Rumps

About me

- Over caffeinated wolf
- Voiding warranties for a living since 2018
- Projects :
  - Done :
    - Bypassing the Hantek DSO software limitation
    - GPS spoofing on DJI Inspire 1
    - Recovering and exploiting IP cameras
  - WIP :
    - Freeway toll gate token reverse engineering
    - NOVAL 4G IoT xxxxx 😏

Twitter / X : @CyberWolf_2077

Blog : whiterose-infosec.super.site/

What this talk is about

- Understanding how companies produces electronic devices
- Checking basic elements on your devices to gain access and add functionalities
- Fucking things up (a lot)

What this talk isn't about

- Motivating you to do so on all your devices 😉

Story 1: Hantek DSO

- Introduction
- Open the oscilloscope
- Finding the serial pins
- Connect the USB / UART
- Edit the config file
- Apply the edit
- Checking the modification

Story 2: Flying anywhere

- Introduction
- Getting to simulate a GPS constellation
- Time to create our fake constellation
- Ready to take off
- Let’s travel around the world !
- Time to do some sketchy shit
- Not fun issue on the DJI app
- Fun side effects

Why pay 500$ a device when you can get the same out of the 250$ version

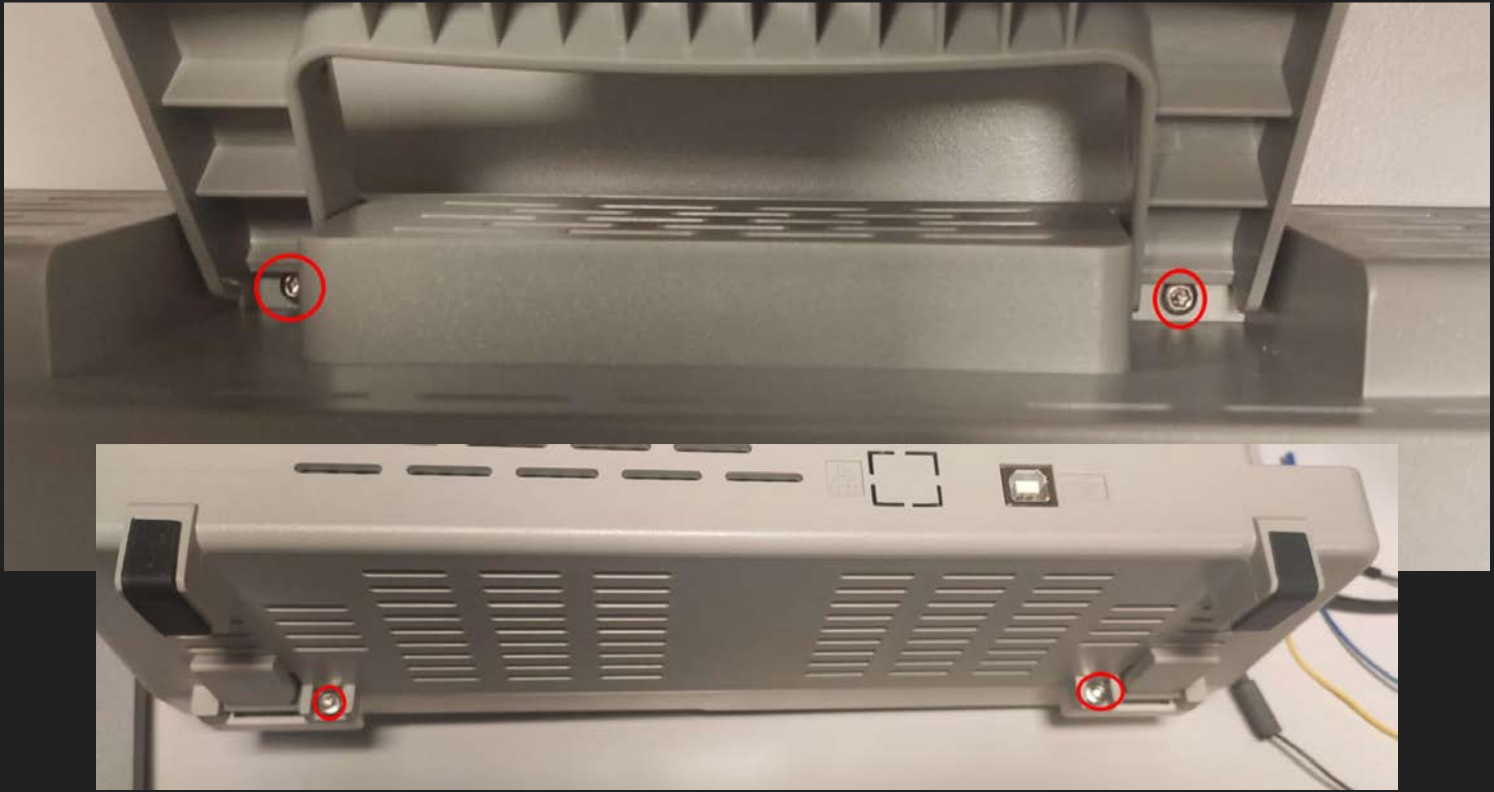
How Hantek (and others) tries to same money but could lose a lot

