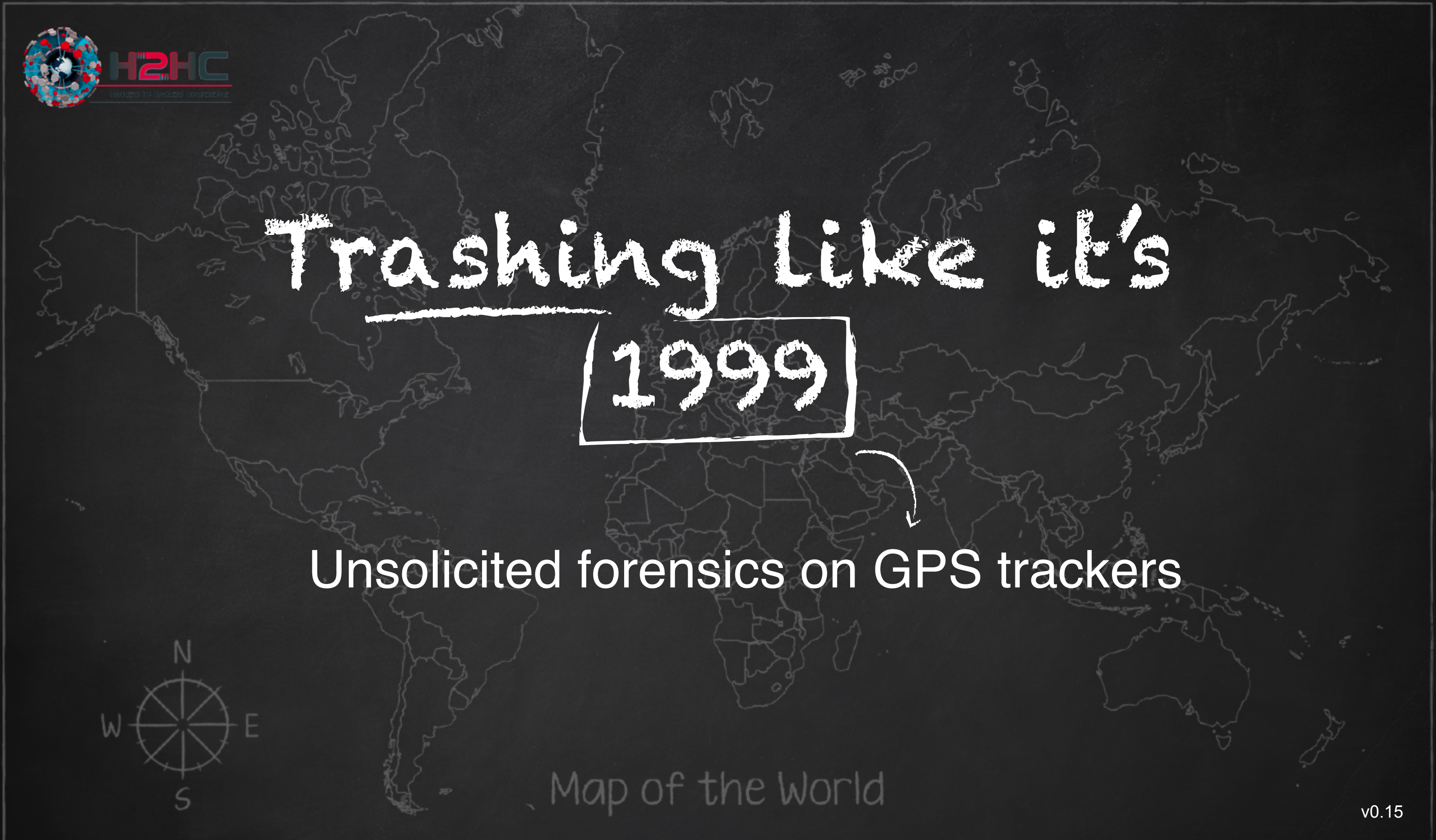
H2HC

HACKERS TO HACKERS CONFERENCE

Trashing like it's 1999

Unsolicited forensics on GPS trackers



v0.15

Disclaimer:

I don’t speak for my employer. All the opinions and information here are of my responsibility.

Matias S. Soler

Sr. Security Researcher at Intel STORM team
@gnuler

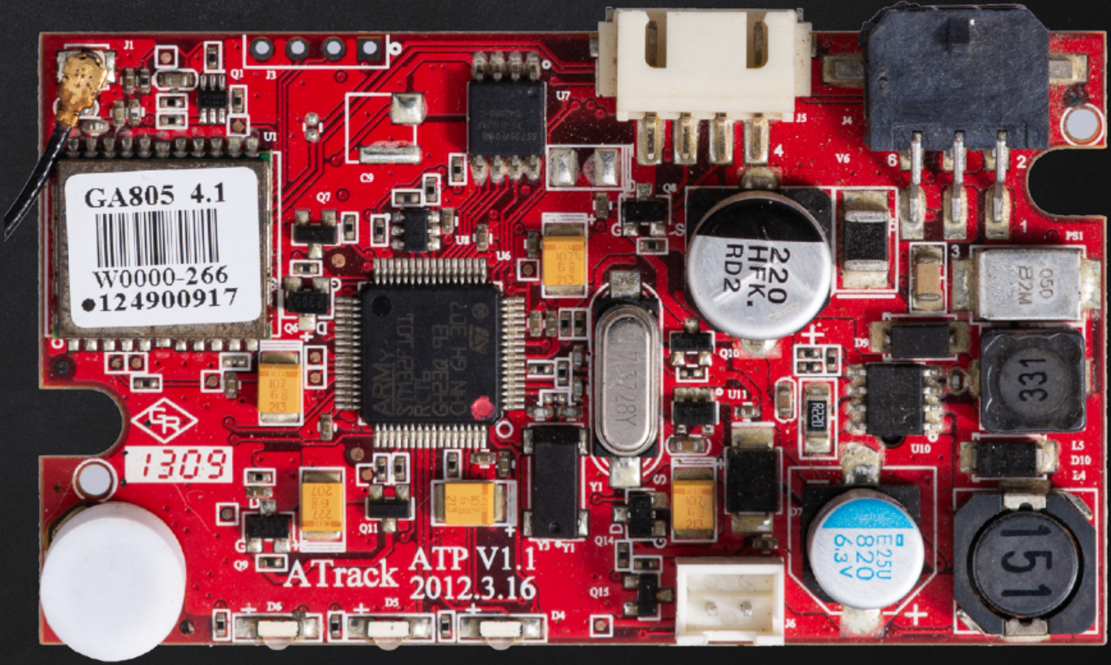
Once upon a time,

In a land far far away...

A dream become true.

What are they?

- Fleet GPS trackers
- GSM/GPRS
- 3 Axis G Sensor
- 2-way voice
- Real-time tracking
- Geofencing
- **Not for end-user**



Power supply

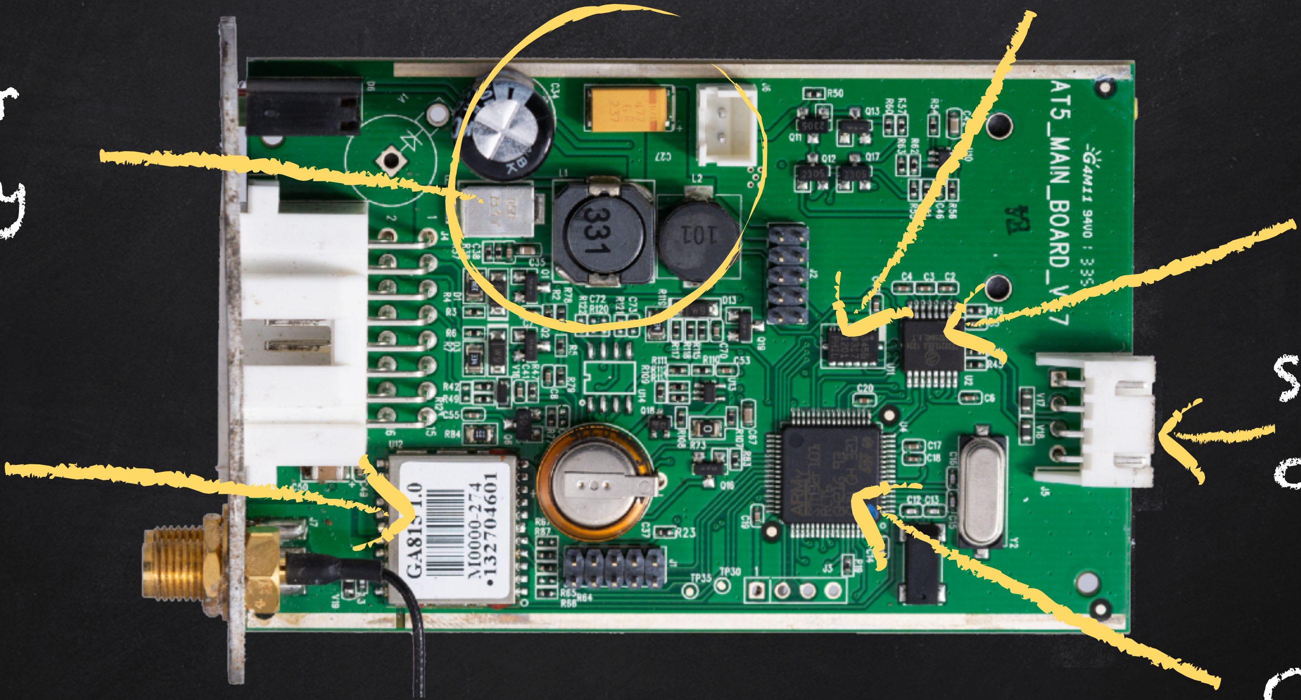
GPS

Accelerometer

rs232 transceiver

Serial connector

CPU

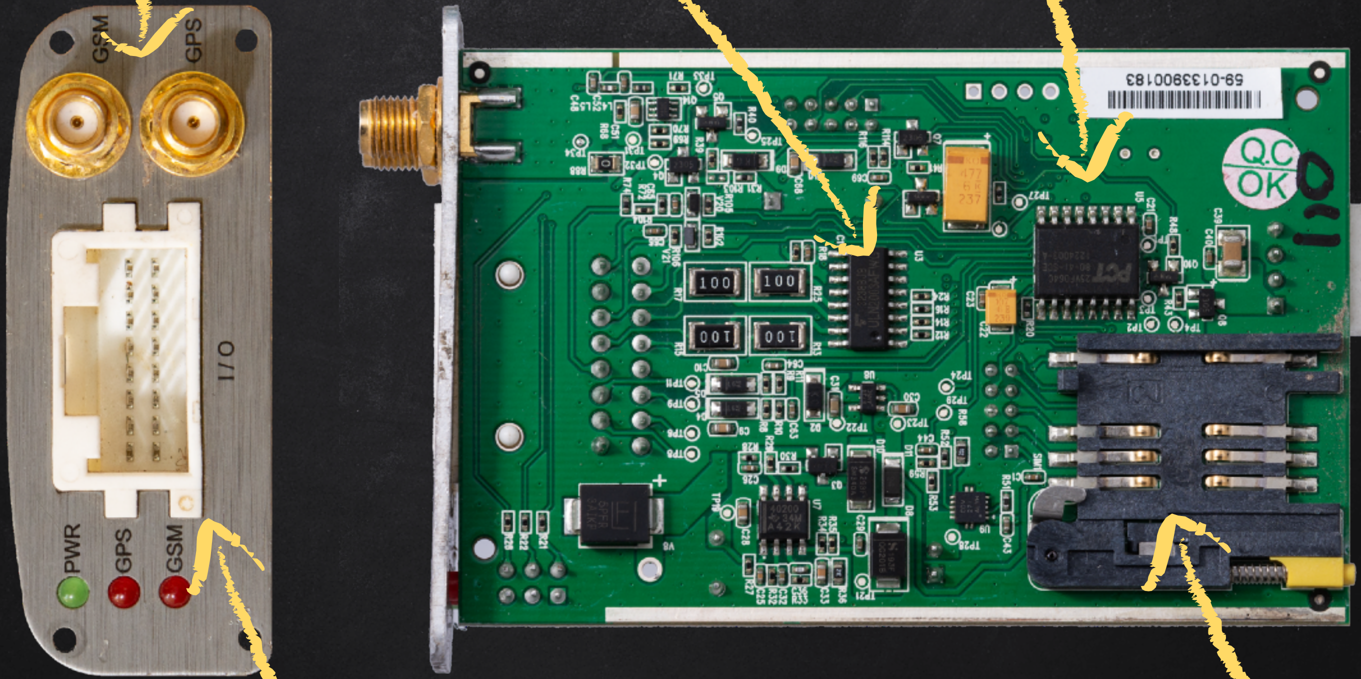


STM32F101/103
ARM Cortex M3 32-bit

GPS, GSM Antennas

Driver

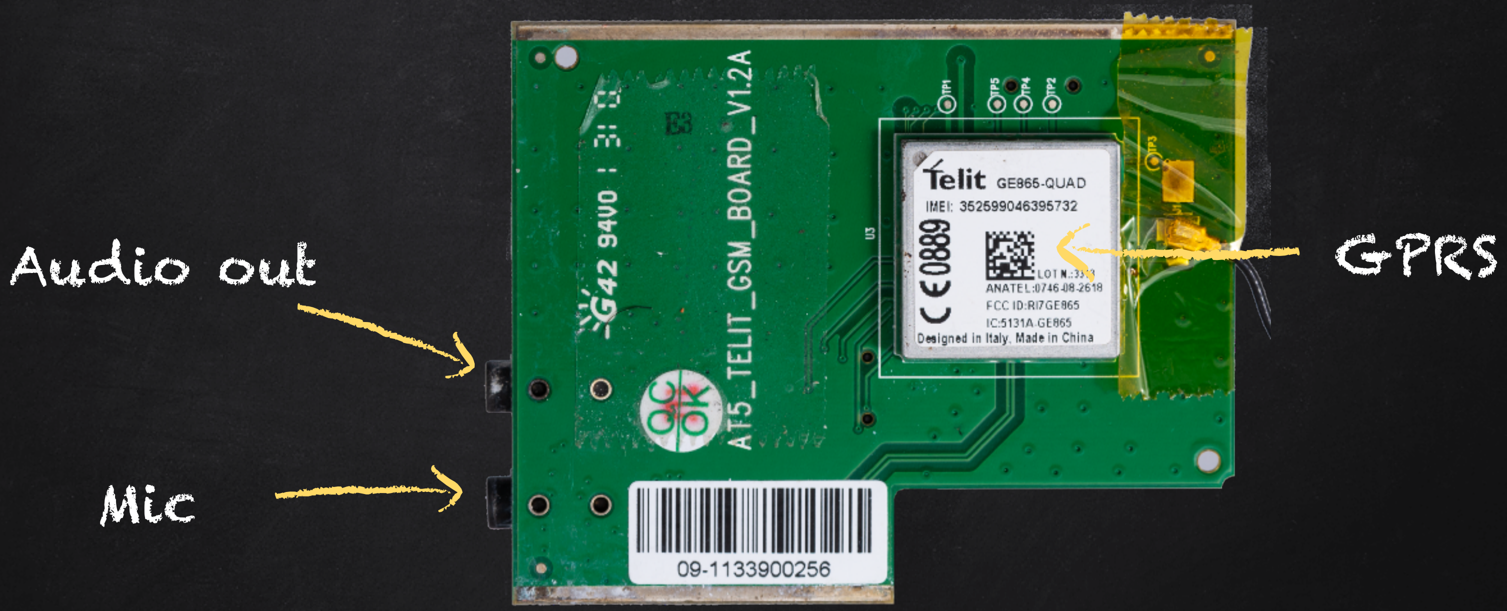
Flash

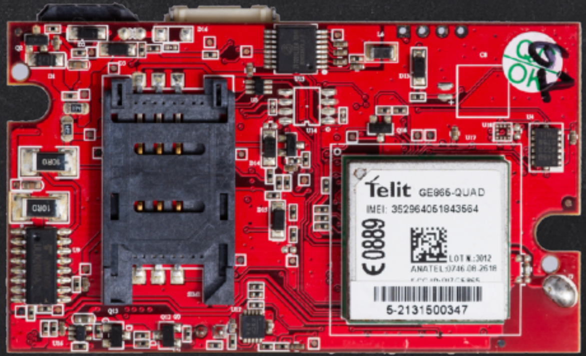


Main Connector

IOs, Power, etc

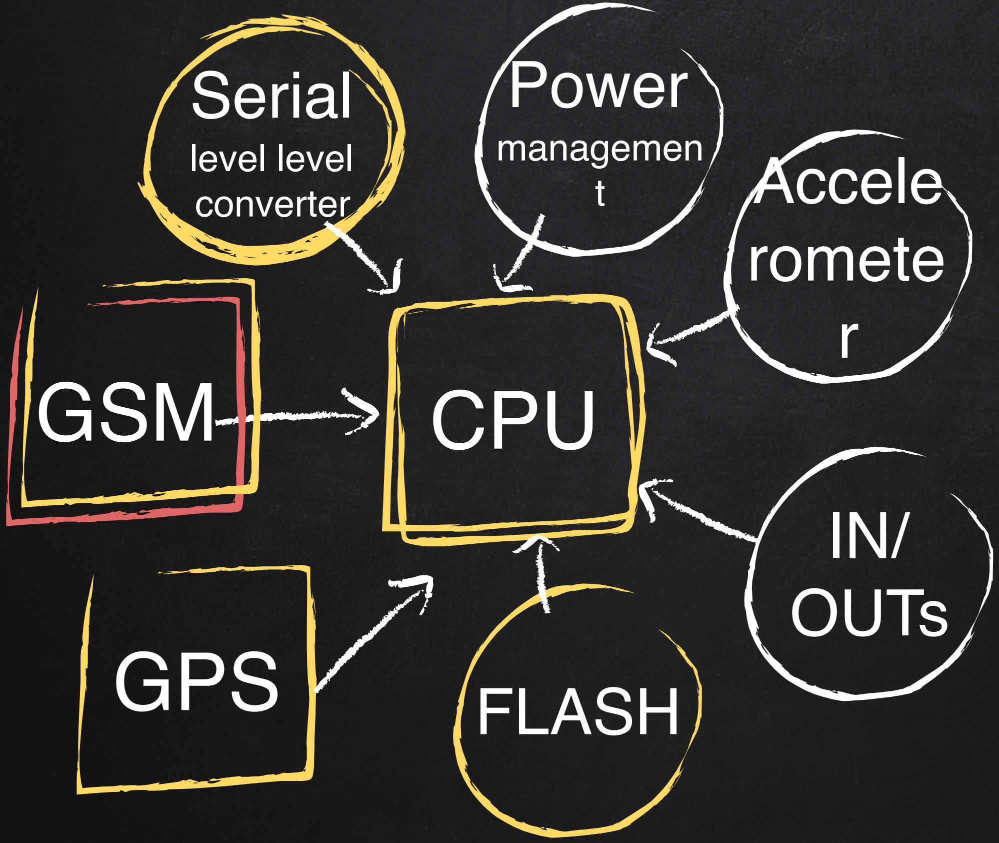
SIM socket


Audio out
Mic
GPRS
Telit GE865-QUAD
IMEI: 352599046395732
LOT N.:33
ANATEL:0746-08-2618
FCC ID:RI7GE865
IC:5131A-GE865
Designed in Italy, Made in China
0889
AT5_TELIT_GSM_BOARD_V1.2A
G42 94V0
09-1133900256



Find all the !

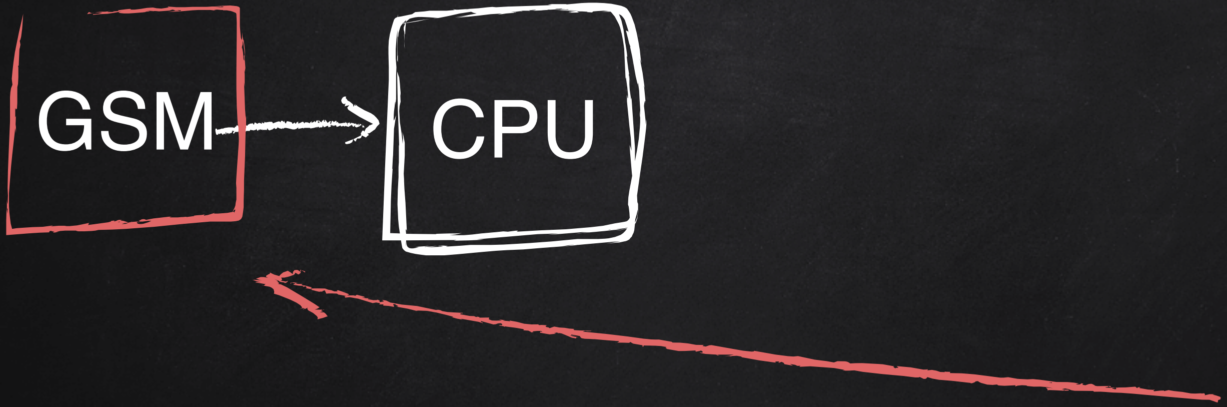
Attack Vectors



Local
Serial Parsers
Flash Parser
Code/Data

Remote
SMS
FTP

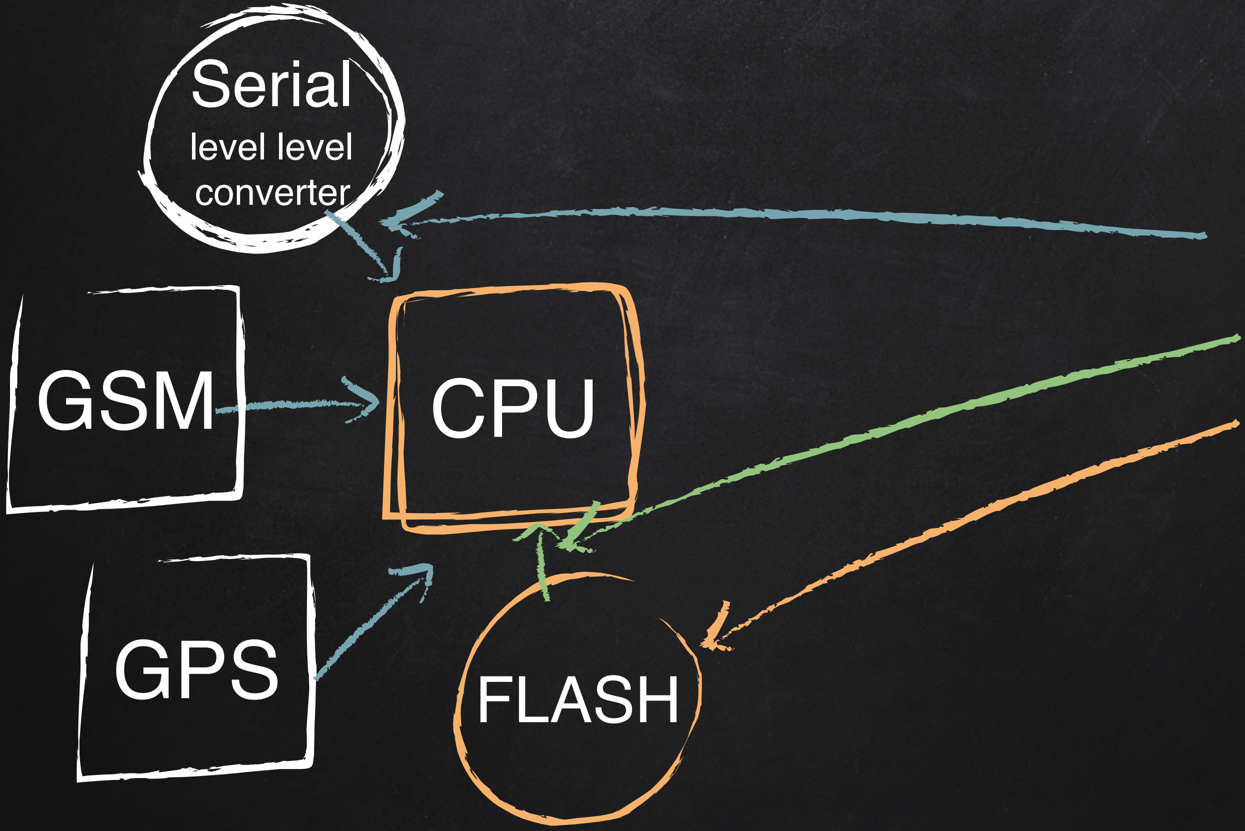
Attack Vectors



Local
Serial Parsers
Flash Parser
Code/Data

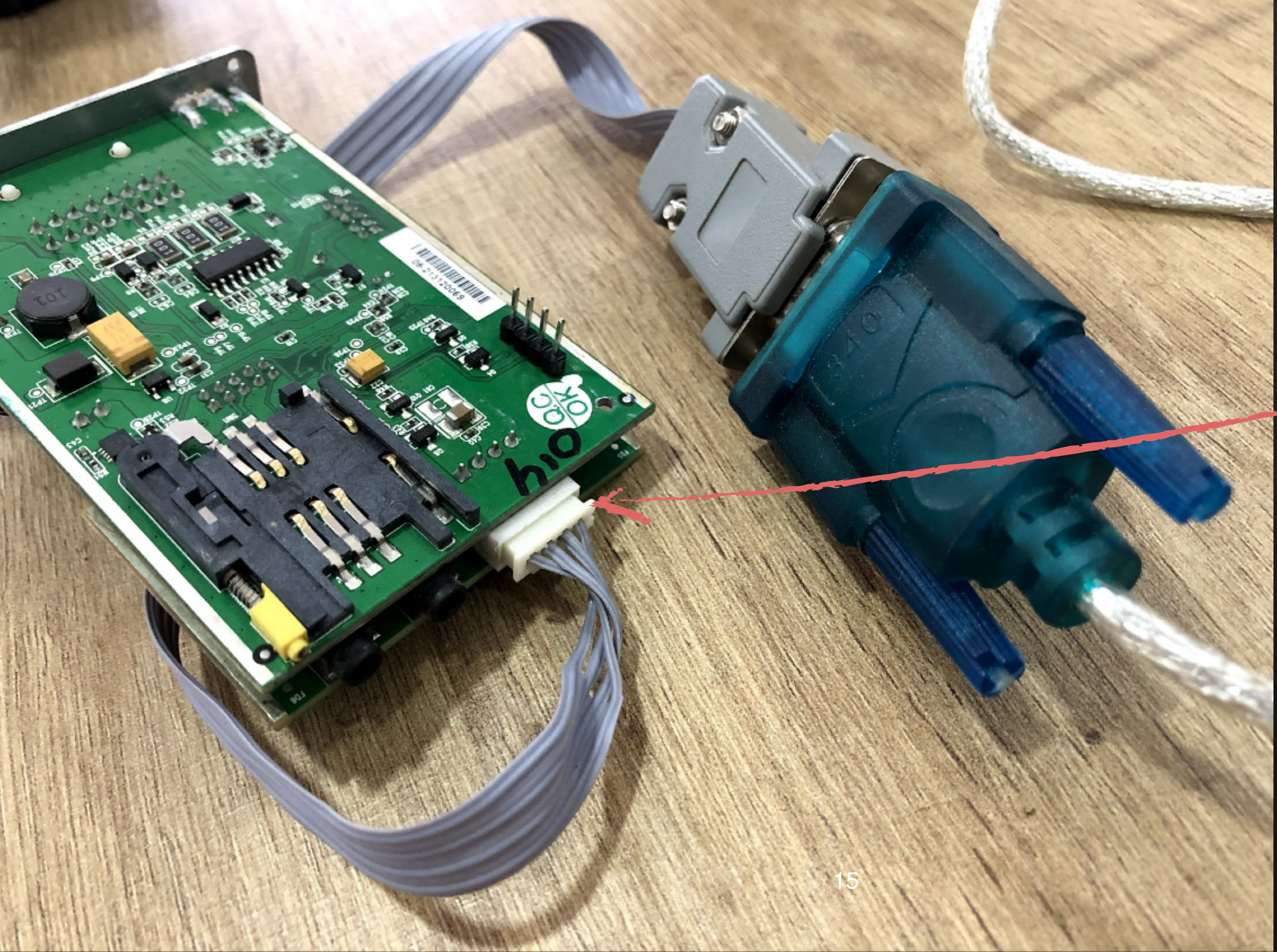
Remote
SMS,GPRS,
FTP

Attack Vectors



Local
Serial Parsers
Flash Parser
Code/Data

Remote
SMS
FTP



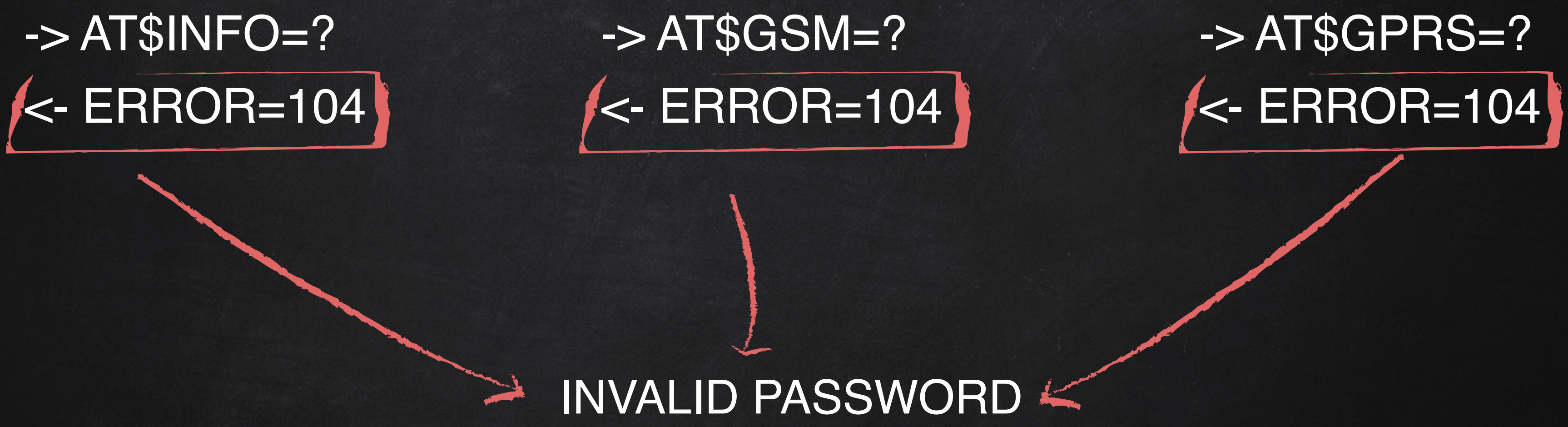
Starting easy: SERIAL PORT

Syntax

```
AT$<Command>[+Tag]=[Password,]<Parameter 1>, ... ,<Parameter N>
```

Examples

```
AT$INFO=?
AT$GPRS=?
AT$FOTA=1,"111.222.333.444",21,"user","passw","file.bin",0
```

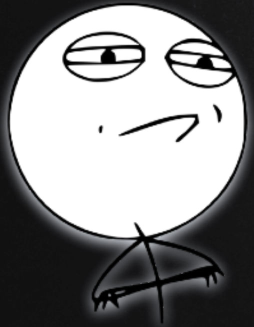


```
-> AT$INFO=?
<- ERROR=104
```

```
-> AT$GSM=?
<- ERROR=104
```

```
-> AT$GPRS=?
<- ERROR=104
```

