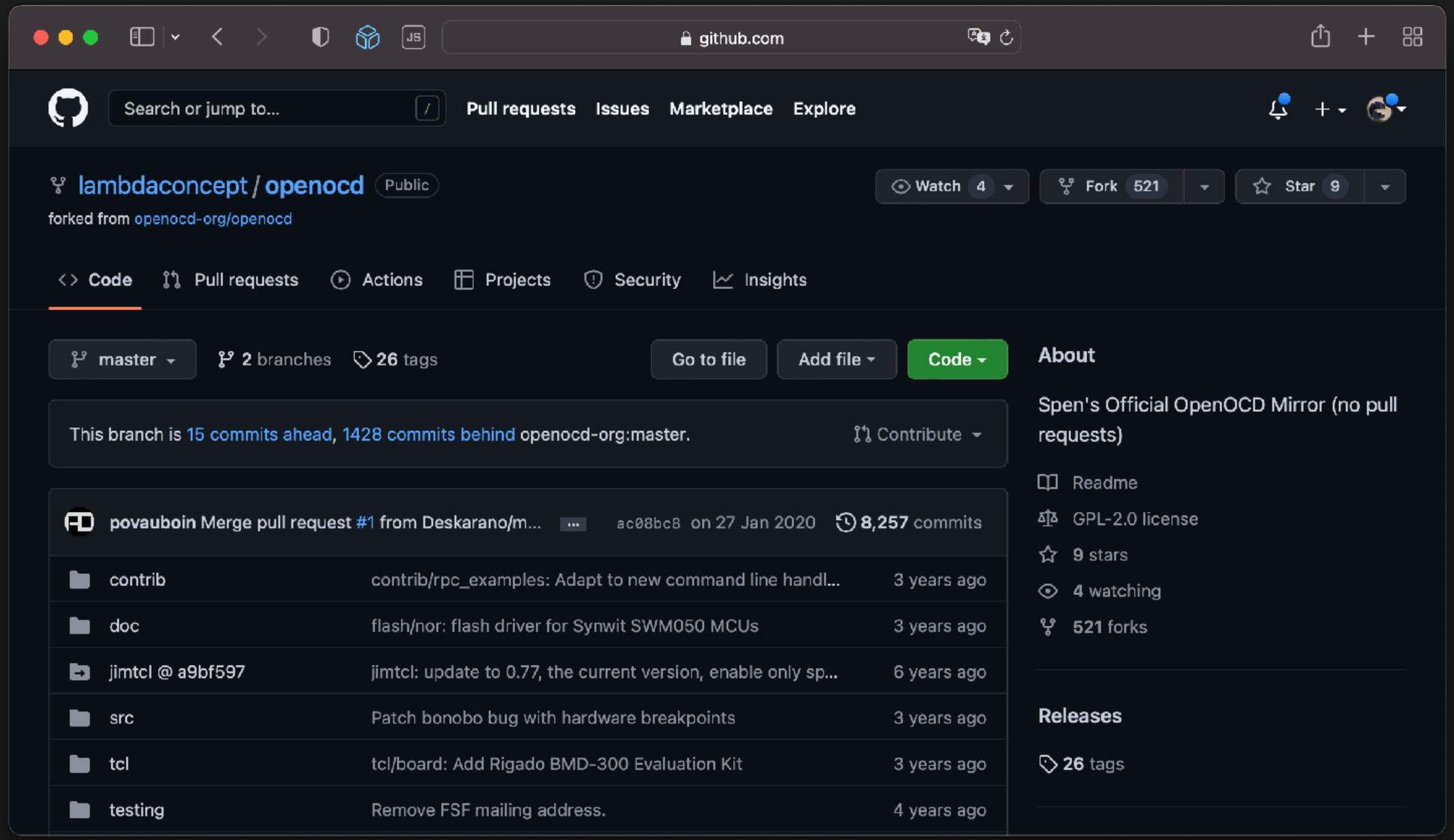
The plan!



The plan!


Set Lightning
to JTAG
via SDQ
Connect
debug
probe
with bonobo
configs


github.com
Search or jump to...
