Trashing like it's 1999

Unsolicited forensics on GPS trackers

Map of the World

v0.13

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

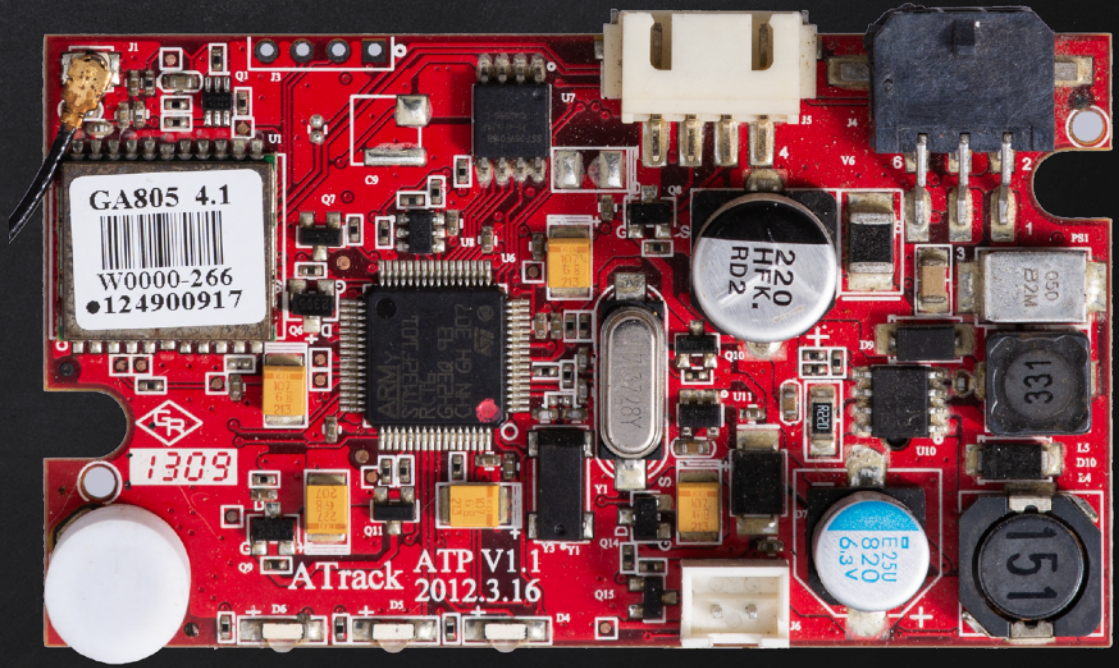
Once upon a time,

In a land far far away...


SeamTrack
www.seamtrack.com
GSM GPS PWR
AT5
AU7
A dream become true.

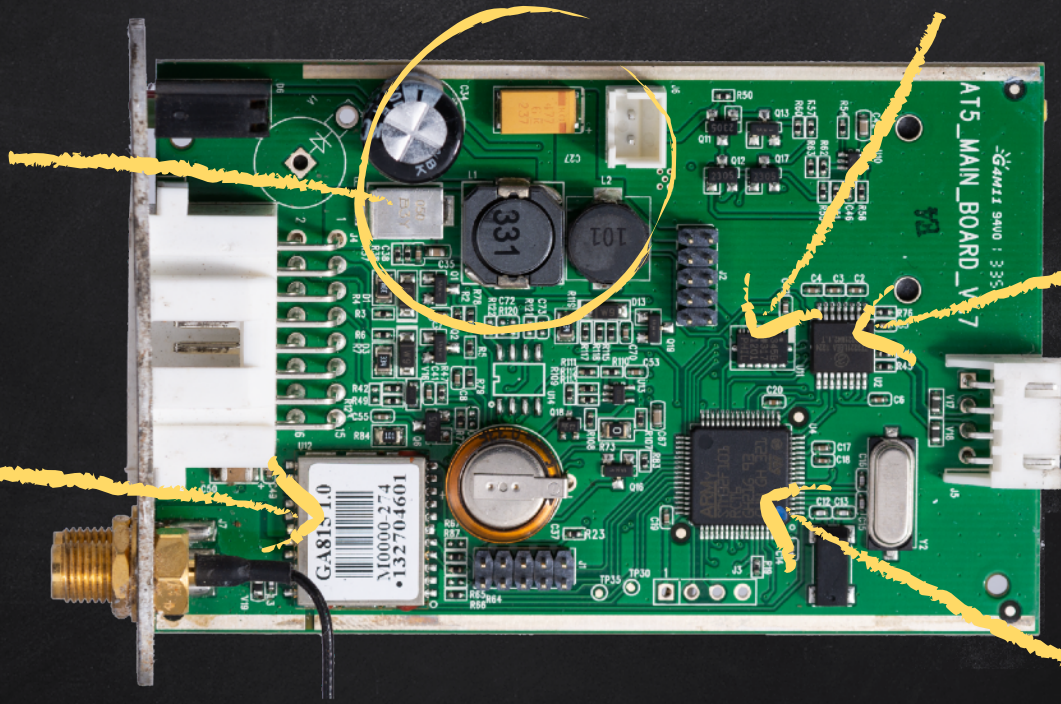
What are they?

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



Accelerometer

Power supply



rs232 transceiver

Serial connector

GPS

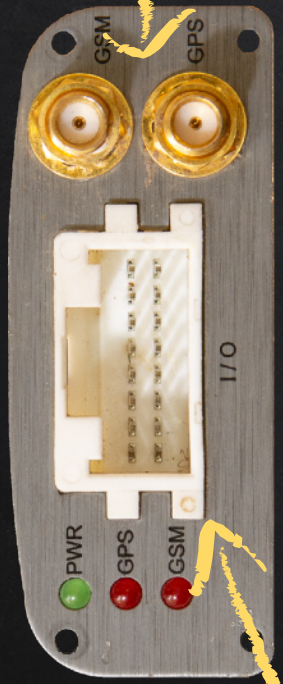
CPU

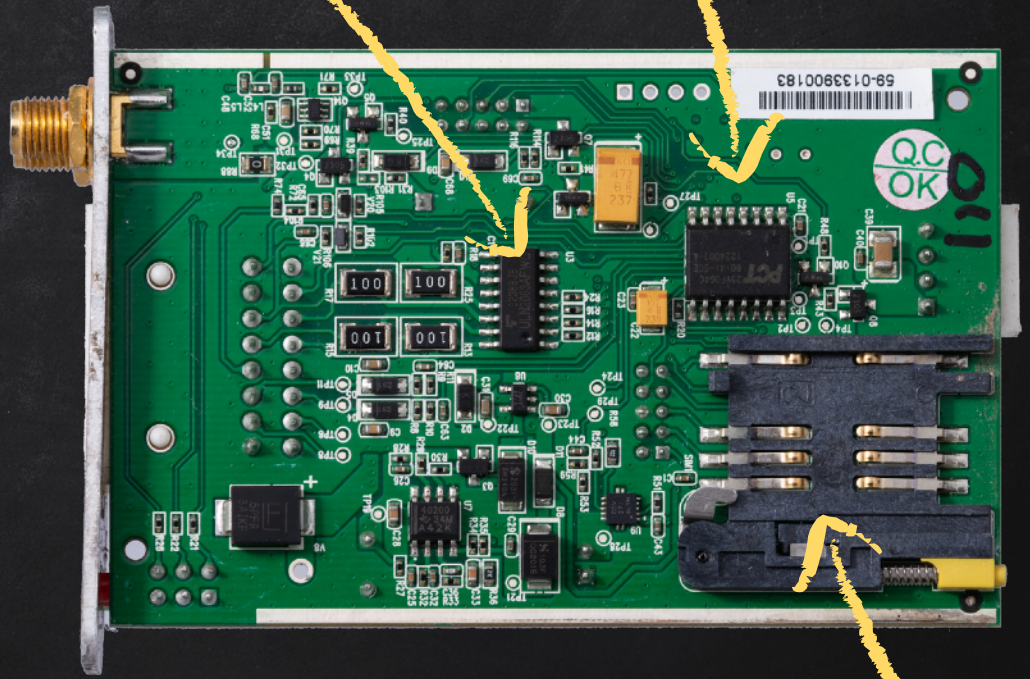
STM32F101/103
ARM Cortex M3 32-bit

GPS, GSM Antennas

Driver

Flash



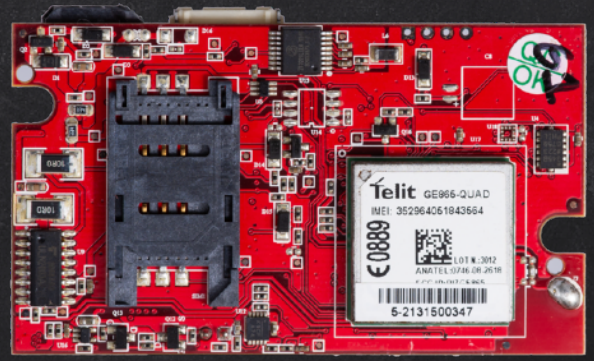


Main Connector

IOs, Power, etc

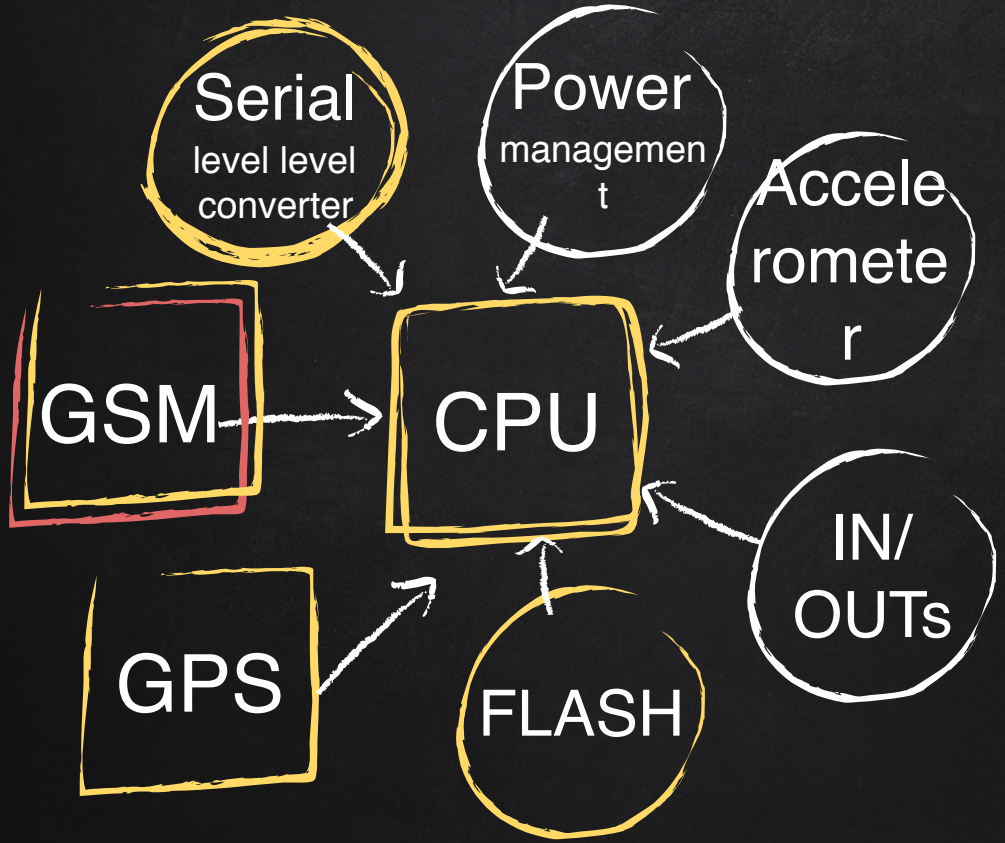
SIM socket


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



Find all the  !

