Análisis Forense de Drones

DRONESVIP | Centro de Instrucción de Aeronáutica Civil

Modulo III

CASO DE ESTUDIO

Objetivos

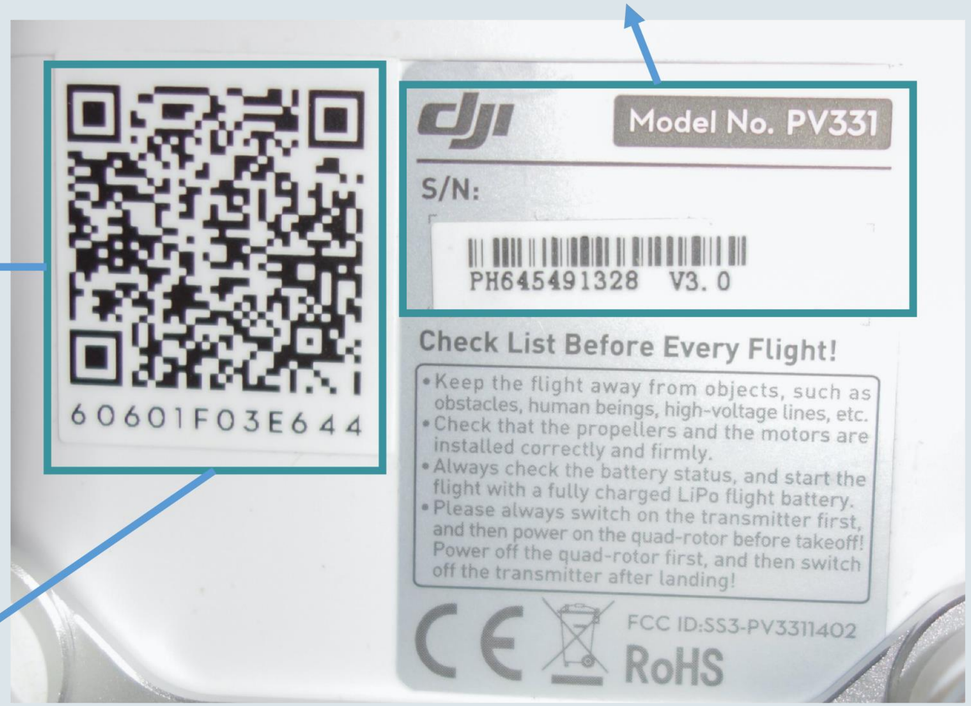
- Aplicar reglas de buena práctica
- Utilizar herramientas forenses
- Verificar la existencia de diferentes fuentes de evidencia
- Reconocer múltiples artefactos forenses
- Identificar y preservar evidencias digitales
- Analizar e interpretar hallazgos

Identificación externa

Identificación externa

Número de Serie y Modelo

QR para descargar la aplicación



MAC Address Details

Company	SZ DJI TECHNOLOGY CO.,LTD
Address	shenzhen guangdong 518057 Hi-Tech Park(South),Nanshan District CHINA
Range	60:60:1F:00:00:00 - 60:60:1F:FF:FF:FF
Type	IEEE MA-L

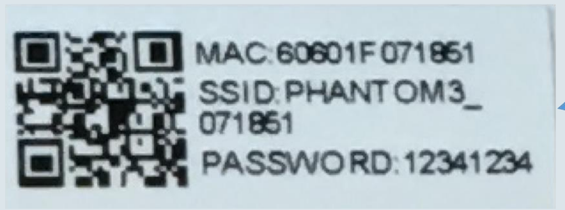
http://m.dji.net/djivision?1=DJI&2=PHANTOM VISION&3=BL252026148842&4=FC200_03e644&5=60601F03E644

