

# Typhoon



A Drone Tale  
All your drones are belong to us

Paolo Stagno

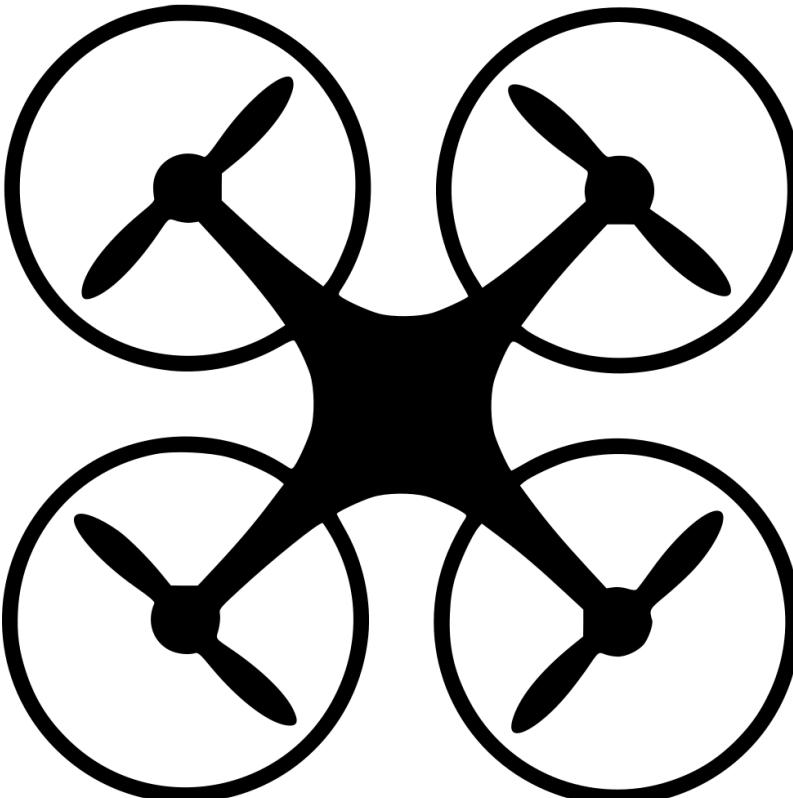
Paolo Stagno  
aka  
VoidSec

voidsec.com  
voidsec@voidsec.com  
 Void\_Sec





# Agenda



- Drone Intro
- Vulnerability Research & Attack Vectors:
  - Radio/Wi-Fi
  - DJI GO (Android App)
  - Firmware
  - GPS
- Reverse Engineering:
  - SDK
- Forensics

# Drone Intro

- Law Enforcement
- First Responder
- Utility companies
- Governments
- Universities
- Terrorism
- Pentest/Red Team



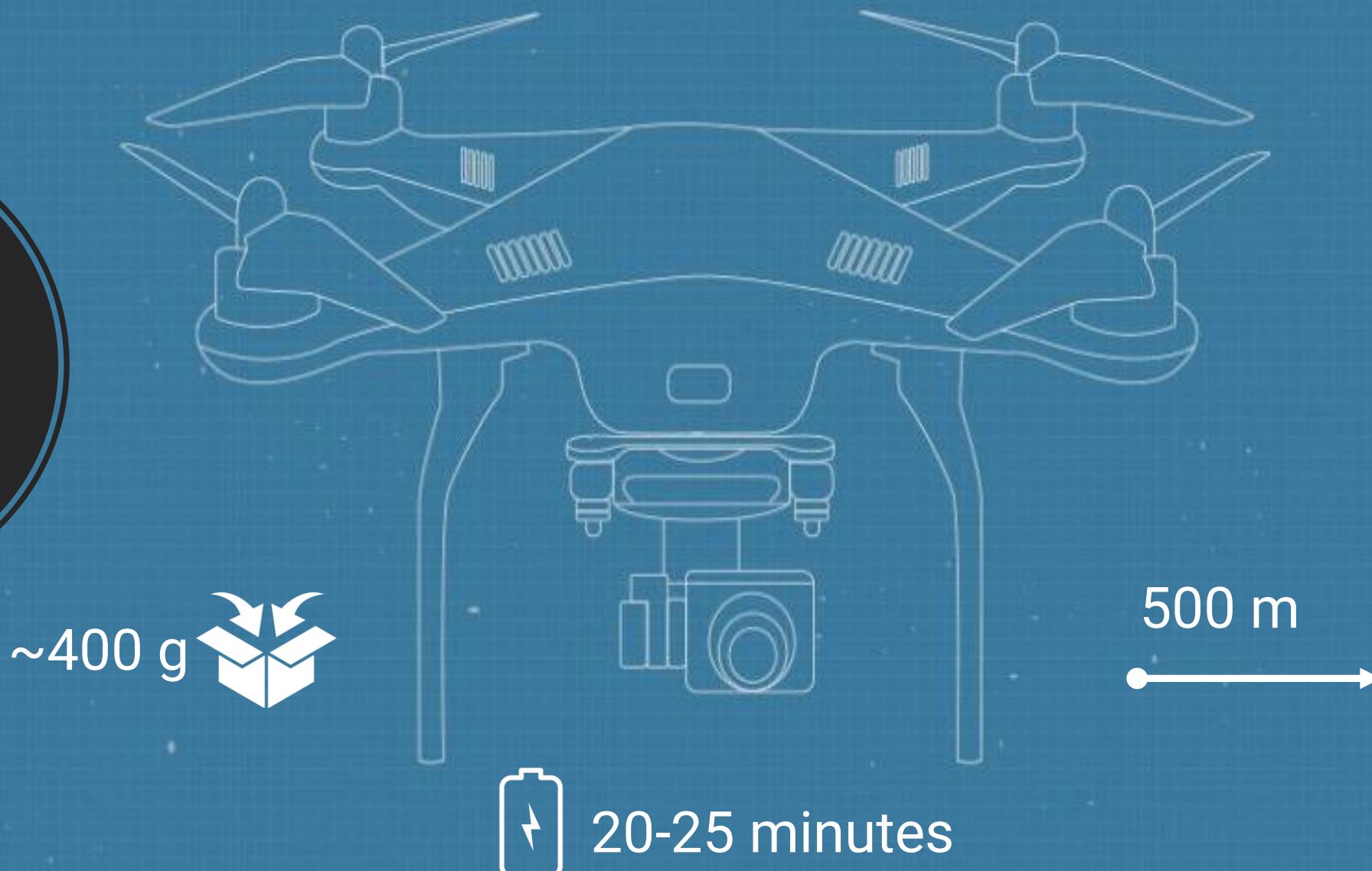
# DJI Phantom Intro



# Phantom 3 Specs

1,2 Kg 

16 m/s 



FPV

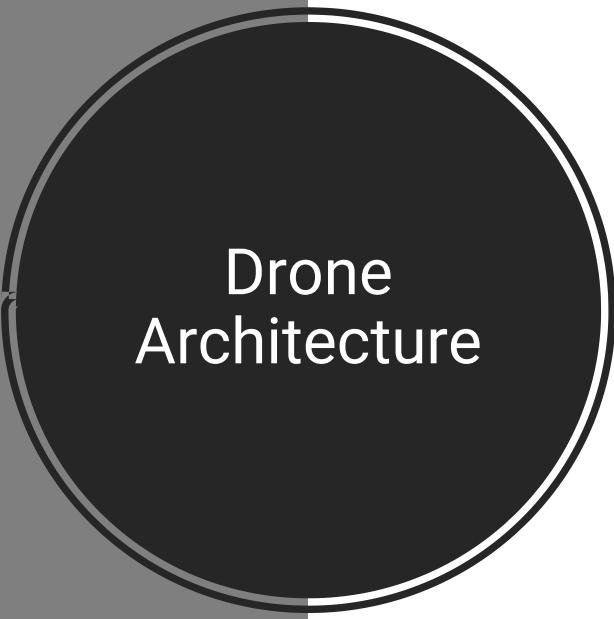


Shooting





# Shooting



## Drone Architecture

### Drone

- Flight controller
- Radio module
- GPS module and other sensors (Compass, Gyroscope, Accelerometer, Barometer)
- Micro-USB & MicroSD Slug (firmware update and media storage only)

