Emulating Amiibos in Software

tales from
reverse engineering
Nintendo’s controller protocol

Paul Weiß – 13.12.2023

What this talk is not

Amiibo = NTAG215 + data

9ct/pc

Way cheaper, easier and less interesting

Where I stole most of this

https://github.com/dekuNukem/Nintendo_Switch_Reverse_Engineering

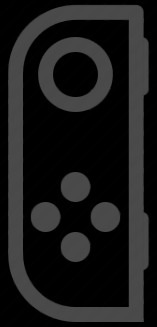
https://github.com/mart1nro/joycontrol

https://github.com/CTCaer/jc_toolkit

https://github.com/Brikwerk/nxbt

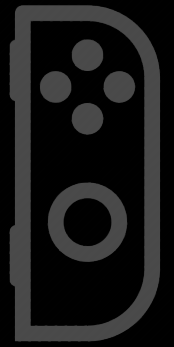
Kinds of Controllers

Joycon (L)



Procon

Joycon (R)



Protocol identical for all of them

No clue what happens when you request
IR or NFC from a left Joycon

Input “Modes”

Input “Modes”

Human Interface Device

Input “Modes”

Human Interface Device

MicroController[Unit]

Input “Modes”

Human Interface Device

MicroController[Unit]

NFC + IR

Input “Modes”

0x2F
Pure HID

Human Interface
Device

MicroController[Unit]

NFC + IR

Input “Modes”

0x2F
Pure HID

0x30
Nintendo HID

More buttons,
Gyro, fixed rate

Human Interface
Device

MicroController[Unit]

NFC + IR

Input “Modes”

0x2F
Pure HID

0x30
Nintendo HID

More buttons,
Gyro, fixed rate

0x31
Nintendo HID
+ 313 byte
data

Human Interface
Device

MicroController[Unit]

NFC + IR

Input “Modes”

0x2F
Pure HID

0x30
Nintendo HID

More buttons,
Gyro, fixed rate

0x31
Nintendo HID
+ 313 byte
data

Human Interface
Device

MicroController[Unit]

NFC + IR

Input “Modes”

0x2F
Pure HID

0x30
Nintendo HID

More buttons,
Gyro, fixed rate

0x31
Nintendo HID
+ 313 byte
data

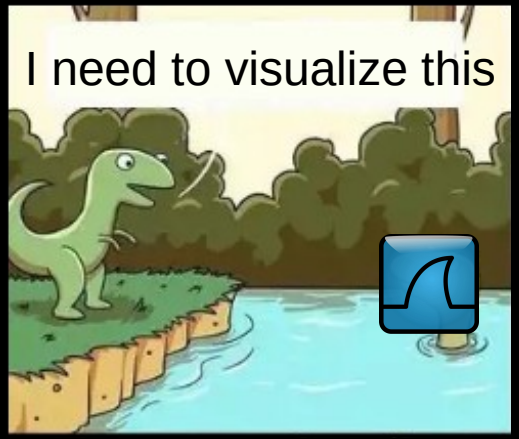
Human Interface
Device

MicroController[Unit]