INVALID PASSWORD



“

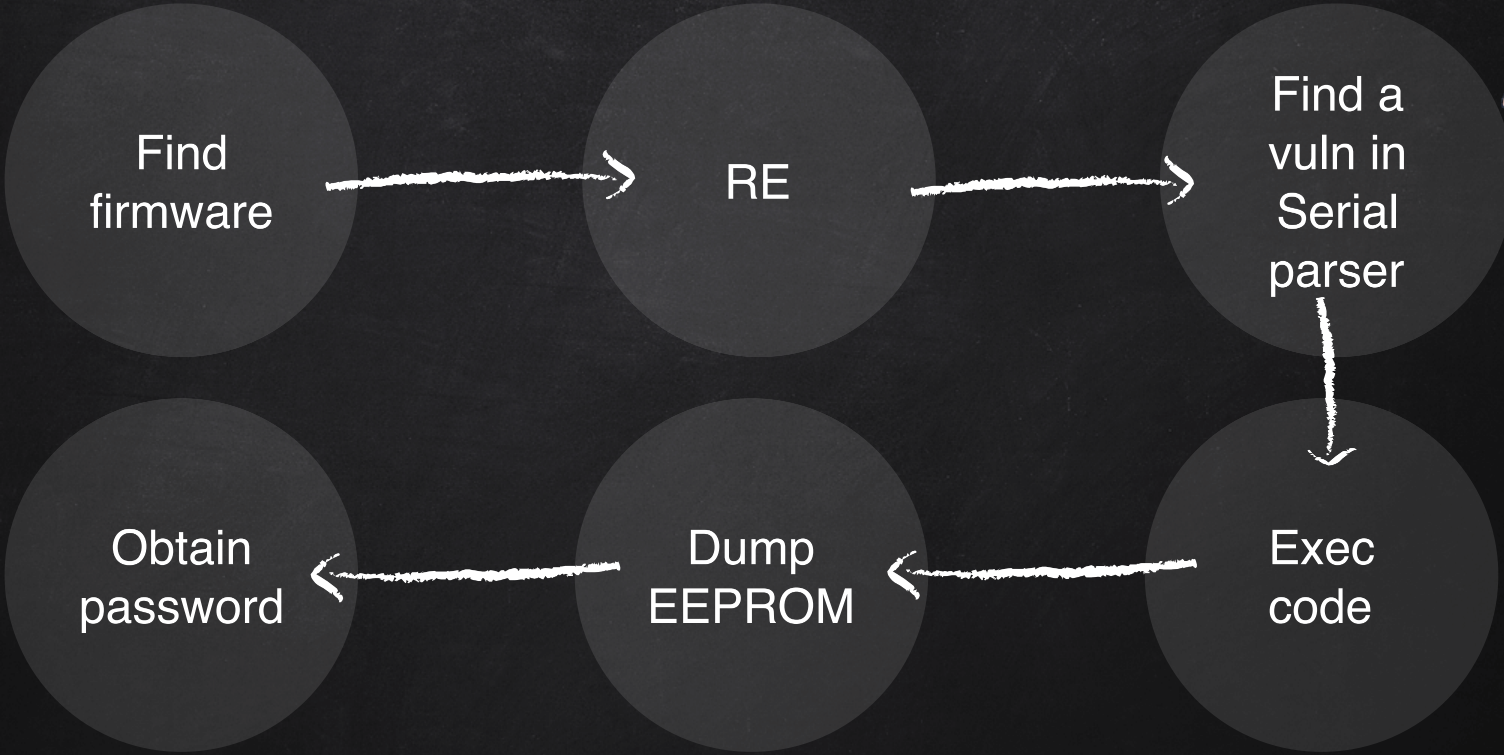
Just try all the possible passwords

“

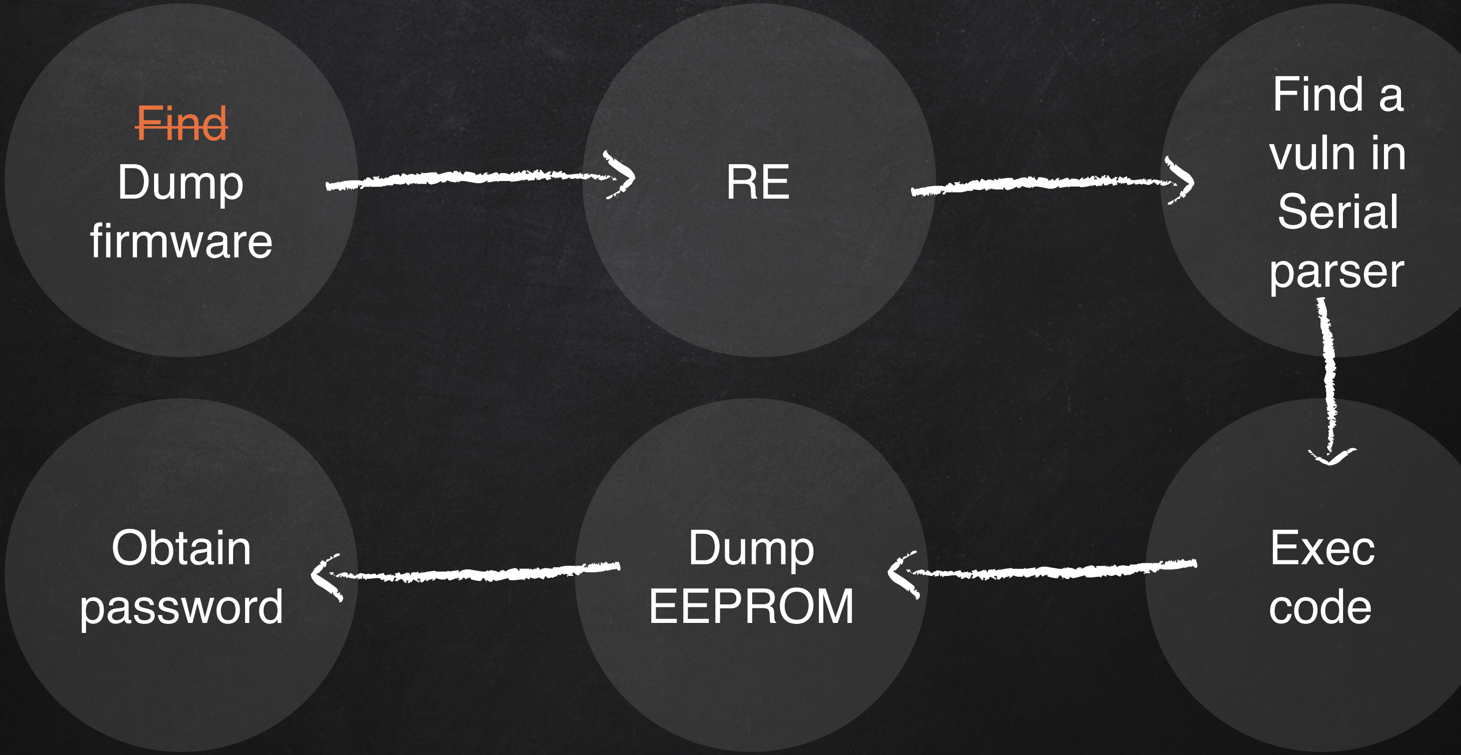
~~Just try all the possible passwords~~

Failed

The plan


Find firmware → RE → Find a vuln in Serial parser → Exec code → Dump EEPROM → Obtain password

The plan



~~Find~~ Dump firmware

RE

Find a vuln in Serial parser

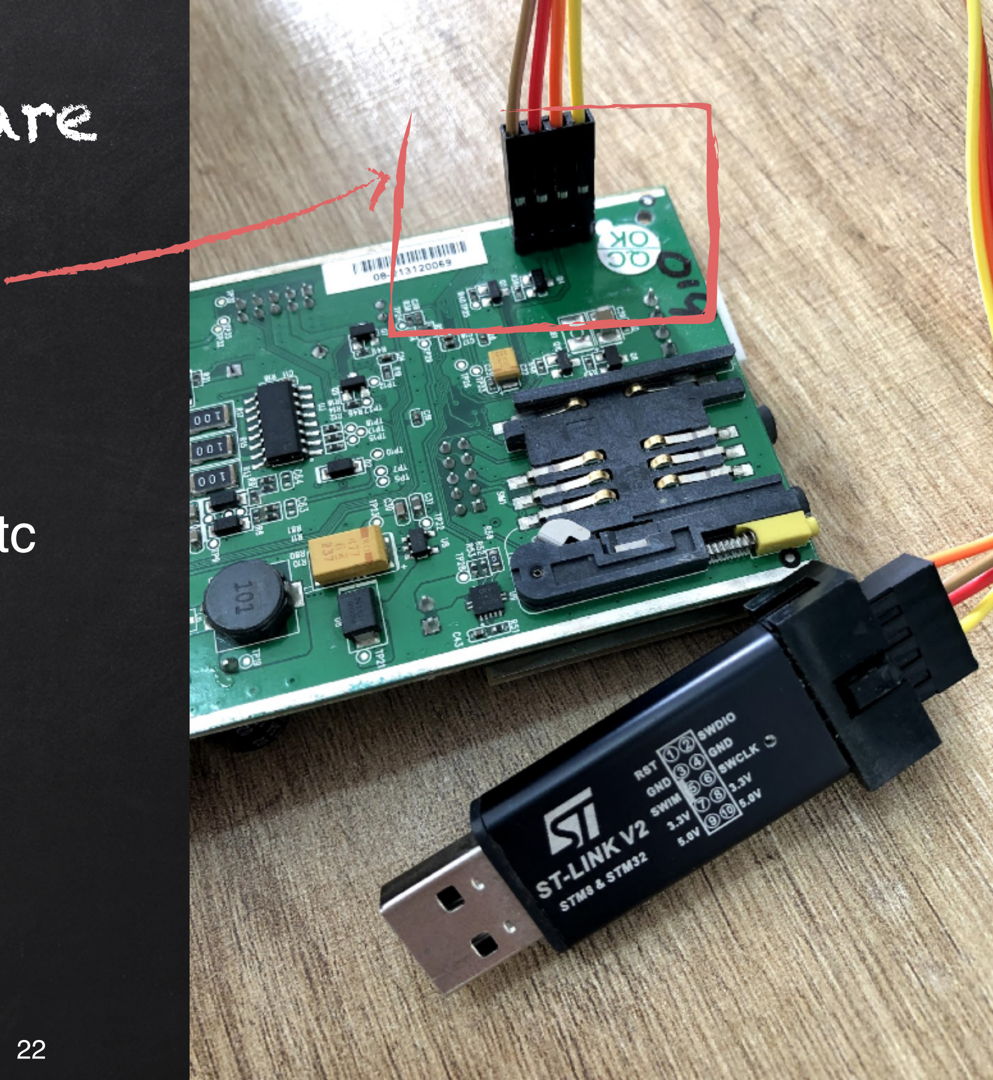
Exec code

Dump EEPROM

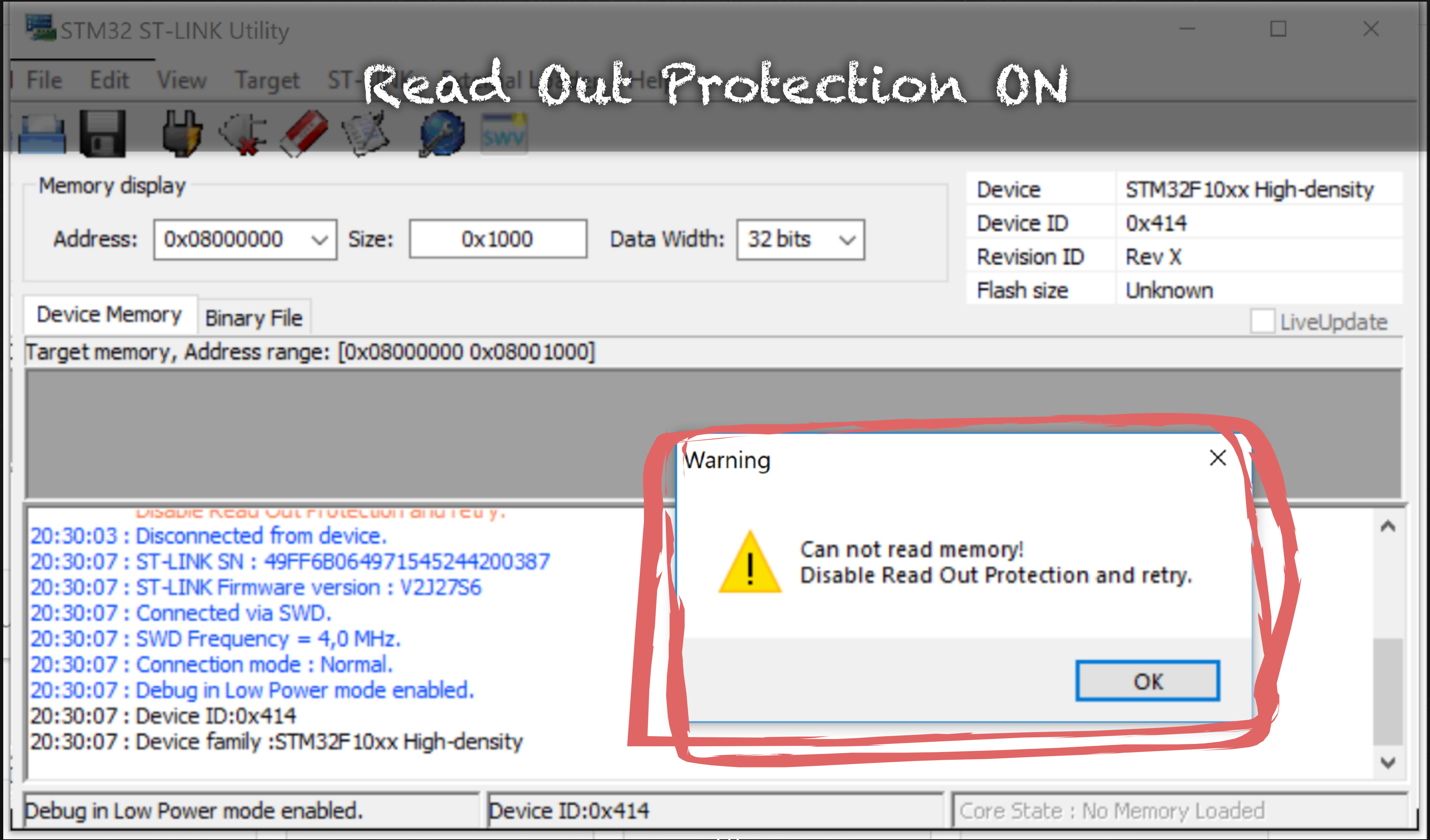
Obtain password

Dumping the firmware

- SWD Interface (Serial Wire Debug)
- Similar to JTAG
- Debug, Read, Write mem & regs, etc
- Need “special”programmer (cheap)



Read Out Protection ON



Memory display

Address: 0x08000000 Size: 0x1000 Data Width: 32 bits

Device	STM32F10xx High-density
Device ID	0x414
Revision ID	Rev X
Flash size	Unknown

Target memory, Address range: [0x08000000 0x08001000]

```
Disable Read Out Protection and retry.
20:30:03 : Disconnected from device.
20:30:07 : ST-LINK SN : 49FF6B064971545244200387
20:30:07 : ST-LINK Firmware version : V2J27S6
20:30:07 : Connected via SWD.
20:30:07 : SWD Frequency = 4,0 MHz.
20:30:07 : Connection mode : Normal.
20:30:07 : Debug in Low Power mode enabled.
20:30:07 : Device ID:0x414
20:30:07 : Device family :STM32F10xx High-density
```

Warning

Can not read memory!
Disable Read Out Protection and retry.

Debug in Low Power mode enabled. Device ID:0x414 Core State : No Memory Loaded

Flash Readout Protection

Level 0: No protection

Level 1: Debug interfaces enabled, flash access locked

Level 2: All debug interfaces disabled (not supported by stm32f1)

Bypass for STM32f0 family:

Awesome research by Obermaier and Tatschner!

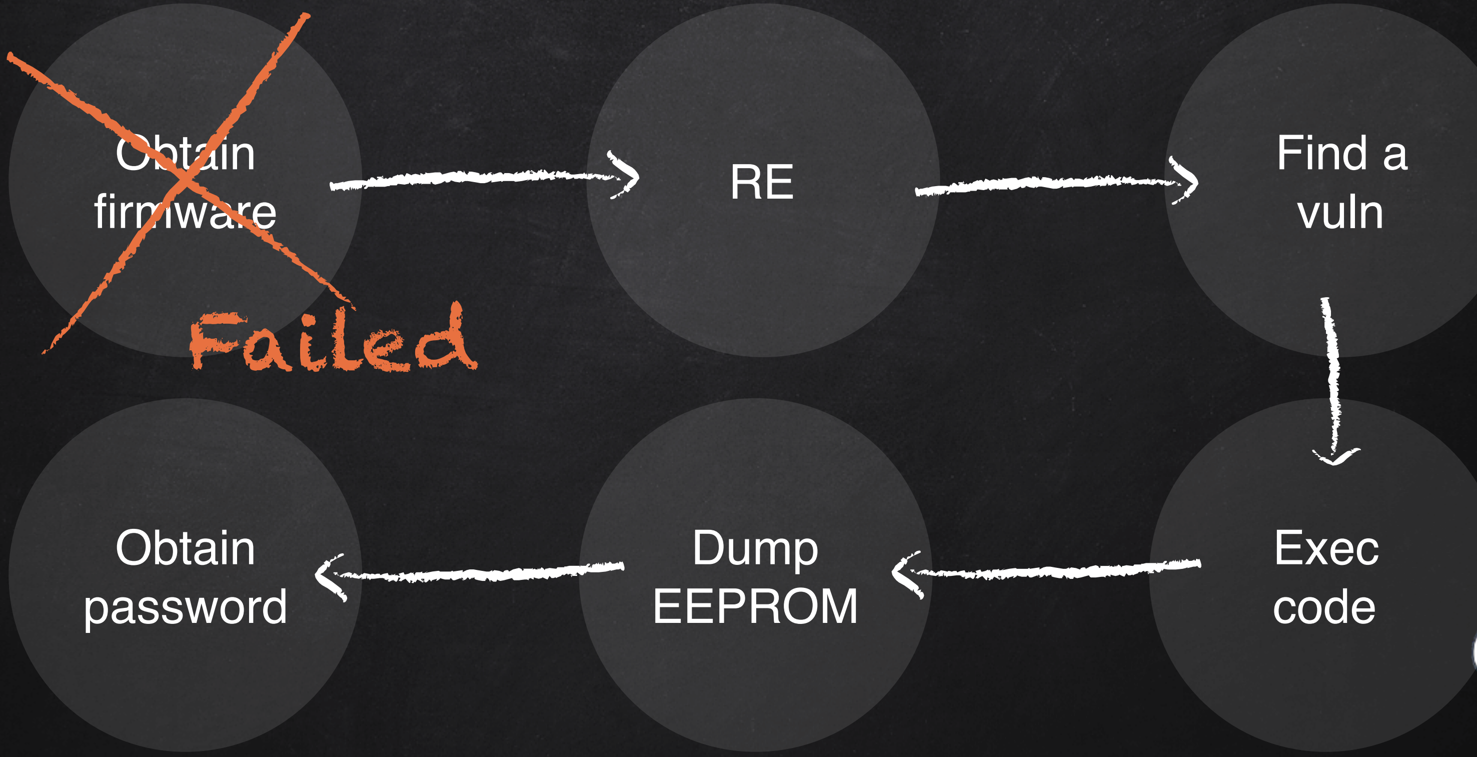
https://www.aisec.fraunhofer.de/content/dam/aisec/ResearchExcellence/woot17-paper-obermaier.pdf

Flash Readout Protection

Level 1: Debug interfaces enabled, flash access locked

- ✘ RAM is RW from SWD
  - ○ Can break target and see snapshot of the stack
- ✘ Can force ‘Boot from RAM’ by setting boot pins
  - ○ Can execute code!
- ✘ code executing from RAM can’ t read the flash

The plan



~~Obtain firmware~~

Failed

RE

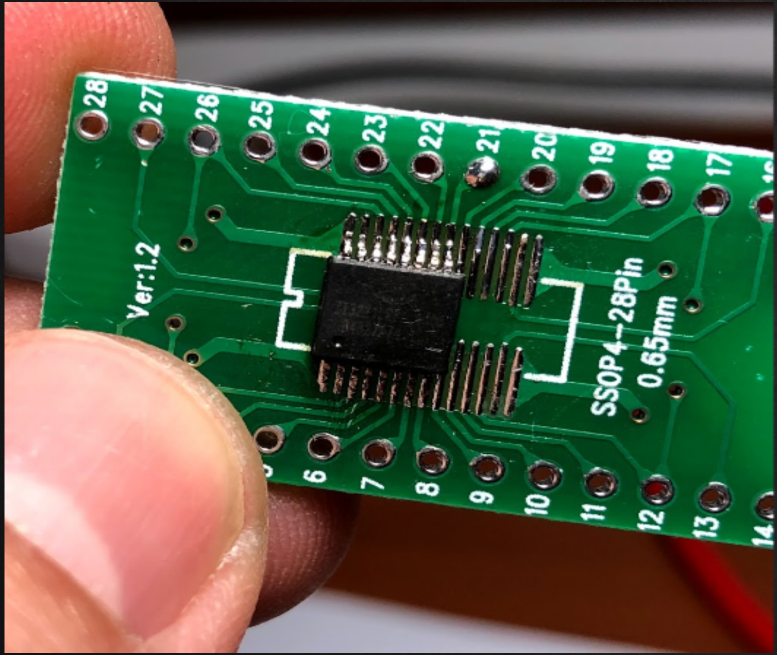
Find a vuln

Exec code

Dump EEPROM

Obtain password

Dumped the flash



- Some IPs from servers
- The password!
- Rest: unknown binary data

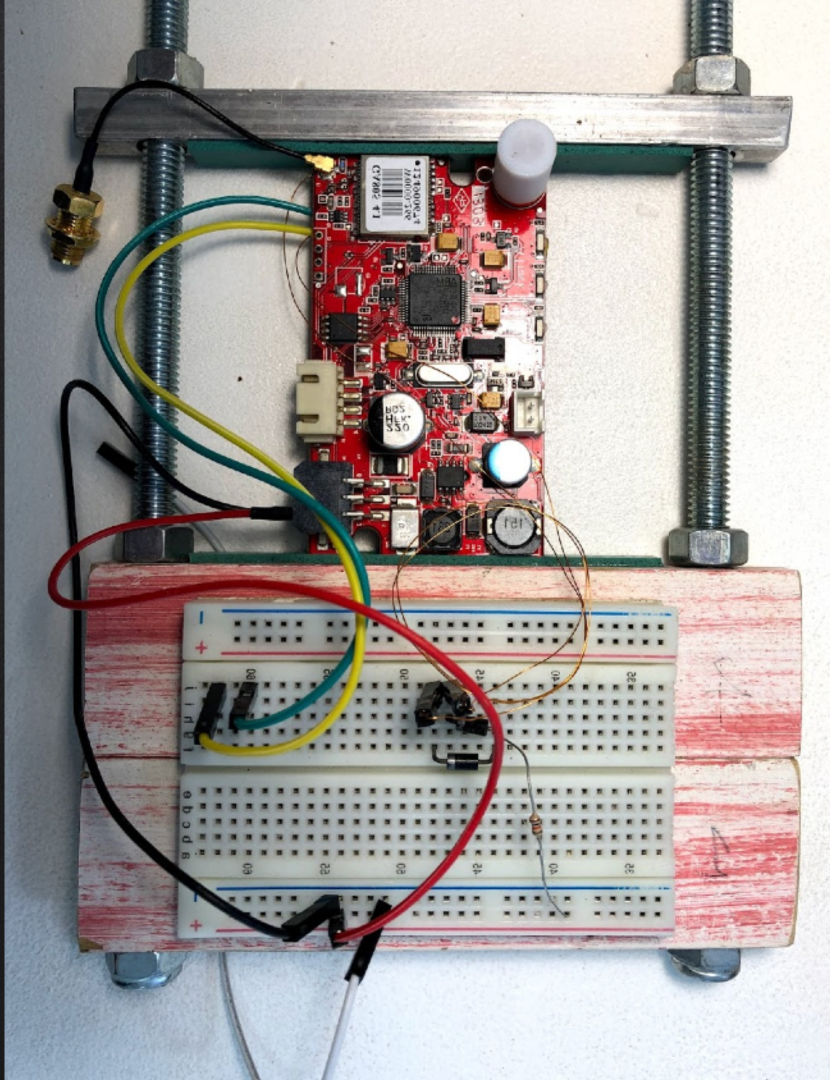
Test your bruteforcer!

```
-> AT$DLOG=thepassw,”090101000000","99010100000"
<- $ERROR=106   (No Log Data Available)
```

:(

Going wild \o/

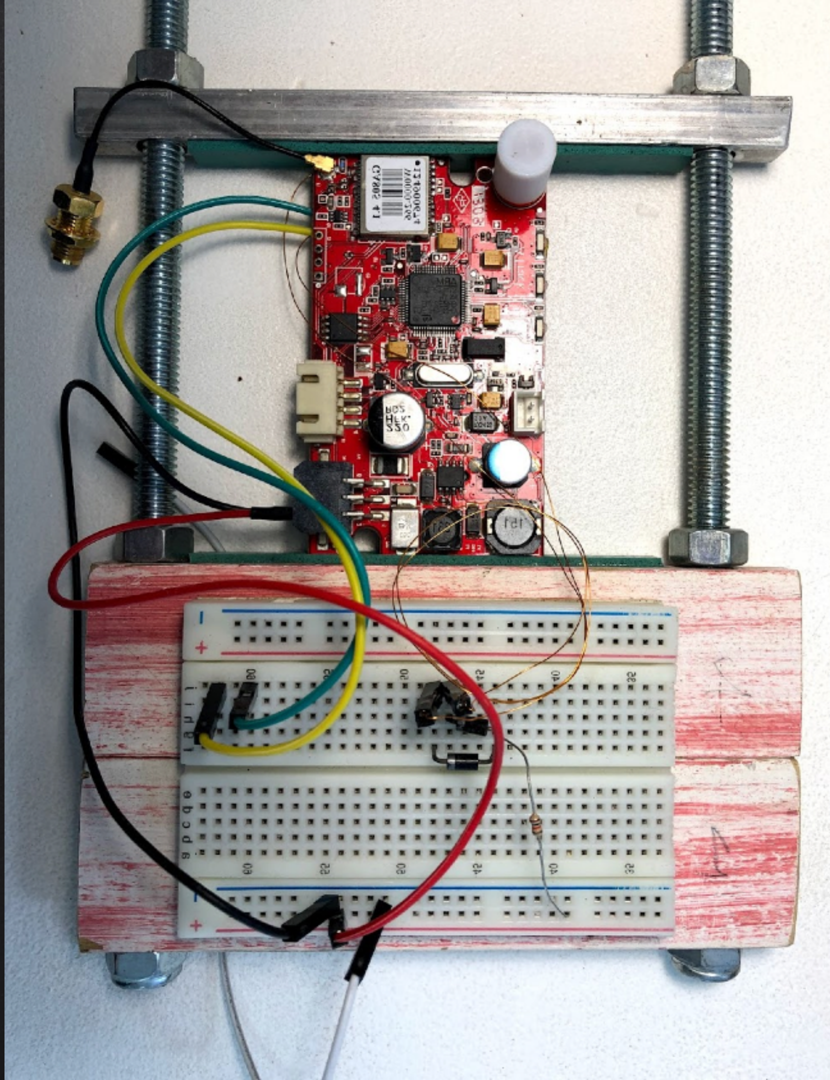
- Fuzzed Serial
- Fuzzed FOTA FTP via GPRS
- TAP into GSM-IC Serial
- Intention toFuzz GSM-IC Serial
- Etc, etc...

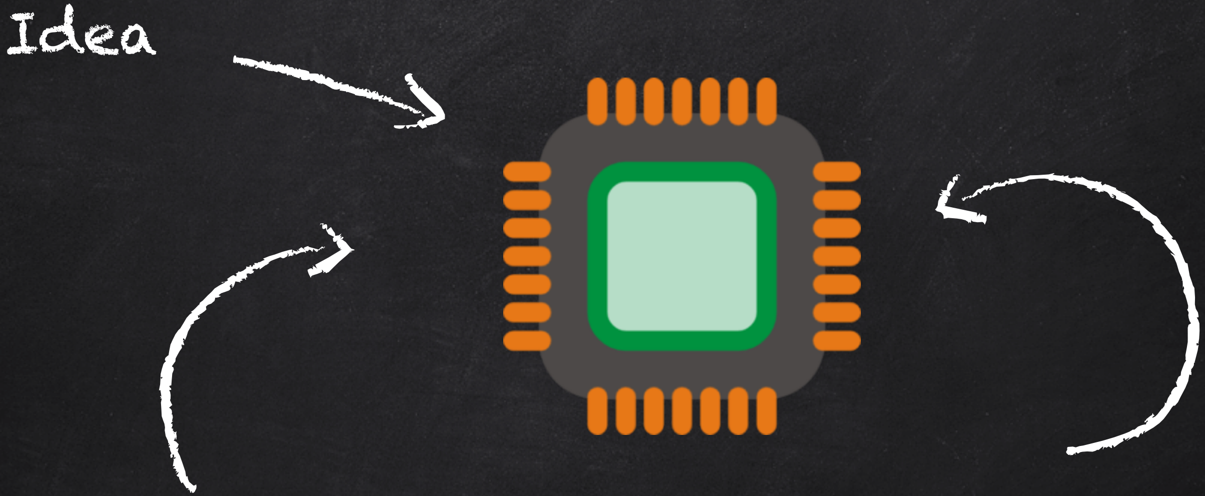


Going wild \o/

- Fuzzed Serial
- Fuzzed FOTA FTP via GPRS
- TAP into GSM-IC Serial
- Intention toFuzz GSM-IC Serial
- Etc, etc...

Failed Again

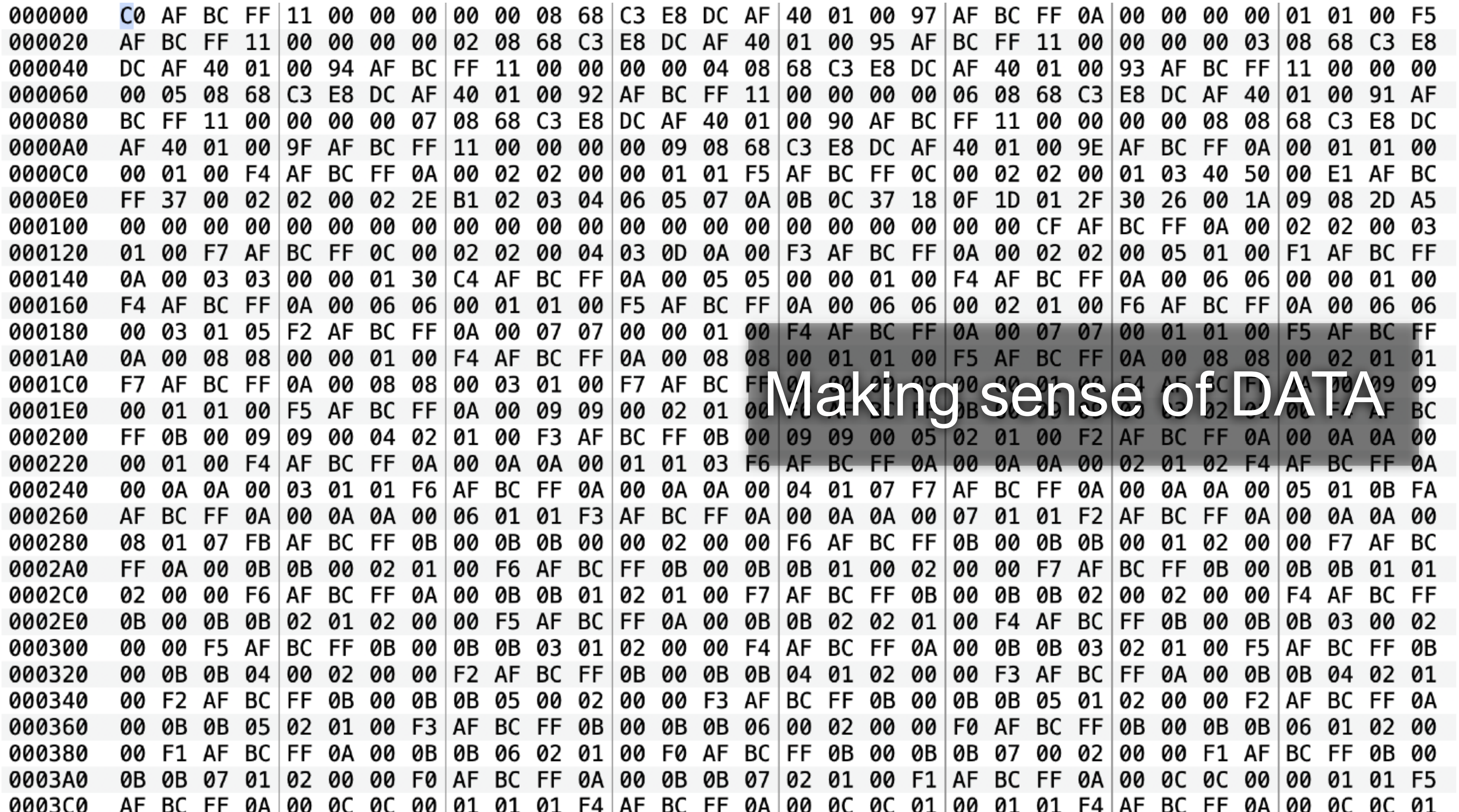




Idea

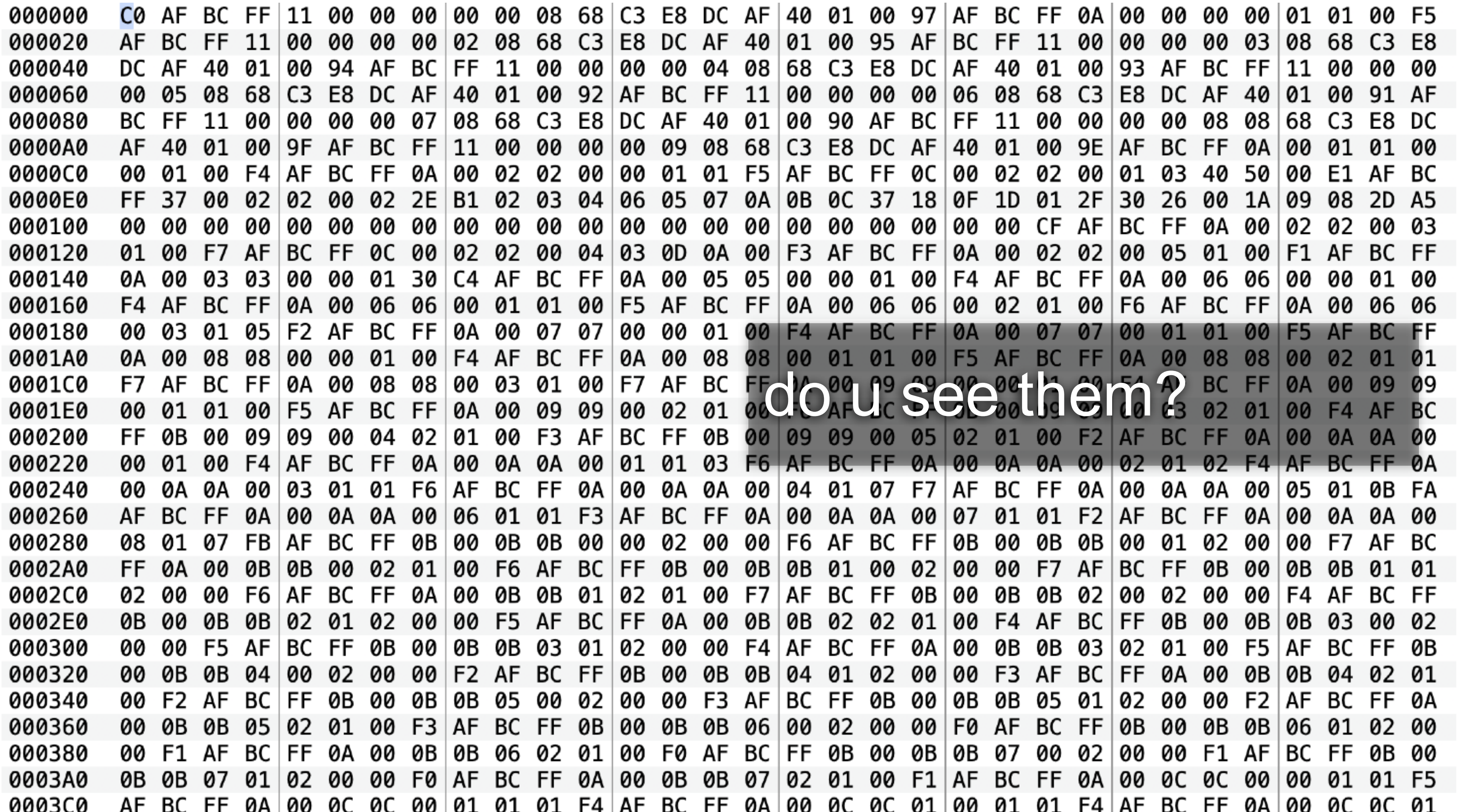
What (secrets) does the flash store?