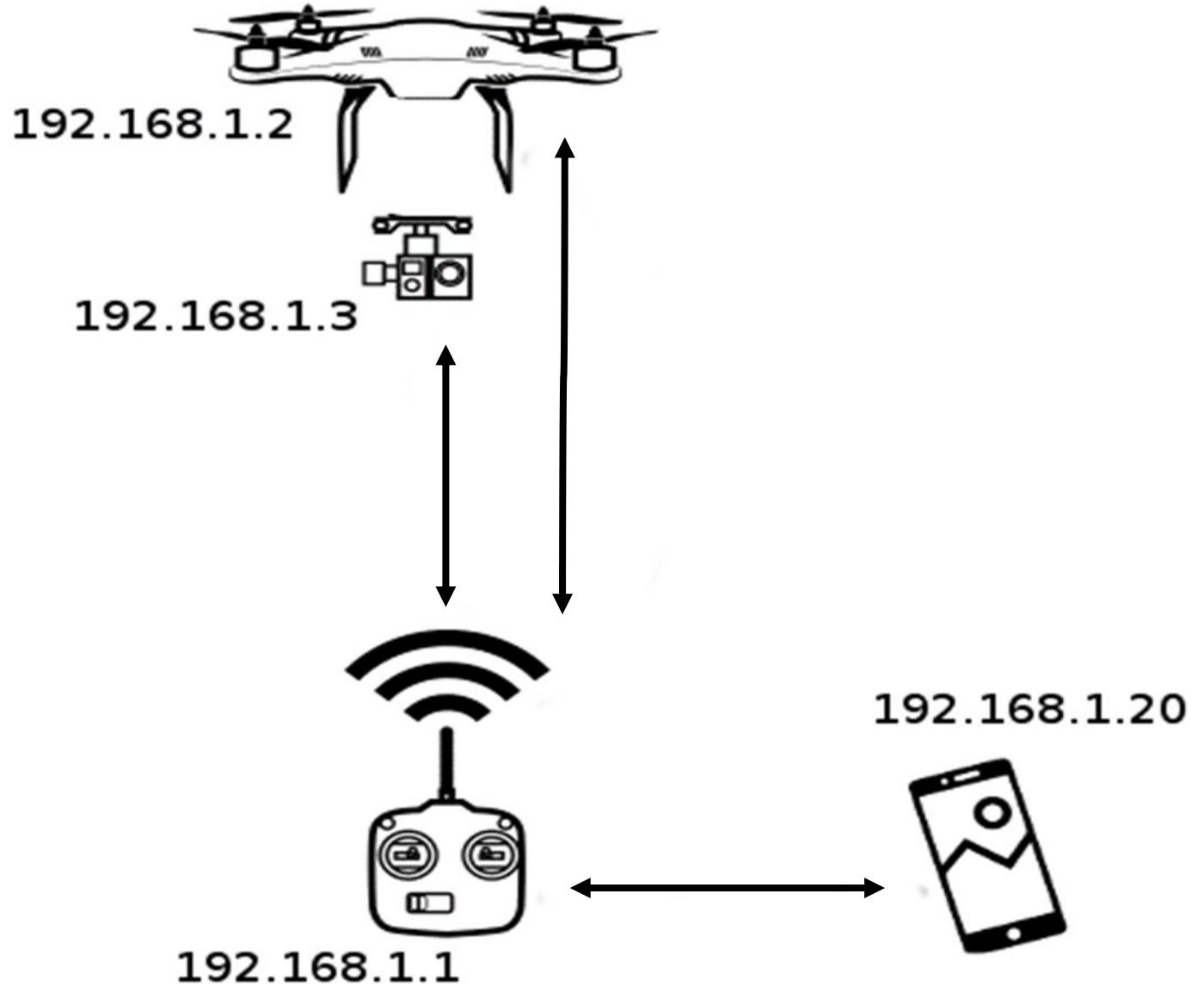
### Remote Controller

- Radio module
- USB Slug (firmware update and SDK only)

### App/SDK

- Connect to Remote Control, display drone information (video feedback, GPS data and compass)
- Drone Navigation (Drone Takeoff, RTH, Waypoint)

# Network Map





Firmware  
V01.07.0090

- Nmap scan report for 192.168.1.1 - Controller
  - 21/tcp open ftp vsftpd 3.0.2
  - 22/tcp closed ssh
  - 23/tcp closed telnet
  - 2345/tcp open unknown
  - 5678/tcp closed unknown
- Nmap scan report for 192.168.1.2 - Aircraft
  - 21/tcp open ftp vsftpd 3.0.2
  - 22/tcp filtered ssh
  - 23/tcp filtered telnet
  - 2345/tcp filtered unknown
  - 5678/tcp open unknown
- Nmap scan report for 192.168.1.3 - Camera
  - 21/tcp open ftp BusyBox ftPD  
| Anonymous FTP login allowed
  - 22/tcp open ssh OpenSSH 6.2
  - 23/tcp open telnet BusyBox telnetd
  - 2345/tcp filtered unknown
  - 5678/tcp filtered unknown



Latest  
Firmware  
V1.09.0200

- Nmap scan report for Controller
  - 21/tcp open ftp
  - 2345/tcp open unknown
- Nmap scan report for Aircraft
  - 21/tcp open ftp
  - 5678/tcp open unknown
- Nmap scan report for Camera
  - 21/tcp open ftp
  - 22/tcp open ssh
  - 23/tcp open telnet



## Radio & Wi-Fi

- Aircraft & Controller:  
Wi-Fi *5.725GHz – 5.825GHz*  
**(NOT the Lightbridge protocol)**
- Video Link: *2.400GHz – 2.483GHz*
- WPA2 encryption
- Default SSID is derived from the MAC address  
of the remote controller.  
**PHANTOM3\_[6 last digits of MAC address].**
- Default associated password is: **12341234**



## Wi-Fi Attacks

- De-auth attacks
- Controller > DJI GO
- Drone has a **client queue**
- If Wi-Fi is lost -> RTH



## Wi-Fi Attacks

### Attack

WEP

Cannot be downgraded to WEP from settings

WPS

No WPS support

WPA 2

4 way handshake brute-force

KRACK

Yes, AP & clients based on OpenWRT

# Wi-Fi Attacks

```
[-----]
[-----]
[-----]
[-----]          FLUXION 4.14      < Fluxion Is The Future >
[-----]
[-----]

[*] Select a wireless attack for the access point

        ESSID: "[N/A]" / [N/A]
        Channel: [N/A]
        BSSID: [N/A] ([N/A])

        [1] Captive Portal Creates an "evil twin" access point.
        [2] Handshake Snopper Acquires WPA/WPA2 encryption hashes.
        [3] Back

Time left: 0 seconds                                100.00%
                                                      
                                                      
KEY FOUND! [qwertyuiop]

Master Key      : 70 90 5A 79 5B 09 3B C1 17 E3 A5 FC CC 51 23 78
                   [REDACTED]

Transient Key   : 13 F6 15 EF 64 4E 41 20 3A B9 99 4C 68 13 DD FD
                   56 23 22 48 30 8B 24 EA 3E BE D7 50 B9 FB 51 7E
```

# Road to Shell

---

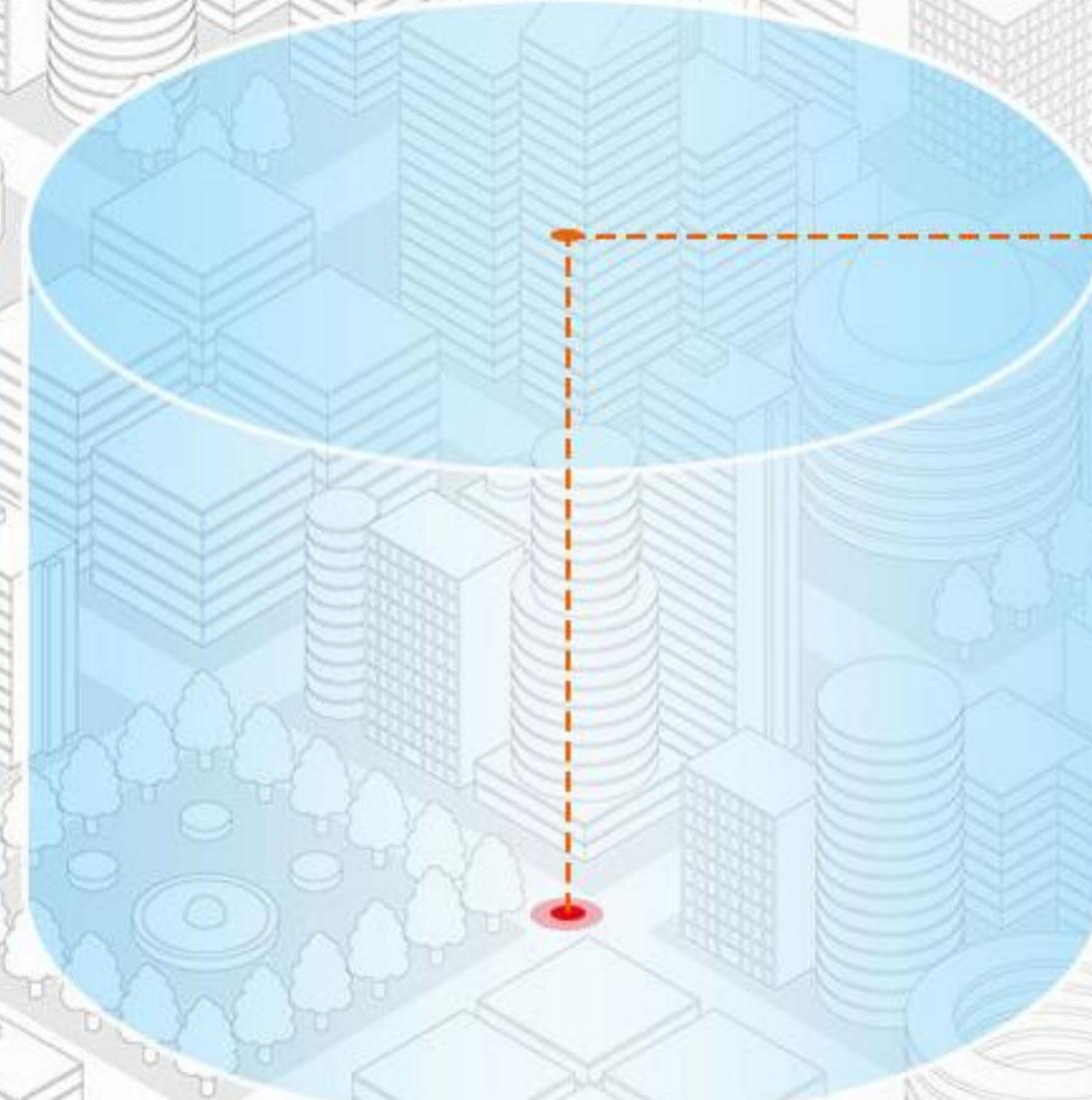
I do not have any  
SSH/FTP/Telnet passwords  
so...