Introduction

Hantek DSO-4072C 2-ch, 70MHz

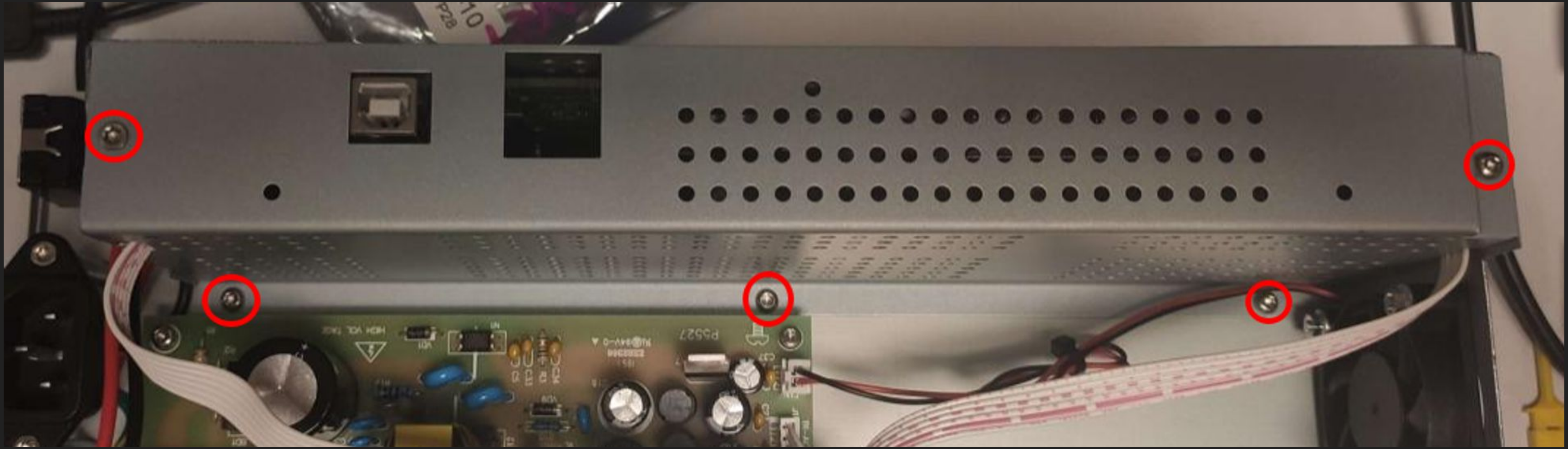
⚠ This is not a tutorial

Open the oscilloscope



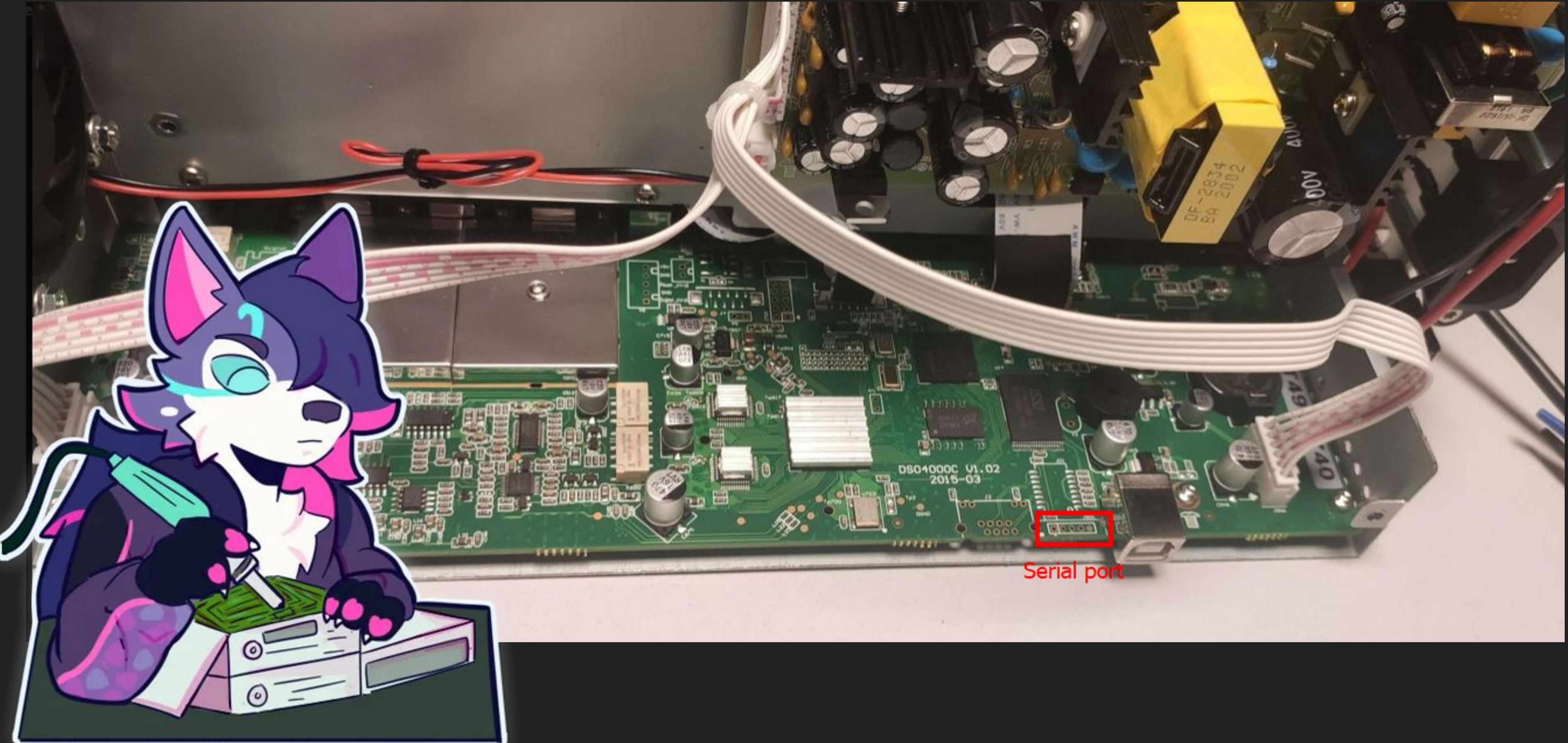
Open the oscilloscope

⚠ This is not a tutorial



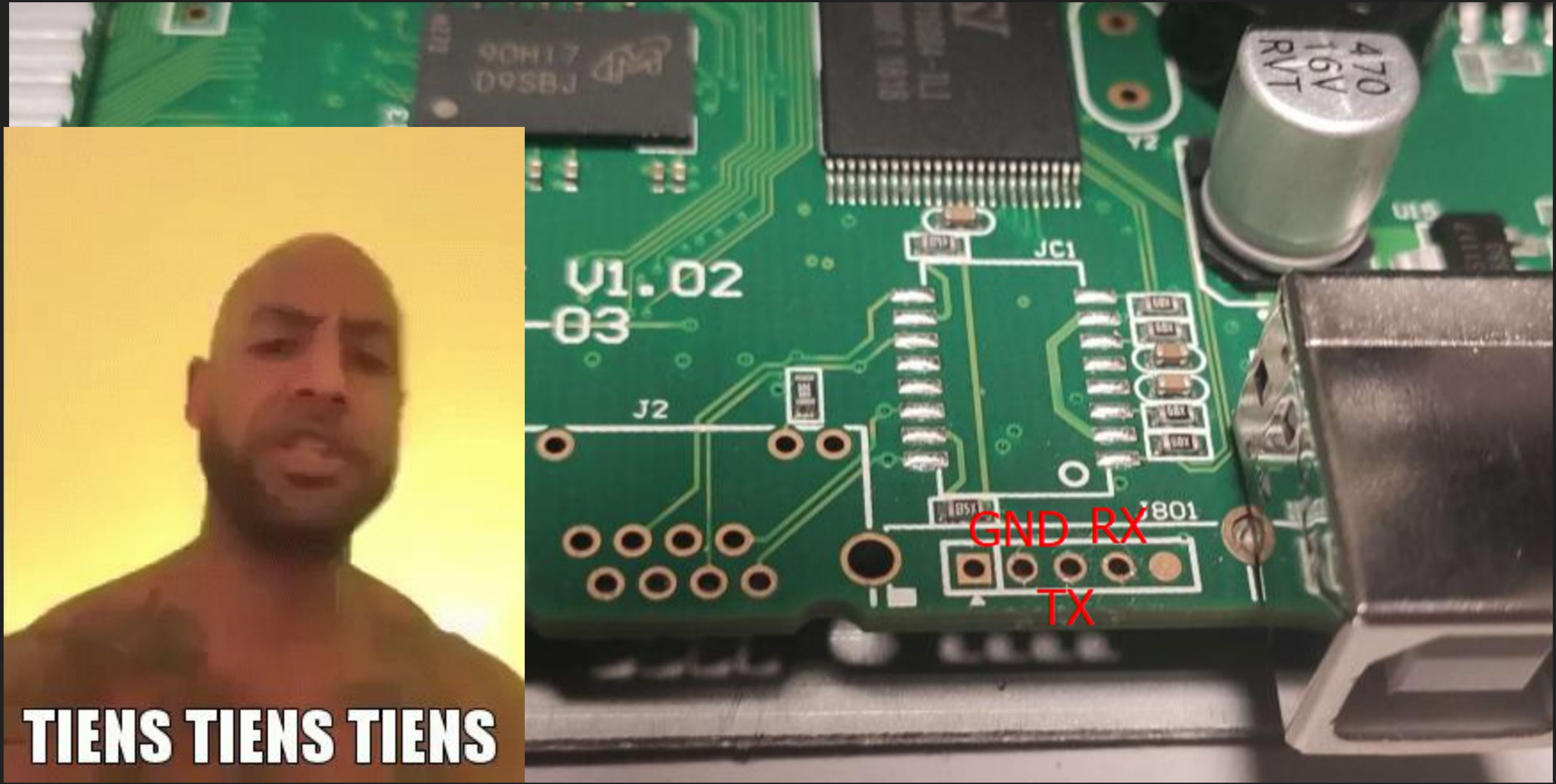
Finding the serial pins

⚠ This is not a tutorial



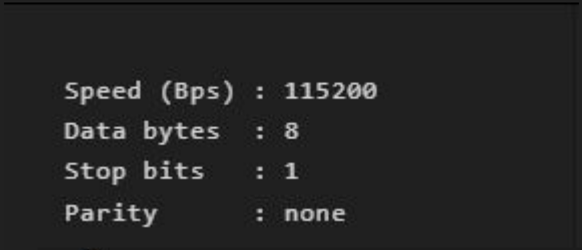
Finding the serial pins

⚠ This is not a tutorial

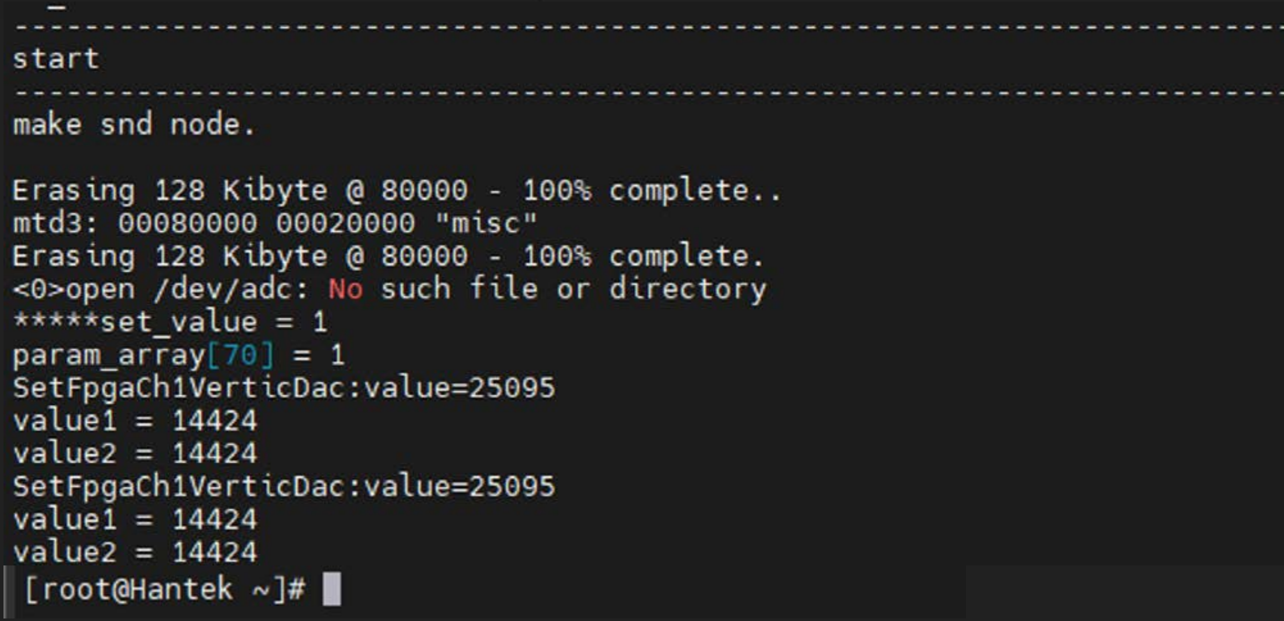


Connect the USB / UART

⚠ This is not a tutorial



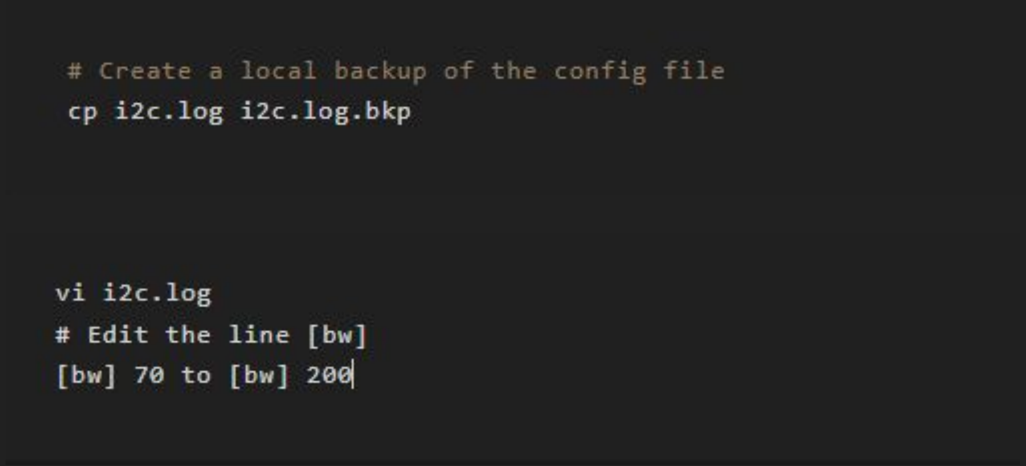
```
Speed (Bps) : 115200
Data bytes  : 8
Stop bits   : 1
Parity      : none
```



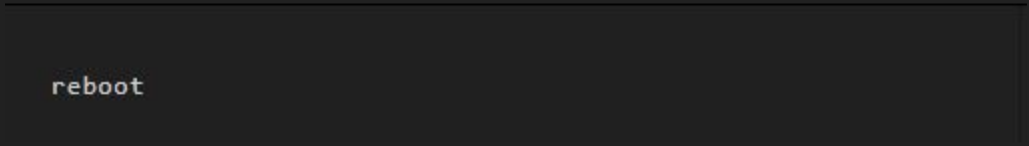
```
 _
--------------------------------------------------------------------------------