https://www.macvendorlookup.com/

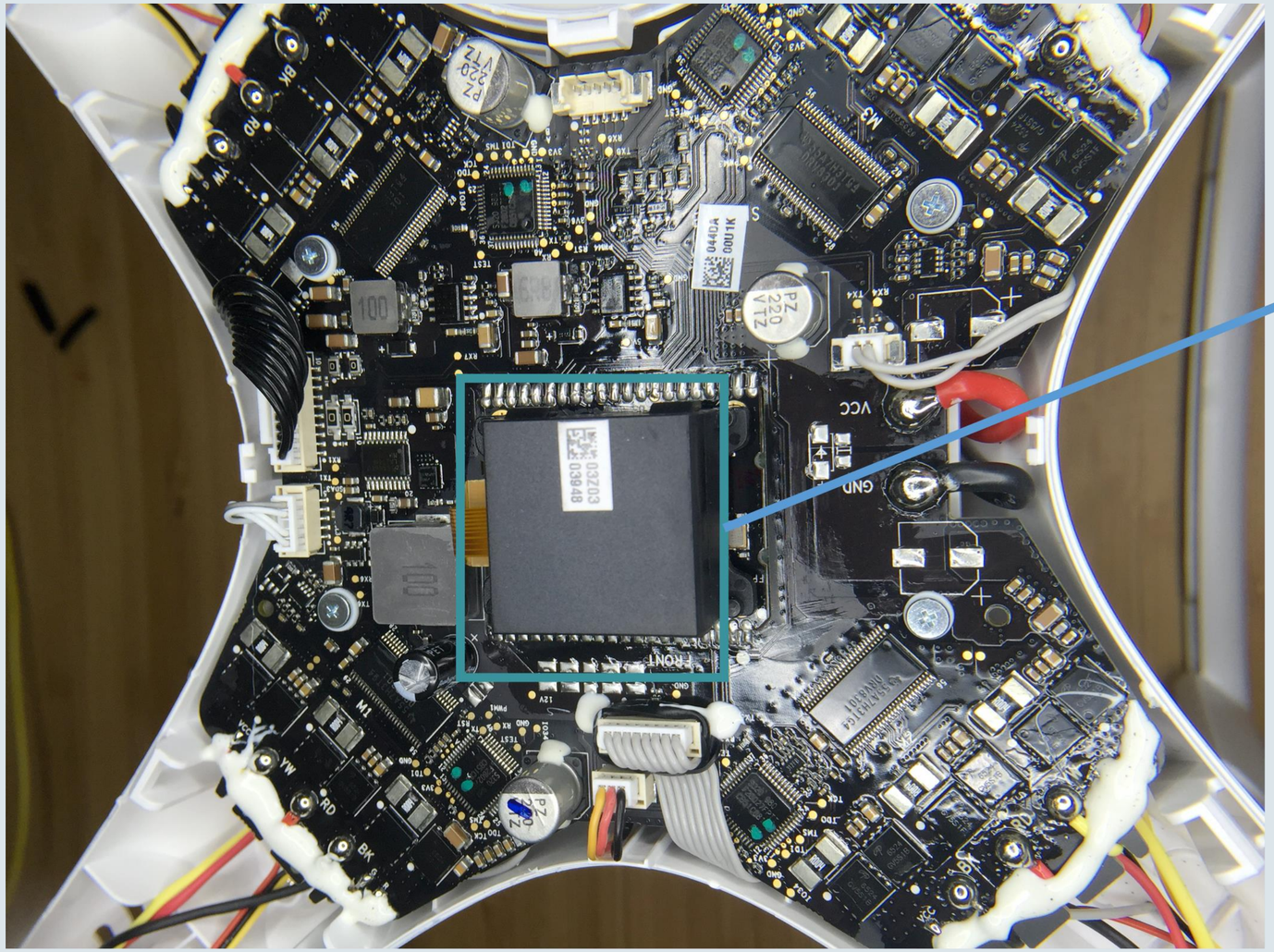
Otros elementos

Batería

Control remoto



Identificación interna

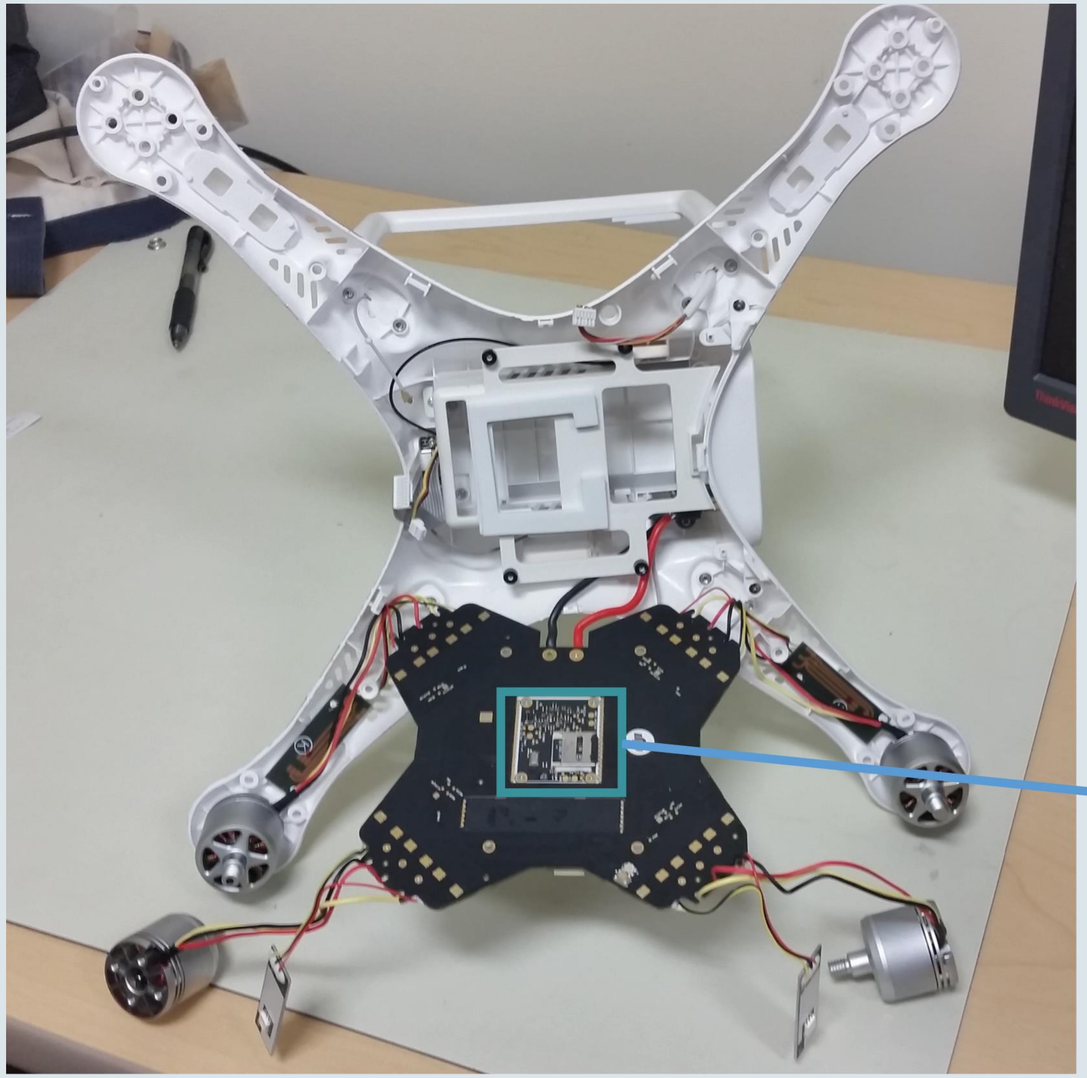


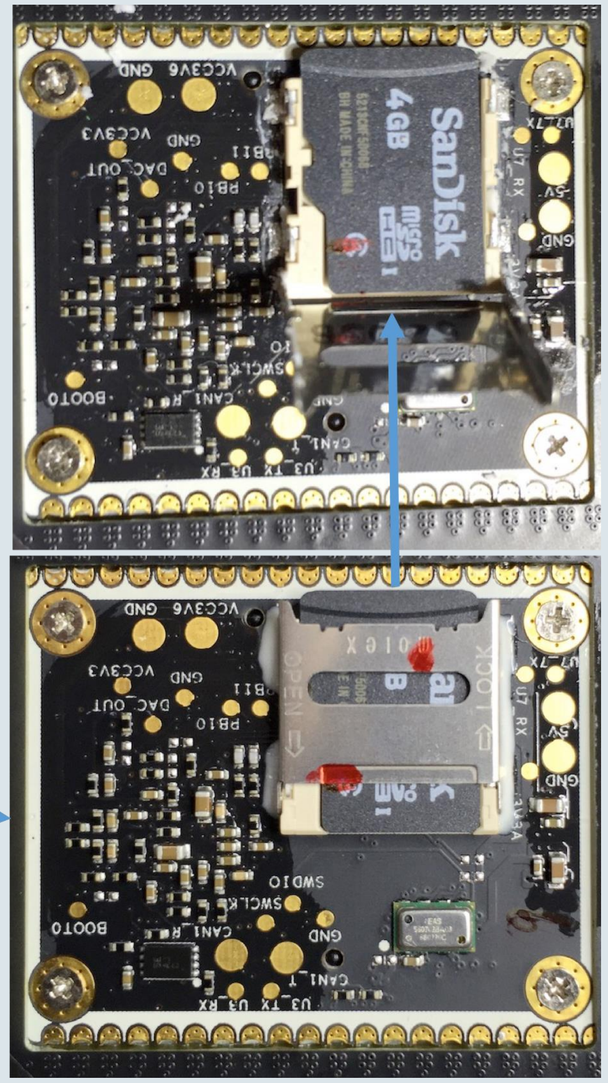
IMU/UMI

Inertial Measurement Unit /
Unidad de Medición Inercial

(Acelerómetro, giróscopo, etc)

Identificación interna

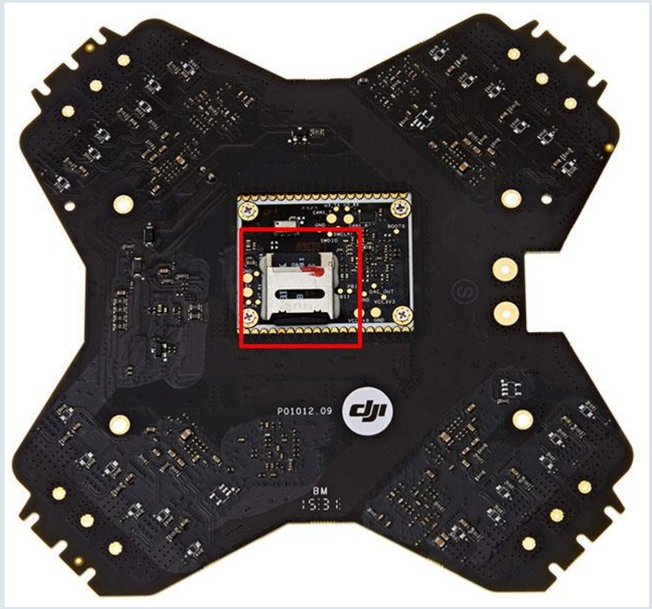




Preservación

SEGÚN EL TIPO DE ACCESO A LA INFORMACIÓN DEL DRONE

DIRECTA



INDIRECTA

Preservación

Técnica directa: realizar imagen forense de los medios de almacenamiento

TARJETA DE MEMORIA EXTERNA TIPO MICRO-SD

BLOQUEADOR DE ESCRITURA

- Adaptador de tarjetas SD con bloqueo de escritura.
- Software Phrozen USB

(http://phrozen-safe-usb.findmysoft.com/)

IMAGEN FORENSE

- Software FTK Imager (https://accessdata.com/product-download/ftk-imager-version-4-3-0)

Preservación

Técnica indirecta: Exportar evidencias lógicas mediante aplicaciones nativas

DESDE EL DRONE ENCENDIDO

BLOQUEADOR DE ESCRITURA

- Software Phrozen USB

(http://phrozen-safe-usb.findmysoft.com/)

EXPORTAR REGISTROS

- Software propietario (https://www.dji.com/downloads/softwares/assistant-dji-2)

Preservación

Resguardar registros en periféricos

DISPOSITIVO MÓVIL

TARJETA DE MEMORIA EXTERNA TIPO MICRO-SD

- Adaptador de tarjetas SD con bloqueo de escritura.
- Software Phrozen USB

(http://phrozen-safe-usb.findmysoft.com/)

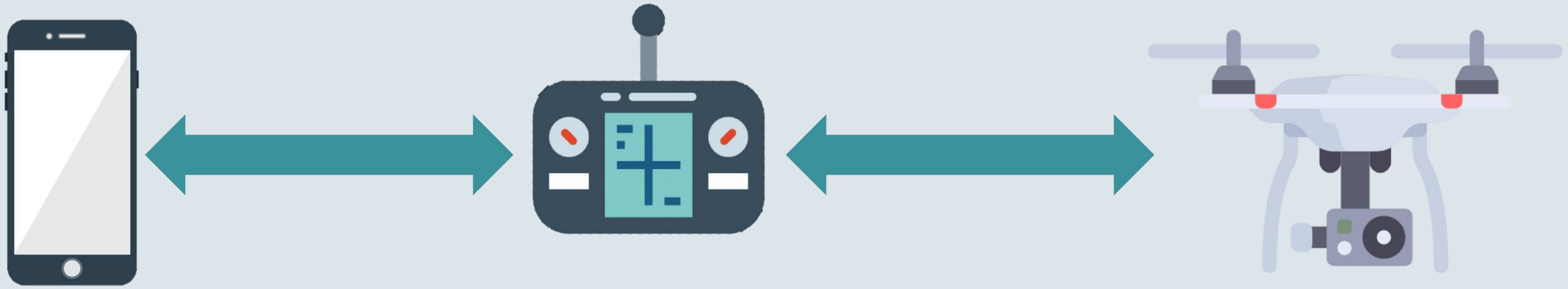
- Software FTK Imager (https://accessdata.com/product-download/ftk-imager-version-4-3-0)

SUITE FORENSE

- UFED 4PC
- Oxygen Forensic
- Magnet Adquire (https://www.magnetforensics.com/resources/magnet-acquire/)

Análisis

Identificación y recolección de evidencias



Dispositivo móvil
(Archivos TXT)

Control remoto

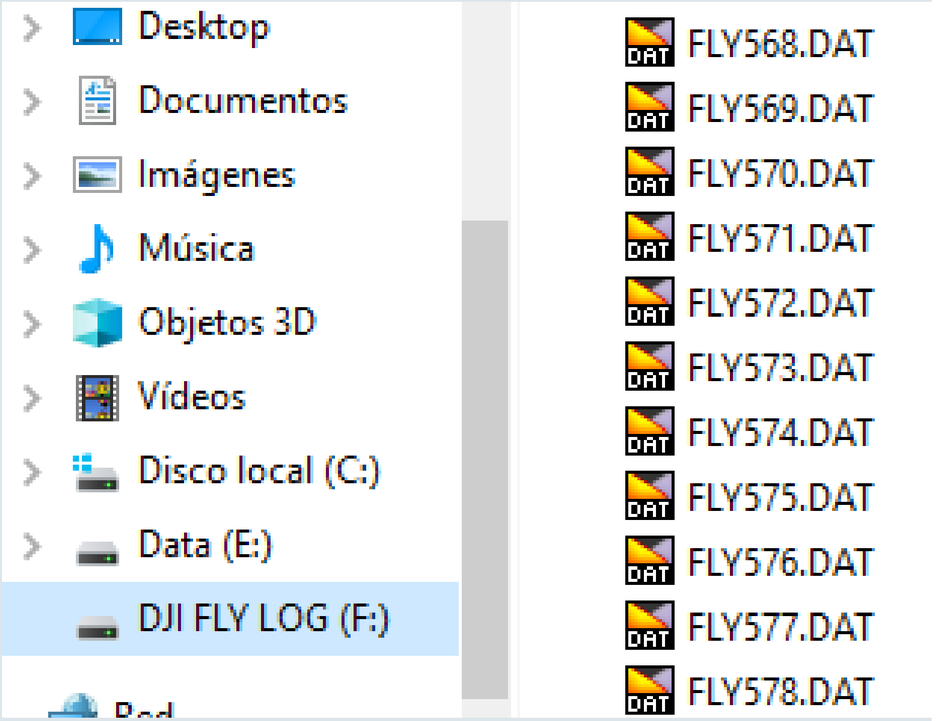
Drone
(Archivos DAT)

Análisis

ARCHIVOS DAT

Identificación y recolección de evidencias:

