

Drone Forensics with Public Data Set

Objectives

- Perform forensics with public drone data set from the CFReDS project.
- Get flight data such as GPS location, time, battery information, error logs, and number of flights.

Task

Task 1. Download Software and Data Set

1. Open the CFReDS project website to download the provided public data set. Click DF001 or DF002 or DF003 to download the data set folder. (Please note, in this module, we will only analysis the DJI Phantom 3 model and the data set that this module is using is DF001.) <https://cfreds-archive.nist.gov/drone-images.html>

Drone Images

Drone Reference Number	Drone Make	Drone Model
DF001	DJI	Phantom 3
DF002	DJI	Phantom 3
DF003	DJI	Phantom 3

After clicking DF001, you will be directed to a Google drive, click 2018_June folder and download two folders, “flight-logs” and “mobile_android”. Note: Open the mobile_android folder to download the “Media01” folder.

The screenshot shows the Google Drive interface. At the top, there's a search bar and a navigation sidebar on the left with options like 'New', 'My Drive', 'Computers', 'Shared with me', 'Recent', and 'Starred'. The main area shows a breadcrumb path: 'Shared with me > df001_DJI_Phantom_3'. Under 'Folders', there are two folders: '2017_June' and '2018_June'. The '2018_June' folder is selected. Below this, another breadcrumb path is shown: 'Shared with me > df001_DJI_Phantom_3 > 2018_June'. Under 'Folders', there are three folders: 'flight_logs', 'mobile_android', and 'mobile_iOS'. The 'mobile_android' folder is highlighted. Below the folders, there's a 'Files' section showing three files, each with a blue document icon and the name 'README_DF001_Dron...'.

2. Download Software

Open website <https://datfile.net/CsvView/downloads.html> to download software CsvView.

[Home](#)
[Documentation](#)
CsvView
[Introduction](#)
[Downloads](#)

DatCon
[Introduction](#)
[Downloads](#)
[Retrieve .DAT P3/Inspire 1](#)
[Retrieve V3 .DAT from AC](#)
[Retrieve V3 .DAT from Tablet](#)
[.CSV column descriptions P3/Inspire 1](#)
[.CSV column descriptions V3 .DAT](#)

DatCon3 Intro

CsvView Downloads

CsvView PC

Beta	CsvView_Version_4.2.6	11/3/2022
	CsvView_Version_4.2.5	11/25/2021
	CsvView_Version_4.2.1	5/14/2021

CsvView Linux/Mac

The following downloads contain the .jar files that can be run directly on a non-Windows systems such as a Mac iOS or Linux system. Although they have been tested on a Windows sytem they have not been tested on either iOS or Linux. They are not supported on either iOS or Linux. They are provided as a convenience for those that find them useful.

Some iOS users have been unable to resolve issues encountered when using a .jar directly. Many of these users have since switched to installing the CsvView PC download package on a VM such as Bootcamp. Others have switched entirely to running CsvView on a Windows system.

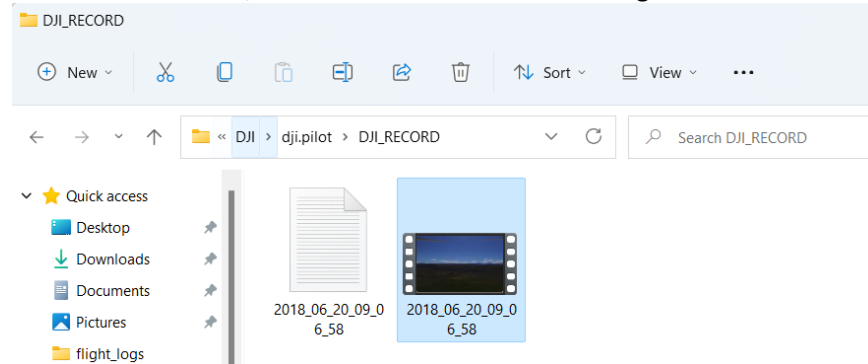
Beta	CsvViewMac_4.2.6	11/03/2022
	CsvViewMac_4.2.5	11/25/2021
	CsvViewMac_4.2.4	7/29/2021

PC Installation Instructions

When the download completes there should be a .zip file in your download directory. Unzip that .zip file into a temporary directory. Then execute (double-click) the CsvViewSetup file. CsvView should then be installed and an offer will be made to start CsvView. The user manual is contained in the downloaded CsvView.zip. It can also be accessed by starting CsvView and selecting the Help menu.