Pull requests
Issues
Marketplace
Explore
lambdaconcept / bonobo-configs
Public
Watch 8
Fork 4
Star 6
Code
Issues
Pull requests
Actions
Projects
Wiki
Security
Insights
master
1 branch
0 tags
Go to file
Add file
Code
povauboin add t7000 config
3f10ba6 on 15 Jul 2020
6 commits
README.md Create README.md 3 years ago
s5l8960x.cfg add s5l8960x config 3 years ago
s8000.cfg config files for iphone 3 years ago
t7000.tcl add t7000 config 2 years ago
t8010.cfg config files for iphone 3 years ago
t8015.cfg disable smp for now 3 years ago
t8020.cfg use utt for halt 3 years ago
README.md
About
Configuration files for BonoboSWD cable
docs.bonoboswd.com/targets.html
Readme
6 stars
8 watching
4 forks
Releases
No releases published


github.com
Search or jump to...
Pull requests
Issues
Marketplace
Explore
lambdaconcept / openocd
Public
forked from openocd-org/openocd
Watch 4
Fork 521
Star 9
Code
Pull requests
Actions
Projects
Security
Insights
master
2 branches
26 tags
Go to file
Add file
Code
This branch is 15 commits ahead, 1428 commits behind openocd-org:master.
Contribute
povauboin Merge pull request #1 from Deskarano/m...
ac08bc8 on 27 Jan 2020
8,257 commits
contrib
contrib/rpc_examples: Adapt to new command line handl...
3 years ago
doc
flash/nor: flash driver for Synwit SWM050 MCUs
3 years ago
jimtcl @ a9bf597
jimtcl: update to 0.77, the current version, enable only sp...
6 years ago
src
Patch bonobo bug with hardware breakpoints
