

# CMT400: Drone Forensics Investigation



Joseph Garnett

GarnettJ@cardiff.ac.uk

2022

School of Computer Science and Informatics

Cardiff University

Supervisor: Dr Shancang Li

## Abstract

Commercial drones are a growing market and each year they become more accessible to the general public. As such, there has been a rise in crimes committed with said devices. This leads to the growing need for a standard forensic analysis procedure for drones. However, many of the devices available on the market have vastly different architectures. Because of this, it has proved a challenge for a standard procedure to emerge. To help with this issue, this paper will consider existing methods for three drones that are available on the market.

By researching and testing existing methods, a better understanding of drone architecture can be established and the methods themselves can be improved or new approaches identified. In this paper, each method will be tested on the device that it was established for, extracting as much evidence as possible and describing the file structures. Then, these findings will be compared to the existing methods, determining their accuracy and forensic value. Finally, any improvements that could be made to these methods will be put forward.

This is done with the primary purpose of strengthening understanding of such devices and improving the methods such that they may be used as in real-world forensic scenarios. However, it is also hoped that these results may be used in future studies as part of creating an all-encompassing methodology for the forensic analysis of drone devices.

## Acknowledgements

I would like to thank my supervisor, Dr Shancang Li for his guidance and support through each stage of this report. Without his support, this work could not have been completed.

I would also like to thank the friends and family who supported me throughout this undertaking.

# Table of Contents

Abstract.....	1
Acknowledgements.....	2
1. Introduction .....	4
1.1. Overview .....	4
1.2. Aims and Objectives.....	5
1.3. Challenges .....	7
1.4. Structure .....	7
2. Literature Review .....	9
3. Examination .....	17
3.1. Tools.....	17
3.2. File Size and Notation .....	18
3.3. Mavic Pro .....	19
3.4. DJI Inspire 2 .....	38
3.5. Parrot Bebop .....	53
4. Method Analysis.....	66
4.1. DJI Mavic Pro.....	66
4.2. DJI Inspire 2 .....	69
4.3. Parrot Bebop 2 .....	71
5. Conclusions .....	75
5.1. Challenges Faced.....	75
5.2. Reflection .....	76
5.3. Future Work .....	78
5.4. Conclusion.....	78
Bibliography .....	80

## 1. Introduction

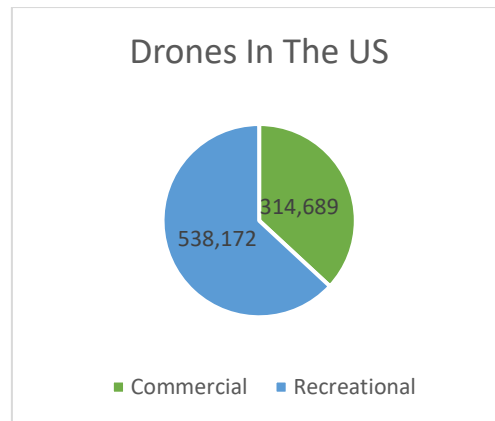
### 1.1. Overview

Drones are aerial devices or aircraft that have no on-board pilot, commonly referred to in literature as Unmanned Aerial Vehicles (UAVs). These devices have a range of purposes including delivering goods, filming, military operations and even as a method of dispensing testing kits during the COVID-19 pandemic. Commercial UAVs, models designed for the general public, have also grown in popularity over the past few years. These devices are typically remotely controlled via some form of remote controller. For commercially available devices, this tends to be a mobile device. The UAV and associated systems are often referred to as Unmanned Aircraft Systems (UAS) in literature (Florio, 2016). As popularity has increased, so too has the number of models available to the general public and this is where the problem lies. As more people have access to these devices, so too has the number of crimes relating to them and a lack of standard architecture has proved difficult for forensic analysts as each device needs to be treated differently from others.

Drone forensics itself is a branch of digital forensics which involves the recovery of digital evidence from UAV devices, under “forensically sound” conditions. This refers to data that has been collected without being altered in any form. To maintain this, investigations usually follow a set of principles, where the data is:

- Well documented, every action taken on the evidence is noted. Marking when, where and how it was used.
- Repeatable, it must be shown that the results could be repeated if the same actions were followed again.
- Consistent, the data that is found cannot be conflicting with the findings or other data.

According to the Federal Aviation Administration in the US, they have just under one million registered drones in their airspace. The distribution of these can be seen in the below figure. Commercial refers to standard drones that are being used for a purpose/task.