Making sense of DATA



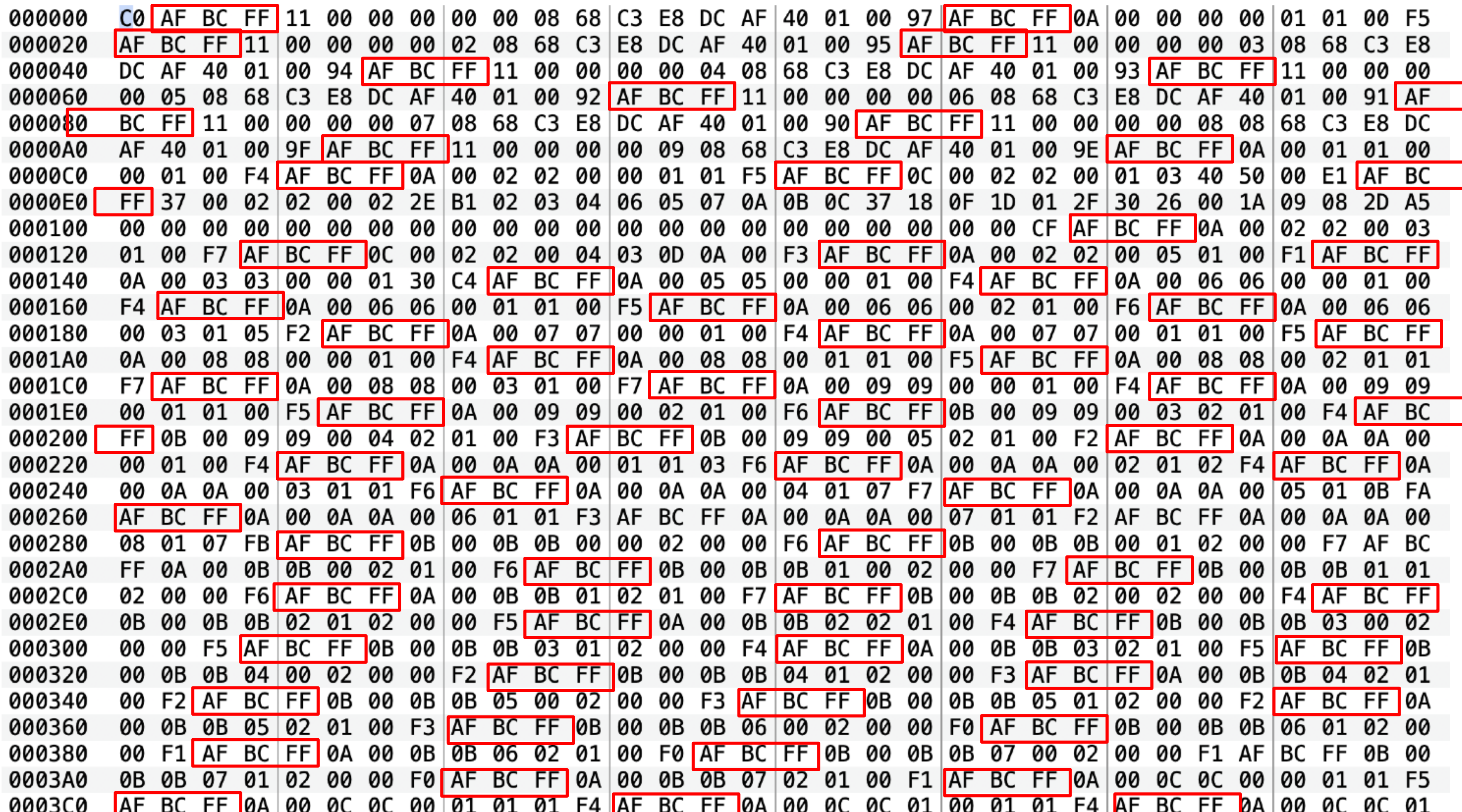
```
000000  C0 AF BC FF  11 00 00 00  00 00 08 68  C3 E8 DC AF  40 01 00 97  AF BC FF 0A  00 00 00 00  01 01 00 F5
000020  AF BC FF 11  00 00 00 00  02 08 68 C3  E8 DC AF 40  01 00 95 AF  BC FF 11 00  00 00 00 03  08 68 C3 E8
000040  DC AF 40 01  00 94 AF BC  FF 11 00 00  00 00 04 08  68 C3 E8 DC  AF 40 01 00  93 AF BC FF  11 00 00 00
000060  00 05 08 68  C3 E8 DC AF  40 01 00 92  AF BC FF 11  00 00 00 00  06 08 68 C3  E8 DC AF 40  01 00 91 AF
000080  BC FF 11 00  00 00 00 07  08 68 C3 E8  DC AF 40 01  00 90 AF BC  FF 11 00 00  00 00 08 08  68 C3 E8 DC
0000A0  AF 40 01 00  9F AF BC FF  11 00 00 00  00 09 08 68  C3 E8 DC AF  40 01 00 9E  AF BC FF 0A  00 01 01 00
0000C0  00 01 00 F4  AF BC FF 0A  00 02 02 00  00 01 01 F5  AF BC FF 0C  00 02 02 00  01 03 40 50  00 E1 AF BC
0000E0  FF 37 00 02  02 00 02 2E  B1 02 03 04  06 05 07 0A  0B 0C 37 18  0F 1D 01 2F  30 26 00 1A  09 08 2D A5
000100  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  00 00 CF AF  BC FF 0A 00  02 02 00 03
000120  01 00 F7 AF  BC FF 0C 00  02 02 00 04  03 0D 0A 00  F3 AF BC FF  0A 00 02 02  00 05 01 00  F1 AF BC FF
000140  0A 00 03 03  00 00 01 30  C4 AF BC FF  0A 00 05 05  00 00 01 00  F4 AF BC FF  0A 00 06 06  00 00 01 00
000160  F4 AF BC FF  0A 00 06 06  00 01 01 00  F5 AF BC FF  0A 00 06 06  00 02 01 00  F6 AF BC FF  0A 00 06 06
000180  00 03 01 05  F2 AF BC FF  0A 00 07 07  00 00 01 00  F4 AF BC FF  0A 00 07 07  00 01 01 00  F5 AF BC FF
0001A0  0A 00 08 08  00 00 01 00  F4 AF BC FF  0A 00 08 08  00 01 01 00  F5 AF BC FF  0A 00 08 08  00 02 01 01
0001C0  F7 AF BC FF  0A 00 08 08  00 03 01 00  F7 AF BC FF  0A 00 09 09  00 00 01 00  F4 AF BC FF  0A 00 09 09
0001E0  00 01 01 00  F5 AF BC FF  0A 00 09 09  00 02 01 00  F6 AF BC FF  0B 00 09 09  00 03 02 01  00 F4 AF BC
000200  FF 0B 00 09  09 00 04 02  01 00 F3 AF  BC FF 0B 00  09 09 00 05  02 01 00 F2  AF BC FF 0A  00 0A 0A 00
000220  00 01 00 F4  AF BC FF 0A  00 0A 0A 00  01 01 03 F6  AF BC FF 0A  00 0A 0A 00  02 01 02 F4  AF BC FF 0A
000240  00 0A 0A 00  03 01 01 F6  AF BC FF 0A  00 0A 0A 00  04 01 07 F7  AF BC FF 0A  00 0A 0A 00  05 01 0B FA
000260  AF BC FF 0A  00 0A 0A 00  06 01 01 F3  AF BC FF 0A  00 0A 0A 00  07 01 01 F2  AF BC FF 0A  00 0A 0A 00
000280  08 01 07 FB  AF BC FF 0B  00 0B 0B 00  00 02 00 00  F6 AF BC FF  0B 00 0B 0B  00 01 02 00  00 F7 AF BC
0002A0  FF 0A 00 0B  0B 00 02 01  00 F6 AF BC  FF 0B 00 0B  0B 01 00 02  00 00 F7 AF  BC FF 0B 00  0B 0B 01 01
0002C0  02 00 00 F6  AF BC FF 0A  00 0B 0B 01  02 01 00 F7  AF BC FF 0B  00 0B 0B 02  00 02 00 00  F4 AF BC FF
0002E0  0B 00 0B 0B  02 01 02 00  00 F5 AF BC  FF 0A 00 0B  0B 02 02 01  00 F4 AF BC  FF 0B 00 0B  0B 03 00 02
000300  00 00 F5 AF  BC FF 0B 00  0B 0B 03 01  02 00 00 F4  AF BC FF 0A  00 0B 0B 03  02 01 00 F5  AF BC FF 0B
000320  00 0B 0B 04  00 02 00 00  F2 AF BC FF  0B 00 0B 0B  04 01 02 00  00 F3 AF BC  FF 0A 00 0B  0B 04 02 01
000340  00 F2 AF BC  FF 0B 00 0B  0B 05 00 02  00 00 F3 AF  BC FF 0B 00  0B 0B 05 01  02 00 00 F2  AF BC FF 0A
000360  00 0B 0B 05  02 01 00 F3  AF BC FF 0B  00 0B 0B 06  00 02 00 00  F0 AF BC FF  0B 00 0B 0B  06 01 02 00
000380  00 F1 AF BC  FF 0A 00 0B  0B 06 02 01  00 F0 AF BC  FF 0B 00 0B  0B 07 00 02  00 00 F1 AF  BC FF 0B 00
0003A0  0B 0B 07 01  02 00 00 F0  AF BC FF 0A  00 0B 0B 07  02 01 00 F1  AF BC FF 0A  00 0C 0C 00  00 01 01 F5
0003C0  AF BC FF 0A  00 0C 0C 00  01 01 01 F4  AF BC FF 0A  00 0C 0C 01  00 01 01 F4  AF BC FF 0A  00 0C 0C 01
```

I see data patterns

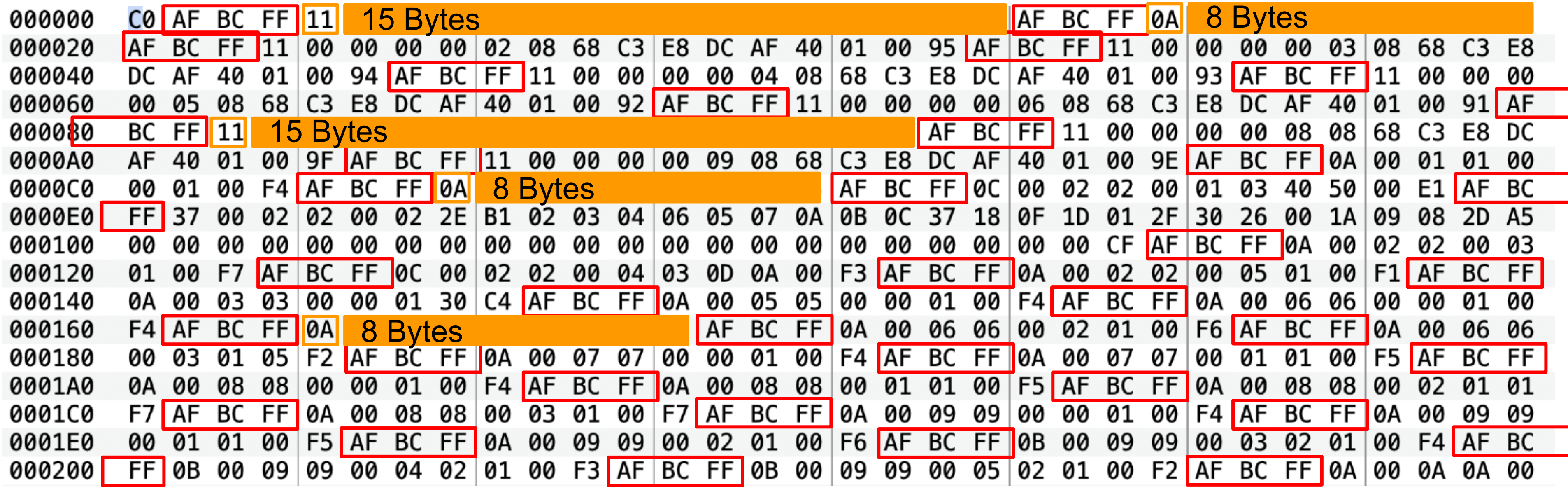


```
000000  C0 AF BC FF 11 00 00 00 00 00 08 68 C3 E8 DC AF 40 01 00 97 AF BC FF 0A 00 00 00 00 01 01 00 F5
000020  AF BC FF 11 00 00 00 00 02 08 68 C3 E8 DC AF 40 01 00 95 AF BC FF 11 00 00 00 00 03 08 68 C3 E8
000040  DC AF 40 01 00 94 AF BC FF 11 00 00 00 00 04 08 68 C3 E8 DC AF 40 01 00 93 AF BC FF 11 00 00 00
000060  00 05 08 68 C3 E8 DC AF 40 01 00 92 AF BC FF 11 00 00 00 00 06 08 68 C3 E8 DC AF 40 01 00 91 AF
000080  BC FF 11 00 00 00 00 07 08 68 C3 E8 DC AF 40 01 00 90 AF BC FF 11 00 00 00 00 08 08 68 C3 E8 DC
0000A0  AF 40 01 00 9F AF BC FF 11 00 00 00 00 09 08 68 C3 E8 DC AF 40 01 00 9E AF BC FF 0A 00 01 01 00
0000C0  00 01 00 F4 AF BC FF 0A 00 02 02 00 00 01 01 F5 AF BC FF 0C 00 02 02 00 01 03 40 50 00 E1 AF BC
0000E0  FF 37 00 02 02 00 02 2E B1 02 03 04 06 05 07 0A 0B 0C 37 18 0F 1D 01 2F 30 26 00 1A 09 08 2D A5
000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CF AF BC FF 0A 00 02 02 00 03
000120  01 00 F7 AF BC FF 0C 00 02 02 00 04 03 0D 0A 00 F3 AF BC FF 0A 00 02 02 00 05 01 00 F1 AF BC FF
000140  0A 00 03 03 00 00 01 30 C4 AF BC FF 0A 00 05 05 00 00 01 00 F4 AF BC FF 0A 00 06 06 00 00 01 00
000160  F4 AF BC FF 0A 00 06 06 00 01 01 00 F5 AF BC FF 0A 00 06 06 00 02 01 00 F6 AF BC FF 0A 00 06 06
000180  00 03 01 05 F2 AF BC FF 0A 00 07 07 00 00 01 00 F4 AF BC FF 0A 00 07 07 00 01 01 00 F5 AF BC FF
0001A0  0A 00 08 08 00 00 01 00 F4 AF BC FF 0A 00 08 08 00 01 01 00 F5 AF BC FF 0A 00 08 08 00 02 01 01
0001C0  F7 AF BC FF 0A 00 08 08 00 03 01 00 F7 AF BC FF 0A 00 09 09 00 00 01 00 F4 AF BC FF 0A 00 09 09
0001E0  00 01 01 00 F5 AF BC FF 0A 00 09 09 00 02 01 00 F6 AF BC FF 0B 00 09 09 00 03 02 01 00 F4 AF BC
000200  FF 0B 00 09 09 00 04 02 01 00 F3 AF BC FF 0B 00 09 09 00 05 02 01 00 F2 AF BC FF 0A 00 0A 0A 00
000220  00 01 00 F4 AF BC FF 0A 00 0A 0A 00 01 01 03 F6 AF BC FF 0A 00 0A 0A 00 02 01 02 F4 AF BC FF 0A
000240  00 0A 0A 00 03 01 01 F6 AF BC FF 0A 00 0A 0A 00 04 01 07 F7 AF BC FF 0A 00 0A 0A 00 05 01 0B FA
000260  AF BC FF 0A 00 0A 0A 00 06 01 01 F3 AF BC FF 0A 00 0A 0A 00 07 01 01 F2 AF BC FF 0A 00 0A 0A 00
000280  08 01 07 FB AF BC FF 0B 00 0B 0B 00 00 02 00 00 F6 AF BC FF 0B 00 0B 0B 00 01 02 00 00 F7 AF BC
0002A0  FF 0A 00 0B 0B 00 02 01 00 F6 AF BC FF 0B 00 0B 0B 01 00 02 00 00 F7 AF BC FF 0B 00 0B 0B 01 01
0002C0  02 00 00 F6 AF BC FF 0A 00 0B 0B 01 02 01 00 F7 AF BC FF 0B 00 0B 0B 02 00 02 00 00 F4 AF BC FF
0002E0  0B 00 0B 0B 02 01 02 00 00 F5 AF BC FF 0A 00 0B 0B 02 02 01 00 F4 AF BC FF 0B 00 0B 0B 03 00 02
000300  00 00 F5 AF BC FF 0B 00 0B 0B 03 01 02 00 00 F4 AF BC FF 0A 00 0B 0B 03 02 01 00 F5 AF BC FF 0B
000320  00 0B 0B 04 00 02 00 00 F2 AF BC FF 0B 00 0B 0B 04 01 02 00 00 F3 AF BC FF 0A 00 0B 0B 04 02 01
000340  00 F2 AF BC FF 0B 00 0B 0B 05 00 02 00 00 F3 AF BC FF 0B 00 0B 0B 05 01 02 00 00 F2 AF BC FF 0A
000360  00 0B 0B 05 02 01 00 F3 AF BC FF 0B 00 0B 0B 06 00 02 00 00 F0 AF BC FF 0B 00 0B 0B 06 01 02 00
000380  00 F1 AF BC FF 0A 00 0B 0B 06 02 01 00 F0 AF BC FF 0B 00 0B 0B 07 00 02 00 00 F1 AF BC FF 0B 00
0003A0  0B 0B 07 01 02 00 00 F0 AF BC FF 0A 00 0B 0B 07 02 01 00 F1 AF BC FF 0A 00 0C 0C 00 00 01 01 F5
0003C0  AF BC FF 0A 00 0C 0C 00 01 01 01 F4 AF BC FF 0A 00 0C 0C 01 00 01 01 F4 AF BC FF 0A 00 0C 0C 01
```

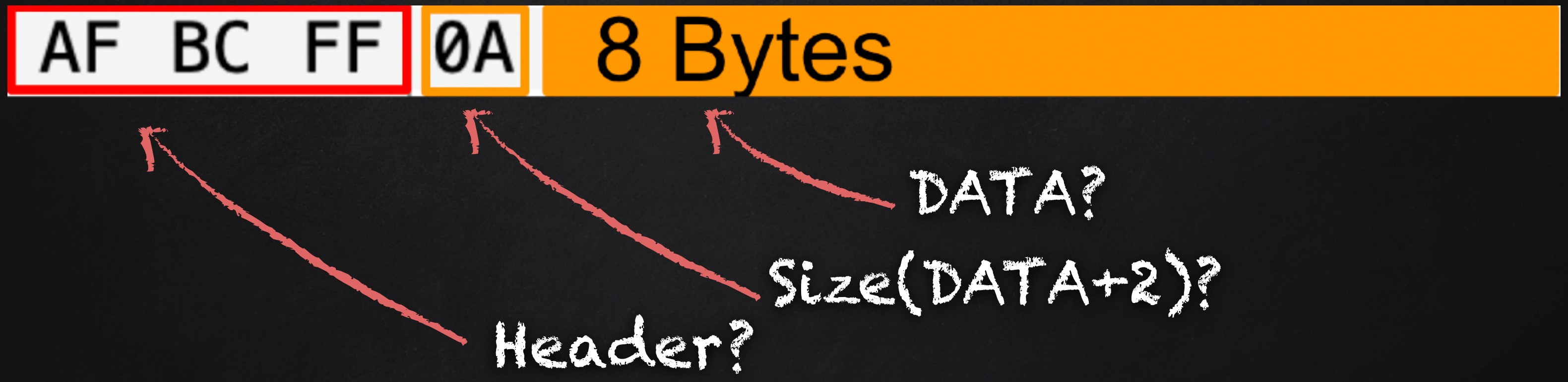
do u see them?



```
000000  C0 AF BC FF 11 00 00 00 00 00 08 68 C3 E8 DC AF 40 01 00 97 AF BC FF 0A 00 00 00 00 01 01 00 F5
000020  AF BC FF 11 00 00 00 00 02 08 68 C3 E8 DC AF 40 01 00 95 AF BC FF 11 00 00 00 00 03 08 68 C3 E8
000040  DC AF 40 01 00 94 AF BC FF 11 00 00 00 00 04 08 68 C3 E8 DC AF 40 01 00 93 AF BC FF 11 00 00 00
000060  00 05 08 68 C3 E8 DC AF 40 01 00 92 AF BC FF 11 00 00 00 00 06 08 68 C3 E8 DC AF 40 01 00 91 AF
000080  BC FF 11 00 00 00 00 07 08 68 C3 E8 DC AF 40 01 00 90 AF BC FF 11 00 00 00 00 08 08 68 C3 E8 DC
0000A0  AF 40 01 00 9F AF BC FF 11 00 00 00 00 09 08 68 C3 E8 DC AF 40 01 00 9E AF BC FF 0A 00 01 01 00
0000C0  00 01 00 F4 AF BC FF 0A 00 02 02 00 00 01 01 F5 AF BC FF 0C 00 02 02 00 01 03 40 50 00 E1 AF BC
0000E0  FF 37 00 02 02 00 02 2E B1 02 03 04 06 05 07 0A 0B 0C 37 18 0F 1D 01 2F 30 26 00 1A 09 08 2D A5
000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CF AF BC FF 0A 00 02 02 00 03
000120  01 00 F7 AF BC FF 0C 00 02 02 00 04 03 0D 0A 00 F3 AF BC FF 0A 00 02 02 00 05 01 00 F1 AF BC FF
000140  0A 00 03 03 00 00 01 30 C4 AF BC FF 0A 00 05 05 00 00 01 00 F4 AF BC FF 0A 00 06 06 00 00 01 00
000160  F4 AF BC FF 0A 00 06 06 00 01 01 00 F5 AF BC FF 0A 00 06 06 00 02 01 00 F6 AF BC FF 0A 00 06 06
000180  00 03 01 05 F2 AF BC FF 0A 00 07 07 00 00 01 00 F4 AF BC FF 0A 00 07 07 00 01 01 00 F5 AF BC FF
0001A0  0A 00 08 08 00 00 01 00 F4 AF BC FF 0A 00 08 08 00 01 01 00 F5 AF BC FF 0A 00 08 08 00 02 01 01
0001C0  F7 AF BC FF 0A 00 08 08 00 03 01 00 F7 AF BC FF 0A 00 09 09 00 00 01 00 F4 AF BC FF 0A 00 09 09
0001E0  00 01 01 00 F5 AF BC FF 0A 00 09 09 00 02 01 00 F6 AF BC FF 0B 00 09 09 00 03 02 01 00 F4 AF BC
000200  FF 0B 00 09 09 00 04 02 01 00 F3 AF BC FF 0B 00 09 09 00 05 02 01 00 F2 AF BC FF 0A 00 0A 0A 00
000220  00 01 00 F4 AF BC FF 0A 00 0A 0A 00 01 01 03 F6 AF BC FF 0A 00 0A 0A 00 02 01 02 F4 AF BC FF 0A
000240  00 0A 0A 00 03 01 01 F6 AF BC FF 0A 00 0A 0A 00 04 01 07 F7 AF BC FF 0A 00 0A 0A 00 05 01 0B FA
000260  AF BC FF 0A 00 0A 0A 00 06 01 01 F3 AF BC FF 0A 00 0A 0A 00 07 01 01 F2 AF BC FF 0A 00 0A 0A 00
000280  08 01 07 FB AF BC FF 0B 00 0B 0B 00 00 02 00 00 F6 AF BC FF 0B 00 0B 0B 00 01 02 00 00 F7 AF BC
0002A0  FF 0A 00 0B 0B 00 02 01 00 F6 AF BC FF 0B 00 0B 0B 01 00 02 00 00 F7 AF BC FF 0B 00 0B 0B 01 01
0002C0  02 00 00 F6 AF BC FF 0A 00 0B 0B 01 02 01 00 F7 AF BC FF 0B 00 0B 0B 02 00 02 00 00 F4 AF BC FF
0002E0  0B 00 0B 0B 02 01 02 00 00 F5 AF BC FF 0A 00 0B 0B 02 02 01 00 F4 AF BC FF 0B 00 0B 0B 03 00 02
000300  00 00 F5 AF BC FF 0B 00 0B 0B 03 01 02 00 00 F4 AF BC FF 0A 00 0B 0B 03 02 01 00 F5 AF BC FF 0B
000320  00 0B 0B 04 00 02 00 00 F2 AF BC FF 0B 00 0B 0B 04 01 02 00 00 F3 AF BC FF 0A 00 0B 0B 04 02 01
000340  00 F2 AF BC FF 0B 00 0B 0B 05 00 02 00 00 F3 AF BC FF 0B 00 0B 0B 05 01 02 00 00 F2 AF BC FF 0A
000360  00 0B 0B 05 02 01 00 F3 AF BC FF 0B 00 0B 0B 06 00 02 00 00 F0 AF BC FF 0B 00 0B 0B 06 01 02 00
000380  00 F1 AF BC FF 0A 00 0B 0B 06 02 01 00 F0 AF BC FF 0B 00 0B 0B 07 00 02 00 00 F1 AF BC FF 0B 00
0003A0  0B 0B 07 01 02 00 00 F0 AF BC FF 0A 00 0B 0B 07 02 01 00 F1 AF BC FF 0A 00 0C 0C 00 00 01 01 F5
0003C0  AF BC FF 0A 00 0C 0C 00 01 01 01 F4 AF BC FF 0A 00 0C 0C 01 00 01 01 F4 AF BC FF 0A 00 0C 0C 01
```



```
000000  C0 AF BC FF 11 15 Bytes                                 AF BC FF 0A 8 Bytes
000020  AF BC FF 11 00 00 00 00 02 08 68 C3 E8 DC AF 40 01 00 95 AF BC FF 11 00 00 00 00 03 08 68 C3 E8
000040  DC AF 40 01 00 94 AF BC FF 11 00 00 00 00 04 08 68 C3 E8 DC AF 40 01 00 93 AF BC FF 11 00 00 00
000060  00 05 08 68 C3 E8 DC AF 40 01 00 92 AF BC FF 11 00 00 00 00 06 08 68 C3 E8 DC AF 40 01 00 91 AF
000080  BC FF 11 15 Bytes                                 AF BC FF 11 00 00 00 00 08 08 68 C3 E8 DC
0000A0  AF 40 01 00 9F AF BC FF 11 00 00 00 00 09 08 68 C3 E8 DC AF 40 01 00 9E AF BC FF 0A 00 01 01 00
0000C0  00 01 00 F4 AF BC FF 0A 8 Bytes                   AF BC FF 0C 00 02 02 00 01 03 40 50 00 E1 AF BC
0000E0  FF 37 00 02 02 00 02 2E B1 02 03 04 06 05 07 0A 0B 0C 37 18 0F 1D 01 2F 30 26 00 1A 09 08 2D A5
000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CF AF BC FF 0A 00 02 02 00 03
000120  01 00 F7 AF BC FF 0C 00 02 02 00 04 03 0D 0A 00 F3 AF BC FF 0A 00 02 02 00 05 01 00 F1 AF BC FF
000140  0A 00 03 03 00 00 01 30 C4 AF BC FF 0A 00 05 05 00 00 01 00 F4 AF BC FF 0A 00 06 06 00 00 01 00
000160  F4 AF BC FF 0A 8 Bytes                   AF BC FF 0A 00 06 06 00 02 01 00 F6 AF BC FF 0A 00 06 06
000180  00 03 01 05 F2 AF BC FF 0A 00 07 07 00 00 01 00 F4 AF BC FF 0A 00 07 07 00 01 01 00 F5 AF BC FF
0001A0  0A 00 08 08 00 00 01 00 F4 AF BC FF 0A 00 08 08 00 01 01 00 F5 AF BC FF 0A 00 08 08 00 02 01 01
0001C0  F7 AF BC FF 0A 00 08 08 00 03 01 00 F7 AF BC FF 0A 00 09 09 00 00 01 00 F4 AF BC FF 0A 00 09 09
0001E0  00 01 01 00 F5 AF BC FF 0A 00 09 09 00 02 01 00 F6 AF BC FF 0B 00 09 09 00 03 02 01 00 F4 AF BC
000200  FF 0B 00 09 09 00 04 02 01 00 F3 AF BC FF 0B 00 09 09 00 05 02 01 00 F2 AF BC FF 0A 00 0A 0A 00
```



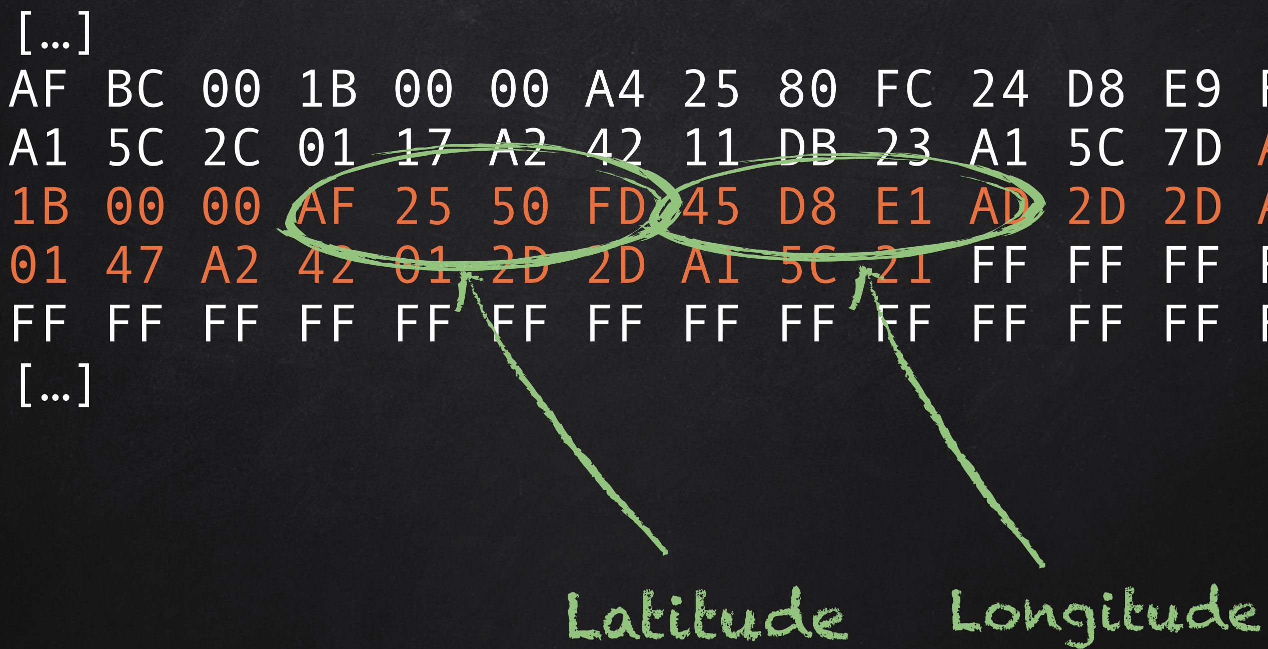
The breakthrough: Differential analysis

[disolder, dump, resolder, run, dump again] x N; Then compare

```
[…]
AF BC 00 1B 00 00 A4 25 80 FC 24 D8 E9 FD DC 23
A1 5C 2C 01 17 A2 42 11 DB 23 A1 5C 7D AF BC FF
1B 00 00 AF 25 50 FD 45 D8 E1 AD 2D 2D A1 5C 1C
01 47 A2 42 01 2D 2D A1 5C 21 FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
[…]
```