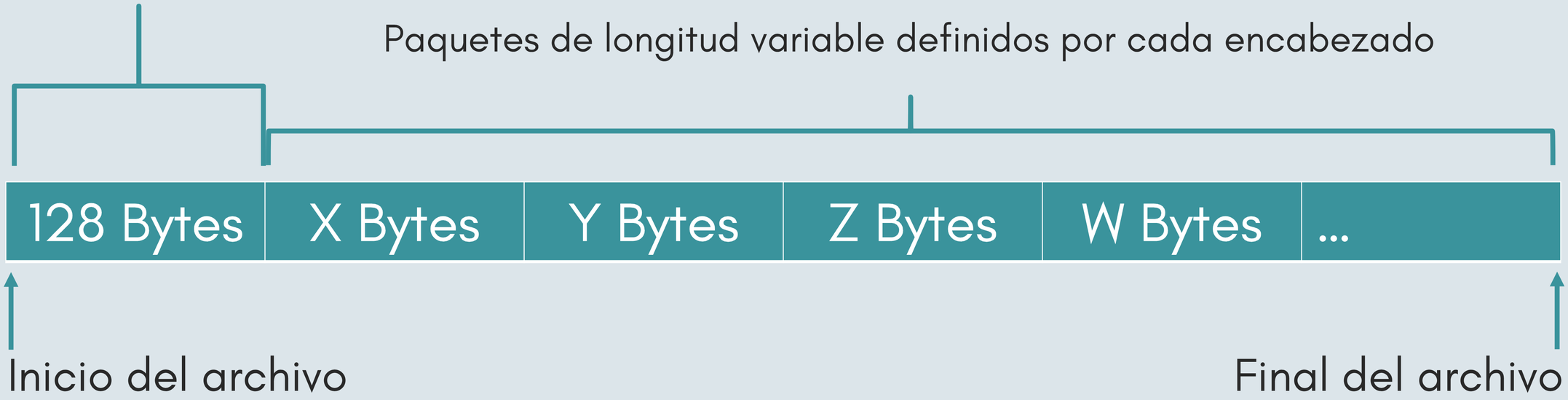
- Se encuentran almacenados en la memoria externa del Drone.
- Contienen registros de GPS, batería, control remoto, estado de vuelo, motores, etc.
- Un nuevo archivo DAT es creado cada vez que se enciende el Drone y cierra el archivo DAT anterior.



Archivos DAT

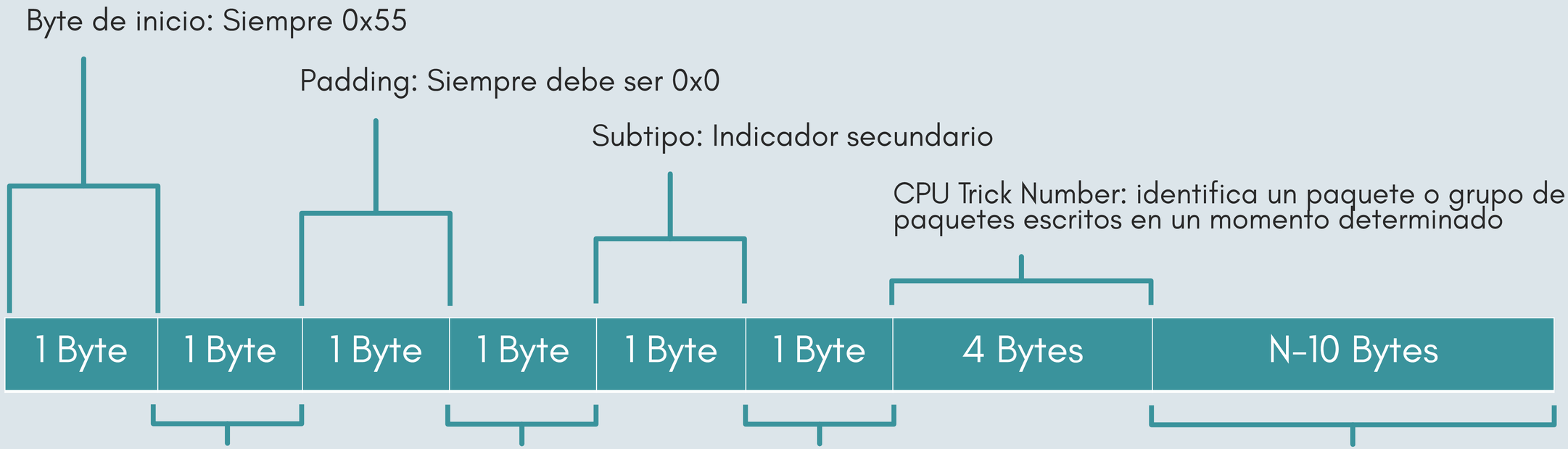
ESTRUCTURA INTERNA

Encabezado: Longitud fija de 128 Bytes. Contiene el número de compilación del archivo DAT.