*Figure 1*

While these numbers are lower in the UK, due to a much lower population, there are still a considerable amount. According to (Drone Safe, 2018), there are at least 20,000 certified drone pilots in the UK. This alone establishes the importance of ensuring that these devices can be policed effectively. Another aspect to consider is their presence in mainstream media. Drones and related devices are no longer a niche hobby, due to the threat they can pose and their potential, most people are now aware of them. Most recently, the BBC reported the use of such drones in the conflict in Ukraine (Abdujalil, 2022) where they are being used to mark military targets. However, their presence is not limited to the news. Drones are now used in almost all industries. Farming, filming, construction, navigation, there are so many applications. As they receive more exposure, the more they will be used with malicious intent.

Unfortunately, there are already a number of examples of drone related crimes. They have been used to 'case' out crimes (Kelly, 2022), smuggle drugs (Davis, 2015), enter restricted airspace (Shackle, 2020), and even perform assassinations (Meitav, 2022). It would appear that the applications for crime are as numerous as applications for good. This only highlights the need for an effective way of dealing with these events.

It is for these reasons, as well as a personal interest, that the topic has been chosen for this paper.

## 1.2. Aims and Objectives

The purpose of this study is to complete an analysis of existing technologies and methodologies that can be used for the forensic analysis of UAS and complete a new

analysis using these methods. Then, propose a set of improvements that could be made to make these methods as effective as possible. In order to achieve this objective, a set of aims shall be established to inform the steps of the investigation:

- Establish the current state of drone forensics, reviewing existing methods of analysis and the tools that they use.
- Use the knowledge of these methods and tools to establish a process of data extraction to be used on their respective drones.
- Use a set of drone images that have been provided, describing the files contained and how they will be examined.
- Begin an analysis of three of these drones, using the method that was established earlier. This will be done to:
  - Establish what the file systems look like for each of the given drones and note where key information is stored.
  - Provide a similar overview of each of the associated files and images (mobile and any other files).
  - Analyse the contents recovered from this analysis, describing what they are and how they can be used.
- Compare this information with the existing method, noting any differences found, as well as the similarities.
- Discuss the effectiveness and accuracy of each method and use that to suggest any potential improvements that could be made, creating an updated method that could be used to forensically analyse these devices in a real-world scenario.
- Reflect on these findings and discuss how they could be used in the future to help create a singular method applicable to the forensic analysis of any drone.

Once each of these aims has been met, a more complete view of how to forensically examine the devices will have been established. Furthermore, a better understanding of drone forensics as a whole will be achieved and then these findings may be used to inform future works in this field.

### 1.3. Challenges

In the undertaking of this task, it is expected that a variety of challenges shall be faced. The first of which will be finding and using existing literature for the creation of methods. As there is a current lack in research on this topic, finding detailed reports will likely be a challenge. However, to get around this potential problem, websites and sources that collect research papers for easy viewing will be used. These collections allow for easy searching and navigating of related papers, reducing the time taken to find them.

As drones are complex pieces of technology, it is also assumed that navigating their file systems will be problematic. As such, tools and techniques will be researched as part of the literature review to help with this process.

Each of the drones that will be used will be different makes or models, therefore, they will likely have their own structure and methods of storing data. This is expected most in drones of different makes.

UAV systems are comprised of more than a singular part. The drone and the device used to control it are vastly different in terms of what they contain. Due to this, different approaches will be needed for each.

Organising and writing such a report will also be a difficult undertaking as there a number of variables and facets to be considered. However, through careful planning, this can be mitigated. The aims that were established above will help to guide the process of the investigation through a considered structure.

### 1.4. Structure

This paper is spilt into five clear sections. This has been done to help maintain focus and structure the findings in a way that can be easily understood. The first of these sections is this introduction. The second a literature review, third the drone examination, fourth the analysis and finally the results and conclusions.

The literature review will review existing articles surrounding the topic of drone forensics. Explaining what it is and how it is done, as well as the issues surrounding it. Then, existing studies on drones will be consulted to establish some of the key differences between them and how an analyst may approach them.



Then the examination will take three of the drones discussed in the review and apply the methods discussed. The results of the analysis will be shown and discussed.

These methods and the results will be analysed. Each of the data artifacts recovered will be compared to what the studies suggested could be recovered and the merits of using the methods will be discussed. Improvements will then be suggested in this section and how they could be worked into the method.