Task 2. Mobile Device Analysis

3. Open folder DJI_RECORD (Media01\Media01\sdcard\DJI\dji.pilot\DJI_RECORD), you will see a video that the drone took, this video is about one of the flights that the drone took.

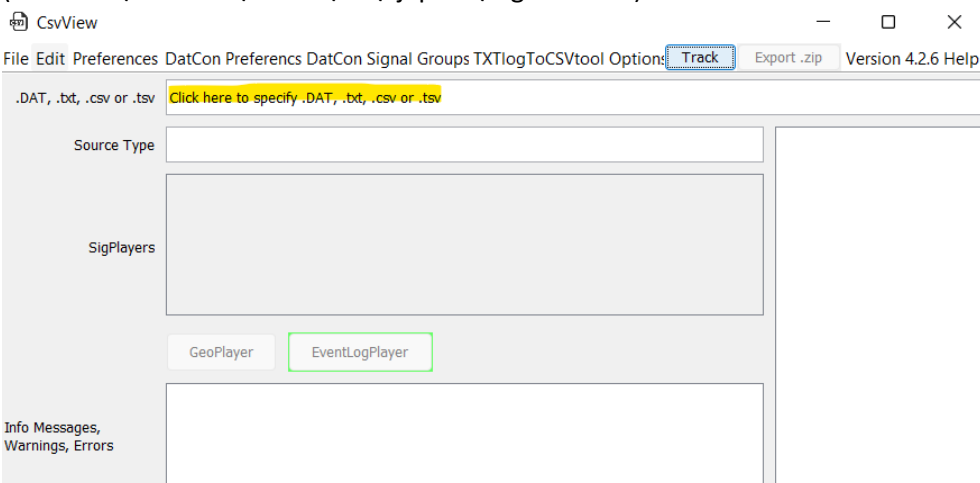


You can also get the information such as date of the flight, drone position, etc. about this flight in the text file that beside this video.

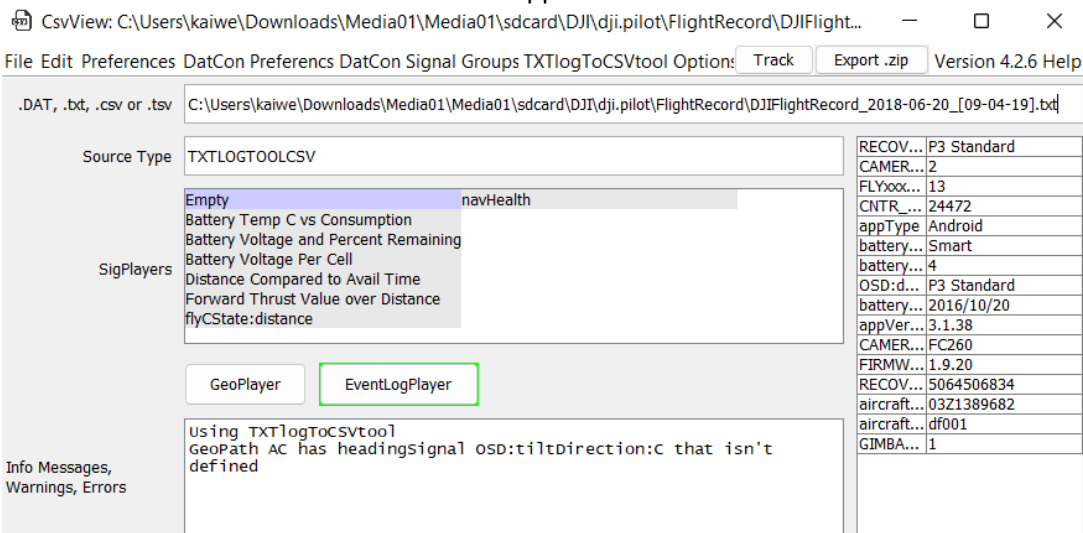
```
2018_06_20_09_06_58 - Notepad
File Edit View

#Wed Jun 20 09:08:16 MDT 2018
Sync_Drone_Time=5853,12399,18529,24587,30983,37963,44045,48970,55321,61453,66842,73921
PixelYDimension_Local=720
PositionGPSAlt=530.0
PositionGPSLng=-106.21978484572108
ProductType=2
PixelXDimension_Local=1280
LocalFileName=2018_06_20_09_06_58
CameraType=2
Video_Resolution_Enum_Drone=10
WhiteBalance=0
FrameJumped=0
Version=1.0
PositionGPSLat=39.96233966103926
EndTimeMsec=80666
FPS_Drone=25
FPS_local=30
PositionRelativeAlt=530.0
Sync_Local_Time=6000,10266,19208,20266,25600,31566,36633,50916,46033,51133,55466,61533
FolderID_Drone=100
ExposureMode=1
```