start
--------------------------------------------------------------------------------
make snd node.

Erasing 128 Kibyte @ 80000 - 100% complete..
mtd3: 00080000 00020000 "misc"
Erasing 128 Kibyte @ 80000 - 100% complete.
<0>open /dev/adc: No such file or directory
*****set_value = 1
param_array[70] = 1
SetFpgaCh1VerticDac:value=25095
value1 = 14424
value2 = 14424
SetFpgaCh1VerticDac:value=25095
value1 = 14424
value2 = 14424
[root@Hantek ~]# █
```

Edit the config file and Applying the edit

⚠️ **This is not a tutorial**



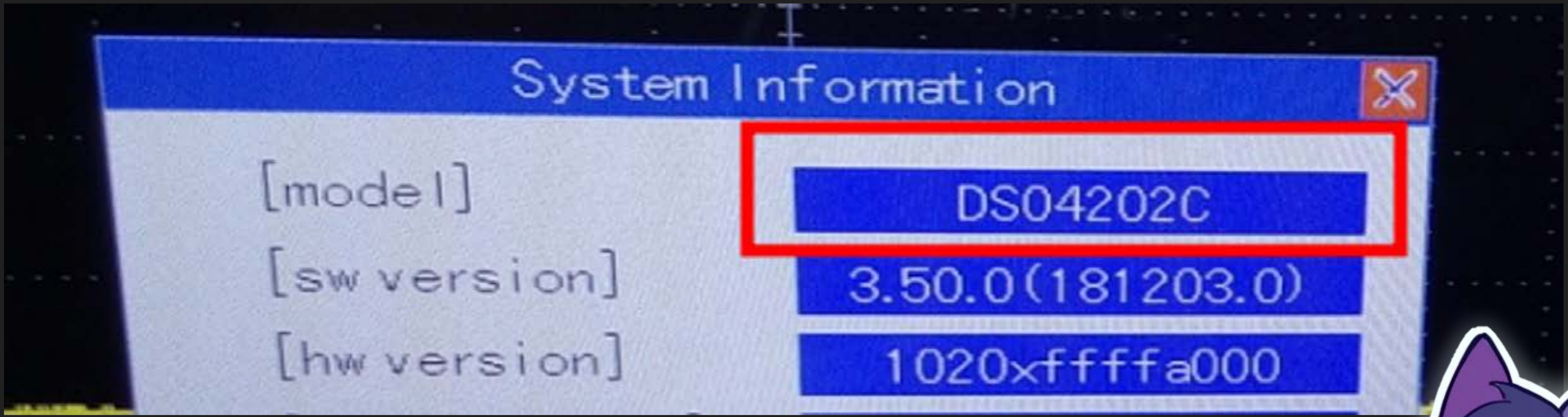
```
# Create a local backup of the config file
cp i2c.log i2c.log.bkp



vi i2c.log
# Edit the line [bw]
[bw] 70 to [bw] 200
```



```
reboot
```