0x21
Commands and
replies

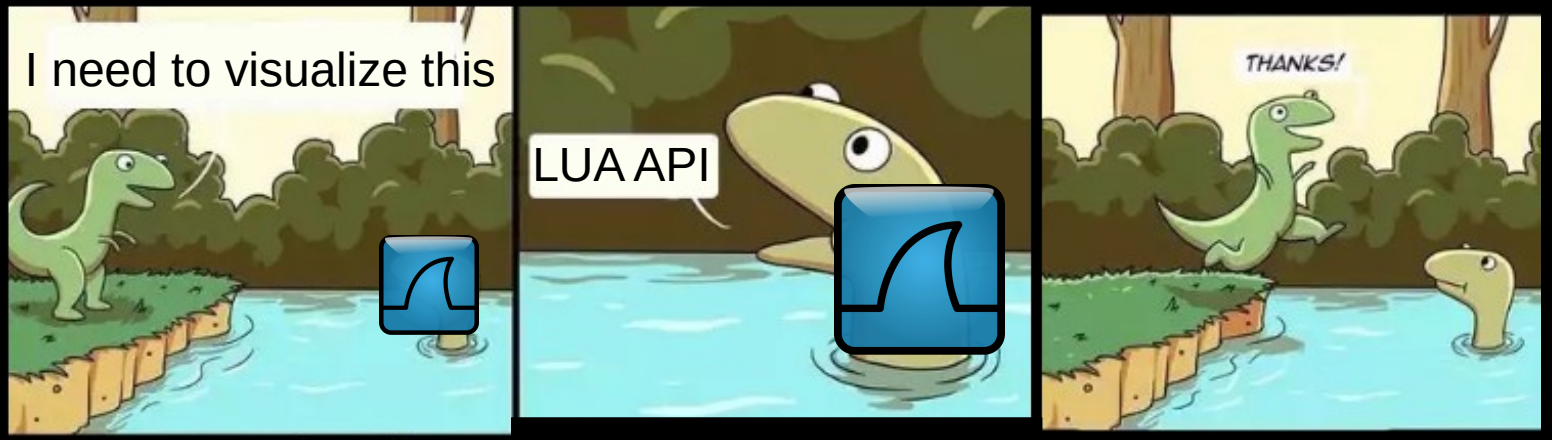
NFC + IR

Visualizing this Bit-Mess

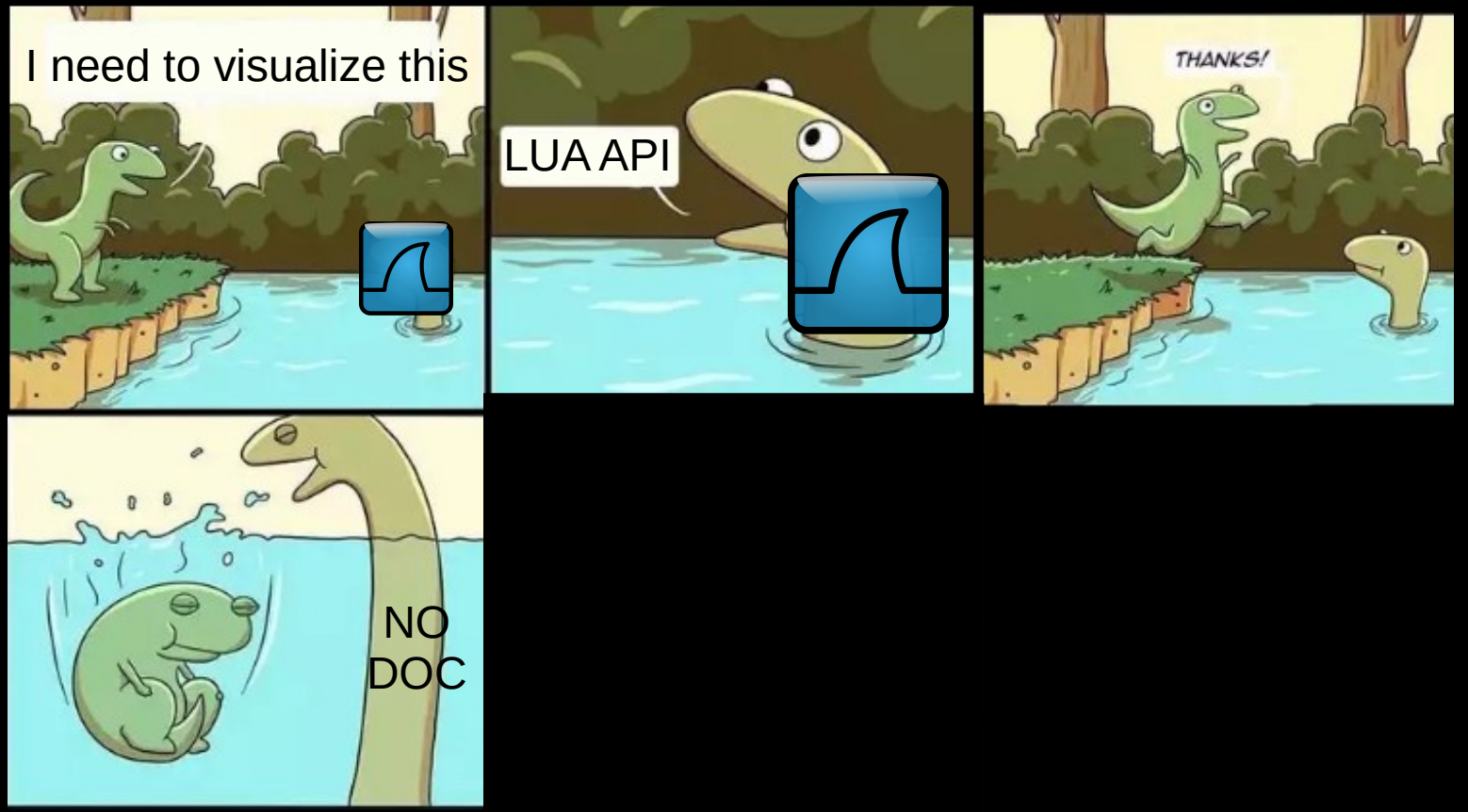


Visualizing this Bit-Mess

