DRONE FORENSIC INVESTIGATION: DJI INSPIRE 2 DRONE AS CASE STUDY

2022 – United Kingdom

Peter Snook

Cardiff University

CONTENTS

TABLE OF FIGURES

ABSTRACT

The topic of drone forensics lacks research and available information that can help law enforcement conduct thorough and well executed investigations. As drones are becoming more widespread and popular amongst the general public there is a need for more solutions that provide detailed insights on how certain drones can be analyzed. The DJI Inspire 2 does not have many recorded incidents indicating malicious activities however, many minor cases have involved damage to public and private property. As of 2021 DJI is still the largest drone manufacturers with a 54% market share (DroneDJ, 2021). As the majority of DJI drones use similar hardware and software, forensic analysis of a DJI drone can be of value for any other case regarding a DJI drone.

The gathering and analysis of valuable artifacts found onboard the DJI Inspire 2 (internal and external SD cards), and two mobile devices (Android and IOS) will be provided in this paper. Finding and analysing flight data, visualizing the paths taken by the drone, identifying devices involved, extracting media taken from onboard cameras, and concluding the event will be explored. One of the main methods covered is the use of a geographic information system to analyse the extracted flight data. This particular method allows for advanced control over how the data is presented. The coordinates stored in the flight data can be projected onto specific maps and satellite images. The symbology can then be classified based on other data such as altitude or time making reconstructing an incident a far easier task. An issue stressed upon in this investigation is the drone's creation of unreliable data, many flight data files can contain missing or unrealistic data resulting in flight paths being hard to distinguish. The use of a geographic information system and the Python tool DATIdentifier aims to combat this problem.

The result of this investigation concludes with the devices and systems involved being identified, unreliable flight data was removed, real flight paths were presented, dates and times of flights were found, and media captured was extracted and matched to its relative flight.

1. INTRODUCTION

Drones or Unmanned Aerial Vehicles (UAVs) are aircrafts without human pilots, crew, or passengers. They are a type of Unmanned Aircraft System (UAS) that are controlled via a ground based device. The capabilities of drones are constantly improving allowing for many drones to be tailored for certain applications, some of these include aerial photography, agriculture monitoring, policing, surveillance, and deliveries. In addition to all these great applications where many people benefit, drones are becoming an increasing popular method for carrying out criminal activities, when these incidents occur, they can pose threats to civilians, businesses, and police.

Drone forensics is an emerging branch of digital forensics where the focus is on processing and analysing data extracted from a drone. This involves recovering data stored on the drone itself and any removable media that is used by the drone. The data will be recovered in a forensically sound manner where analysis can be performed on a copy of this data.

Drone forensics is important as drones are becoming an increasing popular method for certain crimes. They are used to smuggle phones, drugs, and weapons into prisons, disrupt airports, invade privacy, and carry out terrorism. When a drone is used to carry out these activities the user controlling the drone can stay hidden resulting in a culprit that is hard to identify and capture. Drone forensics is used to gather evidence that can be provided in court to bring the culprit to justice.

The aim of this report is to explore possible solutions for analysing elements of drone related crimes in the hopes that it will provide beneficial to future investigations. Law enforcement and others who need gather evidence for cases will have a better understanding of what can be achieved.

The main objective is to recover flight related data including paths taken, exact locations, altitudes, date and time stamps and media captured via the onboard camera. Other objectives include recovering serial numbers and identifying the exact devices used. All this is evidence can ultimately be used to arrive at a conclusion that explains what occurred during the drone related incident.

This report will be structured into three main stages where the devices, flight data and the media captured will be analyzed. A final conclusion will be presented at the end to summarize all evidence found. The initial device analysis stage will involve recovering the makes, models, and serial numbers as well as the file structures used by each device and what each file or directory is used for. The flight data will then be recovered from all possible sources. Methods to identify paths, locations, altitudes and date and time stamps will be shown. A small piece of software developed to help identify accurate and reliable flight data will also be provided here. Media captured via the onboard camera will be sorted and matched to the mobile device that was used to control the drone. Using all three of these stages a conclusion can be met which best describes the incident.

2. Background and Literature Review

2.1 Drone Forensic Use Case: DJI Inspire 2

DJI is a Chinese based company and is one of the biggest providers for drones. They have six series currently available (2022) which include the Mavic, Air, Mini, FPV, Phantom and Inspire. There are also many other companies that offer drones such as Parrot, SenseFly, Skydio and Yuneec. These drones can range in price from a couple hundred to a few thousand, making them accessible to most people. The cheaper drones are still able to capture live videos and images making them the perfect choice for illegal activities. All commercial drones will have some sort of handheld device that allows the user to have full control over the device. Handheld devices are usually either a mobile phone or tablet running IOS/Android or a designated radio controller. In the case where a mobile phone or tablet is used the videos and images taken are sent from the drone to the handheld device. This allows media to be captured where the user is in a hidden location.

One particular case involving drones took place at Gatwick Airport from the 19th to the 21st of December 2018 (Wikipedia, 2022). This incident had no culprit, and no evidence of drones was found apart from nearby sightings. 140,000 passengers and 1,000 flights were affected making this a large problem for all parties involved. Drones are able to move around very quickly coming in and out of public view, making them hard to locate and capture. Even if this incident was not intended as a malicious attack, drones simply being in restricted airspace can still cause mass panic.

In more serious cases drones have reportedly been used by the terrorist group ISIS to collect intelligence and carry ammunition including IEDs and bombs. Approximately on the 15th of October 2018 a DJI Phantom 4 was seized by the Headquarters for the Liberation of Al-Sham (The Meir Amit Intelligence and Terrorism Information Center, 2022). In more developed countries such as the UK similar events are much less likely to happen as explosives and weapons are very hard to come across with all the regulations in place. However, it is still a possibility and countermeasures must be in place. Incidents that are more common in developed countries include smuggling contraband into prisons (BBC News, 2022). Similar large scale incidents have occurred in many countries all over the world (Wikipedia, 2022) and future incidents are inevitable. With cheaper drone models being produced these problems will only become more common, increasing the need for forensics.

Special weapons and methods are being produced to take down these drones if they are being misused. These include devices to launch nets, using other drones that crash into them, jammers, hijacking and the most interesting is eagles that have been trained in the Netherlands (IEEE Spectrum, 2022). Once a drone is downed and captured a large amount of data can be extracted and analyzed to help find and capture the culprit.

There are currently few tools available and minimal research has been made to create a concrete solution to this problem. The tools that exist are not professional and are made by hobbyists stressing that they should not be completely relied on for forensics. Different options should be available to ensure consistency and allow for findings to be more trustworthy. In the case of research, the only information on the DJI Inspire 2 is provided by VTO Inc (as of Spring 2022). This being the only report is insufficient and more solutions must exist. DJI drones do share similarities and certain aspects of research can be used with different makes and models. The outlined methods covered in this investigation are not strictly for the DJI Inspire 2.

2.2 Literature Review

In the past decade, many research efforts have been conducted on various models and makes of drones, they mainly focus on drone crimes and drone forensic investigations. (Kao et al, 2019) has summarized key drone forensic investigation methods used for their case study on the DJI Spark Drone. One important aspect of this case study is the "Temporal Rules" (section 5.1) which covers timestamps and what relations they have. Mentioned in this section is how the two different types of flight logs can exist mutually exclusively depending on if the drone has taken flight or only switched on. This will become apparent in the flight data analysis section as it is encountered various times. The next two sections indicate missing values may occur due to network delay and the times recorded on the drone and mobile device may not be synchronized. These three sections are important as they can impact what we may consider reliable flight data.

The section 2.2 Drone Crime Questions provides us with an important ideology that should be considered for any forensic investigation. The 5W1H (who, what, when, where, why, and how) are essential as we can tell a story that recreates the crime or incident. Not all of them can always be found however, the ones that are answered will still provide as valuable evidence. These are good outlines for an investigation however, before we consider them, we must review the challenges of drone forensics. Understanding the problems that we may encounter puts us in a better position for starting an investigation. (Bouafif et al, 2018) presents many of these challenges including the endeavor of identifying ownership if a drone is damaged and scattered in various locations, acquiring forensic images of drones where preserving the integrity of files may not always be possible and embedded storage containers that are concealed or access-protected.

As our drone technology improves over time new challenges will appear and other challenges may have active solutions created for them. Some technology such as the SD card being a storage medium for the majority of drones has stayed the same for many years. (Roder, Choo, Le-Khac, 2018) made a valid point about the likelihood of the current SD cards being upgraded to flash storage. As 4K and longer flights were in demand in 2018, more people having access to drones and devices that support 4K media will only reduce the time before an upgrade is made. The main challenge here is adapting and creating new forensic methods every time a new model of drone is available.

For many drone forensic investigations DatCon (Datfile, 2022) is the only option when it comes to decrypting the flight data files. (Clark et al, 2017) covers the reverse engineering of this program in depth revealing how exactly it works and what methods are used for decryption (Algorithm 2 – DAT payload decrypt algorithm). Based on this, they have created another tool for decrypting the flight data files found on many DJI drones. Optimally DJI would create their own decryption program specifically designed for their drones however, it does not seem they intend to do so. This leaves hobbyists and other individuals to figure it out and create the tools themselves. Having more than one tool for this purpose can be very important, if the flight data found does not seem as expected the decryption can be done via multiple tools to ensure the data is accurate.

3. METHODOLOGY

3.1 DRONE SPECIFICATIONS

The basic components of the DJI Inspire 2 include an internal and external SD card, motors, propellers, two batteries, gimbal, FPV camera, forward and downward vision system, upward infrared sensor, stabilization sensors and a flight control system. The two SD cards must be recovered as they are essential for this investigation.

The internal SD card is not easily accessible to the normal user, the flight logs created by the drone are stored here. These flight logs are stored in DAT format and contain a vast amount of data including but not limited to latitude, longitude, time stamps, altitude, and motor speeds. The external SD houses all media captured via the onboard camera, this includes any videos or images taken.

Other sensors including gyroscopes and accelerometers are used by the drone to enable easier control over the drone, the stabilization is all done automatically. Some of this data is also recorded in the flight logs.

Control over the drone is done via a mobile device, where the operating system can either be IOS or Android. Initially a connection is established over Wi-Fi, this will link the mobile device to the drone. The application used by newer DJI drones is DJI GO V4 (as of May 2022). This allows the user to manually fly the drone, set automatic flight paths, change configuration settings, and download media captured.

3.2 DRONE FORENSIC PROCEDURES

The process for a drone forensic investigation is the same as any other forensic investigation, the same methodology stages are used. The five key procedures of a drone forensic investigation include the acquisition of the devices involved, identifying the devices, preserving all data contained, analysing the data, and then reporting the results as evidence.

3.2.1 ACQUISITION

In drone forensics the acquisition stage aims to gather all data that may be relevant to the investigation. This can include but is not limited to data contained on internal or external SD cards, flight control systems, sensors, controllers, applications, and operating systems.

For this particular investigation the Drone Forensics Program run by VTO Inc has completed the acquisition stage for us, they have provided all the forensic images to be used in this investigation. VTO Inc is located in Broomfield, Colorado, USA. Their research is sponsored by the United States Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD).

```
Manufacturer: DJI
Model Name: Inspire 2
```

Within this investigation MD5 and SHA1 hash values will be used to maintain the integrity of the data. These values are the result of a calculation made by a hashing algorithm. Running the hashing algorithm on the copies used in analysis and the originals that are preserved should result in the

same hash value. If the hash values do not match, we can determine that a change has been made resulting in evidence that cannot be used.

```
Filename: df025_flight_android_physical.001
Size: 5,289,017,344
MD5: e2eb28031a881ea6ee0d1c26b0e4c8e9
SHA1: 721a1f2b719128c6af34c9f9b66d08b220782ae7
Released: 2017-09-03

Filename: df025_flight_ios_backup.zip
Size: 205,796,020
MD5: 5d92366f386f3266be19e20ca1452876
SHA1: 0de13f8b784feef955c677aee980df90dc546626
Released: 2017-09-03

Filename: df025_external_microSD.001
Size: 16,022,241,280
MD5: da330ae0d0015d9481989402eec632f1
SHA1: 0155b8bb2f9d9452277c056409dd99cf9d29fcdf
Released: 2017-09-03

Filename: df025_internal_microSD.001
Size: 7,948,206,080
MD5: 44fd649f3240fd680510a6f14dc8ac9e
SHA1: 49dba0f721fbb0724fa21097f2a92d0bf98f83da
Released: 2017-09-03
```

These files can be accessed from the following google drive:

```
https://drive.google.com/drive/folders/0B1aBvVt_vSSeMG5BMXhZUzI4VW8
```

VTO Inc have made flights that contain the following data:

```
Date(s):
2017-08-29 - flight(s)

Location:
USA-Colorado
```

The GPS coordinate boundaries are four points with latitude and longitude values that create a polygon that can be mapped onto the earth. The flights VTO Inc made using the DJI Inspire 2 will all be contained within this polygon.

```
GPS Coordinate Boundaries: (of salted data flights)
39.965545, -106.217218
39.959745, -106.213494
39.961579, -106.223373
39.957534, -106.221186

Time Zone: (during salted data flights)
North America - Mountain Daylight Time (MDT)

UTC offset: (during salted data flights)
UTC -6
```

3.2.2 IDENTIFICATION

An important step of any forensically sound investigation is identifying what evidence items are involved. For a drone related incident, the two main evidence items will always be the drone itself and the connected controller or mobile device. A description of all systems involved should be made including makes, models and serial numbers. These can then be matched with the data contained on the device to confirm that the evidence found does originate from that device. Drones should have serial numbers on their electronic components, some may only be revealed once the drone has been taken apart. Controllers and mobile phones involved will also contain a serial number unless tampered with.

3.2.3 PRESERVATION

All suspected devices must be isolated and secured. This preservation stage is done to ensure that the evidence cannot be tampered with, and it remains in the exact same state as when it was acquired. Using forensically sound methods a copy of the data contained on the devices can be made. Only the copy should be used for analysis as this removes all possibilities of damaging the integrity of the original. If the original data is altered or written to it will destroy all integrity of the evidence and it can no longer be used in court.

3.2.4 ANALYSIS

After the acquisition, identification, and preservation stage the process of analysis can begin. The analysis stage involves finding and extracting artifacts that can be used to reconstruct an incident and serve as evidence for a case. This investigation will mainly focus on the analysis stage as the acquisition stage has been completed for us. Unfortunately, VTO Inc has not provided any information regarding the make and models of devices involved (excluding the DJI Inspire 2 drone) so we cannot complete the identification stage. As VTO Inc is a trusted program employed by the united states we can assume the preservation stage has been adhered to. Hash values for every file used will be provided so that the artifacts found can have their integrity checked.

The analysis stage for this drone forensic investigation will involve four main areas:

- Find out exactly what devices were involved.
- Find the paths taken by the drone during its flight.
- Extract all images, videos and thumbnails taken or created by the drone.
- Reconstruct the events and reach a conclusion on what occurred.

This investigation will use different devices, tools, and software throughout. These will be used to recover the evidence items needed to meet the objectives. The devices, tools and software used are described in Table 1 – Tools, Software and Devices used During Analysis.

Tools, Software and Devices	Description
DJI Inspire 2	Drone (UAV)
Android Mobile Device (Samsung Galaxy Tab A)	Controller #1 used for flight
IOS Mobile Device (iPad Mini 4)	Controller #2 used for flight
DJI GO V4 Application	IOS and Android application used to control drone
Autopsy V4.19.2	Open source digital forensics platform
HxD V2.5.0.0	Hex, disk, and memory editor
7 Zip	Open source file archiver
Oracle VM VirtualBox	Type-2 hypervisor for x86 utilization
DB Browser (SQLite)	Visual, open source tool to create, design and edit database files
DatCon V4.2.3 & CSV View V4.2.5	Free offline application that provides the means to analyze log files produced by many DJI drones
Python V3.9	High-level, interpreted, general-purpose programming language.
DCode V5.5	Free forensic utility for converting data found on desktop and mobile devices into human readable timestamps
QGIS V3.24.0	Open-source cross platform desktop geographic information system application that supports viewing, editing, printing, and analysis of geospatial data
ProperTree	Cross platform GUI plist editor written in Python
ALEAPP	Module used for mobile analysis in Autopsy

TABLE 1 – TOOLS, SOFTWARE AND DEVICES USED DURING ANALYSIS

3.2.5 PRESENTATION

Once analysis has been completed where all evidence items needed to make a strong case are obtained, the results can then be presented in such a way that it is clear to the reader what occurred during the incident. All files presented must have their corresponding hash values to ensure that they can be matched to the original. Every step during analysis must be shown including what the evidence items is, where it was found, and how it relates to the case. Screen captures can be shown to help visualize certain aspects, for this investigation many screen captures will be used to illustrate the flight paths and file contents.

4. Initial System Analysis

As mentioned in 3.2.4 Analysis VTO Inc does not provide any specifics on makes, models and serial numbers of devices they used (excluding the drone model) so we cannot match any values. If this were a case where the devices are available for inspection, values found in the extracted data can be compared the serial and model numbers that should be present on the device.

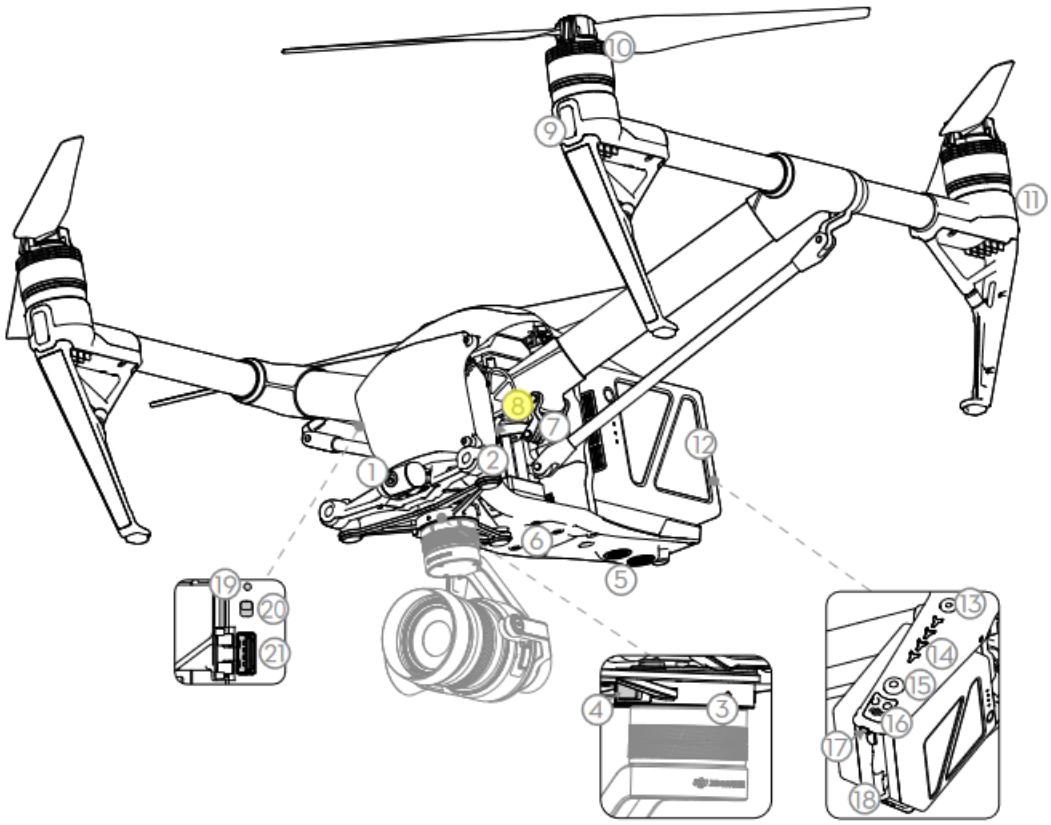
VTO has provided a total of four forensic images:

- Physical Android image.
- IOS backup saved as a compressed file.
- Internal SD card image. This is not easily accessible and is found inside amongst the drones' components and has to be physically removed.
- External SD card image. This is stored on the outside of the drone for easy access.

Two sets of flights were made, set one was created using an Android device as the controller and the other used an IOS device. We should expect to see different flight paths and details for each controller device.

The internal and external SD cards contain data that is a combination of both sets of flights. The flight paths, videos and images captured will have to be matched with their corresponding controller device.

As shown in Figure 1 - Components of a DJI Inspire 2 only the external SD card is shown in the blueprints, it is likely that attempting to access the internal SD card will void any warranty and is not recommended for the normal user.



[1] FPV Camera

[2] Forward Vision System

[3] DJI Gimbal Connector V2.0 (DGC2.0)

[4] Gimbal and Camera Detach Button

[5] Downward Vision System

[6] Extended Device Mounting Position

[7] Transformation Mechanism

[8] Control and Processing Center (with Micro SD Card Slot)

[9] Front LEDs

[10] Propulsion System (with Motors, Propellers, etc.)

[11] Rear LEDs

[12] Intelligent Flight Batteries

[13] Power Button

[14] Battery Level Indicators

[15] Battery Remove Button

[16] Upward Infrared Sensor

[17] Aircraft Status Indicator

[18] DJI CINESSD Slot

[19] Linking Button

[20] USB Mode Switch

[21] USB Port

FIGURE 1 - COMPONENTS OF A DJI INSPIRE 2

4.1 DJI Inspire 2 Drone System Analysis

4.1.1 Drone System Description

The DJI Inspire 2 is a drone (UAV) manufactured by DJI. It was released in late 2016 with a starting price of approximately 3,688 GBP. The drone has built in sensors to help with obstacle avoidance, a new autopilot mode and a choice of UHD cameras. It has a maximum speed of 67 miles per hour with an acceleration of 50mph in 4 seconds. The propellers also enable flying to 2500 to 5000 meters above sea level.

4.1.2 Drone System Analysis

As VTO did not provide serial numbers for the drone itself we cannot confirm any values found. For other cases where you have access to the drone, the components on board should have their serial numbers recorded. Both the Android and IOS devices will be used in this investigation to find serial numbers regarding the drone.

The Android DJI GO application creates a directory in the data section that contains many databases. One valuable database is `[dji.db]`, located at `[data/dji.go.v4/databases]`. Viewing the table `[dji_pilot_publics_model_DJIDeviceInfoStatModel]` provides us with various serial numbers that should be present on the drone. The serial numbers found are shown in Figure 2 – Serial Numbers Present on Android Device.

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Table: dji_pilot_publics_m... | 6 entries | Page 1 of 1 | Export to CSV

id	apptype	createtime	isUploaded	guid	appversion	deviceversion	productype	devicetype	devicesn	user
1	1	1503789052366	1	4453f10b-b39a-442f-a86c-d335aebd1c3b	4.1.5	03.02.35.05	17	1	095XDCK002002W	droneforensics@vtoinc.com
2	1	1503789052424	1	6c0a4444-9773-4b2c-82a1-c9590d862ed3	4.1.5	03.02.35.05	17	2	09UADBH03101HA	droneforensics@vtoinc.com
3	1	1503789052456	1	4b6e2716-3b9b-4818-acc6-d390f616f66c	4.1.5	05.21.24.00	17	3	09KL3A025L	droneforensics@vtoinc.com
4	1	1504034256879	0	8f807600-8dd6-4961-9d3d-48f998af72a7	4.1.5	00.00.00.00	17	2	09UADBH03101H2	droneforensics@vtoinc.com
5	1	1504034271746	0	8cdde560-c9ef-498f-842f-991804da11f2	4.1.5	03.02.89.65	17	0	09CLDCL0050205	droneforensics@vtoinc.com
6	1	1504034271885	0	fa4154b7-1a8b-4e7e-be4e-68425458eff5	4.1.5	03.02.35.05	17	2	09UADBH03101H2	droneforensics@vtoinc.com

FIGURE 2 – SERIAL NUMBERS PRESENT ON ANDROID DEVICE

Unfortunately, the application DJI GO 4 for IOS does not have this equivalent. The log device serial number can be found located in the property list file `[com.dji.go.plist]` (Figure 3 – Serial Numbers Present on IOS Device). The value found is 095XDCK002002W. This file should be saved as it contains more valuable artifacts that can be use later on.

DJILastCommonUpgradeLogFileTime	NUMBER	5.25632576E8
AIRCRAFT_FLIGHT_LOG_DEVICE_SN	STRING	095XDCK002002W
showVoltageOnMainScreen	BOOLEAN	

FIGURE 3 – SERIAL NUMBERS PRESENT ON IOS DEVICE

Knowing these serial numbers is key to linking the mobile devices to the drone. As the same serial number can be found on both the IOS and Android devices, we know that both mobile devices acted as a controller for the exact same drone.

4.2 IOS SYSTEM ANALYSIS

4.2.1 IOS DESCRIPTION

Apple Inc. is an American multinational technology company that specializes in consumer electronics, software, and online services (Wikipedia, 2022). As Apple is the second largest mobile phone manufacturer with 1231 million active iPhone units (Business of Apps, 2022) it is important that there is research investigating IOS backup files. The method Apple uses to structure their IOS backup files is awkward to deal with and cannot be navigated easily without understanding.

4.2.2 IOS FILE STRUCTURE

The overall structure is shown in Figure 4 – IOS File Structure. The folder labelled 00 – ff indicates all possible combinations from 00 to ff, i.e. [00], [01], …, [0f], [10], …, [fe], [ff]. This will total 256 directories, excluding the 4 other files found in the system.

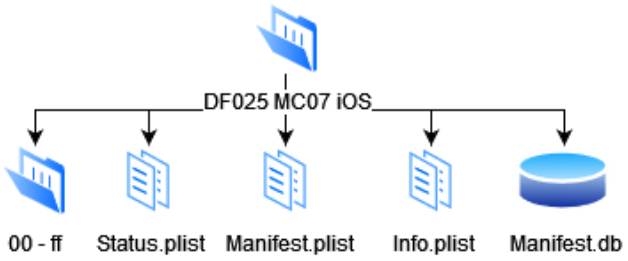


FIGURE 4 – IOS FILE STRUCTURE

All IOS data is stored across the files 00 to ff, the files found in each directory are labelled with a hash value resulting in the directory and file type being unknown. To find this information we need the `[Manifest.db]` database, this contains what each hash value corresponds to. Opening the database in DB Browser results in its hash, domain, relative path, flags, and file. An example is shown in Figure 5 – Contents of Manifest.db.

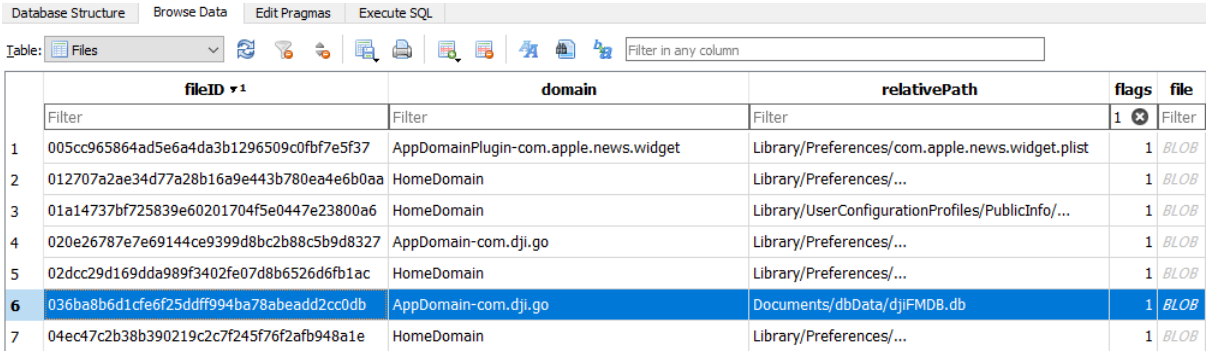
Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: Files — Filter in any column

	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	Filter	Filter
1	4d346d67b1288f4f39ff1218374604ef61d28d20	SysContainerDomain-com.apple.lskdd		2	BLOB
2	71d830da67bcc1a3404a3fa55e6bd6078b45b315	SysContainerDomain-com.apple.lskdd	tmp	2	BLOB
3	54f67d809a0c6389f6077eda64d037a044841788	SysContainerDomain-com.apple.lskdd	Library	2	BLOB
4	ed760fe4ac85871e0b40368327e2bb483d23cc1e	SysContainerDomain-com.apple.lskdd	Library/Preferences	2	BLOB
5	21582ee01def7d9a3c37897ac599f22bdd764a51	SysContainerDomain-com.apple.lskdd	Documents	2	BLOB
6	1edc75757be51191943ae2210cbd839251800c47	AppDomain-com.apple.PassbookUIService		2	BLOB
7	80de008162f467e49120f89d0df4a22afded028c	AppDomain-com.apple.PassbookUIService	Library	2	BLOB
8	5fe1c0a8f141b820af2e66483ccd14913758078d	AppDomain-com.apple.PassbookUIService	Library/Preferences	2	BLOB
9	27a1bd9387371704cb708542c38ed83059da85bd	AppDomain-com.apple.PassbookUIService	Documents	2	BLOB
10	37b5b83449500ce6965cff1a708392049f6bb2c4	AppDomain-com.apple.ServerDocuments		2	BLOB
11	89fb03dd9b109a933509845657d167174b934e73	AppDomain-com.apple.ServerDocuments	Library	2	BLOB
12	c789672aa9c6cc0ac37916e14f12b780c38d2aef	AppDomain-com.apple.ServerDocuments	Library/Preferences	2	BLOB
13	e441b0bab60ce3d29bf5696a2f4ba994f0cb0051	AppDomain-com.apple.ServerDocuments	Documents	2	BLOB
14	a06d938bcd85926fc0ddf52b9afb5d17a0195ece	SysSharedContainerDomain-...		2	BLOB

FIGURE 5 – CONTENTS OF MANIFEST.DB

As an example, to locate the file `[Documents/dbData/djiFMDB.db]`, take the first two values in its hash, in this case it is `[03]` as shown in Figure 6 – Details of djiFMDB.db.



	fileID	domain	relativePath	flags	file
	Filter	Filter	Filter	1	Filter
1	005cc965864ad5e6a4da3b1296509c0fbf7e5f37	AppDomainPlugin-com.apple.news.widget	Library/Preferences/com.apple.news.widget.plist	1	BLOB
2	012707a2ae34d77a28b16a9e443b780ea4e6b0aa	HomeDomain	Library/Preferences/...	1	BLOB
3	01a14737bf725839e60201704f5e0447e23800a6	HomeDomain	Library/UserConfigurationProfiles/PublicInfo/...	1	BLOB
4	020e26787e7e69144ce9399d8bc2b88c5b9d8327	AppDomain-com.dji.go	Library/Preferences/...	1	BLOB
5	02dcc29d169dda989f3402fe07d8b6526d6fb1ac	HomeDomain	Library/Preferences/...	1	BLOB
6	036ba8b6d1cfe6f25ddff994ba78abeadd2cc0db	AppDomain-com.dji.go	Documents/dbData/djiFMDB.db	1	BLOB
7	04ec47c2b38b390219c2c7f245f76f2afb948a1e	HomeDomain	Library/Preferences/...	1	BLOB

FIGURE 6 – DETAILS OF DJIFMDB.DB

The corresponding directory `[03]` will contain this file (Figure 7 – Location of djiFMDB.db in File System). The file can be extracted in the correct type for further analysis.