Checking the modification

⚠ This is not a tutorial



System Information

[model] DSO4202C

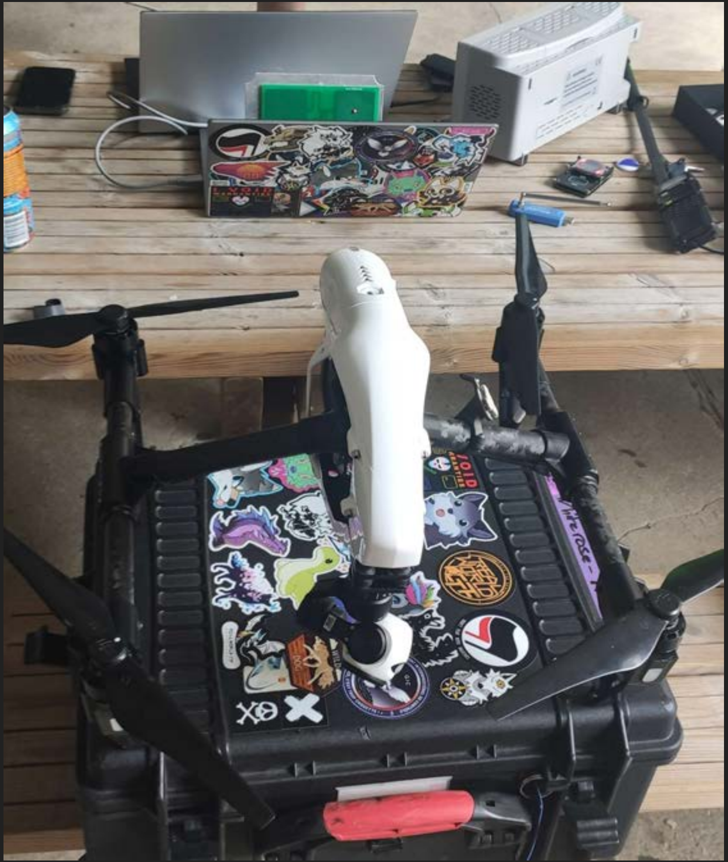
[sw version] 3.50.0(181203.0)

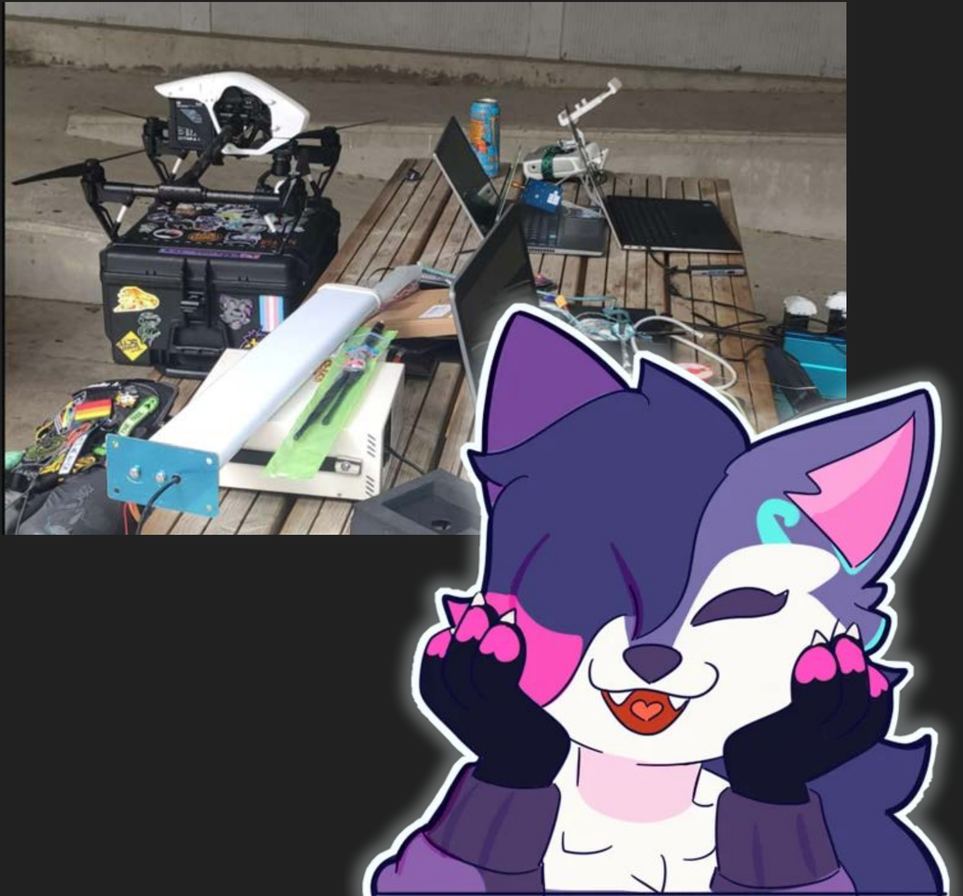
[hw version] 1020xffffa000

Hantek DSO-4202C : 200MHz

Could your drone fly anywhere in the world ?

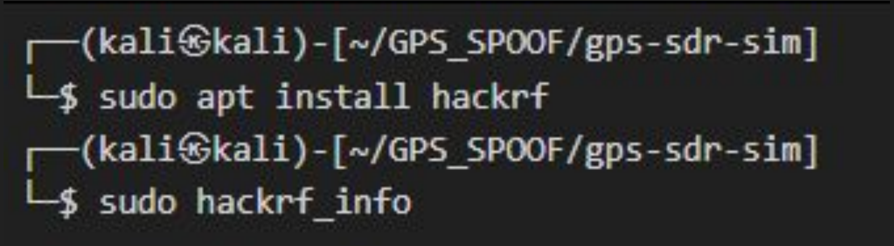
Introduction



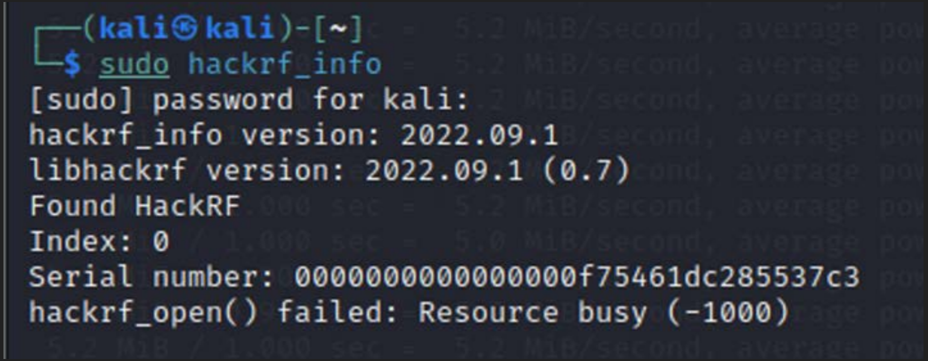


Getting to simulate a GPS constellation

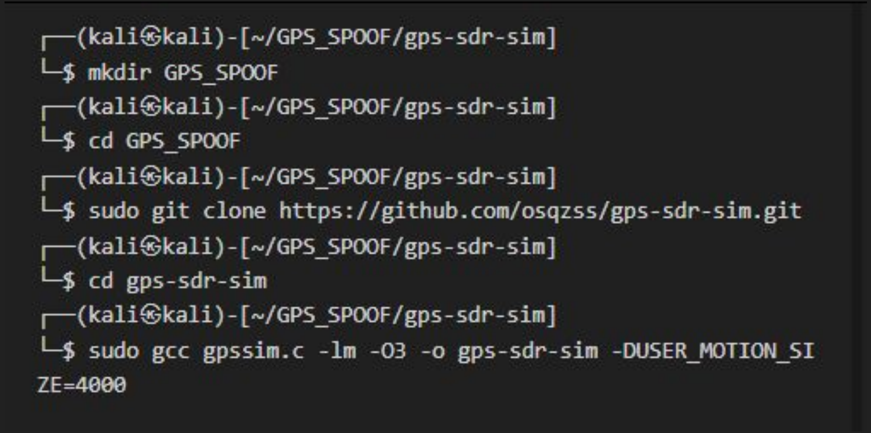
⚠ **This is not a tutorial**



```
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo apt install hackrf
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo hackrf_info
```