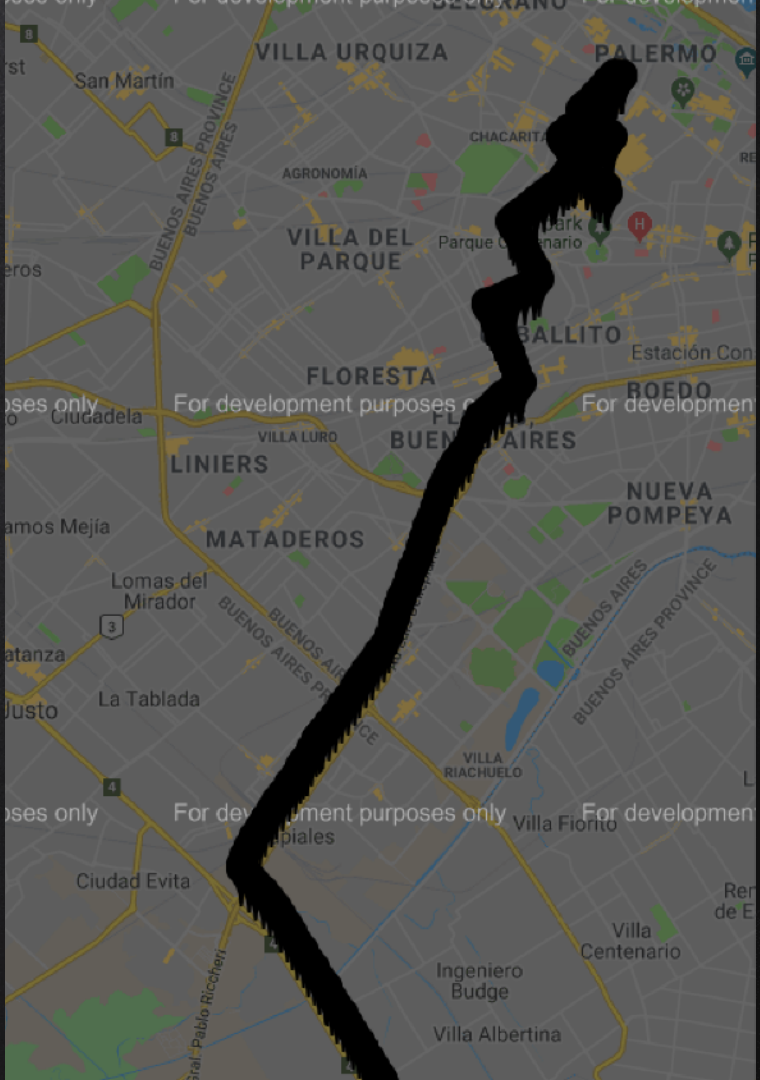
The breakthrough: Differential analysis

[disolder, dump, resolder, run, dump again] x N; Then compare



```
[…]
AF BC 00 1B 00 00 A4 25 80 FC 24 D8 E9 FD DC 23
A1 5C 2C 01 17 A2 42 11 DB 23 A1 5C 7D AF BC FF
1B 00 00 AF 25 50 FD 45 D8 E1 AD 2D 2D A1 5C 1C
01 47 A2 42 01 2D 2D A1 5C 21 FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
[…]
```

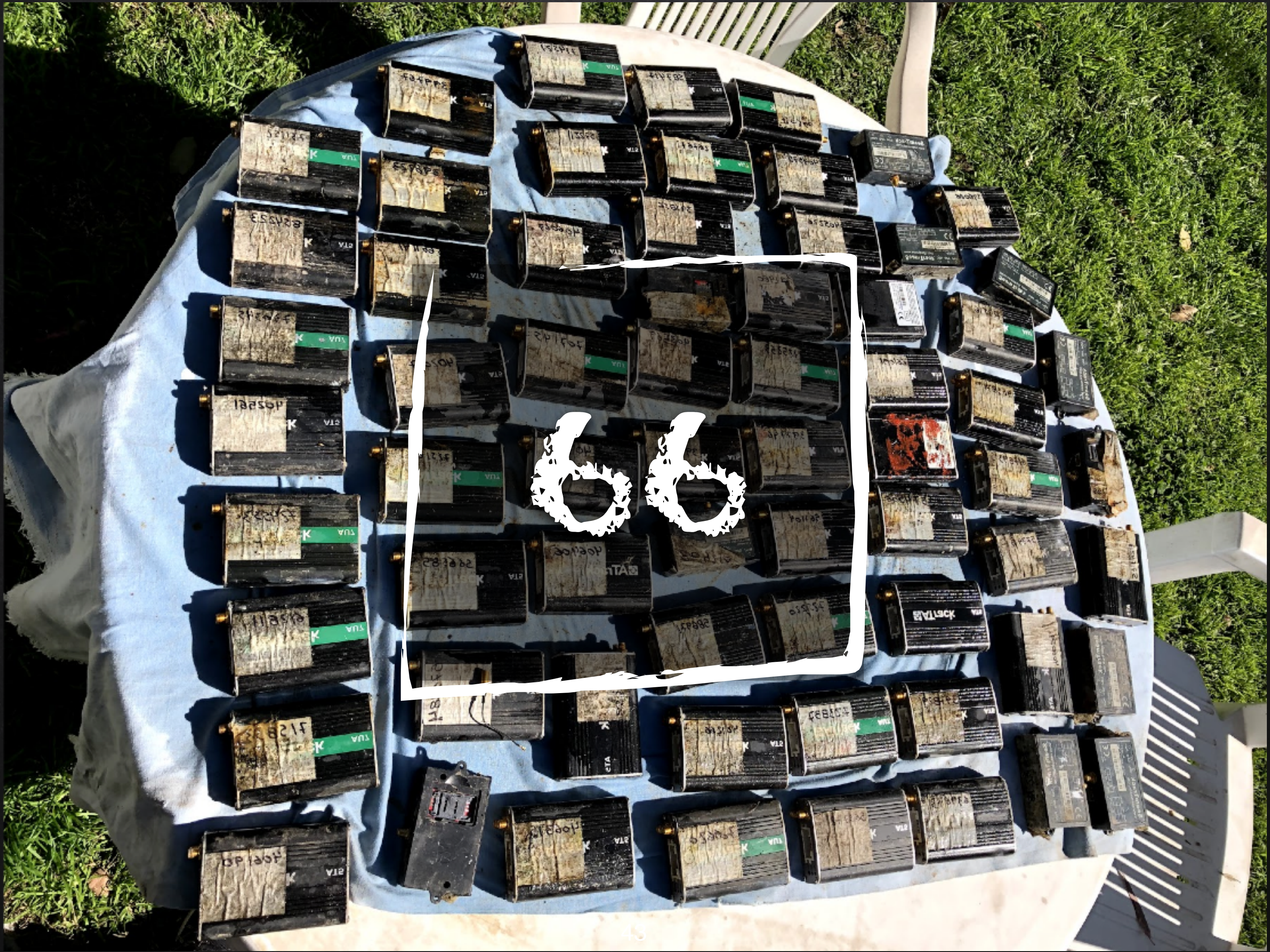
First results!



BUY 'EM ALL

This slide is dedicated to Marie Kondo

How many GPS's are too many GPS's?



66

528

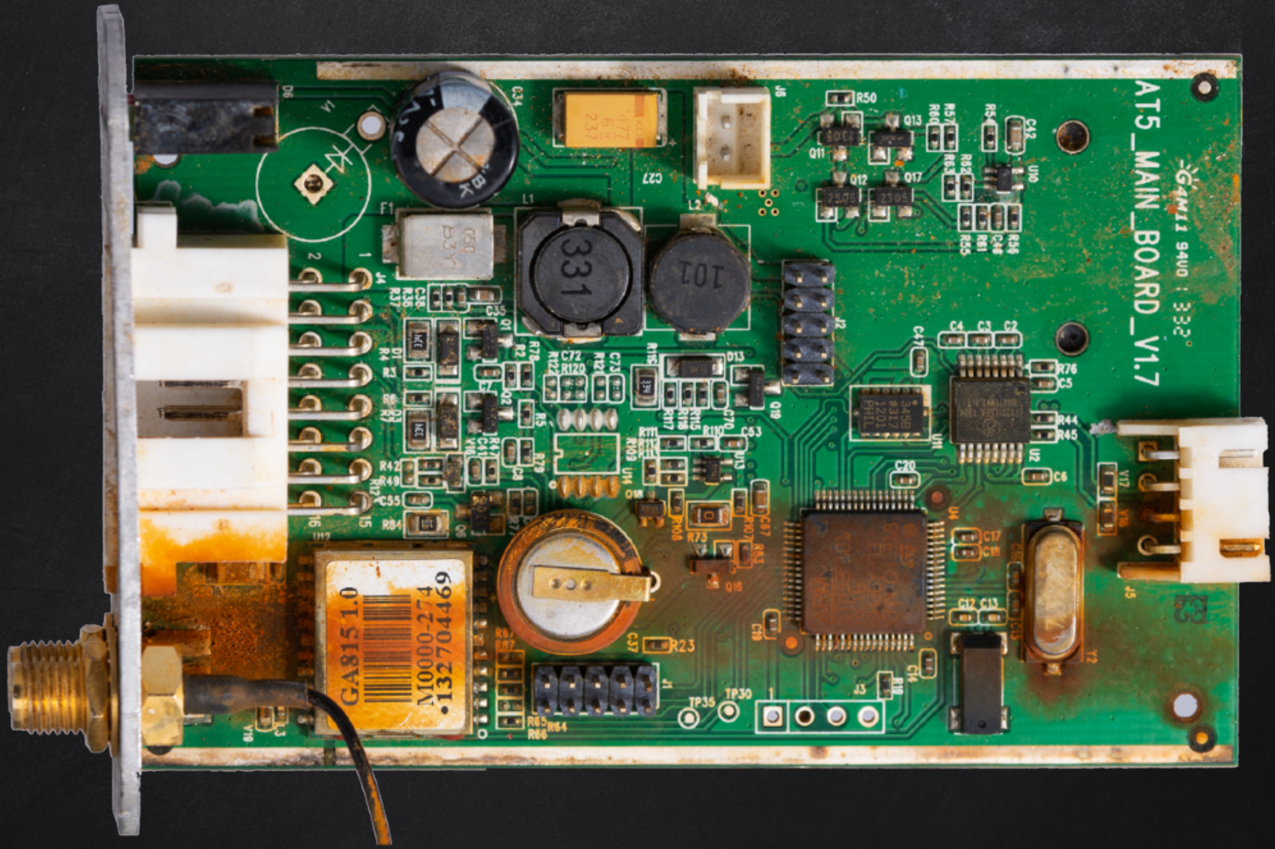
Screws removed

120

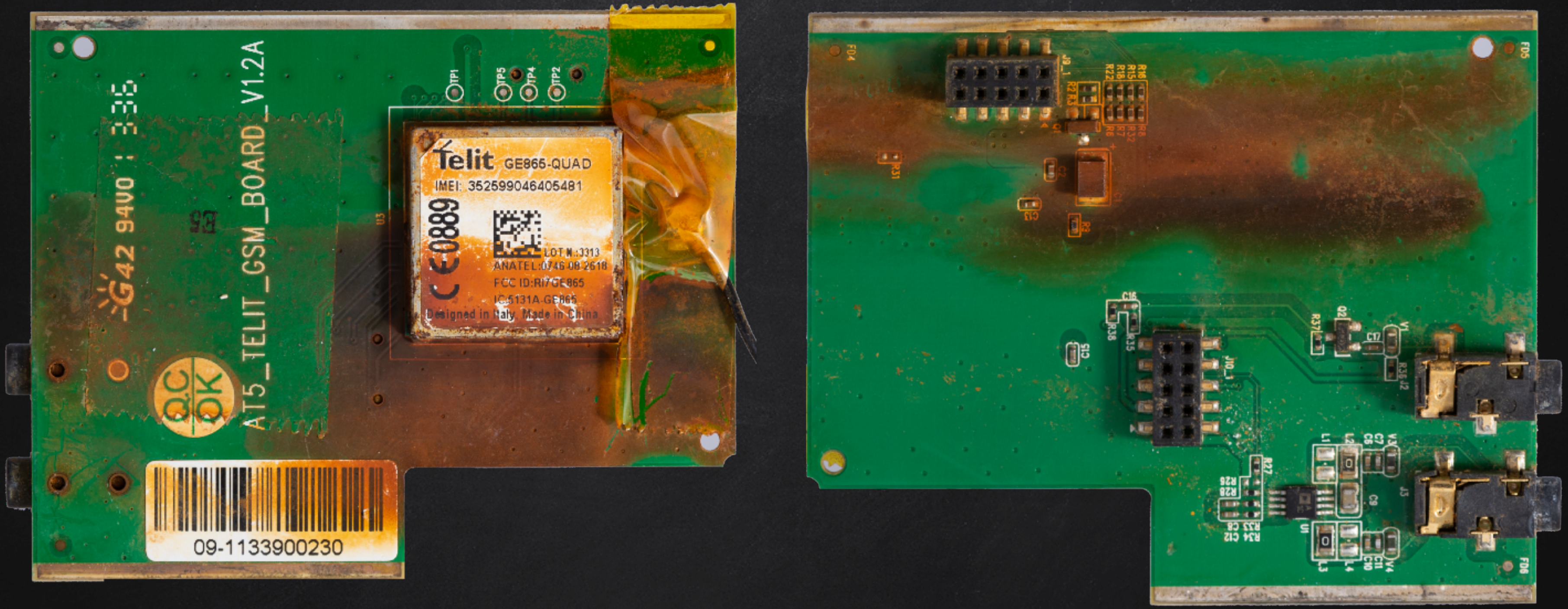
Boards brushed

66

Cases cleaned



Some were in really bad shape
(pics taken after initial cleaning)

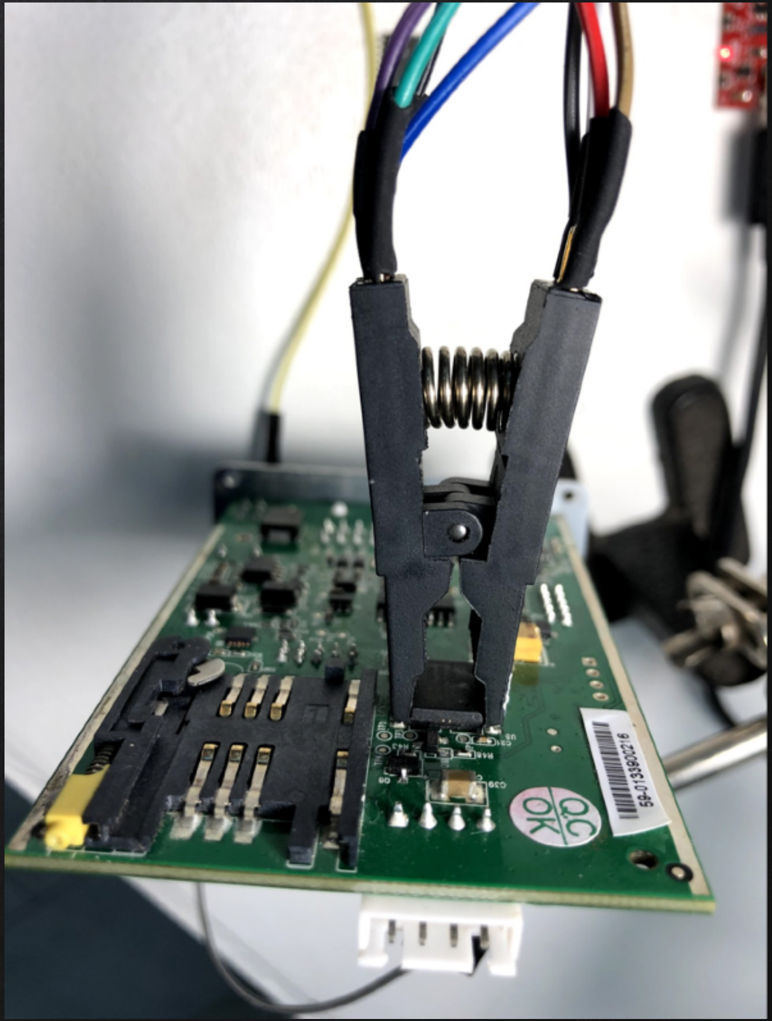


Some were in really bad shape

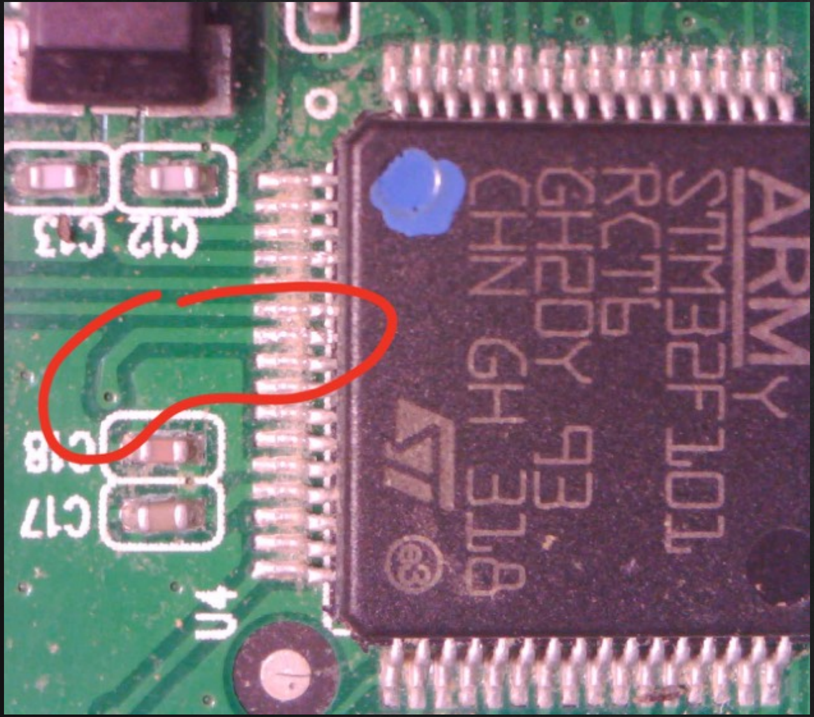
(pics taken after initial cleaning)

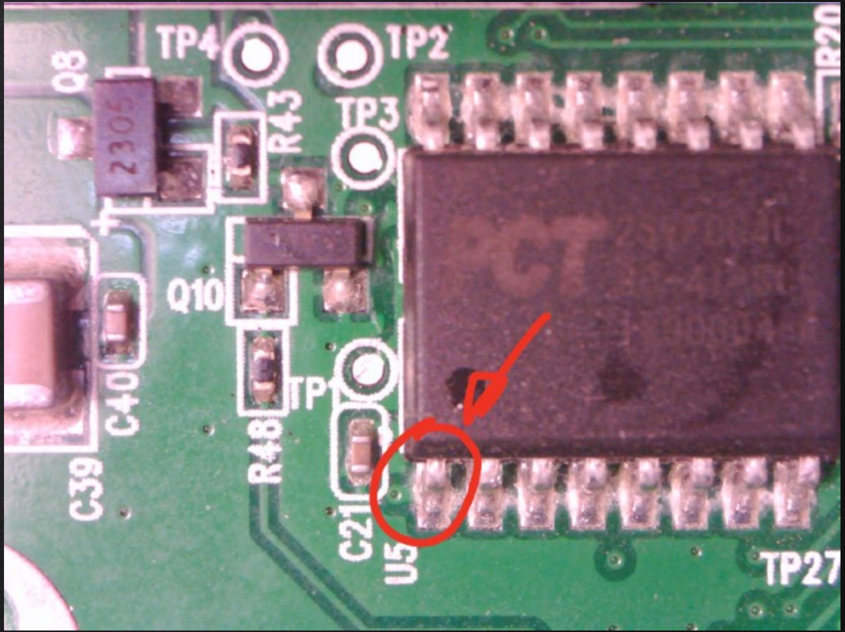
Dumping flash at scale

- ✗ Desolder is time consuming
  - ○ Got a clip
- ✗ Powering device from the probe
  - ○ DANGEROUS. Do not care. YOLO
- ✗ First attempt to dump failed
  - ○ Interference from other chips?
  - ○ We are very likely powering multiple ICs



Hold reset on main IC?



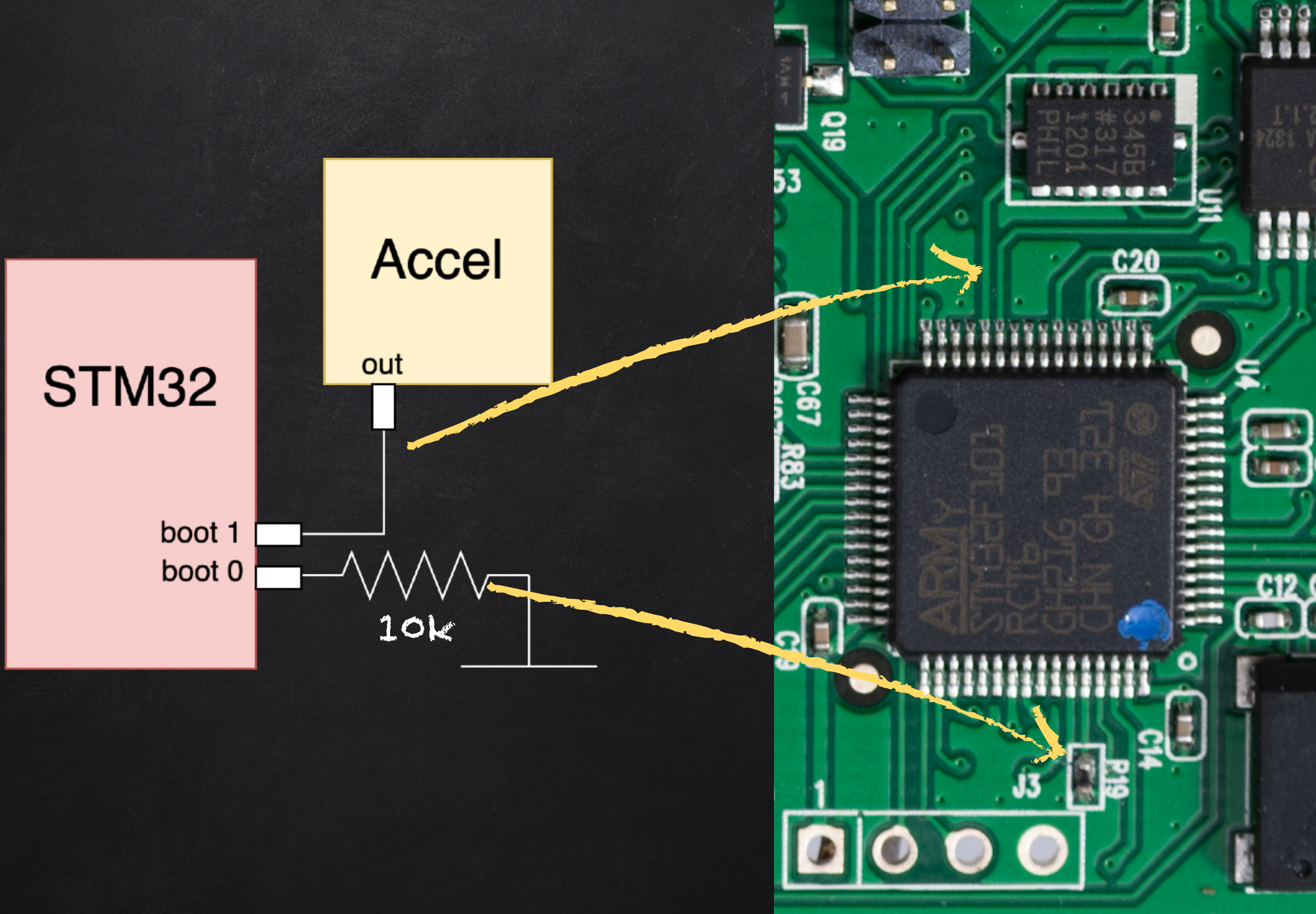


also connected to the FLASH reset :(

What about boot modes?

Boot 1	Boot 0	Mode
X	0	(internal) User Flash
0	1	System memory
1	1	Embedded SMRAM

dont use
the
external
FLASH



Accel

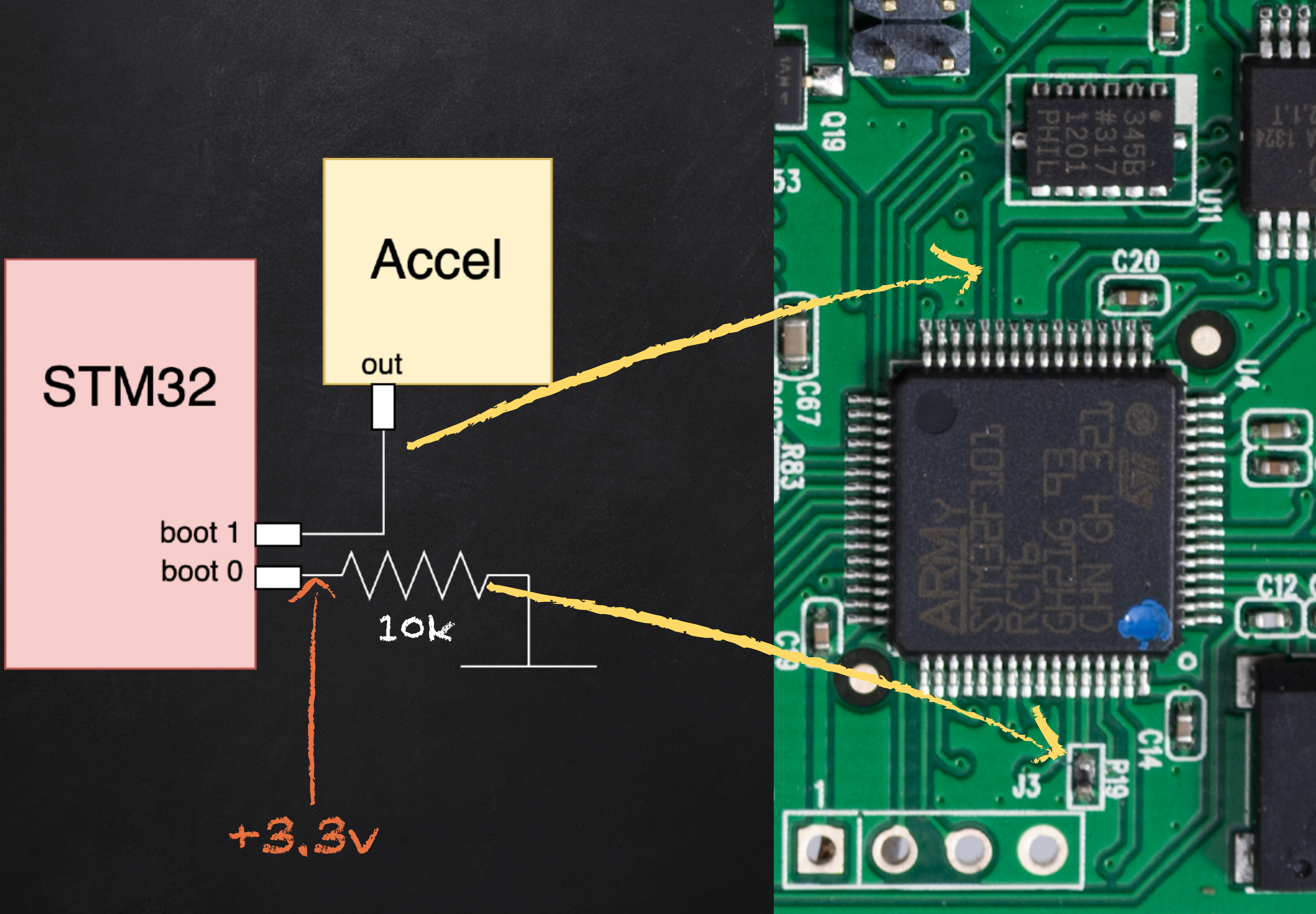
out

STM32

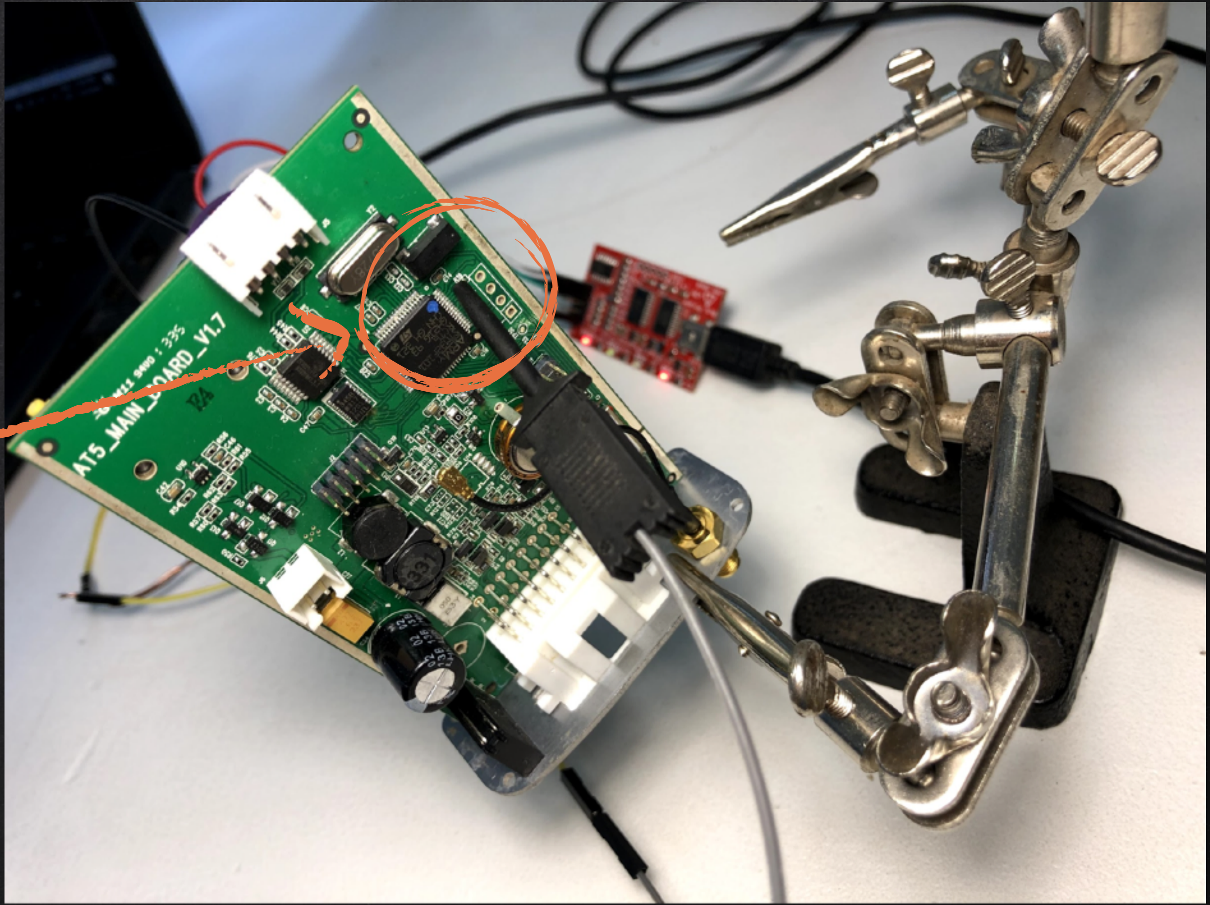
boot 1

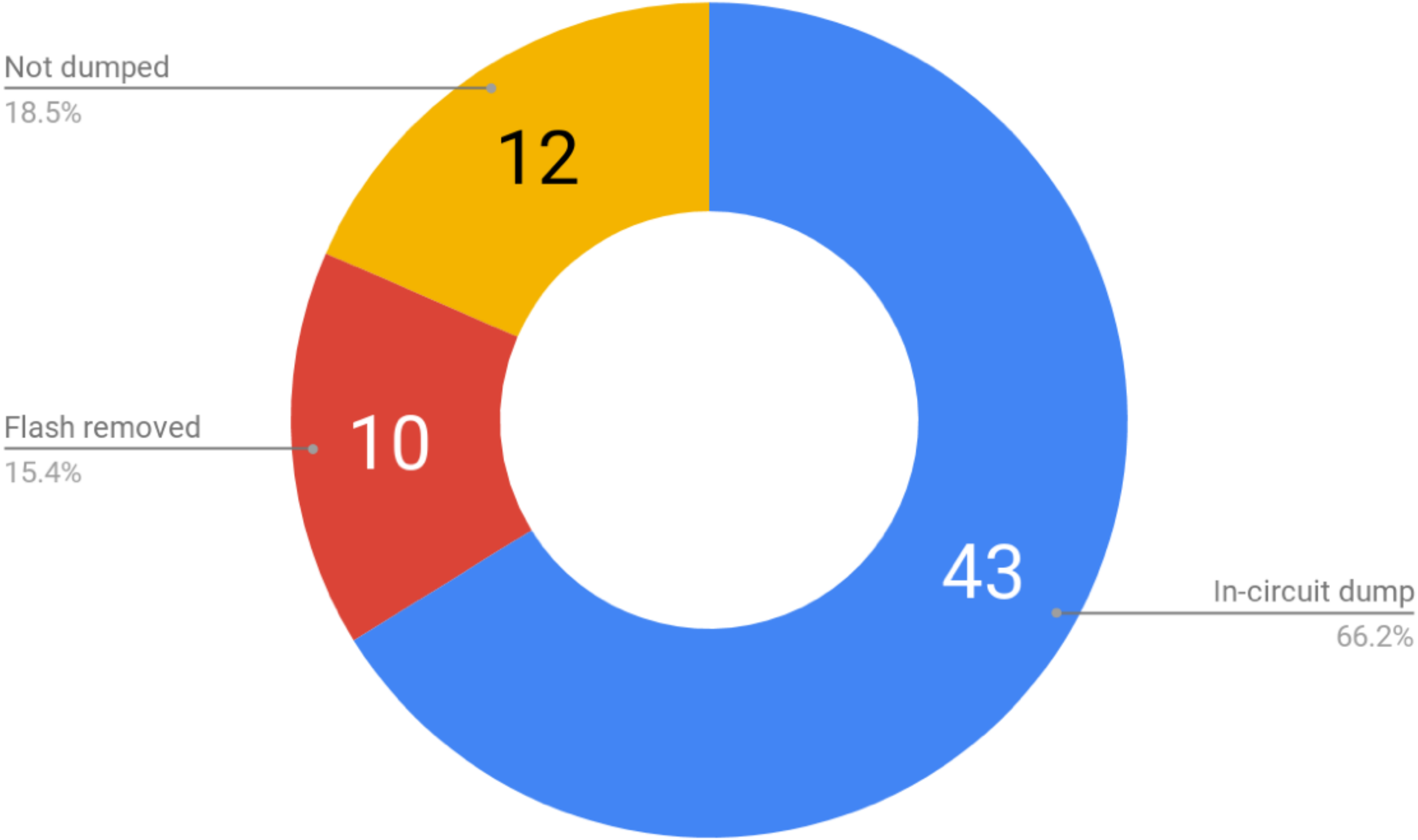
boot 0

10k

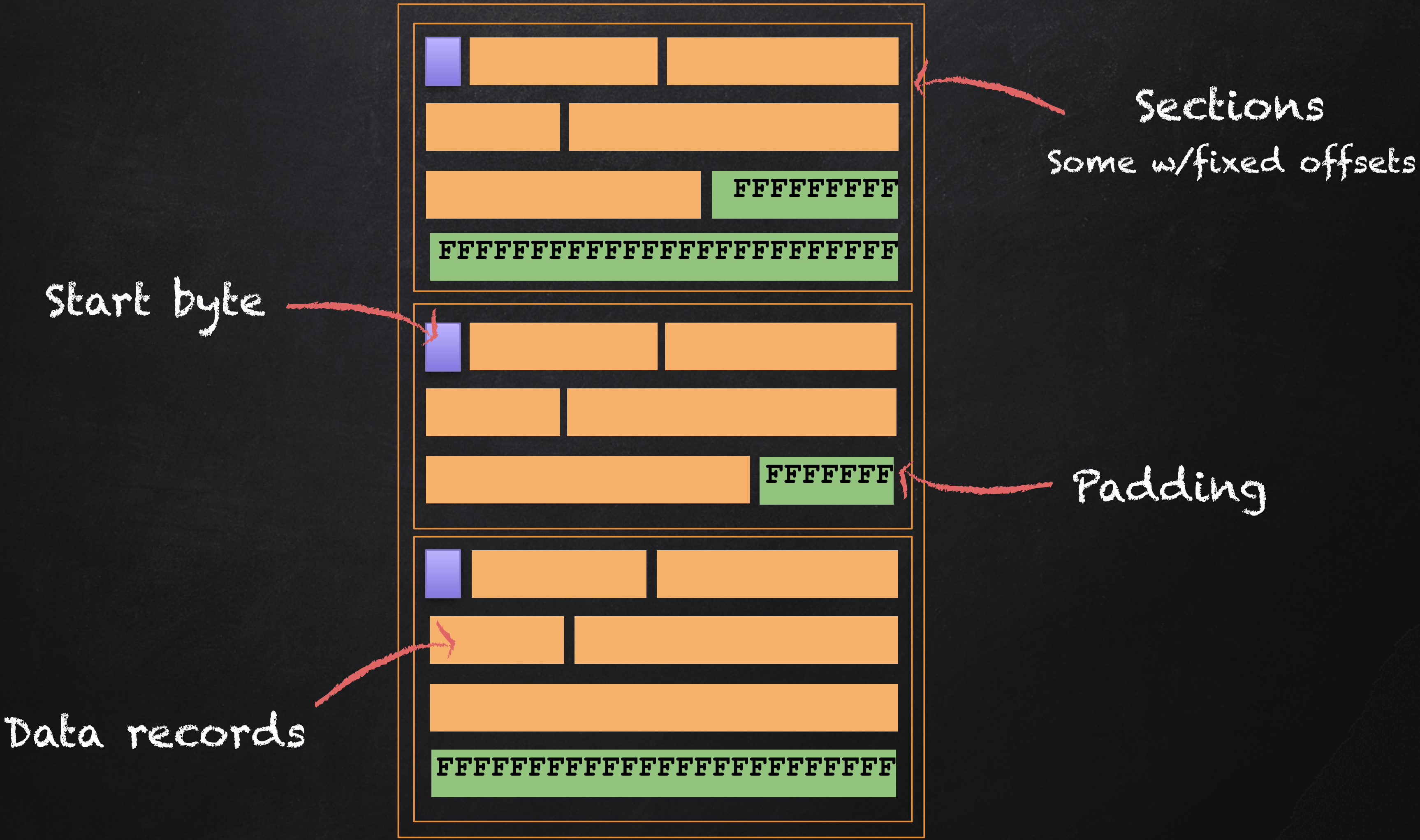

Accel
out
STM32
boot 1
boot 0
10k
+3.3v
Q19
U11
C20
C67
R83
U4
C12
C14
J3
R19
1

Pulling Boot-0 up to force boot to SRAM or System memory




Not dumped
18.5%
12
Flash removed
15.4%
10
43
In-circuit dump
66.2%

aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
amples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very
elpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.
aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
amples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very
elpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.
aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
amples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very
elpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.
aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
amples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very
elpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.
aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
amples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very
elpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
y helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.aving lots of samples is very helpful. Havin
s of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples i
very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful.
aving lots of samples is very helpful. Having lots of samples is very helpful. Having lots of samples is very helpful. Having lots of
mples is very helpful. Having lots of samples is very helpful. Having lots of sam. Having lots of sam. Having lots of sam. Having lot