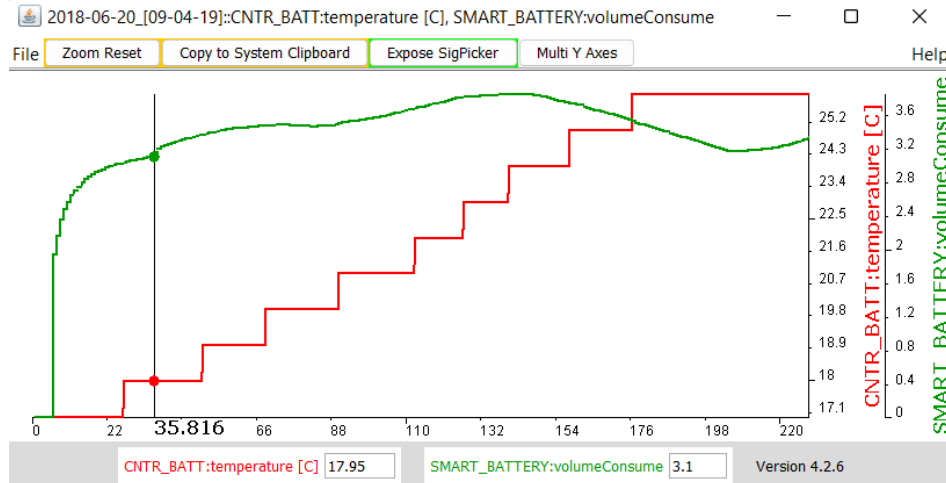
4. Open CsvView, click the highlighted part and choose the file inside the folder FlightRecord (Media01\Media01\sdcard\DJ\ddji.pilot\FlightRecord).



Then the information about the drone will appear.