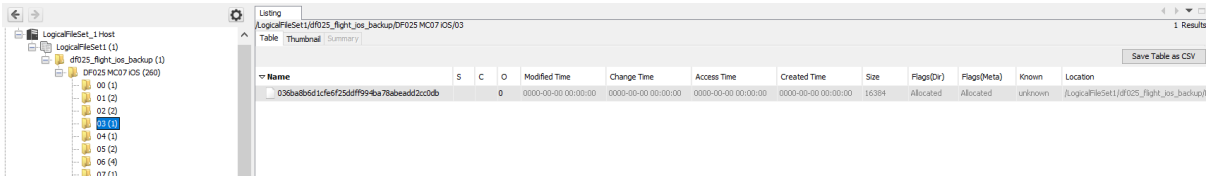


FIGURE 7 – LOCATION OF DJIFMDB.DB IN FILE SYSTEM

Many important evidence artifacts are MacOS Property List files, to analyse the contents of these files the Python program ProperTree as specified in Table 1 – Tools, Software and Devices used During Analysis will be used. This is a useful tool made for viewing any file with the extension .plist.

4.2.3 IOS SYSTEM ANALYSIS

All information regarding the IOS device's make, model and serial number is contained in `[Info.plist]`. This file is not contained in directories 00 to ff, it is in the root of the physical Android image as shown in Figure 4 – IOS File Structure.

Extraction of the Info Property List file provides us with the information shown in Figure 8 – Contents of Info.plist. The device model is an iPad mini 4 with the serial number FNWV3043GHK9. Looking up the serial number with Apples coverage checker (Apple, 2022) confirms that this serial number is an iPad mini 4. This information should be recorded and matched with the serial number found on the back of the device to confirm that further data found in the IOS Backup files do in fact come from this device.

Build Version	String	14F89
Device Name	String	MC 07 - iOS
Display Name	String	MC 07 - iOS
GUID	String	4974258921CF06FD576EA58786569705
Installed Applications	Array	1 child
0	String	com.dji.go
Last Backup Date	Date	Aug 29, 2017 07:20:13 PM
Product Name	String	iPad mini 4
Product Type	String	iPad5,1
Product Version	String	10.3.2
Serial Number	String	FNWV3043GHK9
Target Identifier	String	910c76c14ed64ee886ffdd2611665d842aec939b
Target Type	String	Device
Unique Identifier	String	910C76C14ED64EE886FFDD2611665D842AEC939B
iTunes Files	Dictionary	4 key/value pairs
IC-Info.sidv	Data	<00010001 AD82D365 A3DFC4FF A9A99B7A DBC16C12 (
VoiceMemos.plist	Data	<3C3F786D 6C207665 7273696F 6E3D2231 2E302220 656E
iTunesPrefs	Data	<66727064 01001800 01010001 1E1ECDDD 6A4662BC 1A(
iTunesPrefs.plist	Data	<3C3F786D 6C207665 7273696F 6E3D2231 2E302220 656E
iTunes Settings	Dictionary	0 key/value pairs
iTunes Version	String	12.6.2.20

FIGURE 8 – CONTENTS OF INFO.PLIST

4.2.4 MD5 HASH VALUES OF IOS SYSTEM FILES

File Name	MD5
Info.plist	0e69cea1794086544a3770a3b30a3db9

HASHES 1

4.3 Android System Analysis

4.3.1 Android Description

Android is a mobile operating system based on a modified version of the Linux kernel and other open source software (Wikipedia, 2022). A large majority of mobile devices run Android OS, large companies such as Huawei and Xiaomi can create their own devices and modify the Android OS into a version that is tailored towards their devices and users. Because of this, the location of certain files and directories may vary depending on the version of Android running on the device.

4.3.2 Android System Analysis

In Autopsy we can add the Physical Android Image as an evidence item and using the ALEAPP module we can gather some basic information on what type of device was used. In Figure 9 – ALEAPP Android Details we can identify the mobile device used was a Samsung tablet. This is not enough information on its own to identify the device used as Samsung offer a large range of tablets. To improve the credibility of this evidence the exact model and serial number must be obtained. The data used in the case can then be matched back to the original device seized.

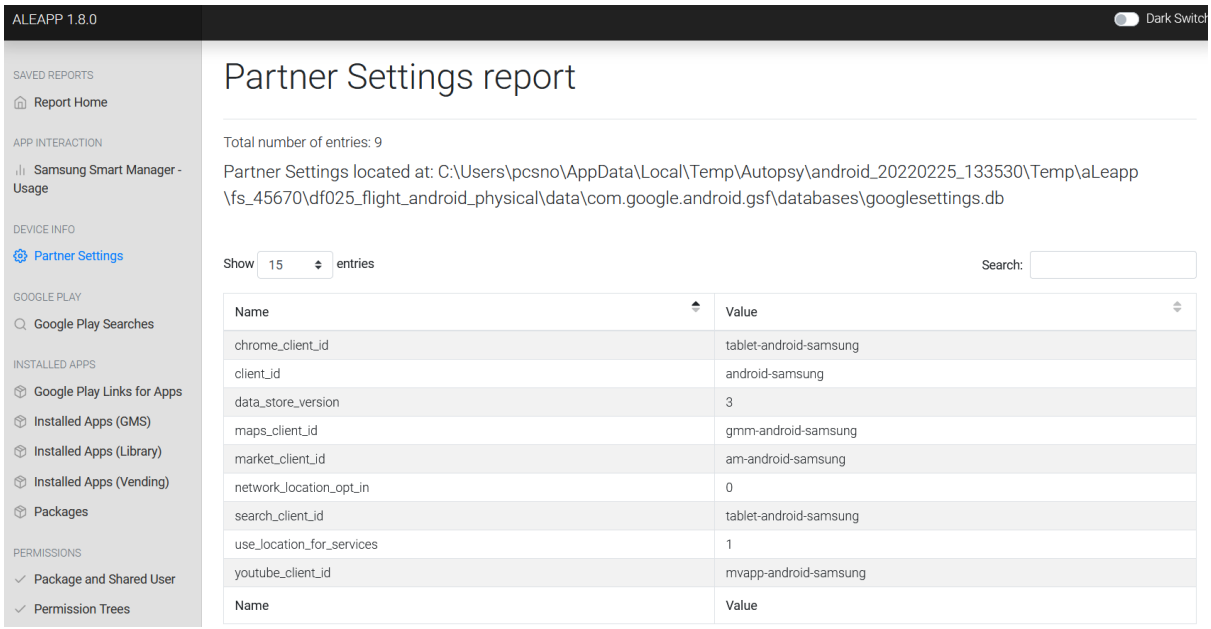


FIGURE 9 – ALEAPP ANDROID DETAILS

To find the exact details of the mobile device in question a deeper look into its files is needed. Many directories and files can be found on Android systems. The vast majority of these files are not useful and should be ignored for any investigation as it will only waste time. One particular file that is essential for identifying the Android device is located at `[misc/wifi/p2p_supplicant.conf]`. All required information regarding the Samsung Tablet can be found here as shown in Figure 10 – Contents of p2p_supplicant.conf. Further information regarding this file and all of its contents can be found on Google Git (Google, 2022).

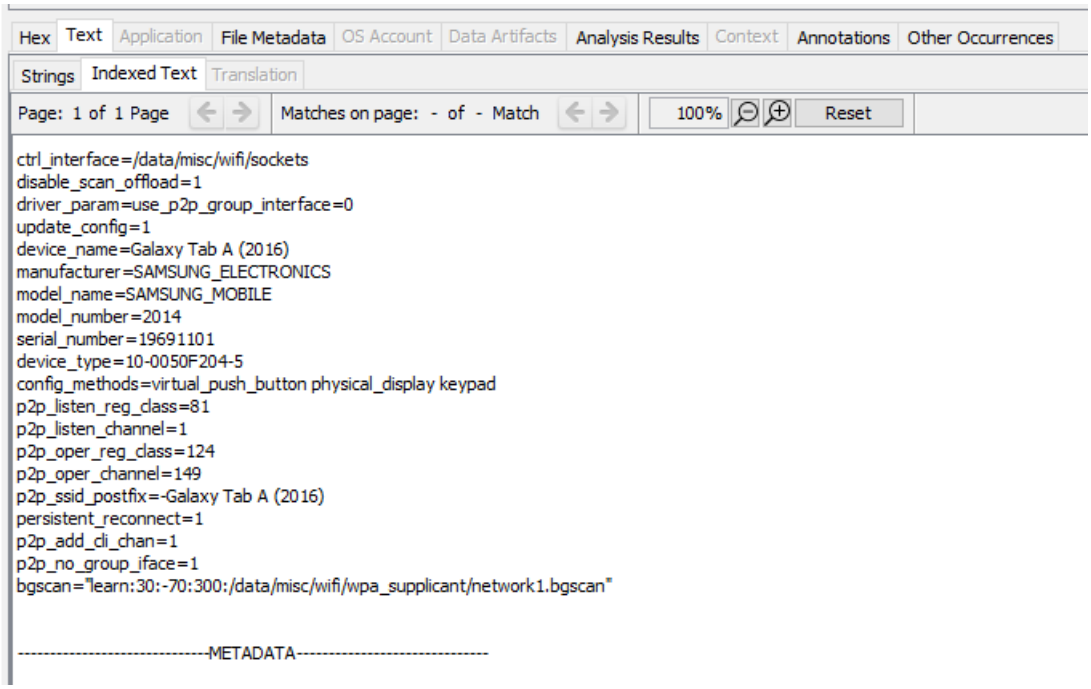


FIGURE 10 – CONTENTS OF P2P_SUPPLICANT.CONF

The device can be identified as a Samsung Galaxy Tab A (2016) with the serial number 19691101. The important details are shown in Table 2 – Android Specifications. This information can be compared to the values found on the real device to prove further evidence obtained does in fact originate from the seized mobile device.

Key	Value
device_name	Galaxy Tab A (2016)
manufacturer	SAMSUNG_ELECTRONICS
model_name	SAMSUNG_MOBILE
model_number	2014
serial_number	19691101
device_type	10-0050F204-5

TABLE 2 – ANDROID SPECIFICATIONS

4.3.3 MD5 Hash Values of Android System Files

File	MD5
p2p_supplicant.conf	52e6ee049863d9cbb8861b12cd9eeb5f

HASHES 2

4.4 External SD Card System Analysis

4.4.1 External SD Card System Analysis

The external SD card is located on the outside of the drone shown in Figure 1 - Components of a DJI Inspire 2 and Figure 11 – Location of External SD Card. It is easily accessible to the general user as it contains the images and videos taken by the drone. These contents are what the majority of consumers are interested in. Using a location like this allows for the media to be quickly transferred to other devices.

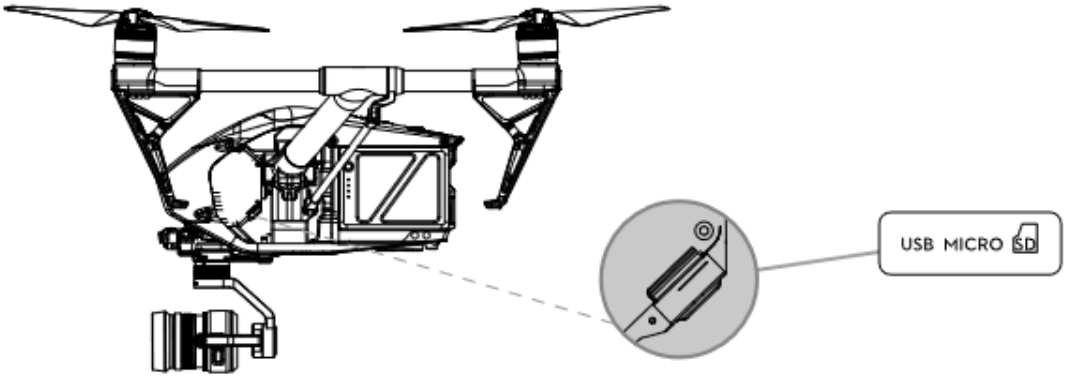


FIGURE 11 – LOCATION OF EXTERNAL SD CARD

The overall structure of the external SD card is shown in Figure 12 – External SD Card File Structure. To identify what exactly each directory's purpose is we can inspect `[CameraLogCur.log]`, all formatting applied to the SD card and camera configuration settings are recorded in this log file. For this certain case, bytes located at offset 517 to 6DA contain all information needed to understand the structure (Figure 13 – Contents of CameraLogCur.log).

The `[MISC]` directory is labelled as private and is likely hidden from normal view as the contents are not needed by most users. Four further directories are contained in `[MISC]`, `[IDX]` is a repair directory and DJI offer no details on what purpose it serves. Closer inspection leads to no useful information contained in any of the four idx files. `[IDX]` can be ignored for this investigation. `[THM]` contains all thumbnails for each video taken, these will be useful along with the videos in `[100MEDIA]` to identify where exactly the drones flight took place. All log files created by the drone are stored in `[LOG]`. The DJI Inspire 2 creates two log files, `[CameraLogCur.log]` is explained above and `[WM620_FW_LOG_AB.txt]` stores all firmware upgrades. Reading the data contained in this file shows the most recent upgrade was loader version 01.01.1418 and firmware version 01.06.1582, this change was made on 2017.08.28 at 11:05:58 (Figure 14 – Contents of WM620_FW_LOG_AB.txt). `[CameraLogCur.log]` contains additional data that can be of further use during analysis of the media captured via the drone. This file will be explored in more detail in the media analysis section. The last directory found in `[MISC]` is `[XCODE]` which was defined simply as Xcode. Xcode is an Apple product for creating software development kits (SDK), this directory is likely used for importing custom SDKs. For this investigation no files were present in `[XCODE]`.

The only other directory present on the external SD card is `[DCIM/100MEDIA]`, all media taken by the drone is stored in this location. The files created here will be visible and accessible to all users.

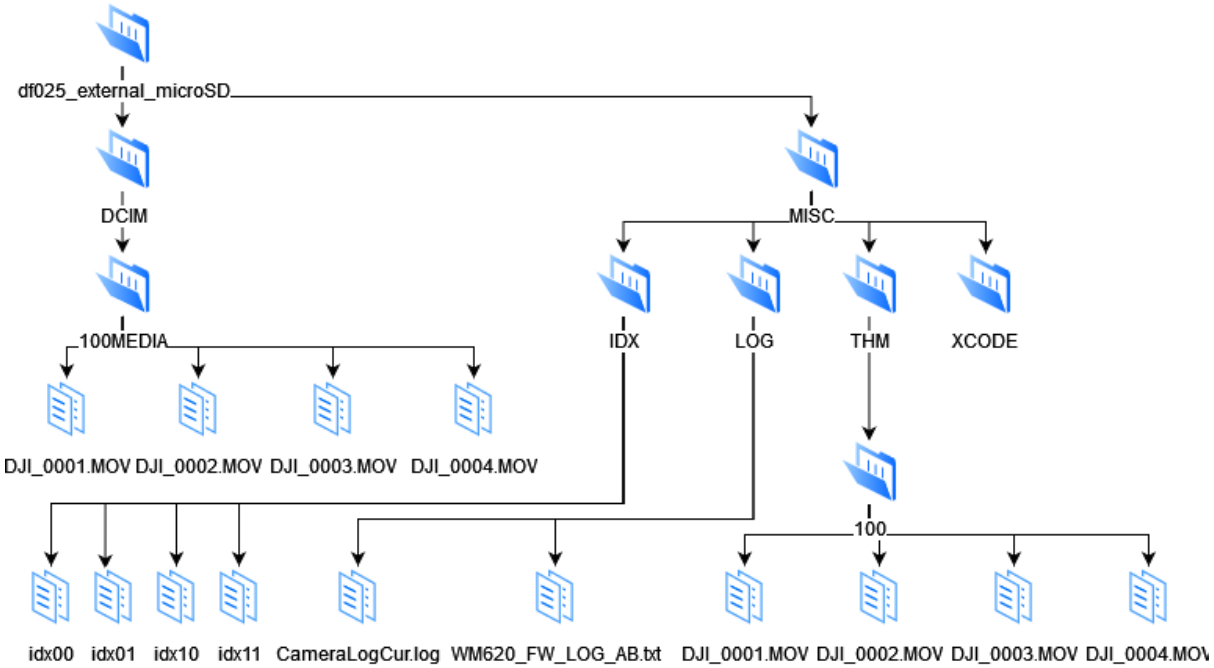


FIGURE 12 – EXTERNAL SD CARD FILE STRUCTURE

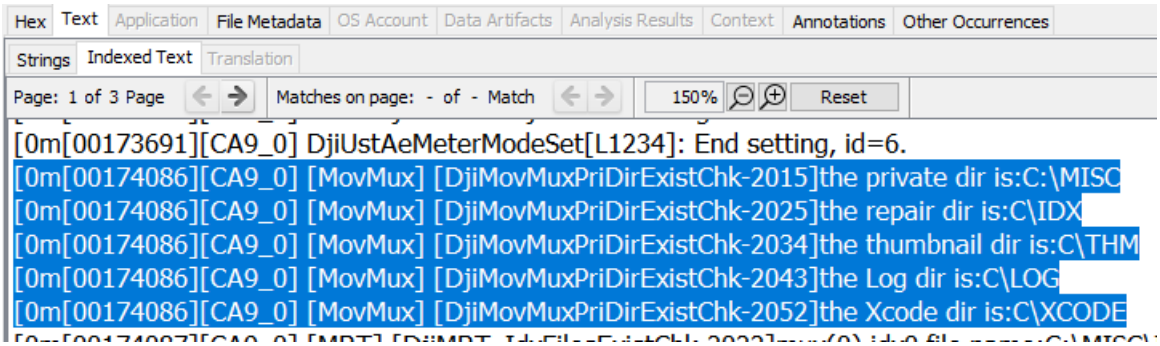


FIGURE 13 – CONTENTS OF CAMERALOGCUR.LOG

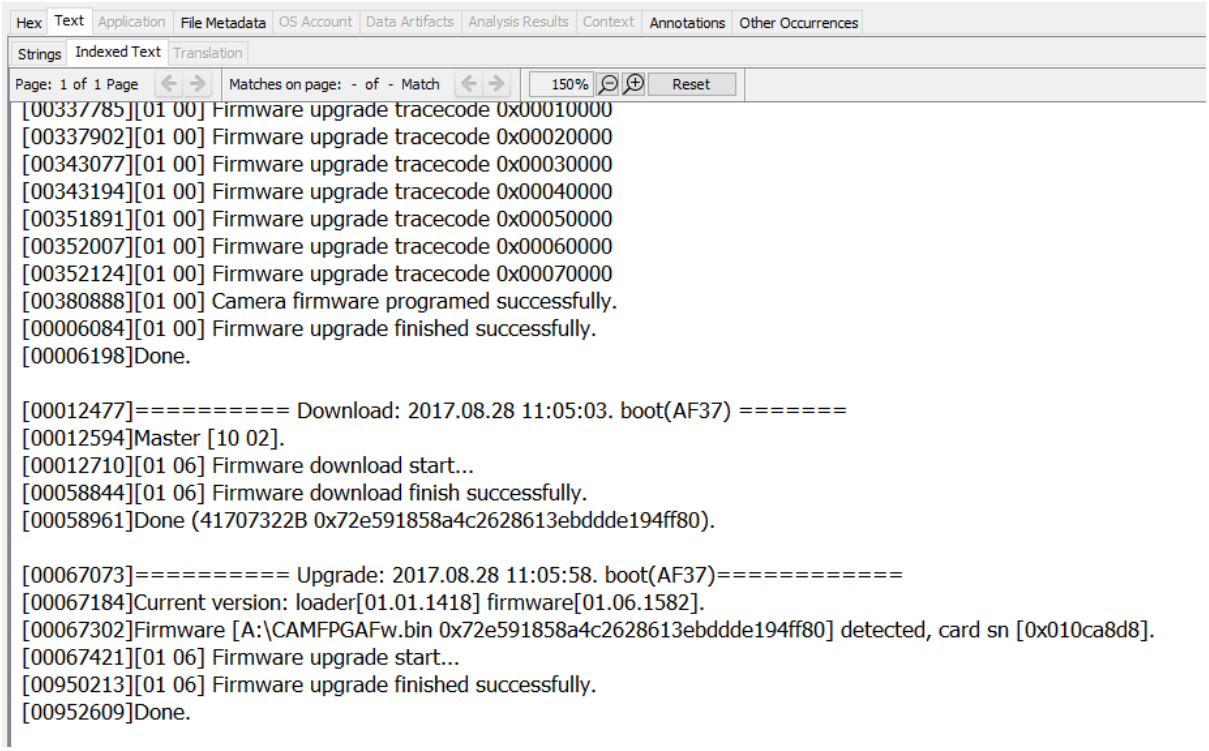


FIGURE 14 – CONTENTS OF WM620_FW_LOG_AB.TXT

4.4.2 MD5 Hash Values of External SD Card System Files

File	MD5
CameraLogCur.log	873a3608e4f817db65abb4e64b50b3f4
WM620_FW_LOG_AB.txt	8be349f6685ec6c6c371105b8863aa23

HASHES 3

4.5 Internal SD Card System Analysis

The internal SD card is not easily accessible without disassembly, the majority of drones with GPS capabilities will have an SD card located amongst its internal components. To retrieve its contents, it will need to be physically removed. The utmost care must be taken with its removal as flight logs are located here and are essential to discovering the flight paths the drone has taken.

Each flight will create a corresponding `[FLYXXX.DAT]` file. The value represented with `[XXX]` will increment after each flight creating logs labelled `[FLY000.DAT]`, `[FLY001.DAT]` and so on. `[PARM.LOG]`, logs the creation of the `[FLYXXX.DAT]` files and contains some vague configuration settings. It does not have any relevant information to flight paths and is not useful in this investigation. `[SYS.DJI]` also does not contain any useful information, only sixteen bytes of data can be found with no readable meaning.

The data retrieved from the internal SD card contains thirteen `[FLYXXX.DAT]` files. The flight data will include paths taken with both the Android and IOS device acting as the controller. The flight data will need to be sorted and matched to the device and its corresponding files. The overall structure of the internal SD card is shown in Figure 15 – Structure of Internal SD Card.

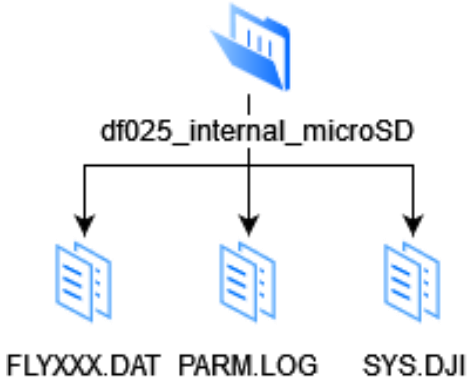


FIGURE 15 – STRUCTURE OF INTERNAL SD CARD

5. Flight Data Analysis

5.1 Flight Data Introduction

A whole host of data is created from start to end of a drone flight. The state of each component is stored along with a time stamp allowing for complete reconstruction of the flight taken. This is the case for most drones that have GPS and advanced capabilities. Many DJI drones are built to a high standard and will do the above, this includes the Inspire, Mavic, Phantom and Air series. However, cheaper drones that are not intended for such professional applications are unlikely to store many details.

5.1.1 DAT and TXT Flight Data File Formats

DJI drones store their flight data in two different formats which are DAT and TXT. These formats are not exclusive to DJI, they are generic data and text files which can be viewed with any text editor. The main issue with the flight data DJI drones create is that they are encrypted with their own technique. They do not provide any software or equipment to decrypt them which can make dealing with them a hassle as third party programs are needed. There are currently very few methods for decrypting these files, both the DAT and TXT formats need different software and programs to successfully extract readable information.

5.1.2 Methods for Reading DAT and TXT Files

DatCon (Datfile, 2022) is recommended by most enthusiasts as it returns a comprehensive spreadsheet with the majority of all data contained on the SD card. It was developed and distributed as of January 2016 with the last update being made on the 20th of July 2021. As of April 2022, DatCon only works with the DAT file format. Another program called CsvView (Datfile, 2022) was created by the same people to cover the TXT format, it also provides a way to visualize both .DAT and TXT log files.

There are other methods that will be explored as being bound to one method for forensic analysis is not optimal. The use of AIRDATA, founded in 2015 and provides a comprehensive drone fleet management operation platform (Airdata UAV, 2022) and QGIS, an Open Source Geographic Information System (QGIS, 2022) will bring other options for creating a case. The TXT files created can be decrypted and viewed in AIRDATA with a friendly user interface that enables easy reconstruction of the flight. DAT files will still need to be decrypted with DatCon, however, QGIS allows for more control over visualizing the paths taken by the drone in question.

Both formats can be found on any mobile device acting as the controller. Whereas the internal SD card will only contain the DAT log files.

5.1.3 DAT Format Challenges

Unfortunately, a problem exists with the DAT format which results in some files that do not contain reliable data and many of their entries are missing. These files can be identified to some degree of accuracy and discarded. A program has been created to help deal with finding these poor quality files, this is covered in 5.5 DAT Identifier Python Program. It should be noted the program is only there to help make decisions.

5.2 Android Flight Data Analysis

5.2.1 Android DJI Application Analysis

ALEAPPs generated report provides an insight into the applications downloaded on the Android device (Figure 16 – Applications Installed on Android Device). Two flight applications were downloaded which include DJI GO 4 and FreeFlight Pro. As VTO Inc have conducted research on many other drones the install of FreeFlight Pro was likely not used for the Inspire 2 as it is designed for drones made by Parrot. DJI also offer a very wide range of applications for different models, shown in Table 3 – Applications Provided by DJI. DJI GO 4 was used for this case and it should be noted that the location of certain files may differ depending on what application was used. The account linked to Google Play services can also be found in the Library section of ALEAPP shown in Figure 17 – Account Linked to DJI GO V4 Application, here the email vto.drone@gmail.com is found.