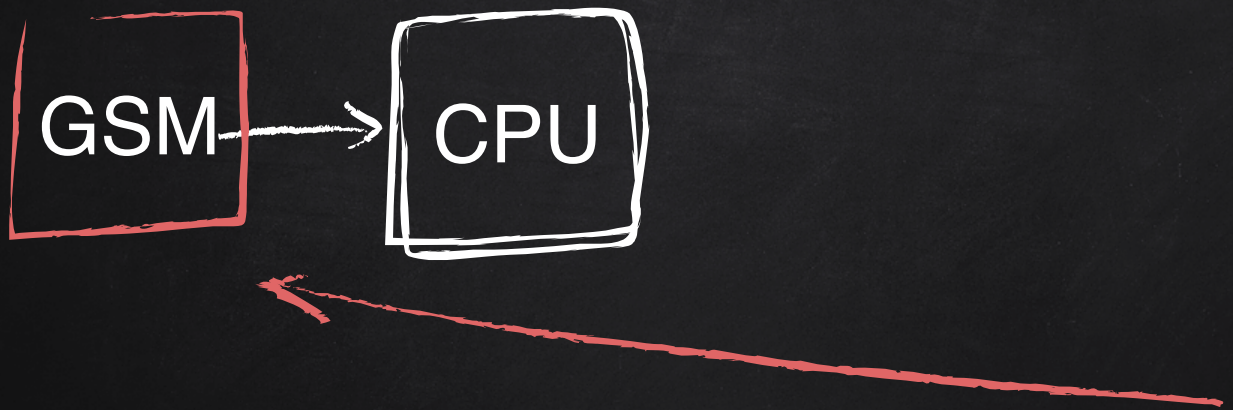
Attack Vectors



Local
Serial Parsers
Flash Parser
Code/Data

Remote
SMS
FTP

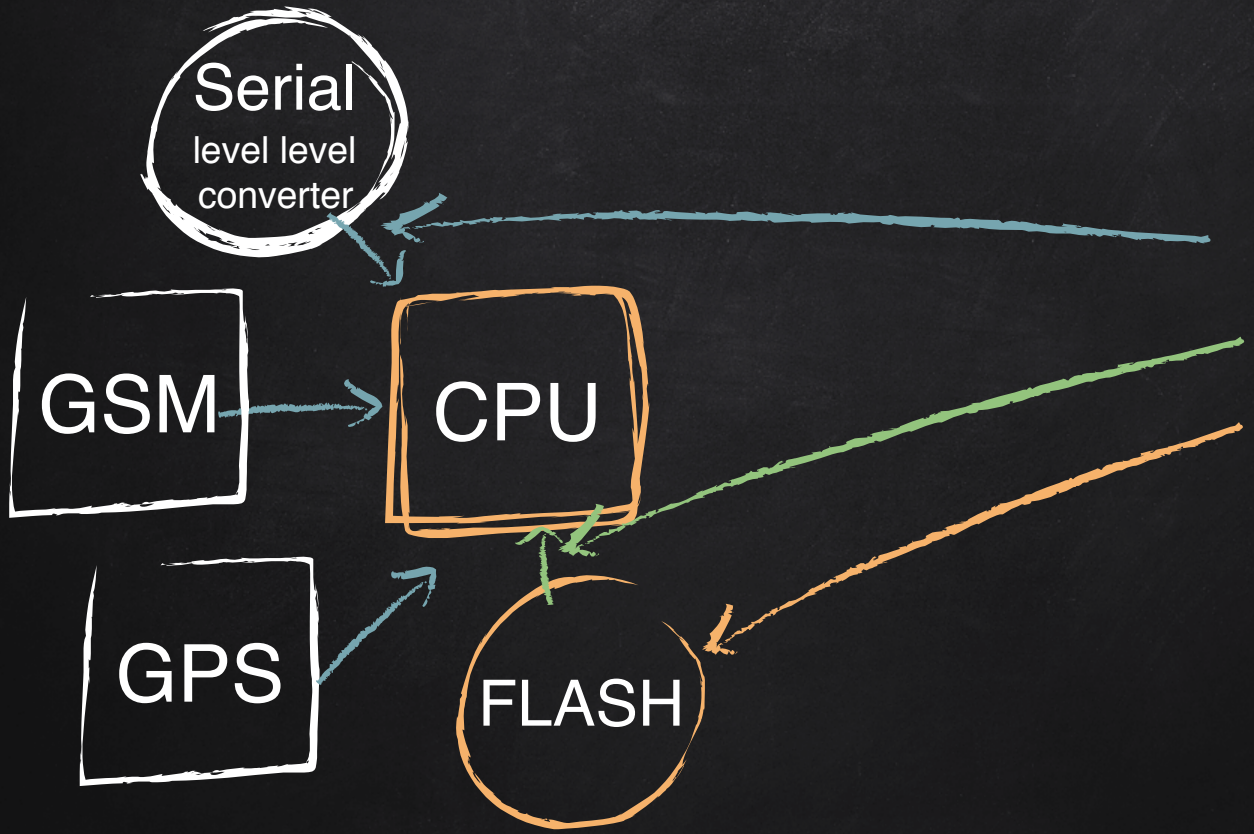
Attack Vectors



Local
Serial Parsers
Flash Parser
Code/Data

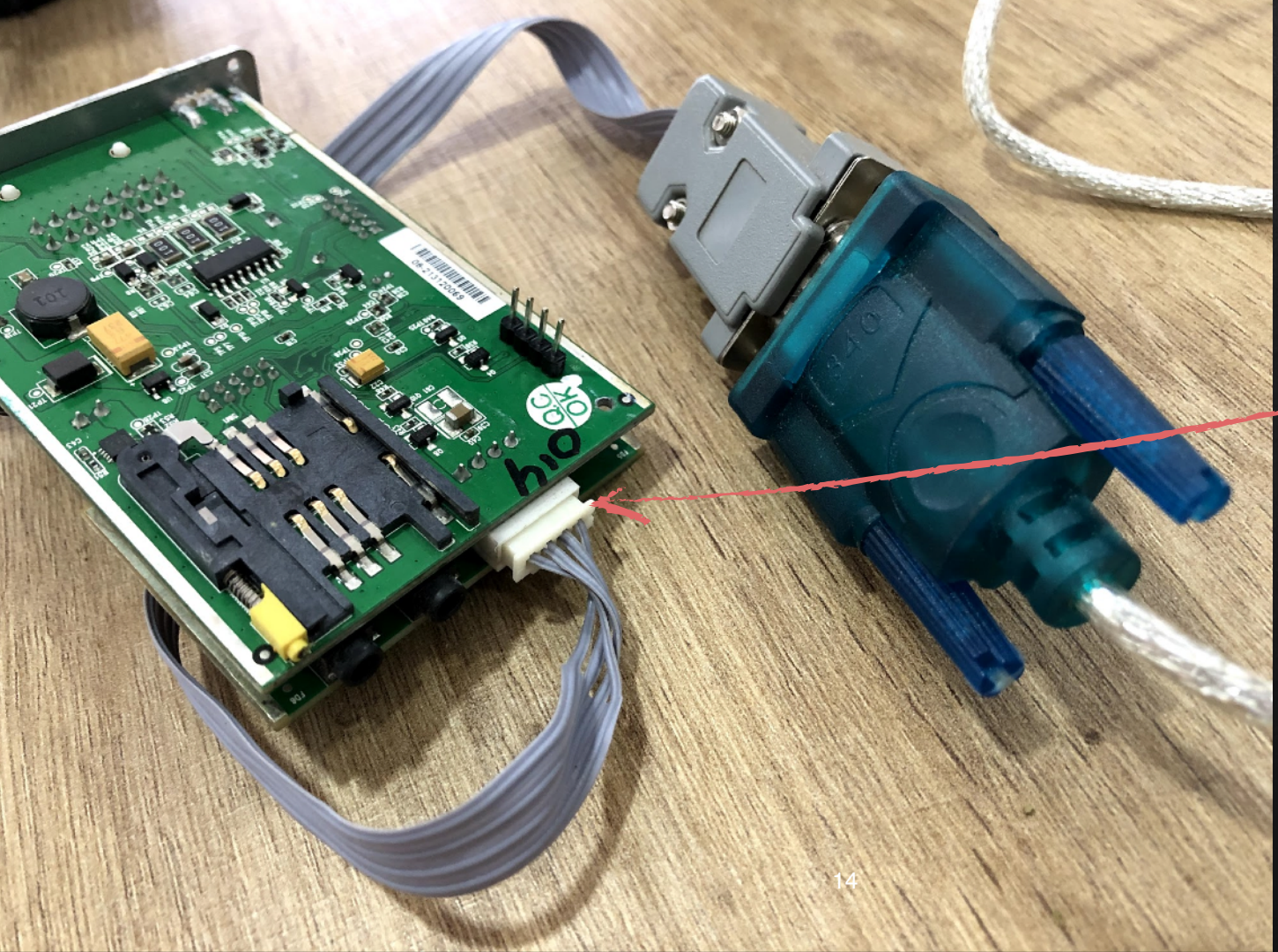
Remote
SMS,GPRS,
FTP

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

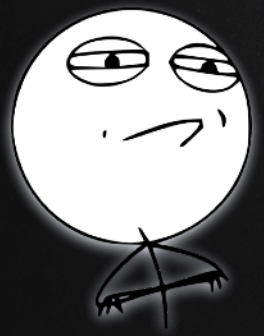
-> AT$GSM=?

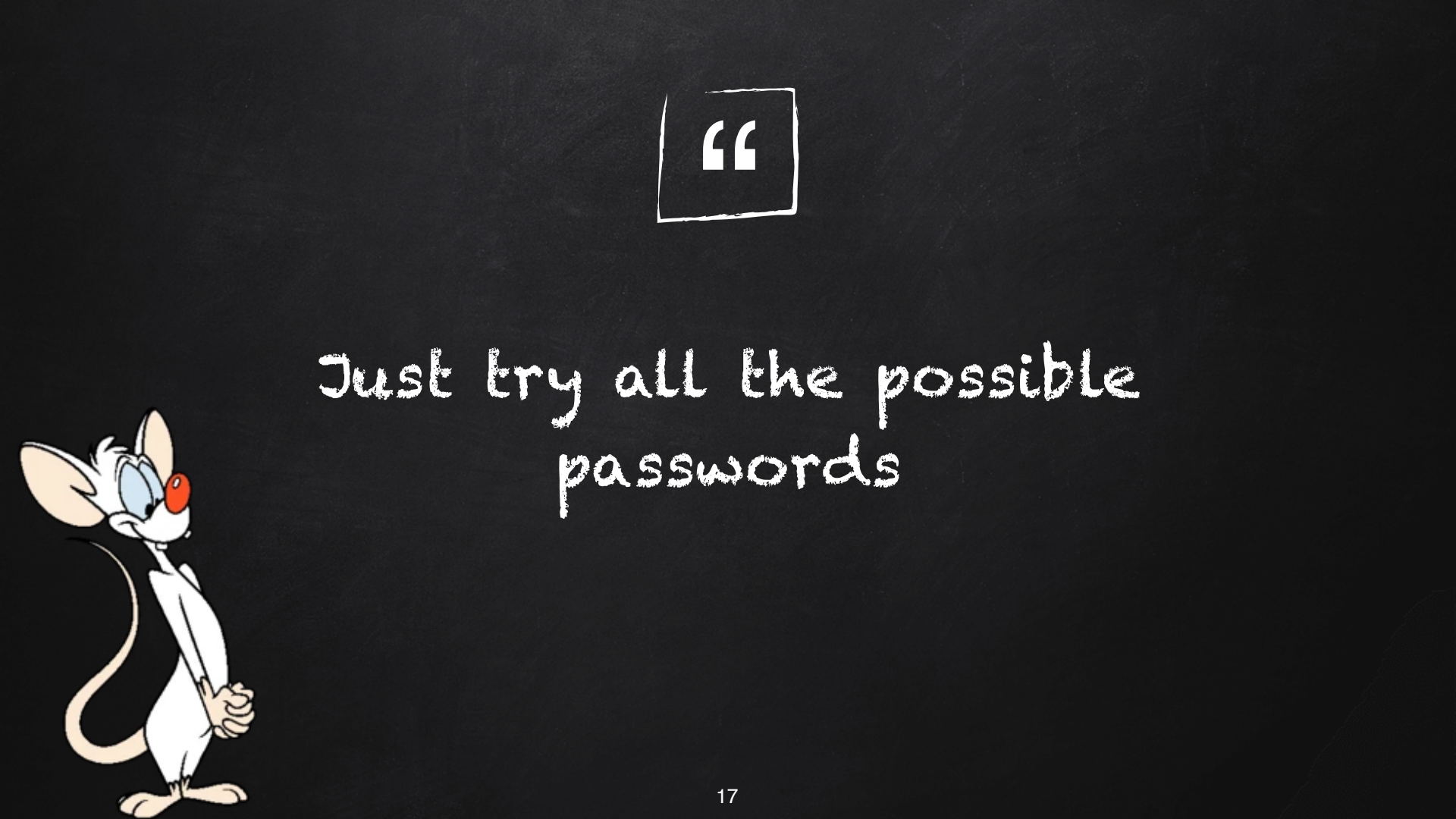
<- ERROR=104

-> AT$GPRS=?