Sections

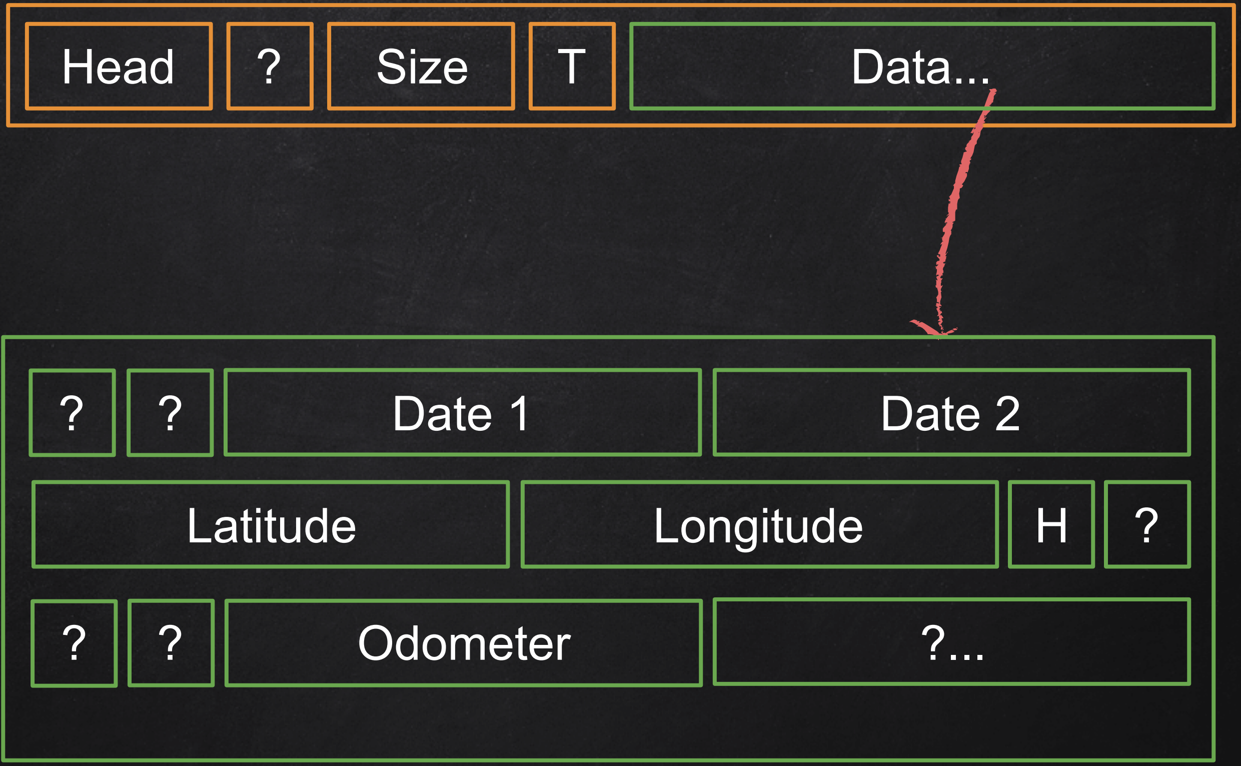
Some w/fixed offsets

Start byte

Padding

Data records

Data record



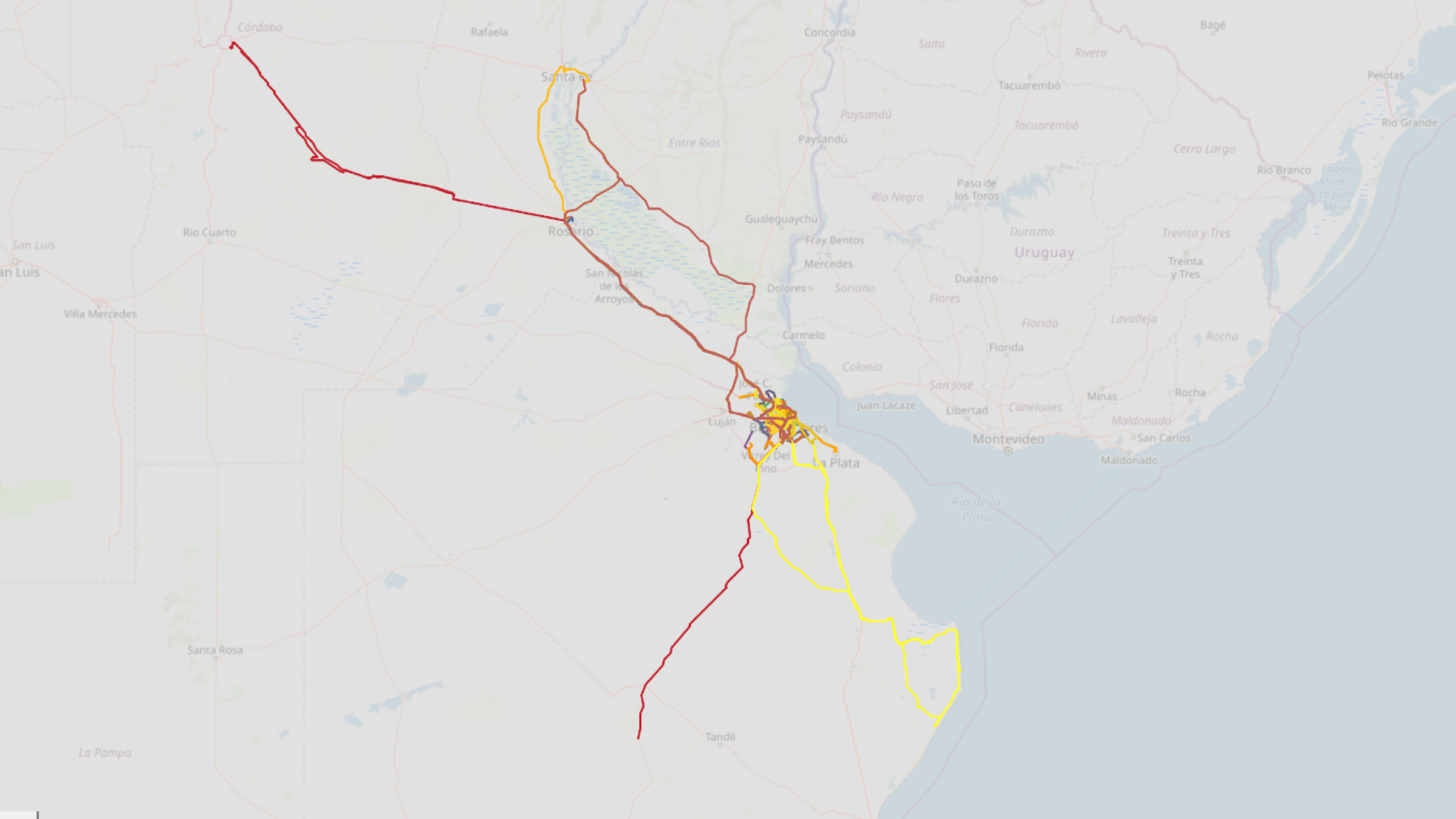
Head | ? | Size | T | Data...

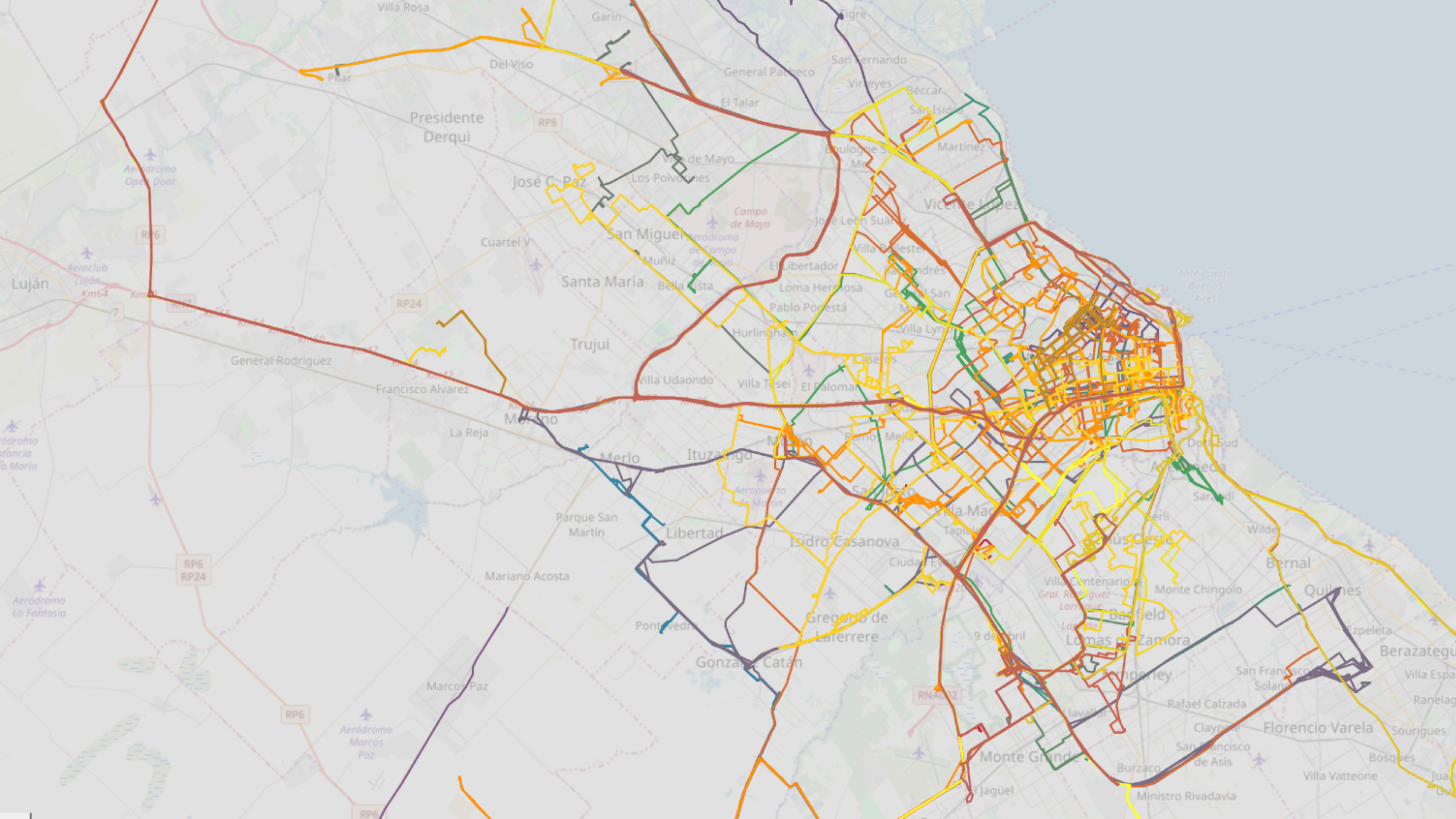
? | ? | Date 1 | Date 2

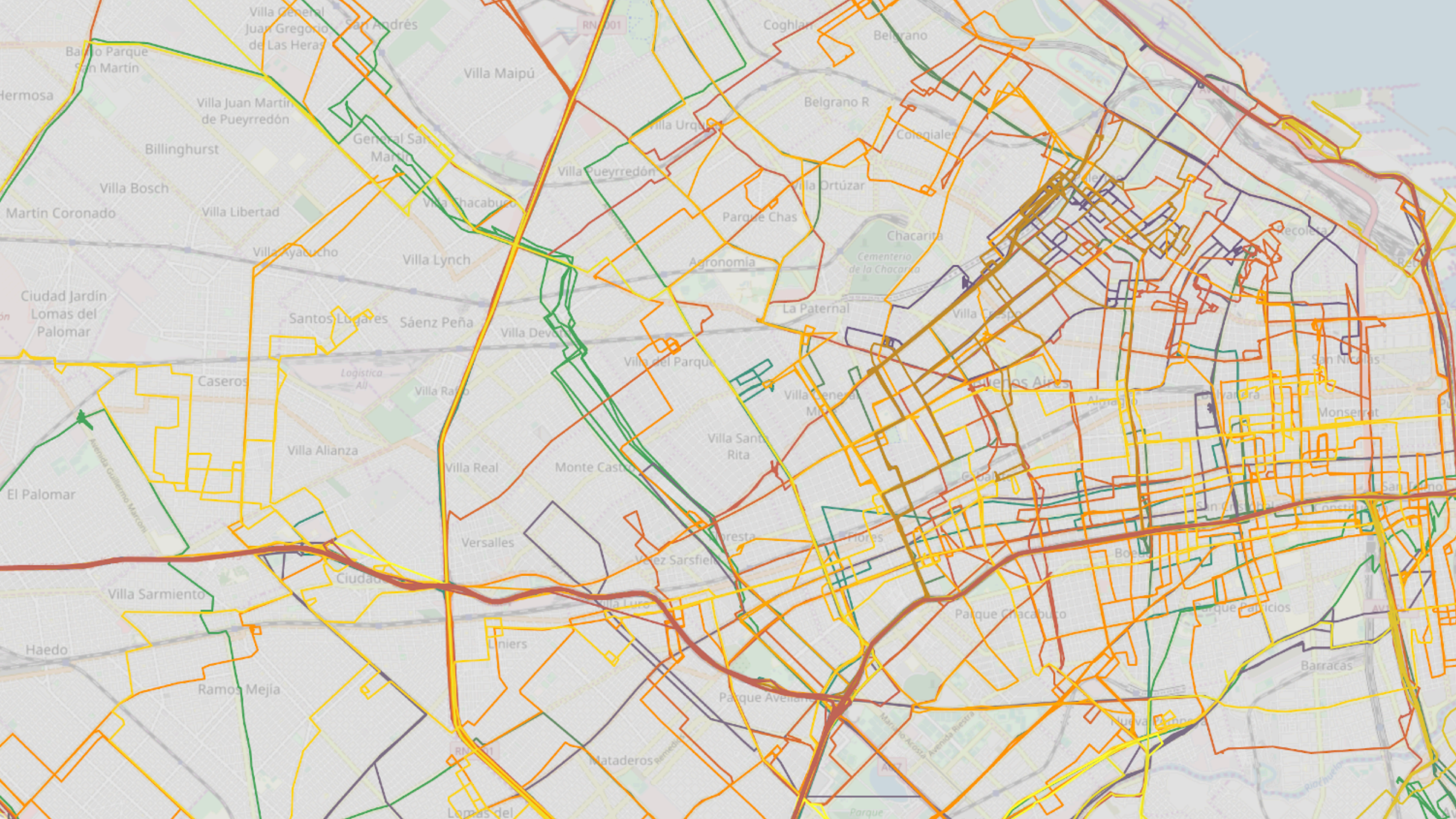
Latitude | Longitude | H | ?

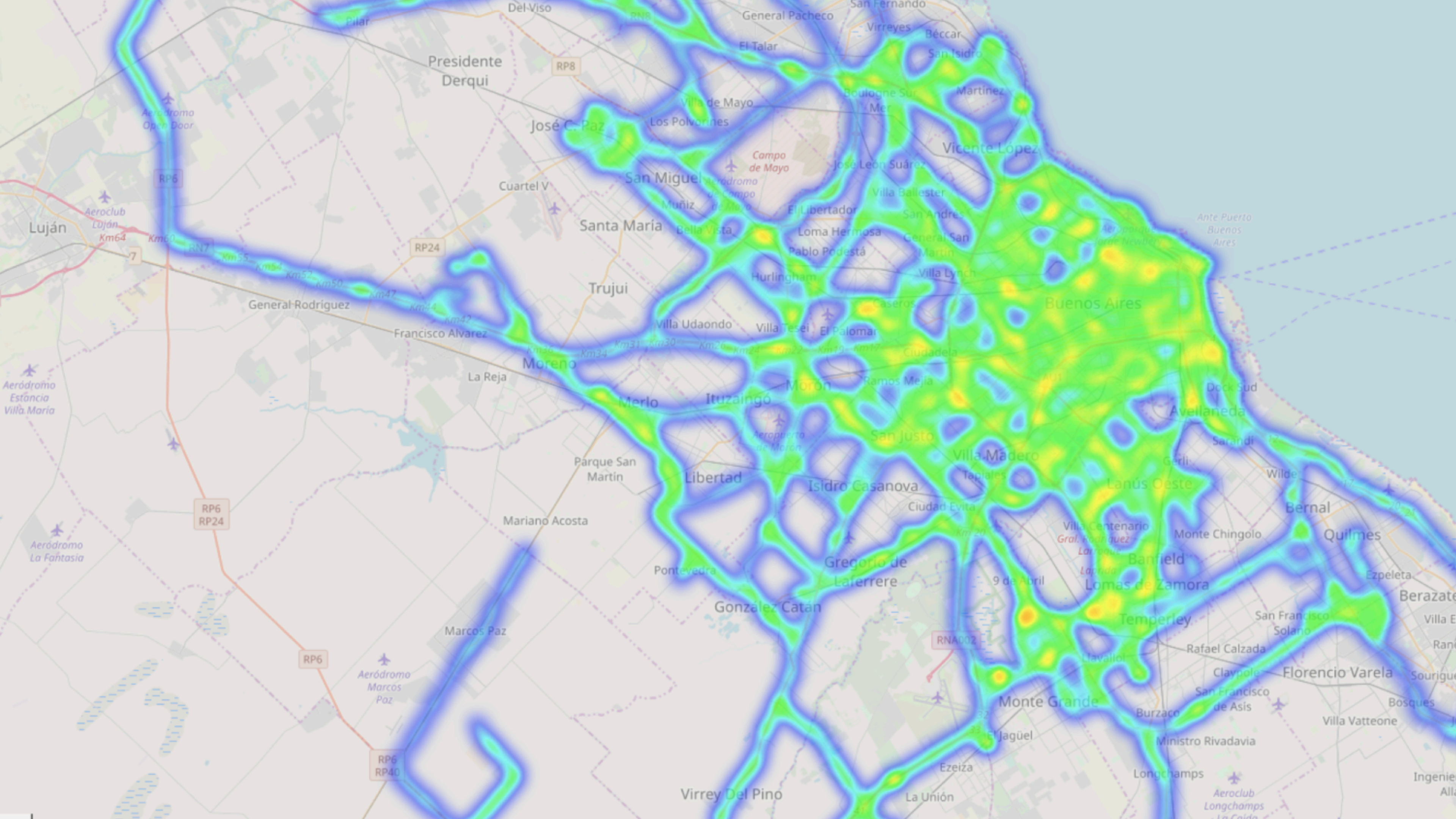
? | ? | Odometer | ?...

GPS log data


Córdoba
Rafaela
Santa Fe
Concordia
Salto
Rivera
Bagé
Pelotas
Tacuarembó
Rio Grande
Paysandú
Tacuarembó
Cerro Largo
Entre Ríos
Paysandú
Rio Branco
Lagoa Mirim / Laguna Merín
Paso de los Toros
Río Negro
Gualeguaychú
Durazno
Uruguay
Treinta y Tres
Fray Bentos
Rosario
Río Cuarto
San Luis
San Luis
Mercedes
Treinta y Tres
Durazno
San Nicolás de los Arroyos
Dolores
Soriano
Flores
Villa Mercedes
Florida
Lavalleja
Rocha
Carmelo
Florida
Colonia
San José
José C. Paz
Juan Lacaze
Libertad
Canelones
Minas
Rocha
Luján
Buenos Aires
Maldonado
Montevideo
San Carlos
Virrey Del Pino
La Plata
Maldonado
Río de la Plata
Santa Rosa
Tandil
La Pampa

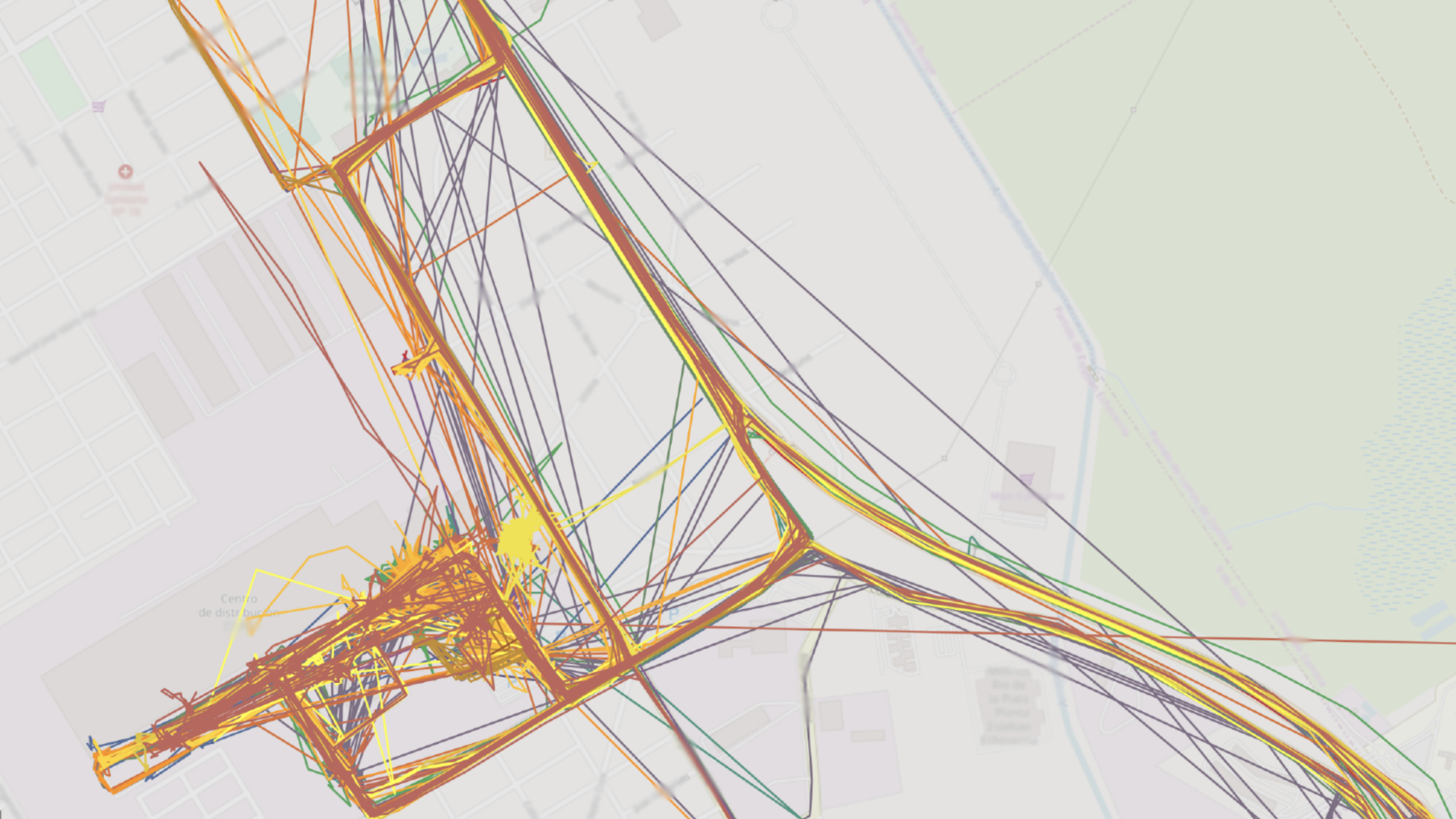

Villa Rosa
Garín
Tigre
San Fernando
General Pacheco
Del Viso
Pilar
Virreyes
Béccar
San Isidro
El Talar
Presidente Derqui
RP8
Martínez
Boulogne Sur Mer
Aeródromo Open Door
Villa de Mayo
Los Polvorines
José C. Paz
Campo de Mayo
Vicente López
RP6
José León Suárez
San Miguel
Aeródromo de Campo de Mayo
Cuartel V
Villa Ballester
Muñiz
El Libertador
San Andrés
Aeroclub Luján
Luján
Santa María
Bella Vista
Loma Hermosa
General San Martín
Ante Puerto Buenos Aires
Km64
RP24
Pablo Podestá
RP7
Trujui
Hurlingham
Villa Lynch
General Rodríguez
Caseros
Villa Udaondo
Villa Tesei
El Palomar
Francisco Álvarez
Moreno
La Reja
Morón
Ramos Mejía
Dock Sud
Aeródromo Estancia Santa María
Merlo
Ituzaingó
Avellaneda
Aeropuerto de Morón
San Justo
Sarandí
Villa Madero
Parque San Martín
Libertad
Tapiales
Isidro Casanova
Piñeiro
Wilde
RP6 RP24
Remedios de Escalada
Lanús Oeste
Bernal
Ciudad Evita
Mariano Acosta
Villa Centenario
Monte Chingolo
Quilmes
Gral. Rodríguez Lanús
Aeródromo La Fantasía
Gregorio de Laferrere
Banfield
Ezpeleta
Pontevedra
9 de Abril
Lomas de Zamora
Berazategui
Gonzalez Catán
Temperley
San Francisco Solano
Villa España
Marcos Paz
Ranelagh
Rafael Calzada
RP6
RNA002
Llavallol
Claypole
Florencio Varela
Sourigues
Aeródromo Marcos Paz
San Francisco de Asís
Bosques
Monte Grande
Burzaco
Villa Vatteone
El Jagüel
Ministro Rivadavia
RP6

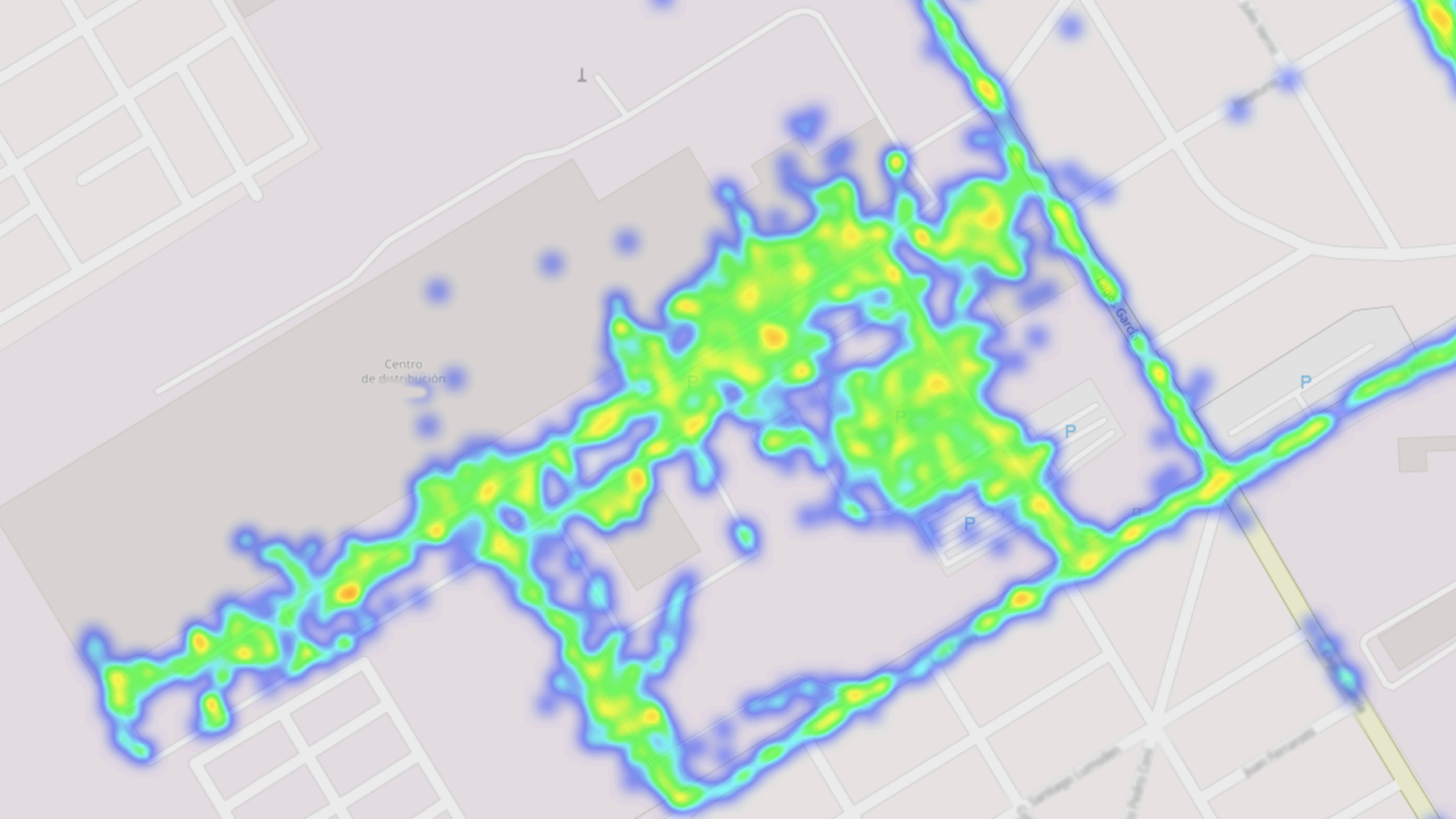

Villa General Juan Gregorio de Las Heras
San Andrés
Coghlan
Belgrano
Barrio Parque San Martín
Hermosa
Villa Maipú
Villa Juan Martín de Pueyrredón
Belgrano R
Billinghurst
General San Martín
Villa Urquiza
Colegiales
Villa Bosch
Villa Pueyrredón
Villa Ortúzar
Martín Coronado
Villa Libertad
Villa Chacabuco
Parque Chas
Chacarita
Recoleta
Villa Ayacucho
Villa Lynch
Agronomía
Cementerio de la Chacarita
Ciudad Jardín Lomas del Palomar
Santos Lugares
Sáenz Peña
La Paternal
Villa Crespo
Villa Devoto
Villa del Parque
San Nicolás
Caseros
Logística All
Villa Raffo
Buenos Aires
Villa General Mitre
Almagro
Balvanera
Monserrat
Villa Alianza
Villa Santa Rita
Avenida Guillermo Marconi
Villa Real
Monte Castro
Caballito
El Palomar
San Cristóbal
Constitución
San Telmo
Floresta
Flores
Versalles
Vélez Sarsfield
Boedo
Ciudadela
Villa Sarmiento
Villa Luro
Parque Chacabuco
Parque Patricios
Haedo
Liniers
Barracas
Ramos Mejía
Parque Avellaneda
Nueva Pompeya
Mataderos
RN 001
Lomas del
Parque