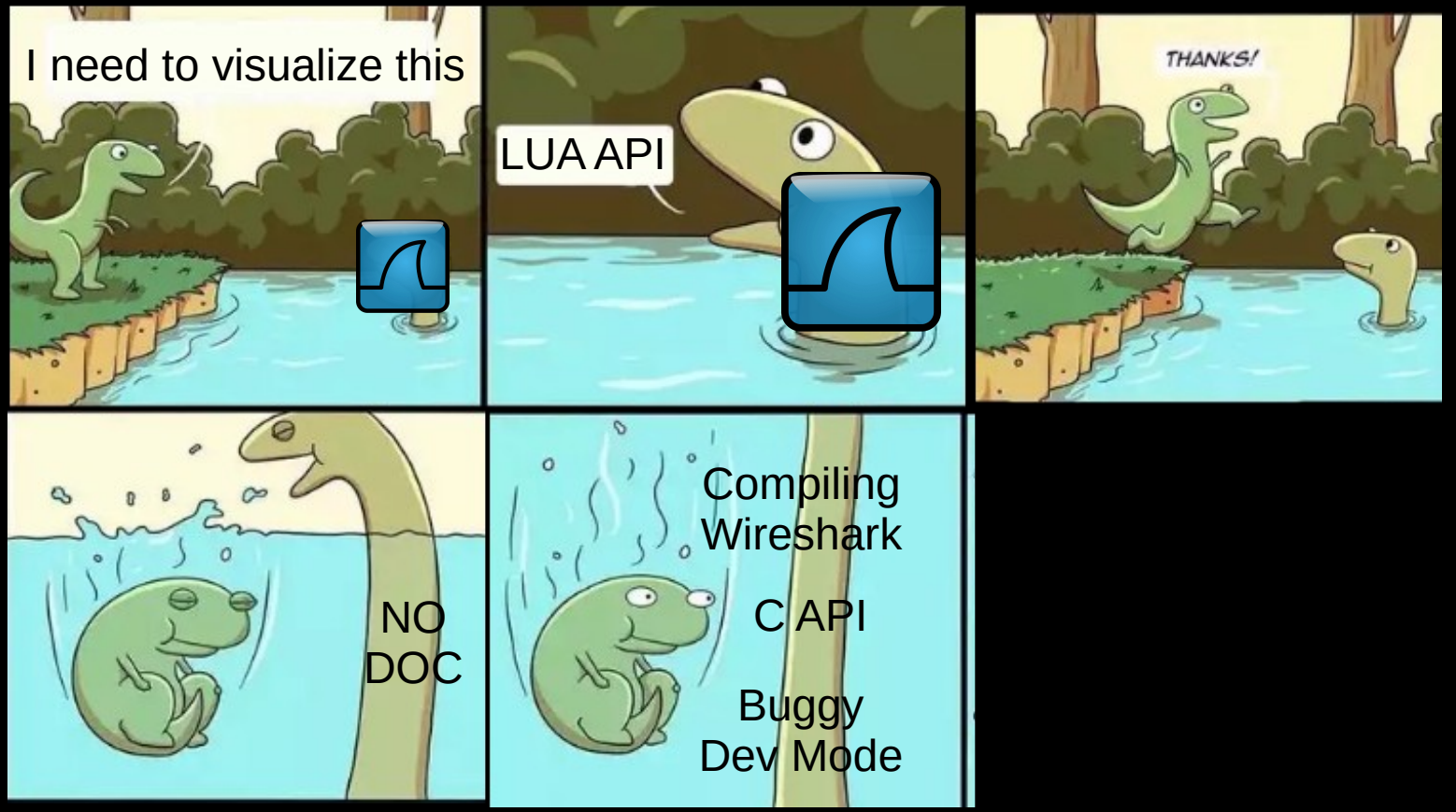
Visualizing this Bit-Mess



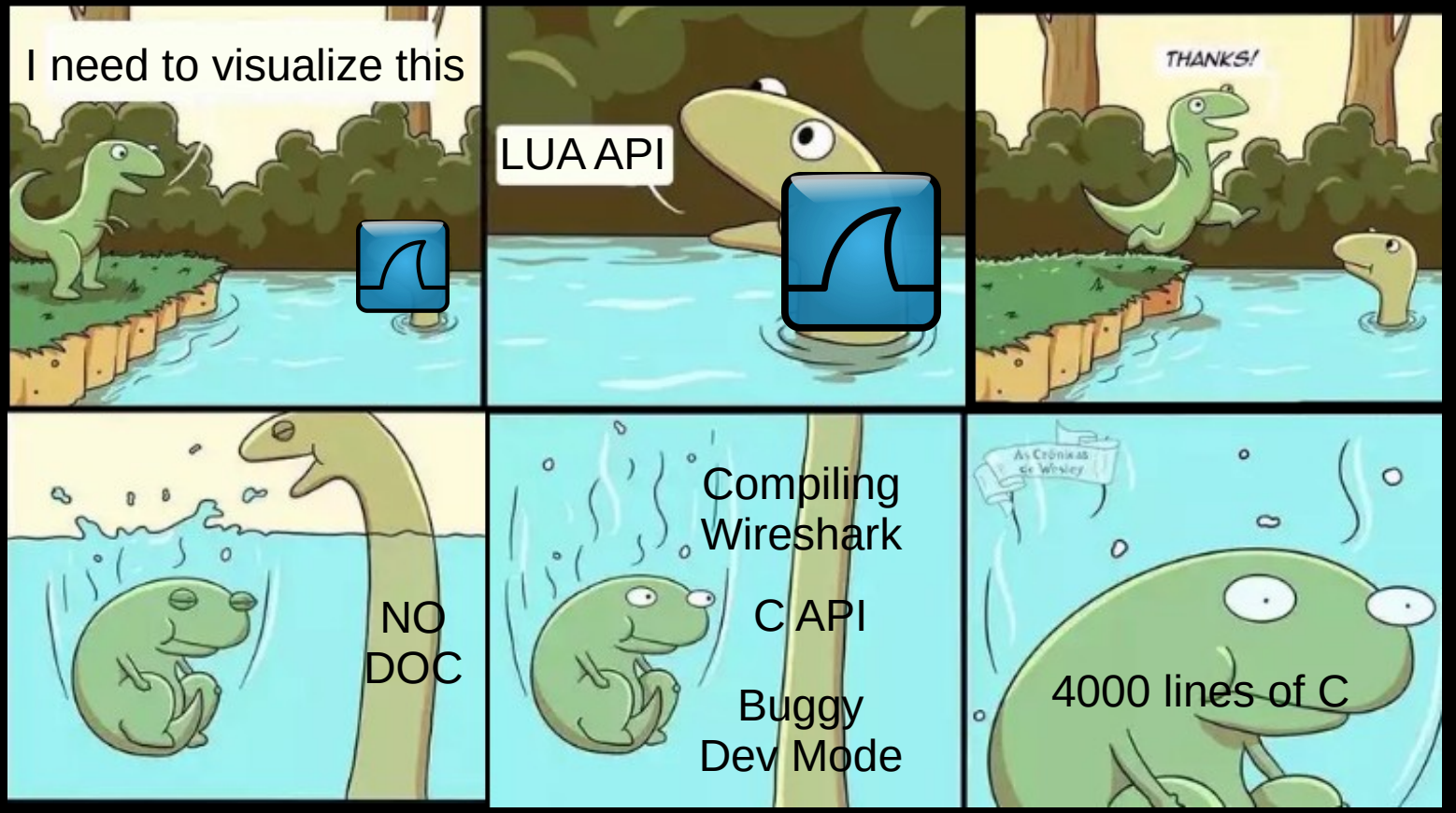
Visualizing this Bit-Mess



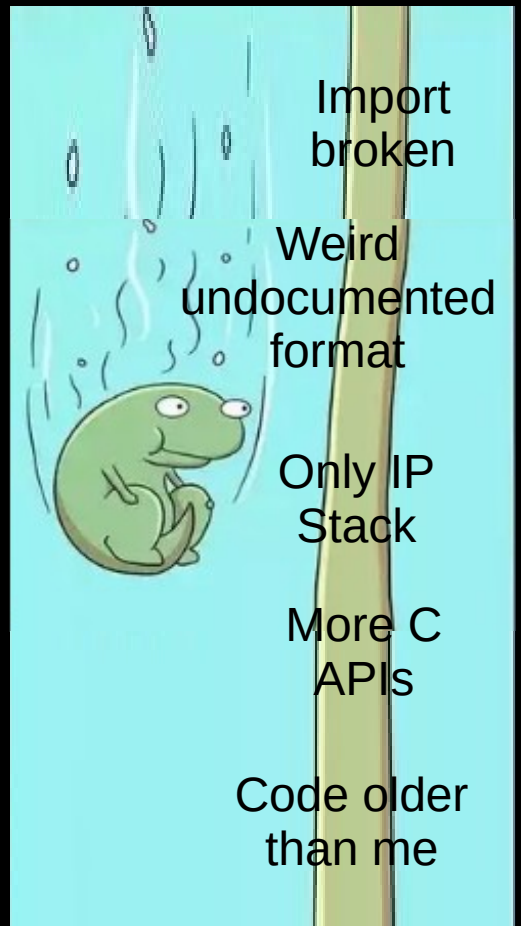
Visualizing this Bit-Mess