DJI GO App Diving

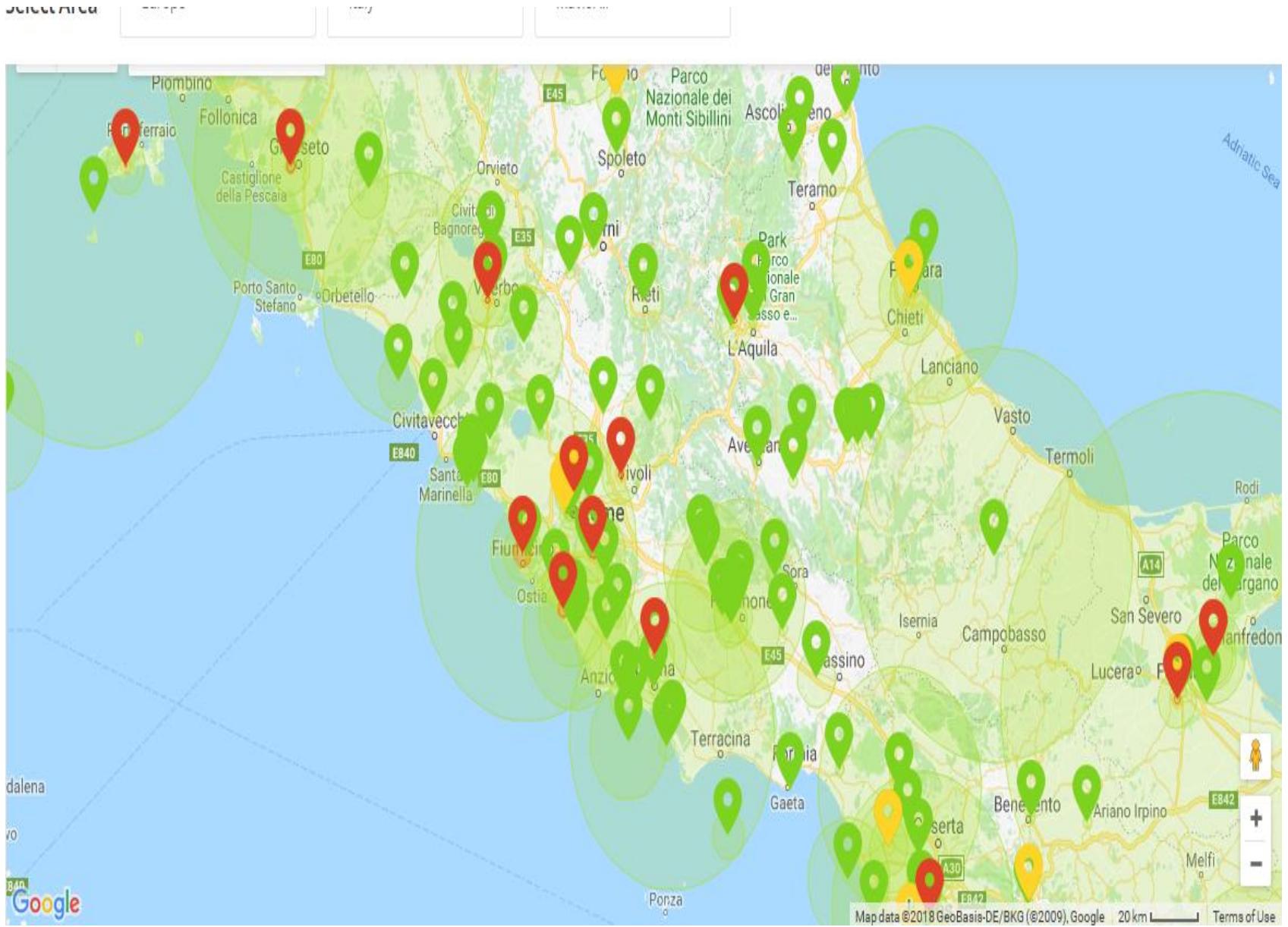




NFZ  
&  
Geofencing



# NFZ & Geofencing





DJI GO  
APP

/res/raw/flyforbid.json

```
"area_id":31681,  
"type":1,  
"shape":1,  
"lat":45.109444,  
"lng":7.641111,  
"radius":500,  
"warning":0,  
"level":2,  
"disable":0,  
"updated_at":1447945800,  
"begin_at":0,  
"end_at":0,  
"name":"Juventus Stadium",  
"country":380,  
"city":"Turin",  
"points":null
```

Restricted Zone: Flight not permitted

19 November 2015



DJI GO  
APP

/res/raw/upgrade\_config.json

```
{  
    "groupName": "GroundWifi",  
    "weight": 20,  
    "isCameraGroup": false,  
    "isSingleFile": true,  
    "upgradeMode": 0,  
    "devices": ["2700"],  
    "ftpDstFileName": "HG310.bin",  
    "ftpPwd": "Big~9China",  
    "ftpUrl": "192.168.1.1",  
    "ftpUsername": "root",  
    "pushDevice": 27  
}
```

# Road to Shell

- Now I have the password
- SSH & Telnet are filtered
- FTP is chrooted

Damn





Firmware

I tried to replace the firmware with a modified version but the firmware have some checksum mechanism.

Damn^2

Strings on .bin matching for common strings like: **password, private, key, ...**, **root** and so on looking for interesting stuff.

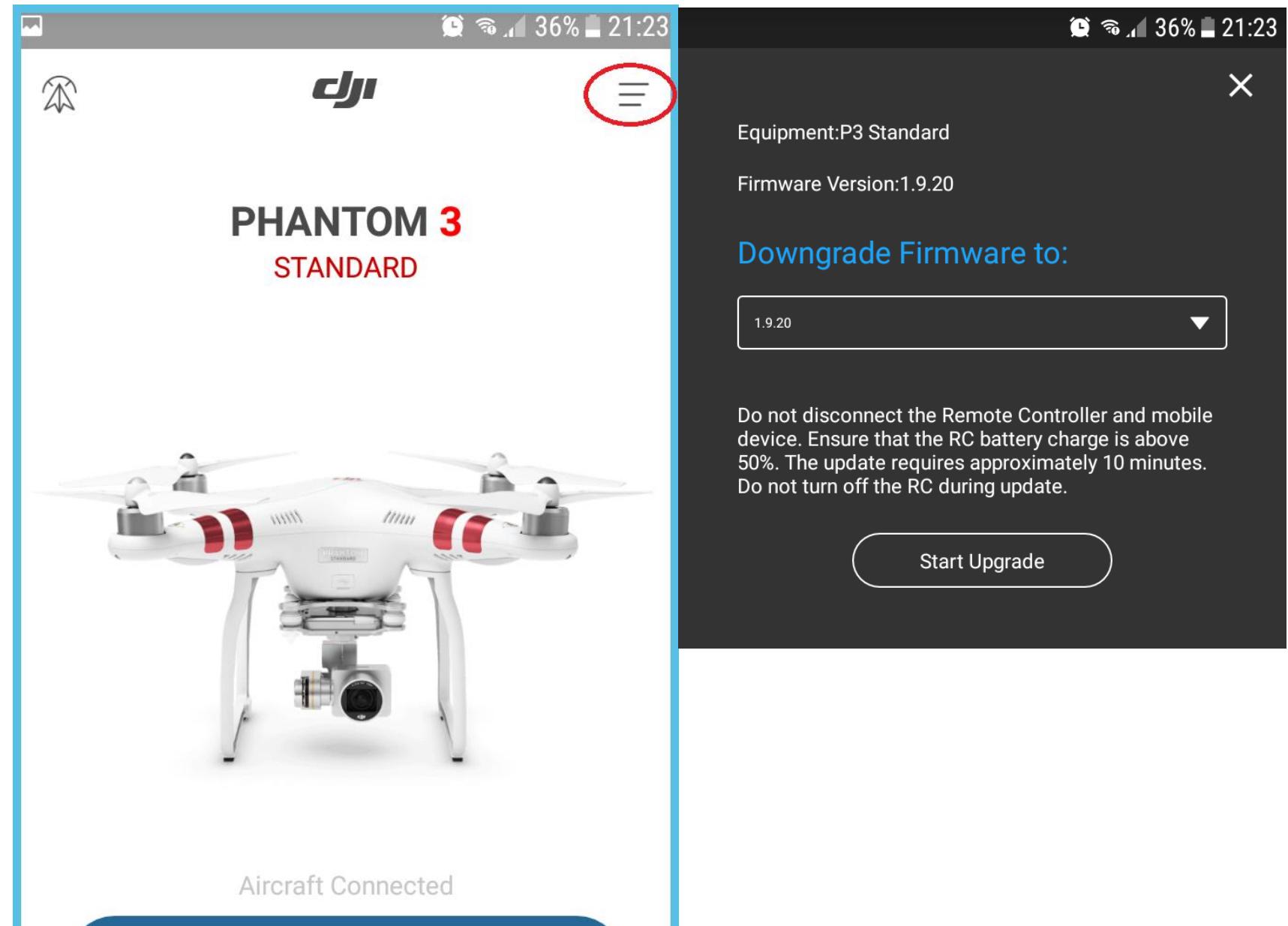
# Password Cracking

root:\$6\$zi2k1pqQ\$aYoxWoM9suJzq4xclz  
0Uh/sMBQxIrM7QzgpNH.UMrX6TAmBx3  
7jN0ygKlnpmHkgilWV5YzpfikkaylTWWo8  
RU0:16184:0:99999:7::: Big~9China

ftp:\$6\$Kt6U5MHk\$aCy81r9Wz49TlfDwSP  
Hkx8bEouNFdt0khJg7Pj1HOJtECe5.t9Kf  
NWOKKQXnyVqjd5whliLQGTQkXfB8p3rB  
X/:10933:0:99999:7::: admin999

default::10933:0:99999:7... none

# Firmware Downgrading





## Filesystem

```
/etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
```

The drone underlying system is a fork of **OpenWRT 14.07 Barrier Breaker**, built for “`ar71xx/generic`”, same version for the controller.