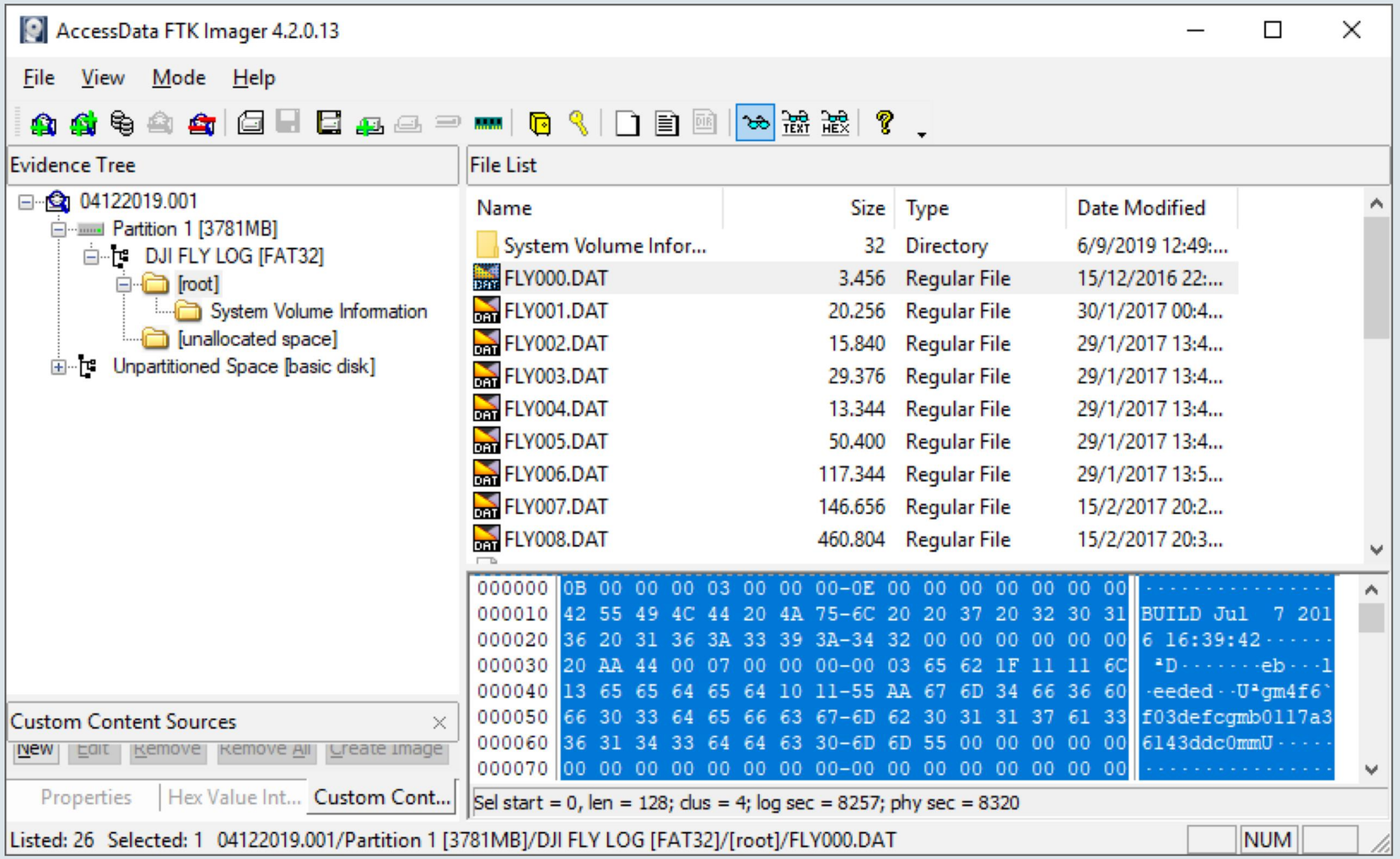
Archivos DAT

ESTRUCTURA DE LOS PAQUETES



Archivos DAT

PREVISUALIZACIÓN Y RECOLECCIÓN CON FTK IMAGER

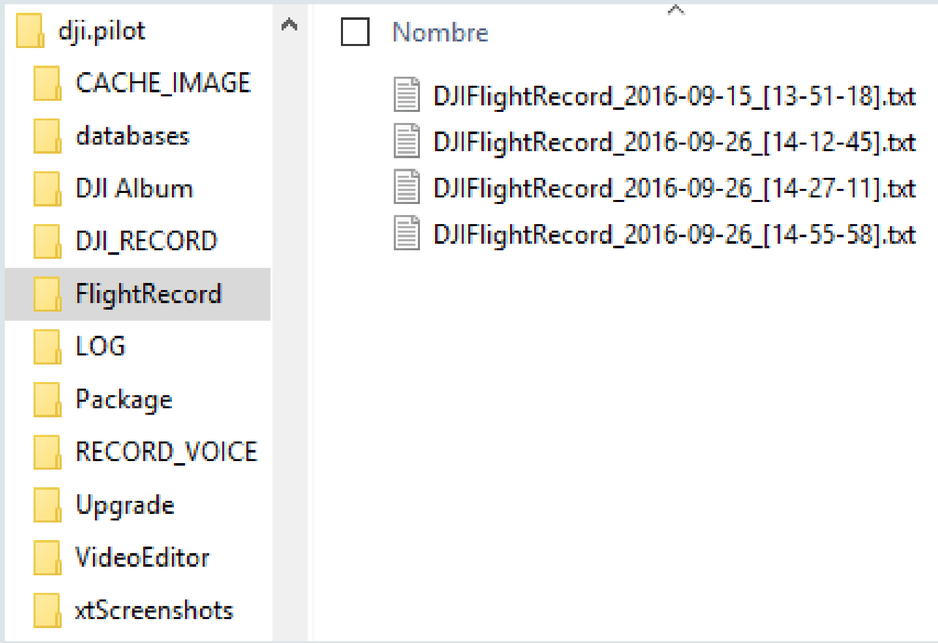


Análisis

ARCHIVOS TXT

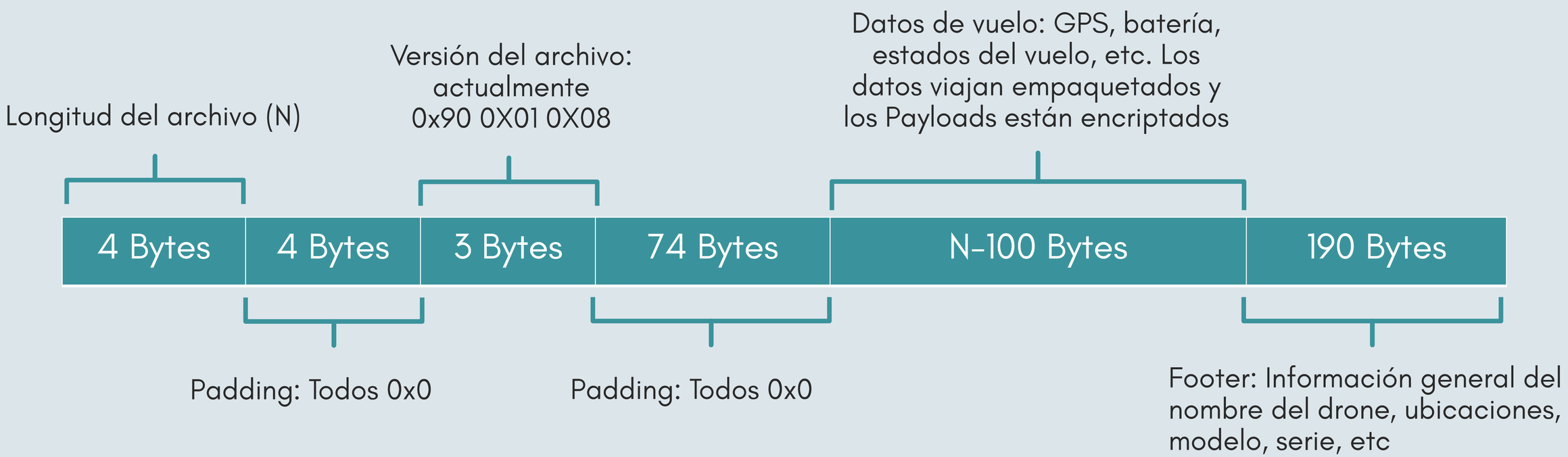
Identificación y recolección de evidencias:

- Se encuentran almacenados en el dispositivo móvil.
- Contiene registros similares a los archivos DAT
- Utiliza un complejo esquema de cifrado.