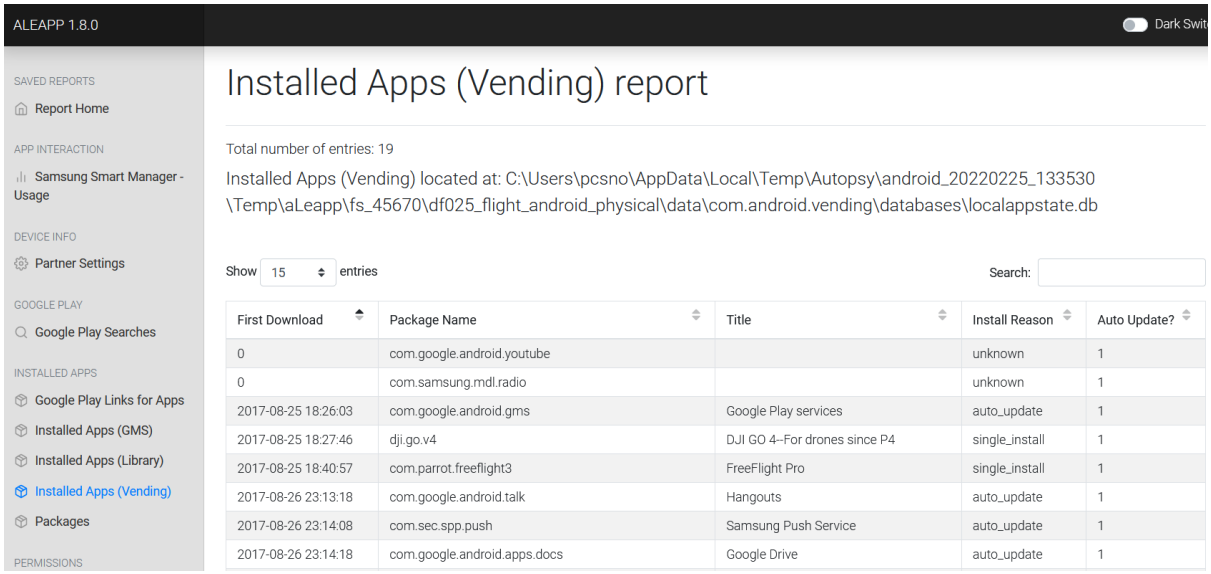


FIGURE 16 – APPLICATIONS INSTALLED ON ANDROID DEVICE

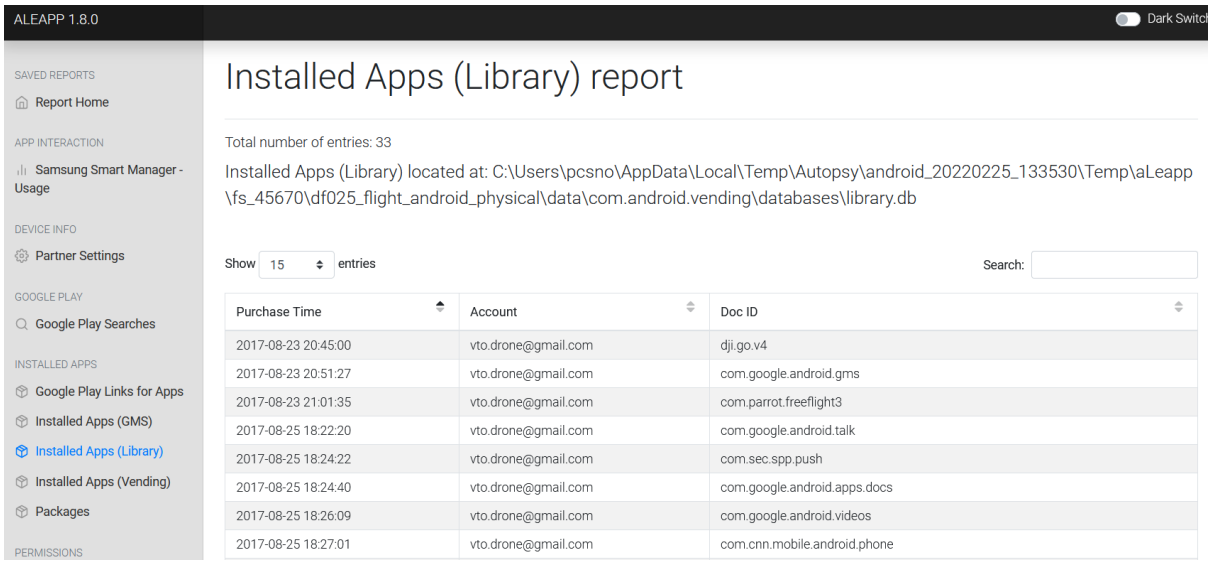


FIGURE 17 – ACCOUNT LINKED TO DJI GO V4 APPLICATION

DJI Flight Applications

DJI Fly	DJI Mimo	RoboMaster	DJI GS Pro (iPad)
DJI Ronin	DJI Pilot	Tello App	DJI Ronin Assistant
DJI Pilot PE	DJI Virtual Flight	Tello EDU APP	DJI GO & GO 4

TABLE 3 – APPLICATIONS PROVIDED BY DJI

The DJI GO 4 application stores its contents in various locations, important artifacts are somewhat easy to find as they are clearly labelled. The flight logs that are needed to determine the paths taken are located in the directory `[media/0/DJI/dji.go.v4/FlightRecord]`. Inspection of this location presents two TXT formatted flight logs. A further directory labelled `[MCDatFlightRecords]` can also be found where its contents contain three DAT formatted flight logs. These five files should provide enough information to reconstruct the route taken by the drone.

5.2.2 TXT Formatted Flight Data Analysis

The TXT flight logs will be analyzed first as AIRDATA can provide us with a quick overview and details including location, drone model and serial numbers. The flight [`DJIFlightRecord_2017-08-29_[13-18-04].txt`] was conducted on the 29th of August, 2017 at 1:18:04PM. The following flight [`DJIFlightRecord_2017-08-29_[13-23-50].txt`] was made approximately 5 minutes later at 1:23:50PM.

The overview of [`DJIFlightRecord_2017-08-29_[13-18-04].txt`] is shown in Figure 18 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-18-04].txt. The path of the drone is accurately mapped onto a satellite image with various values provided that are recorded by the onboard sensors and components. The exact location of activity via drone can be found with this overview, further coordinates and addresses are also specified in the details section as shown in Figure 19 – Time and Location of DJIFlightRecord_2017-08-29_[13-18-04].txt. From the longitude, latitude and address we can determine this flight took place in Arapaho and Roosevelt National Forests, Denver, Colorado. We can also identify the drone used was a DJI Inspire 2, AIRDATA provide the name of drone and camera along with various serial numbers that can be looked up and matched to make the confirmation (Figure 20 – Android Drone Details).

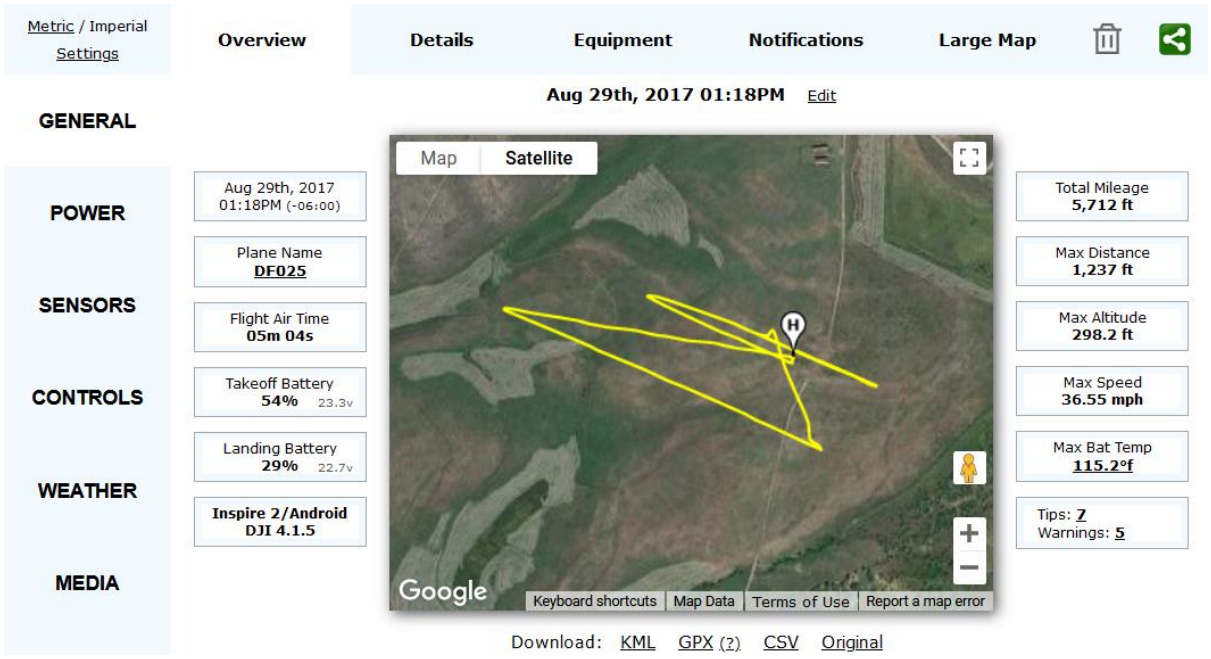


FIGURE 18 – AIRDATA OVERVIEW OF DJIFLIGHTRECORD_2017-08-29_[13-18-04].TXT

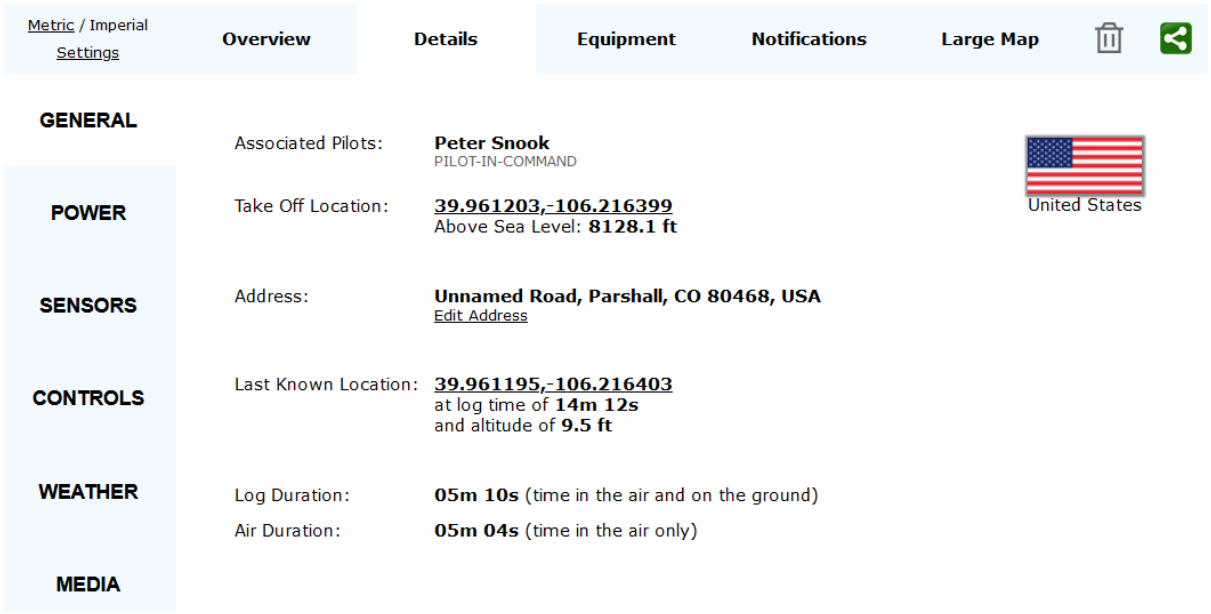


FIGURE 19 – TIME AND LOCATION OF DJIFLIGHTRECORD_2017-08-29_[13-18-04].TXT

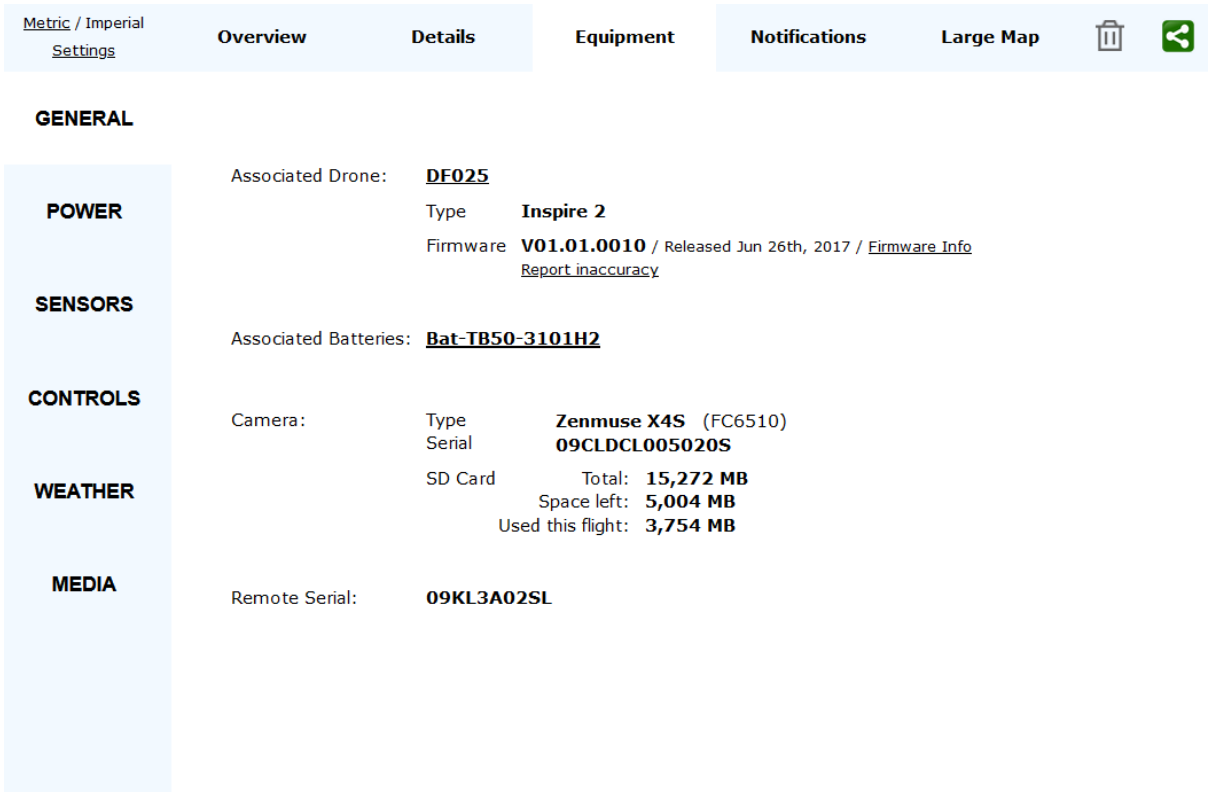


FIGURE 20 – ANDROID DRONE DETAILS

Analysing the second TXT flight log available, [DJIFlightRecord_2017-08-29_[13-23-50].txt] provides us with some sort of anomaly. This log has only recorded 9 seconds of flight data which seems to be a blip that was recorded at the very end of the first flight (Figure 21 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-23-50].txt). This flight takes place at 1:23:50PM and the first flight starts at 1:18:04PM which is a difference of 5 minutes and 46 seconds. The first flight only recorded a total of 5 minutes and 10 seconds meaning that this blip was taken approximately 36 seconds after completing its first flight. It is likely the drone was activated soon after landing.

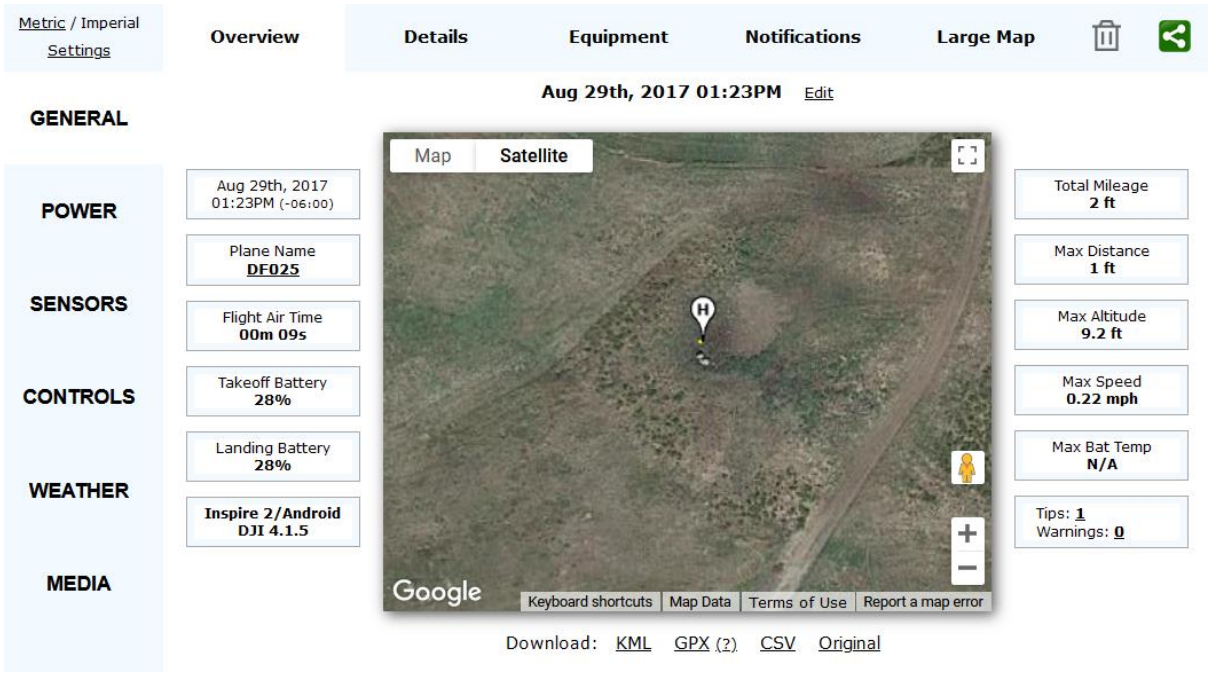


FIGURE 21 – AIRDATA OVERVIEW OF DJIFLIGHTRECORD_2017-08-29_[13-23-50].TXT

5.2.3 DAT Formatted Flight Data Analysis

Unfortunately dealing with the DAT format is not as easy. DatCon is currently used by the vast majority of people to decrypt their DAT flight logs, other options do exist such as DROP - DROne Parser (Devon Clark, 2022). However, this was essentially made using the same method as DatCon. DJI do offer software for decryption (DJI, 2022) but it requires a password which is unlikely to be available and there is no information on how exactly it works.

DatCon is quite a simple program to use, the encrypted DAT file is selected as input and a comprehensive CSV file containing all flight data is created. There are many settings that can be tweaked before decryption, these can create additional log files that may be of use. The other settings including time axis should usually be left untouched. The interface is shown in Figure 22 – DatCon Interface.

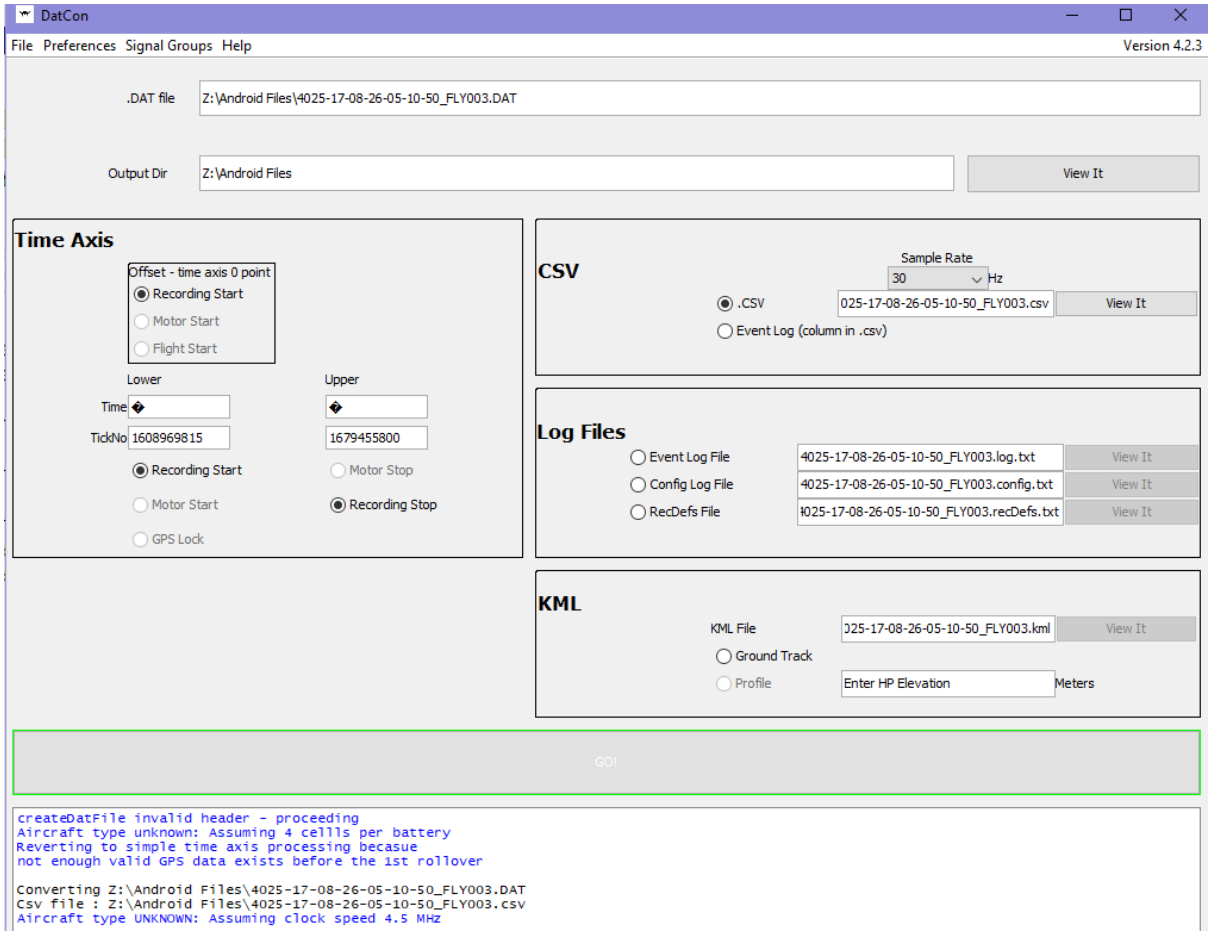


FIGURE 22 – DATCON INTERFACE

Once a readable CSV has been produced it can be analyzed using CsvView or within a geographic information system such as QGIS. QGIS allows for custom map sources and options to visualize the flight data. Initially a map source should be added as a new XYZ Tiles connection (Figure 23 – Adding New XYZ Connection), Google offer various maps that can be accessed using the URLs in Table 4 – Google Maps URLS. As longitude and latitude is used the coordinate reference system must be changed to WGS 84 for accurate results (Figure 24 – Changing Coordinate System to WGS 84)

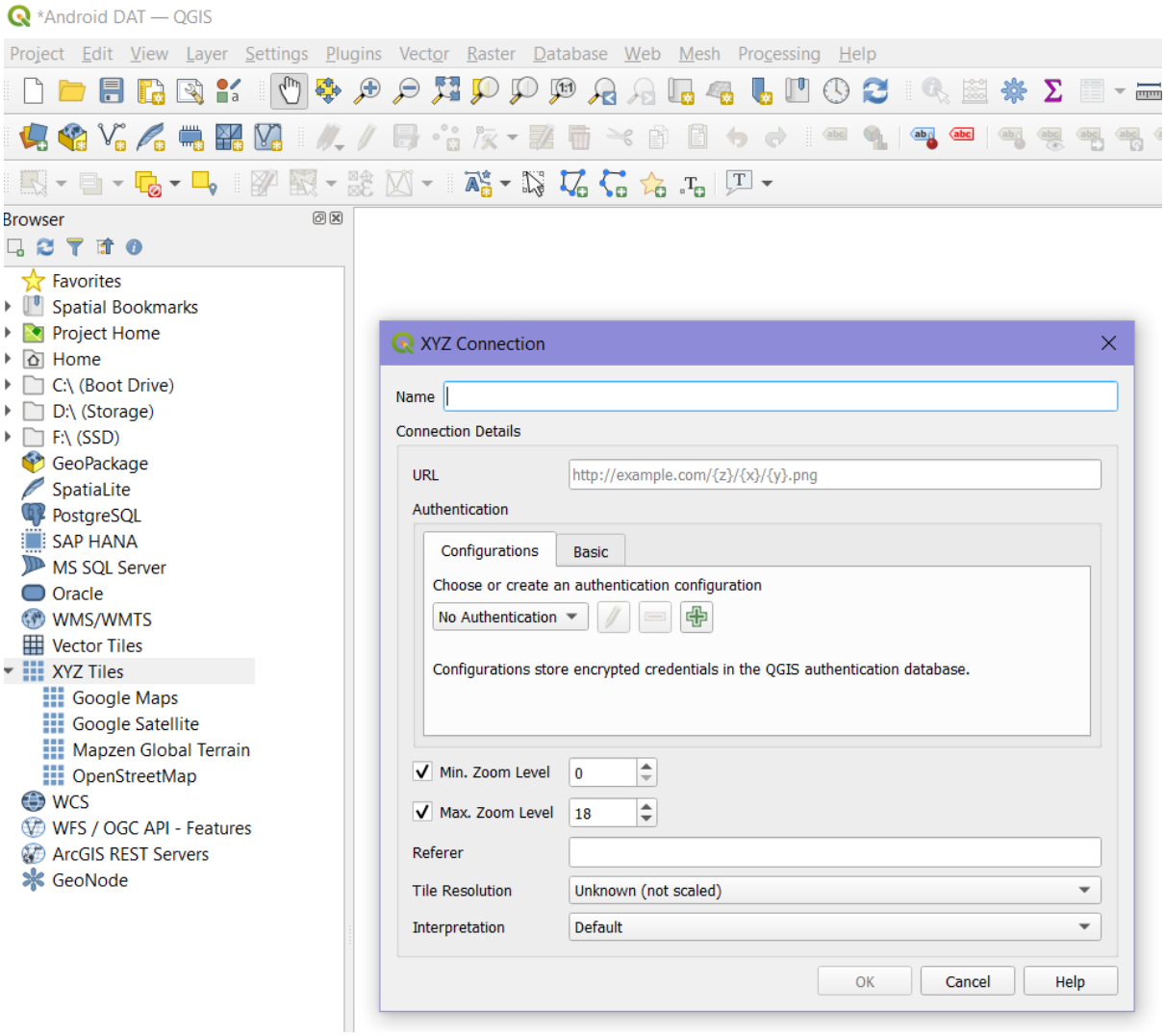


FIGURE 23 – ADDING NEW XYZ CONNECTION

Map Source	URL
Google Maps	https://mt1.google.com/vt/lyrs=r&x={x}&y={y}&z={z}
Google Satellite	https://www.google.cn/maps/vt?lyrs=s@189&gl=cn&x={x}&y={y}&z={z}
Google Satellite Hybrid	https://mt1.google.com/vt/lyrs=y&x={x}&y={y}&z={z}
Google Terrain	https://mt1.google.com/vt/lyrs=t&x={x}&y={y}&z={z}
Google Roads	https://mt1.google.com/vt/lyrs=h&x={x}&y={y}&z={z}

TABLE 4 – GOOGLE MAPS URLS

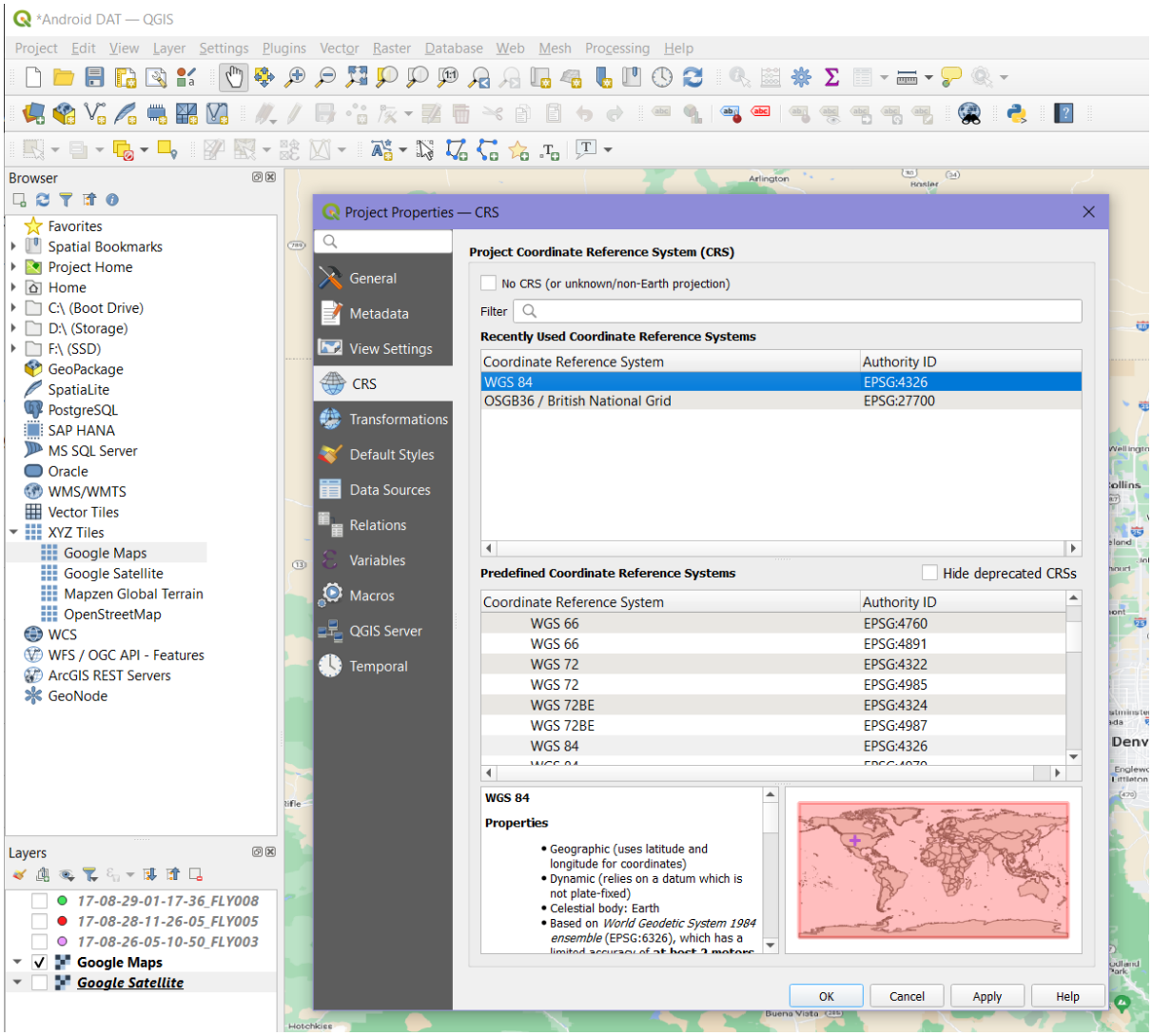


FIGURE 24 – CHANGING COORDINATE SYSTEM TO WGS 84

The CSV files created by DatCon can be added as a new delimited text layer where the point coordinates, X and Y field, are set to GPS:Long (longitude) and GPS:Lat (Latitude). The settings used for this case are shown in Figure 25 – Creation of Text Delimited Layer. Once imported various points indicate locations visited by the drone. As seen in Figure 26 – Unrealistic Android DAT Data, a common issue that occurs with many DAT flight logs is that they contain unrealistic or missing data. The red points are spread all across Canada indicating a flight that is physically impossible for this drone. Many of these DAT files will need to be marked as containing invalid data, this decision will ultimately be based on your interpretation of its contents. A Python program to help distinguish between valid and invalid data is provided in 5.5 DAT Identifier Python Program.