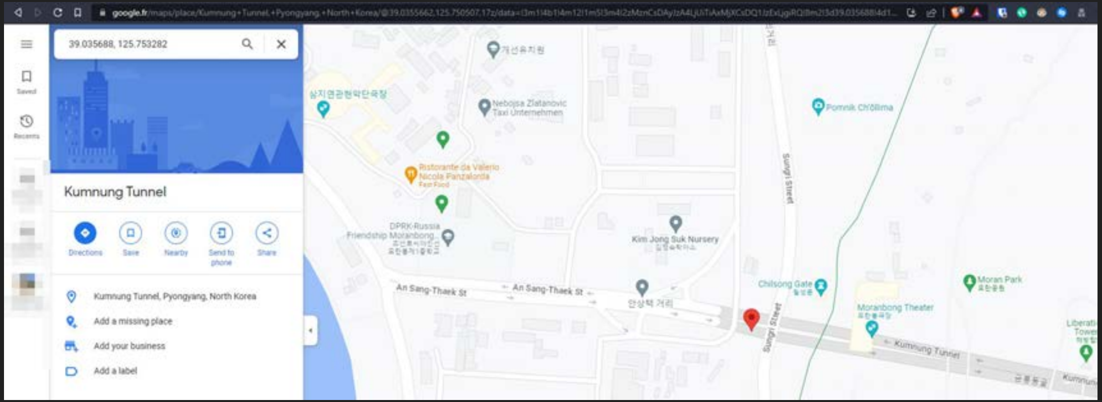
```
┌──(kali㉿kali)-[~]
└─$ sudo hackrf_info
[sudo] password for kali:
hackrf_info version: 2022.09.1
libhackrf version: 2022.09.1 (0.7)
Found HackRF
Index: 0
Serial number: 0000000000000000f75461dc285537c3
hackrf_open() failed: Resource busy (-1000)
```



```
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ mkdir GPS_SPOOF
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ cd GPS_SPOOF
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo git clone https://github.com/osqzss/gps-sdr-sim.git
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ cd gps-sdr-sim
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo gcc gpssim.c -lm -O3 -o gps-sdr-sim -DUSER_MOTION_SI
ZE=4000
```

Time to create our fake constellation

⚠ This is not a tutorial


google.fr/maps/place/Kumnung+Tunnel,+Pyongyang,+North+Korea/@39.0355662,125.750507,17z/data=

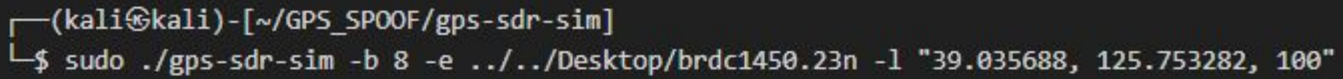
39.035688, 125.753282

Kumnung Tunnel

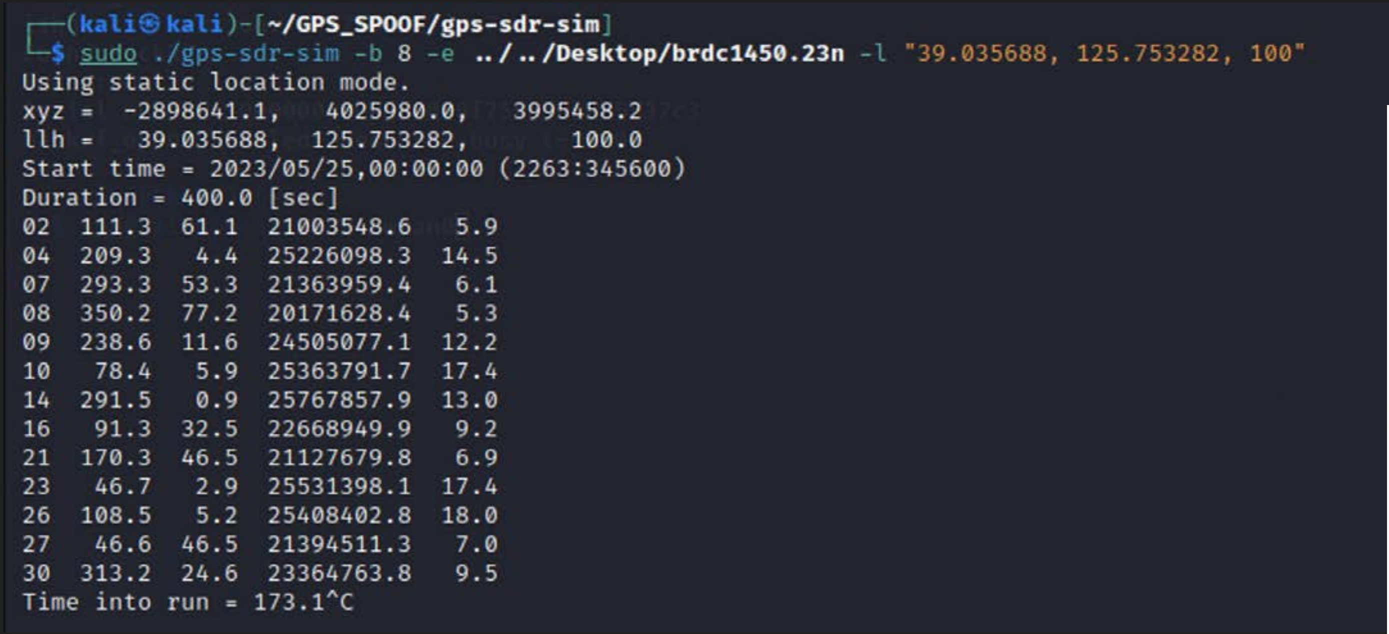
Kumnung Tunnel, Pyongyang, North Korea

Time to create our fake constellation

⚠ This is not a tutorial



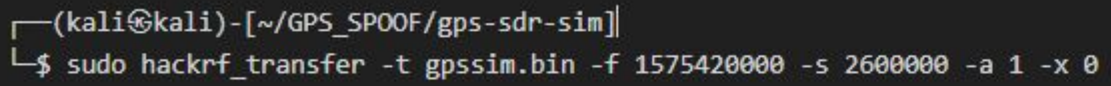
```
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo ./gps-sdr-sim -b 8 -e ../../Desktop/brdc1450.23n -l "39.035688, 125.753282, 100"
```



```
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo ./gps-sdr-sim -b 8 -e ../../Desktop/brdc1450.23n -l "39.035688, 125.753282, 100"
Using static location mode.
xyz =  -2898641.1,   4025980.0,   3995458.2
llh =   39.035688,  125.753282,       100.0
Start time = 2023/05/25,00:00:00 (2263:345600)
Duration = 400.0 [sec]
02  111.3  61.1  21003548.6   5.9
04  209.3   4.4  25226098.3  14.5
07  293.3  53.3  21363959.4   6.1
08  350.2  77.2  20171628.4   5.3
09  238.6  11.6  24505077.1  12.2
10   78.4   5.9  25363791.7  17.4
14  291.5   0.9  25767857.9  13.0
16   91.3  32.5  22668949.9   9.2
21  170.3  46.5  21127679.8   6.9
23   46.7   2.9  25531398.1  17.4
26  108.5   5.2  25408402.8  18.0
27   46.6  46.5  21394511.3   7.0
30  313.2  24.6  23364763.8   9.5
Time into run = 173.1^C
```

⚠ **This is not a tutorial**

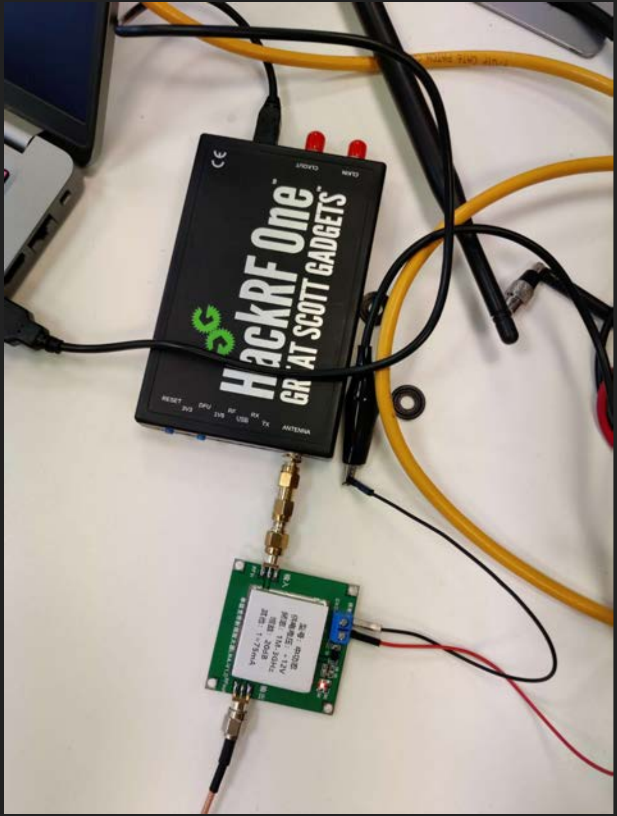
Ready to take off (maybe)