3 years ago
tcl
tcl/board: Add Rigado BMD-300 Evaluation Kit
3 years ago
testing
Remove FSF mailing address.
4 years ago
About
Spen's Official OpenOCD Mirror (no pull requests)
Readme
GPL-2.0 license
9 stars
4 watching
521 forks
Releases
26 tags


USB
Base
j-link
SEGGER
www.segger.com
Target
Saleae

The plan!


Set Lightning
to JTAG
via SDQ
Connect
debug
probe
with bonobo
configs

The plan!


Set Lightning to JTAG via SDQ
Connect debug probe with bonobo configs
It doesn’t really work

The plan!


Set Lightning to JTAG via SDQ
Connect debug probe with bonobo configs
It doesn’t really work
It doesn’t really work

```
[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

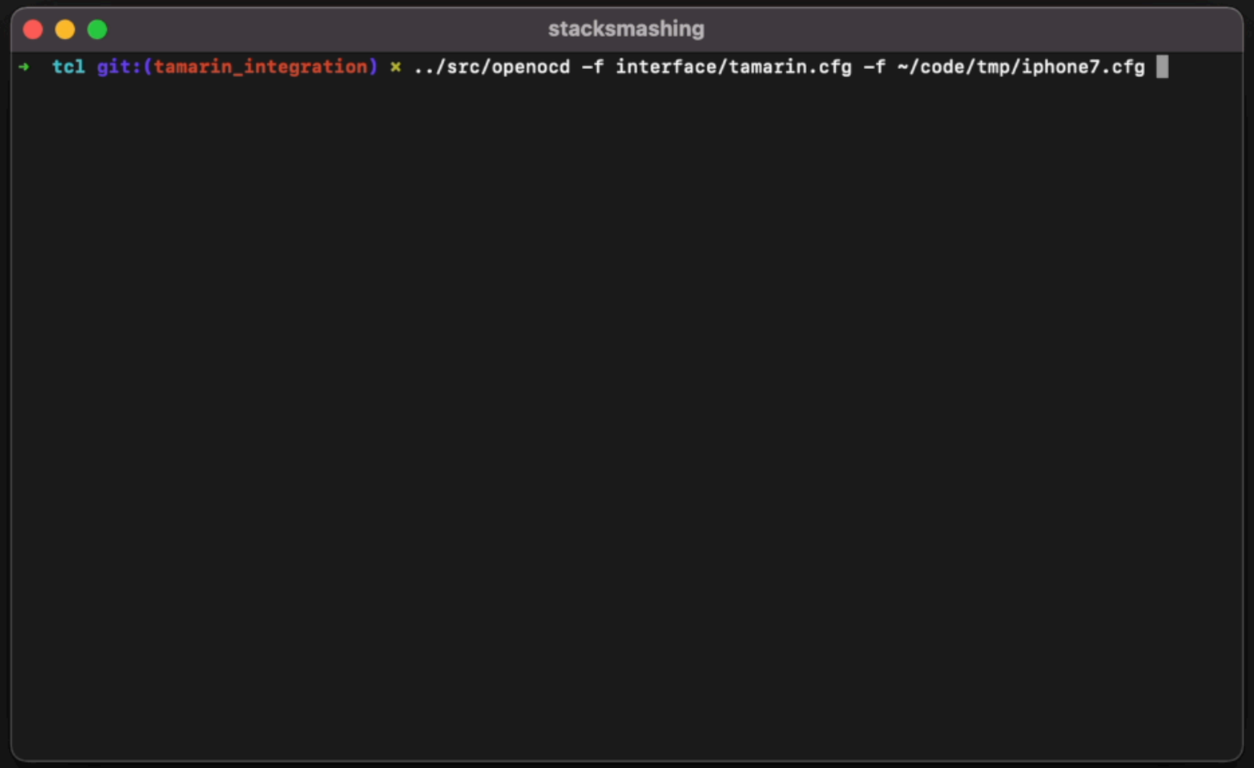