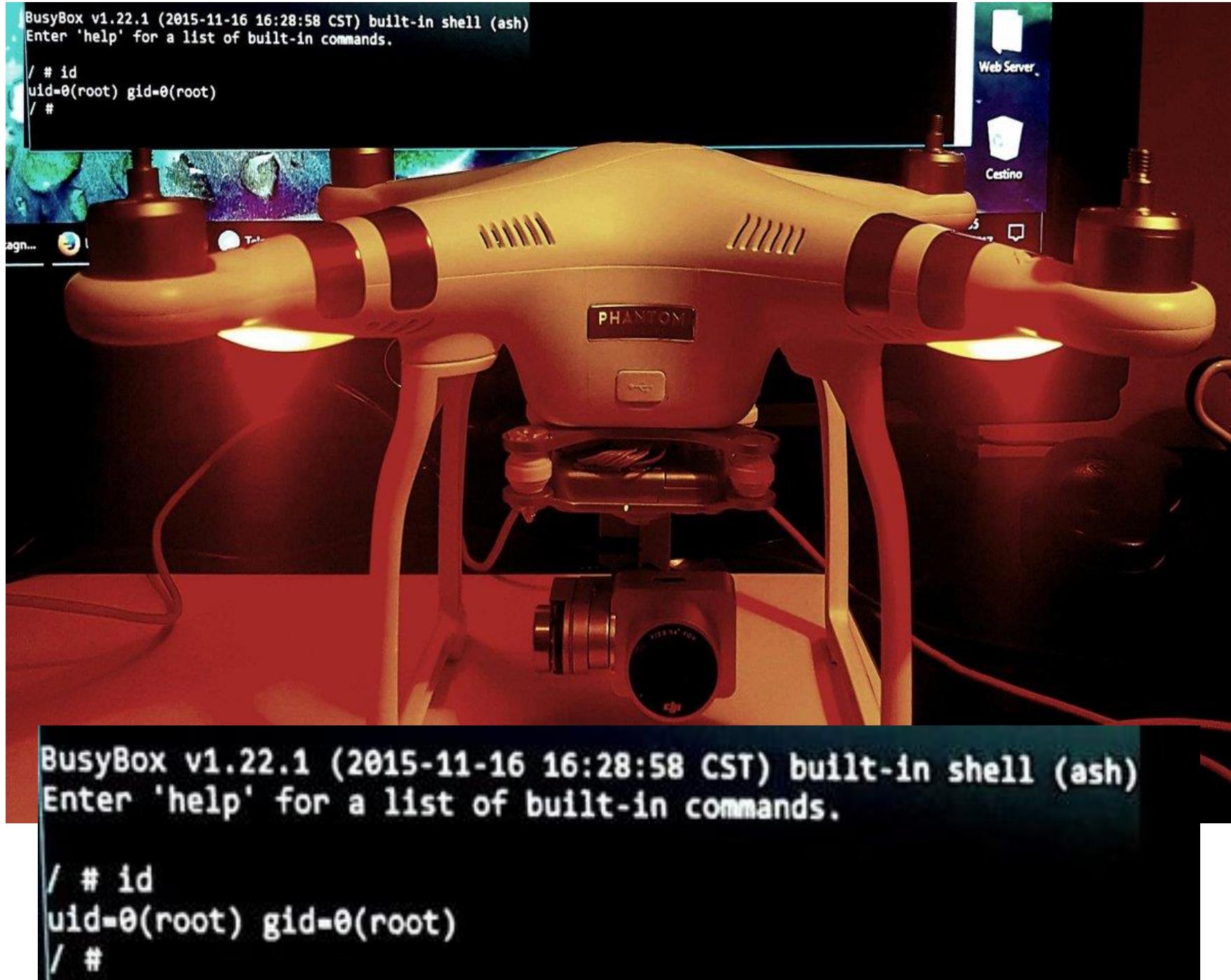
## Services

- **/etc/init.d/rcS**
- **/etc/init.d/rcS\_ap**
- **/etc/init.d/rcS\_aphand**
- **/etc/init.d/rcS\_cli**

These script runs during the **boot process**, adding this code will start the telnet server

```
telnetd -l /bin/ash &
```

# Shell Time





SDK

We can isolate specific instructions sent to the drone with Wireshark, we can implement a custom application that sends only very specific commands.

These commands could include changing the Wi-Fi password or even resetting the Wi-Fi connection.

This knowledge can be leveraged into a full drone takeover.

- DJI SDK Authentication Server
- DJI APP perform Activation Request

## Crack the SDK Authentication Mechanism



The screenshot shows a Java decompiler interface with two panes. The left pane displays a tree view of the class hierarchy under "dji-sdk.jar". The right pane shows the source code for the `DJISDKManager.class`.

```
private void checkPermission()
{
    SDK_LEVEL = 2;
}

private static boolean checkSdkConfigFileExist(Context paramContext)
{
    boolean bool = false;
    FileInputStream localFileInputStream = null;
    try
    {
        localFileInputStream = paramContext.openFileInput(SDK_CONFIG_FILE_NAME);
    }
    catch (FileNotFoundException localFileNotFoundException)
    {
        localFileInputStream = null;
    }
    if (localFileInputStream != null)
    {
        try
        {
            localFileInputStream.close();
        }
        catch (IOException localIOException)
        {
        }
    }
}
```

# Packet Structure

00000000	ff	.
00000001	55 0d 04 33 02 0e 01 00 40 00 01 40 d6	U..3.... @..@.
0000000E	55 0d 04 33 02 0e 02 00 40 09 0c 71 c7	U..3.... @..q.
0000001B	55 0e 04 66 02 1b a6 02 80 00 0e 00 6e a0	U..f.... ....n.
00000029	55 0d 04 33 02 0e 02 00 40 09 0c 71 c7	U..3.... @..q.
00000036	ff	.
00000037	55 0d 04 33 02 0e 03 00 40 09 0c 35 cc	U..3.... @..5.
00000044	55 0e 04 66 02 1b b3 02 80 00 0e 00 59 f6	U..f.... ....Y.
00000052	55 0d 04 33 02 0e 03 00 40 09 0c 35 cc	U..3.... @..5.
0000005F	ff	.
00000060	55 0d 04 33 02 0e 04 00 40 09 0c e9 fc	U..3.... @..
0000006D	55 0e 04 66 02 1b c0 02 80 00 0e 00 25 3f	U..f.... ....%?
0000007B	55 0d 04 33 02 0e 04 00 40 09 0c e9 fc	U..3.... @..
00000000	55 1a 04 b1 0e 02 92 14 00 06 05 00 04 00 04 00	U.....
00000010	04 00 04 00 04 00 17 00 aa 4f	..... .0
0000001A	55 24 04 40 1b 02 c1 02 00 07 01 02 4c 66 41 3f	U\$..@..... LfA?
0000002A	6b 86 d4 00 90 00 82 00 c0 ca 84 3a 9e db 00 1c	k.....
0000003A	00 3a 11 05	...:
0000003E	55 1a 04 b1 0e 02 93 14 00 06 05 00 04 00 04 00	U.....
0000004E	04 00 04 00 04 00 10 00 45 fa	..... E.
00000058	55 1a 04 b1 0e 02 94 14 00 06 05 00 04 00 04 00	U.....
00000068	04 00 04 00 04 00 10 00 d2 00	.....
00000072	55 1a 04 b1 0e 02 95 14 00 06 05 00 04 00 04 00	U.....
00000082	04 00 04 00 04 00 17 00 3d b5	..... =.
0000008C	55 0e 04 66 1b 02 c2 02 00 07 12 02 b0 8a	U..f....
0000009A	55 0e 04 66 1b 02 c3 02 00 07 09 64 92 f9	U..f.... d..
000000A8	55 1a 04 b1 0e 02 96 14 00 06 05 00 04 00 04 00	U.....
000000B8	04 00 04 00 04 00 10 00 0d f9	.....
000000C2	55 12 04 c7 0e 02 97 14 00 06 1e ad 0e 00 00 2a	U..... *
000000D2	6b 6c	k1
000000D4	55 1a 04 b1 0e 02 98 14 00 06 05 00 04 00 04 00	U.....
000000E4	04 00 04 00 04 00 10 00 32 04	..... 2.
000000EE	55 1a 04 b1 0e 02 99 14 00 06 05 00 04 00 04 00	U.....
000000FE	04 00 04 00 04 00 17 00 dd b1	.....
00000108	55 1a 04 b1 0e 02 9a 14 00 06 05 00 04 00 04 00	U.....
00000118	04 00 04 00 04 00 17 00 e5 b0	.....

## Packet Structure

# DJI Packet

HEADER  
(4 Byte)

PAYLOAD  
(variable length)

## Header Structure

Magic byte	Packet length	Version	Custom crc8
<b>0x55</b>	<b>0x0d</b>	<b>0x04</b>	<b>0x33</b>
0101 0101	0000 1101	0000 0100	0011 0011
85	13	4	51

## Payload Structure

Source Type	Target Type	Seq #	Flags	CMD	ID	Opt. bytes
02	06	4e00	40	06	12	540 b

01: Camera

02: App

03: Fly Controller

04: Gimbal

06: Remote Controller

00: general command

01: special command

02: set camera

03: set fly controller

04: set gimbal

05: set battery

06: set remote controller

07: set wifi

# GPS

- GPS signal for civilian usage is unencrypted.
- Replay Attack is the common GPS spoofing method.

Software: gps-sdr-sim

Hardware: HackRF One

Which functions are associated with GPS?

- No-fly zone
- Return to home
- Follow me
- Waypoint



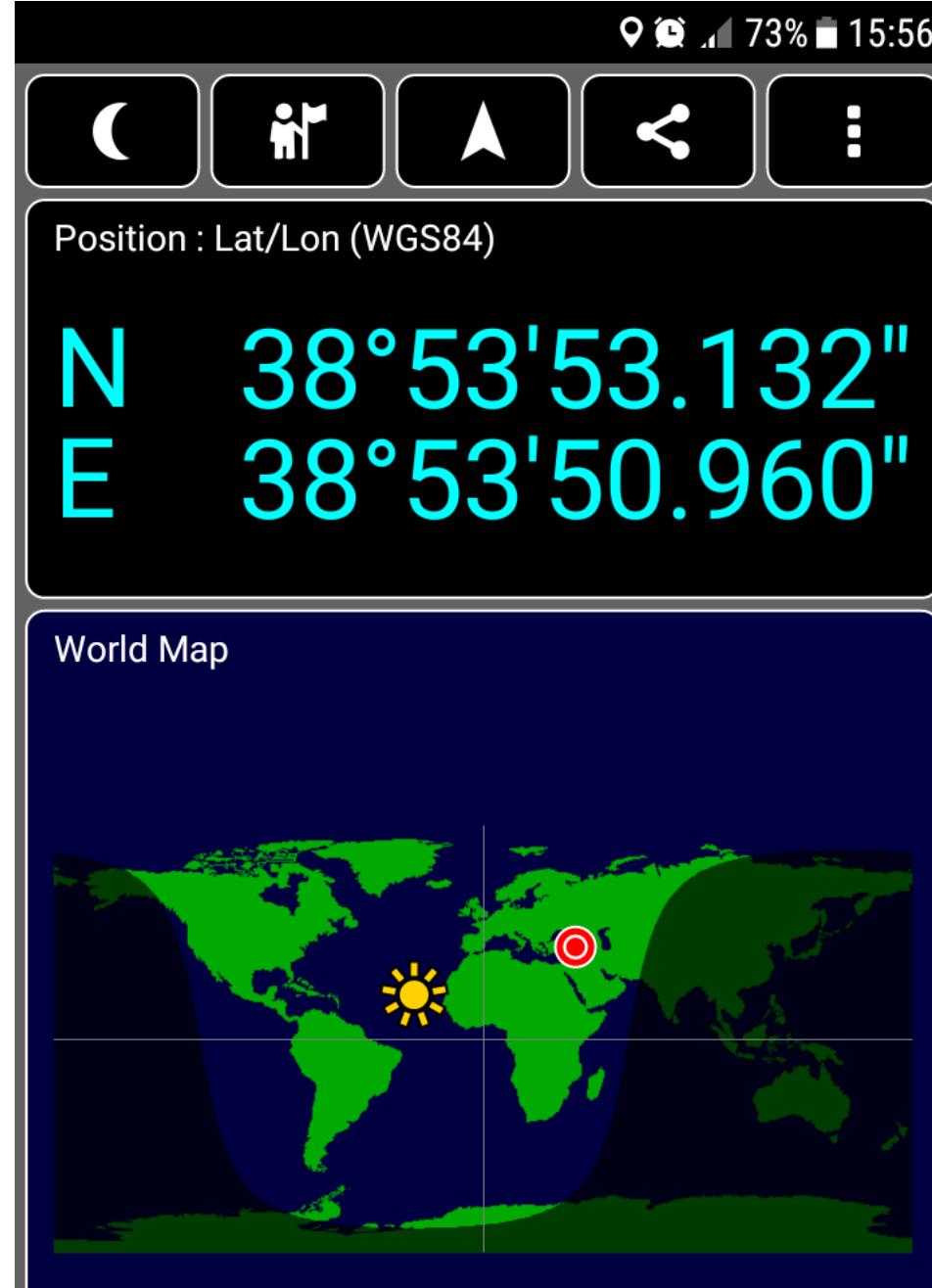
A circular logo with a black background and a white border. Inside the circle, the text "GPS 101" is written in a white, sans-serif font.