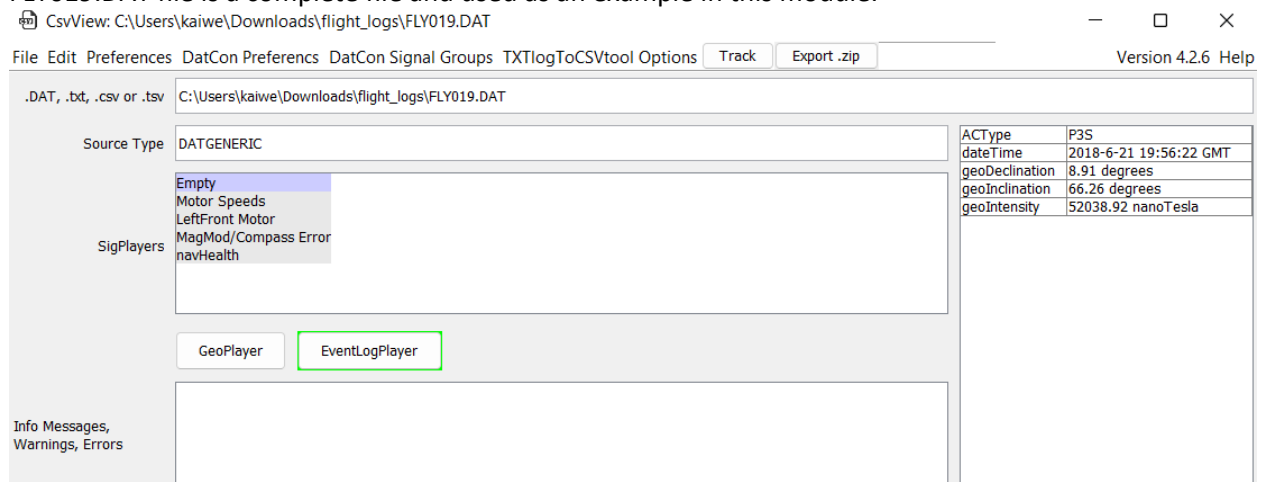


If you click some buttons such as “Battery Temp C vs Consumption”, a graph with the information about the drone appears.



Task 3. Drone Data Analysis

5. Open CsvView, choose the flightlog folder that downloaded before and choose one DAT file to analyze. Please note, since some DAT file is not complete, the analysis result may also not complete, FLY019.DAT file is a complete file and used as an example in this module.



As shown in this screenshot, the information about this flight such as drone type, date of the flight, geo information is shown. This flight date is 2018-06-21 19:56:22 GMT.

ACType	P3S
dateTime	2018-6-21 19:56:22 GMT
geoDeclination	8.91 degrees
geoInclination	66.26 degrees
geoIntensity	52038.92 nanoTesla

6. On the left side, click the “GeoPlayer” button, a map with the flight track is shown.

.DAT, .txt, .csv or .tsv

C:\Users\kaiwe\Downloads\flight_logs\FLY019.DAT

Source Type

DATGENERIC

SigPlayers

Empty

Motor Speeds

LeftFront Motor

MagMod/Compass Error

navHealth

GeoPlayer

EventLogPlayer

Info Messages, Warnings, Errors

GeoPlayer:FLY019

Zoom Reset

GoogleMap Key

Copy to System Clipboard

☒ IMU0

Choose Color

☐ IMU_ATT1(0):yaw:C

Choose Color

☐ IMU_ATT1(0):magYaw:C

Choose Color

☐ IMU_ATT1(0):tiltDirectionEarthFrame:C

Choose Color

☐ IMUCalcs(0)

Choose Color

☐ IMU_ATT1(0):yaw:C

Choose Color

☒ Home

Choose Color

7. Click the “EventLogPlayer” button, the event log is displayed. The line highlighted in pink means the drone takes off, the line highlighted in yellow means the drone landed. These two events mean one flight finished and according to the event log, this drone took off and landed for five times and this is the number of flights.

eventLog::FLY019

```

147.858 : 14506 [LED] changed: set home
148.518 : 14539 [Ctrl<2>] REQ_RC_COMMAND ASST_TAKEOFF_HOLD ctrl_asst_takeoff
149.358 : 14581 [LED] changed: normal led
153.378 : 14782 CTRL reset all by assisted takeoff finish
153.398 : 14783 [Ctrl<1>] REQ_RC_NORMAL ATTI_HOLD ctrl_gps_atti
223.058 : 18266 [M. Stop]landing.RC_Thr
223.058 : 18266 Motor Start 2 Total 115.08
223.058 : 18266 CTRL reset all by motor stopped
223.200 : 18273 set_get_real_name_info
223.200 : 18273 set_real_name_info,data: 1529611350, flag: ad, len:27 14
225.138 : 18368 iwdg_set_max_timeout befor set swdg_timeout(0x00000120)!
225.138 : 18368 iwdg_set_time_out time_out(0x00000ffa)!
225.138 : 18368 iwdg_set_swdg_time_out time_out(4090) set g_swdg_timeout_max(0x000007ab) ||
299.878 : 22060 [M.Start]REQ_RC_NORMAL
299.878 : 22060 [Ctrl<2>] REQ_RC_COMMAND ENGINE_START ctrl_engine_start
299.898 : 22061 [TO.ALT ] 2491.070801
299.898 : 22061 39.9611921 -106.2164697 2511.07 Home Point
301.218 : 22127 [LED] changed: set home
301.898 : 22161 [Ctrl<2>] REQ_RC_COMMAND ASST_TAKEOFF_HOLD ctrl_asst_takeoff
302.718 : 22202 [LED] changed: normal led
305.458 : 22339 [M. Stop]landing.exit_takeoff
305.458 : 22339 Motor Start 3 Total 120.66
305.458 : 22339 CTRL reset all by motor stopped
305.458 : 22339 [Ctrl<2>] REQ_RC_COMMAND ENGINE_START ctrl_engine_start
305.478 : 22340 [Ctrl<1>] REQ_RC_NORMAL ATTI_HOLD ctrl_gps_atti
305.638 : 22348 set_get_real_name_info
305.640 : 22348 set_real_name_info,data: 1529611432, flag: ad, len:27 14
307.438 : 22436 [M.Start]REQ_RC_NORMAL
307.438 : 22436 [Ctrl<2>] REQ_RC_COMMAND ENGINE_START ctrl_engine_start
    
```