You find OpenOCD does not handle SWD WAITs

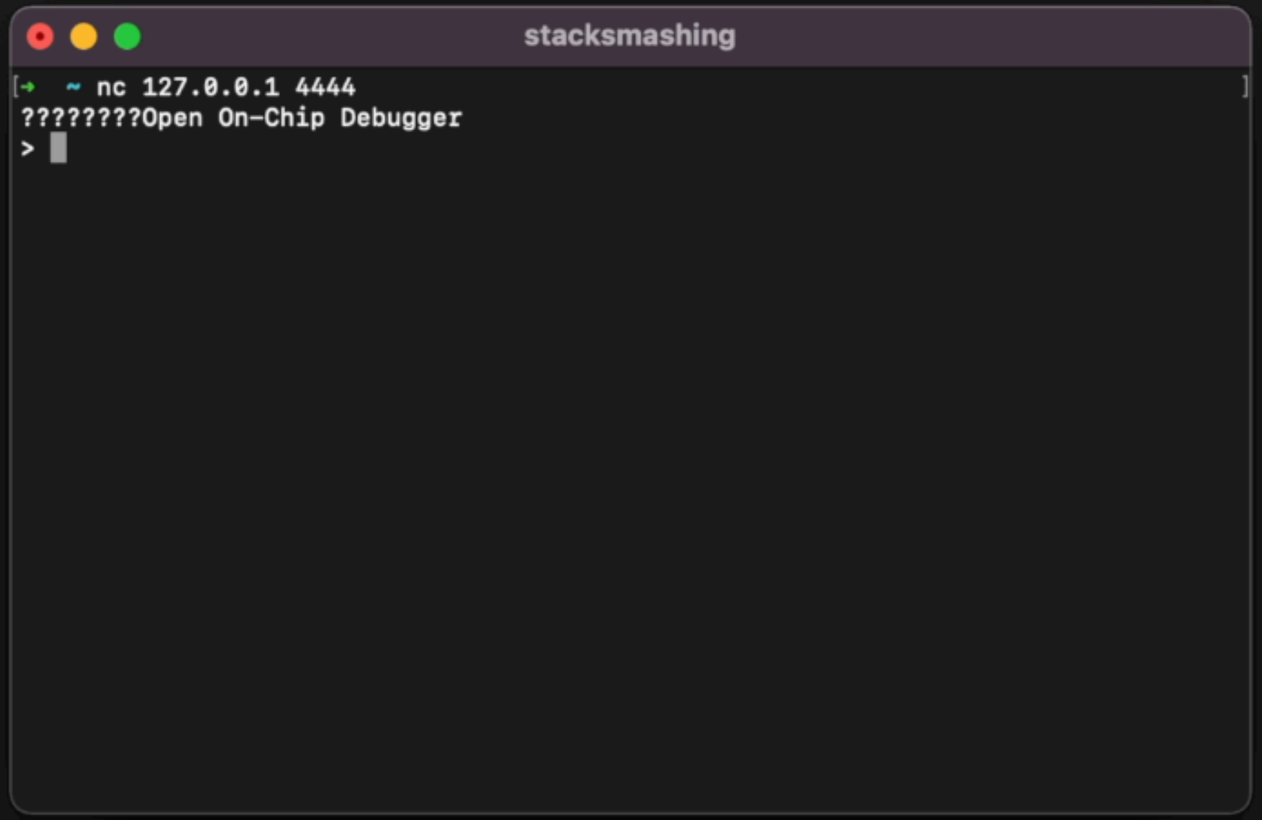
You implement SWD by hand

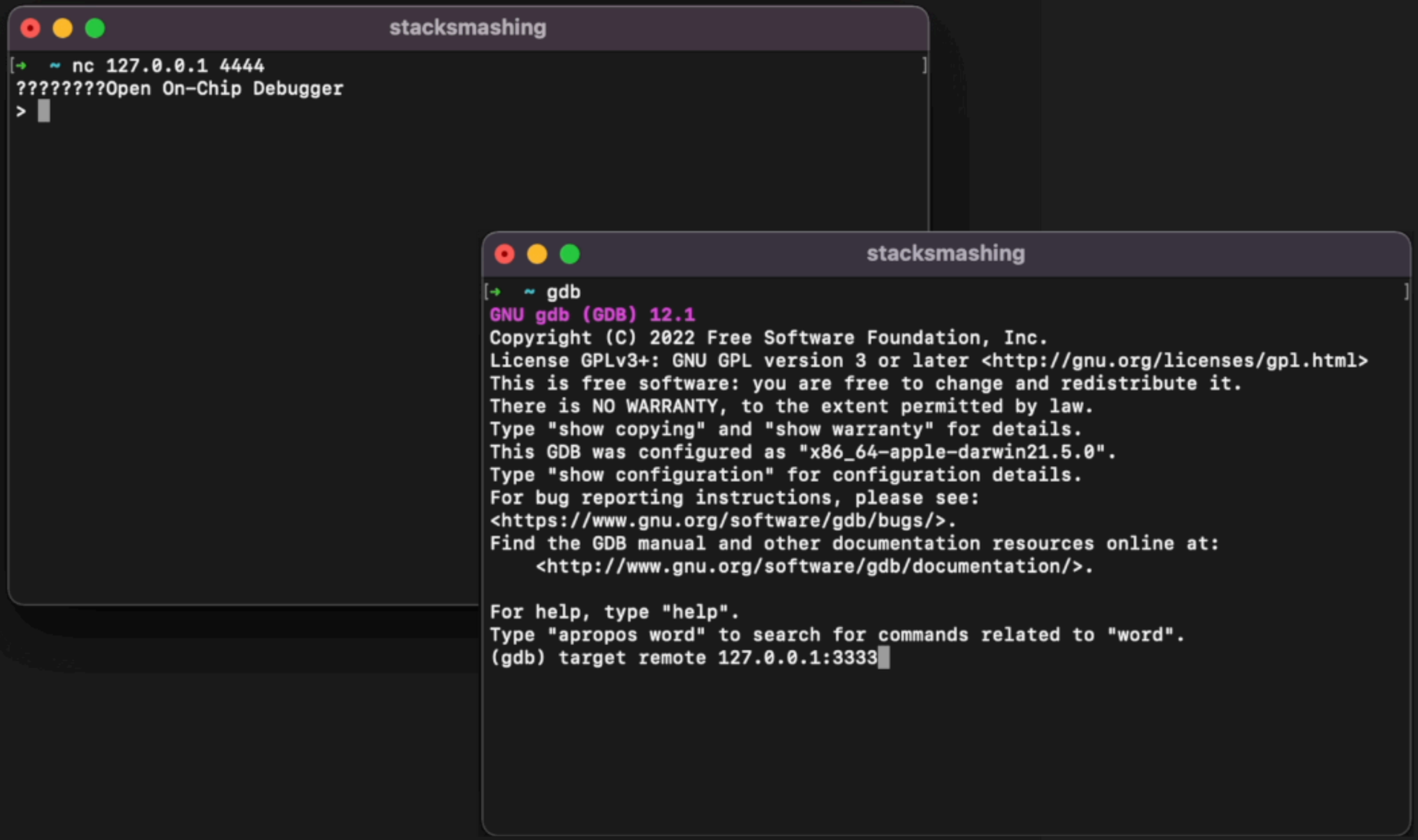
You find a single SWD bit was wrong

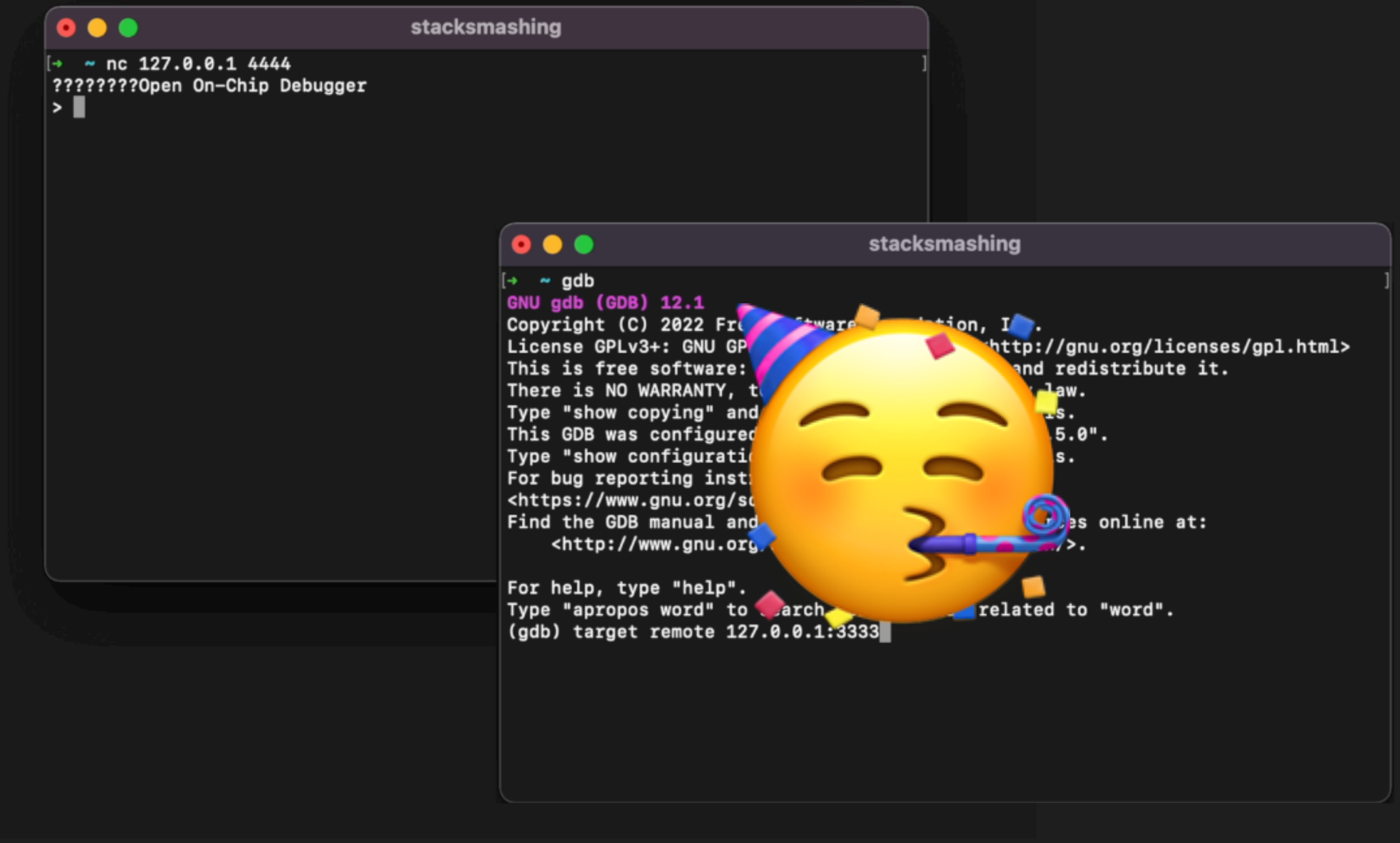
You find a single SWD bit was wrong




stacksmashing
→ tcl git:(tamarin_integration) × ../src/openocd -f interface/tamarin.cfg -f ~/code/tmp/iphone7.cfg


stacksmashing
~ nc 127.0.0.1 4444
????????Open On-Chip Debugger
>


stacksmashing
[➜ ~ nc 127.0.0.1 4444
????????Open On-Chip Debugger
>
stacksmashing
[➜ ~ gdb
GNU gdb (GDB) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-apple-darwin21.5.0".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word".