Visualizing this Bit-Mess



Importing Bluetooth logs

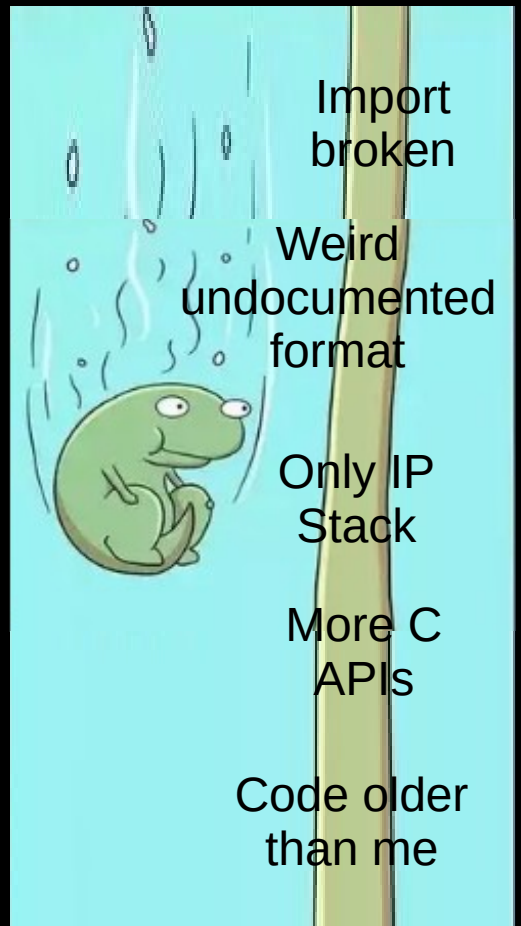


People send you terminal logs

Log EVERYTHING (and into file)

< 0.0014 0500608cb100608cb1