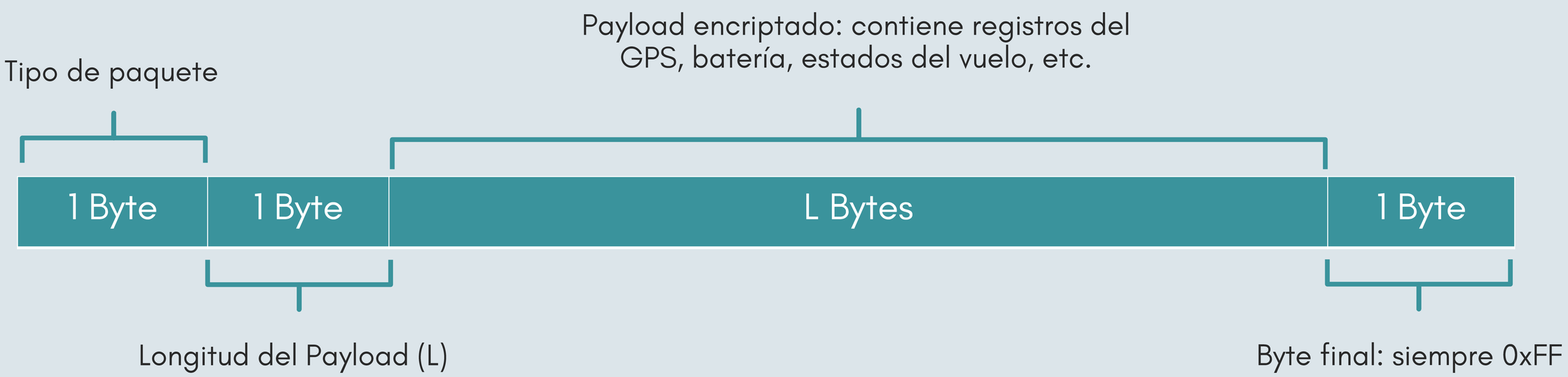
Archivos TXT

ESTRUCTURA INTERNA



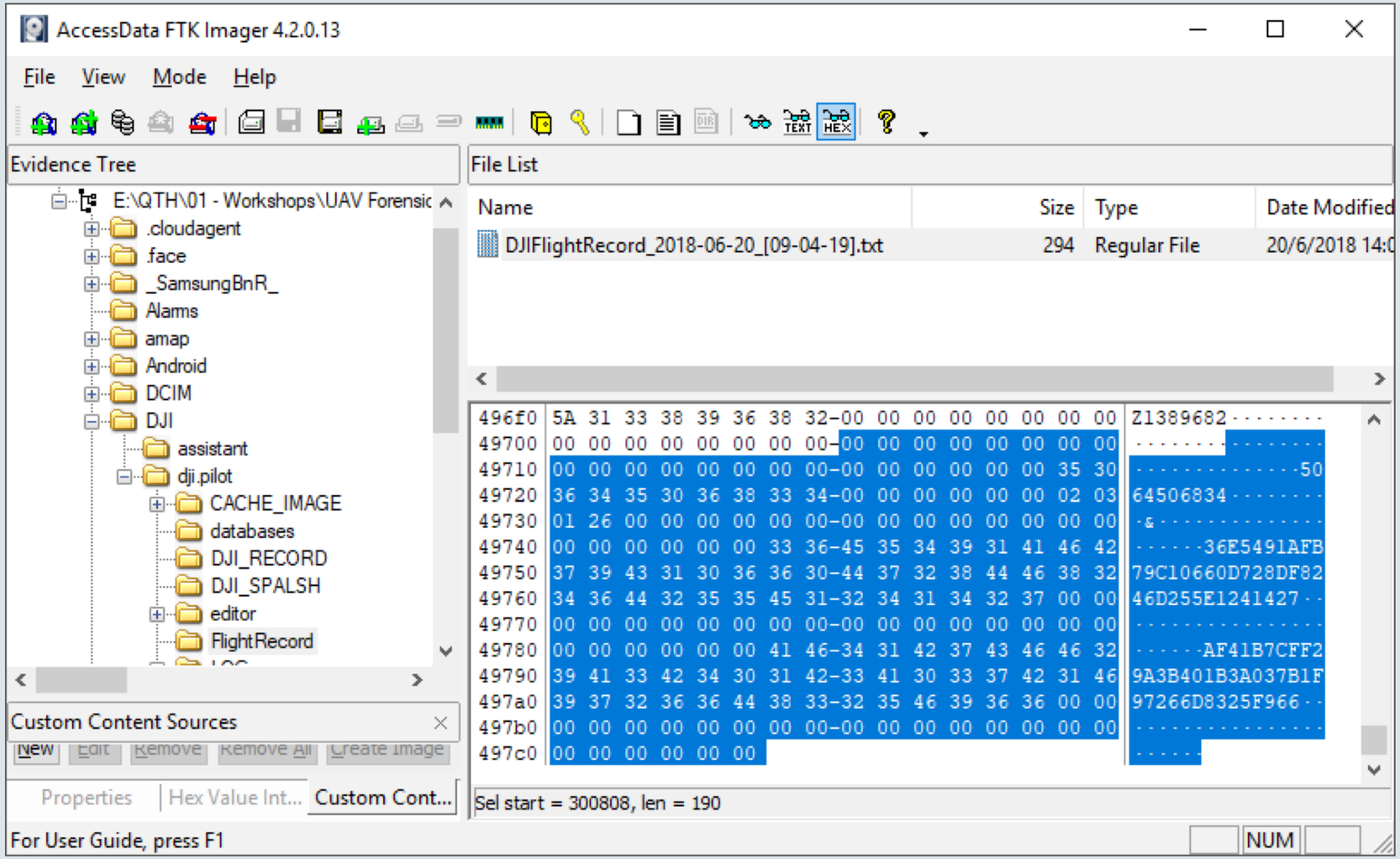
Archivos TXT

ESTRUCTURA DE LOS PAQUETES



Archivos TXT

PREVISUALIZACIÓN Y RECOLECCIÓN CON FTK IMAGER



Análisis

INTERPRETACIÓN DE LAS EVIDENCIAS RECOLECTADAS

ARCHIVOS DAT

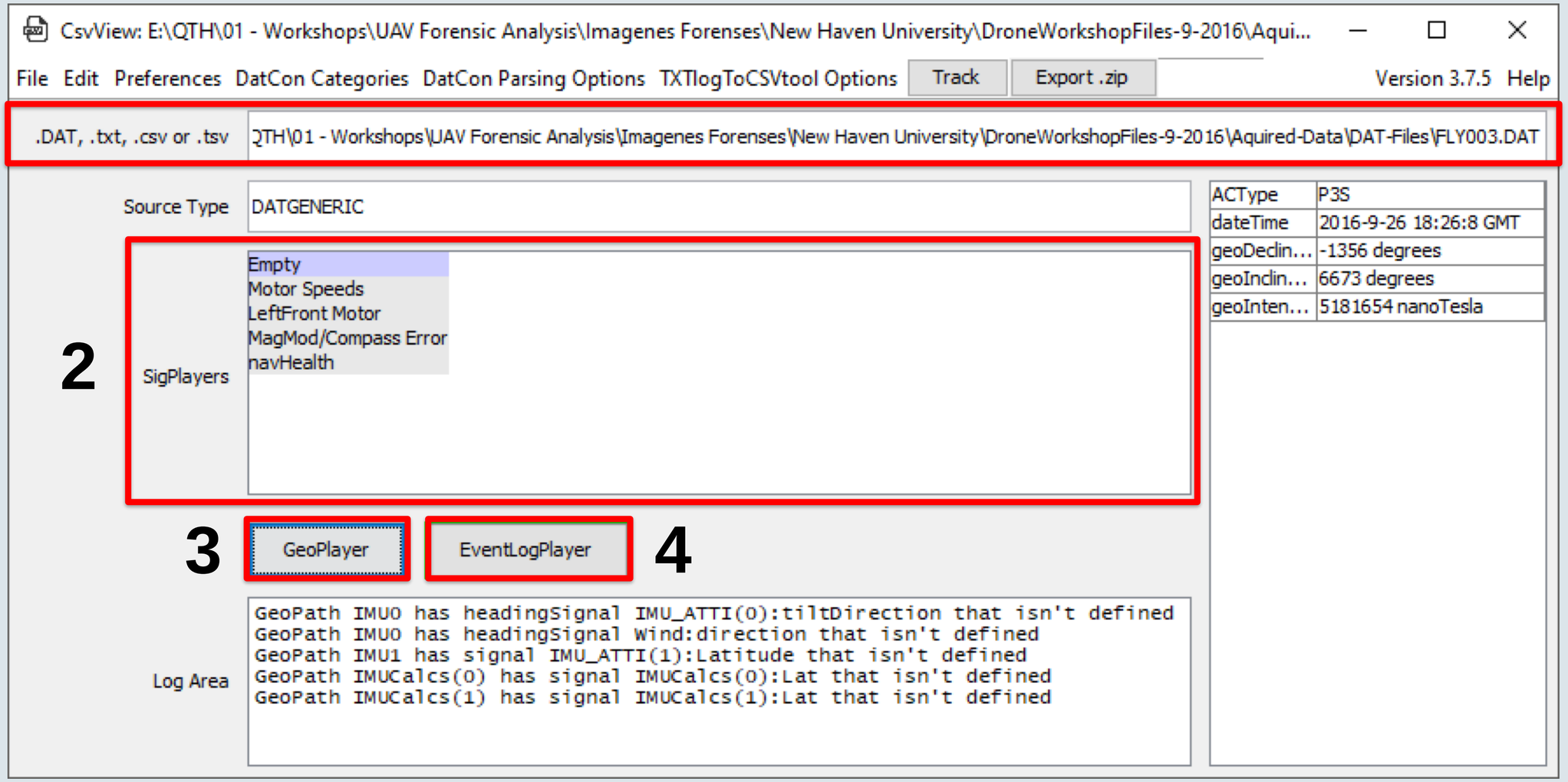
- CsvView (http://datfile.net/CsvView/downloads.html)
- DatCon (http://datfile.net/DatCon/downloads.html)

ARCHIVOS TXT

- CsvView
- AirData (https://app.airdata.com)