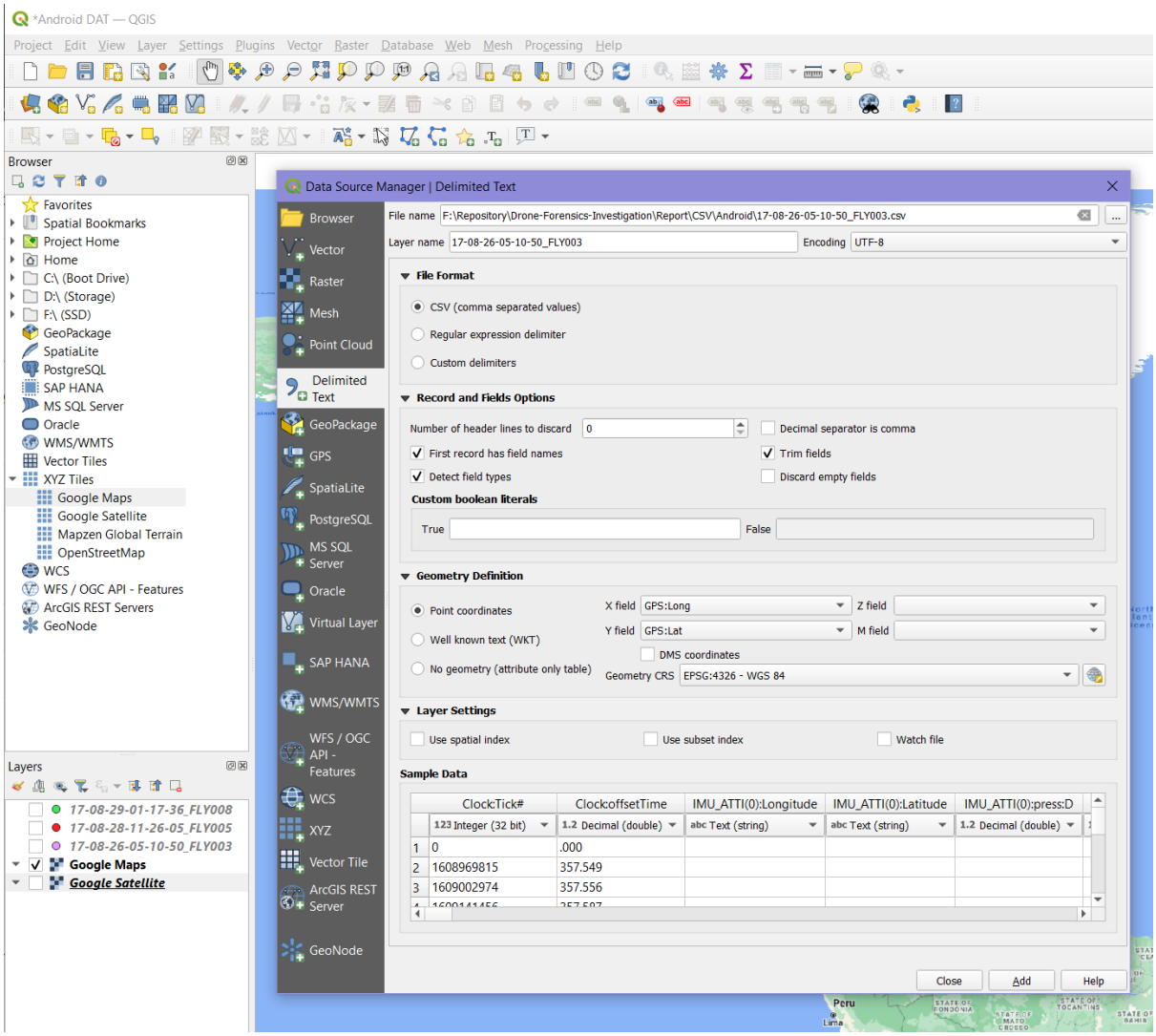


FIGURE 25 – CREATION OF TEXT DELIMITED LAYER

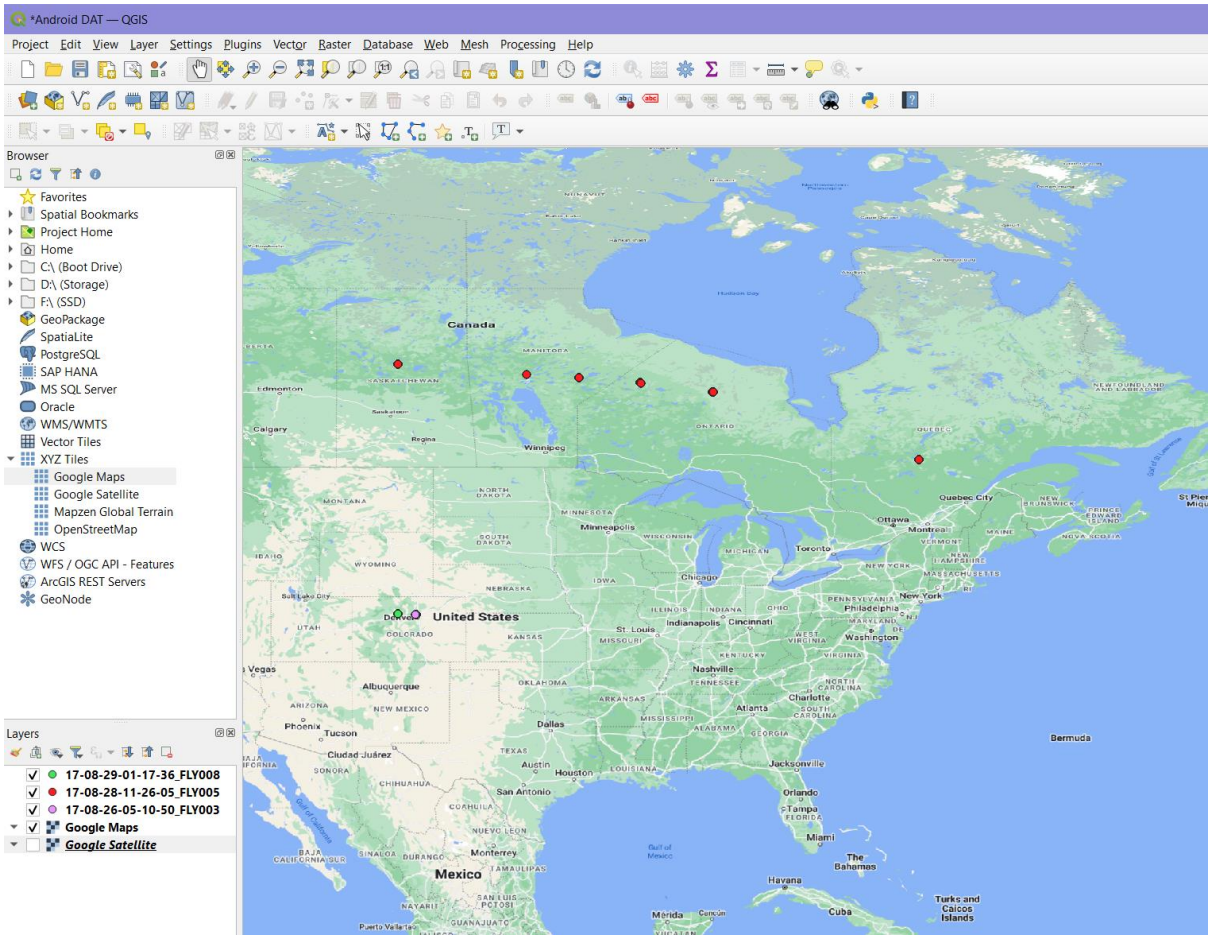


FIGURE 26 – UNREALISTIC ANDROID DAT DATA

As [17-08-28-11-26-05_FLY005.DAT] can be ignored we are left with the two remaining flight logs. Inspecting [17-08-29-01-17-36_FLY008.DAT] (Figure 27 – Flight Data Contained in 17-08-29-01-17-36_FLY008.DAT) with satellite imagery as a map source shows that it resembles the flight taken in the TXT flight log [DJIFlightRecord_2017-08-29_[13-18-04].txt](Figure 18 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-18-04].txt), leading to the conclusion that both a TXT and DAT log are made for each flight. However, [17-08-26-05-10-50_FLY003.DAT] does not match any other records and only contains three points located in Interlocken, Broomfield, Colorado (Figure 28 – Flight Data Contained in 17-08-26-05-10-50_FLY003.DAT). VTO Inc has a headquarters located at 325 Interlocken Parkway, Building C, Broomfield, CO 80021, USA which is the location these points are found. Based on this we can assume these logs were not created during a flight but rather some sort of testing stage. This is important information as we know the DAT logs may still be created even if the drone is not being flown.

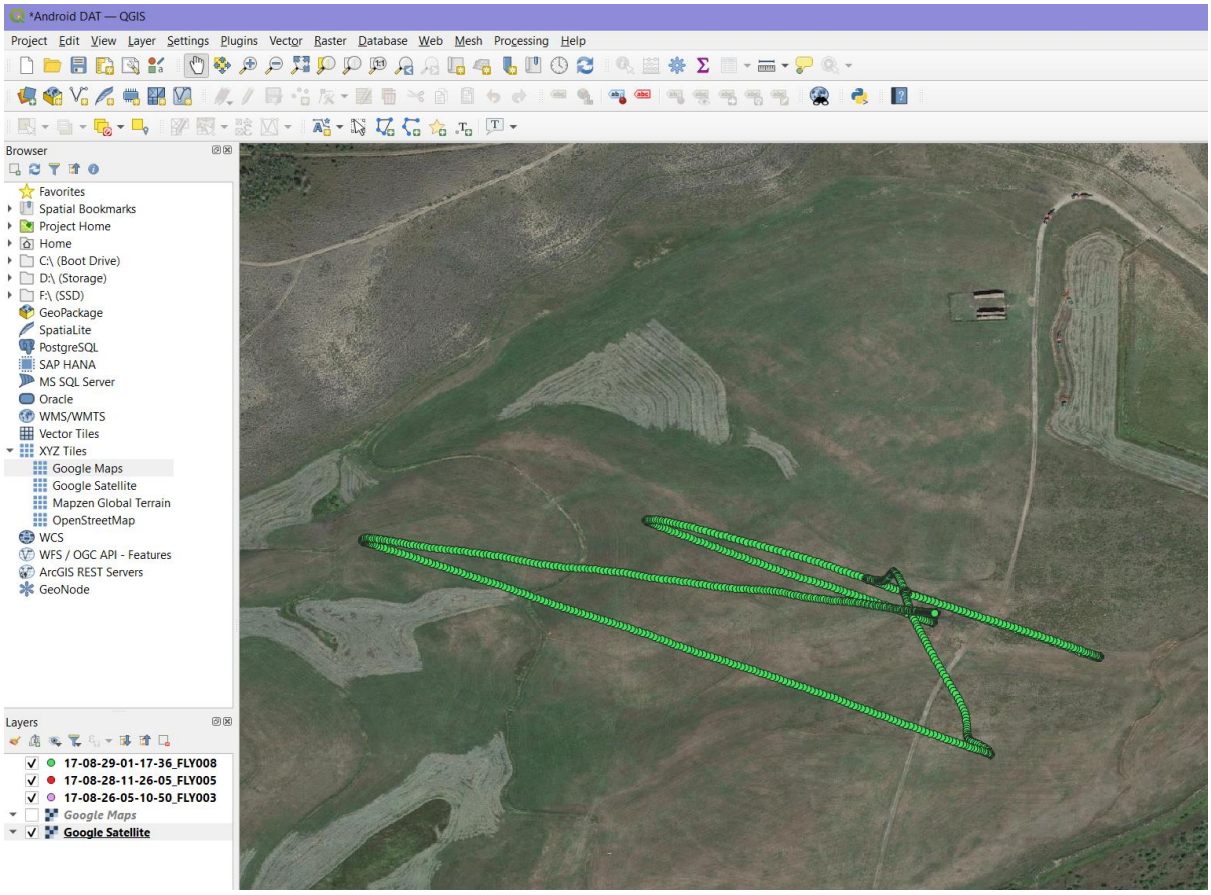


FIGURE 27 – FLIGHT DATA CONTAINED IN 17-08-29-01-17-36_FLY008.DAT

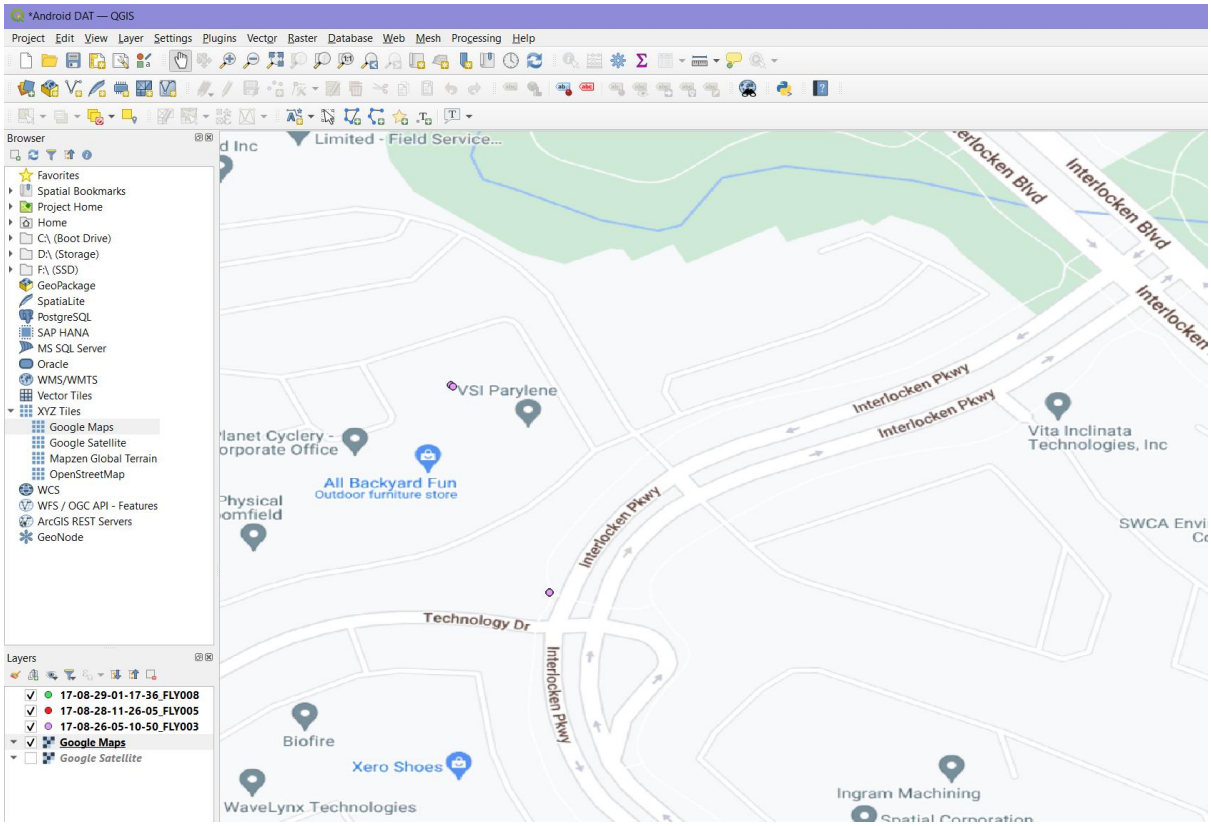


FIGURE 28 – FLIGHT DATA CONTAINED IN 17-08-26-05-10-50_FLY003.DAT

QGIS is very useful for analysing flight paths as we can change the colour of our symbol based on other factors (Figure 29 – Example of Changing Symbology). Any chosen value can be automatically classified to create a visual representation alongside the path taken by the drone. Classification based on time is shown in Figure 30 – Classification using Time, where the white symbol represents the start and red being the end. Classification based on height is also very useful, one available option for height is provided in MSL (Mean Sea Level). In Figure 31 – Classification using MSL Height, white represents lower recorded height whereas red is larger height values.

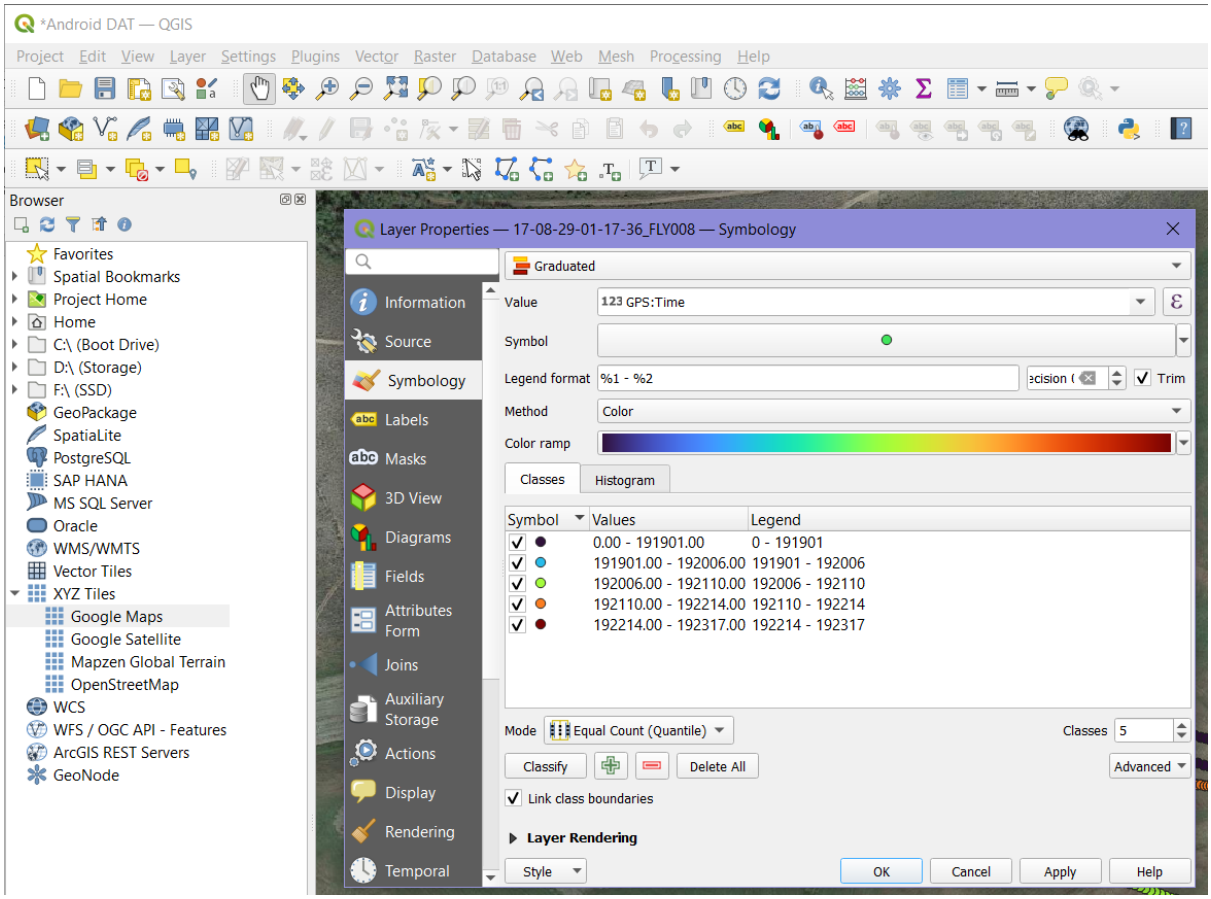


FIGURE 29 – EXAMPLE OF CHANGING SYMBOLOGY

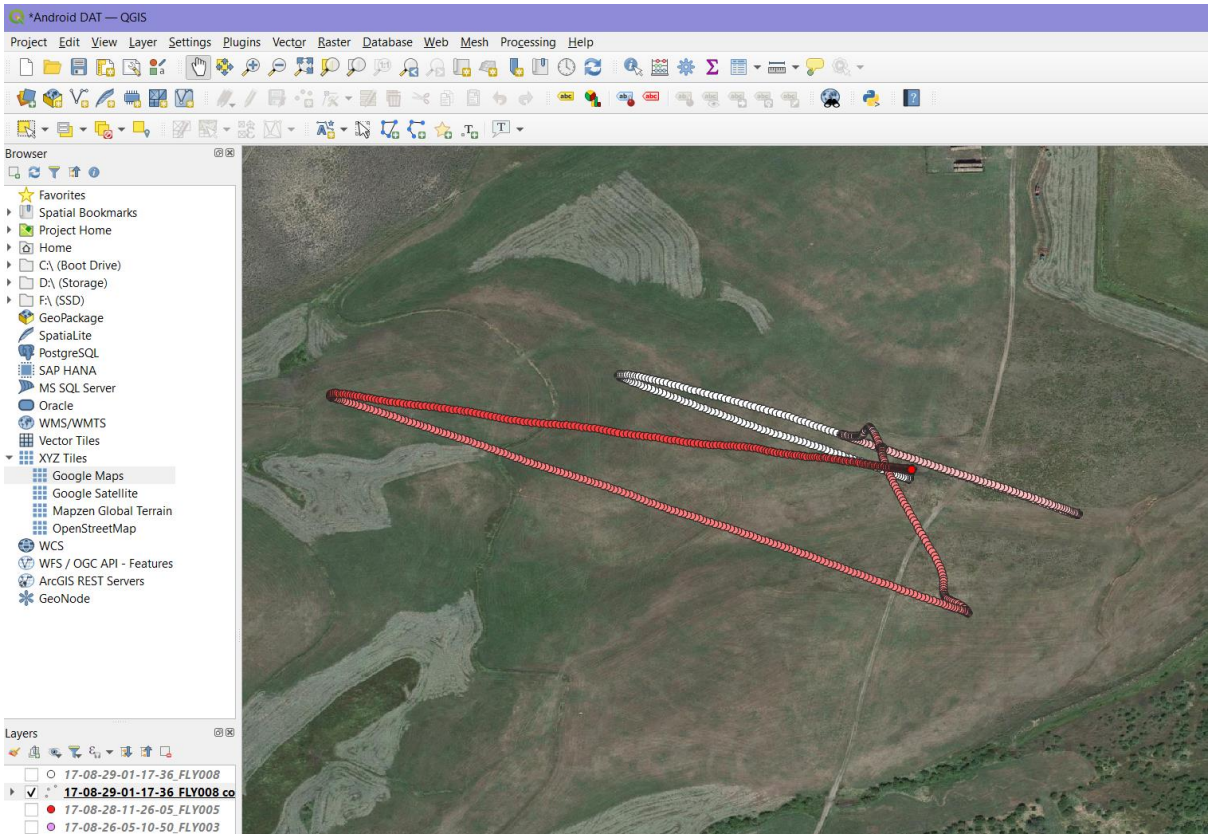


FIGURE 30 – CLASSIFICATION USING TIME

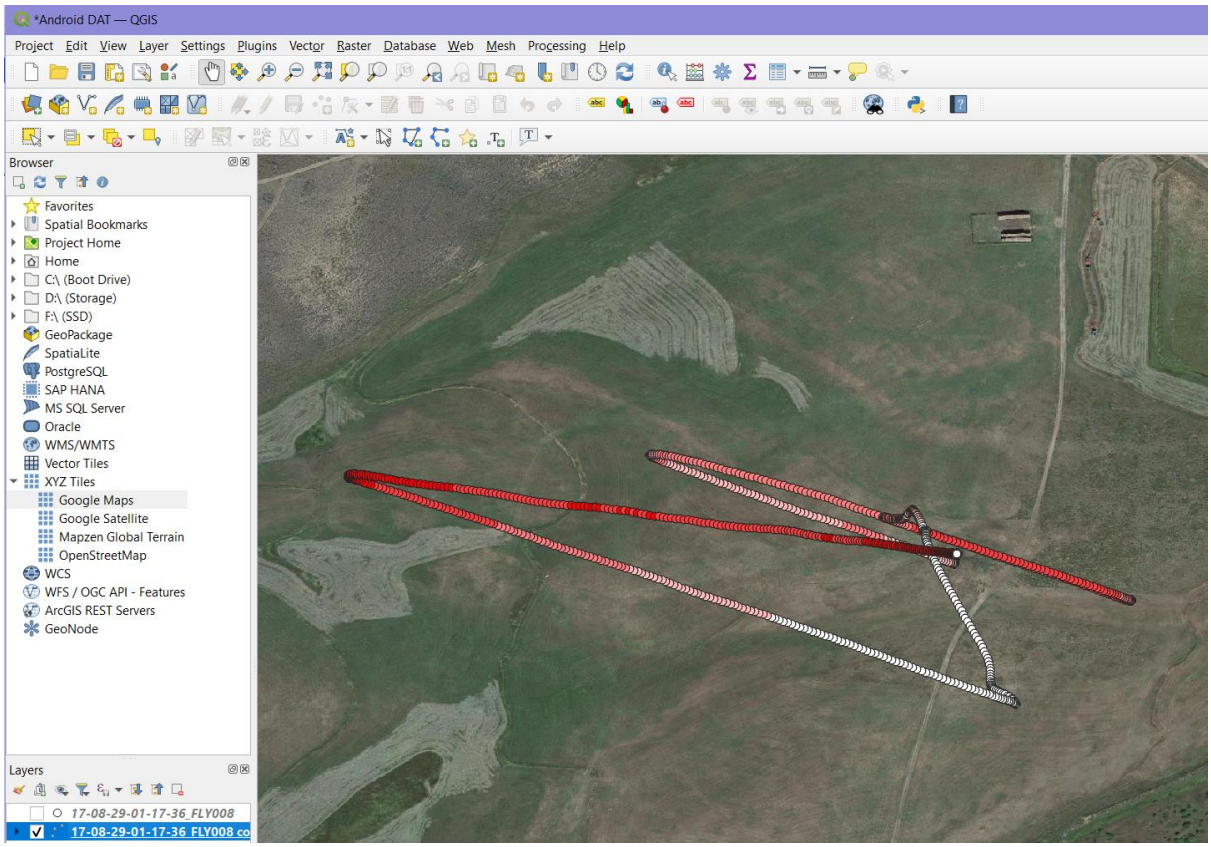


FIGURE 31 – CLASSIFICATION USING MSL HEIGHT

5.2.4 Component Logs Analysis

Excluding the flight logs previously visited, the DJI Inspire 2 creates other useful logs and files that can help reconstruct the events that took place. Other onboard components record data that can be found located in the directory `[media/0/DJI/dji.go.v4/LOG/ERROR_POP_LOG/]`. One file was present here labelled `[29-08-2017-095XDCK002002W]`, this name is important as it contains the date the components were used, and a serial number related to the drone. The contents contain information regarding motors, landing gear and wireless interference (Figure 32 – Contents of 29-08-2017-095XDCK002002W). The time stamps and details found match up with the events that took place in the flight found in Figure 18 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-18-04].txt.