☐ Be synced by other Players
 ☐ Synch other Players
 ☐ Synch and be synced other Players
 ☐ Don't synch with other Players

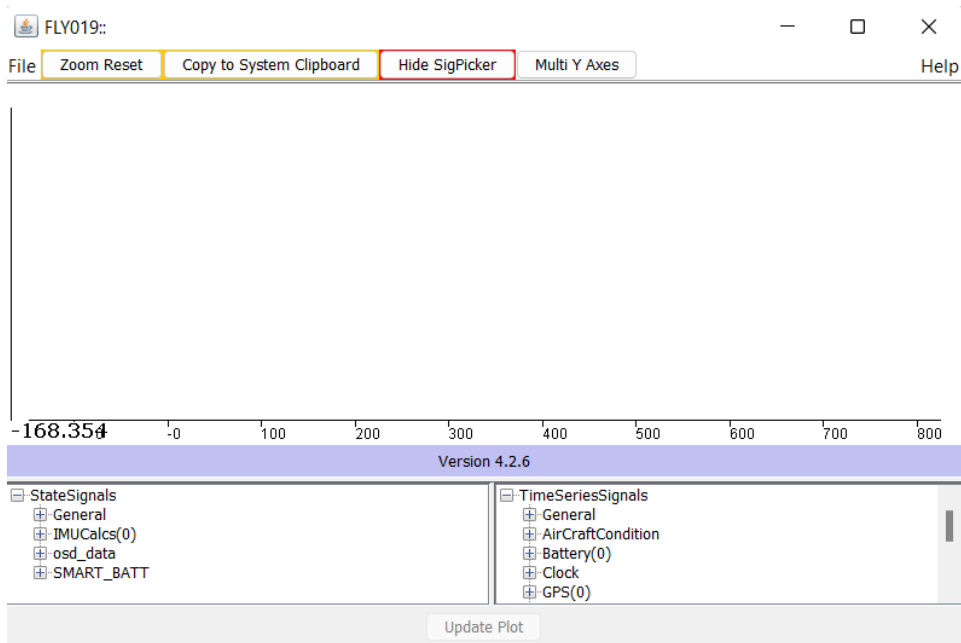
8. Click “Empty” button to open a blank graph.