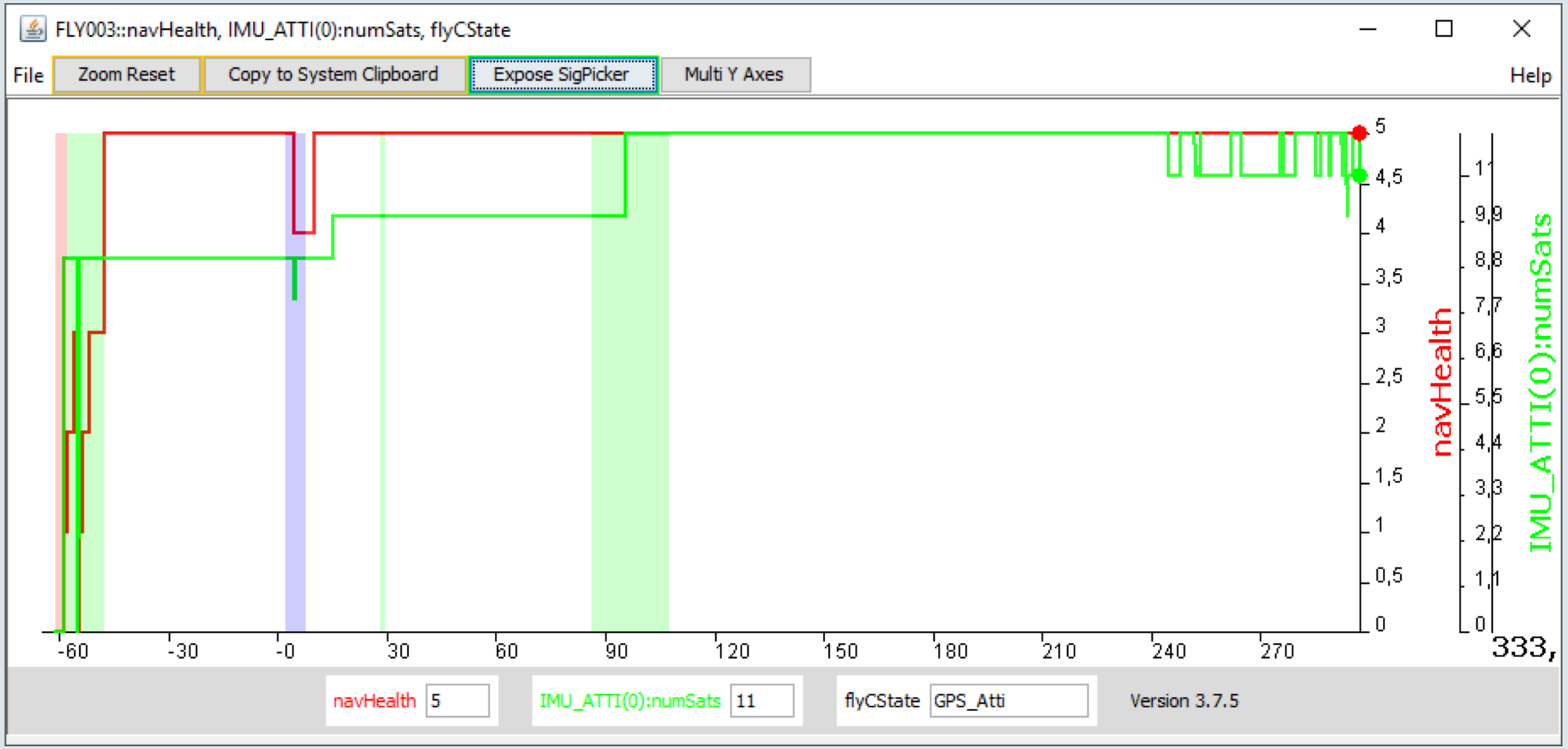
Archivos DAT

INTERPRETACIÓN CON CSV VIEW



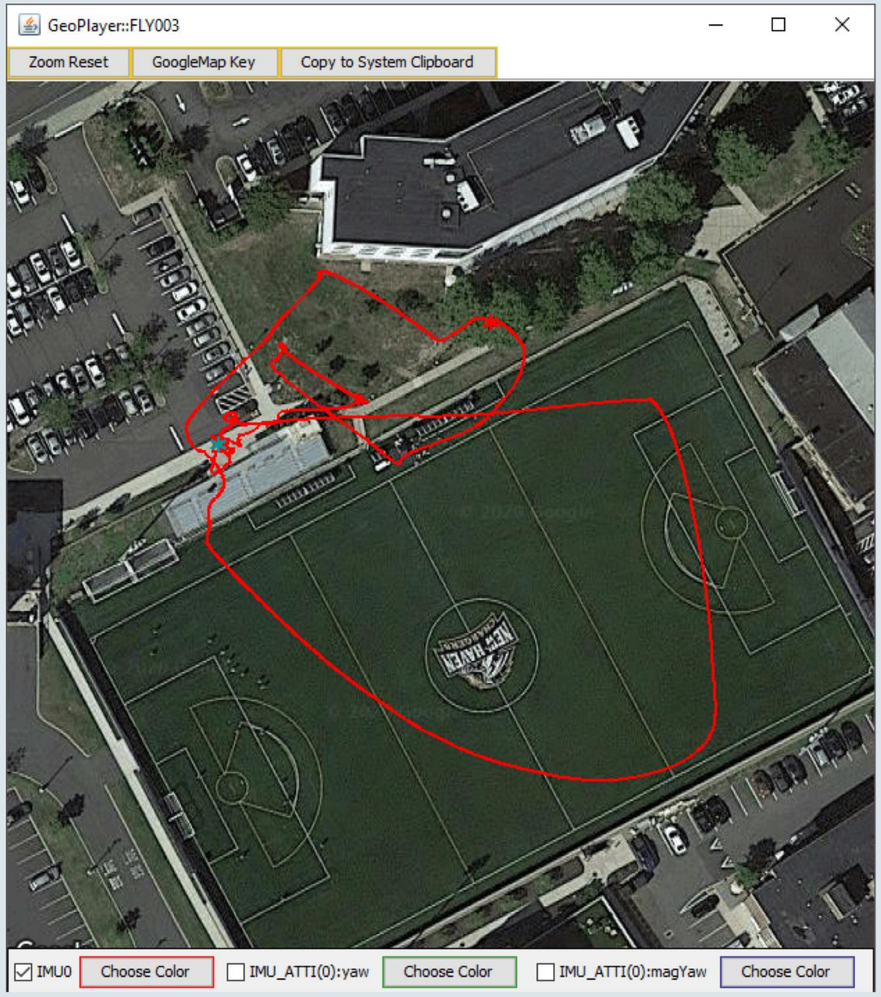
Archivos DAT

INTERPRETACIÓN CON CSV VIEW – SIGPLAYER



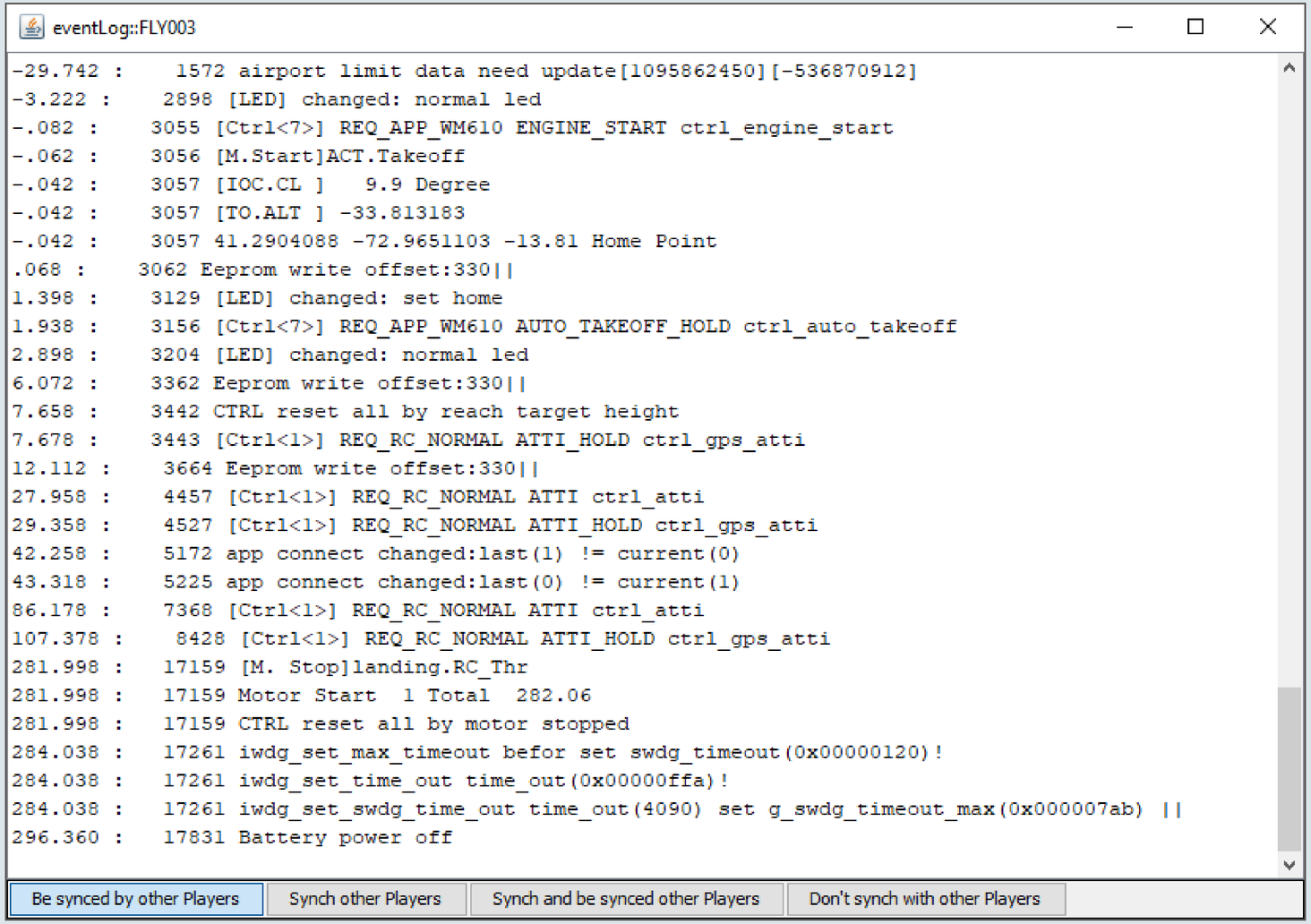
Archivos DAT

INTERPRETACIÓN CON CSV VIEW - GEOPLAYER



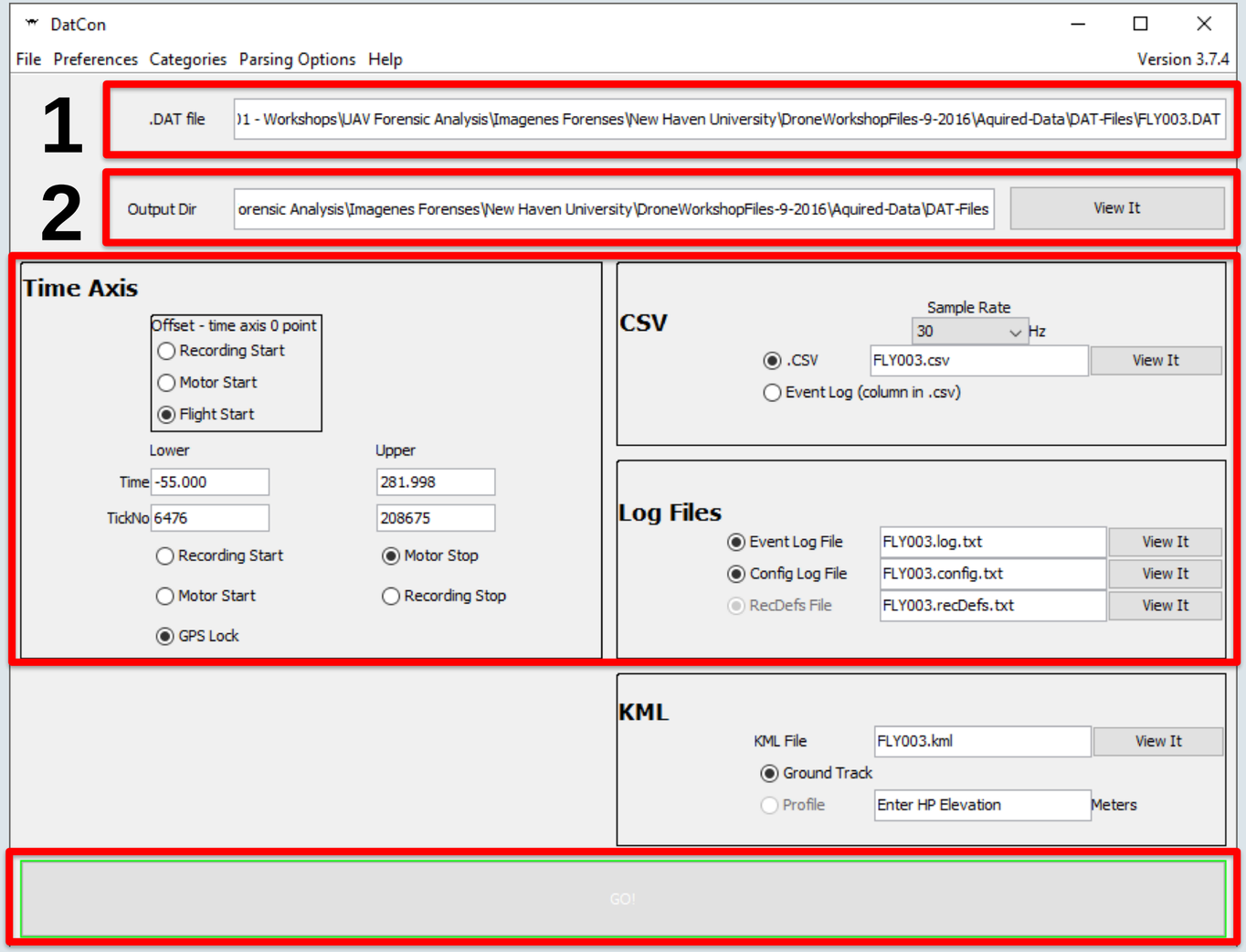
Archivos DAT

INTERPRETACIÓN CON CSV VIEW – EVENT LOG PLAYER



Archivos DAT

INTERPRETACIÓN CON DATCON



Archivos DAT

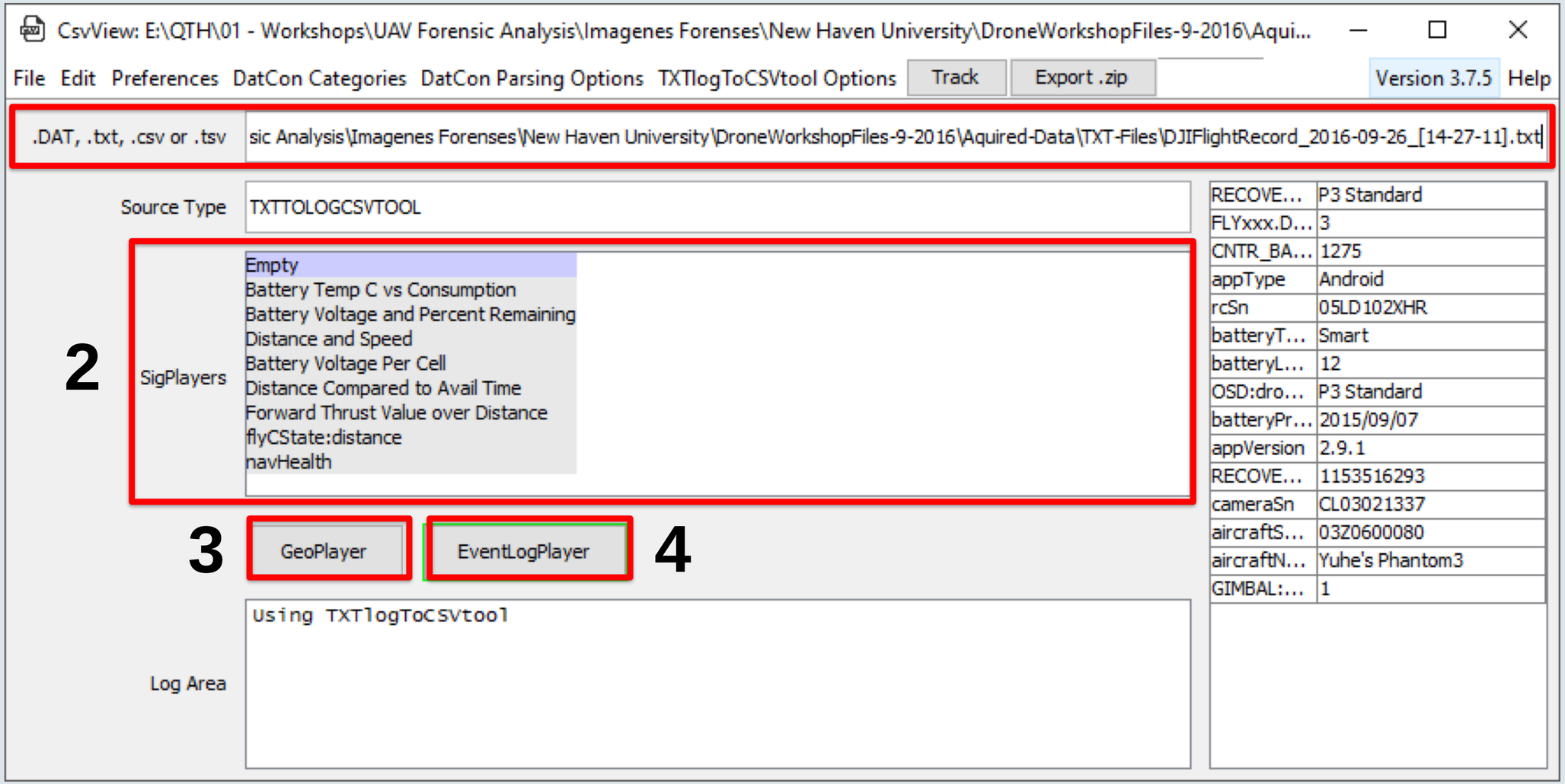
INTERPRETACIÓN CON DATCON – ARCHIVO DE VUELO EN FORMATO CSV