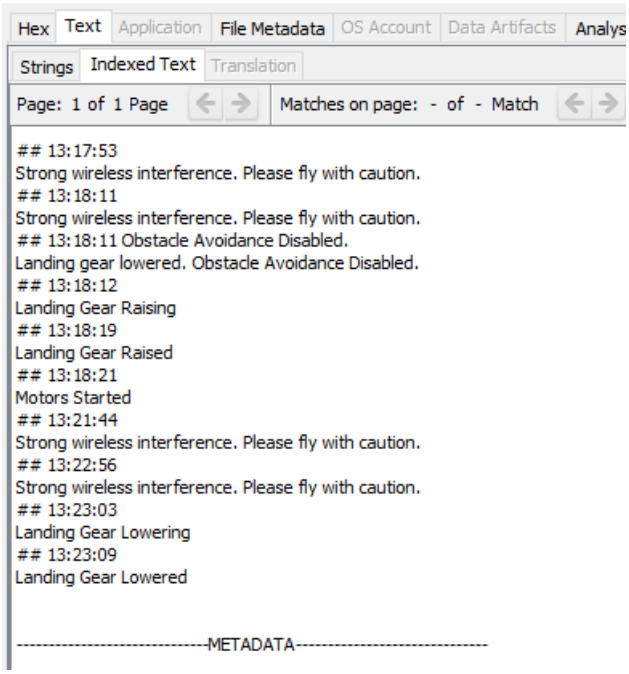


FIGURE 32 – CONTENTS OF 29-08-2017-095XDCK002002W

Advanced drones that have GPS capabilities will usually have a return to home feature that will take over the drone incase the signal is lost via the controller. In this instance we can find this information looking in the directory `[media/0/DJI/dji.go.v4/LOG/MAP/]`, many of the files here contain data that is irrelevant however, if a home point is added it is likely to be stored in one of these logs. In this case `[log-2017-08-29.txt]` provides the latitude and longitude values of the home marker, these coordinates can be found in Figure 33 – Contents of log-2017-08-29.txt

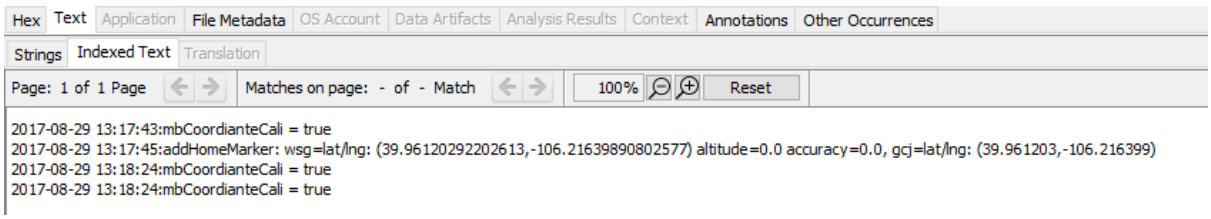


FIGURE 33 – CONTENTS OF LOG-2017-08-29.TXT

The first coordinates specified will be used as they are to a higher degree of accuracy than the second coordinates. Creating a point in QGIS will specify where exactly the home point was set in relation to its flights. In Figure 34 – log-2017-08-29.txt Home Marker, the green icon represents the coordinates found. using this and the classified flight paths we can estimate where the flight started and ended.

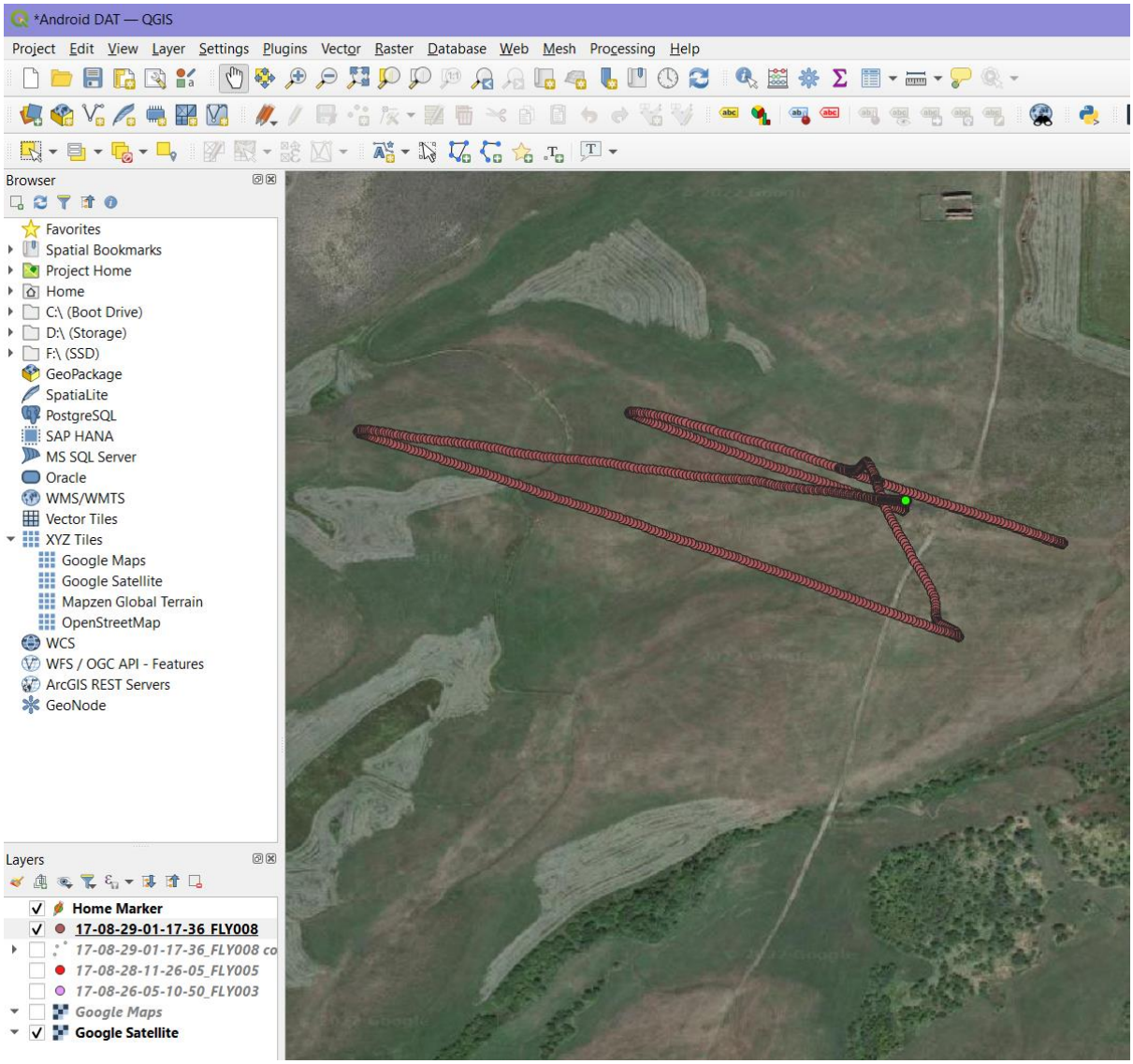


FIGURE 34 – LOG-2017-08-29.TXT HOME MARKER

5.2.4 MD5 Hash Values of Android Flight Data Files

File	MD5
DJIFlightRecord_2017-08-29_[13-18-04].txt	10519434971b57d4fae8fd7b63716d40
DJIFlightRecord_2017-08-29_[13-23-50].txt	f6a40f2ef1bc37dbc551cf61c3885979
17-08-26-05-10-50_FLY003.DAT	61834a204604d03b240ea7c34185f9ce
17-08-28-11-26-05_FLY005.DAT	184a04c54afe3a6d630c7eae708de2c2
17-08-29-01-17-36_FLY008.DAT	0660b1c6d2e15e0ee0f9a910d531a3e8
29-08-2017-095XDCK002002W	389cd6ed0763fd01364eb8552a6e2d48
log-2017-08-29.txt	a7aad79ed47d1a47b921d969fbac46c2

HASHES 4

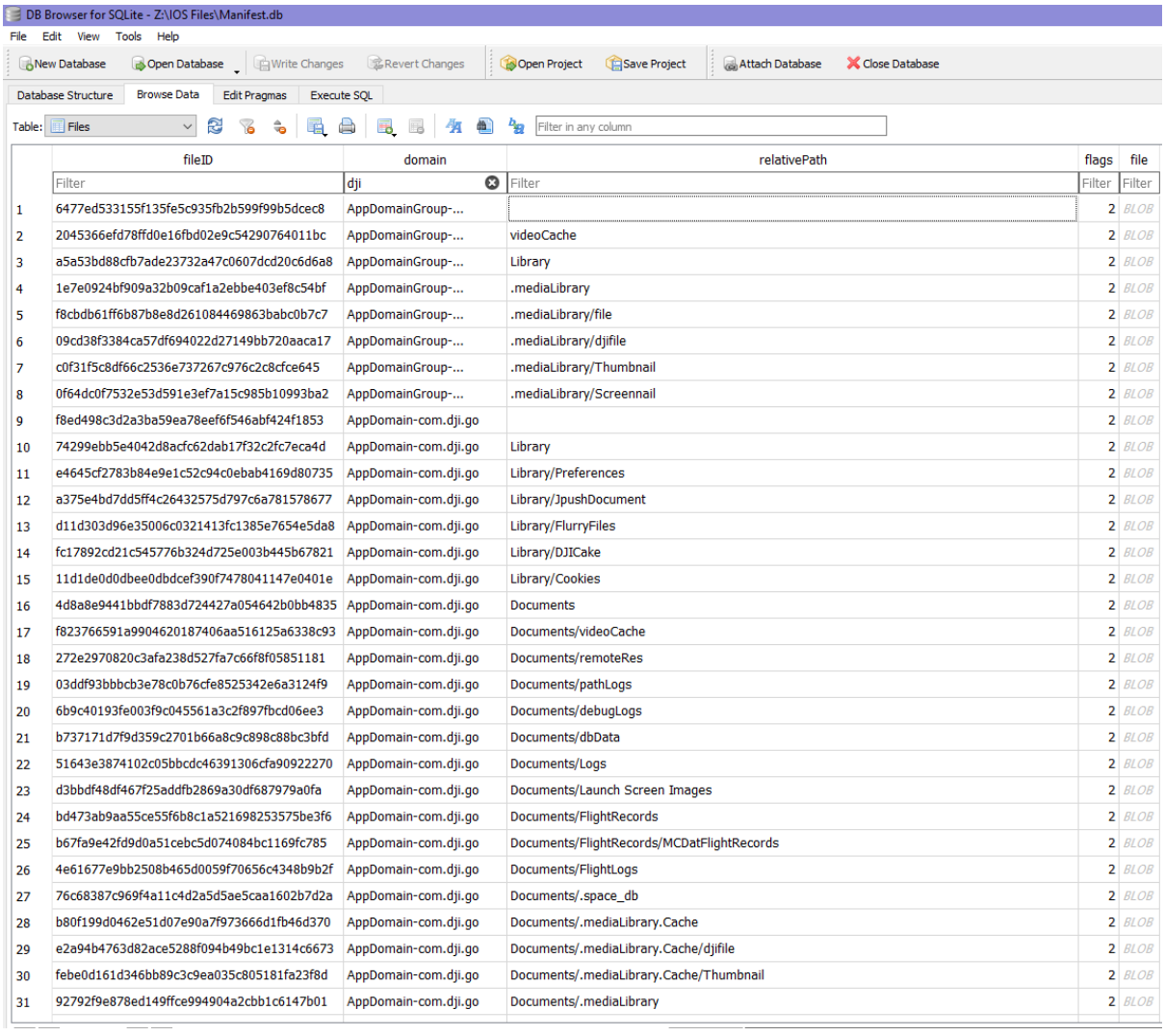
5.3 IOS FLIGHT DATA ANALYSIS

5.3.1 IOS DJI APPLICATION ANALYSIS

To find the flight records in an IOS backup file the installed application used for the flights must be known. Fortunately for us all apps installed on the device, excluding pre-installed, should be present in the file `[Info.plist]`. Figure 35 – Applications Installed on IOS Device shows only DJI GO was installed, which must be what was used to control the drone.

FIGURE 35 – APPLICATIONS INSTALLED ON IOS DEVICE

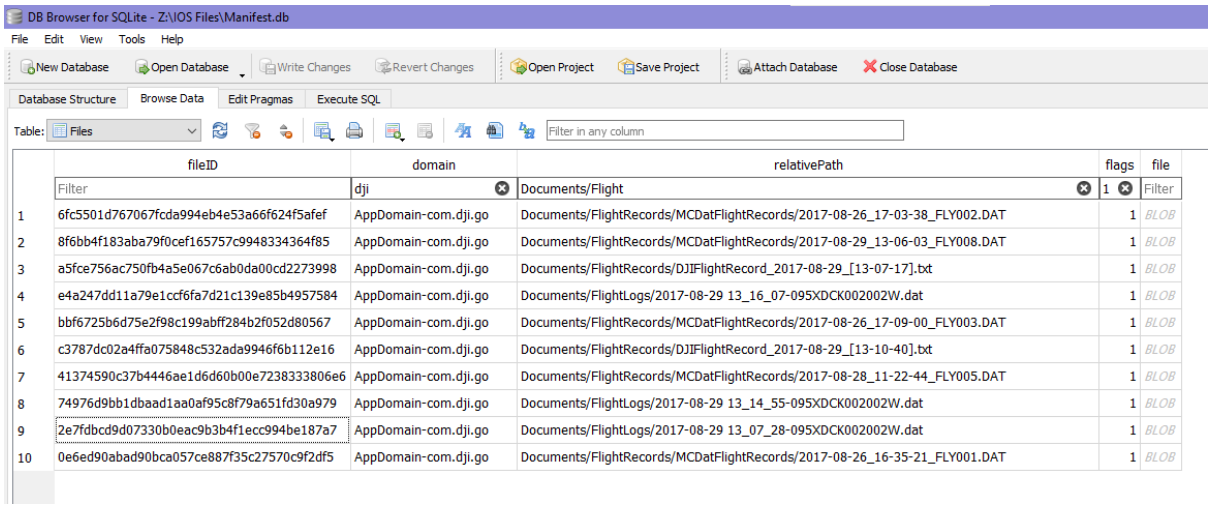
Knowing this we can search for DJI related files and directories in `[Manifest.db]`, which is the database that holds all information regarding where each file and directory is present in the IOS backup structure. Refer back to 4.2.2 IOS File Structure for more information. As shown in Figure 36 – Sample of Directories Found on IOS Device, there are many locations that may hold important artifacts, the same can be said about irrelevant information.



	fileID	domain	relativePath	flags	file
	Filter	dji	Filter	Filter	Filter
1	6477ed533155f135fe5c935fb2b599f99b5dcec8	AppDomainGroup-...		2	BLOB
2	2045366efd78ffd0e16fbd02e9c54290764011bc	AppDomainGroup-...	videoCache	2	BLOB
3	a5a53bd88cfb7ade23732a47c0607dcd20c6d6a8	AppDomainGroup-...	Library	2	BLOB
4	1e7e0924bf909a32b09caf1a2ebbe403ef8c54bf	AppDomainGroup-...	.mediaLibrary	2	BLOB
5	f8cbdb61ff6b87b8e8d261084469863babc0b7c7	AppDomainGroup-...	.mediaLibrary/file	2	BLOB
6	09cd38f3384ca57df694022d27149bb720aaca17	AppDomainGroup-...	.mediaLibrary/djifile	2	BLOB
7	c0f31f5c8df66c2536e737267c976c2c8cfce645	AppDomainGroup-...	.mediaLibrary/Thumbnail	2	BLOB
8	0f64dc0f7532e53d591e3ef7a15c985b10993ba2	AppDomainGroup-...	.mediaLibrary/Screennail	2	BLOB
9	f8ed498c3d2a3ba59ea78eef6f546abf424f1853	AppDomain-com.dji.go		2	BLOB
10	74299ebb5e4042d8acfc62dab17f32c2fc7eca4d	AppDomain-com.dji.go	Library	2	BLOB
11	e4645cf2783b84e9e1c52c94c0ebab4169d80735	AppDomain-com.dji.go	Library/Preferences	2	BLOB
12	a375e4bd7dd5ff4c26432575d797c6a781578677	AppDomain-com.dji.go	Library/JpushDocument	2	BLOB
13	d11d303d96e35006c0321413fc1385e7654e5da8	AppDomain-com.dji.go	Library/FlurryFiles	2	BLOB
14	fc17892cd21c545776b324d725e003b445b67821	AppDomain-com.dji.go	Library/DJICake	2	BLOB
15	11d1de0d0dbee0dbdcef390f7478041147e0401e	AppDomain-com.dji.go	Library/Cookies	2	BLOB
16	4d8a8e9441bbdf7883d724427a054642b0bb4835	AppDomain-com.dji.go	Documents	2	BLOB
17	f823766591a9904620187406aa516125a6338c93	AppDomain-com.dji.go	Documents/videoCache	2	BLOB
18	272e2970820c3afa238d527fa7c66f8f05851181	AppDomain-com.dji.go	Documents/remoteRes	2	BLOB
19	03ddf93bbbcb3e78c0b76cfe8525342e6a3124f9	AppDomain-com.dji.go	Documents/pathLogs	2	BLOB
20	6b9c40193fe003f9c045561a3c2f897fbcd06ee3	AppDomain-com.dji.go	Documents/debugLogs	2	BLOB
21	b737171d7f9d359c2701b66a8c9c898c88bc3bfd	AppDomain-com.dji.go	Documents/dbData	2	BLOB
22	51643e3874102c05bbcdc46391306cfa90922270	AppDomain-com.dji.go	Documents/Logs	2	BLOB
23	d3bbdf48df467f25addfb2869a30df687979a0fa	AppDomain-com.dji.go	Documents/Launch Screen Images	2	BLOB
24	bd473ab9aa55ce55f6b8c1a521698253575be3f6	AppDomain-com.dji.go	Documents/FlightRecords	2	BLOB
25	b67fa9e42fd9d0a51cebc5d074084bc1169fc785	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords	2	BLOB
26	4e61677e9bb2508b465d0059f70656c4348b9b2f	AppDomain-com.dji.go	Documents/FlightLogs	2	BLOB
27	76c68387c969f4a11c4d2a5d5ae5caa1602b7d2a	AppDomain-com.dji.go	Documents/.space_db	2	BLOB
28	b80f199d0462e51d07e90a7f973666d1fb46d370	AppDomain-com.dji.go	Documents/.mediaLibrary.Cache	2	BLOB
29	e2a94b4763d82ace5288f094b49bc1e1314c6673	AppDomain-com.dji.go	Documents/.mediaLibrary.Cache/djifile	2	BLOB
30	febe0d161d346bb89c3c9ea035c805181fa23f8d	AppDomain-com.dji.go	Documents/.mediaLibrary.Cache/Thumbnail	2	BLOB
31	92792f9e878ed149ffce994904a2cbb1c6147b01	AppDomain-com.dji.go	Documents/.mediaLibrary	2	BLOB

FIGURE 36 – SAMPLE OF DIRECTORIES FOUND ON IOS DEVICE

Three particular directories hold the flight logs we are looking for, `[Documents/FlightRecords]` and `[Documents/FlightRecords/MCDatFlightRecords]` are labelled and structured in the same way as the Android device. However, a third directory is present that seems to hold DAT flight logs that does not appear similar to those logs found on the Android or internal SD card, the directory is labelled `[Documents/FlightLogs]`. All suspected flight logs found in these directories are shown in Figure 37 – All IOS Flight Logs. To analyze these logs, they need to be extracted and their original names which are set to hash values labelled file ID, must be renamed to what is shown in the relative path. The end result should look similar to Figure 38 – Extracted and Renamed IOS Flight Logs.



	fileID	domain	relativePath	flags	file
	Filter	dji	Documents/Flight	1	Filter
1	6fc5501d767067fcda994eb4e53a66f624f5afef	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords/2017-08-26_17-03-38_FLY002.DAT	1	BLOB
2	8f6bb4f183aba79f0cef165757c9948334364f85	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords/2017-08-29_13-06-03_FLY008.DAT	1	BLOB
3	a5fce756ac750fb4a5e067c6ab0da00cd2273998	AppDomain-com.dji.go	Documents/FlightRecords/DJIFlightRecord_2017-08-29_[13-07-17].txt	1	BLOB
4	e4a247dd11a79e1ccf6fa7d21c139e85b4957584	AppDomain-com.dji.go	Documents/FlightLogs/2017-08-29 13_16_07-095XDCK002002W.dat	1	BLOB
5	bbf6725b6d75e2f98c199abff284b2f052d80567	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords/2017-08-26_17-09-00_FLY003.DAT	1	BLOB
6	c3787dc02a4ffa075848c532ada9946f6b112e16	AppDomain-com.dji.go	Documents/FlightRecords/DJIFlightRecord_2017-08-29_[13-10-40].txt	1	BLOB
7	41374590c37b4446ae1d6d60b00e7238333806e6	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords/2017-08-28_11-22-44_FLY005.DAT	1	BLOB
8	74976d9bb1dbaad1aa0af95c8f79a651fd30a979	AppDomain-com.dji.go	Documents/FlightLogs/2017-08-29 13_14_55-095XDCK002002W.dat	1	BLOB
9	2e7fdbcd9d07330b0eac9b3b4f1ecc994be187a7	AppDomain-com.dji.go	Documents/FlightLogs/2017-08-29 13_07_28-095XDCK002002W.dat	1	BLOB
10	0e6ed90abad90bca057ce887f35c27570c9f2df5	AppDomain-com.dji.go	Documents/FlightRecords/MCDatFlightRecords/2017-08-26_16-35-21_FLY001.DAT	1	BLOB

FIGURE 37 – ALL IOS FLIGHT LOGS

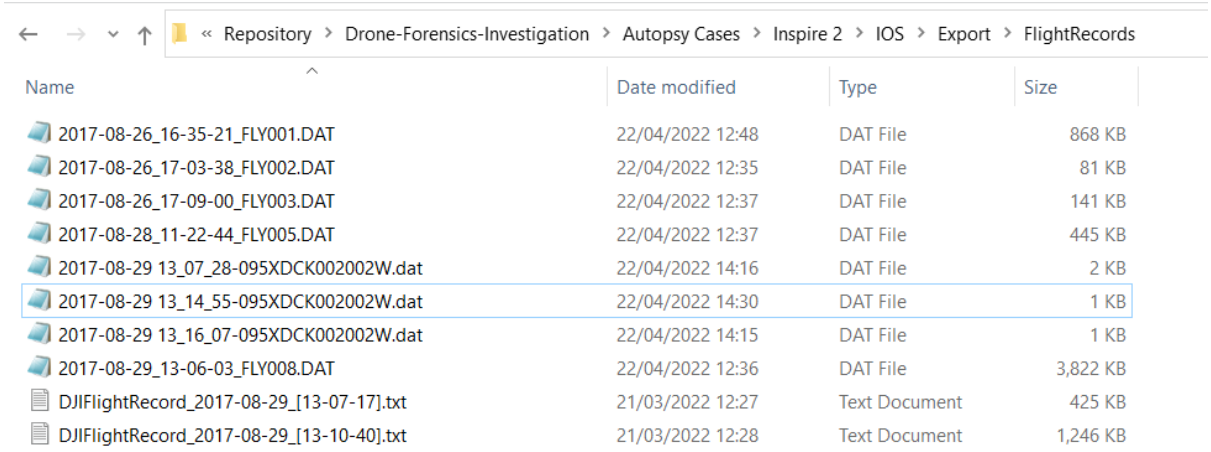


FIGURE 38 – EXTRACTED AND RENAMED IOS FLIGHT LOGS

5.3.2 TXT Formatted Flight Data Analysis

As done previously for the Android device, the two TXT logs will be analyzed first using AIRDATA for its overview and comprehensive details. Both IOS flight logs `[DJIFlightRecord_2017-08-29_[13-07-17].txt]` and `[DJIFlightRecord_2017-08-29_[13-10-40].txt]` were created before the flights logs made via Android by approximately 8 and 11 minutes.

The first flight `[DJIFlightRecord_2017-08-29_[13-07-17].txt]` occurred at 1:07:17PM on the 29th of August 2017. The path taken has been mapped onto a satellite image as shown in Figure 39 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-07-17].txt. We are also provided with an additional thumbnail taken via the onboard camera which can be used to match the flight path to video taken. In Figure 40 – Time and Location of DJIFlightRecord_2017-08-29_[13-07-17].txt we can see that this flight log has recorded 2 minutes and 52 seconds of data and the location the drone was flown is the same airspace as seen in the Androids logs, Arapaho and Roosevelt National Forests, Denver, Colorado (Figure 19 – Time and Location of DJIFlightRecord_2017-08-29_[13-18-04].txt).

The device details given in Figure 41 – IOS Drone Details include the associated drone and various serial numbers. These details match the ones shown in Figure 20 – Android Drone Details confirming the exact same drone was flown via IOS then Android.