.DAT, .txt, .csv or .tsv

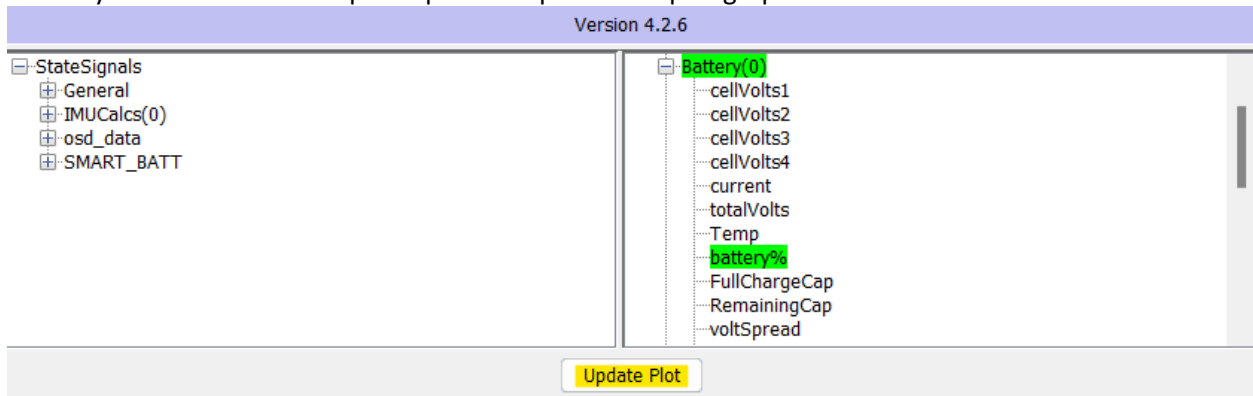
Source Type

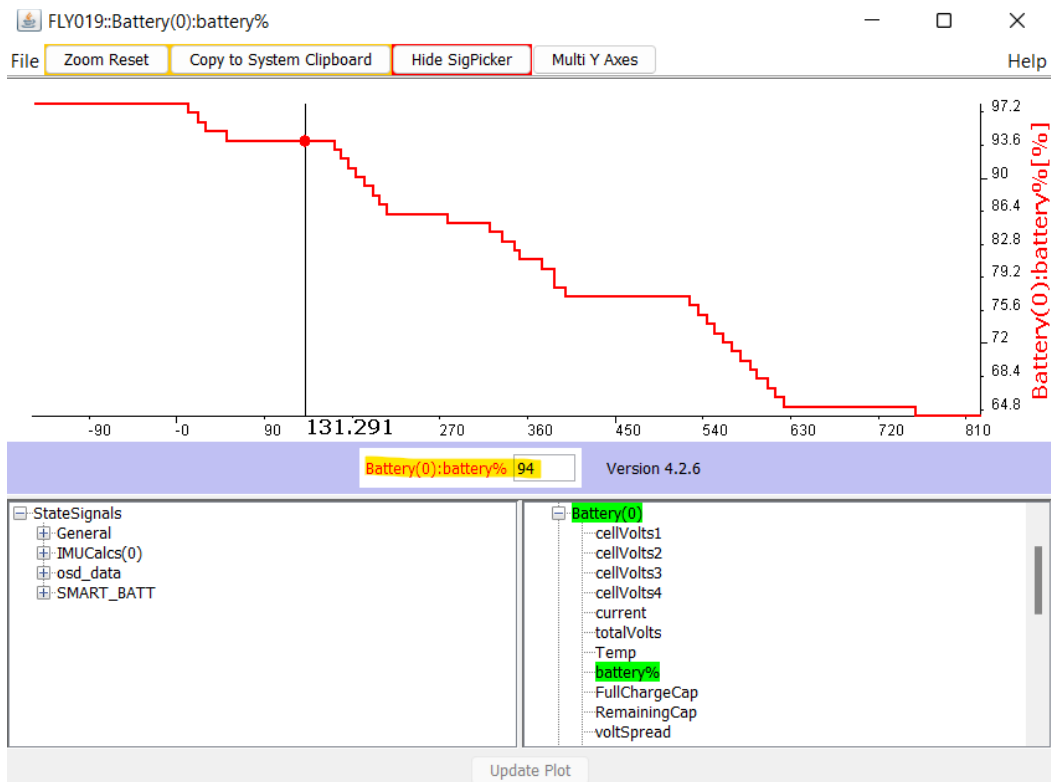
SigPlayers

Empty
 Motor Speeds
 LeftFront Motor
 MagMod/Compass Error
 navHealth



Then click the plus sign beside the “Battery(0)” and to expand the battery information list and click “battery%” and then click “Update plot” to open a new plot graph.





As shown in this graph, the battery information changing with time is shown. And the percentage of the battery is highlighted in yellow. The highest percentage is 98% and the lowest percentage is 46%.