<- ERROR=104

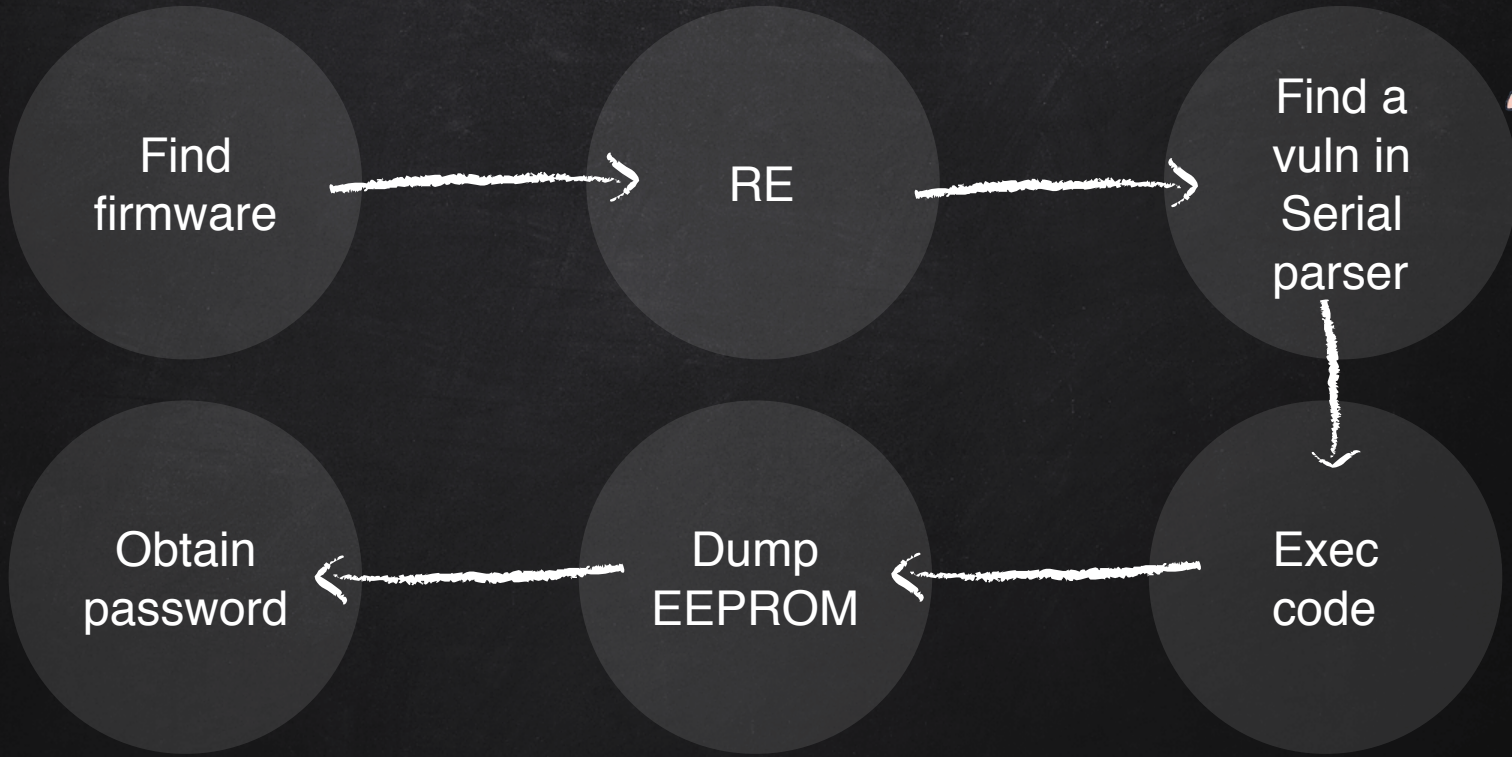
INVALID PASSWORD



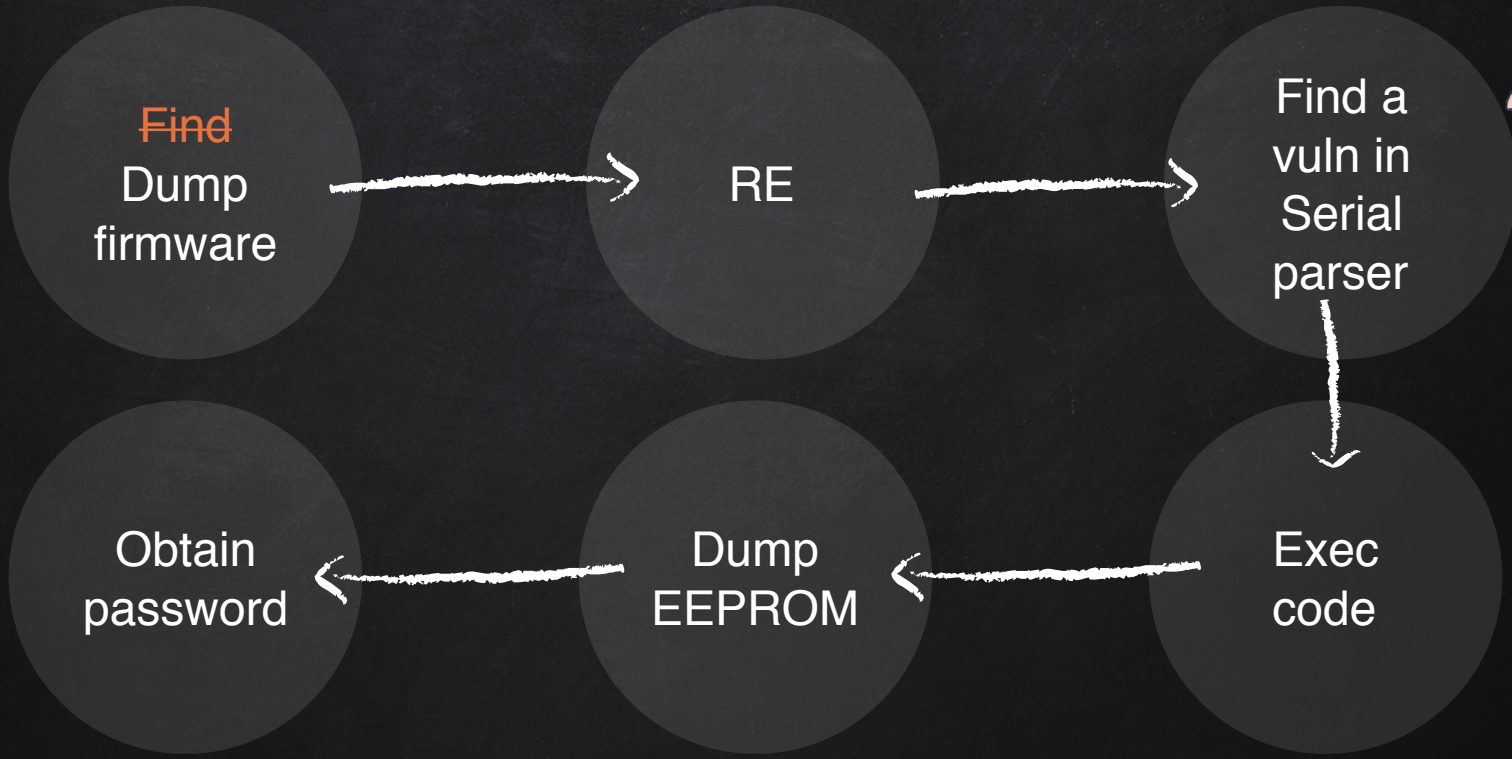

“
Just try all the possible passwords


“
Just try all the possible passwords
Failed

The plan

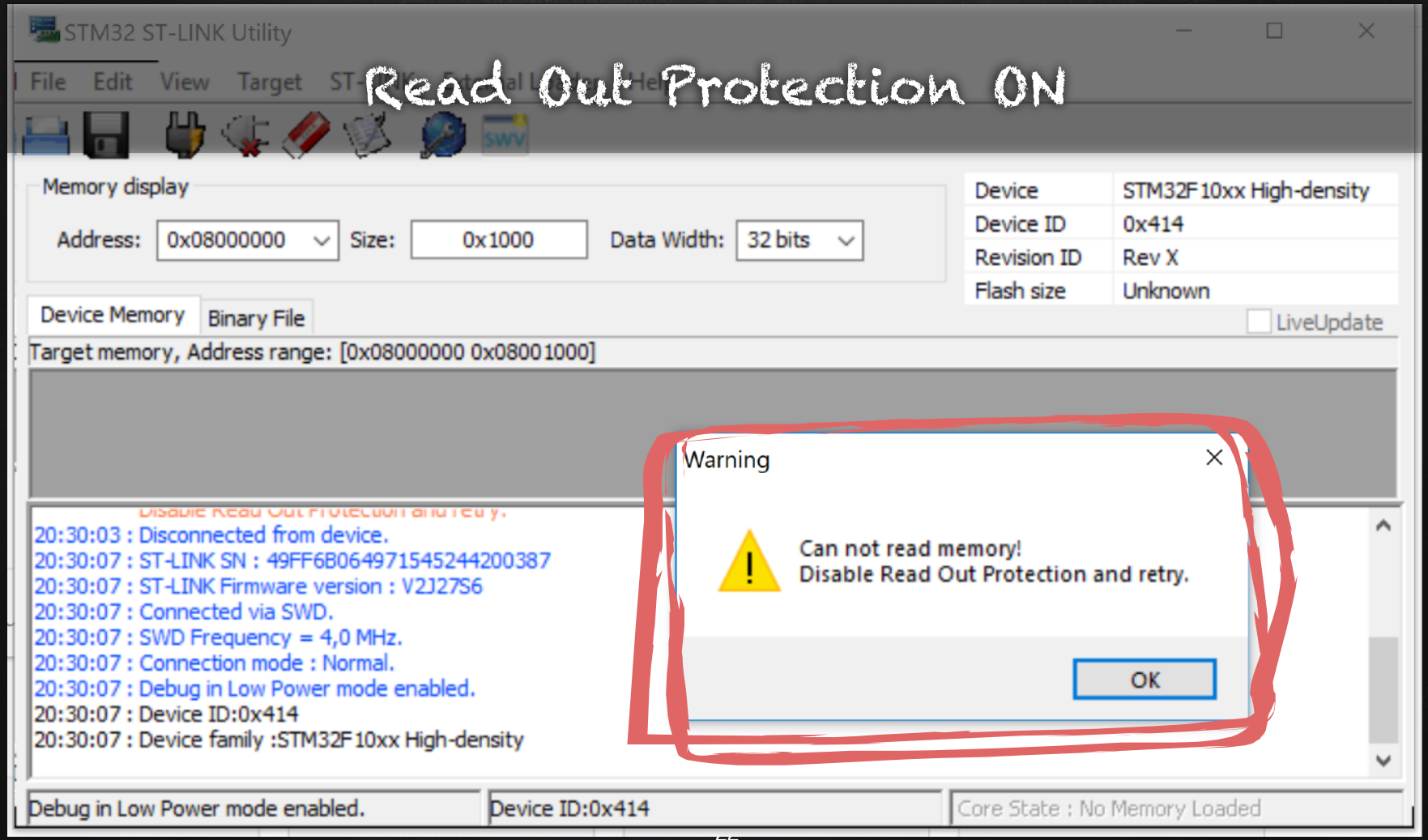

Find firmware
RE
Find a vuln in Serial parser
Exec code
Dump EEPROM
Obtain password

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
STM32 ST-LINK Utility
File Edit View Target
Memory display
Address: 0x08000000
Size: 0x1000
Data Width: 32 bits
Device STM32F10xx High-density
Device ID 0x414
Revision ID Rev X
Flash size Unknown
Device Memory
Binary File
LiveUpdate
Target memory, Address range: [0x08000000 0x08001000]
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.
OK
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!

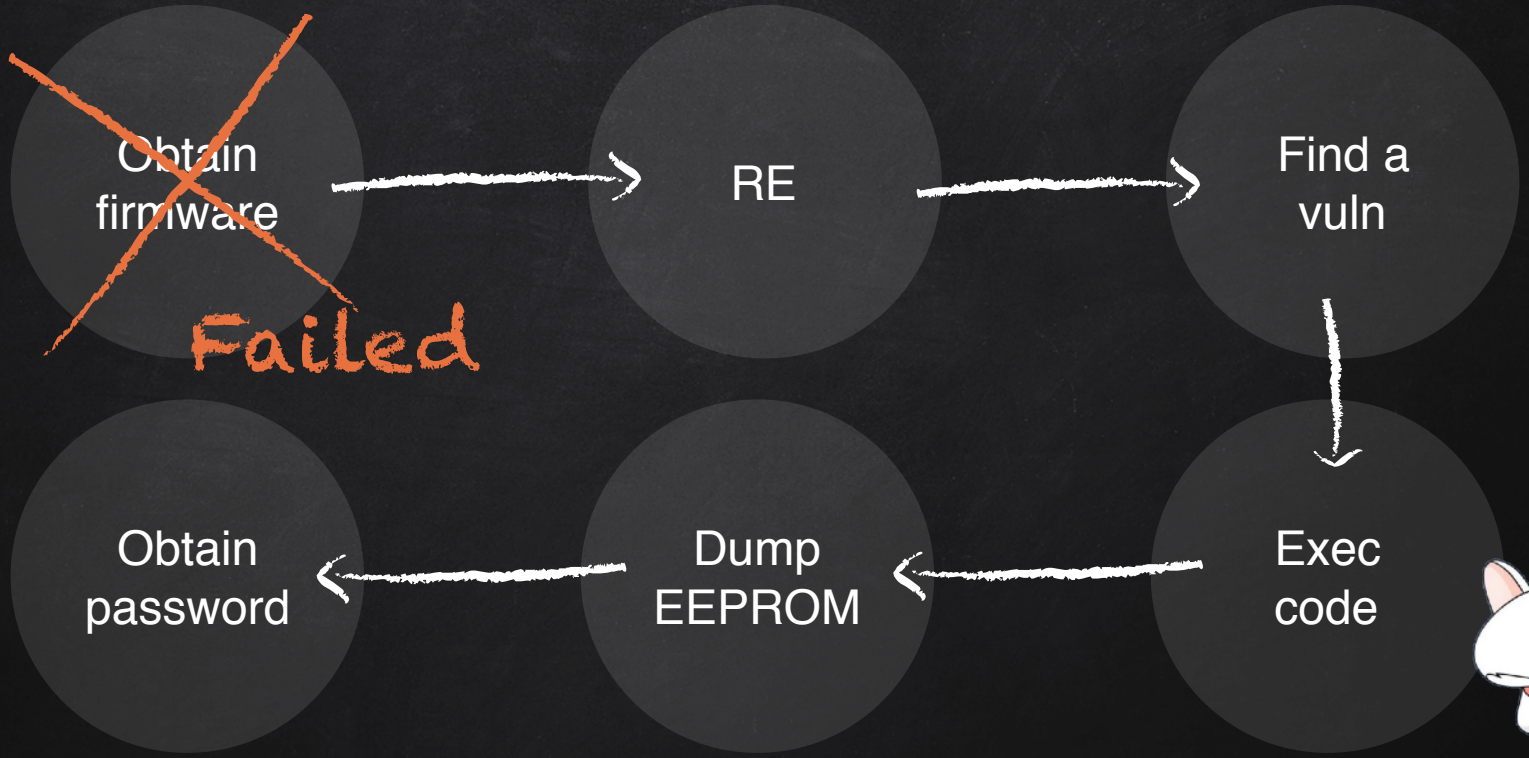
https://www.aisec.fraunhofer.de/content/dam/aisec/ResearchExcellence/woot17-paper-obermaier.pdf

Flash Readout Protection

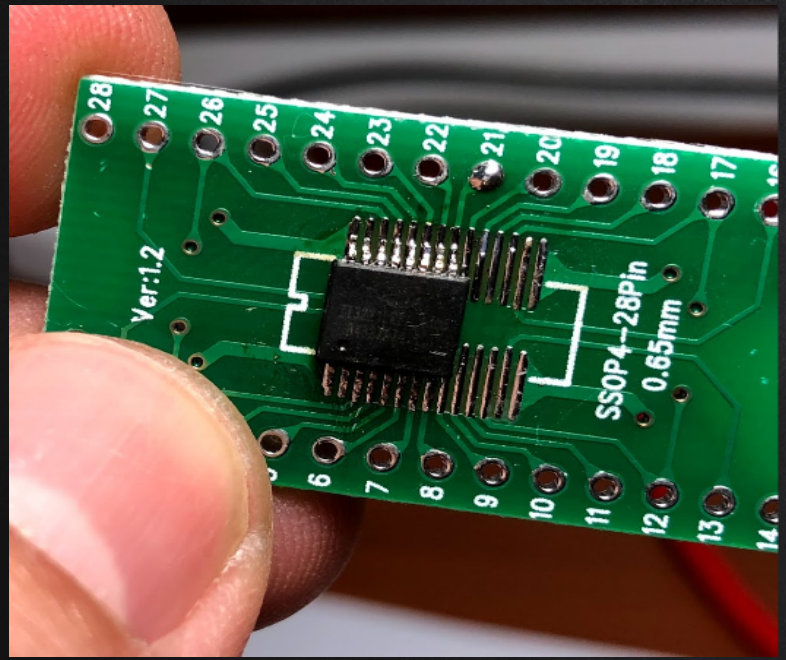
Level 1: Debug interfaces enabled, flash access locked

- ✘ 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

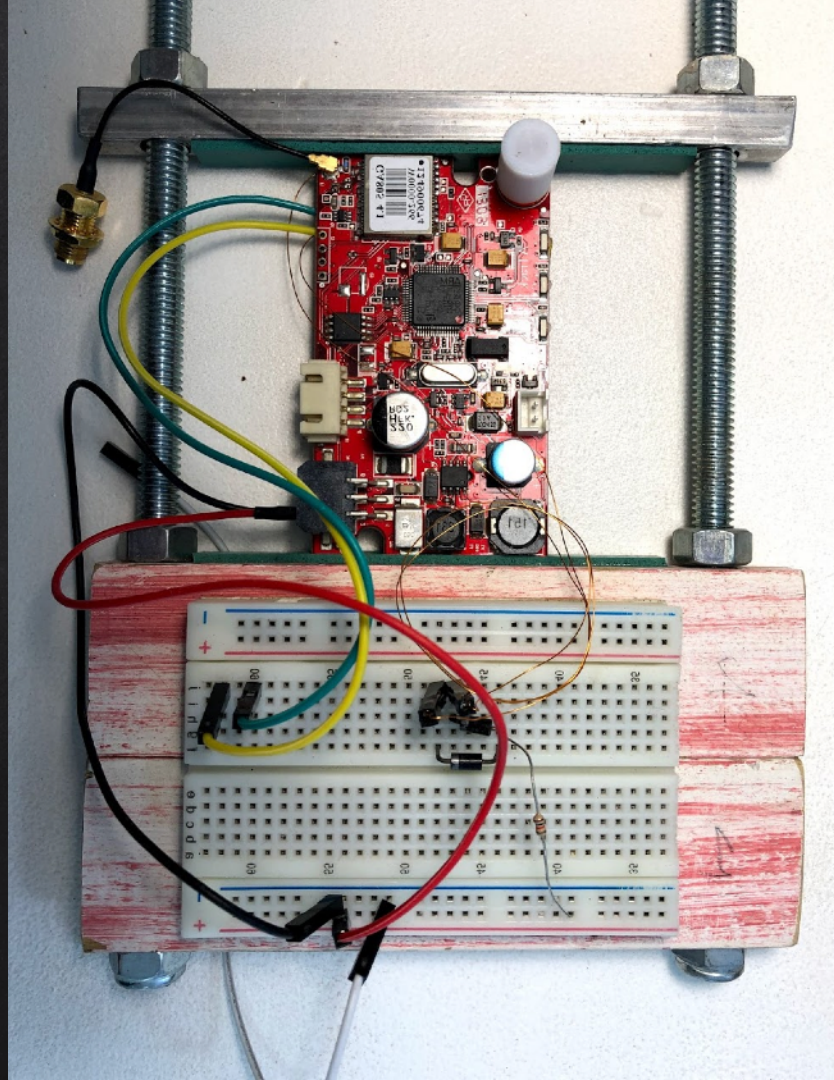
Test your bruteforcer!

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

:(

Going wild \o/

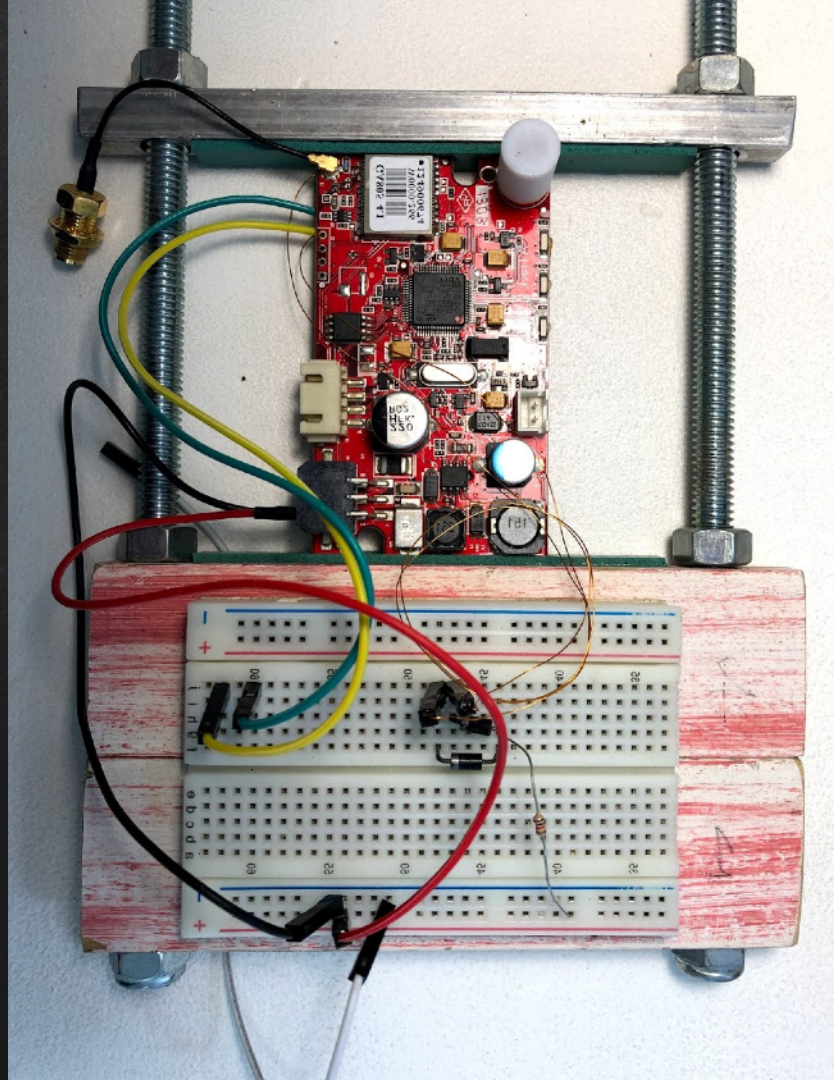
- Fuzzed Serial
- Fuzzed FOTA FTP via GPRS
- TAP into GSM-IC Serial
- Intention toFuzz GSM-IC Serial
- Etc, etc...