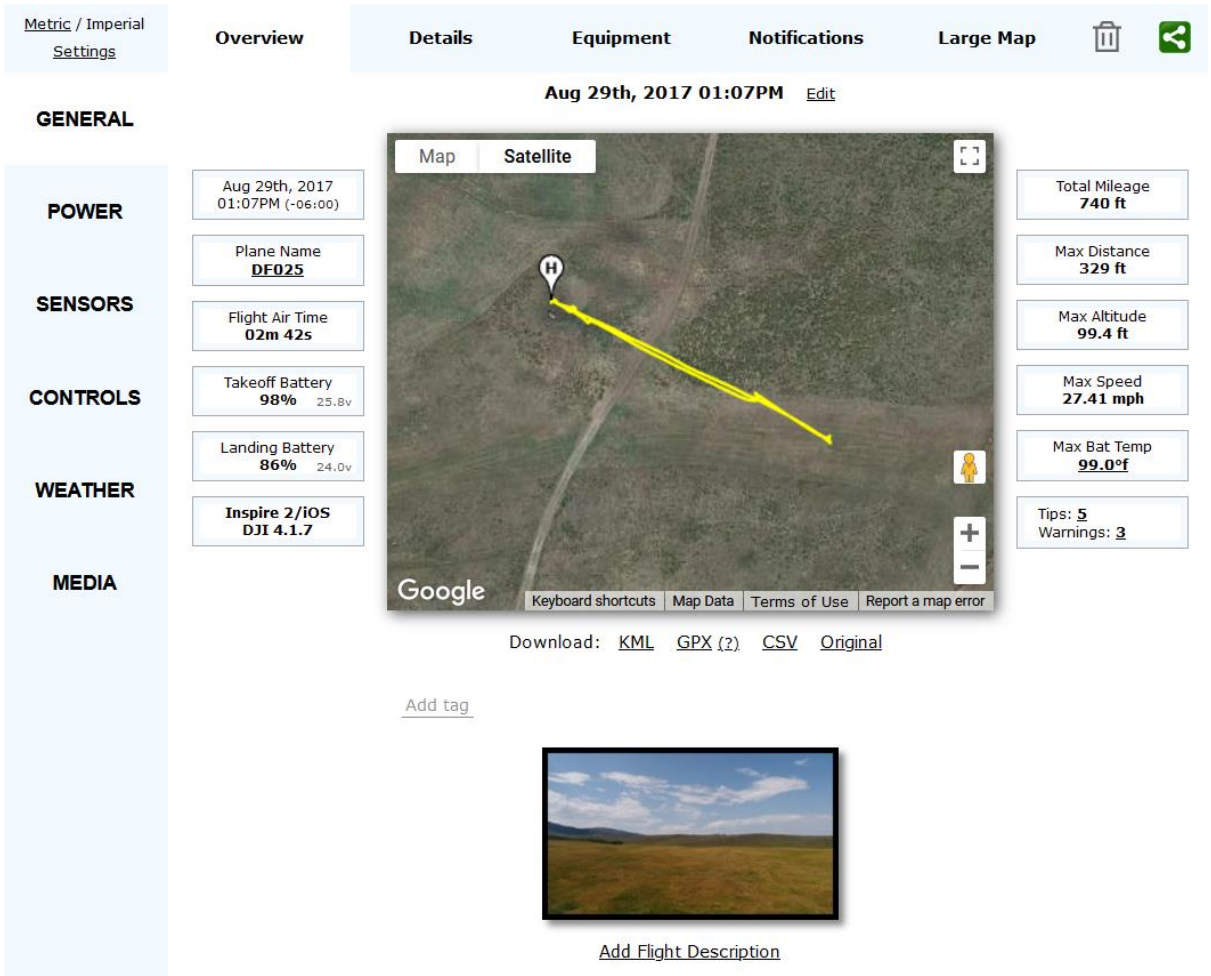


FIGURE 39 – AIRDATA OVERVIEW OF DJIFLIGHTRECORD_2017-08-29_[13-07-17].TXT

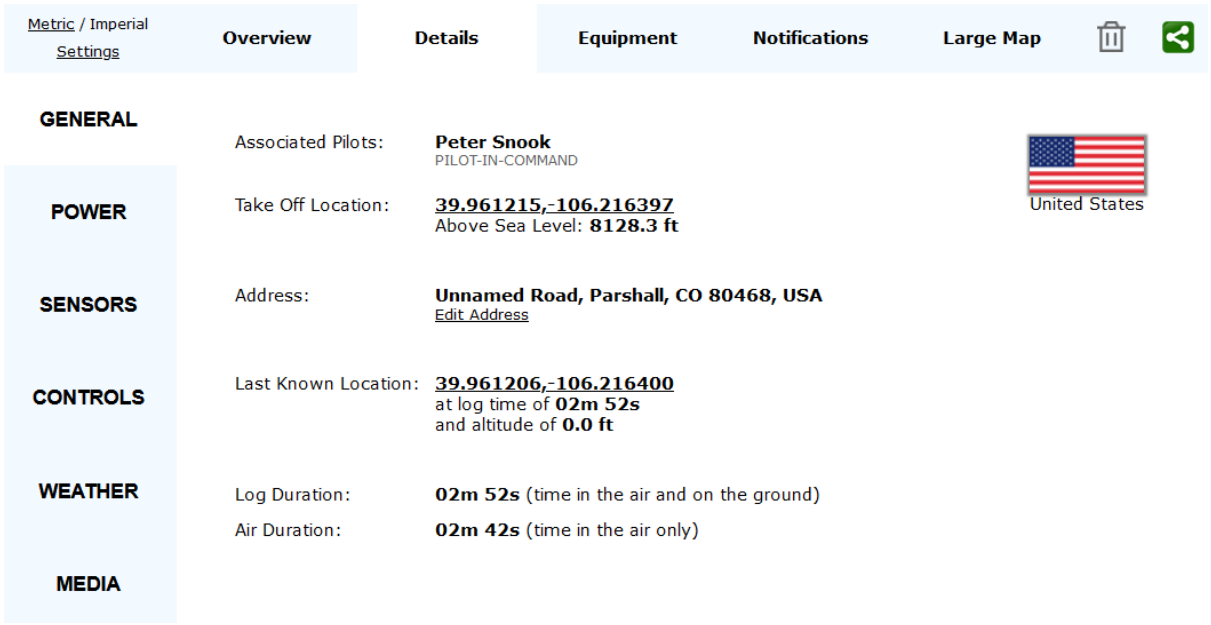


FIGURE 40 – TIME AND LOCATION OF DJIFLIGHTRECORD_2017-08-29_[13-07-17].TXT

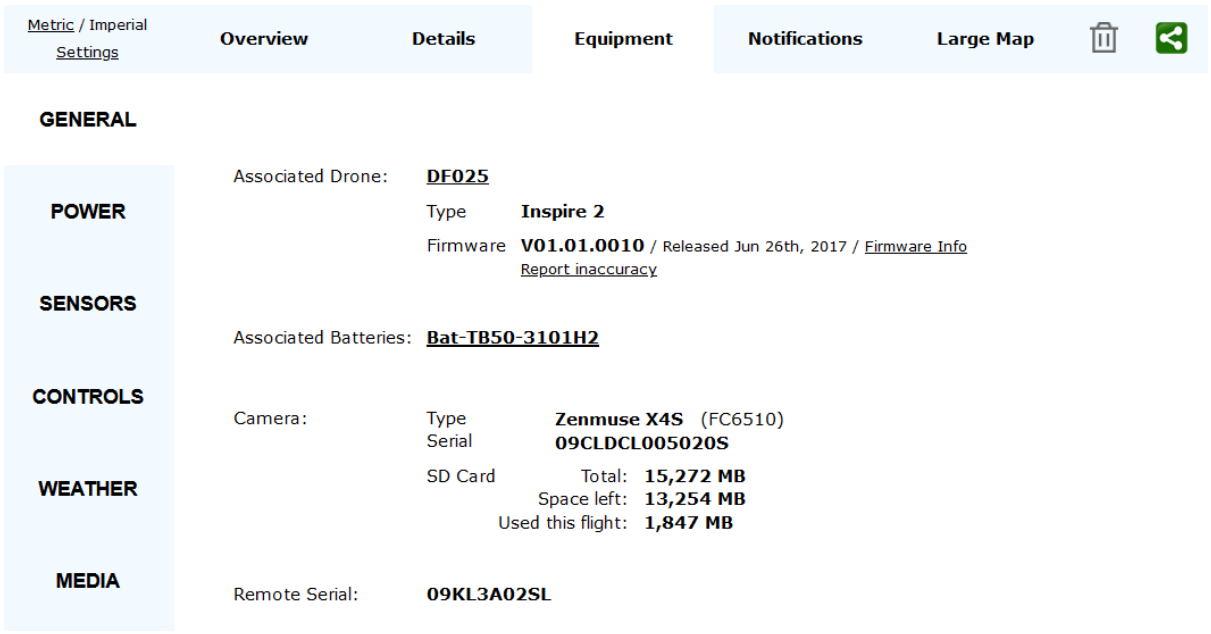


FIGURE 41 – IOS DRONE DETAILS

The second flight `[DJIFlightRecord_2017-08-29_[13-10-40].txt]` took place 3 minutes and 23 seconds after the first at 1:10:40PM. A much larger distance was covered here, approximately five times the previous when comparing the max distances (Figure 42 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-10-40].txt and Figure 39 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-07-17].txt). The time recorded during the log lasted 6 minutes and 9 seconds according to Figure 43 – Time and Location of DJIFlightRecord_2017-08-29_[13-10-40].txt. The location flown is the same airspace as all previous flights found as all coordinates and locations specified point to the same piece of land in Arapaho and Roosevelt National Forests, Denver, Colorado.

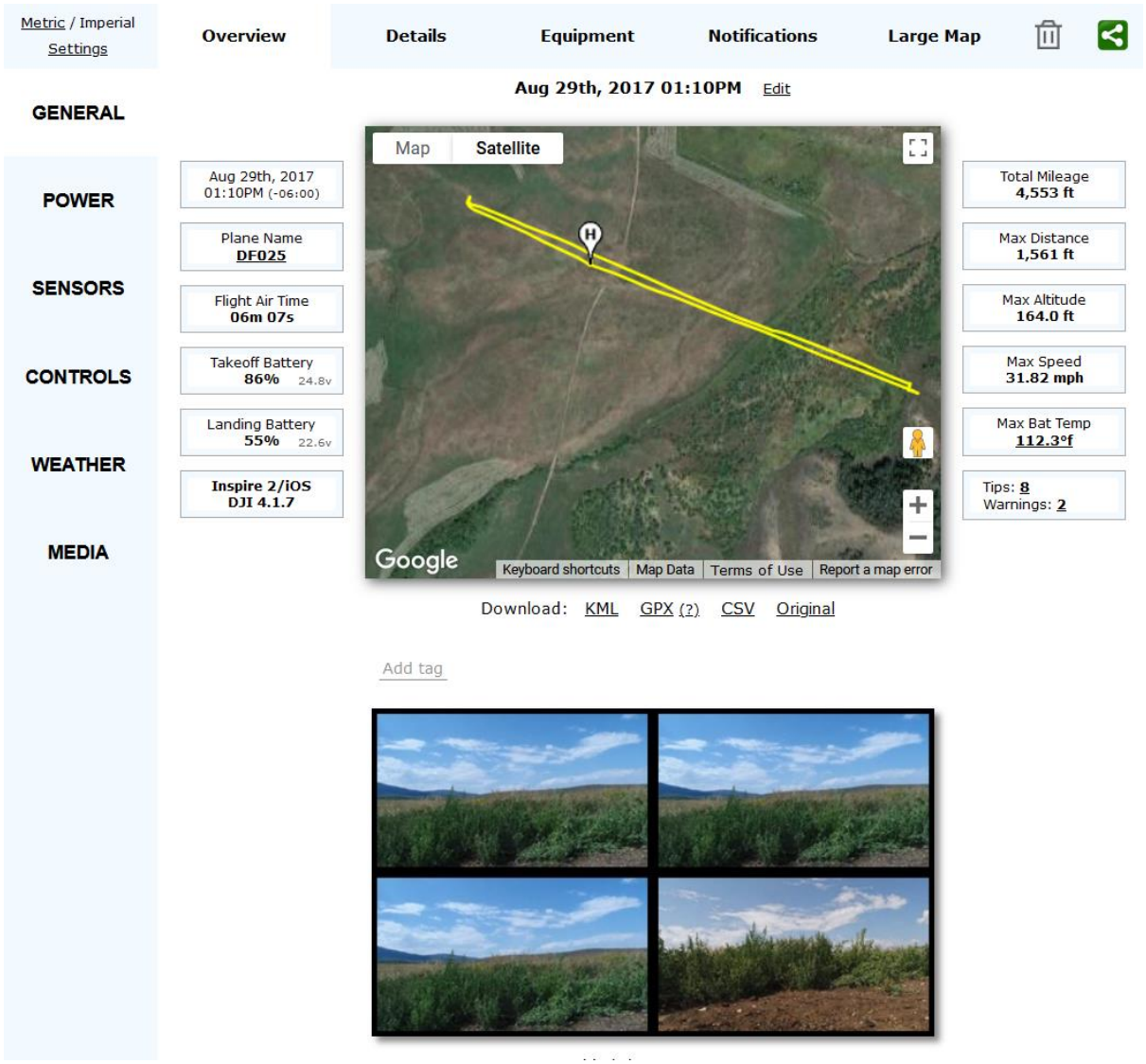


FIGURE 42 – AIRDATA OVERVIEW OF DJIFLIGHTRECORD_2017-08-29_[13-10-40].TXT

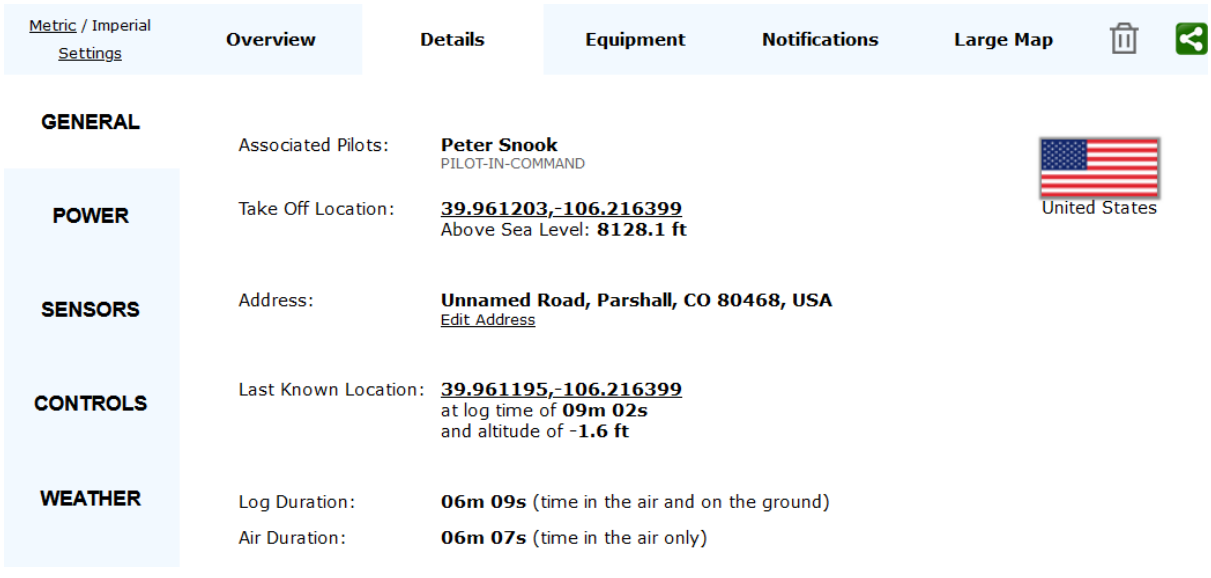


FIGURE 43 – TIME AND LOCATION OF DJIFLIGHTRECORD_2017-08-29_[13-10-40].TXT

5.3.3 DAT Formatted Flight Data Analysis

The conclusion made in the Android section led us to believe that a DAT and TXT log are made for each flight taken. There are a total of five DAT logs, and two TXT logs present in the IOS backup files. If the assumption made is correct, three of these DAT logs will contain unreliable data.

First DatCon will be used to convert all DAT logs into readable CSV files that can be used within QGIS for analysis. In this case the log `[2017-08-29_13-06-03_FLY008.DAT]` seems to only match the path taken in `[DJIFlightRecord_2017-08-29_[13-10-40].txt]`. However, upon closer inspection both TXT flight logs look to be present in the same DAT flight log. We can see the large path taken by the first flight in Figure 44 – Far View of 2017-08-29_13-06-03_FLY008.DAT, and the smaller path in Figure 45 – Close View of 2017-08-29_13-06-03_FLY008.DAT.

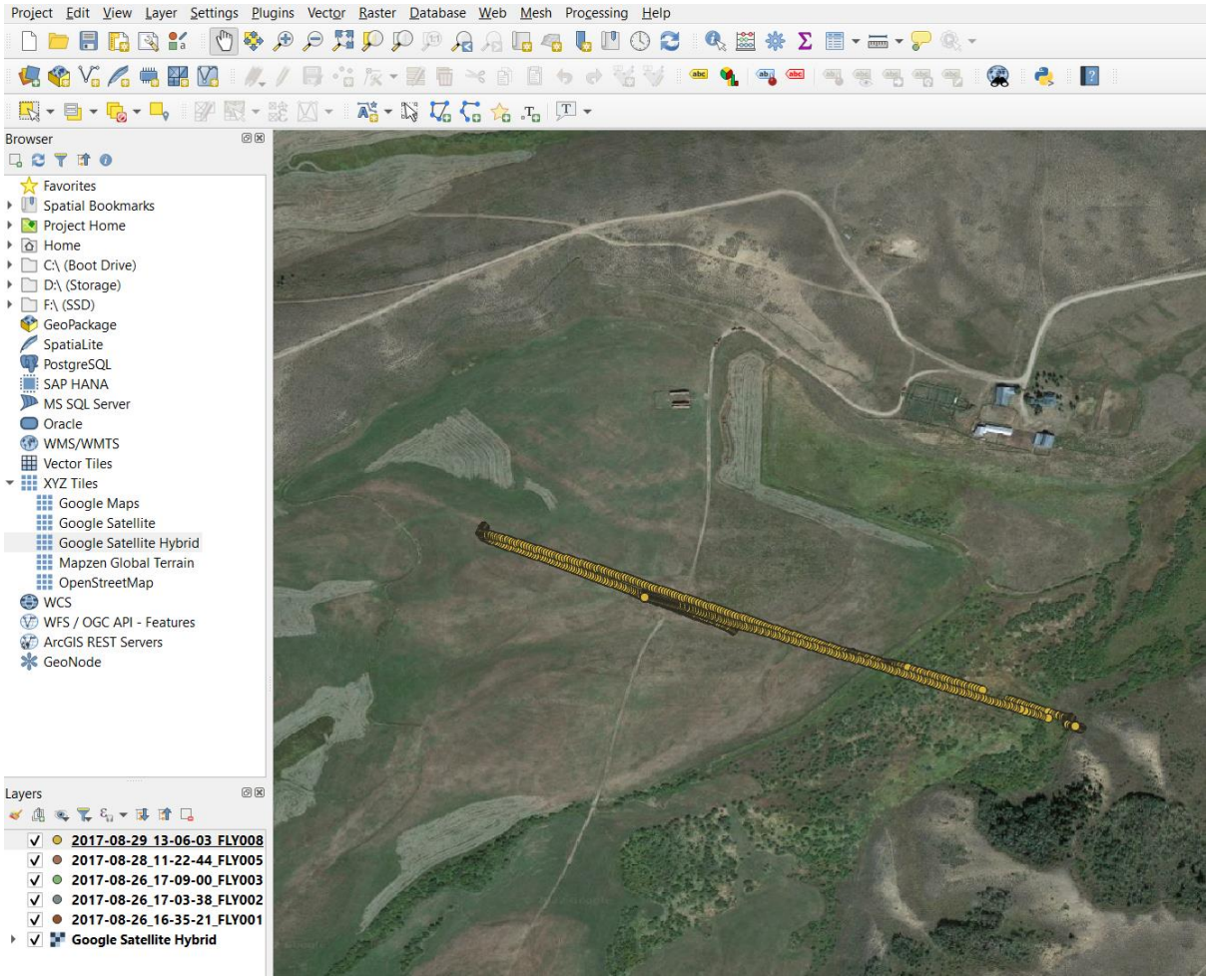


FIGURE 44 – FAR VIEW OF 2017-08-29_13-06-03_FLY008.DAT

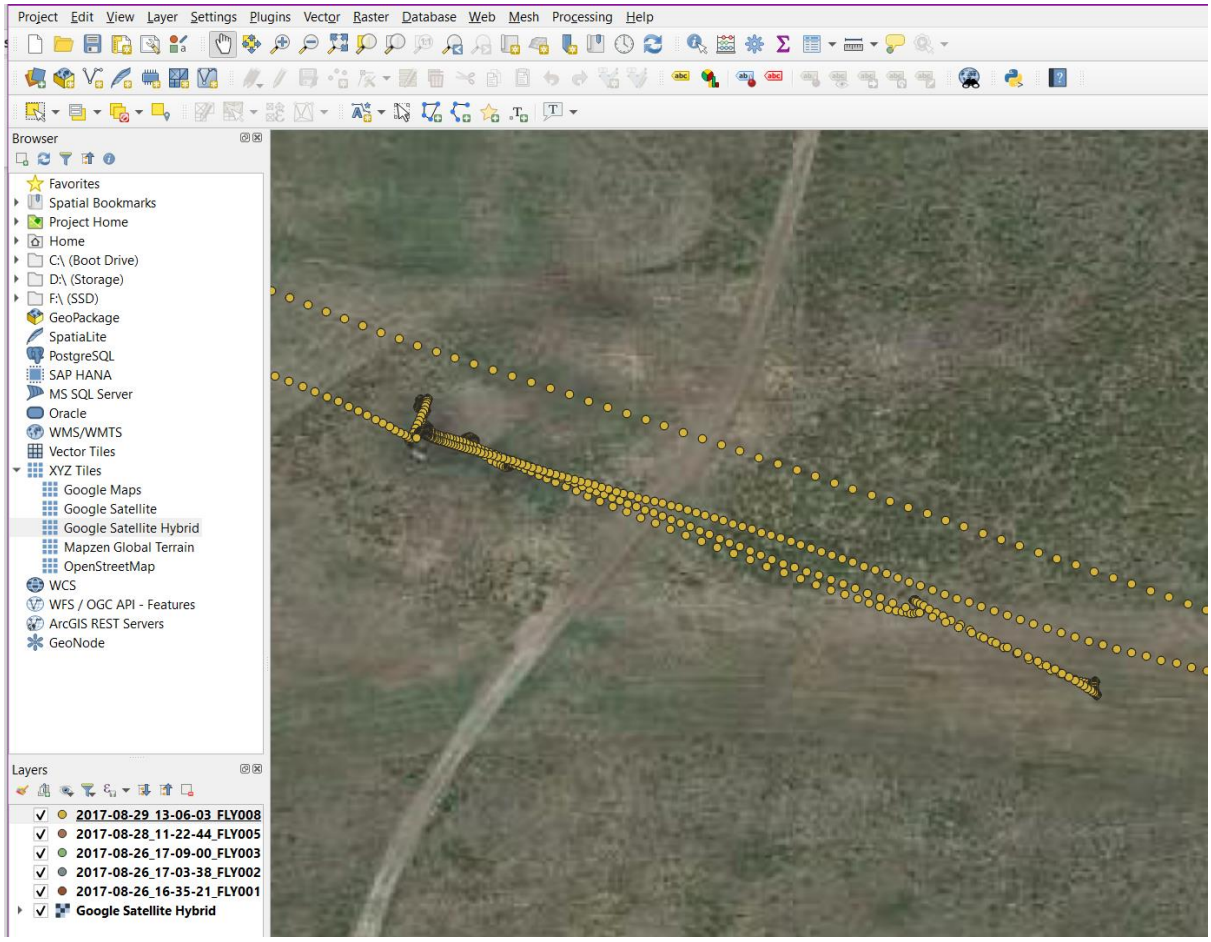


FIGURE 45 – CLOSE VIEW OF 2017-08-29_13-06-03_FLY008.DAT

The four remaining DAT flight logs are not located near `[2017-08-29_13-06-03_FLY008.DAT]`. Figure 46 – Unrealistic IOS Coordinates shows both flight logs `[2017-08-28_11-22-44_FLY005.DAT]` and `[2017-08-26_16-35-21_FLY001.DAT]`, colored red and yellow, contain unrealistic coordinates and should be marked as invalid data. The remaining DAT flight logs contain coordinates that are located in Interlocken, Broomfield, Colorado (Figure 47 – VTO Inc Headquarters Location). We have seen the same locations in the Android flight logs and it is likely the drone was only activated and not flown here.

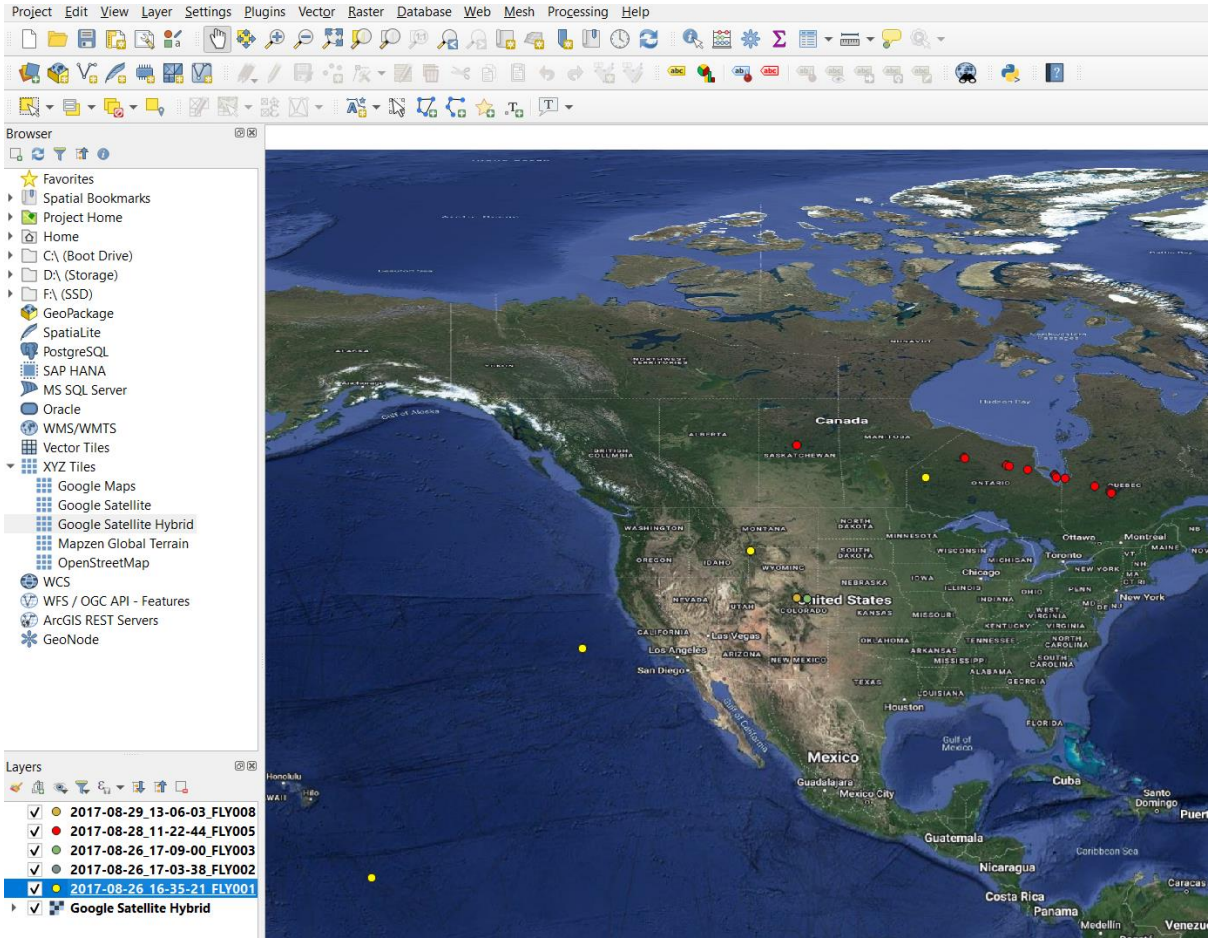


FIGURE 46 – UNREALISTIC IOS COORDINATES

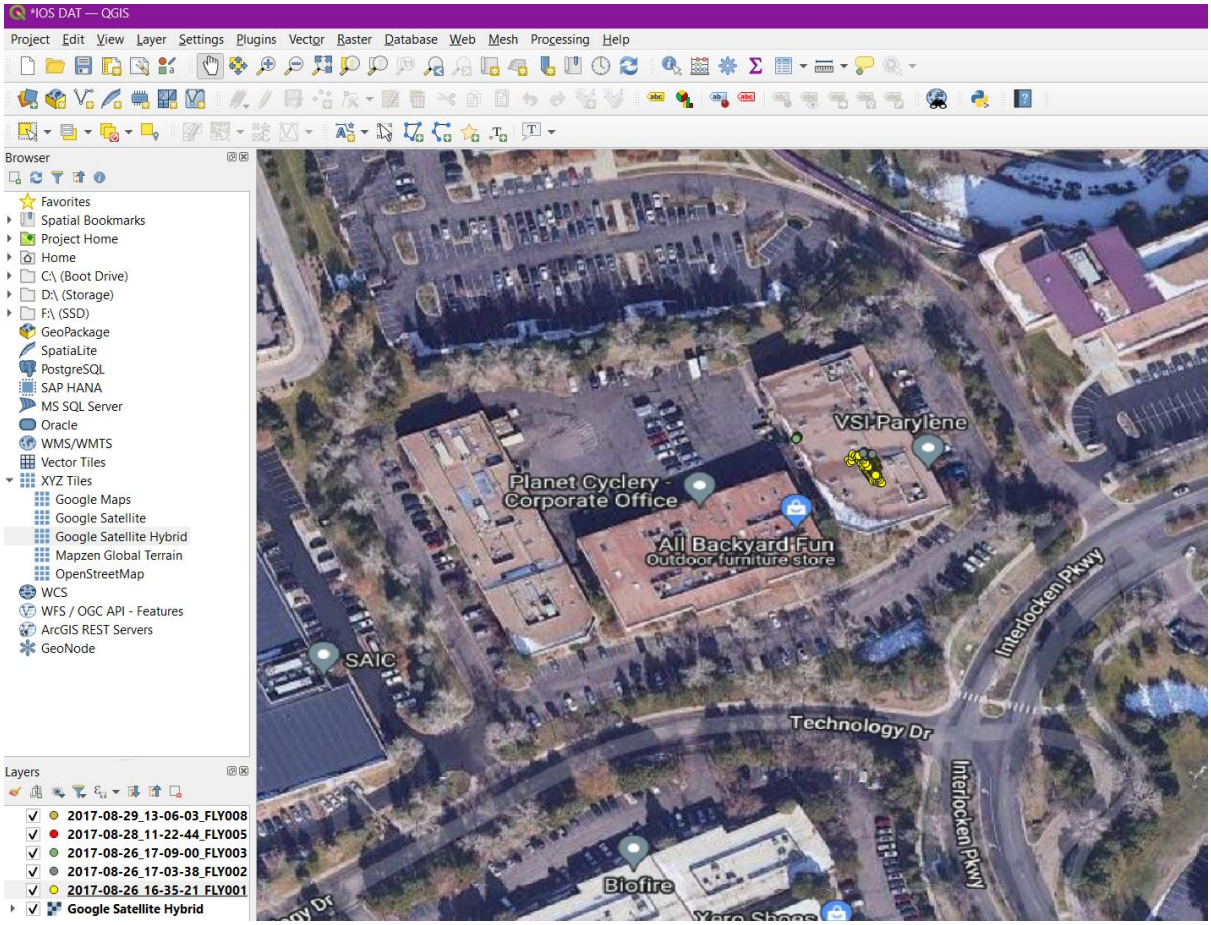


FIGURE 47 – VTO INC HEADQUARTERS LOCATION

5.3.4 Component Logs Analysis

The three remaining logs `[2017-08-29 13_07_28-095XDCK002002W.dat]`, `[2017-08-29 13_14_55-095XDCK002002W.dat]` and `[2017-08-29 13_16_07-095XDCK002002W.dat]` that were found in the IOS backup files do not contain any locational data. Upon further inspection they hold data related to the actions of components on board, it is very similar to what was found on the Android device shown in Figure 32 – Contents of 29-08-2017-095XDCK002002W. The exact contents are provided in Table 5 – Contents of Component Data Logs. From the time stamps provided in all three logs it can be determined that this data was created during the two flights made on the drone.