Del Viso
Pilar
General Pacheco
San Fernando
Virreyes
Béccar
El Talar
San Isidro
Presidente Derqui
RP8
Villa de Mayo
Boulogne Sur Mer
Martínez
Aeródromo Open Door
Los Polvorines
José C. Paz
Campo de Mayo
José León Suárez
Vicente López
RP6
San Miguel
Aeródromo de Campo de Mayo
Cuartel V
Muñiz
Villa Ballester
Aeroclub Luján
Luján
Km64
Km60
El Libertador
San Andrés
Santa María
Bella Vista
Loma Hermosa
General San Martín
Ante Puerto Buenos Aires
RN7
RP24
Pablo Podestá
Aeroparque Jorge Newbery
7
Km55
Villa Lynch
Hurlingham
Trujui
Km50
Km47
General Rodríguez
Km44
Caseros
Buenos Aires
Km42
Villa Udaondo
Villa Tesei
El Palomar
Francisco Álvarez
Km31
Km30
Km26
Km24
Km22
Km19
Km17
Ciudadela
Km36
Km34
Moreno
Aeródromo Estancia Villa María
La Reja
Morón
Ramos Mejía
Dock Sud
Merlo
Ituzaingó
Avellaneda
Aeropuerto de Morón
San Justo
Sarandí
Villa Madero
Gerli
Parque San Martín
Tapiales
Wilde
Libertad
Isidro Casanova
Lanús Oeste
RP6 RP24
Bernal
Ciudad Evita
Mariano Acosta
Villa Centenario
Km 20
Monte Chingolo
Quilmes
Aeródromo La Fantasía
Gral. Rodríguez Lafuente
Lafuente
Gregorio de Laferrere
Banfield
Pontevedra
9 de Abril
Lomas de Zamora
Ezpeleta
Berazategui
González Catán
Temperley
Marcos Paz
San Francisco Solano
Villa E
RNA002
Ran
RP6
Rafael Calzada
Aeródromo Marcos Paz
Llavallol
Claypole
Florencio Varela
Sourigue
San Francisco de Asís
Monte Grande
Bosques
Burzaco
Villa Vatteone
El Jagüel
Ministro Rivadavia
RP6 RP40
Ezeiza
Longchamps
Ingenie Alla
Virrey Del Pino
La Unión
Aeroclub Longchamps
La Colina

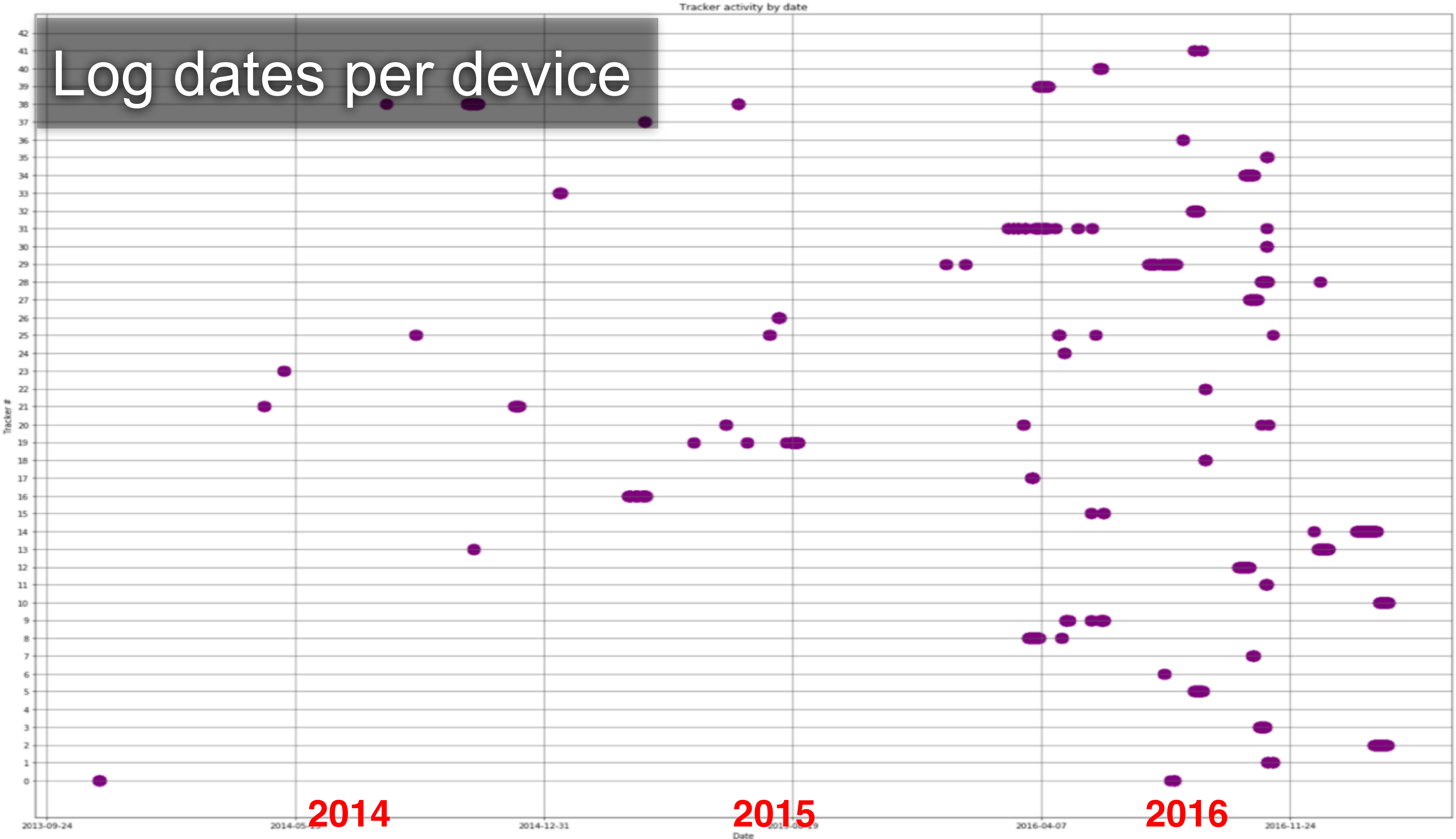
Club Atlético Atlanta
Avenida Corrientes
Darwin
Humboldt
Camargo
Padilla
Murillo
Camargo y Darwin
Jardín de los Árboles
Estudio Jurídico
Bachillerato Popular de Jóvenes y Adultos

ŁÓDŹ


Centro
de distribución


Centro
de distribución
P
P
P
P
Lagos Garc

Log dates per device



Data on queues is not actually erased from the device even after it was sent.

Very likely an optimization

AT$REST=<Action>,<Reset Option>

Bit 0: Maintain command password setting
Bit 1: Maintain SIM PIN code setting
Bit 2: Maintain communication settings

Bit 0: Reboot
Bit 1: Clear message queue
→ Bit 2: Reset all params to factory default
Bit 3: Clear Log queue

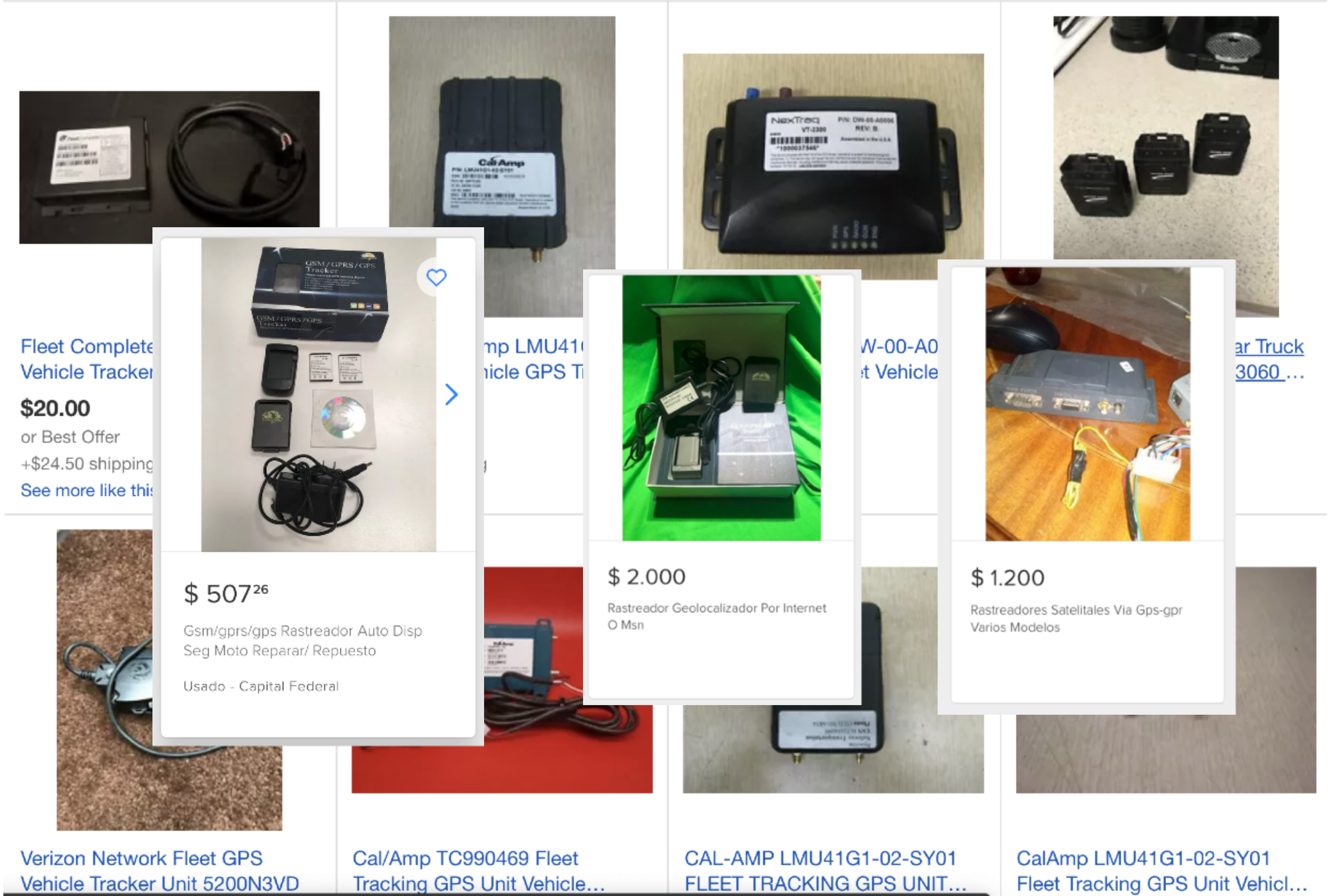
AT$REST=<Action>,<Reset Option>

Bit 0: Maintain command password setting
Bit 1: Maintain SIM PIN code setting
Bit 2: Maintain communication settings

Bit 0: Reboot
Bit 1: Clear message queue
Bit 2: Reset all params to factory default
Bit 3: Clear Log queue

Correct bits must be set in order to erase all potential private information

Should vendors state what data devices store,
and clearly tell the user how to securely wipe them?



Fleet Complete
Vehicle Tracker

$20.00

or Best Offer

+$24.50 shipping

See more like thi

mp LMU41
hicle GPS T

W-00-A0
t Vehicle

ar Truck
3060 ...

$ 507 ^{26}

Gsm/gprs/gps Rastreador Auto Disp Seg Moto Reparar/ Repuesto

Usado - Capital Federal

$ 2.000

Rastreador Geolocalizador Por Internet O Msn

$ 1.200

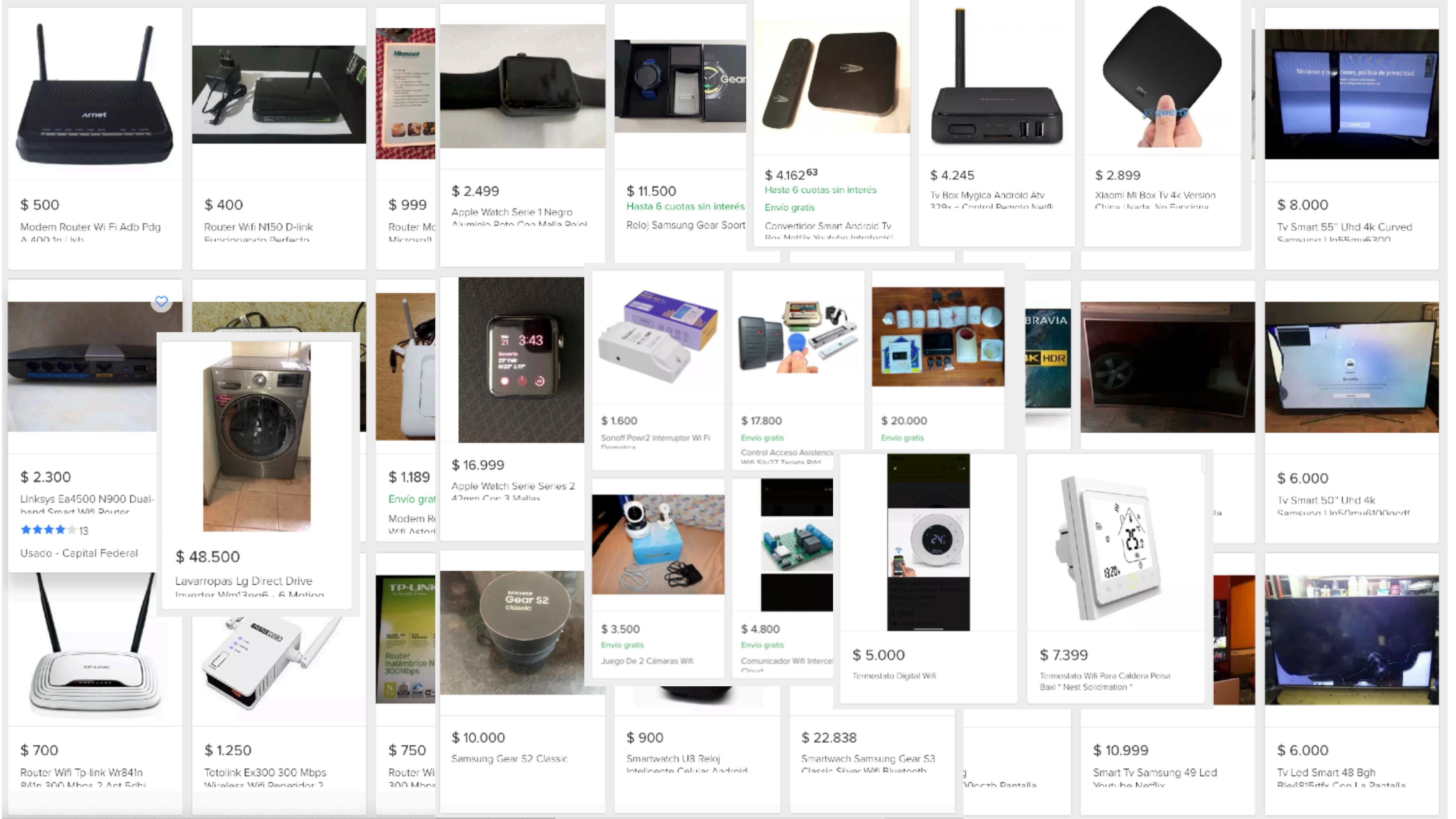
Rastreadores Satelitales Via Gps-gpr Varios Modelos

Verizon Network Fleet GPS Vehicle Tracker Unit 5200N3VD

Cal/Amp TC990469 Fleet Tracking GPS Unit Vehicle...

CAL-AMP LMU41G1-02-SY01 FLEET TRACKING GPS UNIT...

CalAmp LMU41G1-02-SY01 Fleet Tracking GPS Unit Vehicl...



$ 500
Modem Router Wi Fi Adb Pdg A 4001n Usb

$ 400
Router Wifi N150 D-link Funcionando Perfecto

$ 999
Router Mc Microsoft

$ 2.499
Apple Watch Serie 1 Negro Aluminio Roto Con Malla Reloj

$ 11.500
Hasta 6 cuotas sin interés
Reloj Samsung Gear Sport

$ 4.162^{63}
Hasta 6 cuotas sin interés
Envío gratis
Convertidor Smart Android Tv Box Netflix Youtube Introtech!!

$ 4.245
Tv Box Mygica Android Atv 329x + Control Remoto Netfli

$ 2.899
Xiaomi Mi Box Tv 4k Version China Usada. No Funciona

$ 8.000
Tv Smart 55" Uhd 4k Curved Samsung Un55mu6300

$ 2.300
Linksys Ea4500 N900 Dual-band Smart Wifi Router
★★★★☆ 13
Usado - Capital Federal

$ 48.500
Lavarropas Lg Direct Drive Inverter Wm13eg6 - 6 Motion

$ 1.189
Envío grat
Modem Ro Wifi Astord

$ 16.999
Apple Watch Serie Series 2 42mm Con 3 Mallas

$ 1.600
Sonoff Powr2 Interruptor Wi Fi Domotica

$ 17.800
Envío gratis
Control Acceso Asistencia Wifi Sily27 Tarjeta Rfid

$ 20.000
Envío gratis

$ 6.000
Tv Smart 50" Uhd 4k Samsung Un50mu6100gcdf

$ 3.500
Envío gratis
Juego De 2 Cámaras Wifi

$ 4.800
Envío gratis
Comunicador Wifi Interce Cloud

$ 5.000
Termostato Digital Wifi

$ 7.399
Termostato Wifi Para Caldera Peisa Baxi * Nest Solidmation *

$ 700
Router Wifi Tp-link Wr841n 841n 300 Mbps 2 Ant 5dbi

$ 1.250
Totolink Ex300 300 Mbps Wireless Wifi Repetidor 2

$ 750
Router Wi 300 Mbps

$ 10.000
Samsung Gear S2 Classic

$ 900
Smartwatch U8 Reloj Inteligente Celular Android

$ 22.838
Smartwach Samsung Gear S3 Classic Silver Wifi Bluetooth

0eczh Pantalla

$ 10.999
Smart Tv Samsung 49 Led Youtube Netflix

$ 6.000
Tv Led Smart 48 Bgh Ble4815rtx Con La Pantalla

What details of our lives are we throwing to the trash?

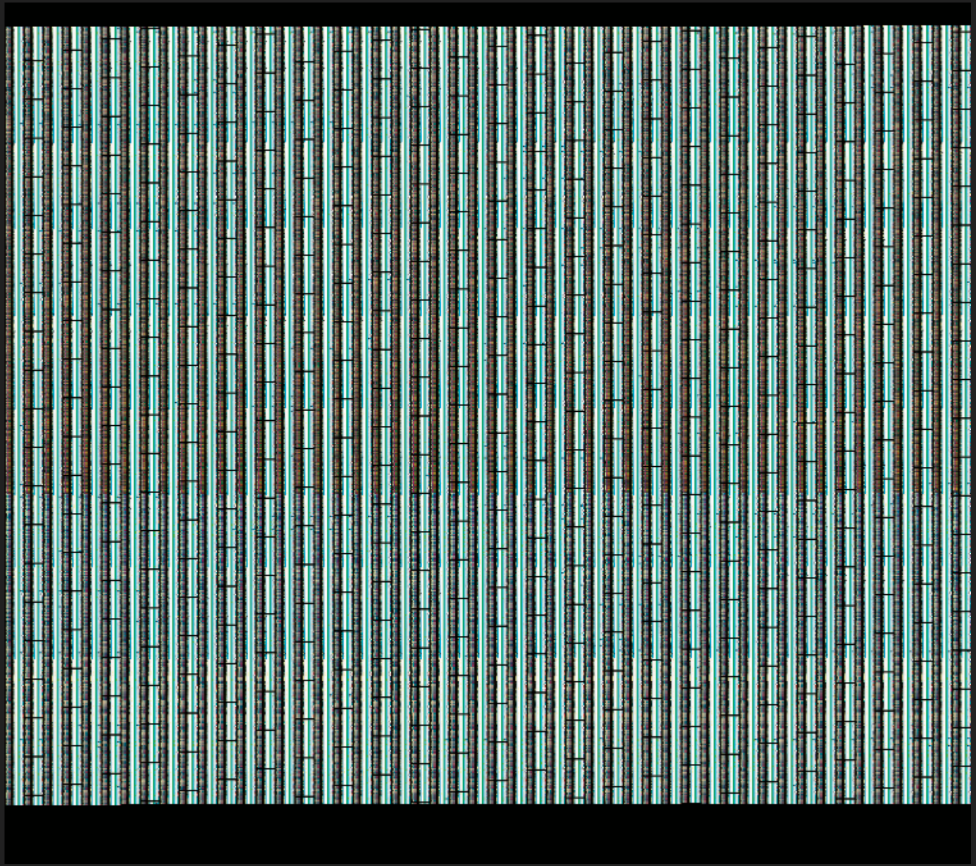
ACK' s

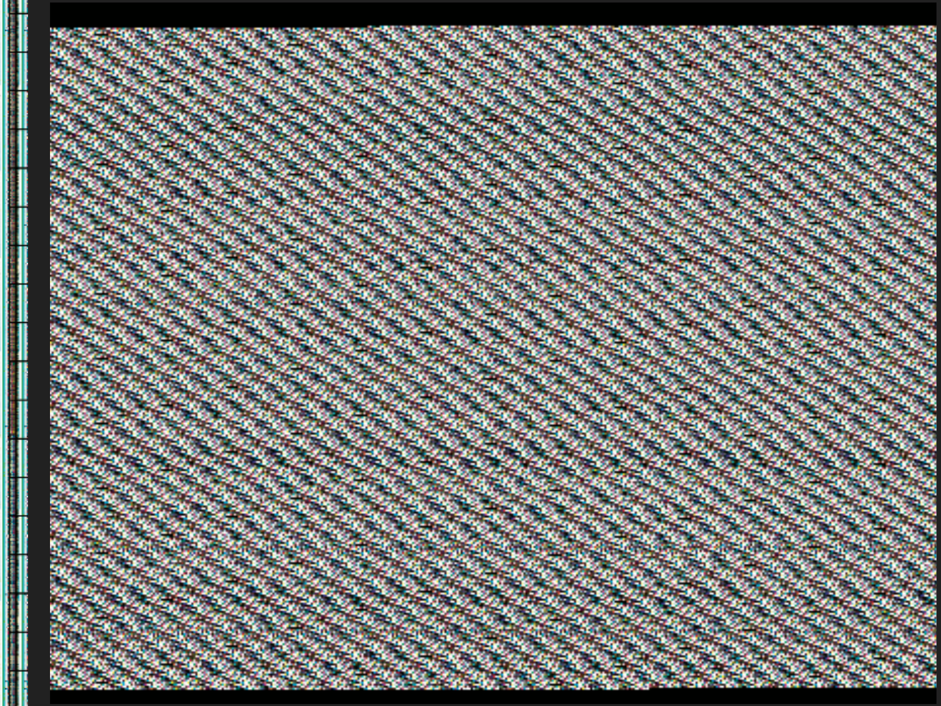
Intel STORM Team! \o/

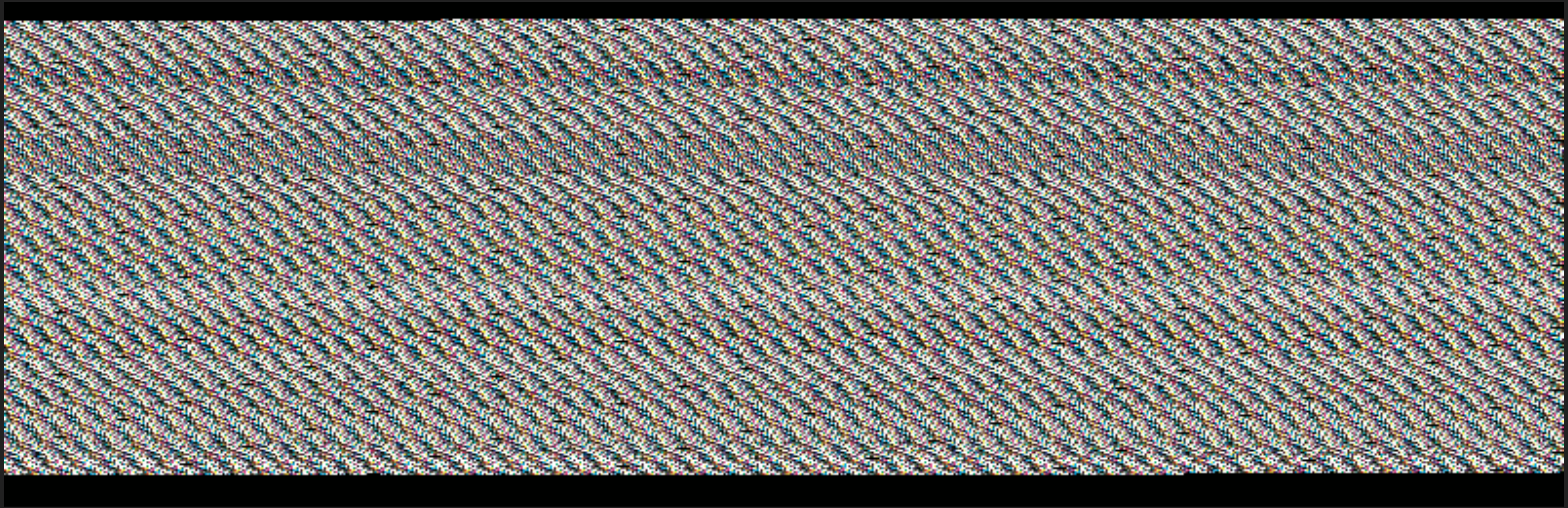
And many friends who have helped in the process:
Anto, Anibal, Nico, Esteban, Facu, Andrés, Emi, etc

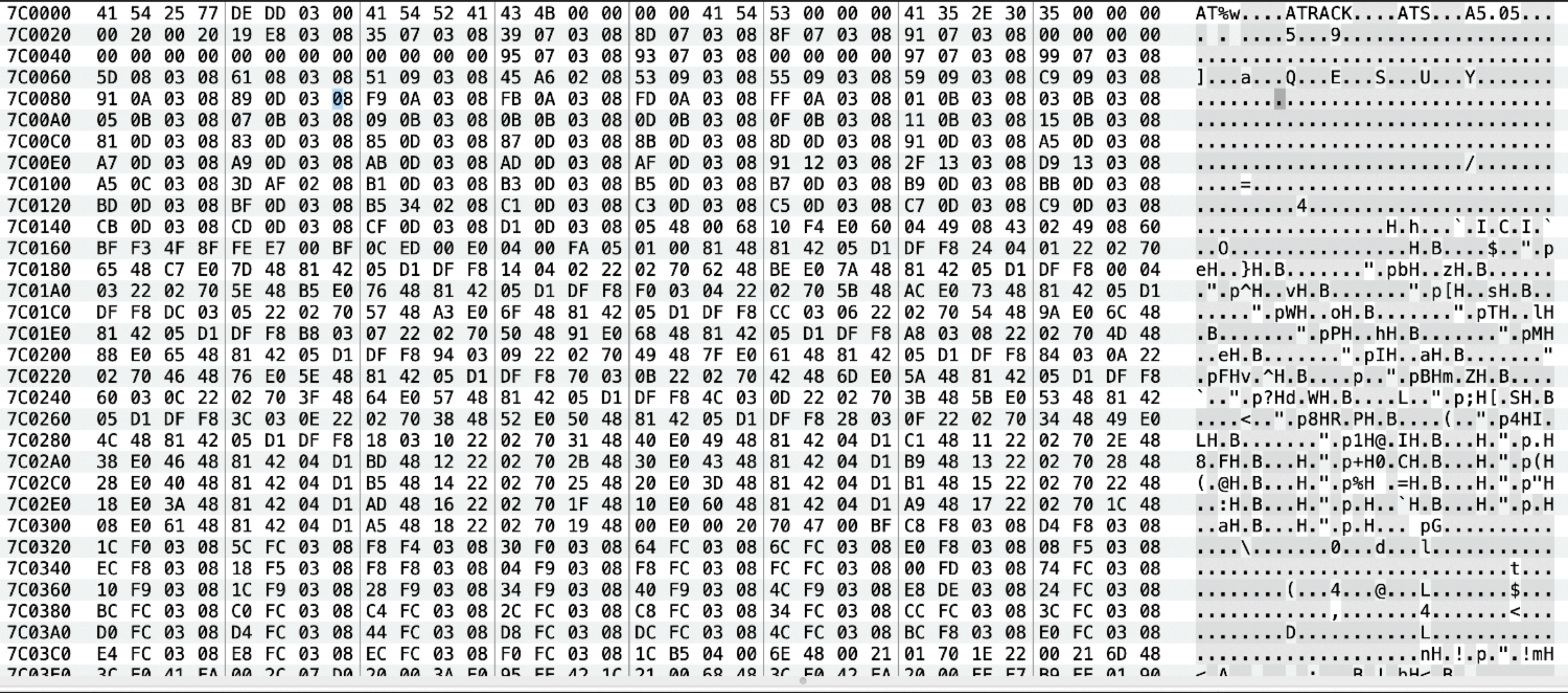
```
Processing ./dumps/002.bin file...
Got 1483 records, 16 were gps logs
Got 3235 records, 314 were gps logs

Processing ./dumps/003.bin file...
Got 1490 records, 0 were gps logs
Got 21864 records, 17612 were gps logs

Processing ./dumps/004.bin file...
Got 1546 records, 16 were gps logs
Got 15932 records, 12602 were gps logs

[…]

Processing ./dumps/006.bin file...
Got 1438 records, 0 were gps logs
Error, unknown data
('0x6be91b',
'000000000000000000000000000000000000000000000000000000000064afbcff390001
00d70e6c568f9f6c564a5383fcaeeceefd0f00020ba906000000010000010000000d007d00
700390026000000')
```

parser was
failing on some
flash dumps
Weird data...