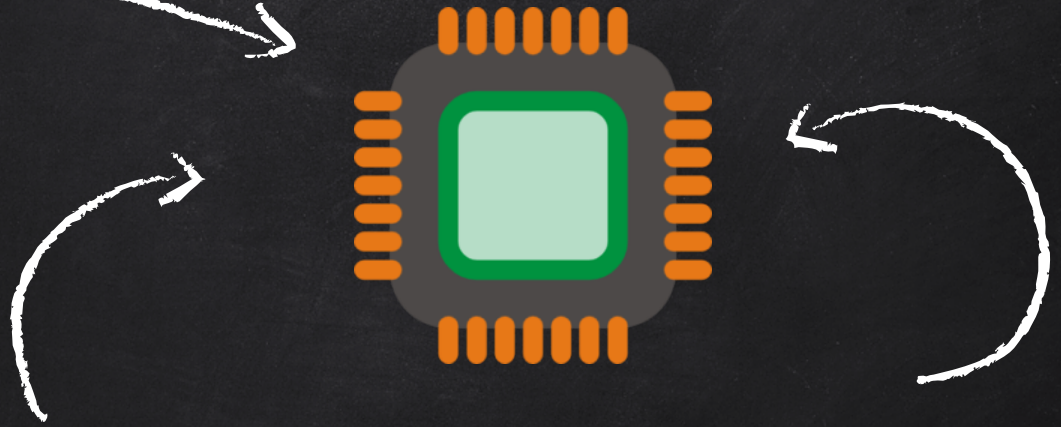
Going wild \o/

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

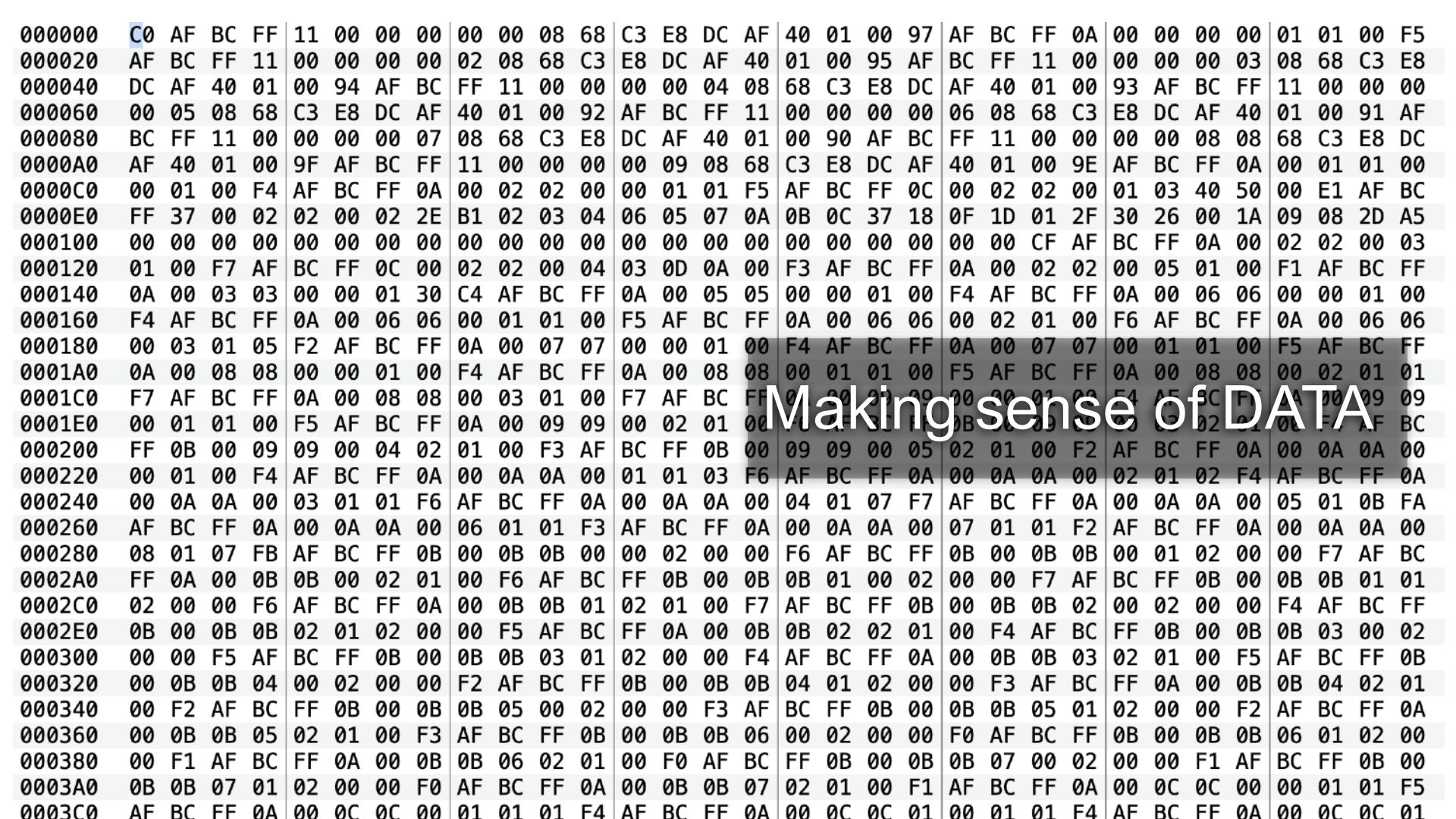
Failed Again



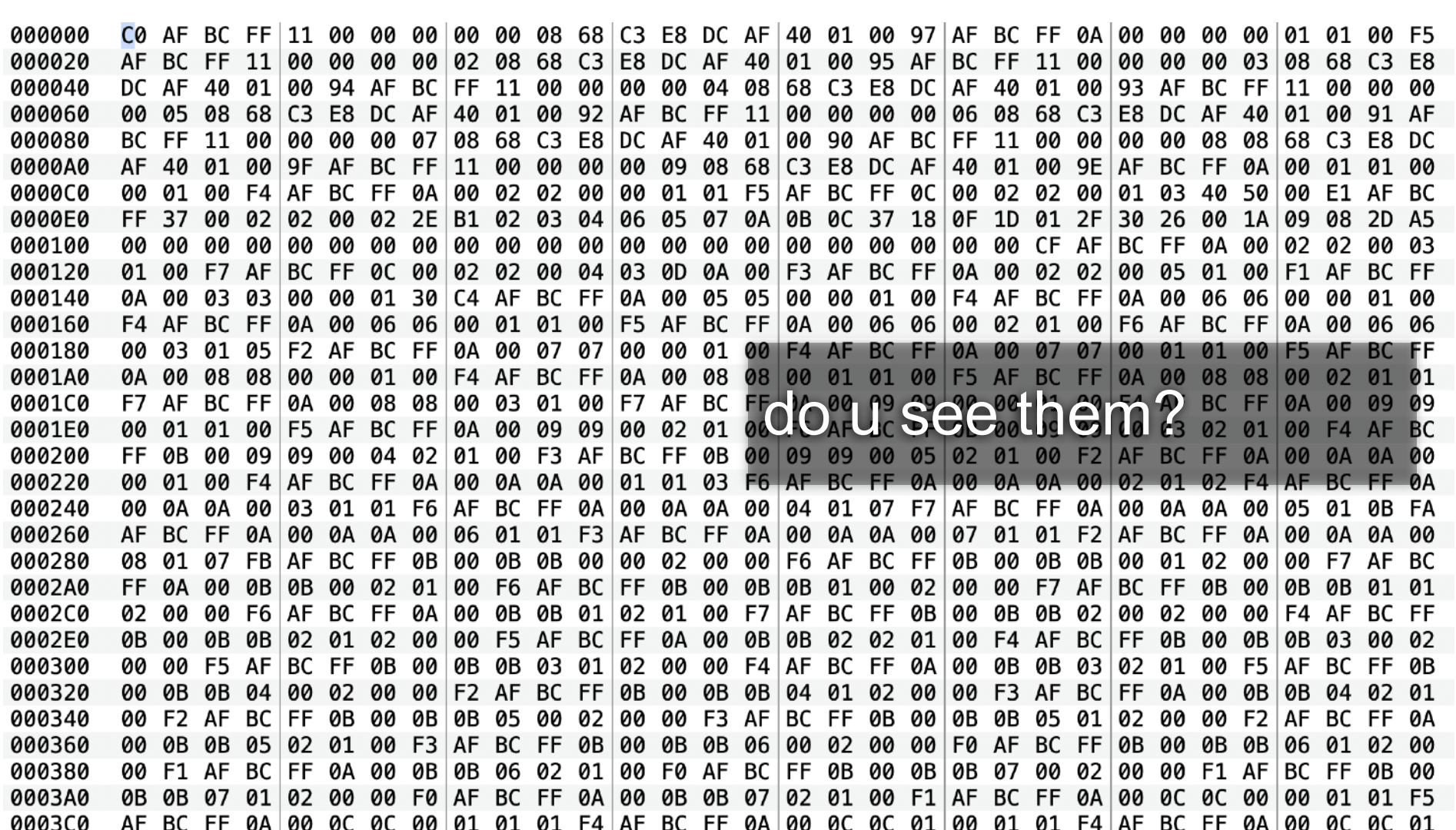
Idea

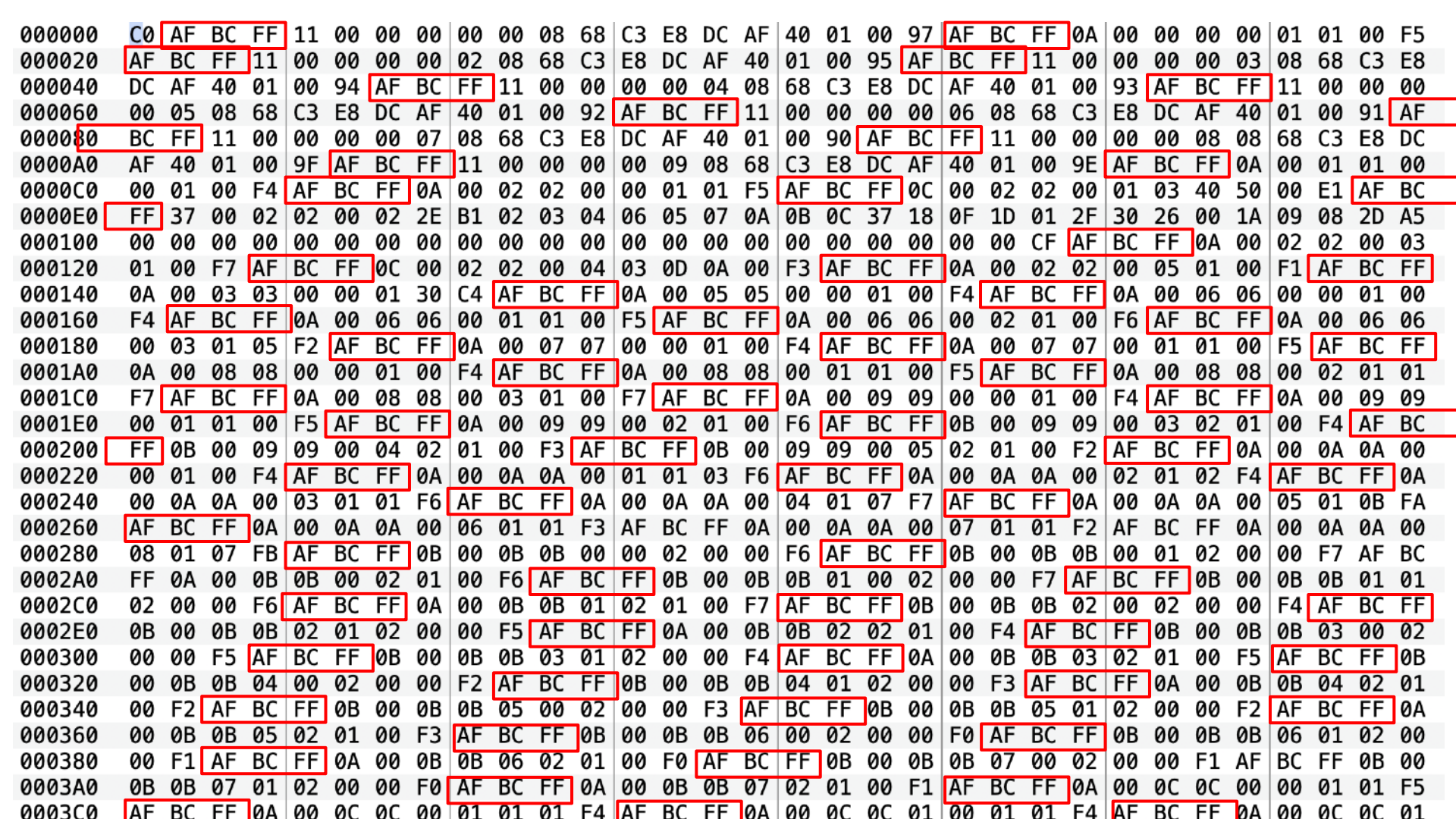


What (secrets) does the flash store?


Making sense of DATA


I see data patterns


do u see them?



```
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
```

AF BC FF | 0A | 8 Bytes

DATA?

Size(DATA+2)?

Header?