File	Contents
2017-08-29 13_07_28-095XDCK002002W.dat	[["2017-08-29 13:07:28","","Home Point Recorded. RTH Altitude: 30m."]],[["2017-08-29 13:07:33","","Landing gear lowered.Obstacle Avoidance Disabled."]],[["2017-08-29 13:08:57","Tips","Aircraft is returning to the Home Point. Minimum RTH Altitude is 30m. You can reset the RTH Altitude in Remote Controller Settings after cancelling RTH."]],[["2017-08-29 13:09:29","","Obstacle Avoidance will be disabled in landing."],["2017-08-29 13:09:30","","Landing gear lowered.Obstacle Avoidance Disabled."]],[["2017-08-29 13:10:00","","Landing Protection Activated. Aircraft will decelerate during landing."],["2017-08-29 13:10:06","","Ground Plain. Safe to Land."]],[["2017-08-29 13:10:40","Tips","Taking Off"],["2017-08-29 13:10:41","Tips","Taking Off"],["2017-08-29 13:10:42","","Home Point Recorded. RTH Altitude: 30m."]],[["2017-08-29 13:11:55","High Wind Velocity","Fly with caution and ensure the aircraft remains within your line of sight."]],[["2017-08-29 13:12:21","High Wind Velocity","Fly with caution and ensure the aircraft remains within your line of sight."]]
2017-08-29 13_14_55-095XDCK002002W.dat	[["2017-08-29 13:14:55","Advanced RTH","Image Transmission Recovered. Aircraft is returning home."]]
2017-08-29 13_16_07-095XDCK002002W.dat	[["2017-08-29 13:16:07","","Obstacle Avoidance will be disabled in landing."]],[["2017-08-29 13:16:07","","Landing gear lowered.Obstacle Avoidance Disabled."]],[["2017-08-29 13:16:39","","Landing Protection Activated. Aircraft will decelerate during landing."],["2017-08-29 13:16:45","","Ground Plain. Safe to Land."]]

TABLE 5 – CONTENTS OF COMPONENT DATA LOGS

5.3.5 MD5 Hash Values of IOS Flight Data Files

File	MD5
DJIFlightRecord_2017-08-29_[13-07-17].txt	dfe8a33a2532f928303070926f0f52c5
DJIFlightRecord_2017-08-29_[13-10-40].txt	8aba751f5e2a79524c3887570a0032bd
2017-08-26_16-35-21_FLY001.DAT	5ecae3678c19ed9b227c6b9060537e4f
2017-08-26_17-03-38_FLY002.DAT	3e098e2943cd9392bf618d22d87d1f1c
2017-08-26_17-09-00_FLY003.DAT	2843c05157bcf5ca2b46ccb1bea49845
2017-08-28_11-22-44_FLY005.DAT	c66778db73d340840e0fee9b56ce68ea
2017-08-29_13-06-03_FLY008.DAT	51a455f2462ef6b25243e4c4ecce2e3e
2017-08-29 13_07_28-095XDCK002002W.dat	5bb6410a0e20d8241a61669d1917e9d0
2017-08-29 13_14_55-095XDCK002002W.dat	97fa51bb0a27bac2a1d9f44e03eca2e3
2017-08-29 13_16_07-095XDCK002002W.dat	dc447858ecb4f7b48a5a1efd4a50e3df

HASHES 5

5.4 Internal SD Card Flight Data Analysis

5.4.1 DAT Flight Data Analysis

The internal SD card contains only DAT formatted flight logs, excluding the other non-relevant logs. A total of thirteen logs are present, an overview of the coordinates is shown in Figure 48 – All Coordinates Present on Internal SD Card. Six of the logs contain unrealistic data and can be marked as invalid. Each of these invalid logs either contain a path that is simply impossible for any consumer drone, or the coordinates are set to (0, 0) creating a single point in the South Atlantic Ocean. The remaining logs are located in the suspected airspace and VTO Inc's Headquarters (Figure 49 – Reliable DAT Flight Logs on Internal SD Card). Viewing Arapaho and Roosevelt National Forests, Denver, Colorado shows three possible flight paths (Figure 50 – Flight Paths on Internal SD Card), the log `[FLY008.DAT]`, colored pink, contains the flight paths of all four flights made here (2 via Android and 2 via IOS). Hiding `[FLY008.DAT]`, leaves two short paths created by `[FLY009.DAT]` and `[FLY007.DAT]` (Figure 51 – Potential Anomalies on Internal SD Card). These are likely anomalies created when the drone is landing, this situation is similar to what appeared in the Android logs shown in Figure 21 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-23-50].txt. The four remaining logs are located in and around VTO Inc's Headquarters, (Figure 52 – Remaining DAT Flight Logs on Internal SD Card). A whole range of paths are shown, and it is very hard to identify what exactly happened. As no paths match the data In the TXT logs, it is impossible to confirm the accuracy in them. The paths that only appear in the DAT logs and not the TXT format are likely made when the drone is not actually in flight.

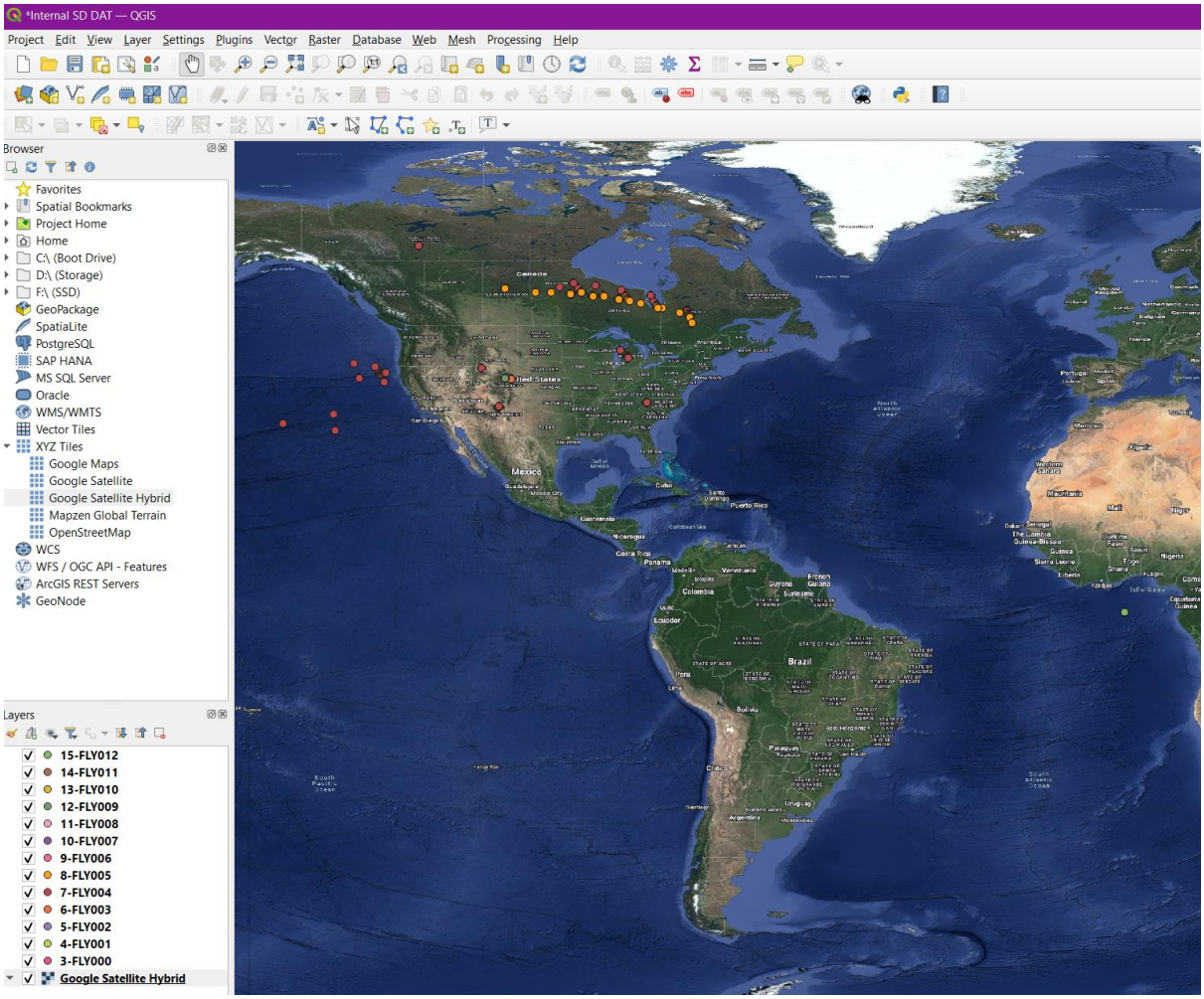


FIGURE 48 – ALL COORDINATES PRESENT ON INTERNAL SD CARD

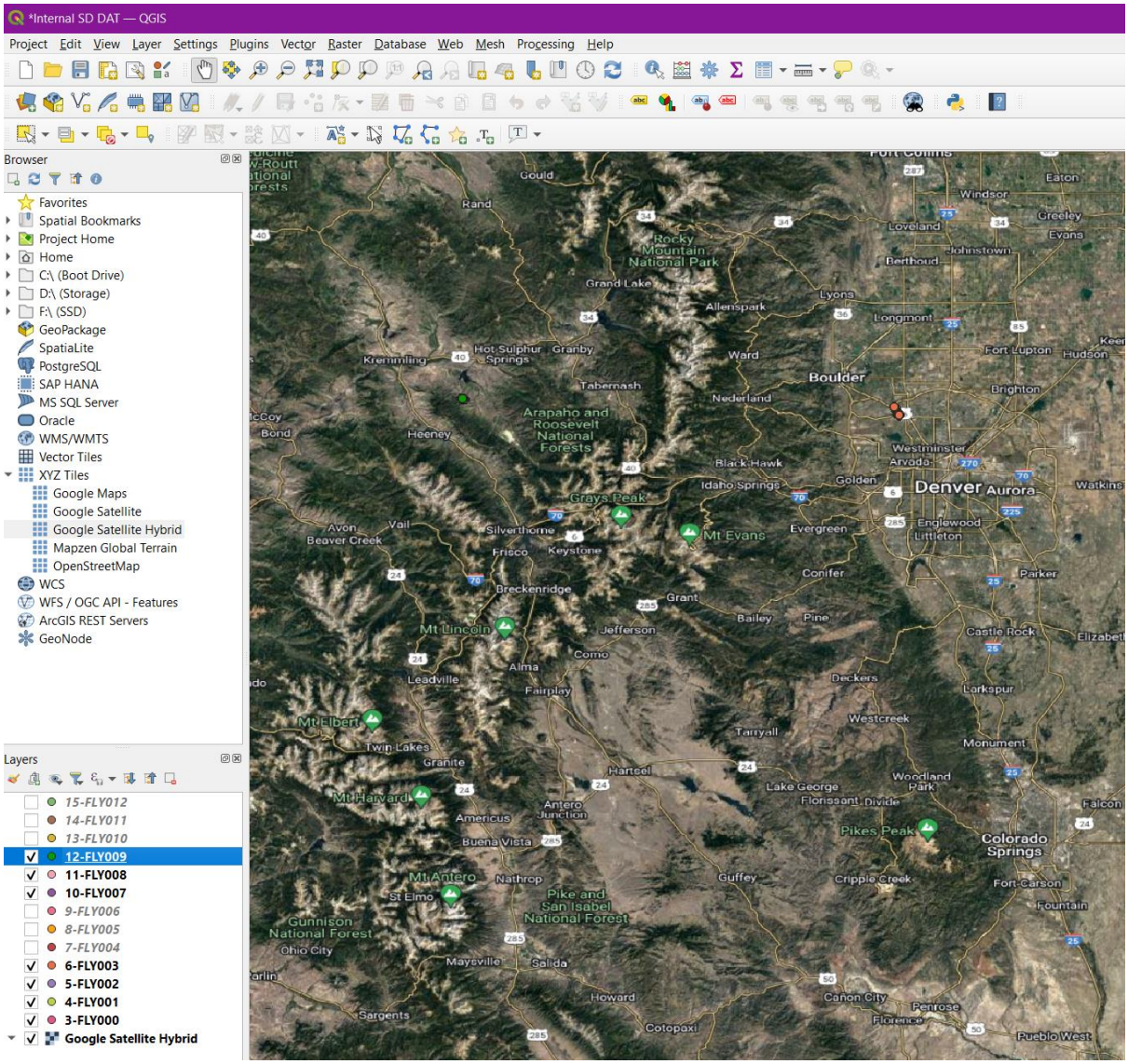


FIGURE 49 – RELIABLE DAT FLIGHT LOGS ON INTERNAL SD CARD

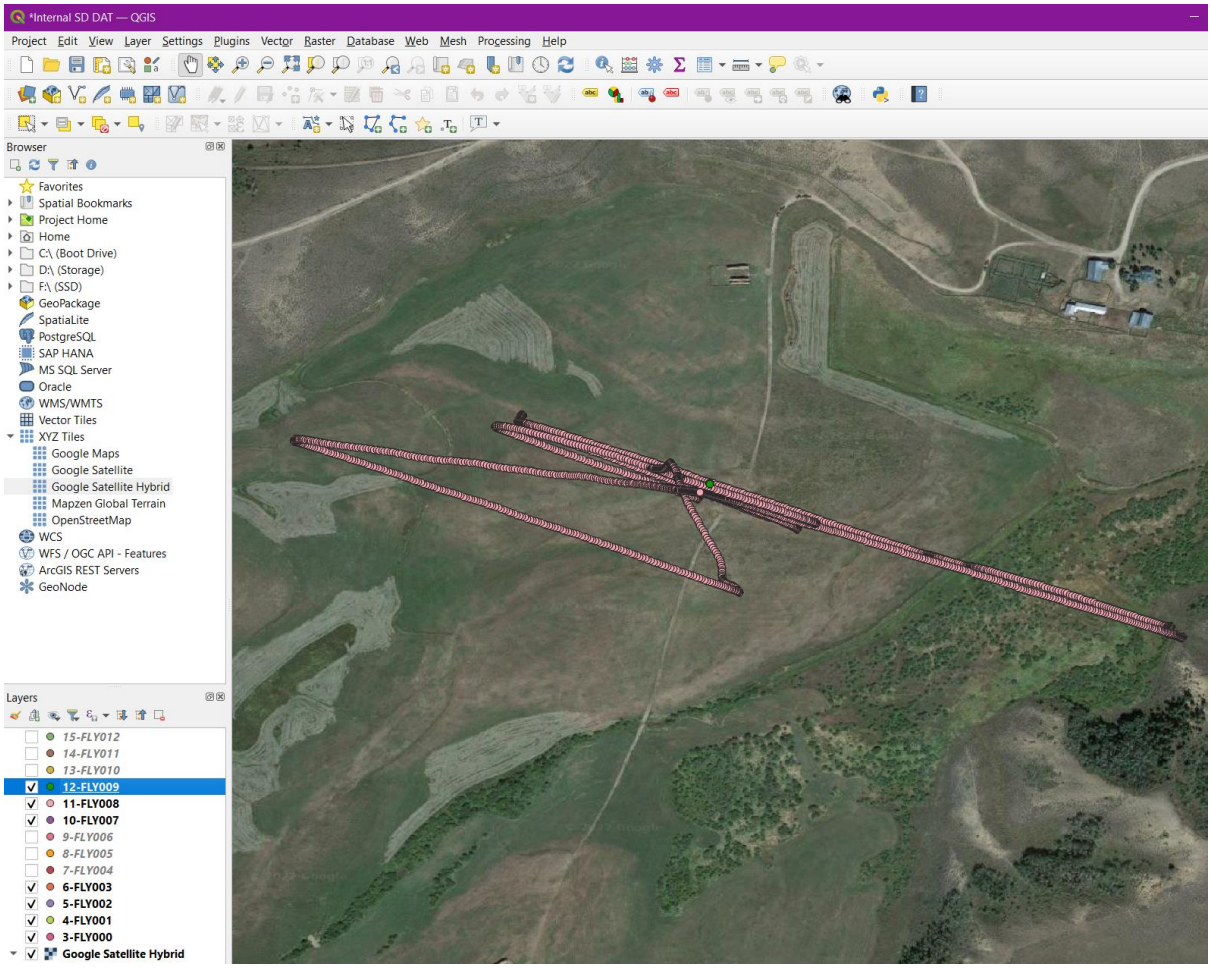


FIGURE 50 – FLIGHT PATHS ON INTERNAL SD CARD

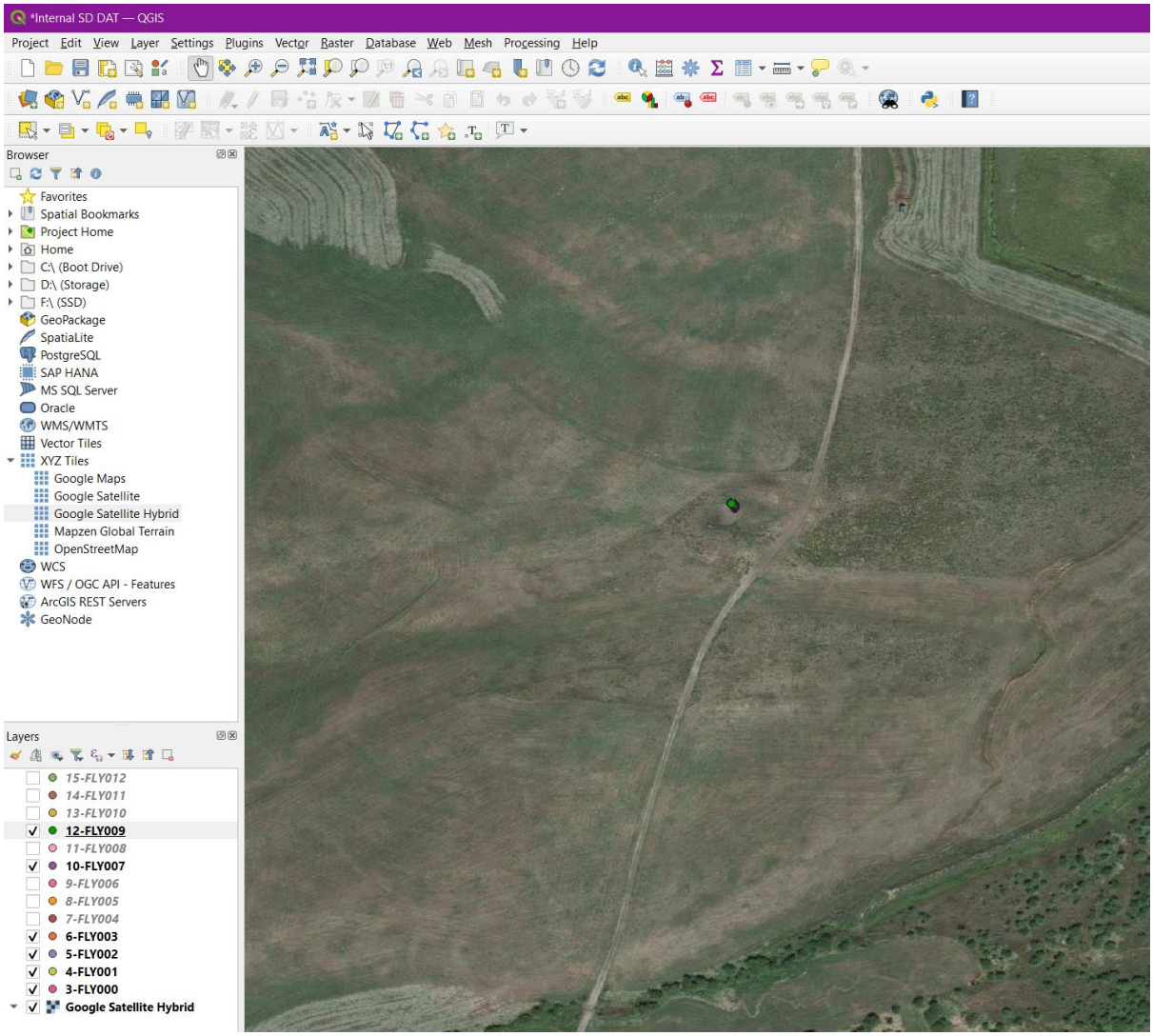


FIGURE 51 – POTENTIAL ANOMALIES ON INTERNAL SD CARD

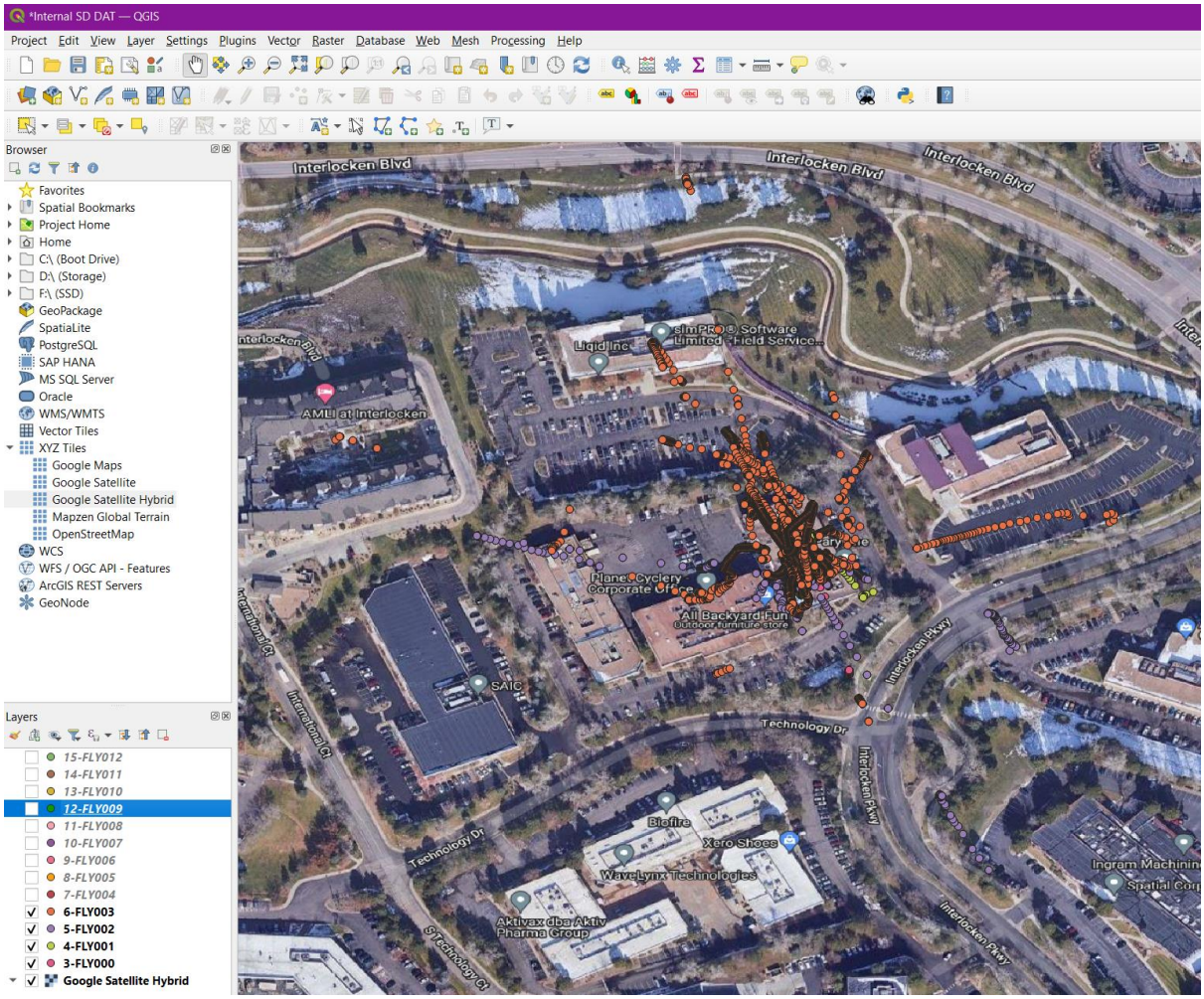


FIGURE 52 – REMAINING DAT FLIGHT LOGS ON INTERNAL SD CARD

5.4.2 MD5 Hash Values of Internal SD Card Flight Data Files

File	MD5
FLY000.DAT	e0aac994ae0605da242b0b01f60f6a5f
FLY001.DAT	0b99262c9bcbb26cab0c8cfbe313bb8d
FLY002.DAT	fda5c12c99bc0d3eba469dc21fdb7ffb
FLY003.DAT	c63233f0dfcc6bdf0b9b7ef3c6365b88
FLY004.DAT	0c35670a0ef3d61440a02ad7b9047807
FLY005.DAT	2a685052e2c2f50ec5cea873973d976d
FLY006.DAT	696a865d26882d025f2fbed11c39b2f7
FLY007.DAT	34a42a5bc41d2b4422ea9205cb774b20
FLY008.DAT	b4d6930837eb2684aec95e200e606f07
FLY009.DAT	1e0b60019060ff1768602dfe27ece192
FLY010.DAT	fe1883ae7c0271df355da76bfd0d5245
FLY011.DAT	69a548032b34189ac0e22148aabe1e2f
FLY012.DAT	2a70d53212c1d66967fc7891ad97ae73

HASHES 6

5.5 DAT IDENTIFIER PYTHON PROGRAM

5.5.1 DAT IDENTIFIER CONTENTS AND USE

The main issue when creating a case using the DAT formatted flight logs is that some may contain unreliable data. Some situations may present data that is not easy to identify whether it should be relied upon. The following Python program was created to assist with this decision making, the code is shown in Table 6 – Contents of DATIdentifier.py. This program was made to be simple for its users, paste it into the directory where the converted DAT flight logs are, this should consist of only CSV files (Figure 53 – Example of Directory Contents). Once the Python program has been executed a directory will be created labelled `[DATIdentifierOUT]`, the contents of the log file called `[DIOutput.txt]` will be present in here.