Finally, in the conclusion, the process that was followed in this study will be discussed. This will include the challenges that were faced, a general reflection on the study as a whole, what work could be done in the future and closing statements.

## 2. Literature Review

Since 2010 there has been rapid growth in the drone industry. Prior to this, these devices' main purpose was for military use or for hobbyists (Vyas, K). However, the market share now has an estimated value of 86 million U.S. dollars in the UK alone (Statista, 2022). This drastic growth is due to an expanding number of uses for the technology (Bouafif et al., 2018). Toys, delivery, photography and filming have all been made possible as the technology behind UAVs has improved. This, combined with easier accessibility and lower cost has helped to popularise these devices and further increase their growth in the market.

As with any new technology, rapid adoption has led to unexpected problems. According to (GOV.UK, 2019) there were 168 police recorded drone incidents across England and Wales in 2018 and this number is expected to increase in the future. While new laws and regulations are being implemented to help prevent crimes committed, there still remains the issue of analysing the contents of a device when a crime has already been committed. Unfortunately, this has remained an area that is not very well understood and lacks a concise methodology for analysis. There have been numerous crimes committed using UAVs since they were introduced where the culprit has eluded authorities due to a lack of a systematic approach for analysing the devices (Iqbal et al., 2019). Therefore, it is imperative that further research is conducted until a satisfactory solution is presented.

Completing a forensically sound analysis of UAVs and their associated devices comes with a number of challenges that have made finding a standard procedure for the task difficult:

- Drone devices can be very complex pieces of technology, sometimes having multiple file systems. This paired with the mobile devices having their own operating system, means that analysts are required to make use of multiple different tools (Kovar, 2015) some of which they may not be familiar with.
- Some models of UAV are difficult to image without risking its integrity as the provided USB connections do not allow direct connection with the physical disk (Bouafif et al., 2020). This means that connection must be established over a network which is far less reliable.

- The hardware components of UASs which make up the physical evidence for analysis are dispersed across multiple devices (the drone used in the crime, the controller). This then adds a step for analysts where they need to establish a connection between the UAV that was seized committing the crime and any remote controllers that were seized during the follow up investigation (Bouafif et al., 2018).
- When developing methods for the analysis of these devices, researchers and analysts tend to use newly bought or 'out of the box' models. While this simulates what the model should be like, it doesn't necessarily align with what it will be like. Users can edit and modify their devices given they have the correct expertise to complicate the process. As (Bouafif et al., 2020) states, flight data can be concealed, or access controlled and in (Horsman, 2016) it is mentioned that Parrot models can be obtained with a development kit which can also be used to make the process more difficult.
- Access to the remote controller for the device may be restricted through the use of an identifier (Elands et al., 2016). This can prolong the investigation, especially so if it uses a unique identifier such as biometric protection.
- Drones vary in the amount of data they log, ranging from detailed to non-existent. Furthermore, it is possible that the devices come with factory reset options, such as in the DJI applications, (Horsman, 2016) determined that such an option on the "Parrot Bebop" model does render the data unrecoverable. Either of these possibilities can lead to scenarios where a device has been seized but contains very little usable evidence in building a case.
- Due to the remote connection between controller and UAV, it is possible for GPS data to be limited, faked and even deleted. (Horsman, 2016) found that by covering a device with strips of aluminium foil, the GPS signals to and from the UAV would be blocked and the flight path would not be recorded. It is also possible to modify GPS data through the use of spoofing to fake where the controlling device is located. All of which to say that the GPS data recovered from a seized device may have been tampered with and extra steps must be taken to establish if this is the case.
- Many drones are small devices with even smaller components and due to their requirement to fly for long distances, are often very lightweight. Meaning, should

the device sustain heavy physical damage, the internal storage may become compromised.

A forensic investigation using the 'DJI Spark' drone was performed in (Kao et al., 2019). Through their analysis they found that forensically important data could be found on the SD card, internal storage, mobile controller and data transferred between controller and UAV. Their proposed methodology consists of:

- 1) Analysing the flight control system "DJI Assistant 2" to display flight data DAT files. 15 of which were recovered.
- 2) Using the CSV analysis software "CsvView 3.6.3" to convert the DAT files to CSV values.
- 3) Utilise the "DJI/dji.go.v4" folder on the mobile device to discover flight data files, including photographs, sound files and flight records.
- 4) Use "ExiftoolGUI v.5.16.0.0" (a tool to view EXIF metadata for images) to review artifacts.
- 5) Analysis was then performed on the SD card using "FTK Imager 3.1.1.8" and "ExiftoolGUI v.5.16.0.0" to identify time, size and media content of recovered files as well as numerous files from the mobile device.