The breakthrough: Differential analysis

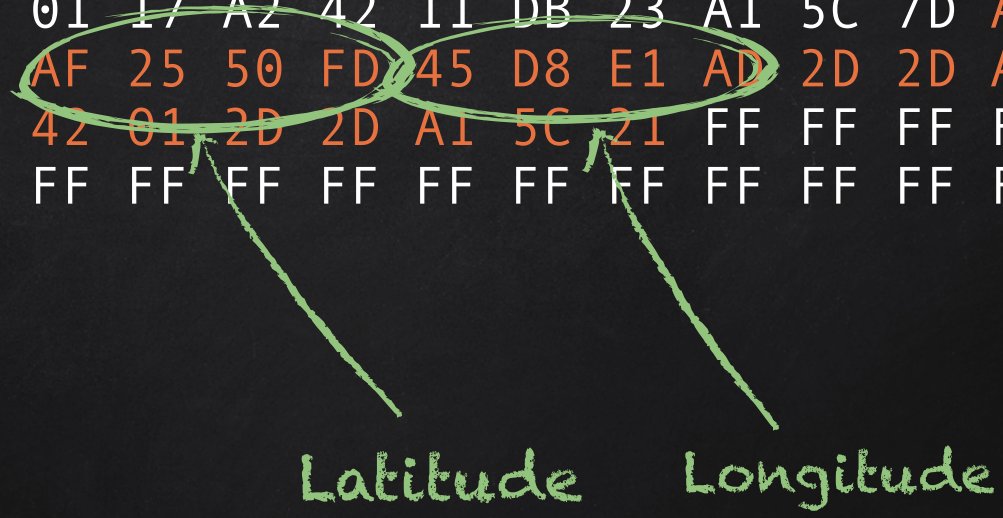
[disolder, dump, resolder, run, dump again] x N; Then compare

```
 […]
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
 […]
```