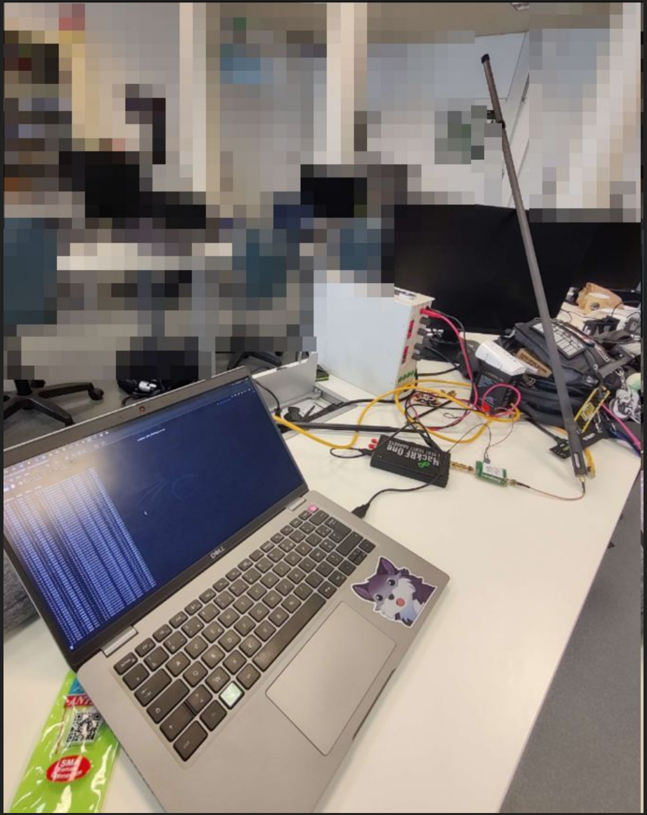


```
┌──(kali㉿kali)-[~/GPS_SPOOF/gps-sdr-sim]
└─$ sudo hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0
```

⚠ This is not a tutorial

Ready to take off (for sure)

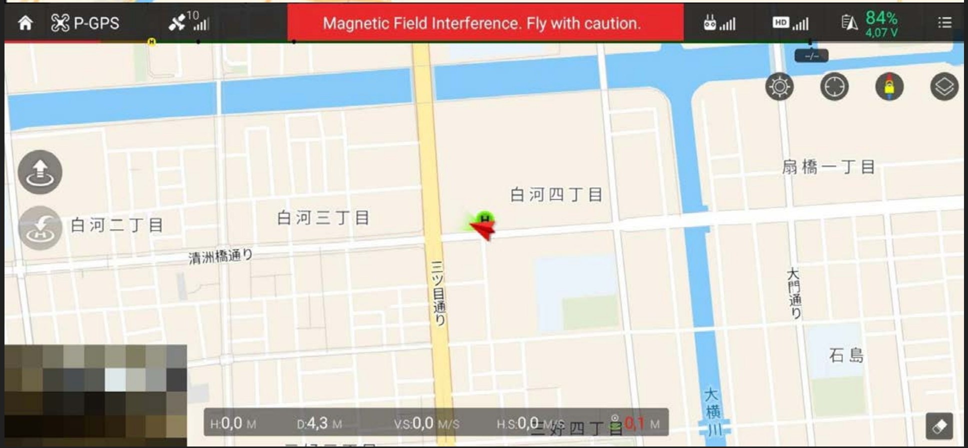


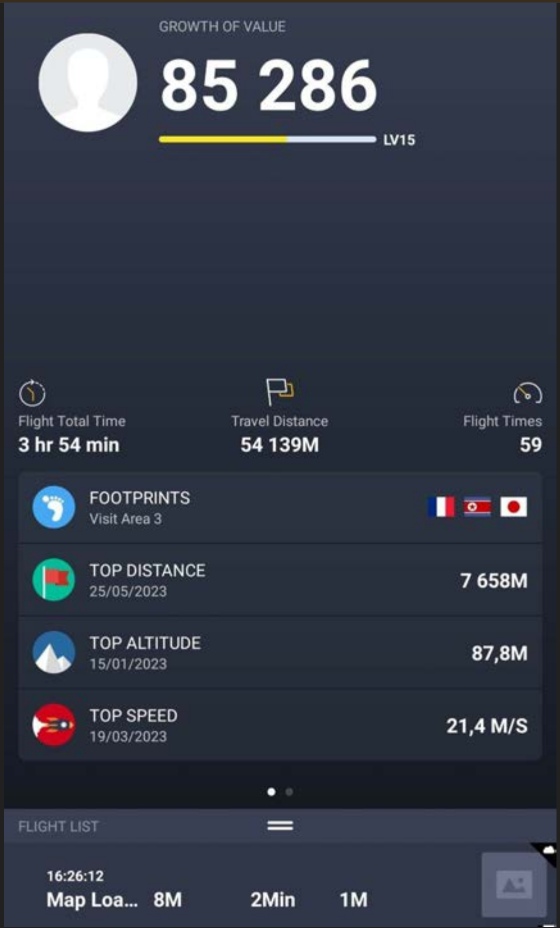


⚠ This is not a tutorial

Let's travel around the world !

대동읍
평양시
P'YŎNGYANG


Magnetic Field Interference. Fly with caution.


GROWTH OF VALUE

85 286

LV15

Flight Total Time	Travel Distance	Flight Times
3 hr 54 min	54 139M	59

FOOTPRINTS
Visit Area 3

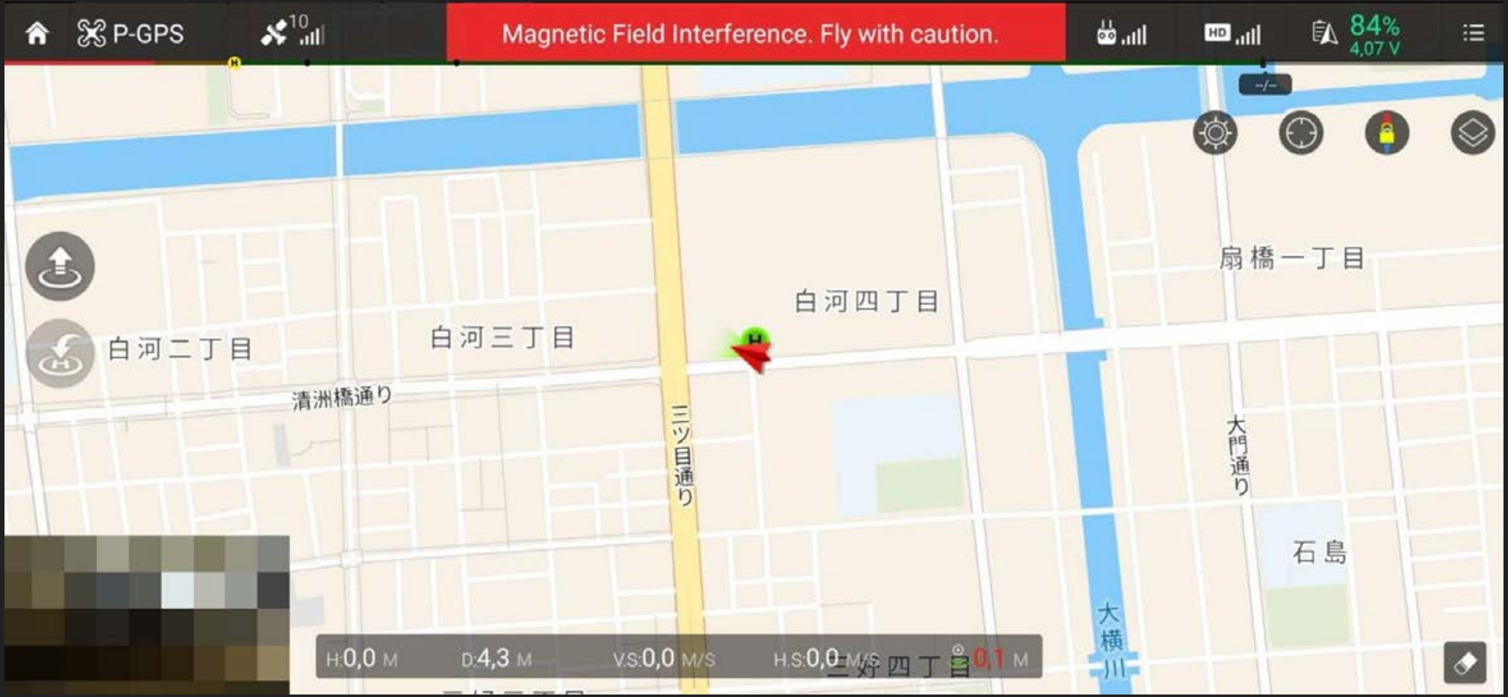
TOP DISTANCE 25/05/2023	7 658M
TOP ALTITUDE 15/01/2023	87,8M
TOP SPEED 19/03/2023	21,4 M/S

FLIGHT LIST

16:26:12
Map Loa... 8M 2Min 1M

⚠ This is not a tutorial

Let’s travel around the world !