The use of Wireshark as a tool to capture packets in the period of controlling a drone was also discussed. However, despite how it would provide valuable information, actively capturing traffic while the UAV is being controlled would be a substantial challenge. Results from this experiment were positive as an association between the drone and mobile device were discovered. Numerous linked files were discovered using this method which could be used to link the crime back to the suspects device. However, there were some discrepancies between the number of files found and the number that should have been present which may have been down to data loss in the transfer.

Furthermore, a study on the 'DJI Mavic Air' model (Yousef & Iqbal, 2016) proposes a similar method of acquisition while offering alternative applications and tools. This method first focuses on the internal storage of the drone and the remote air controller before moving onto the mobile device and applications. As for the tools used, FTK imager is still used to

acquire an image of the SD card and CsvView is used to parse through the DAT files. These tools appear to be of value when performing drone forensics as data acquired using them was mentioned to be of higher quality than that found through the DJI mobile applications. Regarding these applications, “DJI Assistant 2” was also reviewed again as part of another experiment. It is an application containing extra settings and utilities for DJI products such as a flight simulator that can be programmed with chosen flight data (Himmat, Y). This makes it a useful tool for simulating forensic analysis due to the various administrative features. However, the findings of (Yousef & Iqbal, 2016) suggested that the data acquired in this application is easily corruptible and therefore impractical for use in real world scenarios. Another noteworthy application is “DJI GO”, which is used to control DJI drones from a smartphone (DJI, 2022a) which the authors of the experiment were able to extract data from using Apple iTunes. This recovered a number of recorded videos from the test flight. However, they were noted to be of lower quality than those recovered directly from the SD card. The final application to note was “Autopsy”, a part of “The Sleuth Kit” that allows users to view system images and utilise various forensic tools on them.

While DJI brand drones are arguably the most common and popular available (Global Brands, 2020), there are many others. Therefore, it is also worth considering some of these options, such as those made by Parrot and Yuneec. In (Kumar & Agrawal, 2021) testing was performed on drones from DJI, Parrot and Yuneec which highlighted key differences between the models (“DJI Phantom 4 Pro”, “Parrot Bebop 2” and “Yuneec Typhoon H”). Their findings showed that the flight logs for each family of drone were stored in different formats. DJI in .DAT, Parrot in .TXT/.JSON and Yuneec in .csv. They found that the Parrot family of drone required a lot of manual processing to decipher the flight logs, resulting in the development of “FlyLog Converter Tool”. This tool parses the .TXT/.JSON files and converts them to csv similarly to how CsvView could be used on DJI models. They made this tool available to the public through a GitHub repository.

The ‘DJI Phantom 4 Pro’ model needs to be fully charged before data acquisition can take place and then powered on and connected to a computer running ‘DJI Assistant 2’ via micro-USB cable. This should allow .DAT flight logs to be accessed from the UAV’s internal SD card. Internally, when a new flight is logged, it saves the flight number as a new .DAT file and another file named “PARM.LOG” keeps track of the number of flights carried out on the

device. As with other DJI models, in order for the flight logs to be readable by a human they must be converted to csv format. This should provide enough data for an analyst to be able to recreate the flight path taken by the drone during the flight that they are investigating. Analysis of the 'DJI GO 4' application in Autopsy displayed model and owner information for this drone model.

As previously mentioned, 'Parrot Bebop 2' stores its flight logs in .TXT/.JSON as is the case for all models made by Parrot. Another difference from the DJI models to note is that the 'Parrot Bebop 2' stores its files and logs within the flash storage of the device. (Kumar & Agrawal, 2021) used the Android Debugging Bridge (ABD) tool to extract data. ABD is a command-line tool for communicating with a device, providing access to a Unix shell where a number of commands can be run on the device (Android, 2022). ABD can be run on the Bebop 2 model when the device is powered on, and the application is enabled. This then allows a command to be run which creates an image of the internal flash storage, containing the files and logs which the analyst needs. Within this image, flight logs can be found and then converted to readable format. In the case of (Kumar & Agrawal, 2021) an Android device was used, and the files were found in an "com.parrot.freeflight3" application. Once the data has been translated, flight paths, time, drone model, software information, altitude etc.... can all be extrapolated.