Contents

```
import pandas as pd
import numpy as np
import glob
import os

# get names of all csv files in current dir
path = ""
files = glob.glob(path + "*.csv")
# if output folder doesnt exist, create it
if not os.path.exists("DATIdentifierOUT"):
    os.mkdir("DATIdentifierOUT ")
# dictionary for statistics generated
stats_dict = {
    "Longitude Zeros": 0,
    "Longitude Nulls": 0,
    "Latitude Zeros": 0,
    "Latitude Nulls": 0,
    "Height Zeros": 0,
    "Height Nulls": 0,
    "Date Zeros": 0,
    "Date Nulls": 0,
    "Time Zeros": 0,
    "Time Nulls": 0
}
# loop through all csv files found in current dir
for x in range(len(files)):
    # read csv into dataframe
    df = pd.read_csv(files[x], low_memory=False)
    # total rows in df
    num_rows = len(df.index)
    # count number of null cells
    stats_dict["Longitude Nulls"] = df["GPS:Long"].isnull().sum()
    stats_dict["Latitude Nulls"] = df["GPS:Lat"].isnull().sum()
    stats_dict["Height Nulls"] = df["GPS:heightMSL"].isnull().sum()
    stats_dict["Date Nulls"] = df["GPS:Date"].isnull().sum()
    stats_dict["Time Nulls"] = df["GPS:Time"].isnull().sum()
    # count number of zeros present in columns
    # sometimes FLYXXX.DAT files contain cells with large number of
zeros
    try:
        stats_dict["Longitude Zeros"] =
```

```
df["GPS:Long"].value_counts()[0]
    except:
        stats_dict["Longitude Zeros"] = 0
    try:
        stats_dict["Latitude Zeros"] =
df["GPS:Lat"].value_counts()[0]
    except:
        stats_dict["Latitude Zeros"] = 0
    try:
        stats_dict["Height Zeros"] =
df["GPS:heightMSL"].value_counts()[0]
    except:
        stats_dict["Height Zeros"] = 0
    try:
        stats_dict["Date Zeros"] = df["GPS:Date"].value_counts()[0]
    except:
        stats_dict["Date Zeros"] = 0
    try:
        stats_dict["Time Zeros"] = df["GPS:Time"].value_counts()[0]
    except:
        stats_dict["Time Zeros"] = 0
    # convert dataframe to numpy array
    long_array = (df["GPS:Long"].to_numpy())
    lat_array = (df["GPS:Lat"].to_numpy())
    # remove zeros
    long_remove_zeros = long_array[long_array != 0]
    lat_remove_zeros = lat_array[lat_array != 0]
    # remove nan value
    long_remove_nan =
long_remove_zeros[np.logical_not(np.isnan(long_remove_zeros))]
    lat_remove_nan =
lat_remove_zeros[np.logical_not(np.isnan(lat_remove_zeros))]
    # reset warning flags
    long_warning = False
    lat_warning = False
    # if numpy array is not empty
    if long_remove_nan.size != 0:
        # find minmia and maxima values
        long_minima = np.min(long_remove_nan)
        long_maxima = np.max(long_remove_nan)
        # calculate range
        long_range = long_maxima - long_minima
        # set warning if range is large
        if long_range > 1:
            long_warning = True
    if lat_remove_nan.size != 0:
        lat_minima = np.min(lat_remove_nan)
        lat_maxima = np.max(lat_remove_nan)
        lat_range = lat_maxima - lat_minima
        if lat_range > 1:
            lat_warning = True
    # create log file to make identifing poor quality FLYXXX.DAT
files easier
    with open("DATIdentifierOUT /DIOutput.txt", "a") as f:
        print(files[x], file = f)
```

```
        print("--------------------", file = f)
        for key in stats_dict:
            print(key, " : ", stats_dict[key], file = f)
        print("total rows : ", num_rows, file = f)
        if long_warning:
            print("WARNING large change in longitude", file = f)
            print("longitude range : ", long_range, file = f)
        if lat_warning:
            print("WARNING large change in latitude", file = f)
            print("longitude range : ", lat_range, file = f)
        print("--------------------", file = f)
```

TABLE 6 – CONTENTS OF DATIDENTIFIER.PY

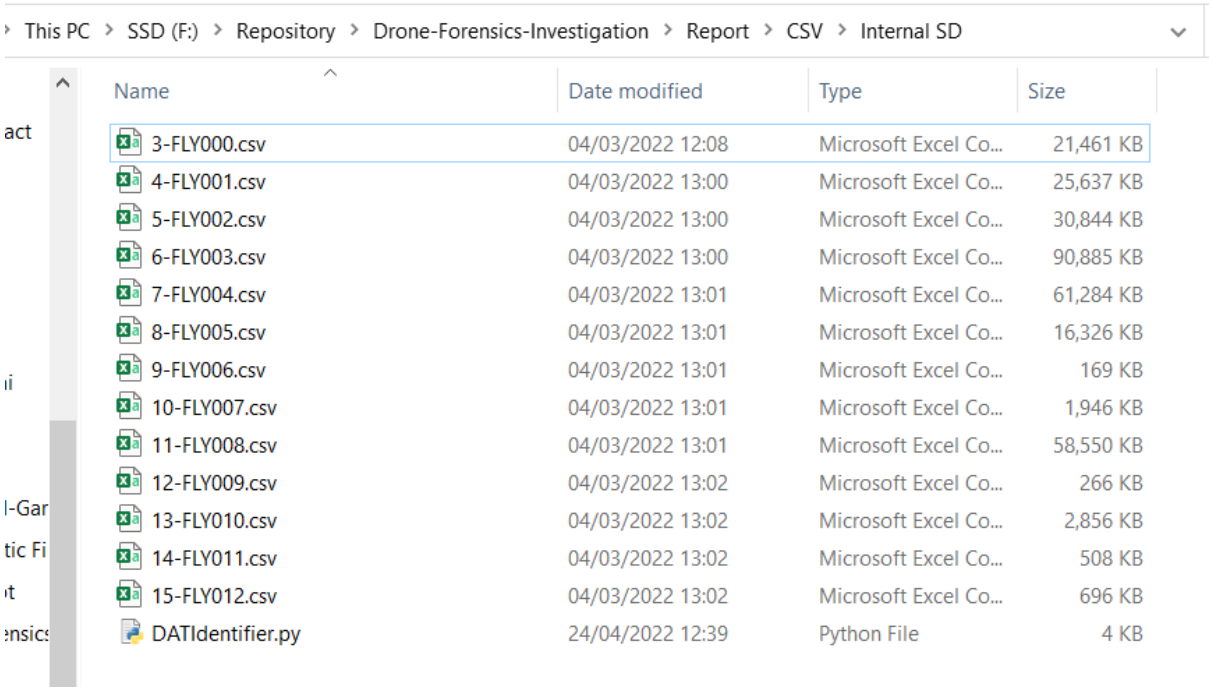


FIGURE 53 – EXAMPLE OF DIRECTORY CONTENTS

5.5.2 DAT IDENTIFIER OUTPUT

The programs output will contain a list of statistics for each CSV file. The number of zero and null values in the GPS data will be shown alongside the columns heading. This can be compared to the total rows and the paths created in QGIS to allow an informed decision to be made. This program should only be used to assist in deciding whether the data is reliable, it is not there to make it for you. The results from running this on the data provided in the internal SD card of the DJI Inspire 2 is shown in Table 7 – Output of DATIdentifier.py.

Example Contents

```
10-FLY007.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  1
Latitude Zeros  :  0
Latitude Nulls  :  1
Height Zeros  :  0
Height Nulls  :  1
Date Zeros  :  0
Date Nulls  :  1
Time Zeros  :  0
Time Nulls  :  1
total rows :  1045
--------------------
11-FLY008.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  1
Latitude Zeros  :  0
Latitude Nulls  :  1
Height Zeros  :  0
Height Nulls  :  1
Date Zeros  :  0
Date Nulls  :  1
Time Zeros  :  0
Time Nulls  :  1
total rows :  29263
--------------------
12-FLY009.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  1
Latitude Zeros  :  0
Latitude Nulls  :  1
Height Zeros  :  0
Height Nulls  :  1
Date Zeros  :  0
Date Nulls  :  1
Time Zeros  :  0
Time Nulls  :  1
total rows :  164
--------------------
13-FLY010.csv
--------------------
Longitude Zeros  :  1917
```

```
Longitude Nulls  :  12
Latitude Zeros  :  1917
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  1929
Date Zeros  :  0
Date Nulls  :  1929
Time Zeros  :  0
Time Nulls  :  1929
total rows :  1929
--------------------
14-FLY011.csv
--------------------
Longitude Zeros  :  391
Longitude Nulls  :  12
Latitude Zeros  :  391
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  403
Date Zeros  :  0
Date Nulls  :  403
Time Zeros  :  0
Time Nulls  :  403
total rows :  403
--------------------
15-FLY012.csv
--------------------
Longitude Zeros  :  516
Longitude Nulls  :  12
Latitude Zeros  :  516
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  528
Date Zeros  :  0
Date Nulls  :  528
Time Zeros  :  0
Time Nulls  :  528
total rows :  528
--------------------
3-FLY000.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  6
Latitude Zeros  :  0
Latitude Nulls  :  6
Height Zeros  :  0
Height Nulls  :  4827
Date Zeros  :  0
Date Nulls  :  4827
Time Zeros  :  0
Time Nulls  :  4827
total rows :  13269
--------------------
4-FLY001.csv
--------------------
```

```
Longitude Zeros  :  0
Longitude Nulls  :  9
Latitude Zeros  :  0
Latitude Nulls  :  9
Height Zeros  :  0
Height Nulls  :  21
Date Zeros  :  0
Date Nulls  :  21
Time Zeros  :  0
Time Nulls  :  21
total rows :  15797
--------------------
5-FLY002.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  37
Latitude Zeros  :  0
Latitude Nulls  :  37
Height Zeros  :  0
Height Nulls  :  759
Date Zeros  :  0
Date Nulls  :  759
Time Zeros  :  0
Time Nulls  :  759
total rows :  19085
--------------------
6-FLY003.csv
--------------------
Longitude Zeros  :  0
Longitude Nulls  :  8
Latitude Zeros  :  0
Latitude Nulls  :  8
Height Zeros  :  0
Height Nulls  :  7369
Date Zeros  :  0
Date Nulls  :  7369
Time Zeros  :  0
Time Nulls  :  7369
total rows :  56427
--------------------
7-FLY004.csv
--------------------
Longitude Zeros  :  1964
Longitude Nulls  :  12
Latitude Zeros  :  1964
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  38981
Date Zeros  :  0
Date Nulls  :  38981
Time Zeros  :  0
Time Nulls  :  38981
total rows :  38981
WARNING large change in longitude
longitude range :  69.27538820000001
```

```
WARNING large change in latitude
longitude range :  31.681808400000005
--------------------
8-FLY005.csv
--------------------
Longitude Zeros  :  1354
Longitude Nulls  :  12
Latitude Zeros  :  1354
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  10462
Date Zeros  :  0
Date Nulls  :  10462
Time Zeros  :  0
Time Nulls  :  10462
total rows :  10462
WARNING large change in longitude
longitude range :  32.137746899999996
WARNING large change in latitude
longitude range :  5.8503266999999965
--------------------
9-FLY006.csv
--------------------
Longitude Zeros  :  162
Longitude Nulls  :  12
Latitude Zeros  :  162
Latitude Nulls  :  12
Height Zeros  :  0
Height Nulls  :  174
Date Zeros  :  0
Date Nulls  :  174
Time Zeros  :  0
Time Nulls  :  174
total rows :  174
--------------------
```

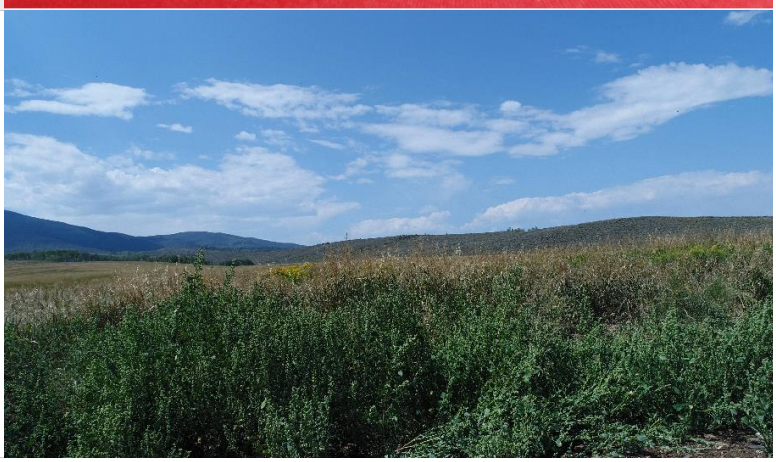
TABLE 7 – OUTPUT OF DATIDENTIFIER.PY

6. Media Analysis

6.1 External SD Card Media Analysis

6.1.1 External SD Card Media Analysis

An important part of reconstructing the events that occurred is retrieving the media that was taken. Media artifacts should be present on the physical Android image, IOS backup file and the external SD card. Starting with the external SD card, a total of eight MOV files are found. Four are found in `[DCIM/100MEDIA]` which is the only visible directory to the normal user. The user will likely extract their videos from here after the flight. The other four are stored in the thumbnail directory `[MISC/THM/100]`, this directory is hidden, and the four videos contained are essentially a copy in reduced resolution. The length and a thumbnail of the four recorded videos are provided in Table 8 – Media Details of External SD Card. Inspecting the bytes for each video finds the same value `[FC6510]` listed in bytes 38 to 3D. We can see that this value corresponds to the Zenmuse X4S camera used on the DJI Inspire 2 (Figure 20 – Android Drone Details and Figure 41 – IOS Drone Details).

Details	**Screen Capture**
DCIM/100MEDIA/DJI_0001.MOV Length: 2:34	
DCIM/100MEDIA/DJI_0002.MOV Length: 5:27	

DCIM/100MEDIA/DJI_0003.MOV Length: 00:35	
DCIM/100MEDIA/DJI_0004.MOV Length: 5:26	

TABLE 8 – MEDIA DETAILS OF EXTERNAL SD CARD

6.1.2 MD5 Hash Values of Media Contained on External SD Card

File	MD5
DJI_0001.MOV	6ec12de50d9860d619f59c3ca14309e1
DJI_0002.MOV	374df6c83d7dec57369de62b18289367
DJI_0003.MOV	a74c876f545d31ea3f1dbf3c3b7d58f5
DJI_0004.MOV	b1e26f6998122638e63a5836c195ea84

HASHES 7

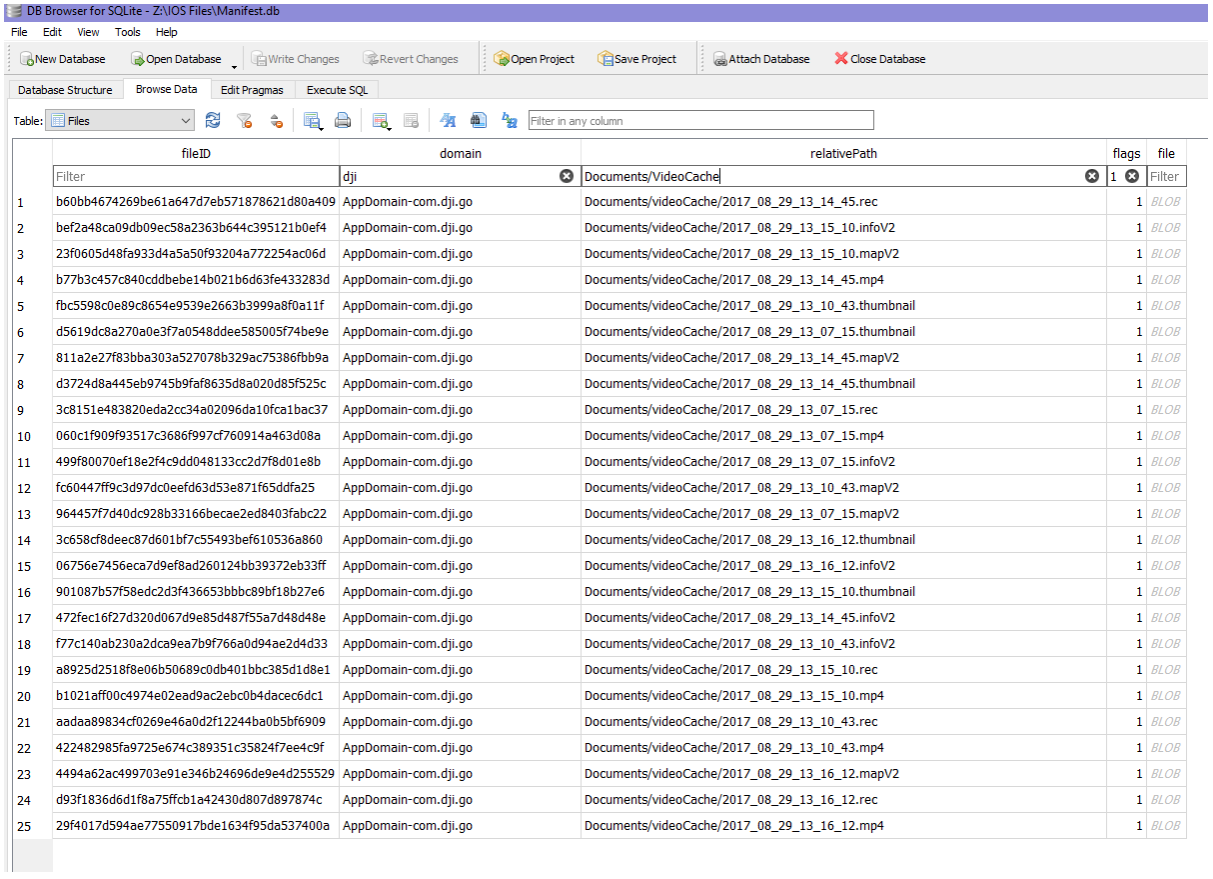
6.2 IOS MEDIA ANALYSIS

6.2.1 IOS MEDIA ANALYSIS

The IOS backup file contains a large amount of data in its video cache. A total of five MP4 files can be found, see Figure 54 – All Files in IOS Video Cache. Lengths and screen captures are provided in Table 9 – Media Details of IOS Device. The first video taken, [2017_08_29_13_07_15.mp4], matches the video [DJI_0001.MOV] extracted from the external SD card.

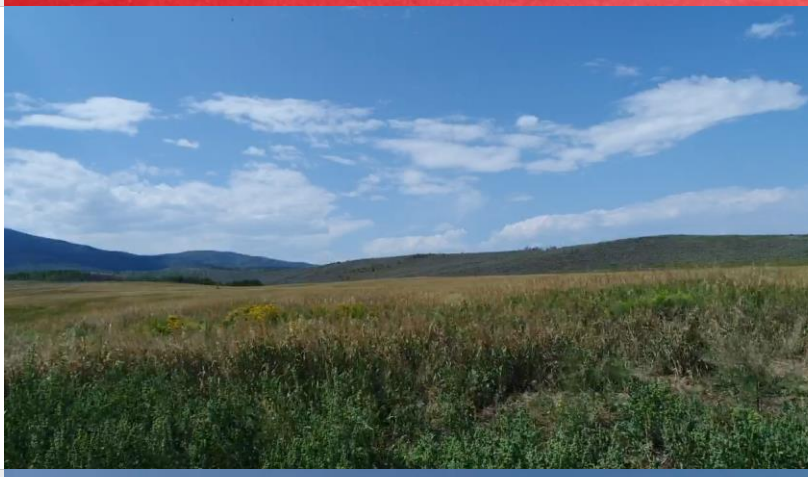
There are an additional four videos on the IOS device that all seem to be from the same flight just chopped up into different files. This would result in an exact 5-minute video if they were put together. Analysing the videos together results in [DJI_0002.MOV] containing the same details as [2017_08_29_13_14_45.mp4], [2017_08_29_13_15_10.mp4] and [2017_08_29_13_15_10.mp4]. However, these videos do not contain the landing sequence, the final MP4 file [2017_08_29_13_16_12.mp4] is the same as [DJI_0003.MOV] and these two videos appear to be the landing part but simply removed from the rest of the video. We are also able to use the thumbnails provided in Figure 39 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-07-17].txt and Figure 42 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-10-40].txtwhich match up to the scenery included in the media.

We do not know if splitting the media up into different sections was intended, but we must assume from now on that single flights may consist of various pieces of media. These can be put together to create the full flight.



	fileID	domain	relativePath	flags	file
	Filter	dji	Documents/VideoCache	1	Filter
1	b60bb4674269be61a647d7eb571878621d80a409	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_14_45.rec	1	BLOB
2	bef2a48ca09db09ec58a2363b644c395121b0ef4	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_15_10.infoV2	1	BLOB
3	23f0605d48fa933d4a5a50f93204a772254ac06d	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_15_10.mapV2	1	BLOB
4	b77b3c457c840cddbebe14b021b6d63fe433283d	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_14_45.mp4	1	BLOB
5	fbc5598c0e89c8654e9539e2663b3999a8f0a11f	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_10_43.thumbnail	1	BLOB
6	d5619dc8a270a0e3f7a0548ddee585005f74be9e	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_07_15.thumbnail	1	BLOB
7	811a2e27f83bba303a527078b329ac75386fbb9a	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_14_45.mapV2	1	BLOB
8	d3724d8a445eb9745b9faf8635d8a020d85f525c	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_14_45.thumbnail	1	BLOB
9	3c8151e483820eda2cc34a02096da10fca1bac37	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_07_15.rec	1	BLOB
10	060c1f909f93517c3686f997cf760914a463d08a	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_07_15.mp4	1	BLOB
11	499f80070ef18e2f4c9dd048133cc2d7f8d01e8b	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_07_15.infoV2	1	BLOB
12	fc60447ff9c3d97dc0eefd63d53e871f65ddfa25	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_10_43.mapV2	1	BLOB
13	964457f7d40dc928b33166becae2ed8403fabc22	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_07_15.mapV2	1	BLOB
14	3c658cf8deec87d601bf7c55493bef610536a860	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_16_12.thumbnail	1	BLOB
15	06756e7456eca7d9ef8ad260124bb39372eb33ff	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_16_12.infoV2	1	BLOB
16	901087b57f58edc2d3f436653bbbc89bf18b27e6	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_15_10.thumbnail	1	BLOB
17	472fec16f27d320d067d9e85d487f55a7d48d48e	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_14_45.infoV2	1	BLOB
18	f77c140ab230a2dca9ea7b9f766a0d94ae2d4d33	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_10_43.infoV2	1	BLOB
19	a8925d2518f8e06b50689c0db401bbc385d1d8e1	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_15_10.rec	1	BLOB
20	b1021aff00c4974e02ead9ac2ebc0b4dacec6dc1	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_15_10.mp4	1	BLOB
21	aadaa89834cf0269e46a0d2f12244ba0b5bf6909	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_10_43.rec	1	BLOB
22	422482985fa9725e674c389351c35824f7ee4c9f	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_10_43.mp4	1	BLOB
23	4494a62ac499703e91e346b24696de9e4d255529	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_16_12.mapV2	1	BLOB
24	d93f1836d6d1f8a75ffcb1a42430d807d897874c	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_16_12.rec	1	BLOB
25	29f4017d594ae77550917bde1634f95da537400a	AppDomain-com.dji.go	Documents/videoCache/2017_08_29_13_16_12.mp4	1	BLOB

FIGURE 54 – ALL FILES IN IOS VIDEO CACHE

Details	Screen Capture
2017_08_29_13_07_15.mp4 Length: 2:33	
2017_08_29_13_10_43.mp4 Length: 3:30	
2017_08_29_13_14_45.mp4 Length: 00:06	

2017_08_29_13_15_10.mp4 Length: 00:52	
2017_08_29_13_16_12.mp4 Length: 00:32	

TABLE 9 – MEDIA DETAILS OF IOS DEVICE

6.2.2 MD5 Hash Values of Media Contained on IOS Device

File	MD5
2017_08_29_13_07_15.mp4	56dad8ebe624de41fa5f5d60eec6776e
2017_08_29_13_10_43.mp4	57f8ffba720831a01a14428e57787114
2017_08_29_13_14_45.mp4	c9a41f598c6bf0b91f7492bff15b14e6
2017_08_29_13_15_10.mp4	e34ab0f55622f147dc6c5f9104227125
2017_08_29_13_16_12.mp4	f78b8cc090df965a238b3b678d8e609f

HASHES 8

6.3 Android Media Analysis

6.3.1 Android Media Analysis

Only one video is contained on the Android device as shown in Table 10 – Media Details of Android Device. The DJI GO 4 application on Android stores media contents in `[media/0/DJI/dji.go.v4/DJI_RECORD]`. The contents displayed in `[2017_08_29_13_18_01.mp4]` can be synced up with the video `[DJI_0004.MOV]` present on the external SD card. The timestamp included in the name is in the same time frame as the flight logs covered in 5.2 Android Flight Data Analysis. This further leads to the conclusion that this media was taken during the flight in Figure 18 – AIRDATA Overview of DJIFlightRecord_2017-08-29_[13-18-04].txt.

Details	Screen Capture
2017_08_29_13_18_01.mp4 Length: 5:41	

TABLE 10 – MEDIA DETAILS OF ANDROID DEVICE

6.3.2 MD5 Hash Values of Media Contained on Android Device

File	MD5
2017_08_29_13_18_01.mp4	8f79918b54e90d4db4716764c030e2c3

HASHES 9

7. Conclusion

7.1 DJI Inspire 2 Conclusion

Overall, many artifacts could be found on each device. To create a substantial case, it is essential that the drone itself and the device acting as a controller is obtained. For this investigation valid serial numbers, flight paths and media were acquired to function as evidence.

The serial numbers found unfortunately could not be compared to the real values found on the devices. However, we were still able to look them up to find that they do indeed match the same device as described in other artifacts. This first step was crucial as we must confirm that the extracted data used for analysis does come from the devices.

A total of three reliable flight paths were identified. Two were made via an iPad Mini 4 and one was made using a Samsung Galaxy Tab A. With the software and tools used including 5.5 DAT Identifier Python Program, AIRDATA and QGIS all accurate flight paths were identified. The flight paths that contained unreliable or missing data were marked as invalid and removed from the investigation. For this case the DJI Inspire 2 was flown a total of three times. A single flight using the Samsung Galaxy Tab A took place at 1:18:04PM MDT, it lasted approximately 5 minutes and 10 seconds. The iPad Mini 4 was used for two flights, one starting at 1:07:17PM MDT, lasting 2 minutes, and 52 seconds. The second flight started at 1:10:40PM MDT and lasted 6 minutes and 9 seconds.

With the coordinates found on the mobile devices and internal SD card we can find that the airspace used for the flights was in Arapaho and Roosevelt National Forests, Denver, Colorado. This matches the coordinate boundaries provided by VTO Inc. Using QGIS the exact paths taken by the DJI Inspire 2 were found, these can be later used as evidence.

A total of ten videos were found across all the devices involved. Four on the external SD card, five on the IOS device and one on the Android device. The shorter video `[DJI_0003.MOV]` on the external SD card was identified as the landing phase for `[DJI_0002.MOV]` resulting in a total of three full length flights recorded. Each media found on the external SD card was also found on the corresponding controller device, two full flights were found on the iPad Mini 4 and one on the Samsung Galaxy Tab A. It was also discovered that the recordings were not always in one piece, many videos were split up into separate parts.

7.2 Future Work

7.2.1 Further Investigations

With drones becoming cheaper and more capable their use in crime will definitively increase. As this is the case the research available should hopefully match this. The DJI Inspire 2 was covered in this investigation where some areas can also apply to other DJI models. For future research, other DJI drone models could be analysed to compare if the methods used for the Inspire 2 can also be used for the other models. This would create a valuable source for others that need to investigate DJI drones.

7.2.2 DAT Identifier Improvements

The DAT Identifier in its current state is a small tool with only one functionality. This could greatly be improved with a method of comparing DAT files, providing a percentage match between two or more different DAT flight logs. This could help identify which mobile device flight logs matches with which internal SD card flight logs.

Other capabilities could include putting together broken up flight logs, small flights that only contain data during landing could be synced up the other pieces to create a full flight log.

More details could be provided in the output log including if the motors were running, average speeds and maximum altitudes.

8. REFLECTION

Carrying out this investigation has provided a valuable insight on how much data and information can be realistically gathered from a single flight made via a drone. Based on the results and other individuals research into drone forensic investigations has proven how essential this topic is in 2022.

Understanding how evidence is gathered, analysed, and presented to create a story that enables a case to be concluded is essential for researching drone forensics. The methods and techniques used have provided a vast range of knowledge related to Android and IOS operating systems, geographical information systems, various forensic tools, and the component makeup of DJI drones. The creation of the DAT Identifier and use of QGIS will hopefully be of use for further investigators and investigations in the future.

REFERENCES

DroneDJ, 2021. *DroneAnalyst report reveals dramatic drop in DJI's commercial drone market share.* [online] Available at: https://dronedj.com/2021/09/14/droneanalyst-dji-market-share-2021/ [Accessed 11 May 2022]

Wikipedia, 2022. *Gatwick Airport drone incident.* [online] Available at: https://en.wikipedia.org/wiki/Gatwick_Airport_drone_incident [Accessed 12 April 2022].

The Meir Amit Intelligence and Terrorism Information Center, 2022. *ISIS's use of drones in Syria and Iraq and the threat of using them overseas to carry out terrorist attacks.* [online] Available at: https://www.terrorism-info.org.il/en/isiss-use-drones-syria-iraq-threat-using-overseas-carry-terrorist-attacks [Accessed 12 April 2022].

BBC News, 2022. *Gang who flew drones carrying drugs into prisons jailed.* [online] Available at: https://www.bbc.co.uk/news/uk-england-45980560 [Accessed 12 April 2022].

Wikipedia, 2022. *List of UAV-related incidents.* [online] Available at: https://en.wikipedia.org/wiki/List_of_UAV-related_incidents [Accessed 12 April 2022].

IEEE Spectrum, 2022. *Dutch Police Training Eagles to Take Down Drones.* [online] Available at: https://spectrum.ieee.org/dutch-police-training-eagles-to-take-down-drones [Accessed 12 April 2022].

Kao et al, 2019. *Drone Forensic Investigation: DJI Spark Drone as a Case Study.*

Bouafif et al, 2018. *Drone Forensics: Challenges and New Insights.*

Roder, Choo, Le-Khac, 2018. *Unmanned Aerial Vehicle Forensic Investigation Process: DJI Phantom 3 Drone as a Case Study.*

Clark et al, 2017. *DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom 3.*

Wikipedia, 2022. *Apple Inc.* [online] Available at: https://en.wikipedia.org/wiki/Apple_Inc [Accessed 12 April 2022].

Business of Apps, 2022. *Apple Statistics (2022).* [online] Available at: https://www.businessofapps.com/data/apple-statistics [Accessed 12 April 2022].

Apple, 2022. *Check Coverage*. [online] Available at: https://checkcoverage.apple.com/gb/en [Accessed 9 May 2022].

Wikipedia, 2022. *Android (operating system).* [online] Available at: https://en.wikipedia.org/wiki/Android_(operating_system) [Accessed 12 April 2022].

Google, 2022. *p2p_supplicant.conf - device/lge/hammerhead*. [online] Available at: https://android.googlesource.com/device/lge/hammerhead/+/bb70fbd/p2p_supplicant.conf [Accessed 9 May 2022].

Datfile, 2022. *DatCon.* [online] Available at: https://datfile.net/DatCon/intro.html [Accessed 9 May 2022].

Datfile, 2022. *CsvView.* [online] Available at: https://datfile.net/CsvView/intro.html [Accessed 9 May 2022].

Airdata UAV, 2022. *Drone Data Management and Flight Analysis.* [online] Available at: https://airdata.com [Accessed 18 April 2022].

QGIS, 2022. *Discover QGIS.* [online] Available at: https://www.qgis.org/en/site/about/index.html [Accessed 18 April 2022].

Devon Clark, 2022. *GitHub - unhcfreg/DROP: Drone Parser*. [online] Available at: https://github.com/unhcfreg/DROP [Accessed 21 April 2022].

DJI, 2022. *DJI Decrypt Tool - Download Center - DJI*. [online] Available at: https://www.dji.com/uk/downloads/softwares/dji-decrypt-tool [Accessed 21 April 2022].