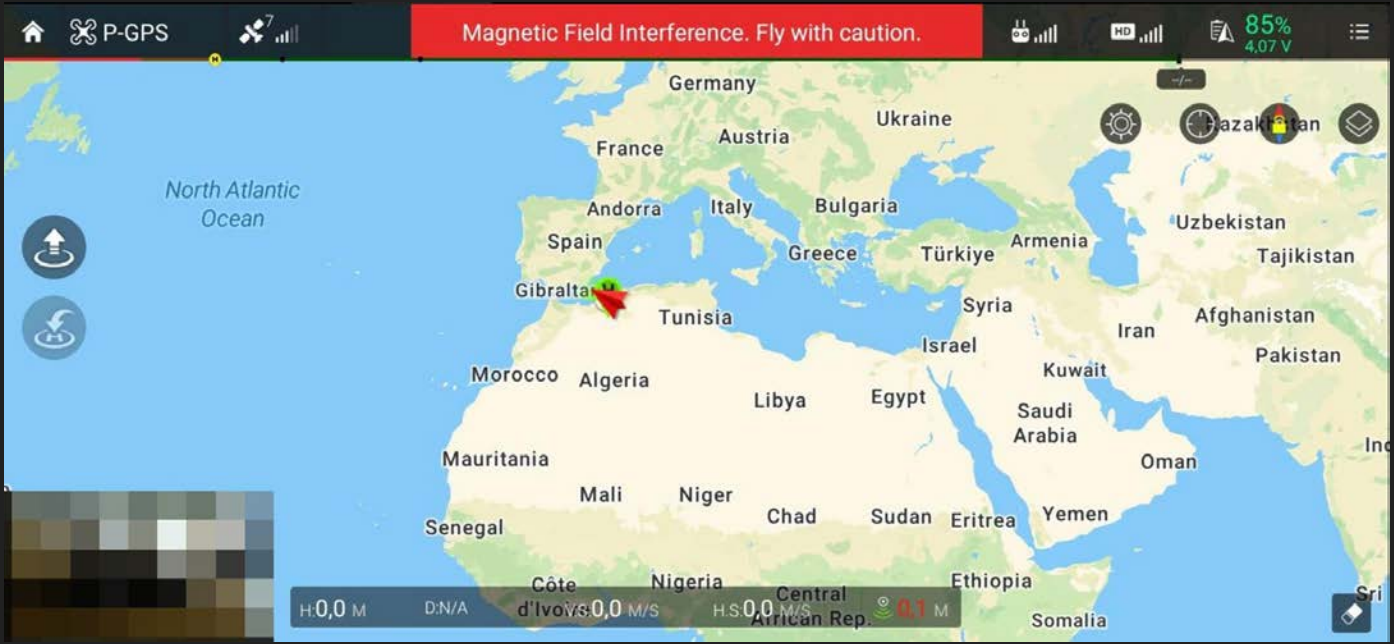


Magnetic Field Interference. Fly with caution.

H:0,0 M D:4,3 M V.S:0,0 M/S H.S:0,0 M/S 0,1 M

⚠️ This is not a tutorial

Let’s travel around the world !



Magnetic Field Interference. Fly with caution.

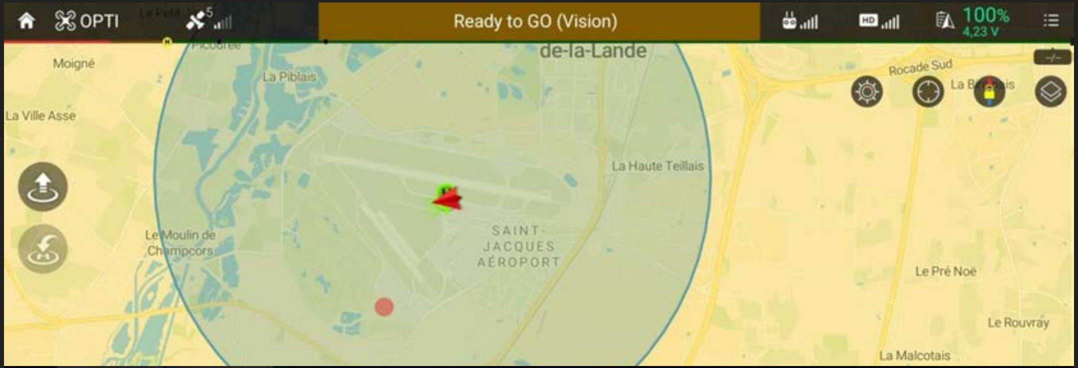
⚠️ This is not a tutorial

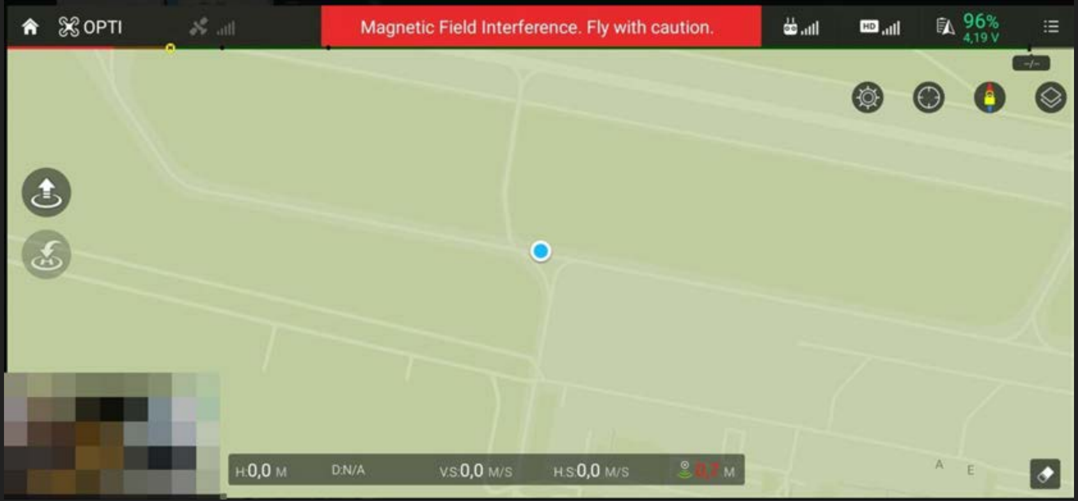
Time to do some sketchy shit

Aer Lingus
NO DRONE ZONE
It is illegal to operate drones in this area
Report suspicious activity to the Airport Police. Telephone: 01-814 4300
IAA
DublinAirport