## GPS 101

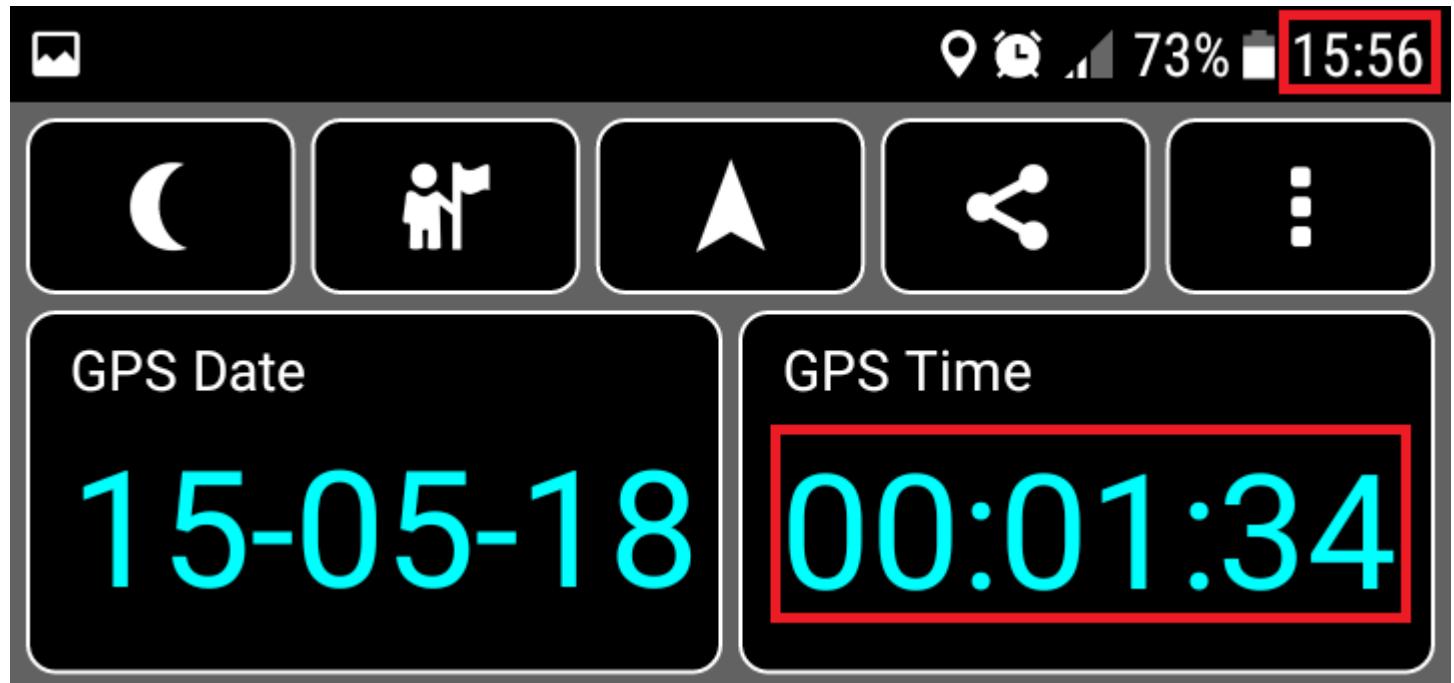
### Ephemeris Data

- GPS satellites transmit information about their location (current and predicted), timing and "health" via what is known as ephemeris data.
- This data is used by the GPS receivers to estimate location relative to the satellites and thus position on earth.
- Ephemeris data is considered good for up to 30 days (max).