'Yuneec Typhoon H' has arguably the easiest process of the three UAVs considered during their investigation as Yuneec stores flight logs in csv format on the device, which is already human readable, requiring no translation step once it has been extracted. Just like 'Parrot Bebop 2', the important logs and files are stored in the flash storage. This should be accessible through the use of USB connection between drone and computer, allowing for imaging on the computer. Once access has been gained, the relevant data can be found. According to (Salamh et al., 2019), this is a relatively straightforward process as all that is needed is to find the data and view or extract it via the help of software such as Autopsy. For example, all videos can be found in the "DCIM" folder. Furthermore, the file containing flight information is named "FlightLog". Thanks to this and to the data not being encrypted, it is relatively easy to find the flight data that is required to plot a flight path that was undertaken by the device.

While Parrot left the 'toy-drone' market in 2019 (O'Kane, 2019), their previous models still exist and are available for anyone prepared to look for them. Because of this, there is still every possibility that a person committing a criminal act could use one of these devices. Therefore, it is still important to make sure that forensically sound analysis methods and tools are established for device from this manufacturer.

In (Yousef et al., 2020) another study on emerging DJI models was performed. Namely, the 'DJI Mavic 2 Pro', 'DJI Mavic Air', 'DJI Spark' and 'DJI Phantom 4'. This study followed a singular investigation method for each of the chosen devices and then discusses the varying data that is extracted from each. The proposed method is as follows:

1. Establishing the testing environment by formatting the devices memories and restoring them to their factory settings using the two DJI applications discussed in other pieces of literature and then conducting new test flights to establish sample data to use within the experiment.
2. Using 'Apple iTunes' to acquire an iOS backup and using 'FTK imager' to recover a physical image of the external SD cards for each of the drones while powered off.
3. Access the internal memories of the 'Mavic 2 Pro' and 'Mavic Air' models by establishing a USB connection between them and the forensic workstation while the devices are powered on and once again using 'FTK imager'.
4. Extract a logical back-up of the mobile device used in the experiment (iPhone 6) using Apple iTunes once again for its backup utility. Relevant files were found in the folder path "~/Library/Application Support/MobileSync/Backup" on the Mac OS for their experiment.
5. Analysis of DJI GO 4 application using Apple iTunes and viewing the various packages of the DJI Assistant 2 software.

Using this method, Yousef et al. were able to recover a significant amount of data from each of the models. Media files were recovered from the 'Mavic Air' and 'Mavic 2 Pro' in a folder named "/DCIM/100MEDIA". The files found here consisted of JPEGs and MP4s which had a 4-digit naming scheme which related to the time of creation, with the prefix 'DJI'. Like the previously discussed study, these files can also be found through analysis of DJI's mobile application. However, at a lower quality. EXIF data embedded inside the recovered JPEGs can be viewed using Autopsy and contain metadata about the image such as date, file

source and GPS relating to when and where the images were taken. According to the study, the UAV's serial number, country code, machine platform and the email address used to log in during the flight can be recovered from the logical back up of the mobile device. This was located in a folder with the name "com.dji.go.plist" after parsing. The files recovered from 'DJI Assistant 2' and 'DJI GO 4' are in .dat format and CsvView was recommended for decoding them. However, only the 'DJI Assistant 2' DJI Spark files could be decoded this way in the study. These files contain flight data that could be used to recreate a flight path.

According to (Bader & Baggili, 2010), while iTunes was not designed for forensic examinations, the application can be used to retrieve enough data to consider using it for such investigations. Due to this, it is a worthwhile tool to use in the field of drone forensics as it is simple to understand and use. Allowing analysts to collect the data that is needed to perform an analysis without relying on specialist equipment or tools.

Details for many common models of UAV can be found in (Marcella, 2021). It contains a large amount of information about what can be found on UAV devices, where, how to access it and risks that should be considered when extracting data from the devices. The chapter focuses on DJI models and contains some information about devices that are not commonly discussed in other available papers. Most worth noting are 'DJI Inspire 2' and 'MATRICE 600 PRO', which despite their popularity, are lacking in available studies.