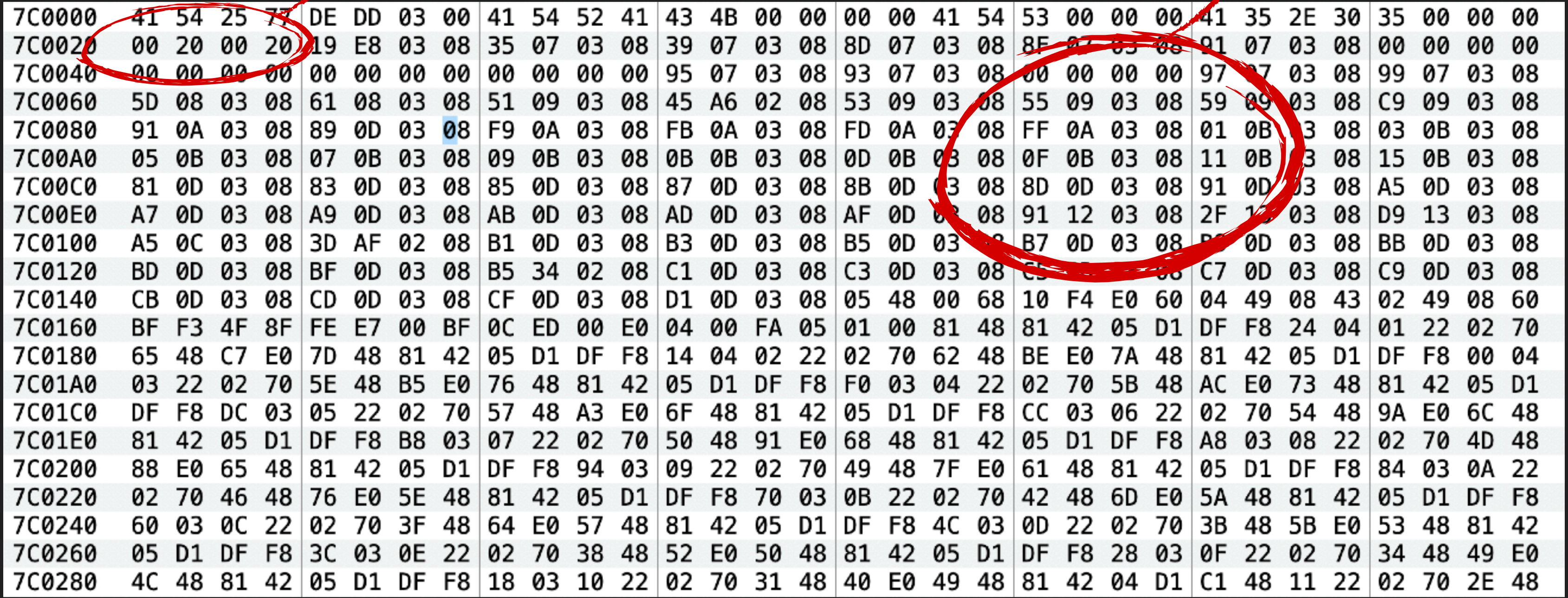




```
7C0000  41 54 25 77 DE DD 03 00 41 54 52 41 43 4B 00 00 00 00 41 54 53 00 00 00 41 35 2E 30 35 00 00 00  AT%w....ATRACK....ATS...A5.05...
7C0020  00 20 00 20 19 E8 03 08 35 07 03 08 39 07 03 08 8D 07 03 08 8F 07 03 08 91 07 03 08 00 00 00 00  . . ....5...9...................
7C0040  00 00 00 00 00 00 00 00 00 00 00 00 95 07 03 08 93 07 03 08 00 00 00 00 97 07 03 08 99 07 03 08  ................................
7C0060  5D 08 03 08 61 08 03 08 51 09 03 08 45 A6 02 08 53 09 03 08 55 09 03 08 59 09 03 08 C9 09 03 08  ]...a...Q...E...S...U...Y.......
7C0080  91 0A 03 08 89 0D 03 08 F9 0A 03 08 FB 0A 03 08 FD 0A 03 08 FF 0A 03 08 01 0B 03 08 03 0B 03 08  ................................
7C00A0  05 0B 03 08 07 0B 03 08 09 0B 03 08 0B 0B 03 08 0D 0B 03 08 0F 0B 03 08 11 0B 03 08 15 0B 03 08  ................................
7C00C0  81 0D 03 08 83 0D 03 08 85 0D 03 08 87 0D 03 08 8B 0D 03 08 8D 0D 03 08 91 0D 03 08 A5 0D 03 08  ................................
7C00E0  A7 0D 03 08 A9 0D 03 08 AB 0D 03 08 AD 0D 03 08 AF 0D 03 08 91 12 03 08 2F 13 03 08 D9 13 03 08  ......................../.......
7C0100  A5 0C 03 08 3D AF 02 08 B1 0D 03 08 B3 0D 03 08 B5 0D 03 08 B7 0D 03 08 B9 0D 03 08 BB 0D 03 08  ....=...........................
7C0120  BD 0D 03 08 BF 0D 03 08 B5 34 02 08 C1 0D 03 08 C3 0D 03 08 C5 0D 03 08 C7 0D 03 08 C9 0D 03 08  .........4......................
7C0140  CB 0D 03 08 CD 0D 03 08 CF 0D 03 08 D1 0D 03 08 05 48 00 68 10 F4 E0 60 04 49 08 43 02 49 08 60  .................H.h...`.I.C.I.`
7C0160  BF F3 4F 8F FE E7 00 BF 0C ED 00 E0 04 00 FA 05 01 00 81 48 81 42 05 D1 DF F8 24 04 01 22 02 70  ..O................H.B....$..".p
7C0180  65 48 C7 E0 7D 48 81 42 05 D1 DF F8 14 04 02 22 02 70 62 48 BE E0 7A 48 81 42 05 D1 DF F8 00 04  eH..}H.B.......".pbH..zH.B......
7C01A0  03 22 02 70 5E 48 B5 E0 76 48 81 42 05 D1 DF F8 F0 03 04 22 02 70 5B 48 AC E0 73 48 81 42 05 D1  .".p^H..vH.B.......".p[H..sH.B..
7C01C0  DF F8 DC 03 05 22 02 70 57 48 A3 E0 6F 48 81 42 05 D1 DF F8 CC 03 06 22 02 70 54 48 9A E0 6C 48  .....".pWH..oH.B.......".pTH..lH
7C01E0  81 42 05 D1 DF F8 B8 03 07 22 02 70 50 48 91 E0 68 48 81 42 05 D1 DF F8 A8 03 08 22 02 70 4D 48  .B.......".pPH..hH.B.......".pMH
7C0200  88 E0 65 48 81 42 05 D1 DF F8 94 03 09 22 02 70 49 48 7F E0 61 48 81 42 05 D1 DF F8 84 03 0A 22  ..eH.B.......".pIH..aH.B......."
7C0220  02 70 46 48 76 E0 5E 48 81 42 05 D1 DF F8 70 03 0B 22 02 70 42 48 6D E0 5A 48 81 42 05 D1 DF F8  .pFHv.^H.B....p..".pBHm.ZH.B....
7C0240  60 03 0C 22 02 70 3F 48 64 E0 57 48 81 42 05 D1 DF F8 4C 03 0D 22 02 70 3B 48 5B E0 53 48 81 42  `..".p?Hd.WH.B....L..".p;H[.SH.B
7C0260  05 D1 DF F8 3C 03 0E 22 02 70 38 48 52 E0 50 48 81 42 05 D1 DF F8 28 03 0F 22 02 70 34 48 49 E0  ....<..".p8HR.PH.B....(..".p4HI.
7C0280  4C 48 81 42 05 D1 DF F8 18 03 10 22 02 70 31 48 40 E0 49 48 81 42 04 D1 C1 48 11 22 02 70 2E 48  LH.B.......".p1H@.IH.B...H.".p.H
7C02A0  38 E0 46 48 81 42 04 D1 BD 48 12 22 02 70 2B 48 30 E0 43 48 81 42 04 D1 B9 48 13 22 02 70 28 48  8.FH.B...H.".p+H0.CH.B...H.".p(H
7C02C0  28 E0 40 48 81 42 04 D1 B5 48 14 22 02 70 25 48 20 E0 3D 48 81 42 04 D1 B1 48 15 22 02 70 22 48  (.@H.B...H.".p%H .=H.B...H.".p"H
7C02E0  18 E0 3A 48 81 42 04 D1 AD 48 16 22 02 70 1F 48 10 E0 60 48 81 42 04 D1 A9 48 17 22 02 70 1C 48  ..:H.B...H.".p.H..`H.B...H.".p.H
7C0300  08 E0 61 48 81 42 04 D1 A5 48 18 22 02 70 19 48 00 E0 00 20 70 47 00 BF C8 F8 03 08 D4 F8 03 08  ..aH.B...H.".p.H... pG..........
7C0320  1C F0 03 08 5C FC 03 08 F8 F4 03 08 30 F0 03 08 64 FC 03 08 6C FC 03 08 E0 F8 03 08 08 F5 03 08  ....\.......0...d...l...........
7C0340  EC F8 03 08 18 F5 03 08 F8 F8 03 08 04 F9 03 08 F8 FC 03 08 FC FC 03 08 00 FD 03 08 74 FC 03 08  ............................t...
7C0360  10 F9 03 08 1C F9 03 08 28 F9 03 08 34 F9 03 08 40 F9 03 08 4C F9 03 08 E8 DE 03 08 24 FC 03 08  ........(...4...@...L.......$...
7C0380  BC FC 03 08 C0 FC 03 08 C4 FC 03 08 2C FC 03 08 C8 FC 03 08 34 FC 03 08 CC FC 03 08 3C FC 03 08  ............,.......4.......<...
7C03A0  D0 FC 03 08 D4 FC 03 08 44 FC 03 08 D8 FC 03 08 DC FC 03 08 4C FC 03 08 BC F8 03 08 E0 FC 03 08  ........D...........L...........
7C03C0  E4 FC 03 08 E8 FC 03 08 EC FC 03 08 F0 FC 03 08 1C B5 04 00 6E 48 00 21 01 70 1E 22 00 21 6D 48  ....................nH.!.p.".!mH
7C03E0  3C F0 41 FA 00 2C 07 D0 20 00 3A F0 95 FF 42 1C 21 00 68 48 3C F0 42 FA 20 00 FF F7 B9 FF 01 90  <.A...,.. .:...B.!.hH<.B. ......
```

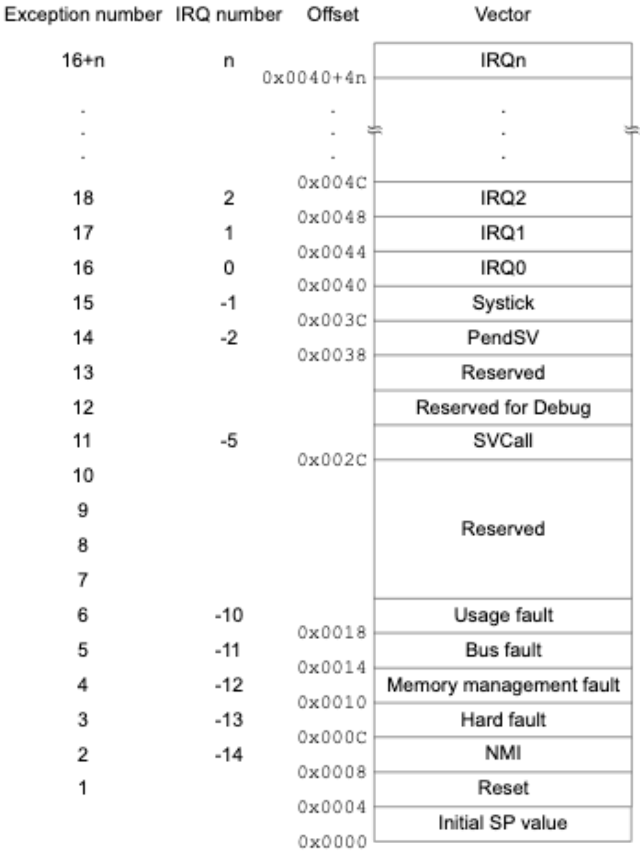
0x20002000

0x0803xxxx



```
7C0000   41 54 25 77  DE DD 03 00  41 54 52 41  43 4B 00 00  00 00 41 54  53 00 00 00  41 35 2E 30  35 00 00 00
7C0020   00 20 00 20  19 E8 03 08  35 07 03 08  39 07 03 08  8D 07 03 08  8F 07 03 08  91 07 03 08  00 00 00 00
7C0040   00 00 00 00  00 00 00 00  00 00 00 00  95 07 03 08  93 07 03 08  00 00 00 00  97 07 03 08  99 07 03 08
7C0060   5D 08 03 08  61 08 03 08  51 09 03 08  45 A6 02 08  53 09 03 08  55 09 03 08  59 09 03 08  C9 09 03 08
7C0080   91 0A 03 08  89 0D 03 08  F9 0A 03 08  FB 0A 03 08  FD 0A 03 08  FF 0A 03 08  01 0B 03 08  03 0B 03 08
7C00A0   05 0B 03 08  07 0B 03 08  09 0B 03 08  0B 0B 03 08  0D 0B 03 08  0F 0B 03 08  11 0B 03 08  15 0B 03 08
7C00C0   81 0D 03 08  83 0D 03 08  85 0D 03 08  87 0D 03 08  8B 0D 03 08  8D 0D 03 08  91 0D 03 08  A5 0D 03 08
7C00E0   A7 0D 03 08  A9 0D 03 08  AB 0D 03 08  AD 0D 03 08  AF 0D 03 08  91 12 03 08  2F 13 03 08  D9 13 03 08
7C0100   A5 0C 03 08  3D AF 02 08  B1 0D 03 08  B3 0D 03 08  B5 0D 03 08  B7 0D 03 08  B9 0D 03 08  BB 0D 03 08
7C0120   BD 0D 03 08  BF 0D 03 08  B5 34 02 08  C1 0D 03 08  C3 0D 03 08  C5 0D 03 08  C7 0D 03 08  C9 0D 03 08
7C0140   CB 0D 03 08  CD 0D 03 08  CF 0D 03 08  D1 0D 03 08  05 48 00 68  10 F4 E0 60  04 49 08 43  02 49 08 60
7C0160   BF F3 4F 8F  FE E7 00 BF  0C ED 00 E0  04 00 FA 05  01 00 81 48  81 42 05 D1  DF F8 24 04  01 22 02 70
7C0180   65 48 C7 E0  7D 48 81 42  05 D1 DF F8  14 04 02 22  02 70 62 48  BE E0 7A 48  81 42 05 D1  DF F8 00 04
7C01A0   03 22 02 70  5E 48 B5 E0  76 48 81 42  05 D1 DF F8  F0 03 04 22  02 70 5B 48  AC E0 73 48  81 42 05 D1
7C01C0   DF F8 DC 03  05 22 02 70  57 48 A3 E0  6F 48 81 42  05 D1 DF F8  CC 03 06 22  02 70 54 48  9A E0 6C 48
7C01E0   81 42 05 D1  DF F8 B8 03  07 22 02 70  50 48 91 E0  68 48 81 42  05 D1 DF F8  A8 03 08 22  02 70 4D 48
7C0200   88 E0 65 48  81 42 05 D1  DF F8 94 03  09 22 02 70  49 48 7F E0  61 48 81 42  05 D1 DF F8  84 03 0A 22
7C0220   02 70 46 48  76 E0 5E 48  81 42 05 D1  DF F8 70 03  0B 22 02 70  42 48 6D E0  5A 48 81 42  05 D1 DF F8
7C0240   60 03 0C 22  02 70 3F 48  64 E0 57 48  81 42 05 D1  DF F8 4C 03  0D 22 02 70  3B 48 5B E0  53 48 81 42
7C0260   05 D1 DF F8  3C 03 0E 22  02 70 38 48  52 E0 50 48  81 42 05 D1  DF F8 28 03  0F 22 02 70  34 48 49 E0
7C0280   4C 48 81 42  05 D1 DF F8  18 03 10 22  02 70 31 48  40 E0 49 48  81 42 04 D1  C1 48 11 22  02 70 2E 48
```

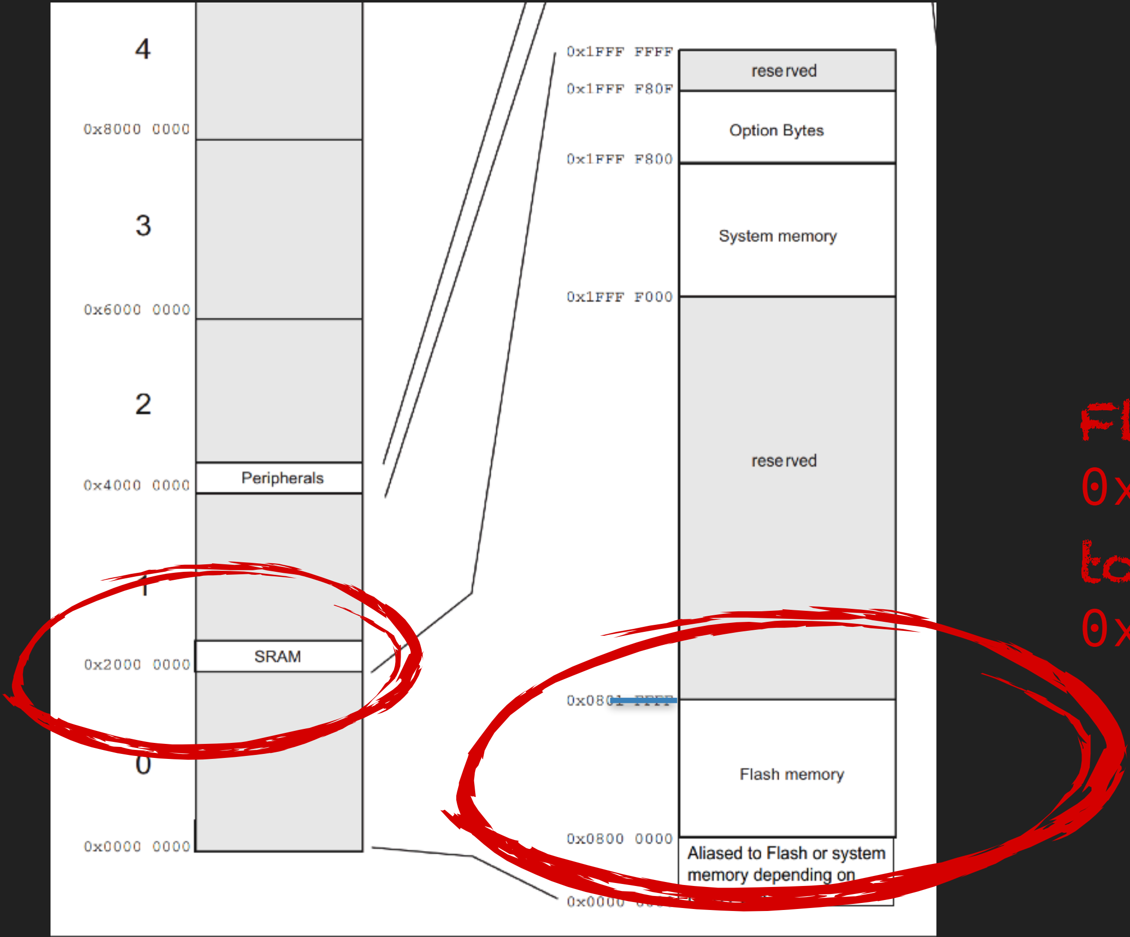
Is that a firmware?



Exception number	IRQ number	Offset	Vector
16+n	n	0x0040+4n	IRQn
. . .		. . . 0x004C	. . .
18	2	0x0048	IRQ2
17	1	0x0044	IRQ1
16	0	0x0040	IRQ0
15	-1	0x003C	Systick
14	-2	0x0038	PendSV
13			Reserved
12			Reserved for Debug
11	-5	0x002C	SVCall
10			Reserved
9			
8			
7			
6	-10	0x0018	Usage fault
5	-11	0x0014	Bus fault
4	-12	0x0010	Memory management fault
3	-13	0x000C	Hard fault
2	-14	0x0008	NMI
1		0x0004	Reset
		0x0000	Initial SP value

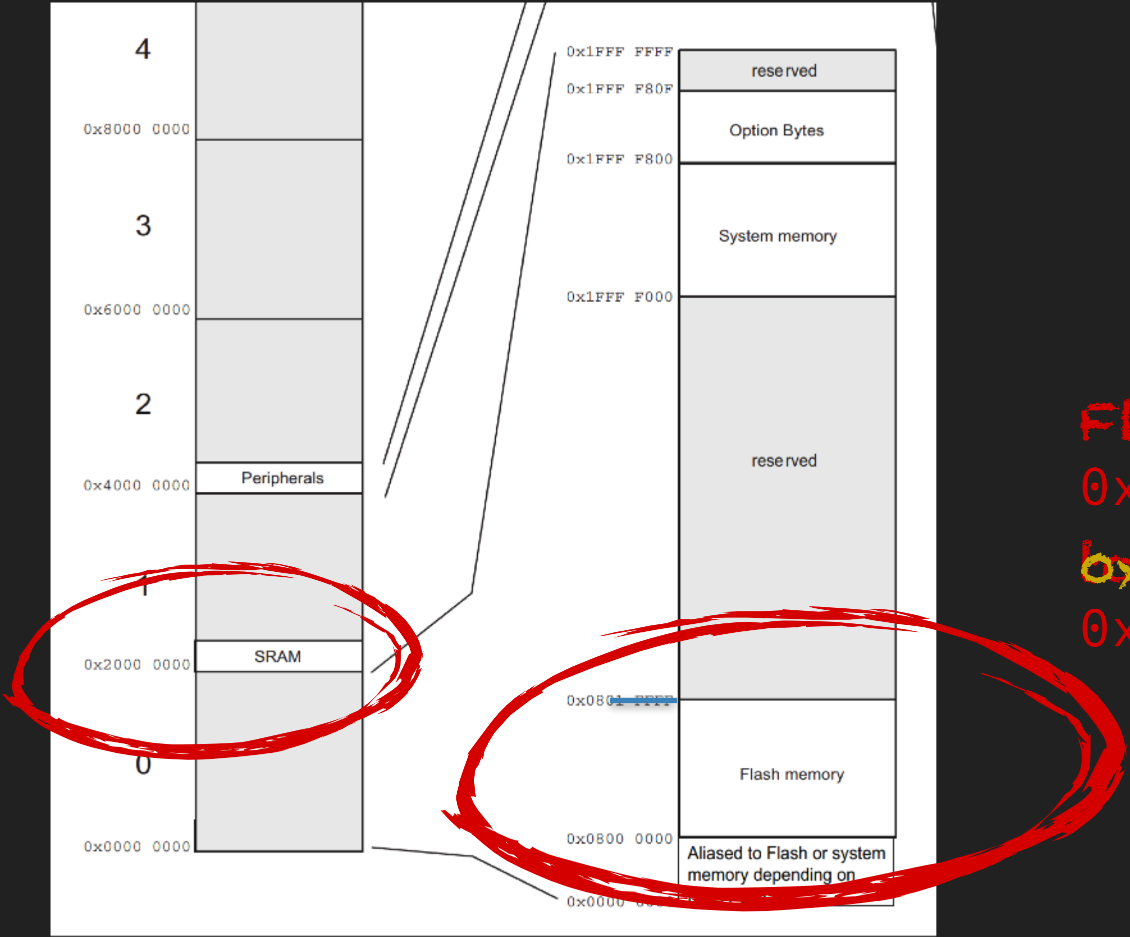
STM32f10xRC Memory map

SRAM:
0x20000000
to
0x20007fff



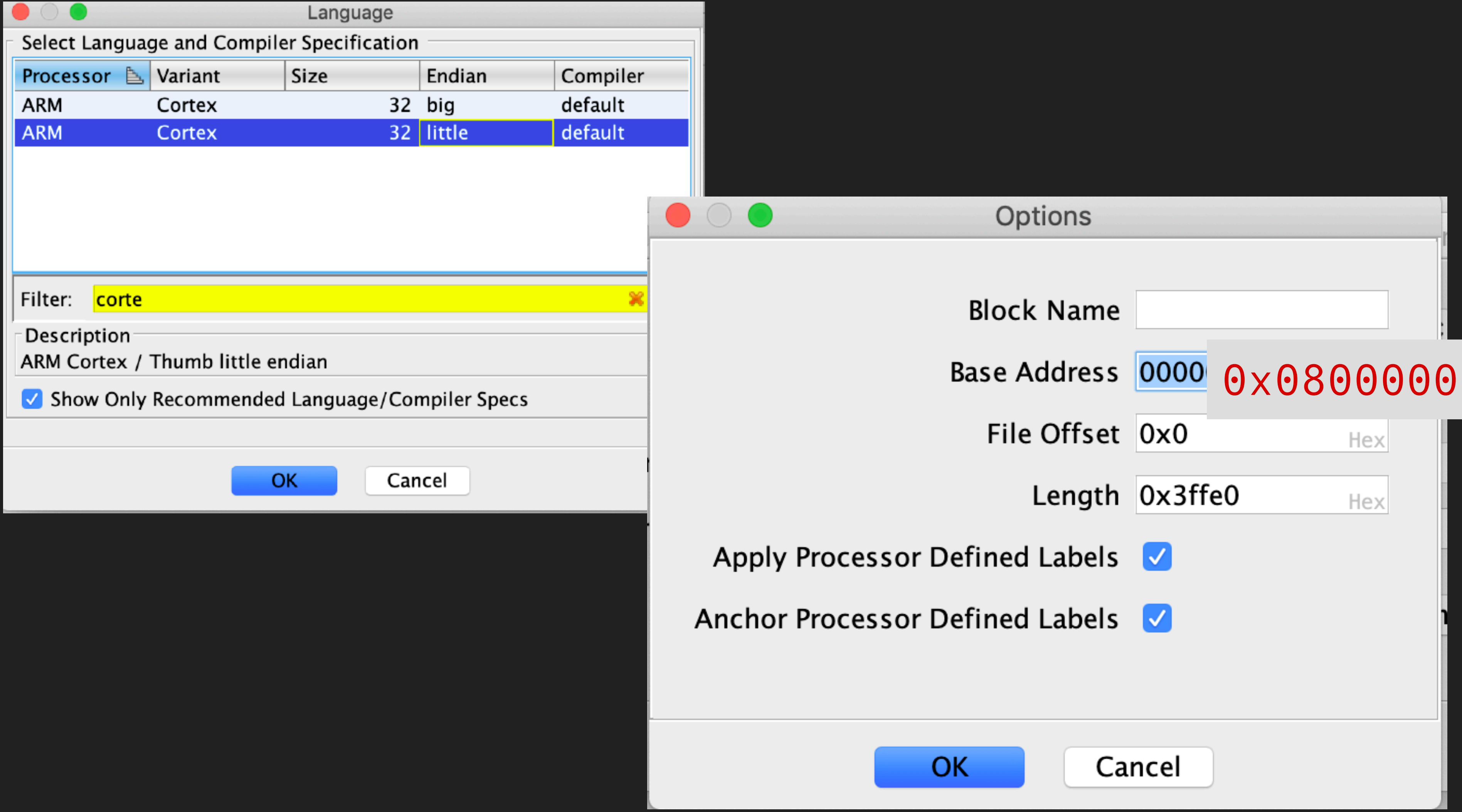
Flash:
0x08000000
to
0x0803FFFF

STM32f103 Memory map



SRAM:
0x20000000
0x20002000
0x20007fff

Flash:
0x08000000
0x0803xxxx
0x0803FFFF



Language

Select Language and Compiler Specification

Processor	Variant	Size	Endian	Compiler
ARM	Cortex	32	big	default
ARM	Cortex	32	little	default

Filter: corte

Description

ARM Cortex / Thumb little endian

☑ Show Only Recommended Language/Compiler Specs

Options

Block Name:

Base Address: 0000(

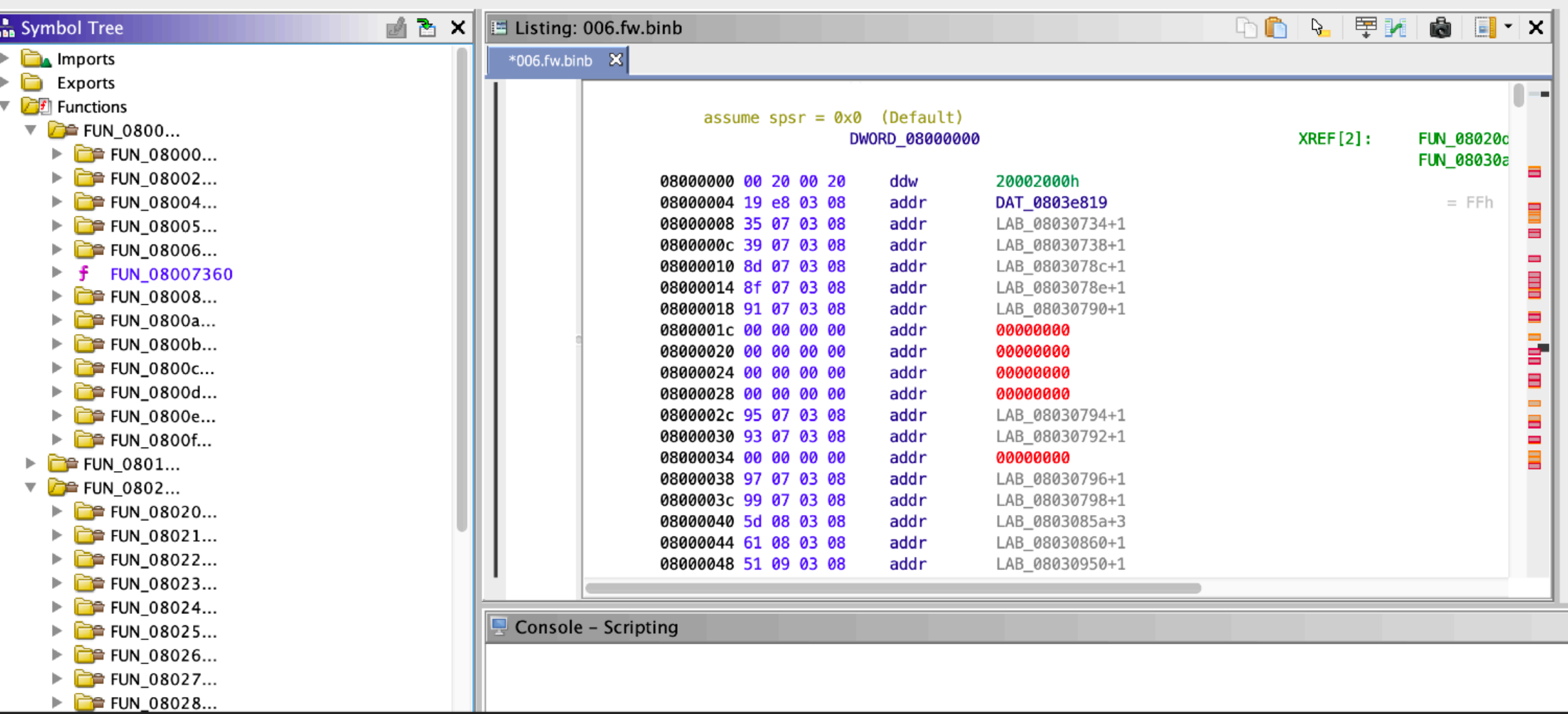
0x0800000

File Offset: 0x0 Hex

Length: 0x3ffe0 Hex

Apply Processor Defined Labels ☑

Anchor Processor Defined Labels ☑



Symbol Tree

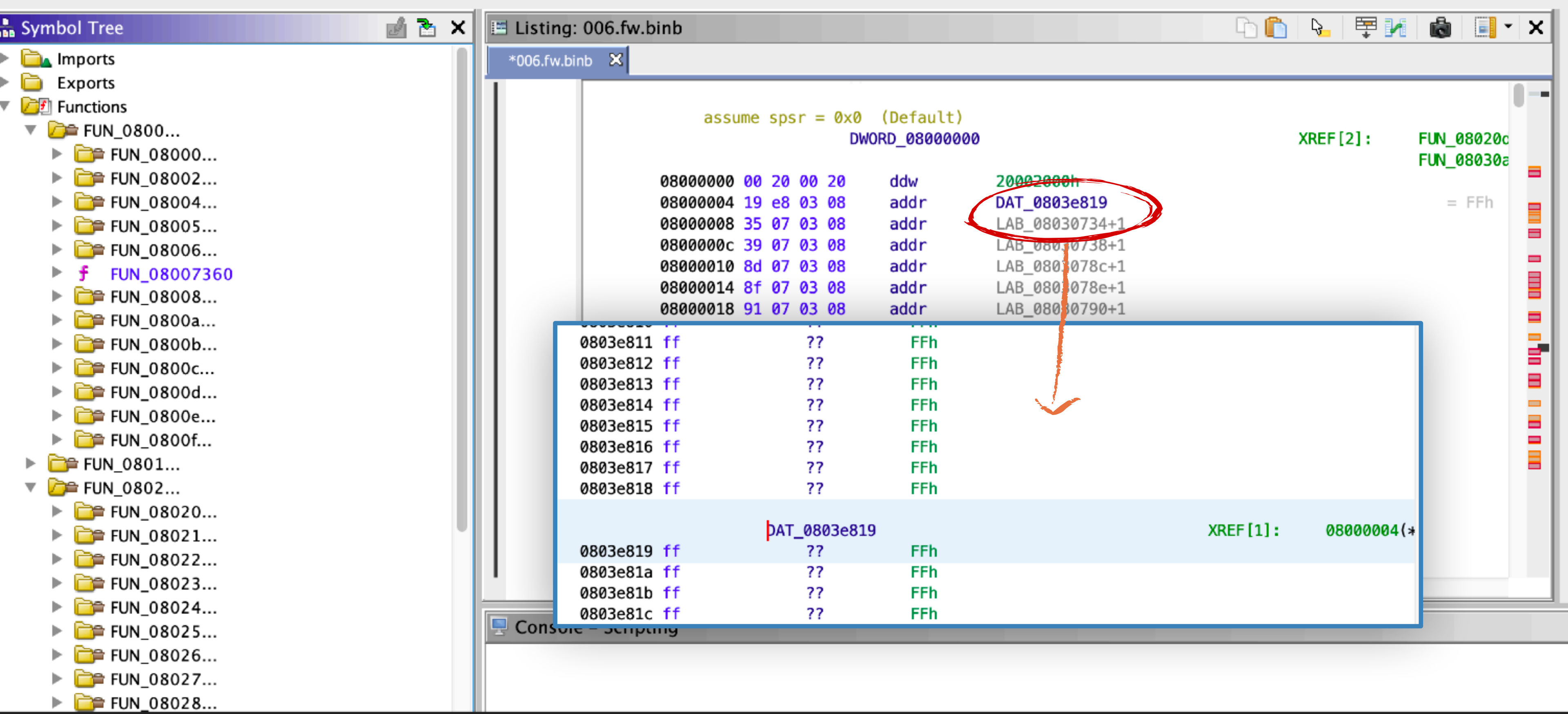
- Imports
- Exports
- Functions
  - FUN_0800...
    - FUN_08000...
    - FUN_08002...
    - FUN_08004...
    - FUN_08005...
    - FUN_08006...
    - FUN_08007360
    - FUN_08008...
    - FUN_0800a...
    - FUN_0800b...
    - FUN_0800c...
    - FUN_0800d...
    - FUN_0800e...
    - FUN_0800f...
  - FUN_0801...
  - FUN_0802...
    - FUN_08020...
    - FUN_08021...
    - FUN_08022...
    - FUN_08023...
    - FUN_08024...
    - FUN_08025...
    - FUN_08026...
    - FUN_08027...
    - FUN_08028...