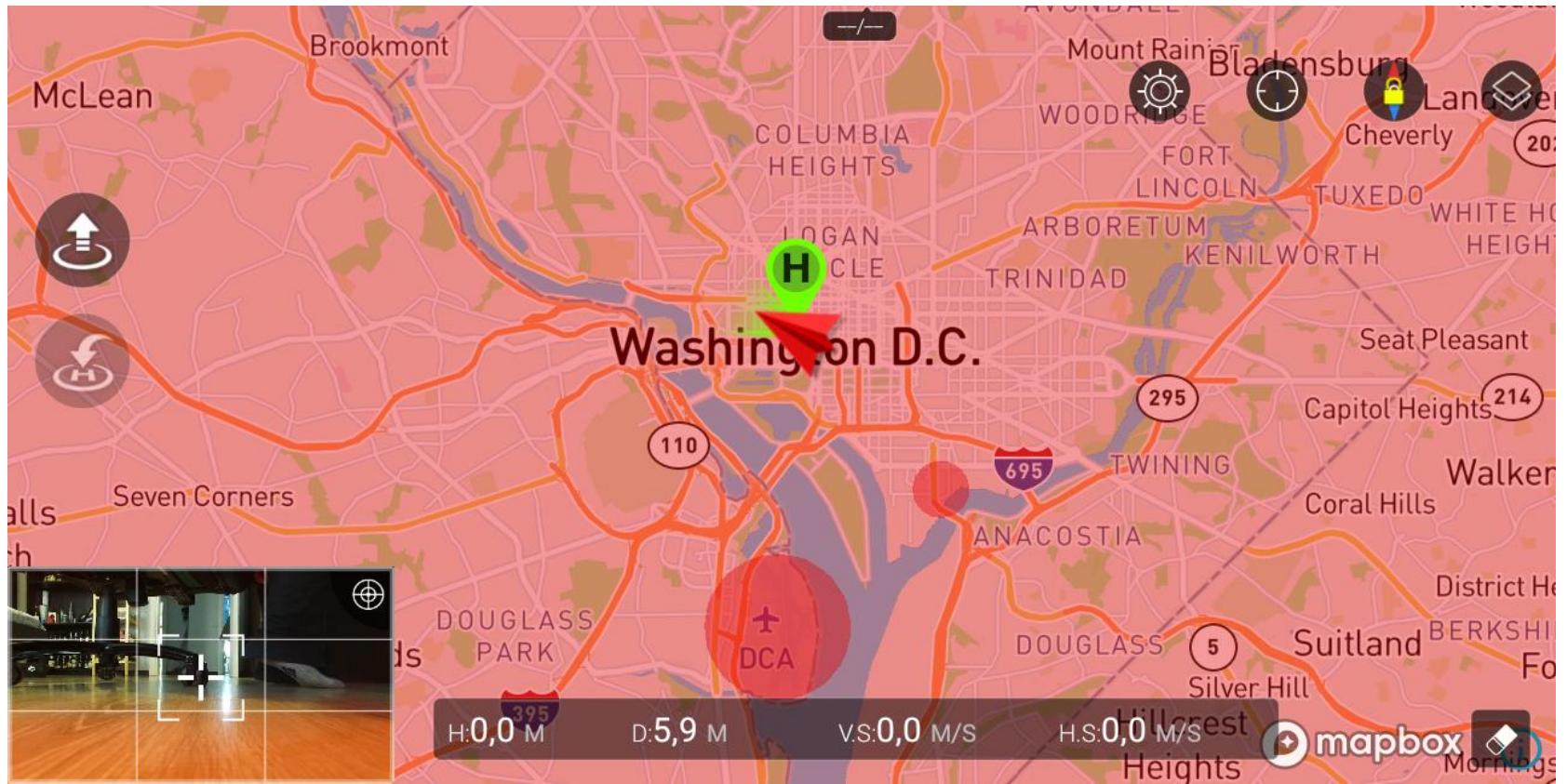
# GPS Replaying



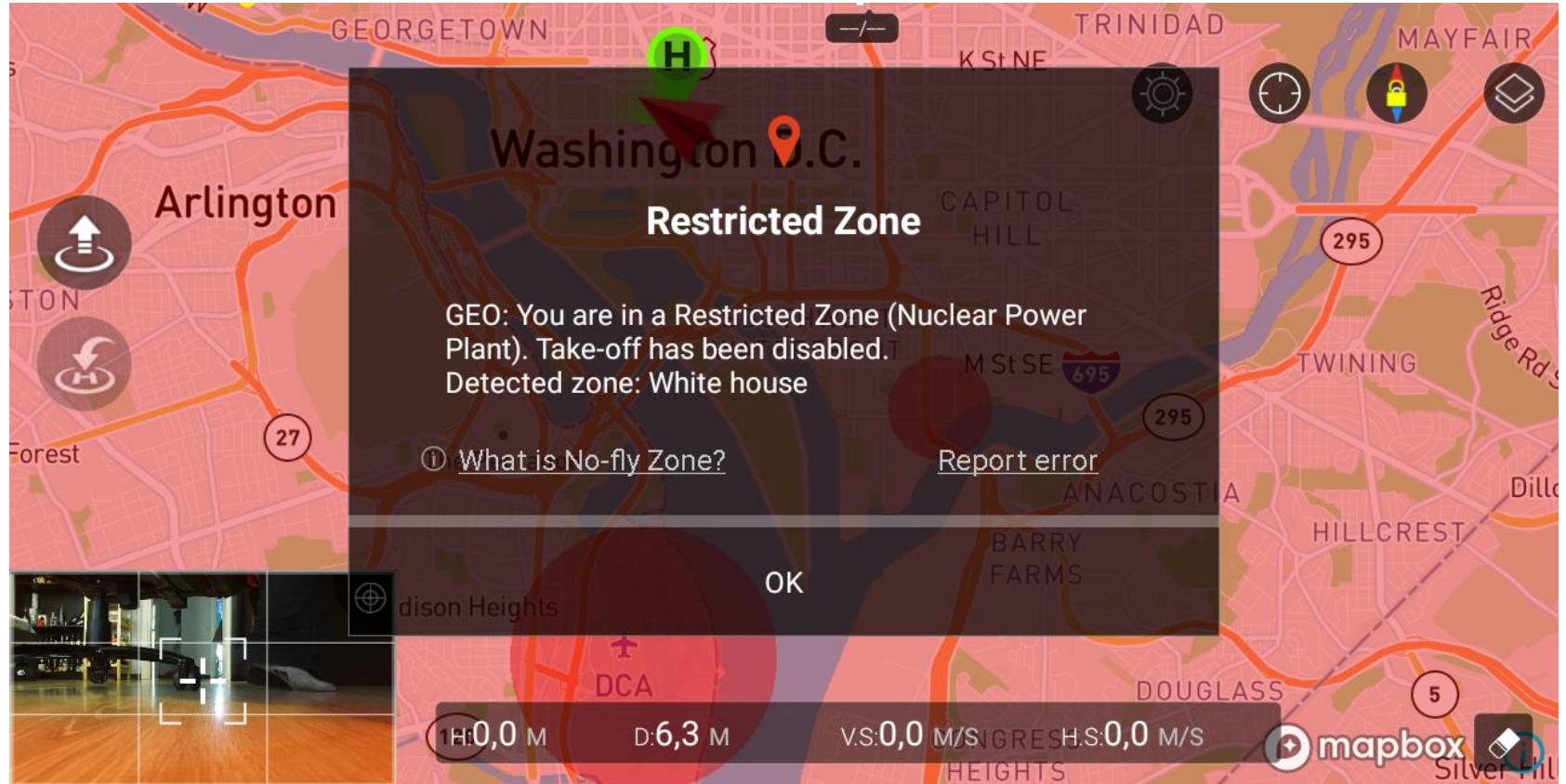
GPS  
Replaying



GPS  
NFZ



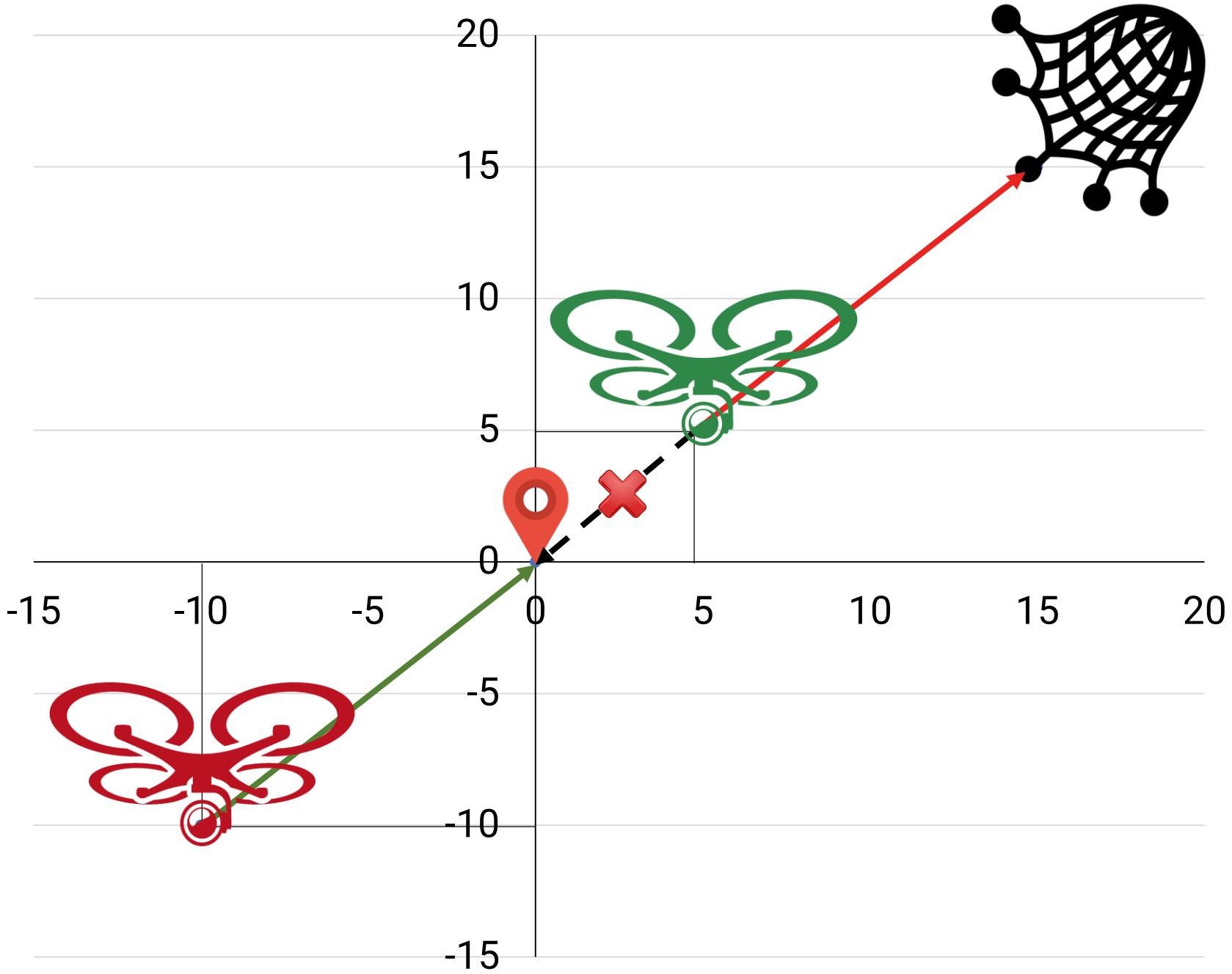
# GPS NFZ



PoC  
Time



# Drone Takeover



# Detect Fake GPS

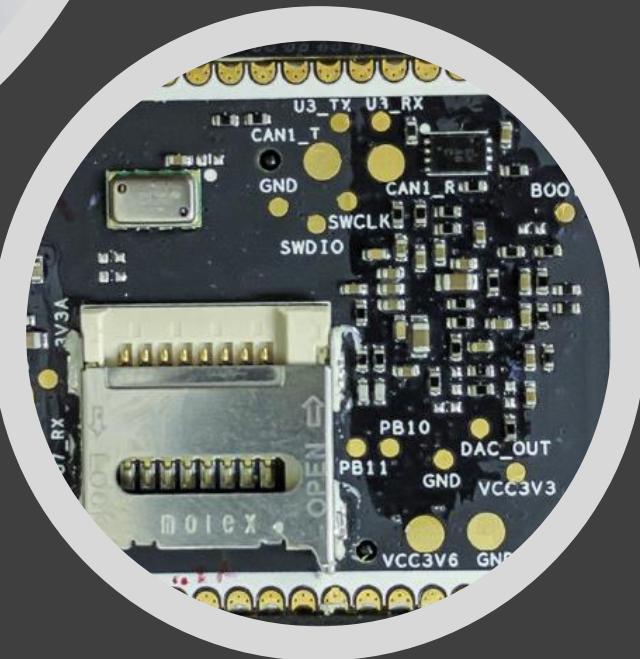
- Validate the GPS sub-frame
- Validate the time between satellite time and real time on device
- Check the speed between point to point

```
0f1a310f 10a675e7 3ef280f1 bb1f8dea 84ece851 83947364
b7bd0653 00138a30 037754bf 07228933 275b2251 bfea0f3c
24312bf8 0011095c 25c0aefa 85766c96 a6a1310c 3fe8d83a
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000
```