> 0.0156 0518638cf118638cf13010000000000000000000

Importing Bluetooth logs



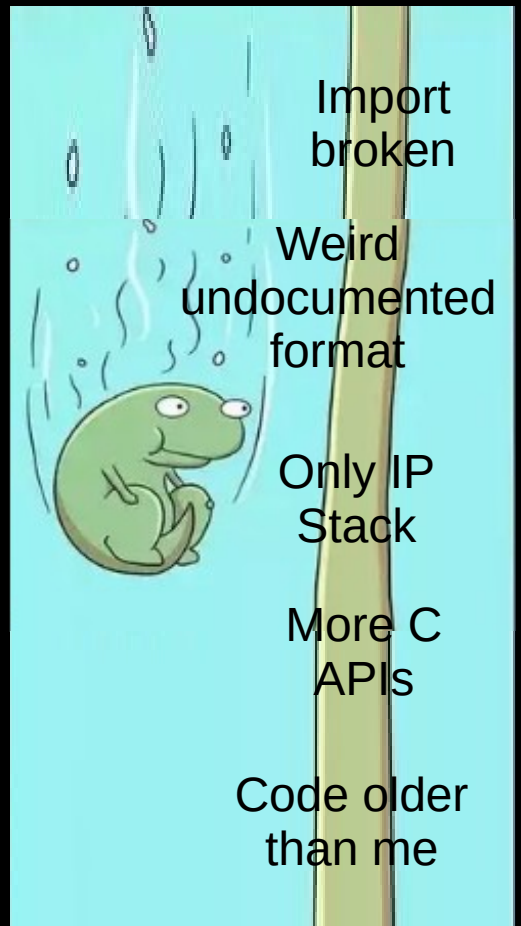
People send you terminal logs

Log EVERYTHING (and into file)