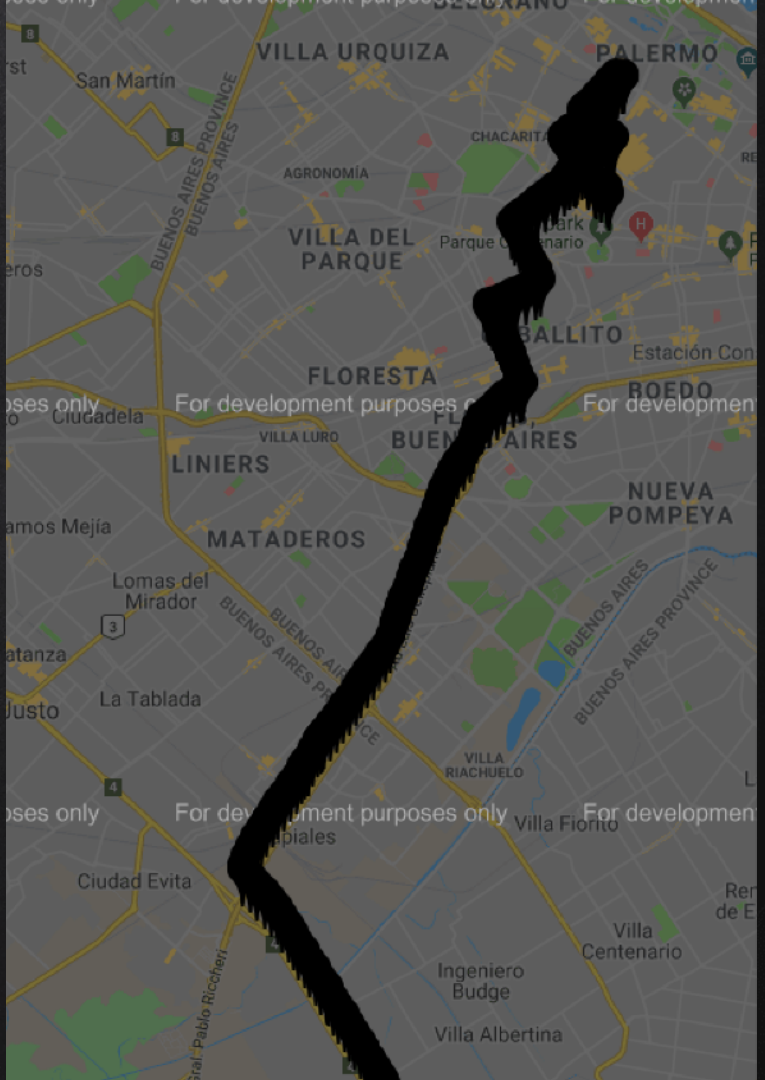
The breakthrough: Differential analysis

[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
[…]
```



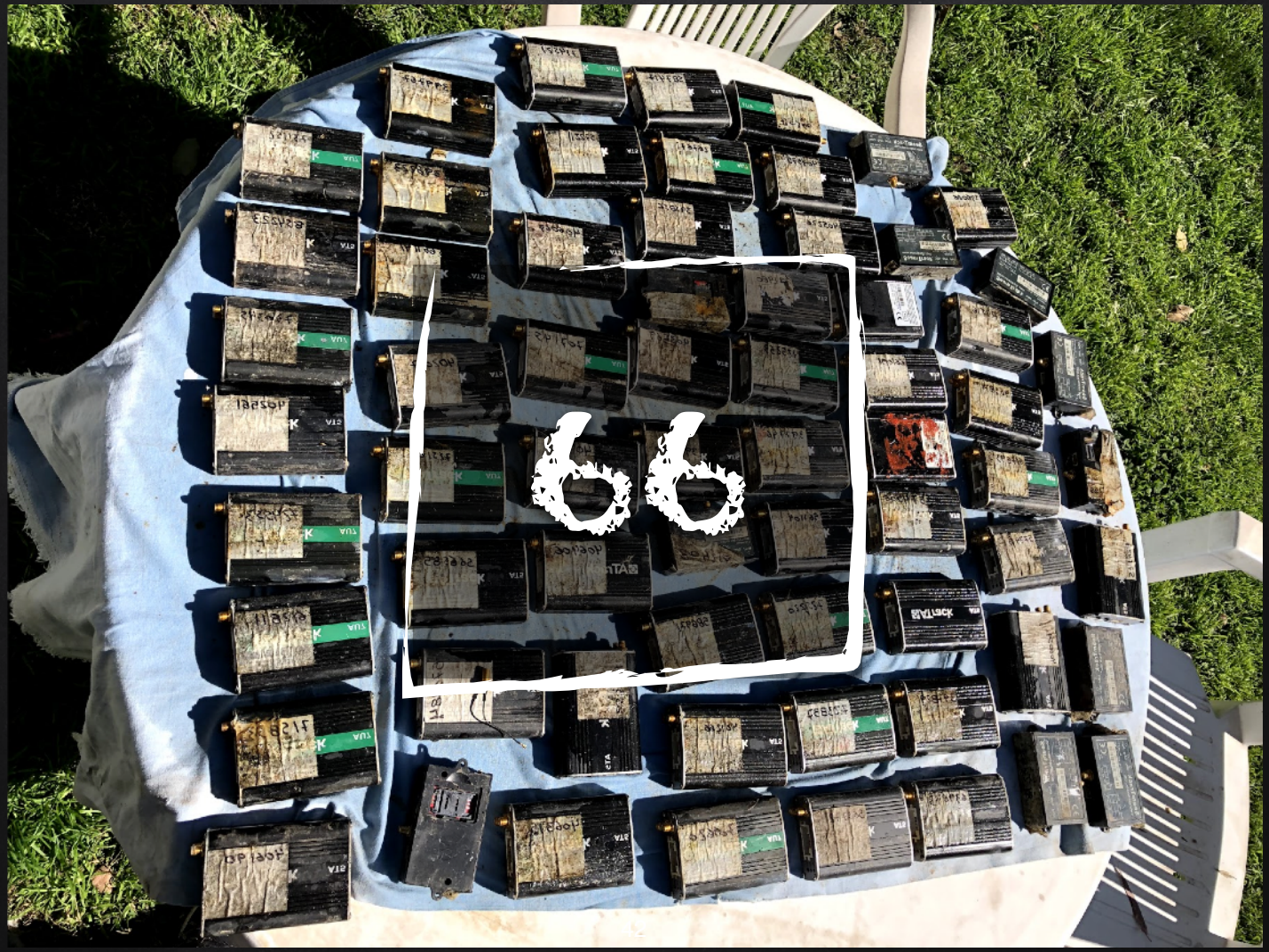
First results!



BUY 'EM ALL

This slide is dedicated to Marie Kondo


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


66

528

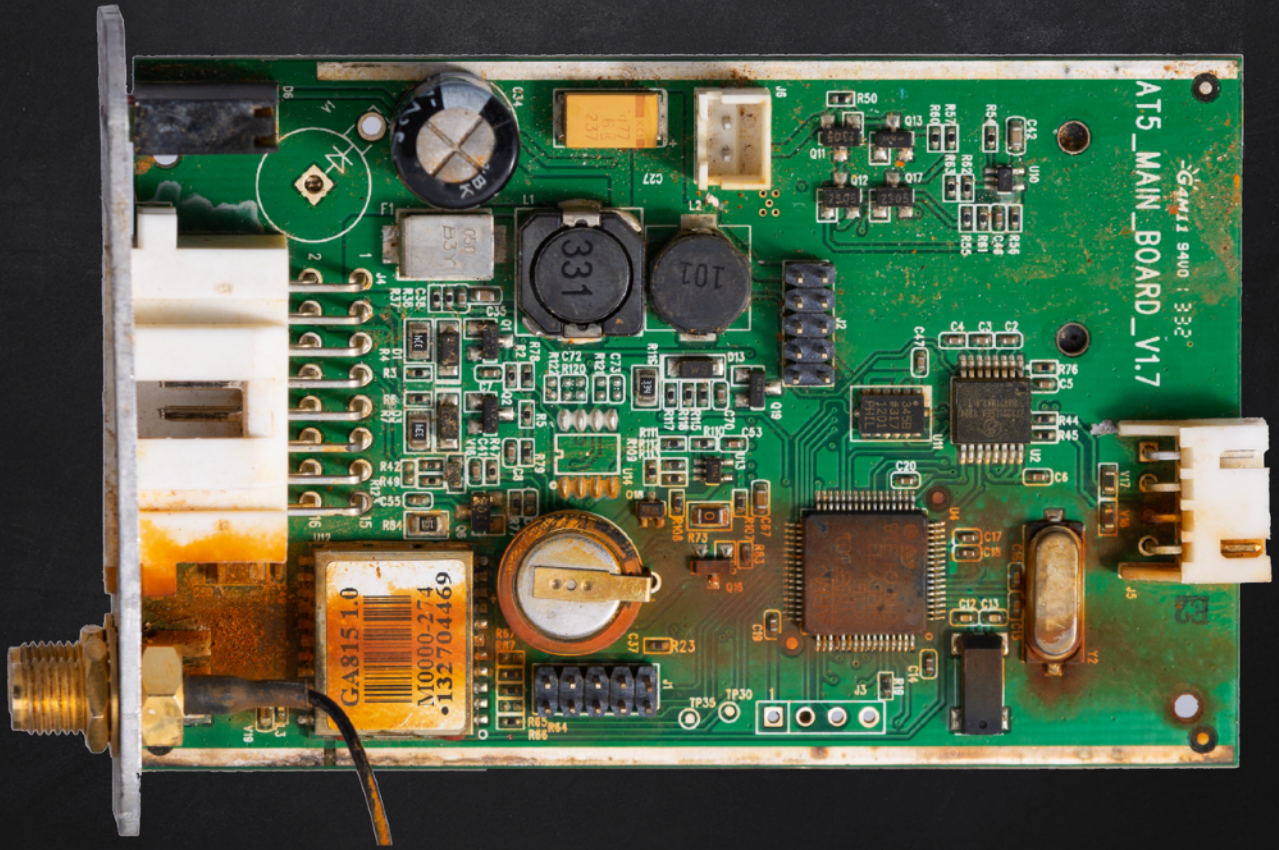
Screws removed

120

Boards brushed

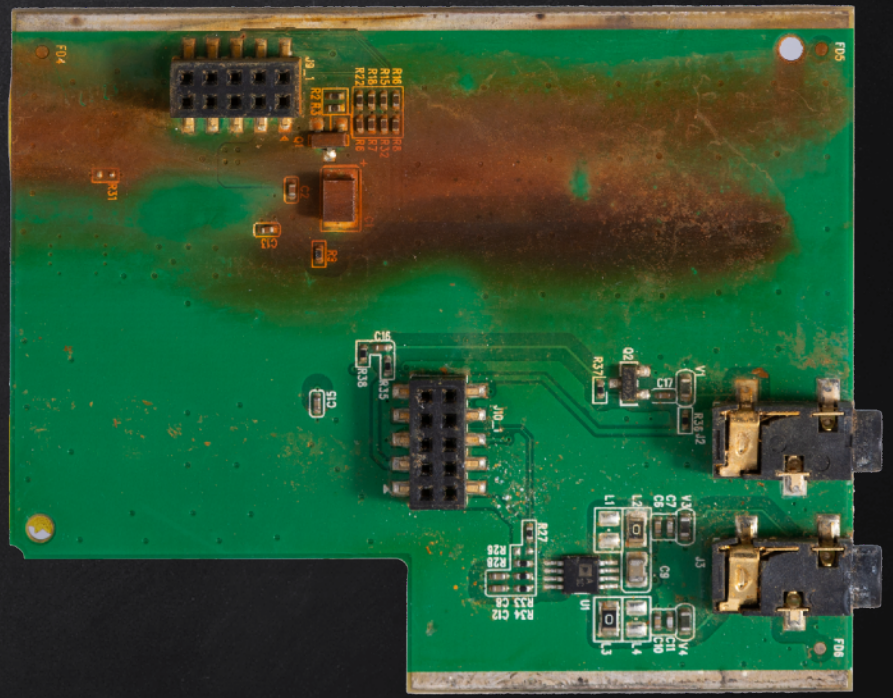
66

Cases cleaned



Some were in really bad shape

(pics taken after initial cleaning)



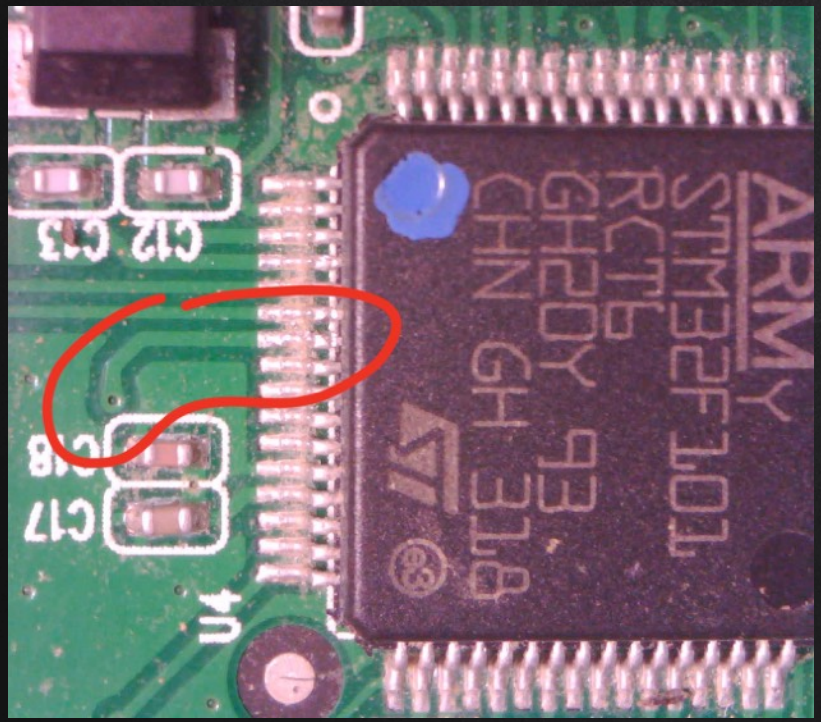
Some were in really bad shape

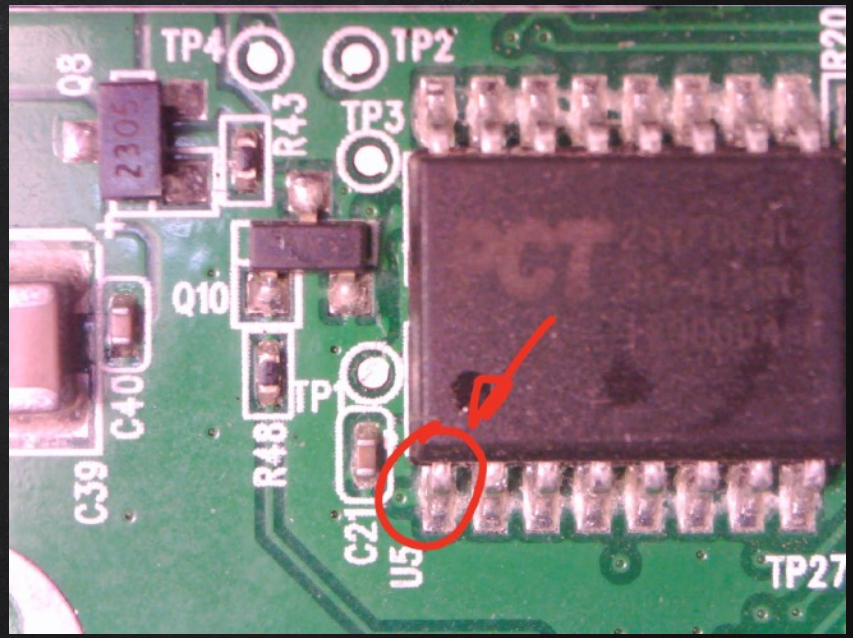
(pics taken after initial cleaning)

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?



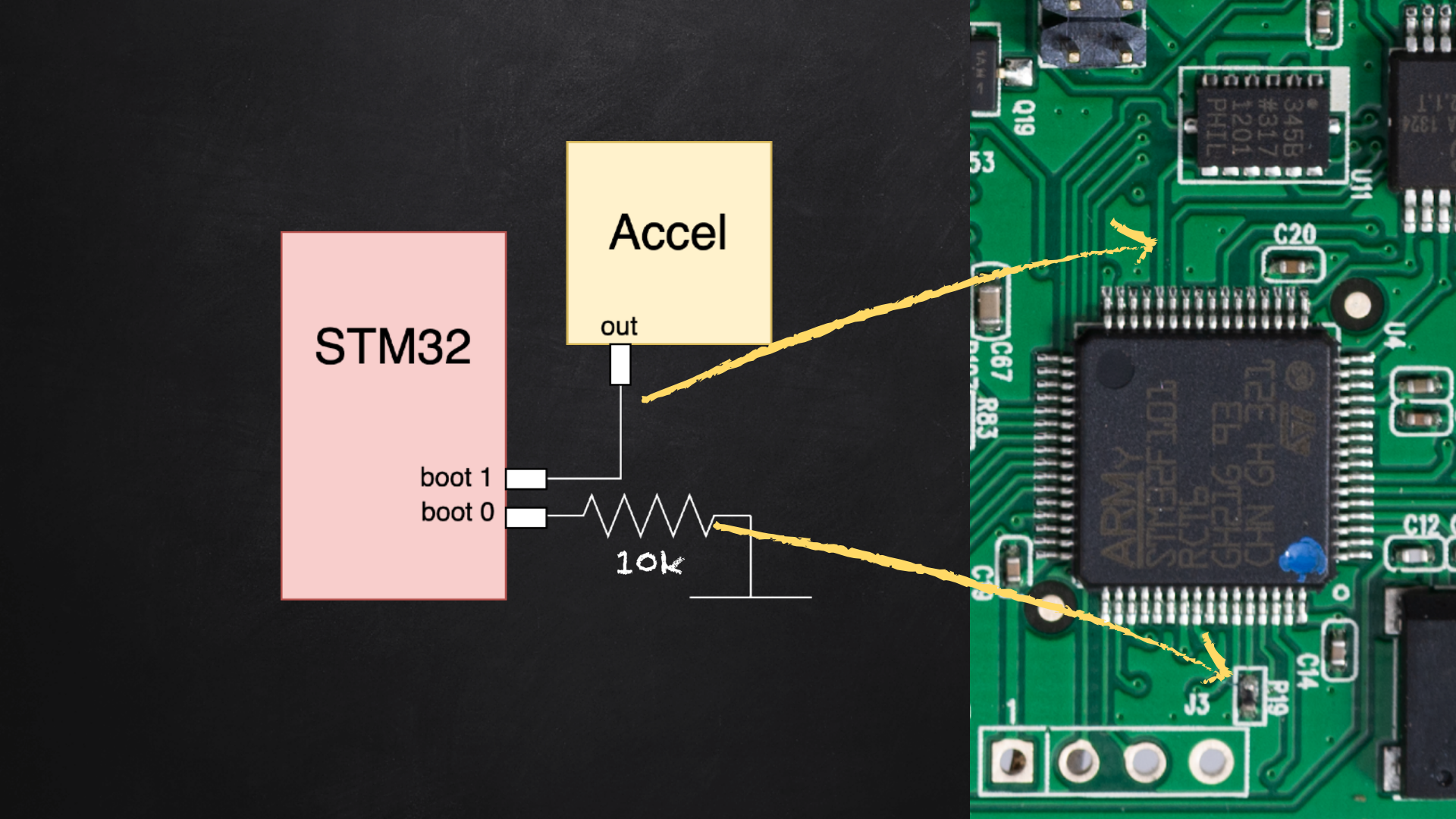


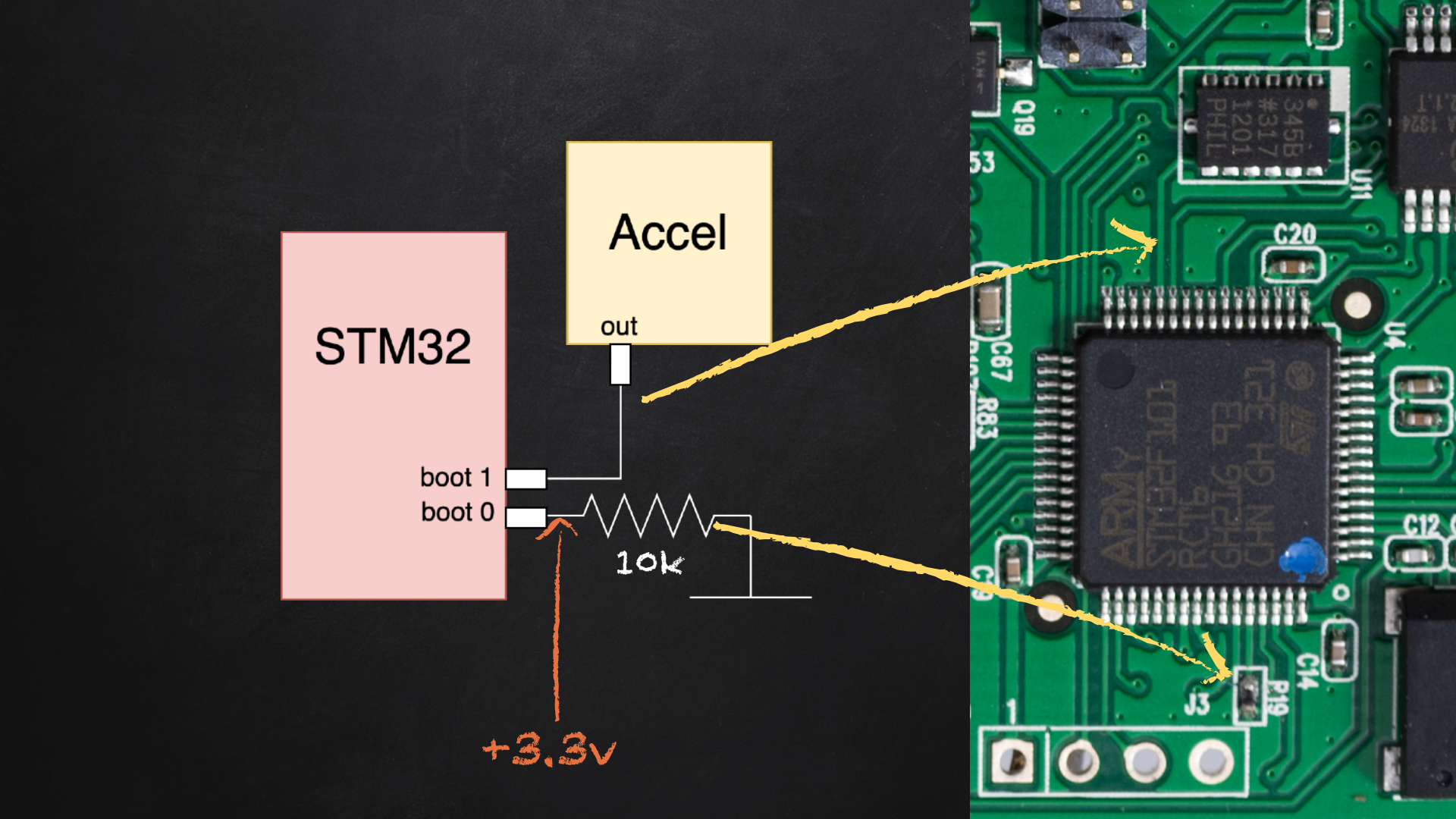
also connected to the FLASH reset :(

What about boot modes?

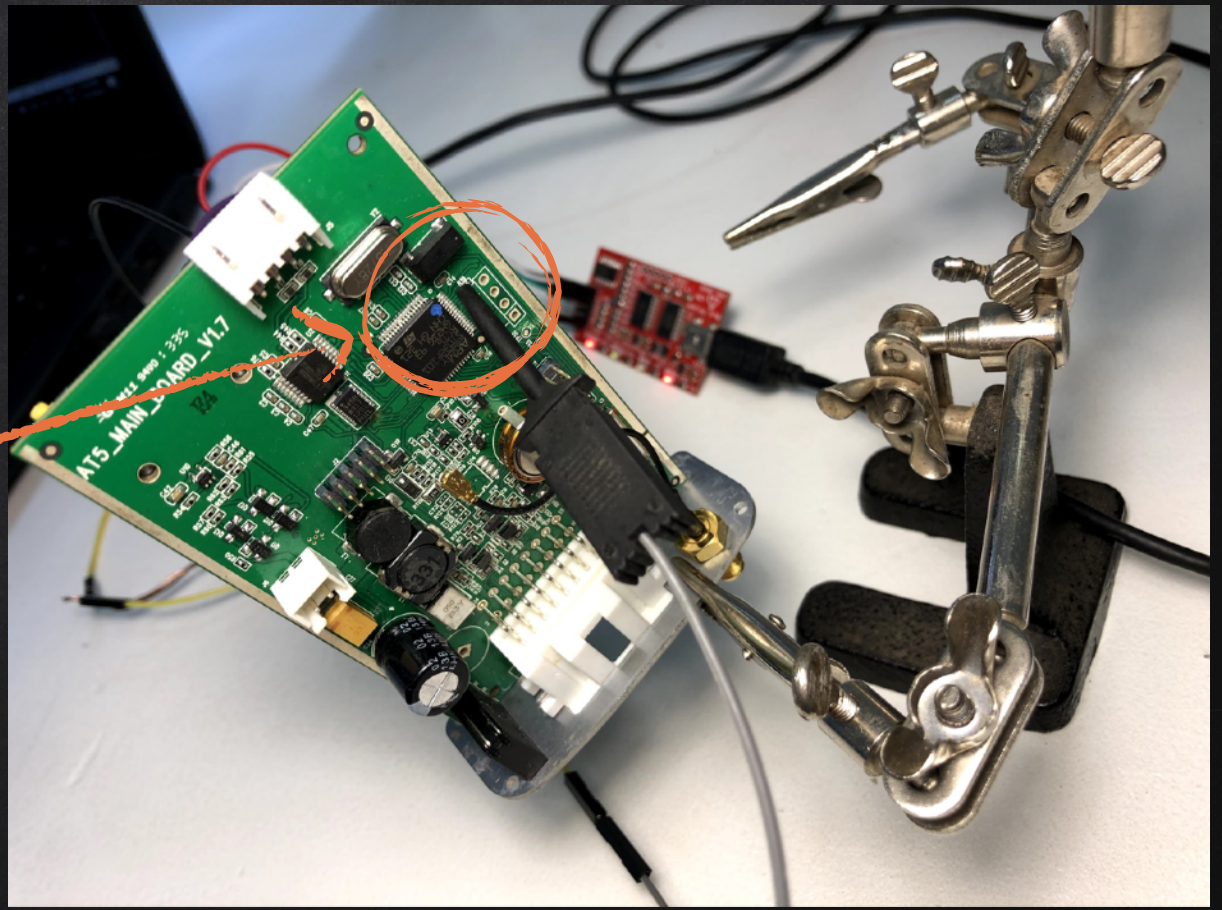
Boot 1	Boot 0	Mode
X	0	(internal) User Flash
0	1	System memory
1	1	Embedded SMRAM

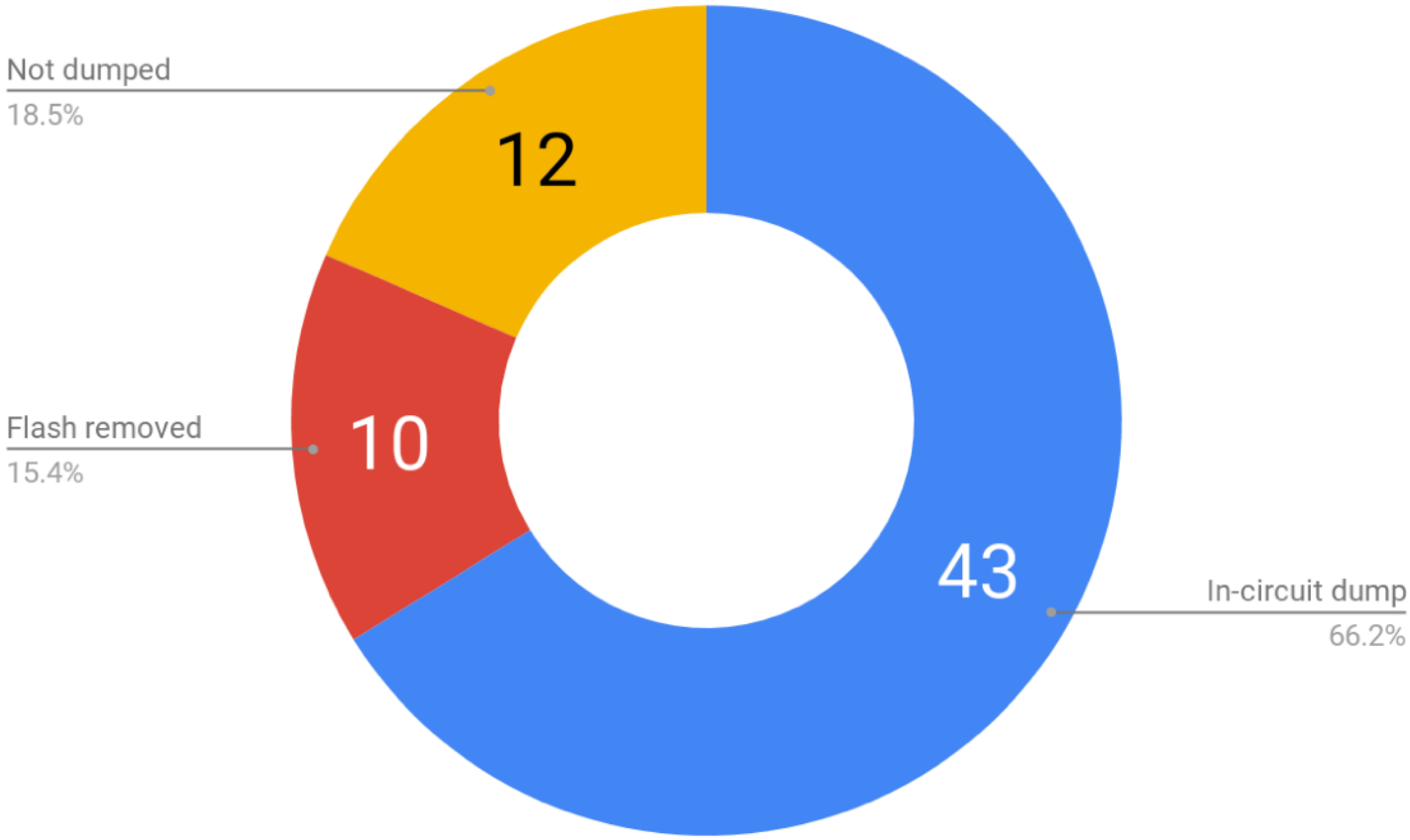
don't use the external FLASH


Accel
out
STM32
boot 1
boot 0
10k


Accel
out
STM32
boot 1
boot 0
10k
+3.3v

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

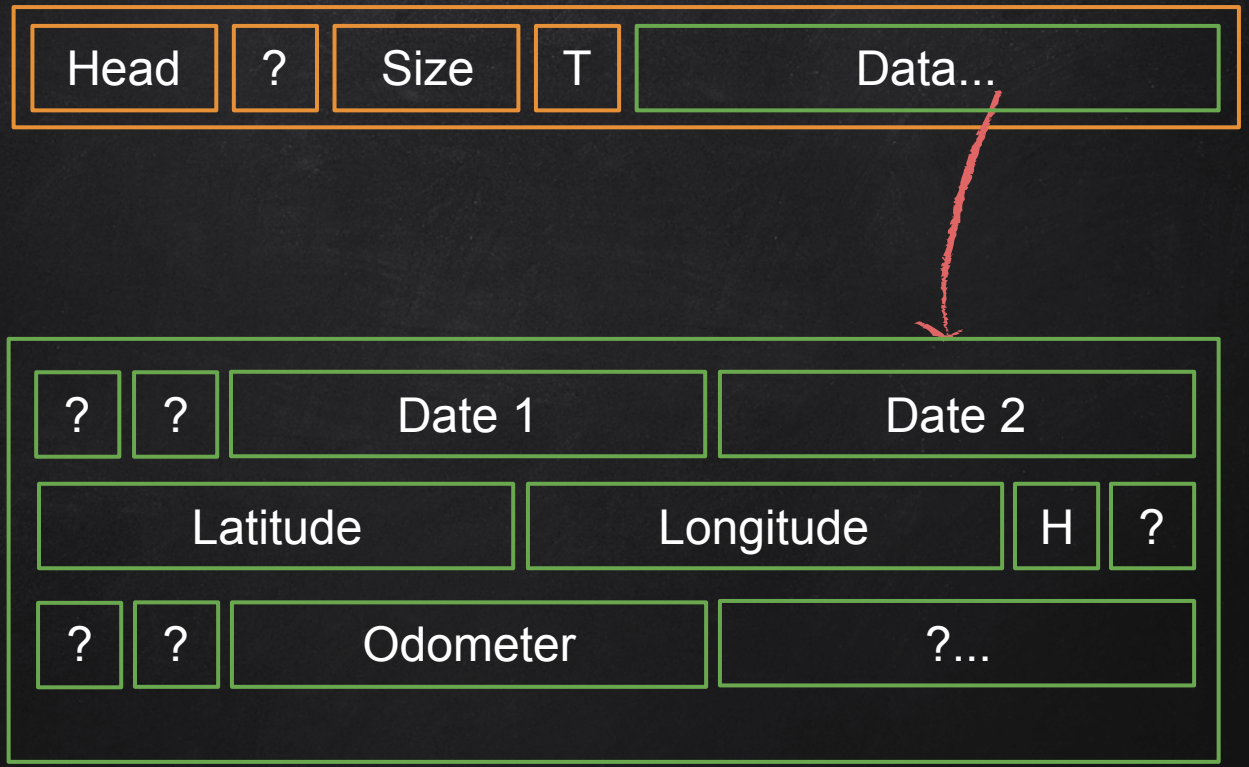
Some w/fixed offsets

Start byte

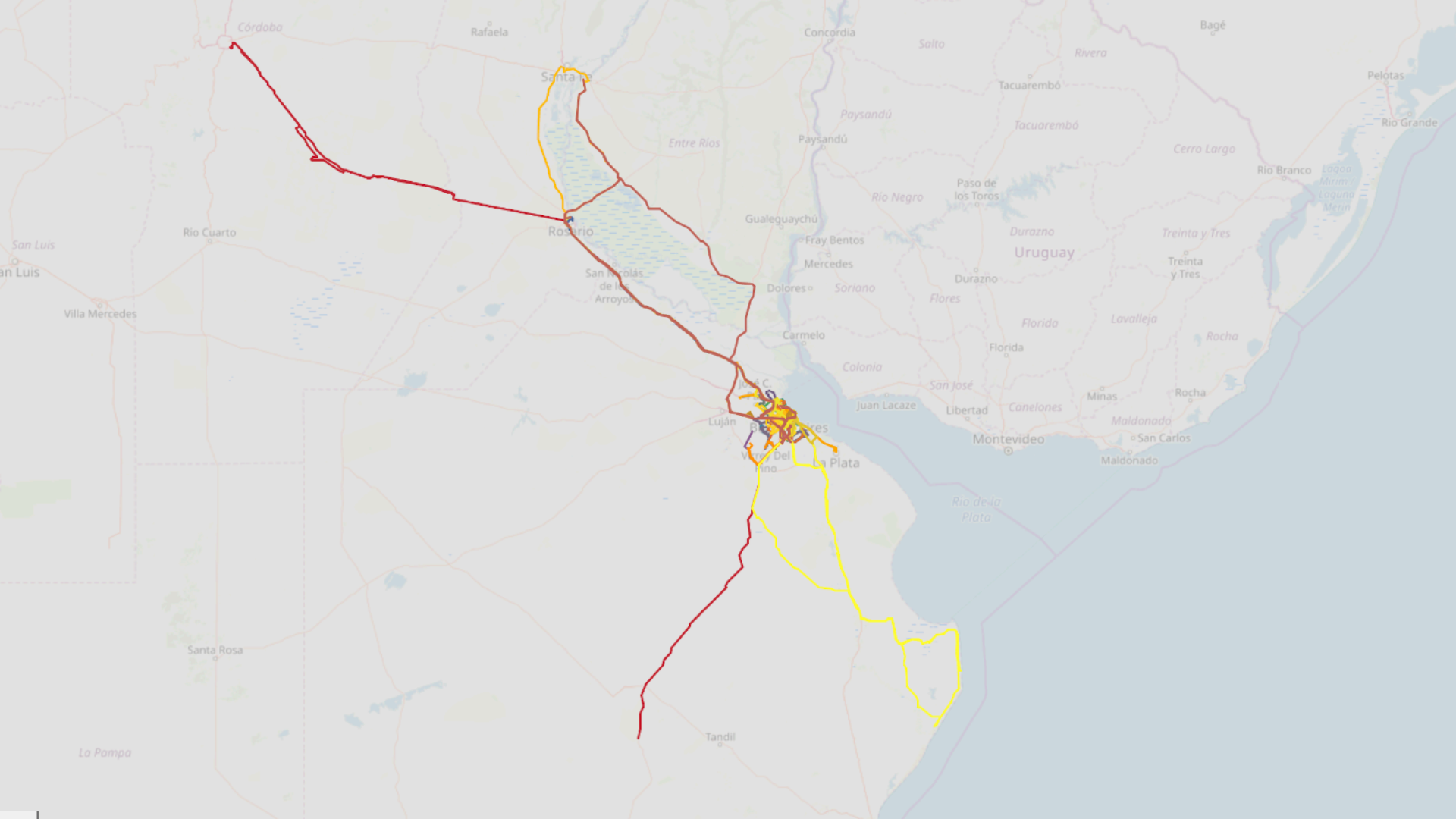
Padding

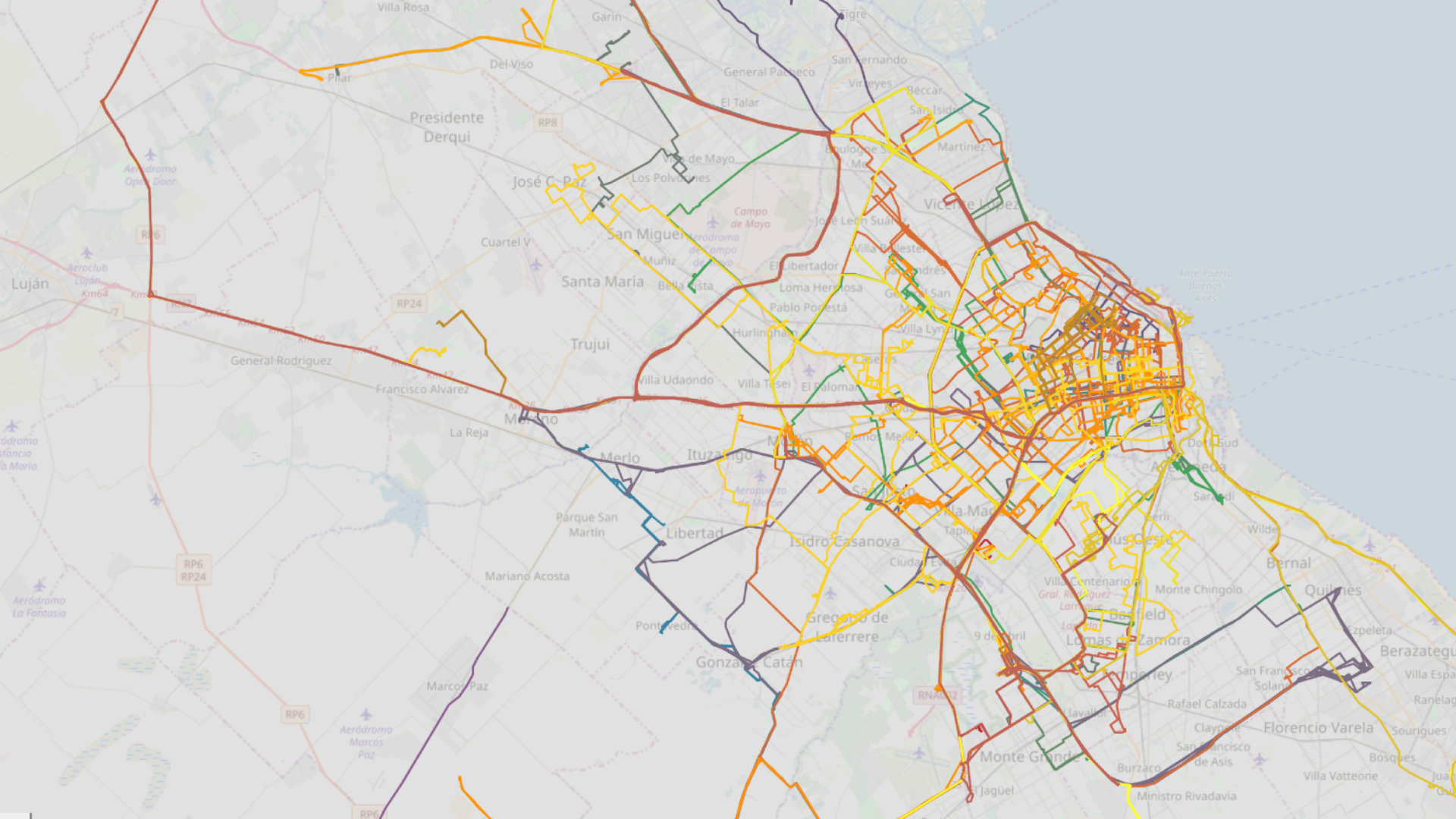
Data records

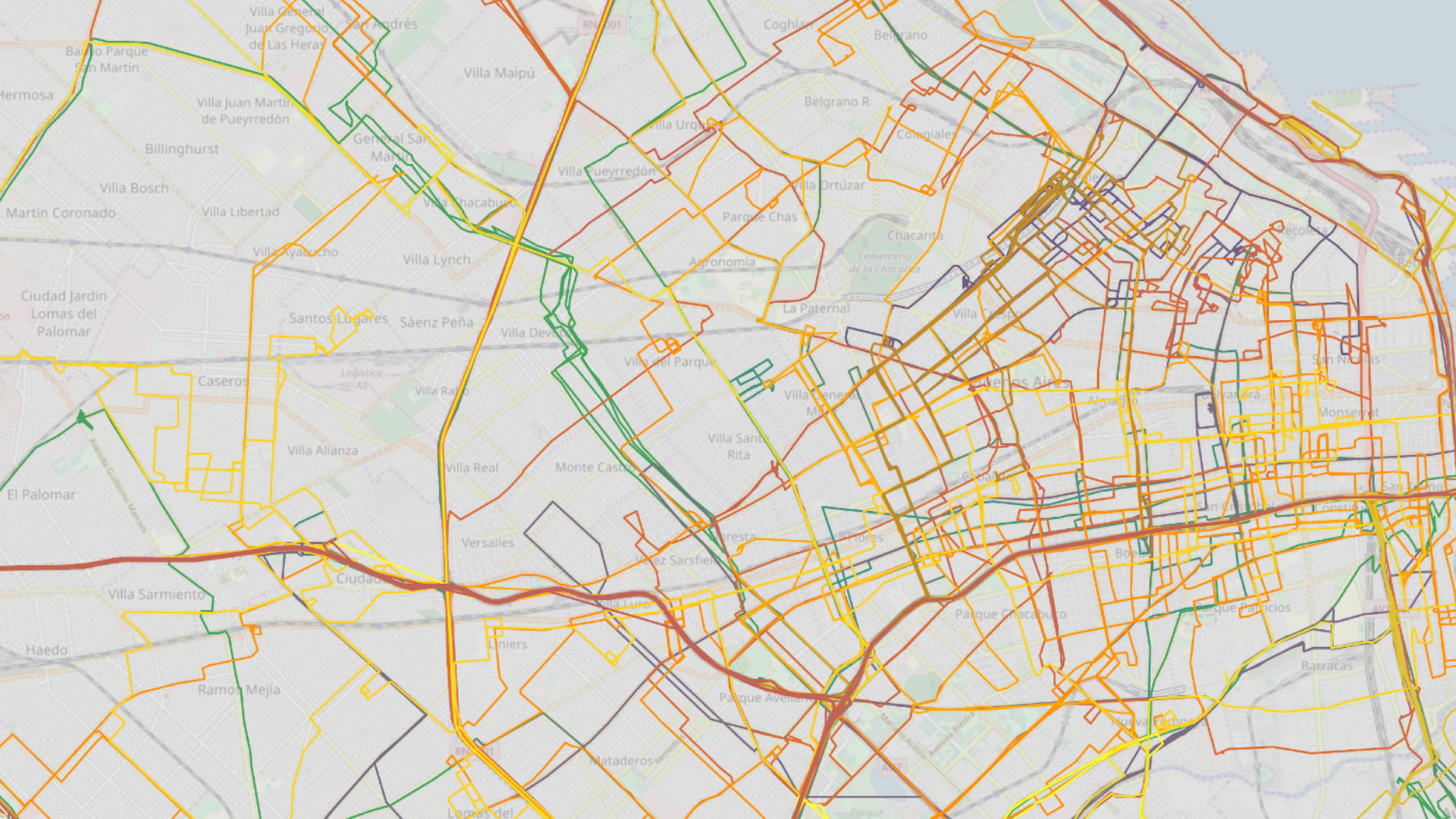
Data record



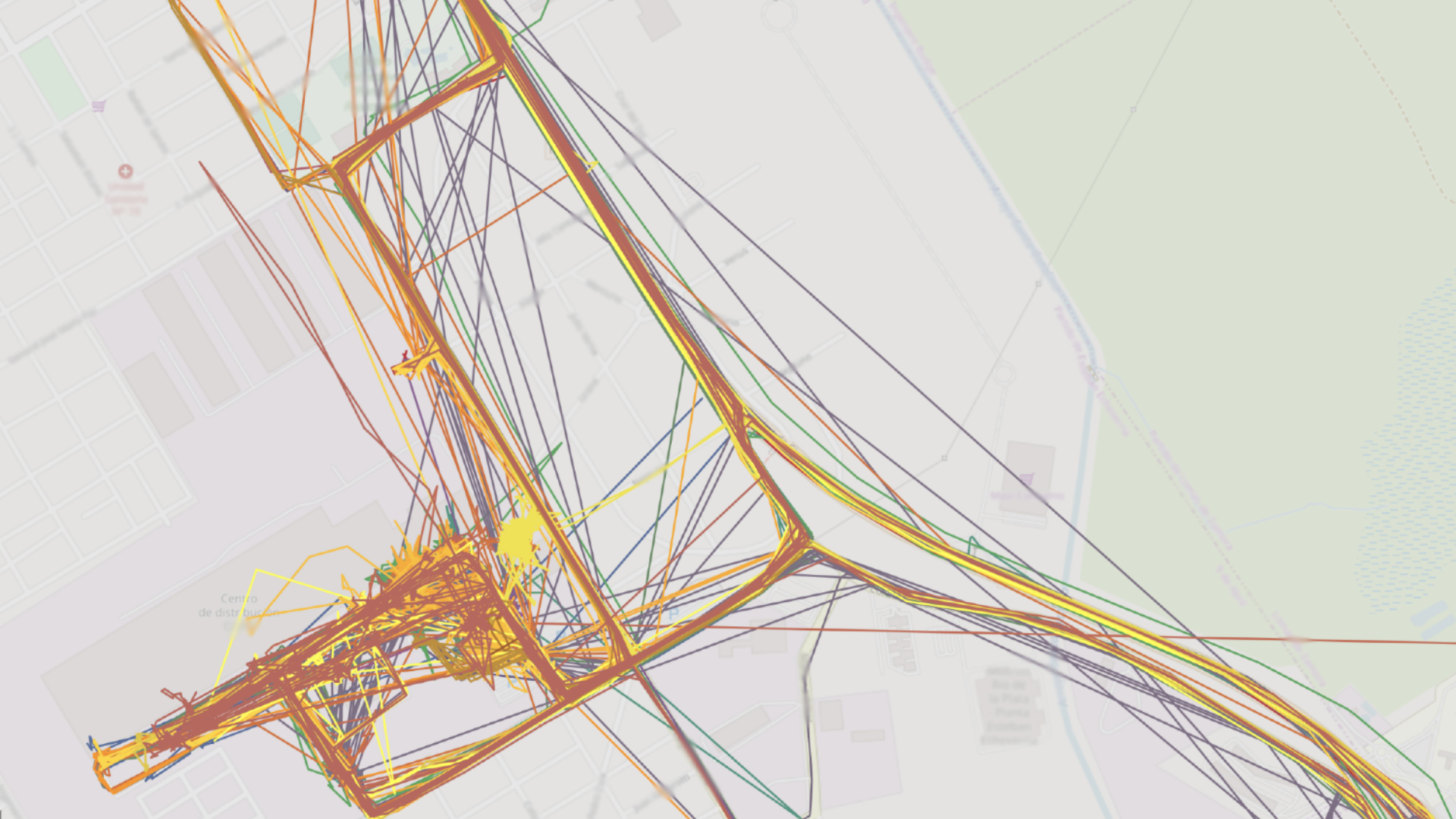
GPS log data


Córdoba
Rafaela
Concordia
Salto
Rivera
Bagé
Pelotas
Santa Fe
Tacuarembó
Paysandú
Tacuarembó
Rio Grande
Entre Rios
Paysandú
Cerro Largo
Rio Branco
Rio Negro
Paso de los Toros
Gualeguaychú
Rosario
Fray Bentos
Durazno
Treinta y Tres
Uruguay
Rio Cuarto
San Luis
Mercedes
Treinta y Tres
Durazno
Dolores
Soriano
Flores
Villa Mercedes
Florida
Lavalleja
Carmelo
Florida
Rocha
Colonia
San José
Minas
Rocha
Juan Lacaze
Libertad
Canelones
Maldonado
Montevideo
San Carlos
Maldonado
La Plata
Rio de la Plata
Santa Rosa
Tandil
La Pampa

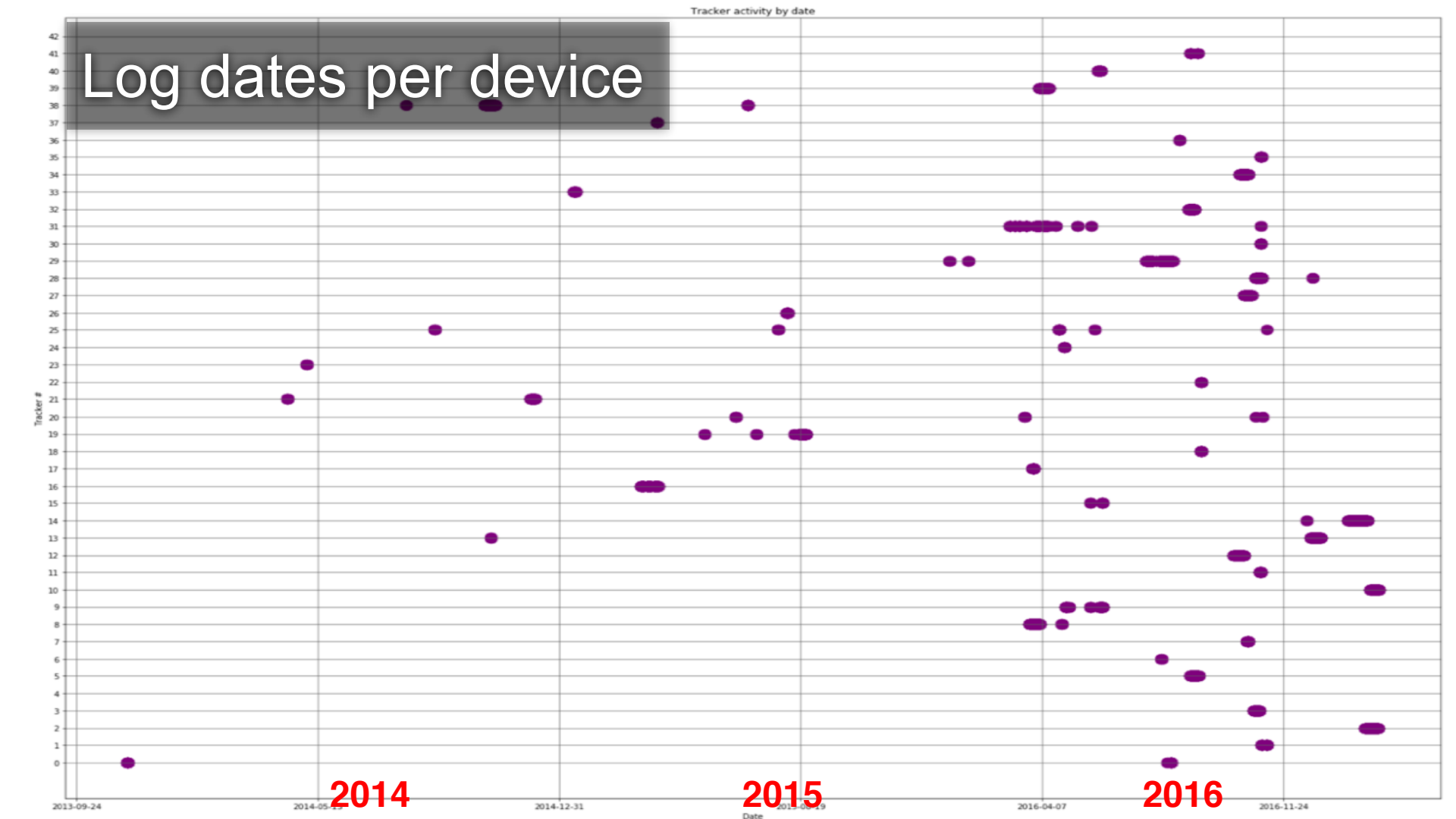

Villa Rosa
Garin
Tigre
Pilar
Del Viso
San Fernando
General Pacheco
Virreyes
Béccar
El Talar
San Isidro
Presidente
Derqui
RP8
Martínez
Villa de Mayo
Los Polvorines
José C. Paz
Campo
de Mayo