(gdb) target remote 127.0.0.1:3333


stacksmashing
~ nc 127.0.0.1 4444
????????Open On-Chip Debugger
>
stacksmashing
~ gdb
GNU gdb (GDB) 12.1
Copyright (C) 2022 Fr
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
This GDB was configured
5.0".
Type "show configurati
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
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

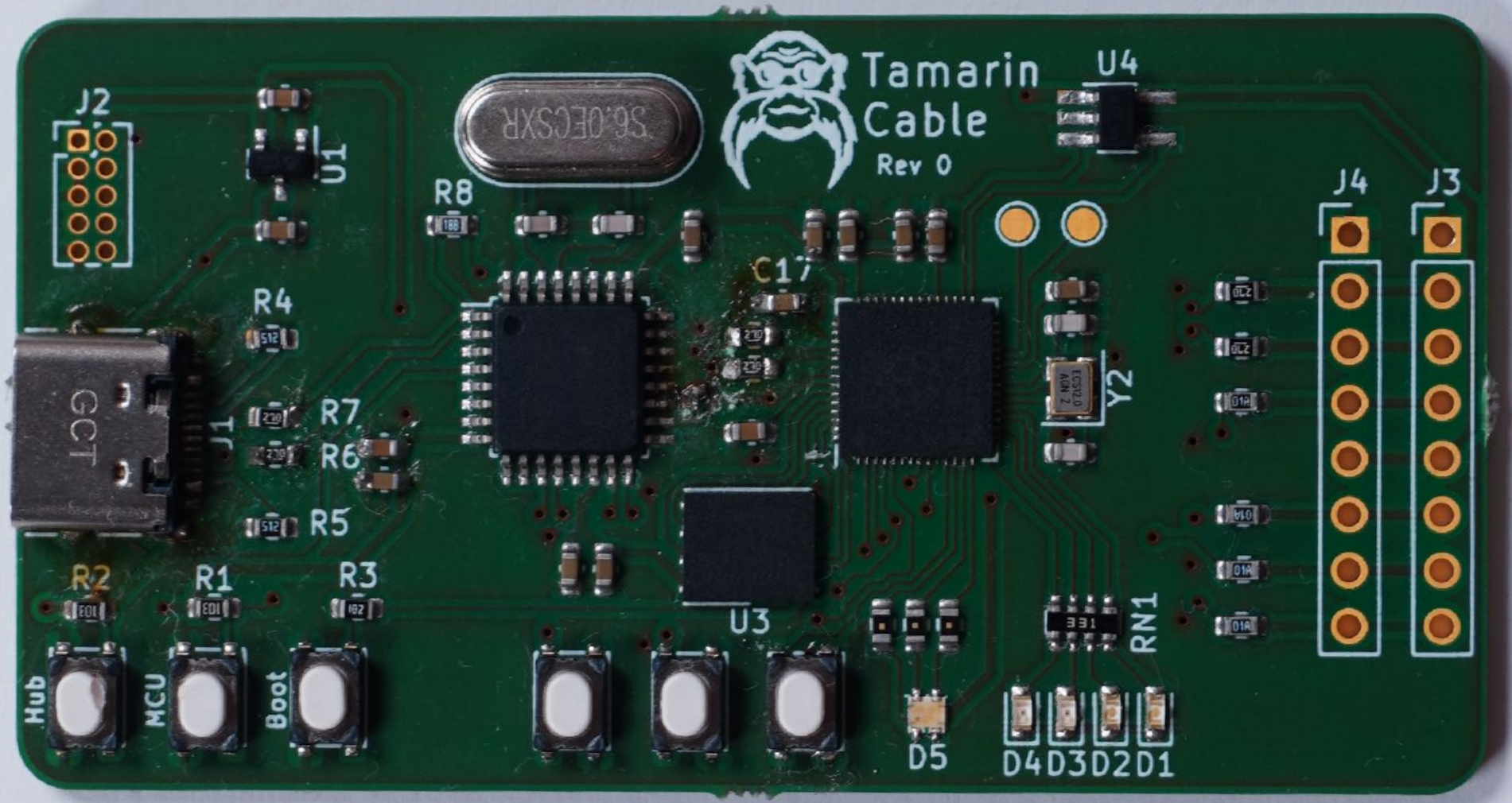