# Forensics

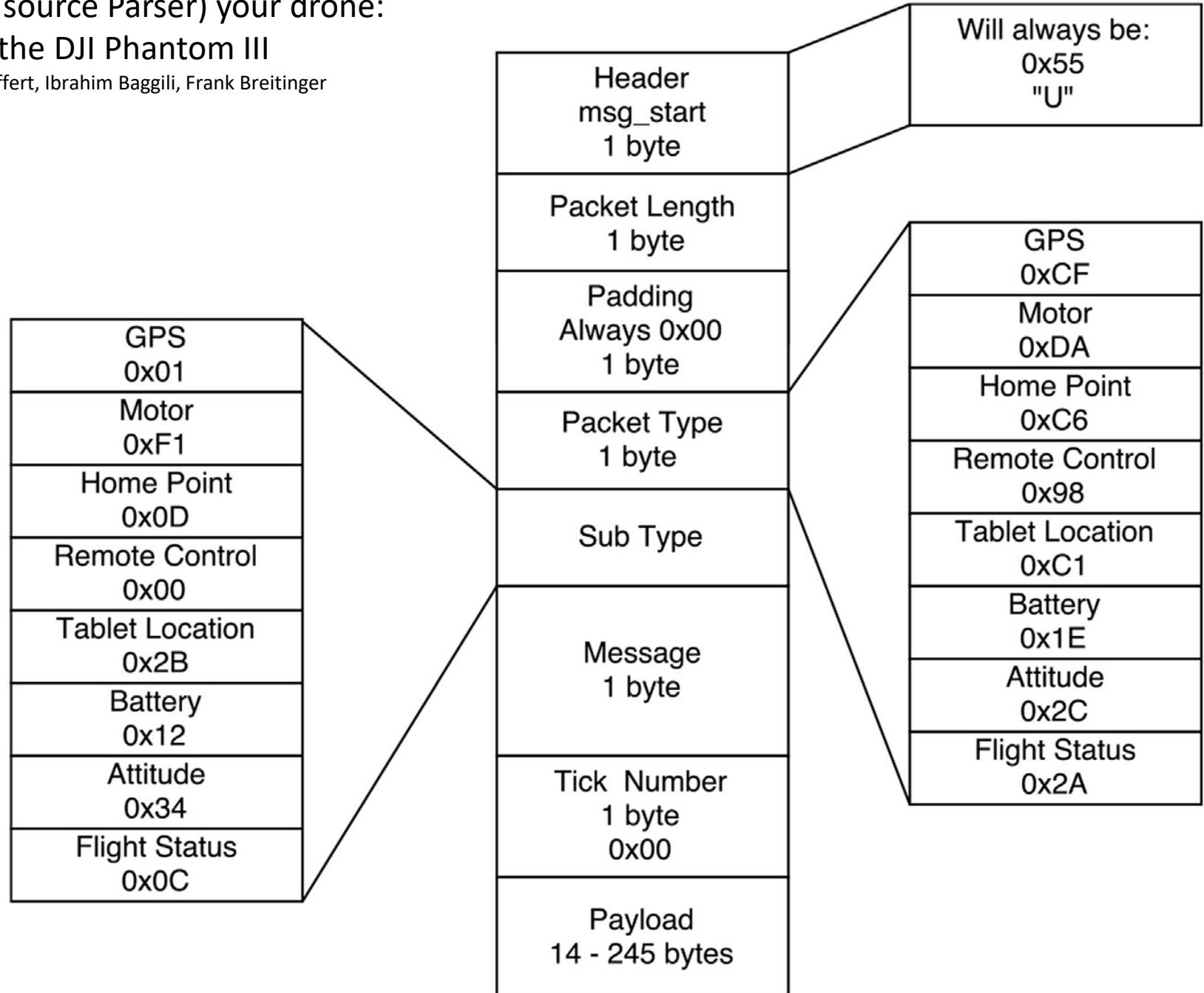
Two proprietary file formats:

- .dat file in non volatile memory
- .txt file on mobile device



# DAT Structure

DROP (DRone Open source Parser) your drone:  
Forensic analysis of the DJI Phantom III  
Devon R. Clark\*, Christopher Meffert, Ibrahim Baggili, Frank Breitinger





## Flight Data

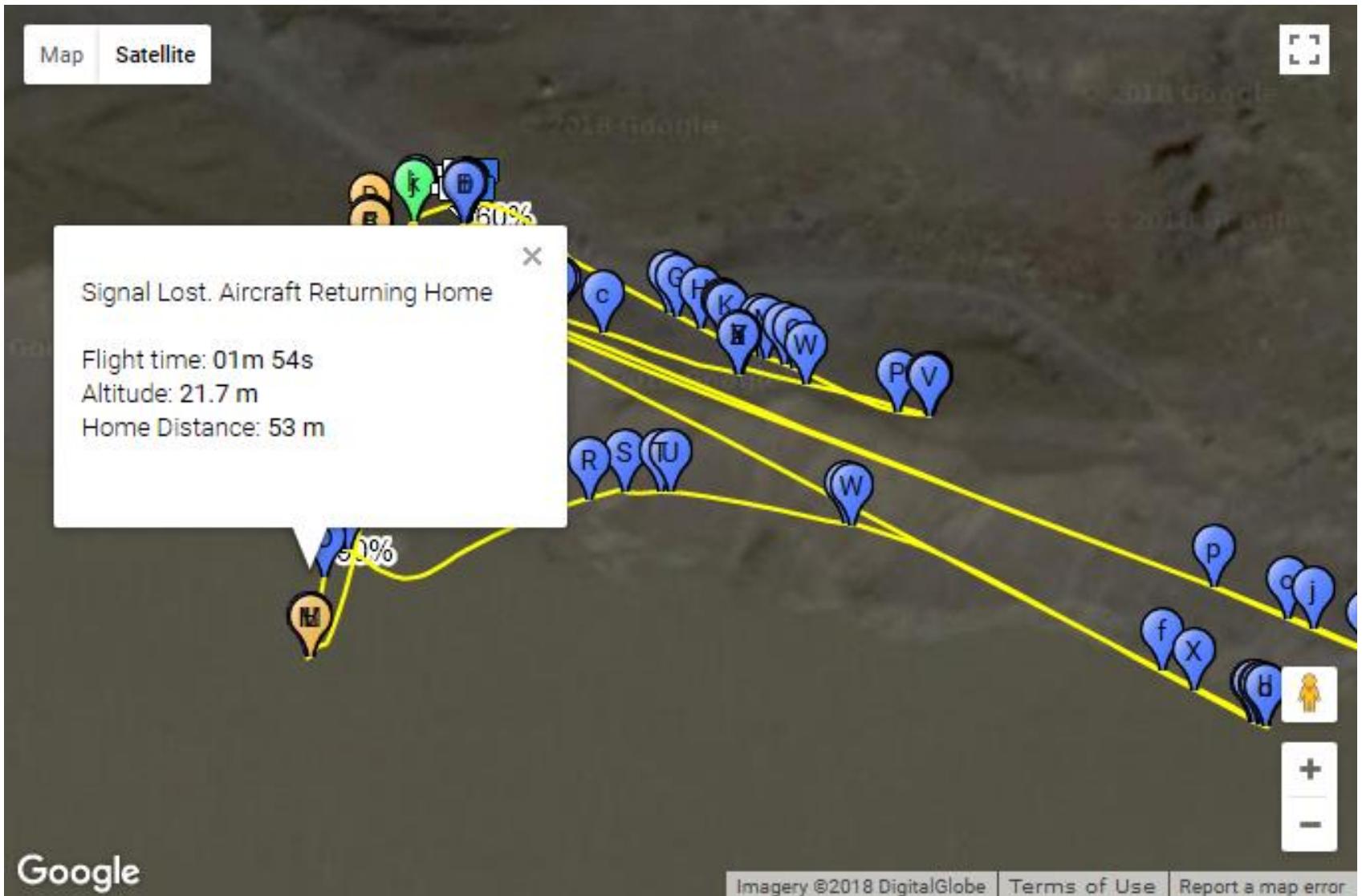
- Photos & Video (GEO Tagging)
- Flight Stats (compass, battery, etc)
- Autopilot Data
- GPS Data (location of drone)
- Pitch, roll and yaw of Gimbal & aircraft
- No-fly zones
- User email addresses
- Last known home point
- Device serial number

# Flight Data

Apr 17th, 2016 01:13PM [Edit](#)



