## Internal SD Card [8]

A drawing of a machine

Description automatically generated with low confidence

Internal SD card contains:

* 12 encrypted FLYXXX.DAT files.
* 1 SYS.DJI file containing 13 bytes of data.
* 1 PARM.LOG file that shows the FLYXXX.DAT files being created.

Analysis of DAT files:

For some reason many of the DAT files are missing lots of GPS data. Only 3 of the 12 files have no missing GPS data. These 3 DAT files are:

FLY007.DAT, FLY008.DAT, FLY009.DAT.

FLY00X (0, 1, 2, 3) are only missing a vey small percentage of coordinates but many timestamps and height data is missing.

The remaining FLY0XX (4, 5, 6, 10, 11, 12) are missing almost all GPS data and the some of the coordinates change in a way that is infeasible for a drone.

Comparing the videos stored on the external SD card to the GPS data and satellite imagery, FLY00X (7, 8, 9) are the best matches to the videos taken.

## External SD Card

A picture containing transport

Description automatically generated

The external SD card contains 8 videos taken on the drone, 2 log files and 4 octet-streams.

A log file named WM620\_FW\_LOG\_AB.txt, this contains information about firmware that has been downloaded / upgraded.

The first 5 entries time stamps specify 01/01/2000.

After this the time stamps are updated to 28/08/2017

Last upgrade was to version: loader [01.01.1418], firmware [01.06.1582].

The other log file found was CameraLogCur.log.

There is some SD formatting feedback, we can tell what some of the directories are from this:

[0m[00174086][CA9\_0] [MovMux] [DjiMovMuxPriDirExistChk-2015]the private dir is:C:\MISC

[0m[00174086][CA9\_0] [MovMux] [DjiMovMuxPriDirExistChk-2025]the repair dir is:C\IDX

[0m[00174086][CA9\_0] [MovMux] [DjiMovMuxPriDirExistChk-2034]the thumbnail dir is:C\THM

[0m[00174086][CA9\_0] [MovMux] [DjiMovMuxPriDirExistChk-2043]the Log dir is:C\LOG

[0m[00174086][CA9\_0] [MovMux] [DjiMovMuxPriDirExistChk-2052]the Xcode dir is:C\XCODE

Camera events are recorded in this log file.

[0m[00181394][CA9\_0] ===[DJI\_AVENC] AVENC\_VideoTaskEntry[L1031]: Video(1) total encoded 25465(5093), size 66993302, Duration = 169908 ms

[0m[00181394][CA9\_0] ===[DJI\_RLV] RLV\_ProcData[L1238]: recv EOS & return directly

[0m[00181394][CA9\_0] [FSM State] New bind: PostpState: 0, VprocState: 2

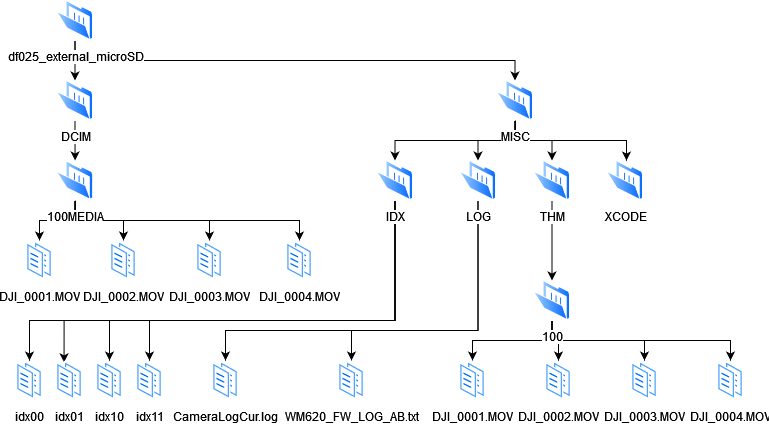
[0m[00181394][CA9\_0] ===[DJI\_AVENC] AVENC\_VideoTaskEntry[L999]: Video(1) Recv tsk stop req, send tsk stop ack

[0m[00181394][CA9\_0] ===[DJI\_AVENC] AVENC\_VideoStop[L799]: Video(1) Duration 169908, encoded 25465(5093), fps 149(29)

[0m[00181394][CA9\_0] DjiTaskDelete[L225]: success to destroy DjiVideo\_2nd task

The 4 idx files present in the IDX folder are not important and do not contain any relevant information.

External SD card file structure:



The videos stored in DCIM contain the camera model used during the flight.

For all 4 videos taken, the bytes at offset 38 – 3D contain FC6510 which corresponds to the DJI Zenmuse X4S camera.

## Android dd

A large number of artifacts can be found on the connected mobile device:

data/dji.go.v4/app\_data/config/rfg\_key.pem : encrypted private key

The inspire 2 uses “here maps” which creates the following file:

[media/0/.here-maps/uniqueDeviceId.txt] – unique 36-byte string:

319a2272-e898-43a5-8ff7-cd40f21e9277

[data/dji.go.v4/files/.here-maps/uniqueUserId.txt] – unique 36-byte string:

45c6ba33-08cb-4a15-8a21-b13d10ce4cbd

Various images can be found in: [/media/0/DJI/dji.go.v4/CACHE\_IMAGE/]

Videos can be found in: [/media/0/DJI/dji.go.v4/DJI\_RECORD/], for each video there is a corresponding info file that contains data about that flight.