Bonobo

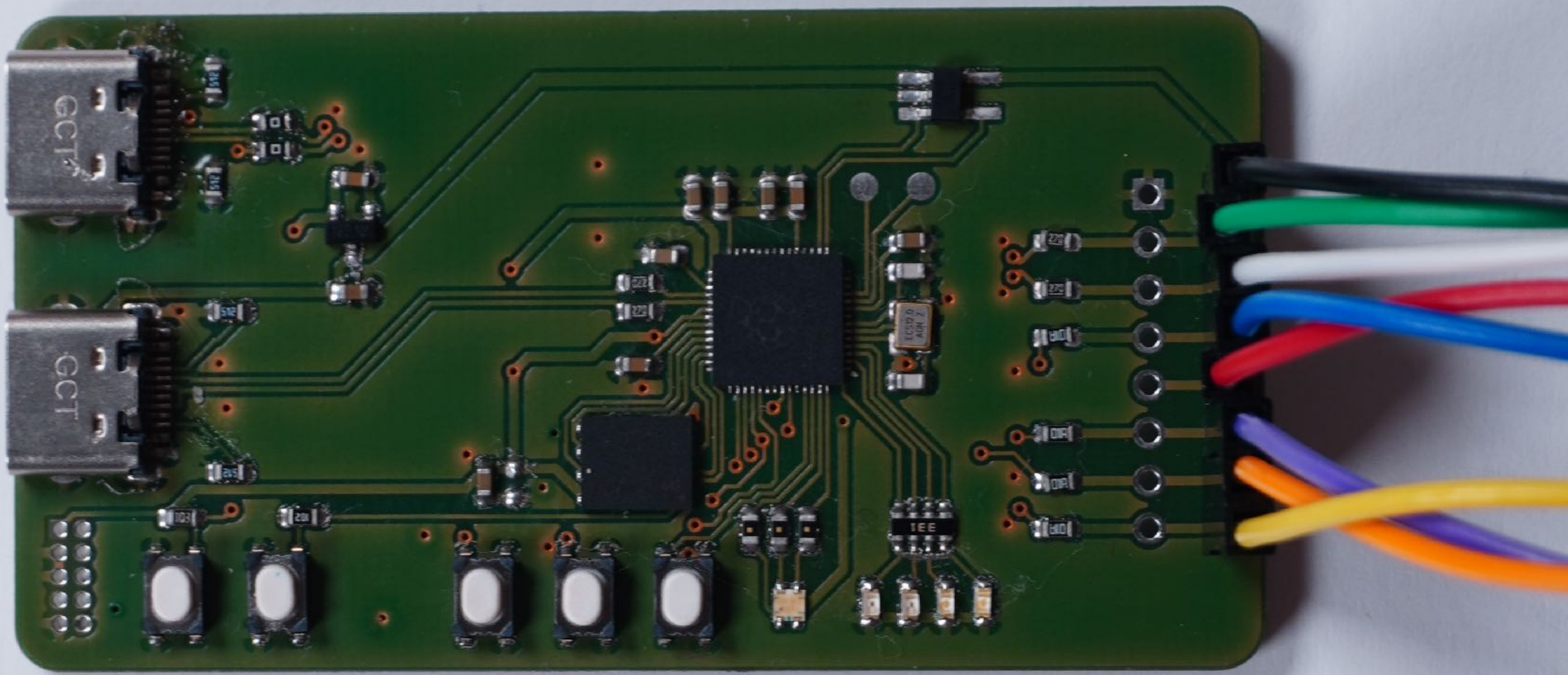


Tamarin Cable

github.com/stacksmashing/tamarin-firmware


stacksmashing
Good morning!
1: JTAG mode
2: DCSD mode
3: Reset device
4: Reset and enter DFU mode
R: Reset Tamarin cable
>


Tamarin
Cable
Rev 0
J2
U1
R8
U4
J4
J3
C17
R4
Y2
J1
GCT
R7
R6
R5
R2
R1
R3
U3
RN1
Hub
MCU
Boot
D5
D4D3D2D1


GCT
GCT

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