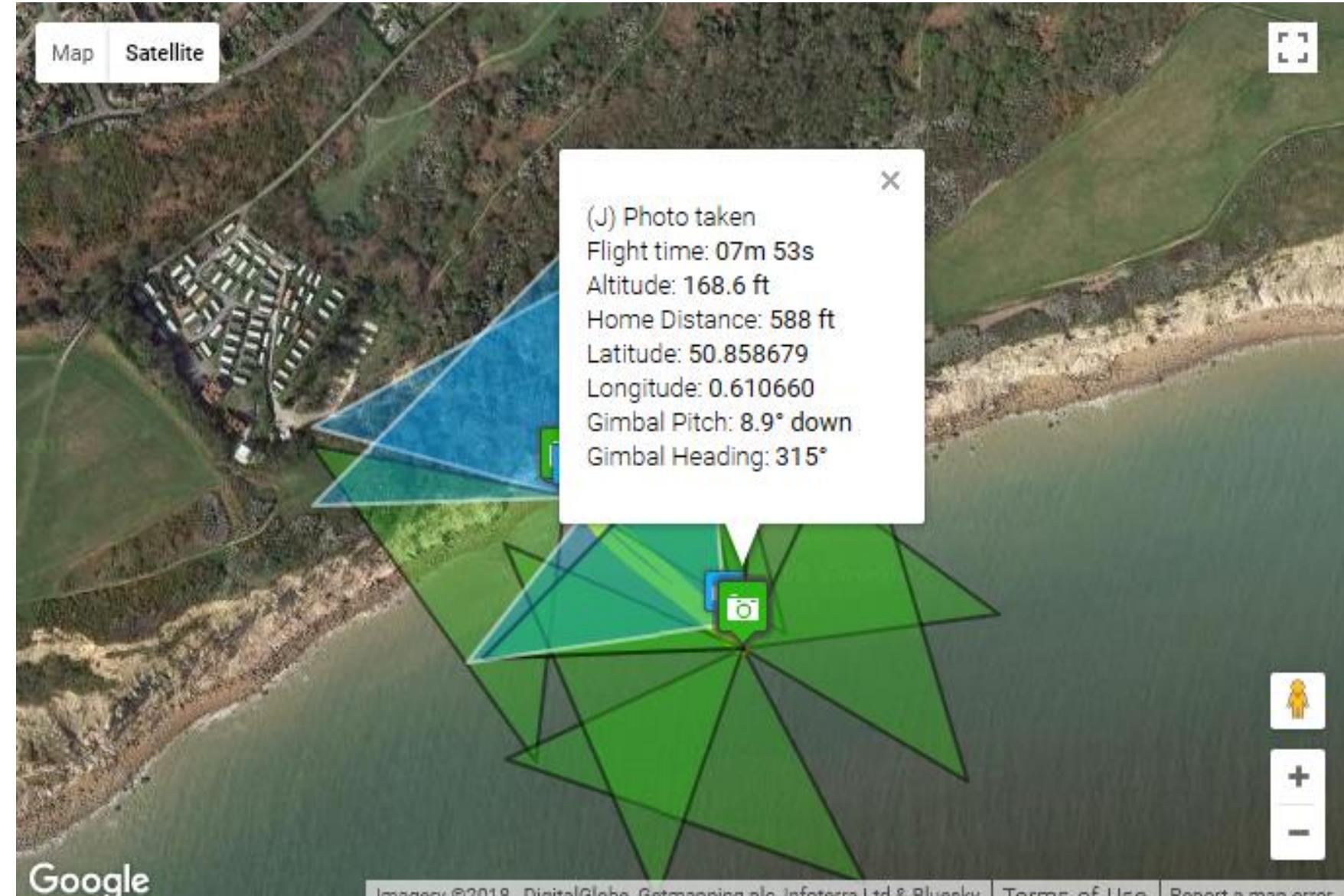
# Flight Data



# Flight Data

	Flight time	Altitude	Home Distance	Type	Notification
A	00m 00s	0.0 m	0 m	Mode	<a href="#">Mode changed to GPS Atti</a>
B	00m 00s	0.0 m	0 m	Tip	<a href="#">Setting new Return-To-Home altitude to 30m (98 ft)</a>
C	00m 02s	-0.3 m	0 m	Mode	<a href="#">Mode changed to Assisted Takeoff</a>
D	00m 02s	-0.3 m	0 m	Warning	<a href="#">Battery temperature is below 15 degrees Celsius. Warm up the battery temperature to above 25 degree Celsius to ensure a safe flight.</a>
E	00m 02s	-0.3 m	0 m	Warning	<a href="#">Return-to-Home Altitude:30M</a>
F	00m 21s	0.2 m	0 m	Tip	<a href="#">Setting new Return-To-Home altitude to 40m (131 ft)</a>
G	00m 28s	-0.3 m	0 m	Mode	<a href="#">Mode changed to GPS Atti</a>
H	01m 24s	21.8 m	53 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
I	01m 24s	21.8 m	53 m	Mode	<a href="#">Mode changed to GPS Atti</a>
J	01m 29s	21.6 m	53 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
K	01m 32s	21.5 m	53 m	Mode	<a href="#">Mode changed to GPS Atti</a>
L	01m 51s	21.6 m	53 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
M	01m 54s	21.7 m	53 m	Warning	<a href="#">Signal Lost. Aircraft Returning Home</a>
N	01m 54s	21.6 m	53 m	Mode	<a href="#">Mode changed to Go Home</a>
O	02m 10s	39.2 m	42 m	Mode	<a href="#">Mode changed to GPS Atti</a>
	02m 17s	39.0 m	37 m	 <span style="width: 20%;">90% Battery</span>	<a href="#">90% Battery</a>
P	02m 27s	39.6 m	38 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
Q	02m 27s	39.6 m	38 m	Mode	<a href="#">Mode changed to GPS Atti</a>
R	02m 37s	39.3 m	43 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
S	02m 39s	39.4 m	45 m	Mode	<a href="#">Mode changed to GPS Atti</a>
T	02m 42s	39.6 m	49 m	Mode	<a href="#">Mode changed to WiFi Reconnect</a>
U	02m 42s	39.6 m	50 m	Mode	<a href="#">Mode changed to GPS Atti</a>

# Flight Data



# Sharing Data

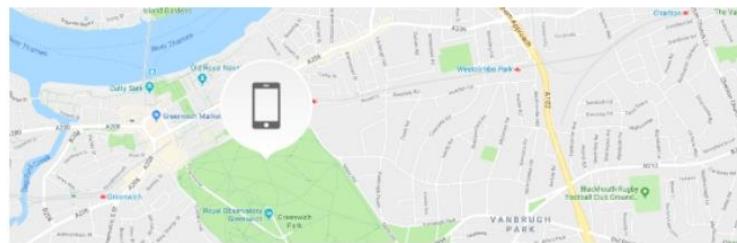
## Authorize DJI To Access Your Information

You can set whether to allow DJI to access your personal information below. DJI strictly follows the DJI Privacy Policy to access and process your information. **Some features may not function if you deny DJI's access.** You can change information access authorization in the APP's Settings page.

### Mobile Device GPS Information



GPS information of the mobile device running the App. Denying DJI access to this information will cause the following features no longer function:  
Find My Drone, Map in Camera View.



### DJI Device Hardware Information



Information of DJI device that is paired with the App, including serial numbers of the main control, gimbal, camera and battery. Denying DJI access to this information will cause the following features no longer function:  
Unlock restriction zone application, flight record update, device activation.

### Approximate location



Location information after reducing accuracy (reduce accuracy to 5-10 km radius) of DJI device and mobile device GPS information. It is used to ensure the normal operation of the restricted area, and also ensure flight safety.

Denying DJI access to this information will cause the App cannot provide you services.

### DJI Device GPS Information



GPS information of the DJI device that is paired with the App. Denying DJI access to this information will cause the following features no longer function:  
Find My Drone, Map in Camera View, Location in Gallery.





## Lost & Found

- Images have no checksum mechanism.
- We can show wrong images to the controller.
- Compass e Magnetic fields (Compass Calibration)



## Defenses

- Drone netting
- Drone shooting
- Jamming
- EMP
- Cyber
- Geofencing & NFZ
- Laser
- Missile

# Drone Netting



Predator  
Bird



Confetti  
Gun



Jet  
Ski



# A US ally shot down a \$200 drone with a \$3 million Patriot missile

*This will be a bigger problem as more drones show up on the battlefield*

By Andrew Liptak | [@AndrewLiptak](#) | Mar 16, 2017, 10:13am EDT

f [t](#) [e](#) SHARE



Photo by Sean Gallup/Getty Images

Defenses

[Ref.](#)

# News

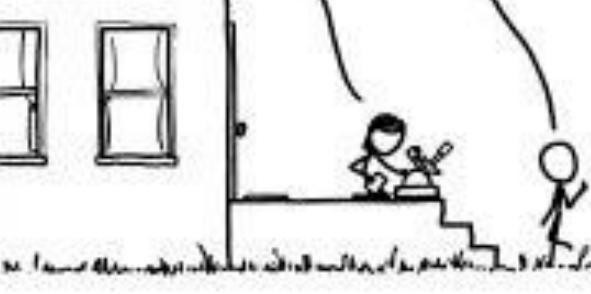
At least 140,000 passengers on 1000 flights have faced disruption

Gatwick's December Drone Closure Cost Airlines \$64.5 million



PEOPLE IN THE PARK KEEP FLYING DRONES NEAR ME, SO I'VE BUILT A SYSTEM TO SHOOT THEM DOWN.

COOL! OH YEAH,  
THERE'S ONE NOW.  
TIME FOR A TEST!



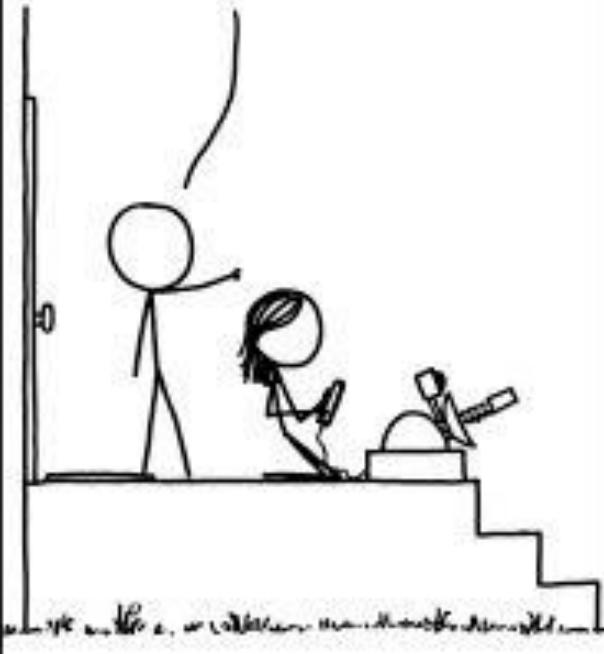
OKAY, LOCKING ON...

WAIT, IT JUST  
CRASHED.

DAMN.



HERE COMES ANOTHER ONE! AIM FOR... NOPE, IT GOT STUCK IN A TREE.



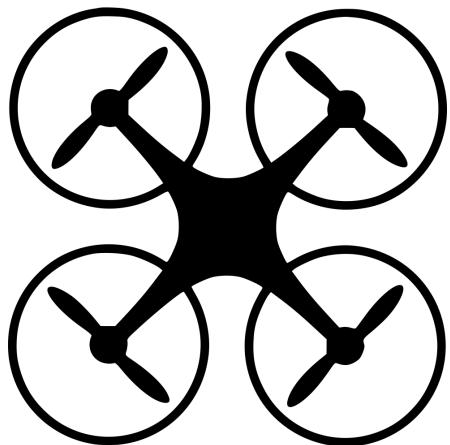
THREE HOURS LATER...

FINALLY, TWO MORE JUST-  
NO, ONE CRASHED AND THE  
OTHER IS HURTLED SIDEWAYS  
TOWARD THE LAKE.

WILL YOU PEOPLE LEARN  
TO FLY THESE THINGS?!



## Further Work



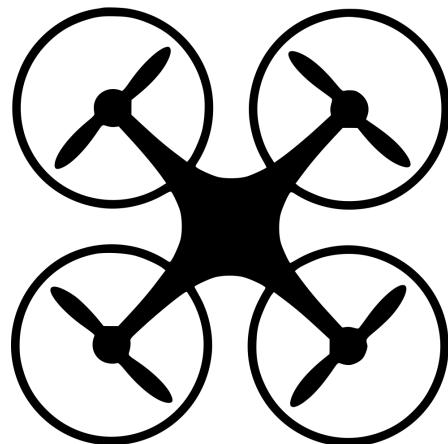
- Full Network protocol analysis, maybe build a ground station the through SDK
- Binaries and services analysis and vulnerabilities research
- Finding some cool exploits
- Play with something more complex

## Further Work

- **AUDS Anti-UAV Defence System**
  - eg. DJI AeroScope, Skylock Anti Drone and so on...



## Previous Work & References



- [DJI Phantom 3](#)
- [DROP \(DRone Open source Parser\)](#)
- [dronesec.xyz](#)
- [How Can Drones Be Hacked?](#)
- Defcon/Black Hat Drone/UAV Talks
- [Drone vs Patriot](#)
- [GPS Spoofing](#)
- [Hak5 Parrot AR](#)
- [Skyjack](#)
- [Maldrone](#)
- [airdata.com](#)
- [DJI CRC16](#)
- [dex2jar](#)
- [Jadx](#)
- [JD-GUI](#)
- [GPS-SDR-SIM](#)
- [GPSpoof](#)
- [DJI No Fly Zone](#)
- [DJI AeroScope](#)
- [Skylock](#)

# FAQ Time

Paolo Stagno  
voidsec@voidsec.com  
voidsec.com



"Some things in life are unpredictable,  
your Security does not have to be one of them"