#Tue Aug 29 13:23:55 MDT 2017

CameraType=14

Source\_File\_Path=/storage/emulated/0/DJI/dji.go.v4/DJI\_RECORD/2017\_08\_29\_13\_18\_01.mp4

FPS\_Drone=30

EndTimeMsec=215566

LocalFileName=2017\_08\_29\_13\_18\_01

StartTimeMsec=0

FolderID\_Drone=100

WhiteBalance=0

ImageDescription=

Is\_HD=false

ISO=0

PixelXDimension\_Drone=3840

PixelYDimension\_Local=720

Video\_Type=0

ExposureMode=1

PixelXDimension\_Local=1280

Sync\_Drone\_Time=7739,10243,13166,17484,22828,28293,32599,36034,40358,45841,50535,55214,59855,63959,68522,73740,78836,84197,86647,90039,92968,96905,99662,102338,104825,106996,110468,113223,117175,121175,125314,131002,135925,139527,143519,146677,151497,155151,158650,162680,166987,172283,176312,179887,182363,186269,189288,193734,197827,201572,205188,207399,209901,213518,217348,220554,224732,228851,231399,233505,235970,238332,240760,244560,248691,251438,256806,259160,263279,265891,269138,271503,275080,278610,282589,284844,287577,290020,293200,297016,298884,301920,306275,309728,313035,315368,319290,323430,326604,329867,332365,335430,338034,342211,344462

Version=1.0

Video\_Resolution\_Enum\_Drone=16

FPS\_local=30

CaptureDate=2017/08/29 13\:18\:01

UUID\_Drone=442776886

File\_Source\_Type=1

FileID\_Drone=4

ProductType=17

LocationString=

PositionRelativeAlt=0.0

PositionGPSLat=39.961195212421835

FrameJumpped=67

ApertureSize=630

PixelYDimension\_Drone=2160

Sync\_Local\_Time=0,1133,2633,5799,9799,13599,16766,19066,21866,25899,29199,32799,35899,38699,42033,45666,49466,53699,54733,56666,58466,60999,62033,63599,64666,65833,67933,69633,72166,74533,76933,80866,84533,87099,89633,91733,95266,97666,99733,102666,105466,109433,112399,114933,116266,118599,120599,123566,125899,128466,130966,132166,133199,135333,137866,139799,142166,144733,146199,147266,148466,149799,150799,153333,156033,157466,161533,162766,165866,167133,169199,170533,172499,174699,177099,178299,179799,181233,183099,185599,186166,187966,190433,192799,194433,195633,198366,200933,202766,204799,206099,207999,209599,212099,213299

ShutterSpeed=0

DeviceMaker=DJI

PositionGPSAlt=0.0

PositionGPSLng=-106.21639911173384

3 encrypted FLYXXX.DAT files [/media/0/DJI/dji.go.v4/FlightRecord/MCDatFlightRecords/]

Large number of log files in Location: [/media/0/DJI/dji.go.v4/LOG/CACHE/], many of these can be useful as we can see when the UAV was connected / disconnected.

[media/0/DJI/dji.go.v4/LOG/ERROR\_POP\_LOG/] contains useful files that show us when components on the UAV are used.

## 13:17:53

Strong wireless interference. Please fly with caution.

## 13:18:11

Strong wireless interference. Please fly with caution.

## 13:18:11 Obstacle Avoidance Disabled.

Landing gear lowered. Obstacle Avoidance Disabled.

## 13:18:12

Landing Gear Raising

## 13:18:19

Landing Gear Raised

## 13:18:21

Motors Started

## 13:21:44

Strong wireless interference. Please fly with caution.

## 13:22:56

Strong wireless interference. Please fly with caution.

## 13:23:03

Landing Gear Lowering

## 13:23:09

Landing Gear Lowered

[media/0/DJI/dji.go.v4/LOG/MAP/] Various log files are saved here. If a home marker is set, it is in one of these files.

2017-08-29 13:17:45:addHomeMarker: wsg=lat/lng: (39.96120292202613,-106.21639890802577) altitude=0.0 accuracy=0.0, gcj=lat/lng: (39.961203,-106.216399)

## IOS

Graphical user interface

Description automatically generated with medium confidence

IOS backup files are also provided.

To read IOS backup files the “Manifest.db” must be found first, it should be the in the highest directory. IOS uses SQLite, I will be using DB Browser to load the file. To sort the data, in the domain “dji” is used and the flag is set to show only 1s.

Flags:

1 = File

2 = Folder

4 = Unknown

Graphical user interface, text, application

Description automatically generated

It is much easier to find important files this way.

Here a flight record is found, to find this file in the IOS backup file structure look at the first 2 bytes in the file ID. The first 2 bytes for this record are “a5”.

Graphical user interface

Description automatically generated with low confidence

The encrypted flight log can be found here:

Graphical user interface, text, application, email

Description automatically generated

Each flight will create various files:

Graphical user interface, text, application, email

Description automatically generated

.rec is a plist file which can be read using proper tree <https://github.com/corpnewt/ProperTree> , it contains some timestamps and the model of drone.

Mp4 file can be extracted, .mp4 must be added to the end of the file to view it.

The infoV2 file is encrypted?