Cuartel V
San Miguel
Muñiz
Bella Vista
Santa María
Luján
RP6
RP24
Trujui
General Rodriguez
Francisco Alvarez
Villa Udaondo
La Reja
Moreno
Merlo
Ituzaingó
Parque San
Martín
Libertad
Mariano Acosta
RP6
RP24
Gregorio de
Laferrere
Isidro Casanova
Monte Chingolo
Bernal
Quilmes
Lomas de Zamora
Florencio Varela
Rafael Calzada
Monte Grande
Burzaco
Ministro Rivadavia
Marcos Paz
RP6
RP6


Villa Maipú
Villa Juan Martín de Pueyrredón
Billinghurst
Villa Bosch
Martín Coronado
Villa Libertad
Villa Lynch
Ciudad Jardín Lomas del Palomar
Santos Lugares
Sáenz Peña
Caseros
Villa Alianza
El Palomar
Villa Real
Monte Castro
Versalles
Villa Sarmiento
Haedo
Ramos Mejía
Villa Urquiza
Villa Pueyrredón
Villa Ortúzar
Parque Chas
Chacarita
Agronomía
La Paternal
Villa del Parque
Villa Santa Rita
Belgrano
Belgrano R
Coghlan
Colegiales
Palermo
Barracas
Mataderos
Parque Avellaneda
Parque Chacabuco
Parque Patricios


Del Viso
Pilar
Presidente Derqui
RP8
General Pacheco
San Fernando
Virreyes
Béccar
El Talar
San Isidro
Villa de Mayo
Los Polvorines
José C. Paz
Martínez
Boulogne Sur Mer
Vicente López
Campo de Mayo
Cuartel V
San Miguel
Muñiz
Bella Vista
Santa María
Luján
Aeroclub Luján Km64
RP6
RP24
Trujui
Villa Ballester
San Andrés
General San Martín
Villa Lynch
Hurlingham
Loma Hermosa
Pablo Podestá
El Libertador
Ante Puerto Buenos Aires
Buenos Aires
General Rodriguez
Francisco Alvarez
Villa Udaondo
Villa Tesei
El Palomar
Ciudadela
Moreno
La Reja
Morón
Ramos Mejía
Merlo
Ituzaingó
Aeródromo Estancia Villa María
Avellaneda
Dock Sud
San Justo
Villa Madero
Sarandí
Parque San Martín
Libertad
Isidro Casanova
Lanús Oeste
Wilde
Bernal
Quilmes
Mariano Acosta
Aeródromo La Fantasía
Ciudad Evita
Villa Centenario
Monte Chingolo
Banfield
Gregorio de Laferrere
Pontevedra
9 de Abril
Lomas de Zamora
Ezpeleta
Berazategui
González Catán
Temperley
San Francisco Solano
Rafael Calzada
Florencio Varela
Marcos Paz
RNA002
Aeródromo Marcos Paz
Claypole
Monte Grande
San Francisco de Asís
Burzaco
Bosques
Villa Vatteone
Jáuregui
Ministro Rivadavia
Ezeiza
Longchamps
Virrey Del Pino
La Unión
Aeroclub Longchamps
RP6
RP40




Centro
de distribución
P
P
P
P

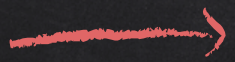

Log dates per device
Tracker activity by date
Tracker #
Date
2013-09-24
2014-05-13
2014-12-31