⚠ This is not a tutorial

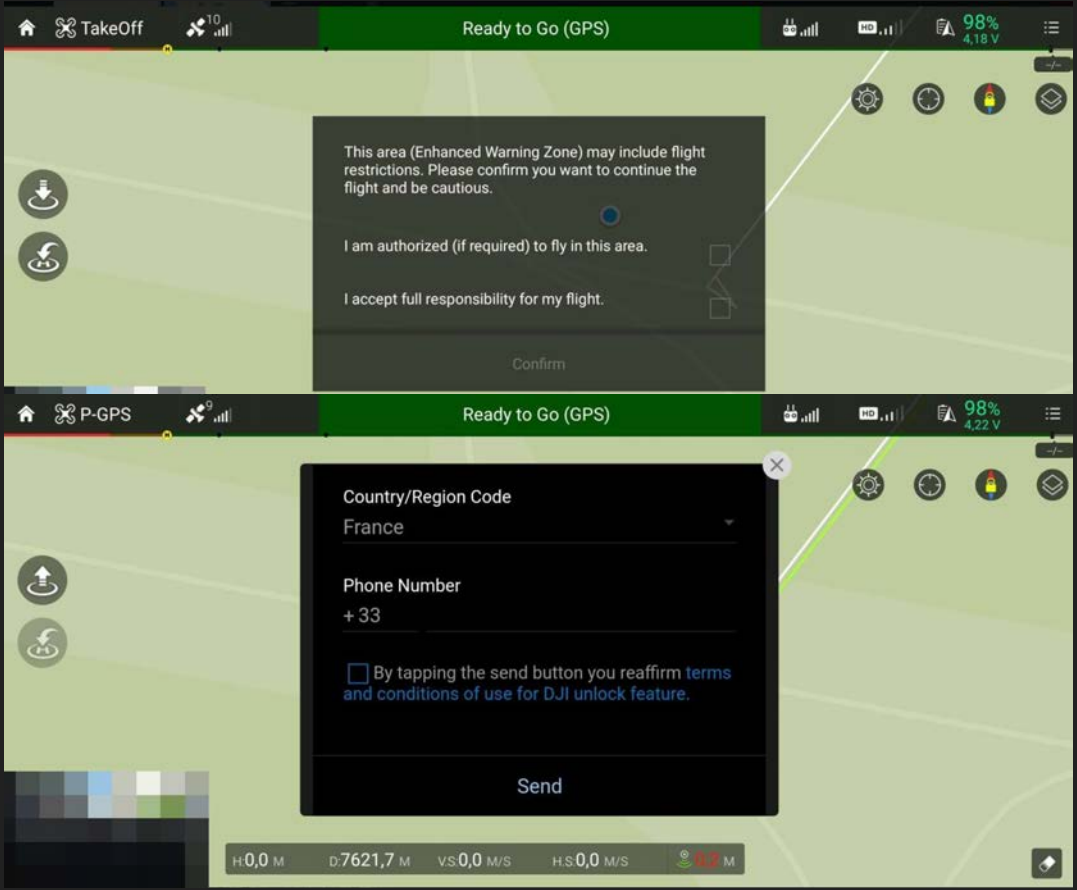
Time to do some sketchy shit


Ready to GO (Vision)


Magnetic Field Interference. Fly with caution.

Not fun issue on the DJI app

⚠ This is not a tutorial



This area (Enhanced Warning Zone) may include flight restrictions. Please confirm you want to continue the flight and be cautious.

I am authorized (if required) to fly in this area. □

I accept full responsibility for my flight. □

Confirm

Country/Region Code
France

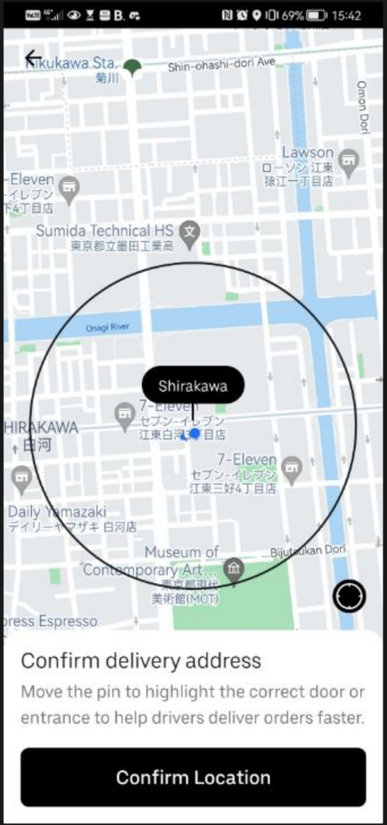
Phone Number
+ 33

□ By tapping the send button you reaffirm terms and conditions of use for DJI unlock feature.

Send

⚠ This is not a tutorial

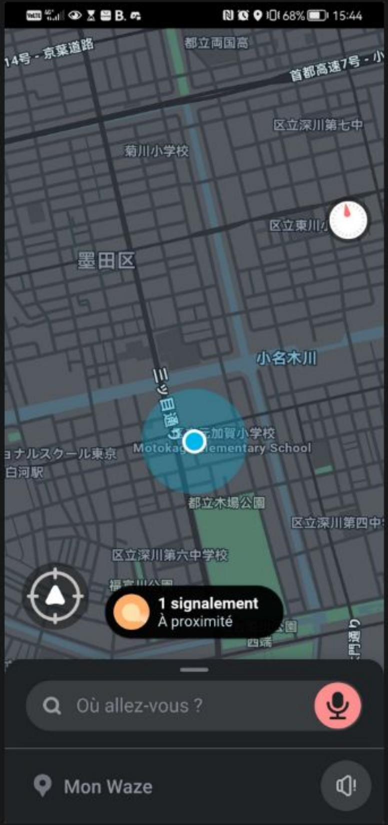
Fun side effects



Confirm delivery address

Move the pin to highlight the correct door or entrance to help drivers deliver orders faster.

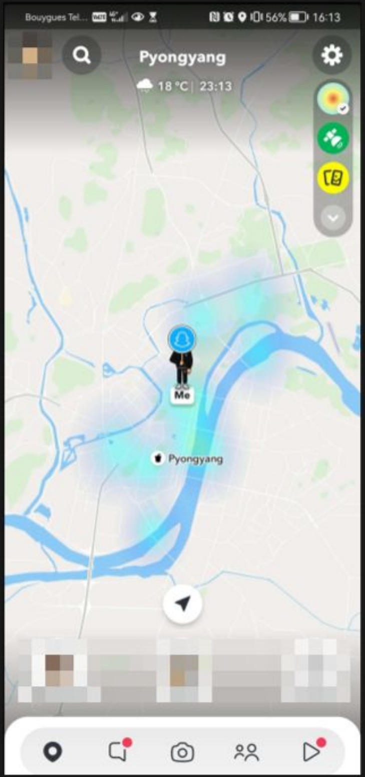
Confirm Location



1 signalement
À proximité

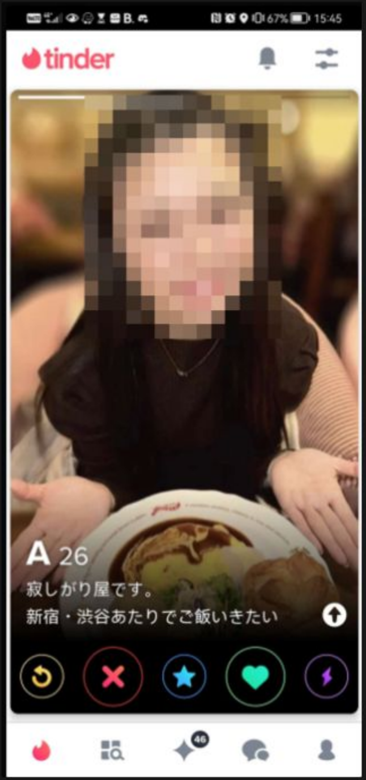
Où allez-vous ?

Mon Waze



Pyongyang

18 °C | 23:13



A 26

寂しがり屋です。

新宿・渋谷あたりでご飯いきたい

Hantek DSO

- https://github.com/WiZZteXX/DSO4xx4c/blob/i2c-tools/Hacking%20the%20HANTEK%20DSO4xx4BC.pdf
- https://www.eevblog.com/forum/testgear/hantek-tekway-dso-hack-get-200mhz-bw-for-free/
- https://www.eevblog.com/forum/testgear/upgrading-the-hantek-dso4072c-osciloscope-bandwidth-from-70mhz-to-200mhz/
-

DJI spoofing

- https://github.com/osqzss/gps-sdr-sim
- https://cddis.nasa.gov/archive/gnss/data/daily/
-

Questions