A1

	A
1	latitude,longitude,altitude(feet),ascent(feet),speed(mph),distance(feet),time(millisecond),datetime(utc),satellites,voltage(v),max_altitude(feet),max_ascent(feet),max_speed(mph),max_distance(feet),compas
2	41.2904087520873,-72.9651103103011,123.27288485024,0,0,0,0,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_Atti,
3	41.2904087504213,-72.9651103169825,123.27288485024,0,0,0.00192987867068,100,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0.00192987867068,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_
4	41.2904087515445,-72.965110415862,123.27288485024,0,0,0.0289390101124,200,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0.0289390101124,9.7,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_Att
5	41.2904087525584,-72.9651104145146,123.27288485024,0,0,0.0285694562948,300,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0.0289390101124,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_A
6	41.2904087627385,-72.9651104194819,123.27288485024,0,0,0.0301818907296,400,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0.0301818907296,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_A
7	41.2904087637505,-72.9651104191045,123.27288485024,0,0,0.0301292332476,500,2016-09-26 18:27:12,9,0,123.27288485024,0,0,0.0301818907296,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_A
8	41.2904086649004,-72.965110519489,123.27288485024,0,0,0.065578086088,600,2016-09-26 18:27:13,9,0,123.27288485024,0,0,0.065578086088,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_Atti,
9	41.2904086564856,-72.9651105093741,123.27288485024,0,0,0.064768046692,700,2016-09-26 18:27:13,9,0,123.27288485024,0,0,0.065578086088,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_Atti
10	41.2904086575796,-72.9651105087913,123.27288485024,0,0,0.064418965316,800,2016-09-26 18:27:13,9,0,123.27288485024,0,0,0.065578086088,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_Atti
11	41.2904086591549,-72.9651105083416,123.27288485024,0,0,0.064008532232,900,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.065578086088,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS
12	41.2904085578418,-72.9651105216727,123.27288485024,0,0,0.0915436381,1000,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.0915436381,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_At
13	41.290408559238,-72.9651105220346,123.27288485024,0,0,0.091212929428,1100,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.0915436381,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GPS_A
14	41.2904085601886,-72.9651106218176,123.27288485024,0,0,0.110430449728,1200,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.110430449728,9.8,0,0,1024,1024,1024,1024,9.4,0,67,4.014,4.016,4.013,4.016,0,0,6,GP
15	41.2904085479044,-72.9651106198373,122.94480085024,-0.328084,0,0.11291667028,1400,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.11291667028,9.8,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,0,
16	41.2904085482491,-72.9651106195736,122.94480085024,-0.328084,0,0.112779203084,1500,2016-09-26 18:27:13,9,16.059,123.27288485024,0,0,0.11291667028,9.9,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,0
17	41.290408449339,-72.965110615908,122.94480085024,-0.328084,0,0.13863517504,1600,2016-09-26 18:27:14,9,16.059,123.27288485024,0,0,0.13863517504,9.9,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,0,0,6
18	41.2904084525926,-72.9651106155242,122.94480085024,-0.328084,0,0.137627300992,1700,2016-09-26 18:27:14,9,16.059,123.27288485024,0,0,0.13863517504,9.9,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,0
19	41.2904084553539,-72.9651107124752,122.61671685024,-0.656168,0,0.1545193619,1800,2016-09-26 18:27:14,9,16.059,123.27288485024,0,0,0.1545193619,9.9,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,0,0,6
20	41.2904084510436,-72.9651107172834,122.61671685024,-0.656168,0,0.156562012884,1900,2016-09-26 18:27:14,9,16.059,123.27288485024,0,0,0.156562012884,9.9,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.013,4.016,
21	41.2904084522675,-72.9651107134709,122.61671685024,-0.656168,0,0.155504270068,2000,2016-09-26 18:27:14,9,16.058,123.27288485024,0,0,0.156562012884,10,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.012,4.016,
22	41.290408454801,-72.9651107118559,122.28863285024,-0.984252,0,0.154540031192,2100,2016-09-26 18:27:14,9,16.058,123.27288485024,0,0,0.156562012884,10,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.012,4.016,0,
23	41.2904083612452,-72.9651107175472,122.28863285024,-0.984252,0,0.181102696084,2200,2016-09-26 18:27:14,9,16.058,123.27288485024,0,0,0.181102696084,10,0,0,1024,1024,1024,1024,9.5,0,67,4.014,4.016,4.012,4.016,