2015-08-19
2016-04-07
2016-11-24
2014
2015
2016

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

Very likely an optimization

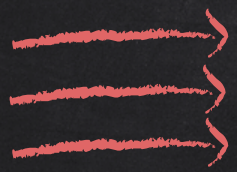
AT$REST=<Action>,<Reset Option>

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 this

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

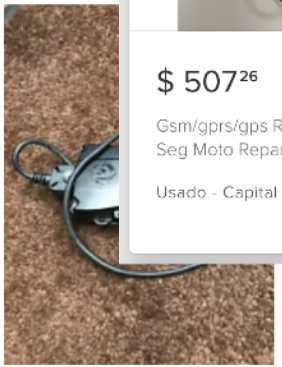
Usado - Capital Federal

$ 2.000

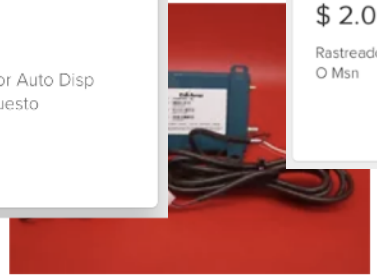
Rastreador Geolocalizador Por Internet O Msn

$ 1.200

Rastreadores Satelitales Via Gps-gpr Varios Modelos

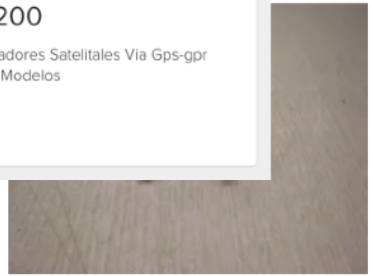


Verizon Network Fleet GPS Vehicle Tracker Unit 5200N3VD



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 400 1n Usb

$ 400

Router Wifi N150 D-link Funcionando Perfecto

$ 999

Router Mc Microsoft

$ 2.499

Apple Watch Serie 1 Negro Aluminio Pote 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 Introducción

$ 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

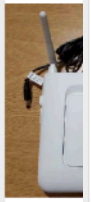
Linksys Ea4500 N900 Dual-band Smart Wifi Router

13

Usado - Capital Federal

$ 48.500

Lavarropas Lg Direct Drive Inverter Wm13eg6 - 6 Motion



$ 1.189

Envío grat

Modem R Wifi Astor

$ 16.999

Apple Watch Serie Series 2 42mm Con 3 Mallas

$ 1.600

Sonoff Powr2 Interruptor Wi Fi Domotica

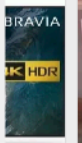
$ 17.800

Envío gratis

Control Acceso Asistencia Wifi Silv27 Tarjeta Rfid

$ 20.000

Envío gratis



$ 6.000

Tv Smart 50" Uhd 4k Samsung Un50mu6300gcdf

$ 700

Router Wifi Tp-link Wr841n 841n 300 Mbps 2 Ant Sdbi

$ 1.250

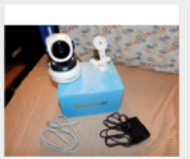
Totolink Ex300 300 Mbps Wireless Wifi Repetidor 2

$ 750

Router Wi 300 Mbps

$ 10.000

Samsung Gear S2 Classic



$ 3.500

Envío gratis

Juego De 2 Cámaras Wifi

$ 4.800

Envío gratis

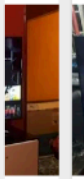
Comunicador Wifi Interce Cloud

$ 5.000

Termostato Digital Wifi

$ 7.399

Termostato Wifi Para Caldera Peisa Baxi * Nest Solidmation *



$ 6.000

Tv Led Smart 48 Bgh Ble4815rtfv Con La Pantalla

$ 900

Smartwatch U8 Reloj Inteligente Celular Android

$ 22.838

Smartwach Samsung Gear S3 Classic Silver Wifi Bluetooth

$ 10.999

Smart Tv Samsung 49 Led Youtube Netflix

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