< 0.0014 0500608cb100608cb1
> 0.0156 0518638cf118638cf1301000000000000000000

Importing is still a pain, because:

Importing Bluetooth logs



People send you terminal logs

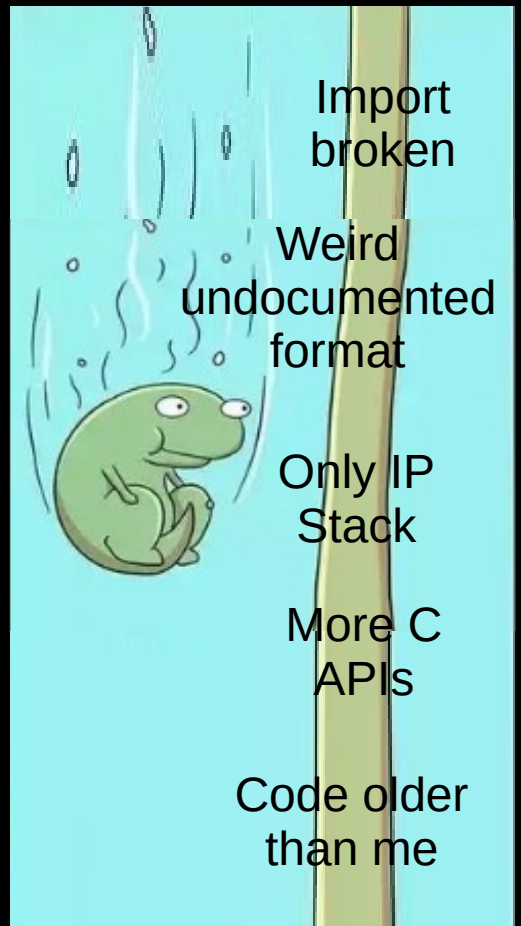
Log EVERYTHING (and into file)

< 0.0014 0500608cb100608cb1
> 0.0156 0518638cf118638cf1301000000000000000000

Importing is still a pain, because:

- Bluetooth is connection based

Importing Bluetooth logs



People send you terminal logs

Log EVERYTHING (and into file)

< 0.0014 0500608cb100608cb1
> 0.0156 0518638cf118638cf1301000000000000000000

Importing is still a pain, because:

- Bluetooth is connection based
- See left

The actual Protocol

On paper very simple Request – Reply system

BUT:

The actual Protocol

On paper very simple Request – Reply system

BUT:

The actual Protocol

Using Python scripts to run Man in the Middle attack on Bluetooth connections works kinda

The actual Protocol

Using Python scripts to run Man in the Middle attack on Bluetooth connections works kinda

=> seq_no, ack_seq_no, continuation_flag

The actual Protocol

Using Python scripts to run Man in the Middle attack on Bluetooth connections works kinda

=> seq_no, ack_seq_no, continuation_flag

Implementing the emulator in Python not so much, because testing is a pain

The actual Protocol

Using Python scripts to run Man in the Middle attack on Bluetooth connections works kinda

=> seq_no, ack_seq_no, continuation_flag

Implementing the emulator in Python not so much, because testing is a pain

Also bugs in python’s Bluetooth sockets, I didn’t want to compile that too

Does it work?

Does it work?

Depends on your definition

Does it work?

Depends on your definition

- Yes, you can use it to emulate amiibos fully

Does it work?

Depends on your definition

- Yes, you can use it to emulate amiibos fully

- Yes, you have to restart the entire thing after writing an amiibo

Does it work?

Depends on your definition

- Yes, you can use it to emulate amiibos fully
- Yes, you have to restart the entire thing after writing an amiibo
- Yes, you can use this to crash the switch, linux kernel 6.?+ and btstack

Does it work?

Depends on your definition

- Yes, you can use it to emulate amiibos fully
- Yes, you have to restart the entire thing after writing an amiibo
- Yes, you can use this to crash the switch, linux kernel 6.?+ and btstack
- Yes, this breaks your bluetooth stack in ways you haven’t seen before

Thanks for your Attention

The parts I didn’t steal

https://github.com/Poohl/joycontrol

https://gist.github.com/Poohl/e0f254b3e02051b18c7e9f4f032883be

https://github.com/Poohl/joycontrol-pico