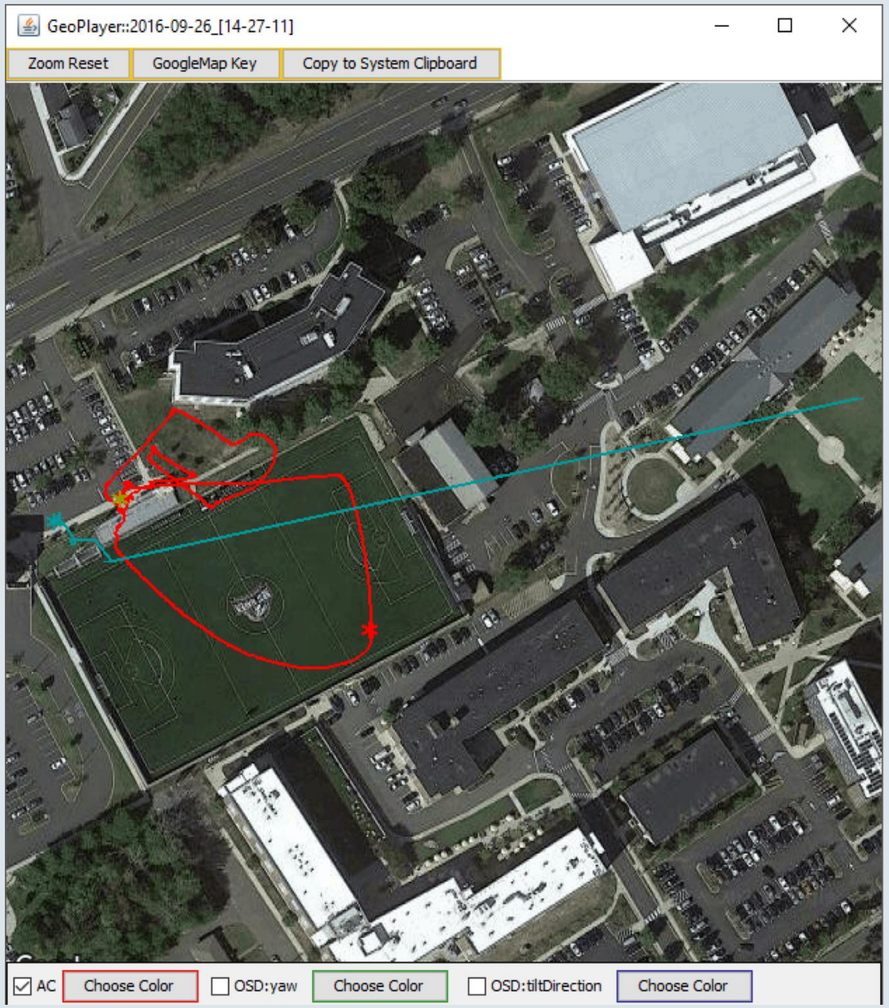
Archivos TXT

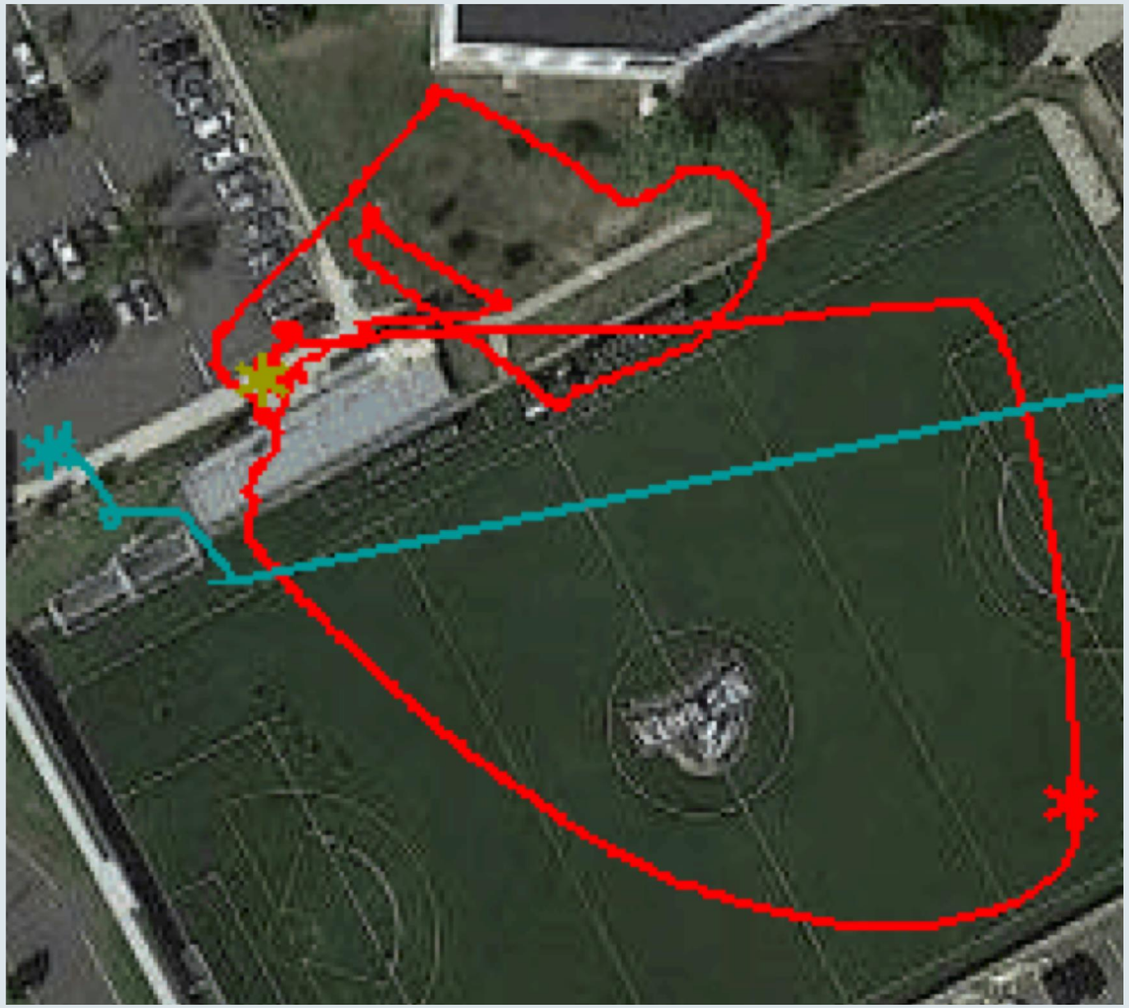
INTERPRETACIÓN CON CSV VIEW



Archivos TXT

INTERPRETACIÓN CON CSV VIEW - GEOPLAYER





Archivos TXT

INTERPRETACIÓN CON AIRDATA

Metric / Imperial
Settings

Overview | Details | Notifications | Large Map

GENERAL
POWER
SENSORS
CONTROLS
WEATHER
MEDIA

Sep 26th, 2016 02:27PM Edit

Sep 26th, 2016
02:27PM (-04:00)

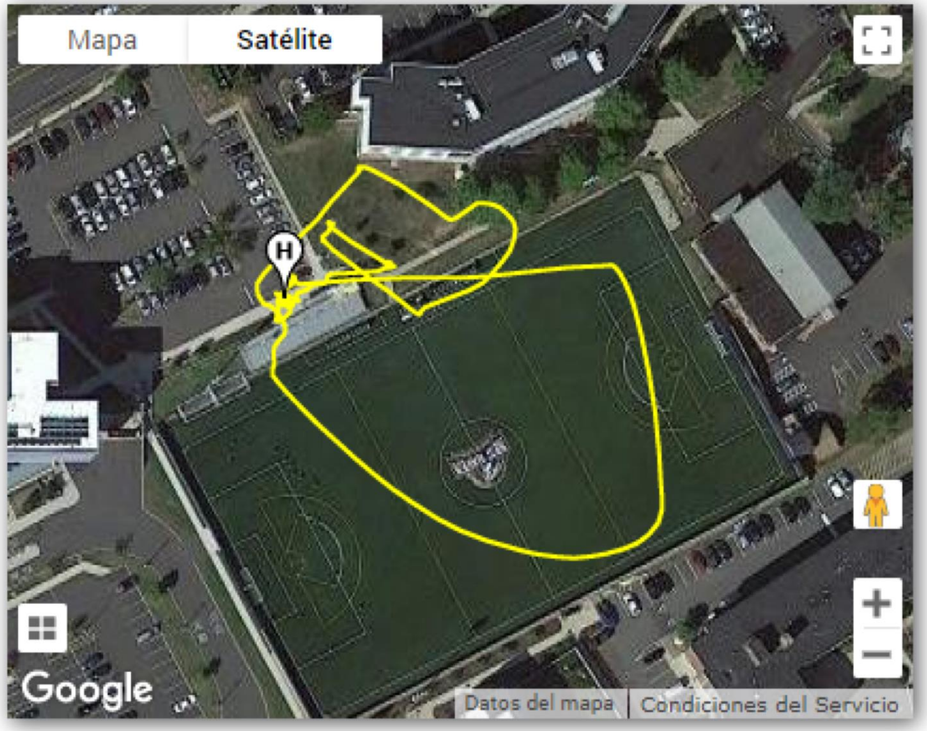
Plane Name
Yuhes Phantom3

Flight Air Time
04m 37s

Takeoff Battery
67% 16.1v

Landing Battery
54% 14.8v

P3S/Android
DJI 2.9.1



Total Kilometrage
480 m

Max Distance
92 m

Max Altitude
51.0 m

Max Speed
8.55 m/s

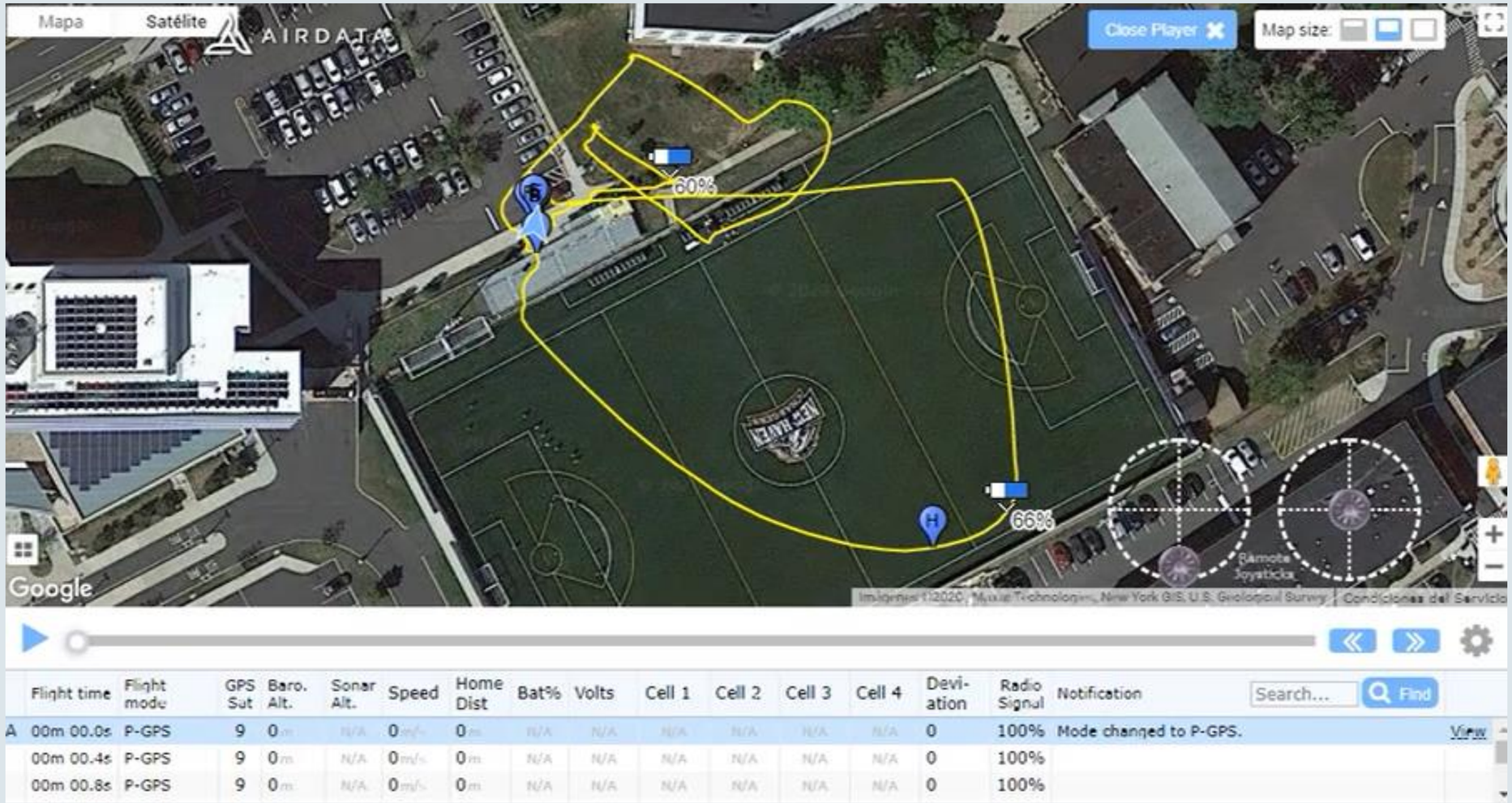
Max Bat Temp
41.95°c

Tips: 2
Warnings: 0

Download: KML GPX (?) CSV Original

Archivos TXT

INTERPRETACIÓN CON AIRDATA - REPRODUCTOR



Archivos TXT

INTERPRETACIÓN CON AIRDATA - MEDIA

Otras evidencias

METADATOS EN ARCHIVOS MULTIMEDIA

- Software ExifDataView

  (https://www.nirsoft.net/utils/exif_data_view.html)

Property ID	Property Group	Property Name	Value Type	Value Length	Value
0x010e	Image	ImageDescription	String	27	DCIM\100MEDIA\DJI_0008.JPG
0x010f	Image	EquipMake	String	4	DJI
0x0110	Image	EquipModel	String	7	FC300C
0x011a	Image	XResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x0131	Image	SoftwareUsed	String	11	Photos 1.5
0x0132	Image	DateTime	String	20	2016:09:26 14:30:31
0x829a	Camera	ExposureTime	Rational	8	19 / 50000
0x829d	Camera	FNumber	Rational	8	2.80
0x9003	Camera	DTOrig	String	20	2016:09:26 14:30:31
0x9004	Camera	DTDigitized	String	20	2016:09:26 14:30:31

PRESENTACIÓN DE RESULTADOS

- ✓ Portada.
- ✓ Introducción/Antecedentes.
- ✓ Motivación y objeto.
- ✓ Descripción de los elementos aportados.
- ✓ Metodología aplicada y desarrollo.
- ✓ Posible relación de causalidad.
- ✓ Conclusiones.
- ✓ Anexos.
- ✓ Firma.

Muchas gracias!

Seguinos en redes sociales

DRONESVIP | Centro de Instrucción de Aeronáutica Civil