Listing: 006.fw.binb

*006.fw.binb

```
            assume spsr = 0x0  (Default)
                        DWORD_08000000                          XREF[2]:     FUN_08020c
                                                                             FUN_08030a
  08000000 00 20 00 20     ddw        20002000h
  08000004 19 e8 03 08     addr       DAT_0803e819                                = FFh
  08000008 35 07 03 08     addr       LAB_08030734+1
  0800000c 39 07 03 08     addr       LAB_08030738+1
  08000010 8d 07 03 08     addr       LAB_0803078c+1
  08000014 8f 07 03 08     addr       LAB_0803078e+1
  08000018 91 07 03 08     addr       LAB_08030790+1
  0800001c 00 00 00 00     addr       00000000
  08000020 00 00 00 00     addr       00000000
  08000024 00 00 00 00     addr       00000000
  08000028 00 00 00 00     addr       00000000
  0800002c 95 07 03 08     addr       LAB_08030794+1
  08000030 93 07 03 08     addr       LAB_08030792+1
  08000034 00 00 00 00     addr       00000000
  08000038 97 07 03 08     addr       LAB_08030796+1
  0800003c 99 07 03 08     addr       LAB_08030798+1
  08000040 5d 08 03 08     addr       LAB_0803085a+3
  08000044 61 08 03 08     addr       LAB_08030860+1
  08000048 51 09 03 08     addr       LAB_08030950+1
```

Console - Scripting

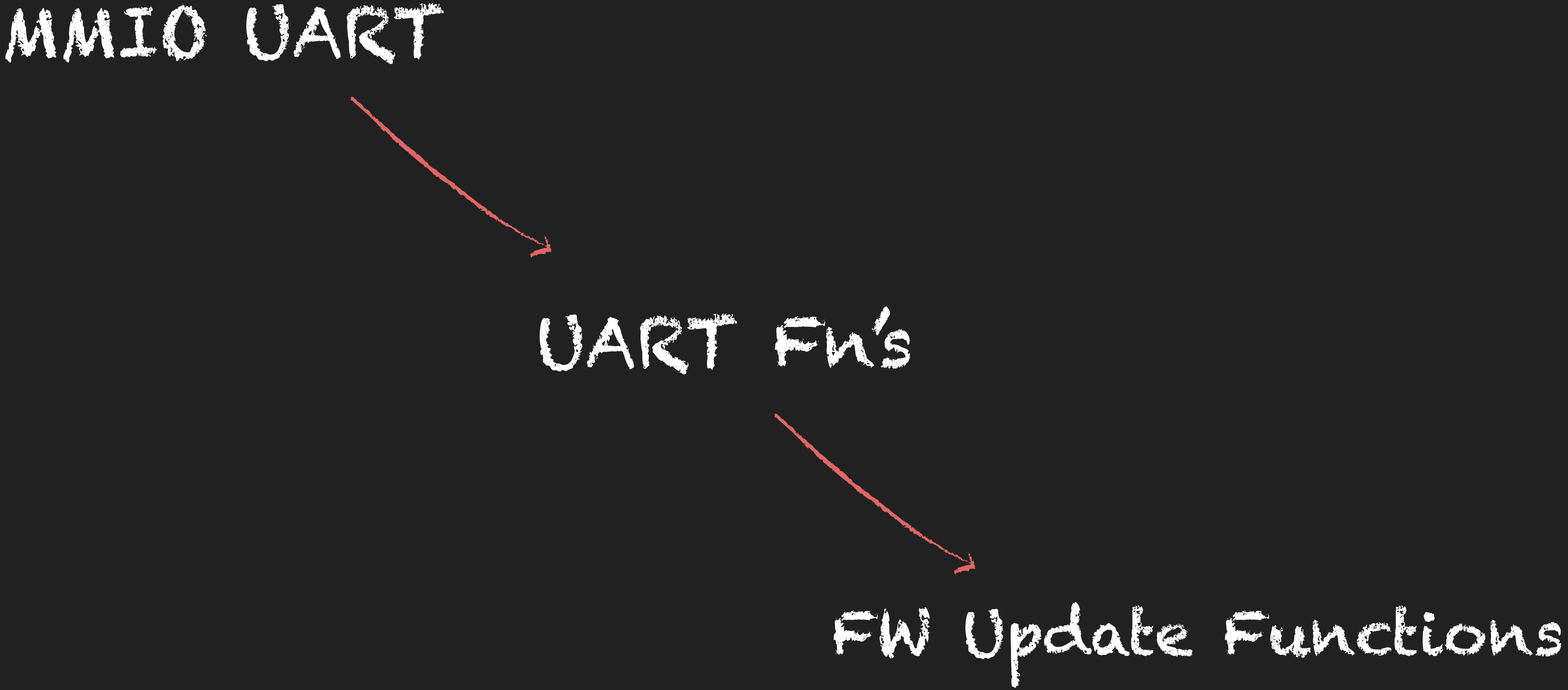


```
              assume spsr = 0x0  (Default)
                        DWORD_08000000                      XREF[2]:     FUN_08020c
                                                                         FUN_08030a
08000000 00 20 00 20     ddw       20002000h
08000004 19 e8 03 08     addr      DAT_0803e819                                 = FFh
08000008 35 07 03 08     addr      LAB_08030734+1
0800000c 39 07 03 08     addr      LAB_08030738+1
08000010 8d 07 03 08     addr      LAB_0803078c+1
08000014 8f 07 03 08     addr      LAB_0803078e+1
08000018 91 07 03 08     addr      LAB_08030790+1
```

```
0803e811 ff          ??         FFh
0803e812 ff          ??         FFh
0803e813 ff          ??         FFh
0803e814 ff          ??         FFh
0803e815 ff          ??         FFh
0803e816 ff          ??         FFh
0803e817 ff          ??         FFh
0803e818 ff          ??         FFh

               DAT_0803e819                          XREF[1]:     08000004(*
0803e819 ff          ??         FFh
0803e81a ff          ??         FFh
0803e81b ff          ??         FFh
0803e81c ff          ??         FFh
```

Reset function not in the FW?

Fake firmware update to dump all the flash



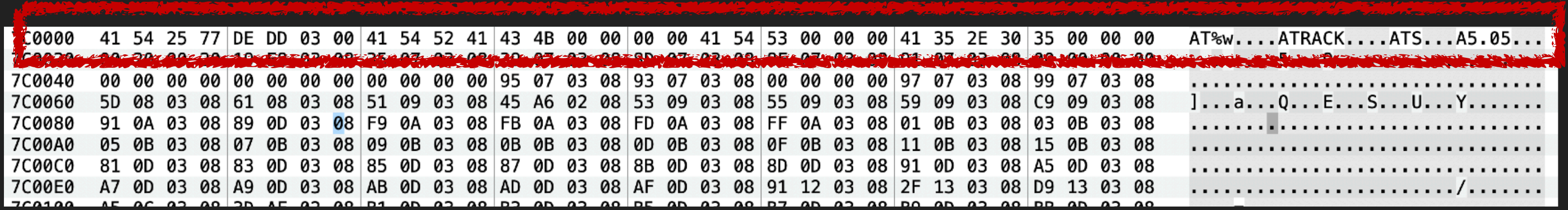
MMIO UART

UART Fn's

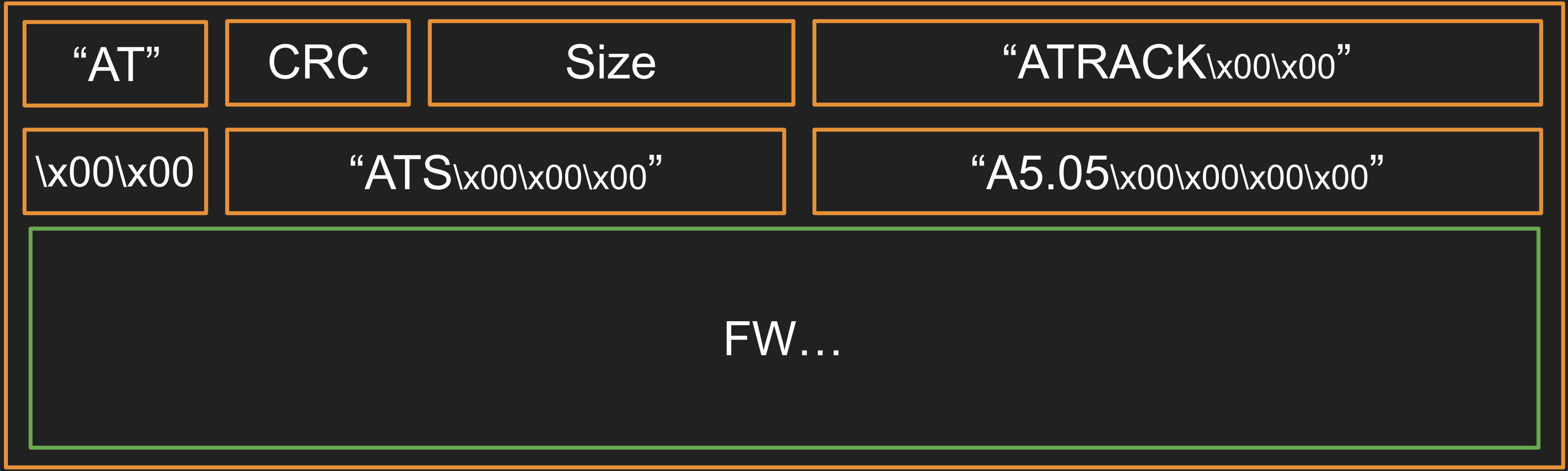
FW Update Functions

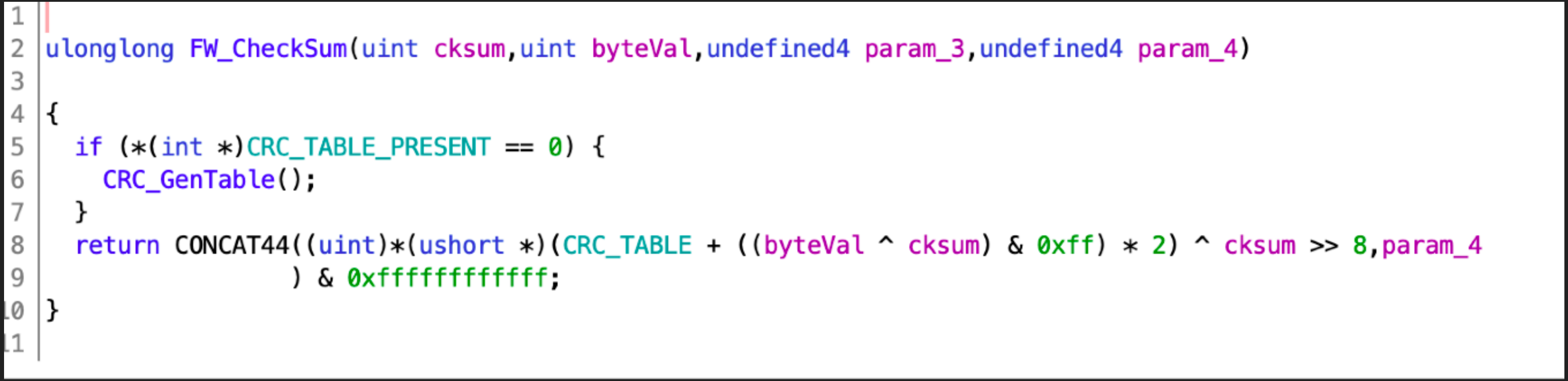
Reversed firmware update format, so far

Checksum?m etc



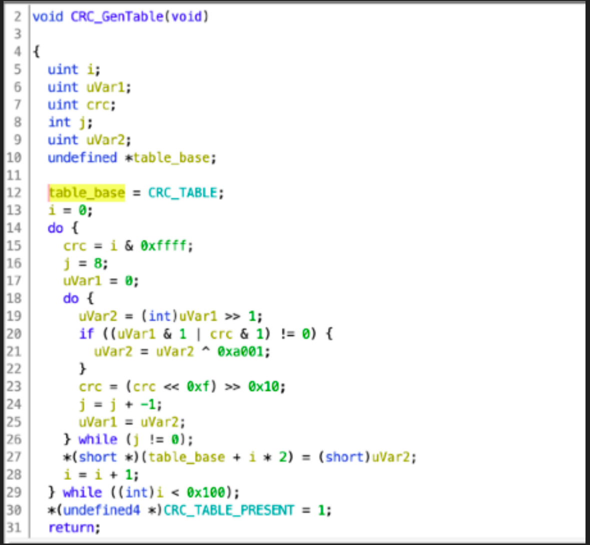
```
7C0000  41 54 25 77 DE DD 03 00 41 54 52 41 43 4B 00 00 00 00 41 54 53 00 00 00 41 35 2E 30 35 00 00 00   AT%w....ATRACK....ATS...A5.05...
7C0040  00 00 00 00 00 00 00 00 00 00 00 00 95 07 03 08 93 07 03 08 00 00 00 00 97 07 03 08 99 07 03 08   ................................
7C0060  5D 08 03 08 61 08 03 08 51 09 03 08 45 A6 02 08 53 09 03 08 55 09 03 08 59 09 03 08 C9 09 03 08   ]...a...Q...E...S...U...Y.......
7C0080  91 0A 03 08 89 0D 03 08 F9 0A 03 08 FB 0A 03 08 FD 0A 03 08 FF 0A 03 08 01 0B 03 08 03 0B 03 08   ................................
7C00A0  05 0B 03 08 07 0B 03 08 09 0B 03 08 0B 0B 03 08 0D 0B 03 08 0F 0B 03 08 11 0B 03 08 15 0B 03 08   ................................
7C00C0  81 0D 03 08 83 0D 03 08 85 0D 03 08 87 0D 03 08 8B 0D 03 08 8D 0D 03 08 91 0D 03 08 A5 0D 03 08   ................................
7C00E0  A7 0D 03 08 A9 0D 03 08 AB 0D 03 08 AD 0D 03 08 AF 0D 03 08 91 12 03 08 2F 13 03 08 D9 13 03 08   ......................../.......
```





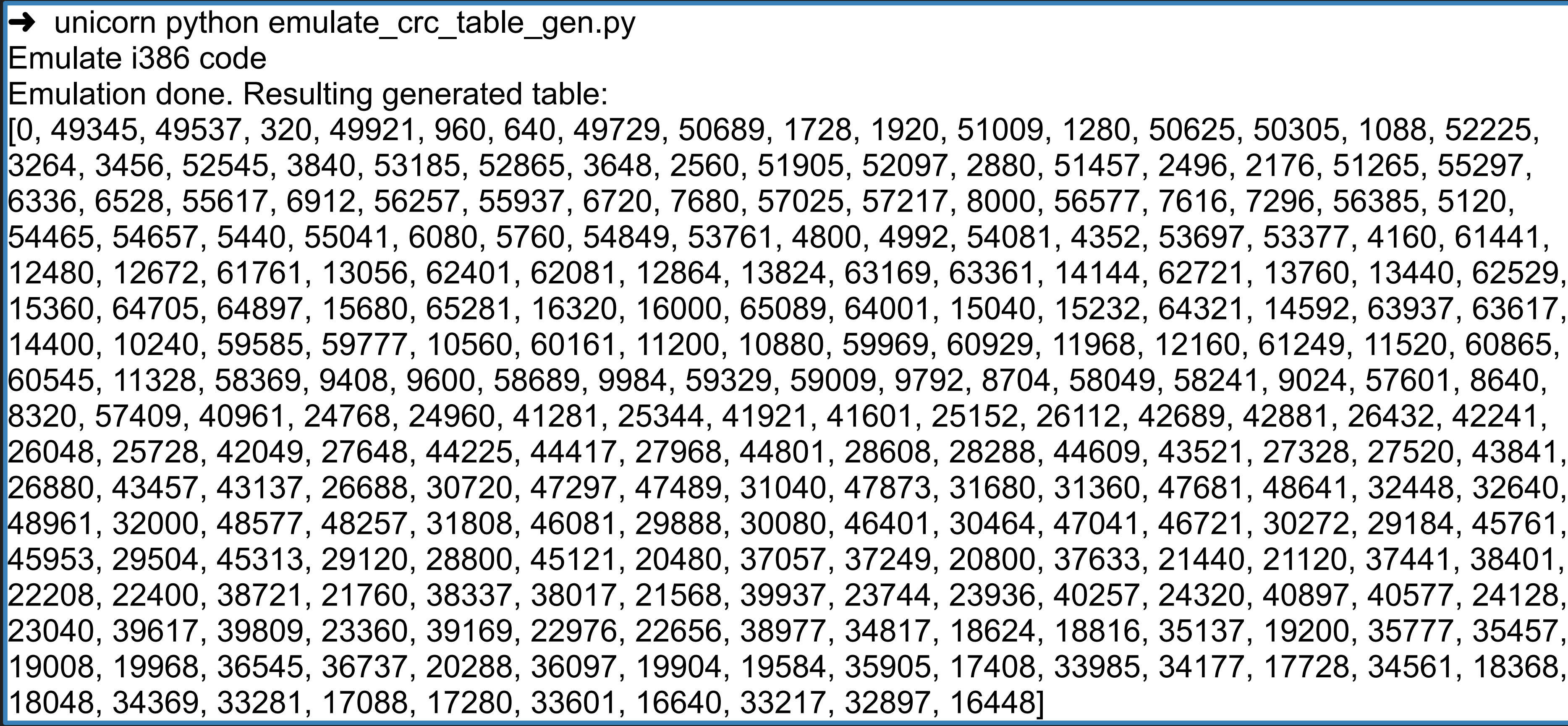
```

ulonglong FW_CheckSum(uint cksum,uint byteVal,undefined4 param_3,undefined4 param_4)

{
  if (*(int *)CRC_TABLE_PRESENT == 0) {
    CRC_GenTable();
  }
  return CONCAT44((uint)*(ushort *)(CRC_TABLE + ((byteVal ^ cksum) & 0xff) * 2) ^ cksum >> 8,param_4
                 ) & 0xffffffffffff;
}

```

What is the crc ?

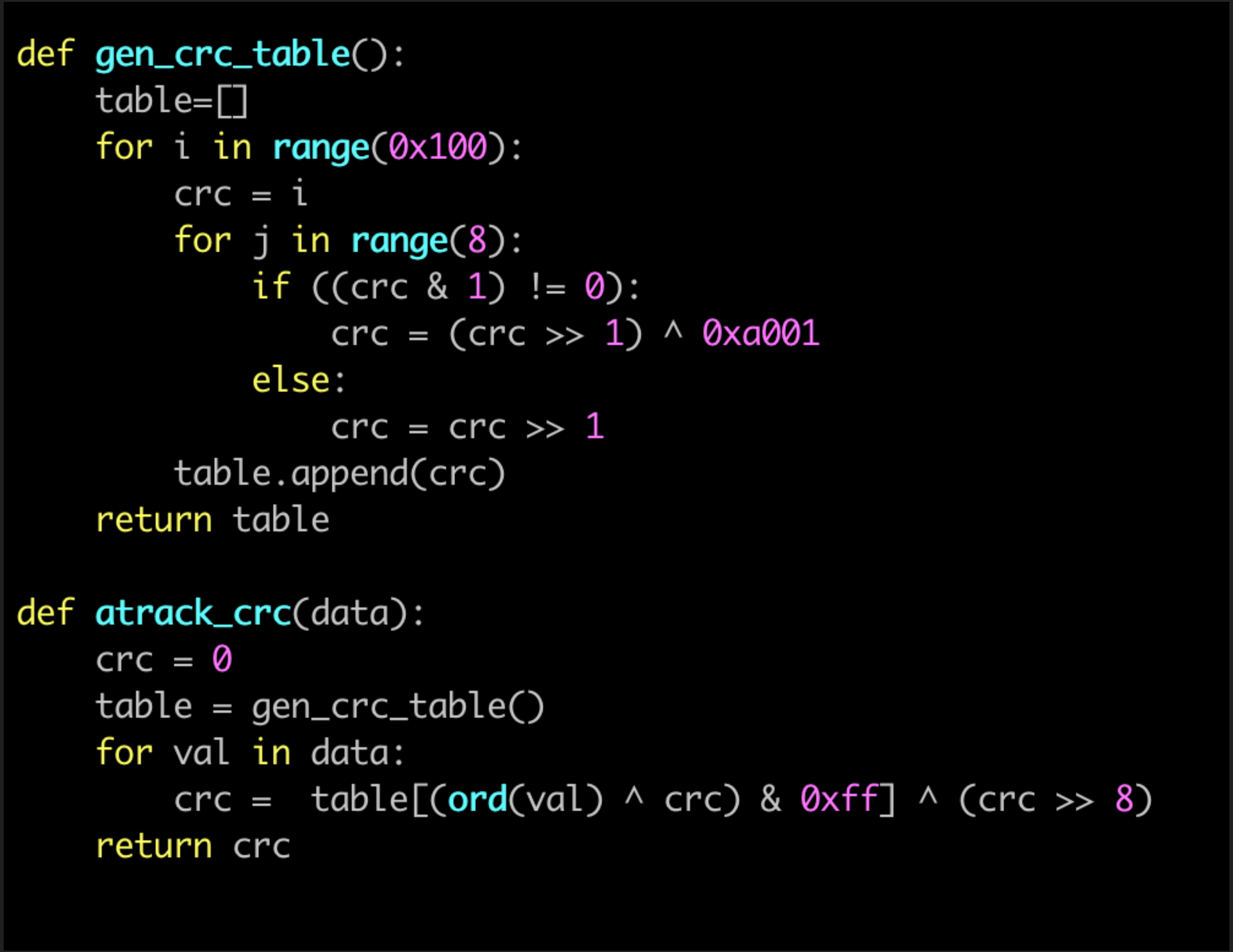


```
void CRC_GenTable(void)

{
  uint i;
  uint uVar1;
  uint crc;
  int j;
  uint uVar2;
  undefined *table_base;

  table_base = CRC_TABLE;
  i = 0;
  do {
    crc = i & 0xffff;
    j = 8;
    uVar1 = 0;
    do {
      uVar2 = (int)uVar1 >> 1;
      if ((uVar1 & 1 | crc & 1) != 0) {
        uVar2 = uVar2 ^ 0xa001;
      }
      crc = (crc << 0xf) >> 0x10;
      j = j + -1;
      uVar1 = uVar2;
    } while (j != 0);
    *(short *)(table_base + i * 2) = (short)uVar2;
    i = i + 1;
  } while ((int)i < 0x100);
  *(undefined4 *)CRC_TABLE_PRESENT = 1;
  return;
```

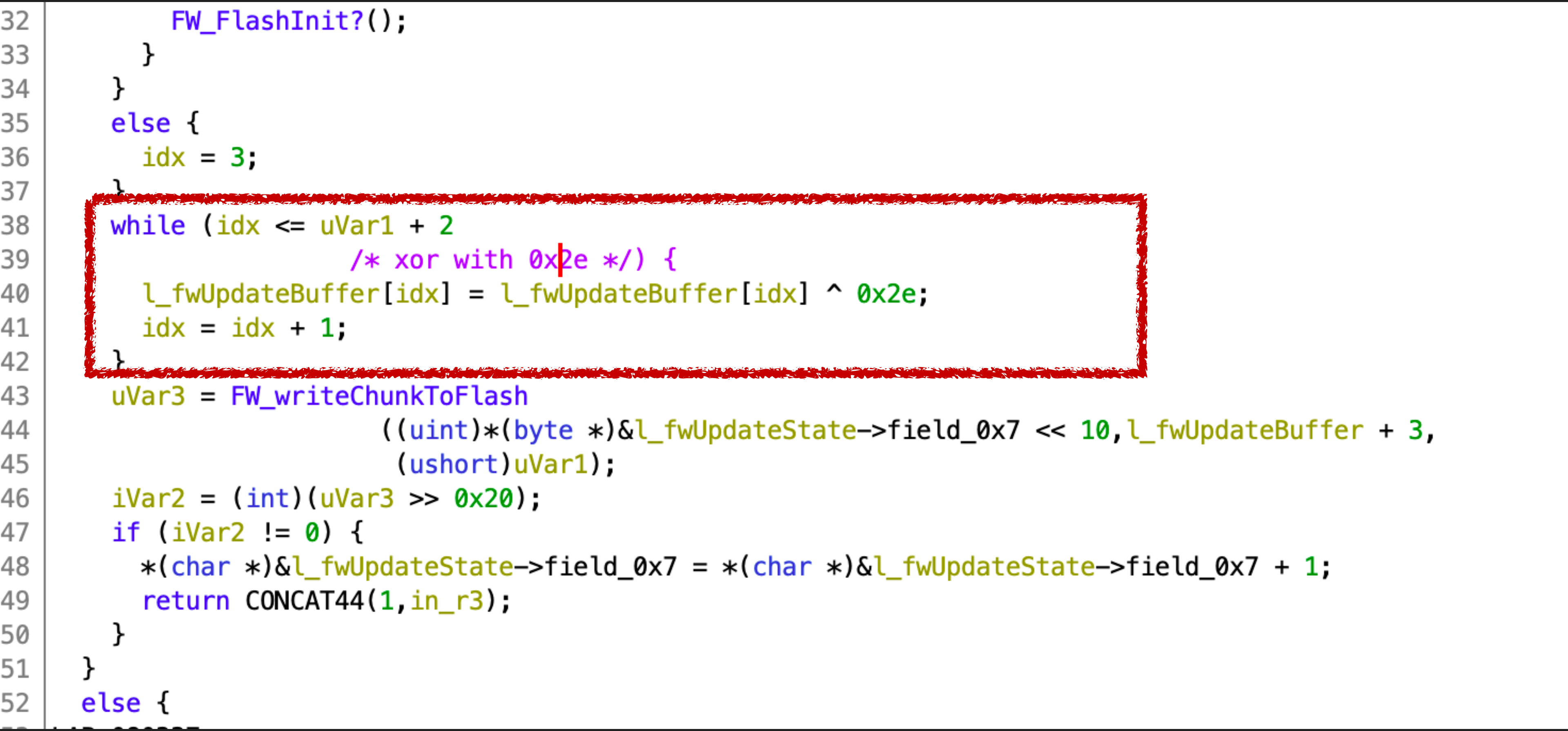
Emulate table generation function with unicorn



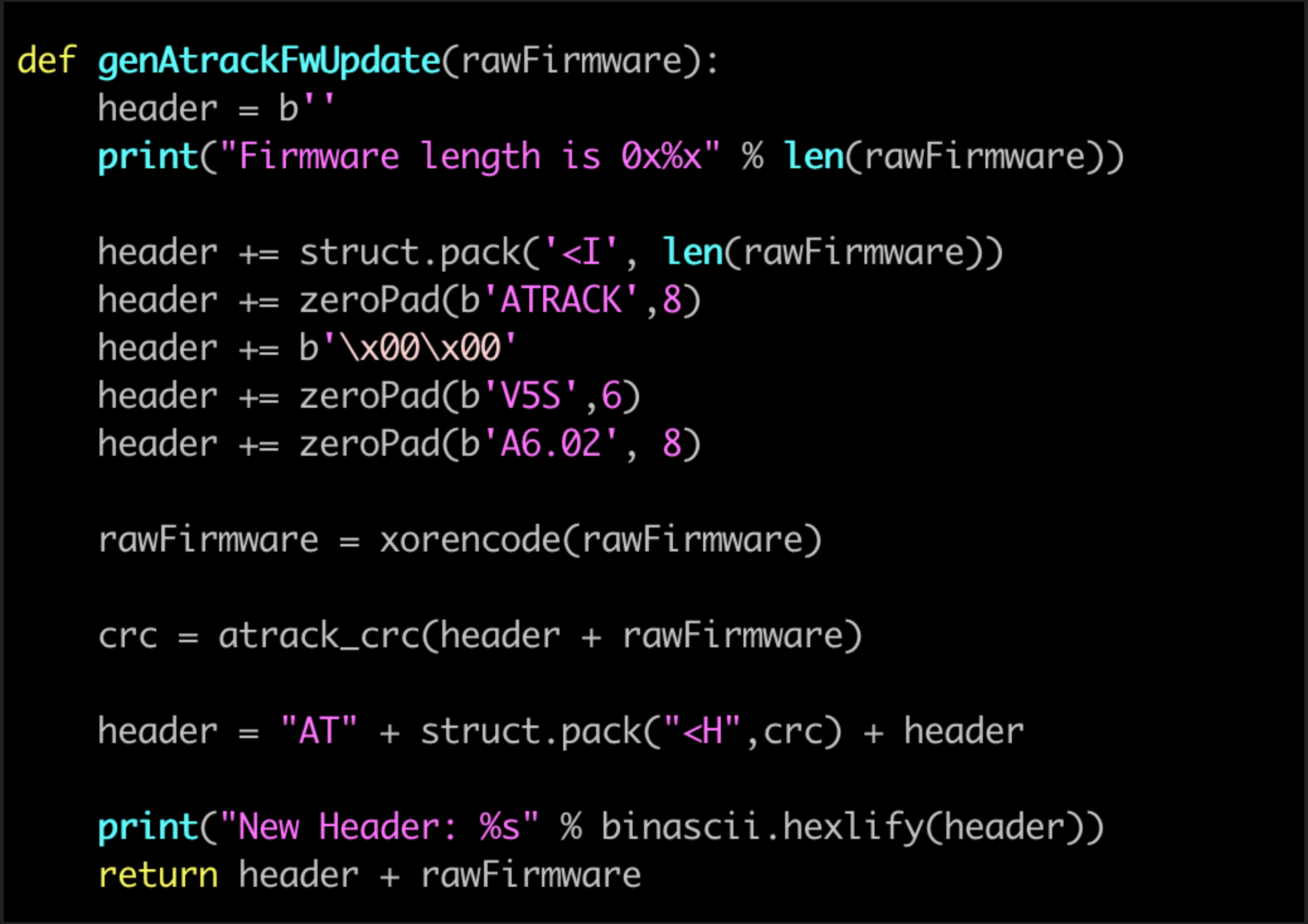
```
➜  unicorn python emulate_crc_table_gen.py
Emulate i386 code
Emulation done. Resulting generated table:
[0, 49345, 49537, 320, 49921, 960, 640, 49729, 50689, 1728, 1920, 51009, 1280, 50625, 50305, 1088, 52225,
3264, 3456, 52545, 3840, 53185, 52865, 3648, 2560, 51905, 52097, 2880, 51457, 2496, 2176, 51265, 55297,
6336, 6528, 55617, 6912, 56257, 55937, 6720, 7680, 57025, 57217, 8000, 56577, 7616, 7296, 56385, 5120,
54465, 54657, 5440, 55041, 6080, 5760, 54849, 53761, 4800, 4992, 54081, 4352, 53697, 53377, 4160, 61441,
12480, 12672, 61761, 13056, 62401, 62081, 12864, 13824, 63169, 63361, 14144, 62721, 13760, 13440, 62529,
15360, 64705, 64897, 15680, 65281, 16320, 16000, 65089, 64001, 15040, 15232, 64321, 14592, 63937, 63617,
14400, 10240, 59585, 59777, 10560, 60161, 11200, 10880, 59969, 60929, 11968, 12160, 61249, 11520, 60865,
60545, 11328, 58369, 9408, 9600, 58689, 9984, 59329, 59009, 9792, 8704, 58049, 58241, 9024, 57601, 8640,
8320, 57409, 40961, 24768, 24960, 41281, 25344, 41921, 41601, 25152, 26112, 42689, 42881, 26432, 42241,
26048, 25728, 42049, 27648, 44225, 44417, 27968, 44801, 28608, 28288, 44609, 43521, 27328, 27520, 43841,
26880, 43457, 43137, 26688, 30720, 47297, 47489, 31040, 47873, 31680, 31360, 47681, 48641, 32448, 32640,
48961, 32000, 48577, 48257, 31808, 46081, 29888, 30080, 46401, 30464, 47041, 46721, 30272, 29184, 45761,
45953, 29504, 45313, 29120, 28800, 45121, 20480, 37057, 37249, 20800, 37633, 21440, 21120, 37441, 38401,
22208, 22400, 38721, 21760, 38337, 38017, 21568, 39937, 23744, 23936, 40257, 24320, 40897, 40577, 24128,
23040, 39617, 39809, 23360, 39169, 22976, 22656, 38977, 34817, 18624, 18816, 35137, 19200, 35777, 35457,
19008, 19968, 36545, 36737, 20288, 36097, 19904, 19584, 35905, 17408, 33985, 34177, 17728, 34561, 18368,
18048, 34369, 33281, 17088, 17280, 33601, 16640, 33217, 32897, 16448]
```



```python
def gen_crc_table():
    table=[]
    for i in range(0x100):
        crc = i
        for j in range(8):
            if ((crc & 1) != 0):
                crc = (crc >> 1) ^ 0xa001
            else:
                crc = crc >> 1
        table.append(crc)
    return table

def atrack_crc(data):
    crc = 0
    table = gen_crc_table()
    for val in data:
        crc =  table[(ord(val) ^ crc) & 0xff] ^ (crc >> 8)
    return crc
```



```
      FW_FlashInit?();
    }
  }
  else {
    idx = 3;
  }
  while (idx <= uVar1 + 2
                  /* xor with 0x2e */) {
    l_fwUpdateBuffer[idx] = l_fwUpdateBuffer[idx] ^ 0x2e;
    idx = idx + 1;
  }
  uVar3 = FW_writeChunkToFlash
                    ((uint)*(byte *)&l_fwUpdateState->field_0x7 << 10,l_fwUpdateBuffer + 3,
                     (ushort)uVar1);
  iVar2 = (int)(uVar3 >> 0x20);
  if (iVar2 != 0) {
    *(char *)&l_fwUpdateState->field_0x7 = *(char *)&l_fwUpdateState->field_0x7 + 1;
    return CONCAT44(1,in_r3);
  }
}
else {
```



```
def genAtrackFwUpdate(rawFirmware):
    header = b''
    print("Firmware length is 0x%x" % len(rawFirmware))

    header += struct.pack('<I', len(rawFirmware))
    header += zeroPad(b'ATRACK',8)
    header += b'\x00\x00'
    header += zeroPad(b'V5S',6)
    header += zeroPad(b'A6.02', 8)

    rawFirmware = xorencode(rawFirmware)

    crc = atrack_crc(header + rawFirmware)

    header = "AT" + struct.pack("<H",crc) + header

    print("New Header: %s" % binascii.hexlify(header))
    return header + rawFirmware
```

To be continued..

ACK's

Intel STORM Team! \o/

And many friends who have helped in the process:

Anto, Anibal, Nico, Esteban, Facu, Andrés, Emi, etc