The Inspire 2 model uses the standard .DAT file format common amongst DJI devices and lacks encryption. This allows tools such as csvView and DatCon to access and visualise important files. These files contain flight logs and general diagnostic data from each time the device has been turned on. This data is found on the onboard SD that is found in the device's camera. Flight records for the device are stored in the format "DJIFlightRecord\_[DATE].txt", which is similar to most DJI models. An exception that the study noted was the 'Mavic Mini' model which uses the format "field\_flight.txt". However, according to a study in 2021 (Stanković et al., 2021), the later 'Mavic Mini' models revert back to the standard naming scheme. In regard to the Inspire 2 model, once the SD card has been extracted an examiner can image it using the tools and techniques already discussed.

The 'Matrice 600 Pro' is DJI's largest model of UAV (DJI, 2022). Unfortunately, there is not a lot of available forensic data for the device (likely due to it being discontinued). The study



does note that it shares a lot of similarities with other DJI models. It was also noted that controller data for the device is stored in the internal memory until powered off. Therefore, a logical extraction needs to be made while the device is powered on. This is not a unique process to this UAV. If possible, it should be attempted with any seized device so as to preserve as much data as possible (Kostadinov, 2019).

### 3. Examination

In order to determine how accurate the information presented during the literature review is, individual testing of these methods and devices must be undertaken. This section of the report will focus on three types of drones to perform an analysis on. Using the provided images of the UAV and associated mobile device, each will be compared and contrasted to previous works to determine whether files and evidence are located are the same. Then, a conclusion can be made on how effective methods of data acquisition are and if any improvements can be made.

For the purposes of the project, three of these shall be selected for analysis. The number three was chosen to provide a balance between feasibility and varied results. The devices selected for this study are the 'DJI Mavic Pro', 'DJI Inspire 2', and 'Parrot Bebop'. As discussed in the literature, DJI controls almost 70% of the market for commercial drones. Two of their devices have been chosen for this paper to represent this. Due to their control of the market, it is likely for any given device that is seized to be manufactured by DJI and it is therefore valuable for these devices to be covered. Firstly, the 'Mavic Pro' model was chosen for its popularity. According to statistics released by Aloft, one of the market leaders for drone airspace systems and technologies (Aloft, 2022), this model is by far their most commonly sold. Apparently making up for 21.83% of their DJI sales (Ziering, 2018). For a second DJI model, 'DJI Inspire 2' was chosen because of its popularity with many users to this day. Parrot was chosen as a second manufacturer over others because there were more available studies on Parrot devices than manufacturers like Yuneec and the difference in market share between the two is fairly negligible. The study performed by Kumar and Agrawal in 2021 was by far the most extensive one found for Parrot drones and therefore offered good opportunities for comparison. Due to this, the 'Parrot Bebop 2' was selected over other models like the Anafi which is one of their most popular (Taylor, 2022) but lacks available studies.

#### 3.1. Tools

A number of tools and resources will be utilised for. These are as follows:

**Autopsy version 4.19.3** – A digital forensics platform and graphical interface to ‘The Sleuth Kit’ and other digital tools (Autopsy, 2022). This tool shall be used for the viewing and analysis of the provided images.

**Google Drive** – The platform which the files were shared and downloaded from.

**VTO Labs** – The drone data used in this experiment was originally provided by VTO Labs (VTO Labs, 2022). VTO are an organisation that are focused on drone forensic research and as part of their ‘Drone Forensics Program’, released a number of data sets hosted by the National Institute of Standards and Technology (NIST). These datasets contain salted data with which testers can verify locations of important files without access to the physical devices. Likewise, that is how they will be used within this study.

**DatCon version 4.2.3** – An application capable of reading .DAT files and outputting the data held within in a readable format (DatCon, 2021). This will be used on the flight log files recovered from the DJI devices to recover the data held within.

**SWF File Player** – A tool for playing video files with the .swf file extension. This file format can be found on the devices to be analysed and requires special software to be played.

**Google Earth** – Google Earth is a web tool or ‘Geobrowser’ that uses satellite imagery to display a virtual globe. It can be used to find and plot coordinates anywhere in the world. This functionality will be used to recreate flight paths recovered from the images.

**Parrot Drone Flight Log Converter v1.1** – This was the tool developed by Kumar and Agrawal in their 2021 study. It is capable of reading the .txt and .JSON files produced by the Parrot Bebop 2 and Parrot Anafi respectively and convert them into an easier to read .csv file. In this study, it will be used to read the flight logs recovered from the Bebop 2.

### 3.2. File Size and Notation

Due to the size of the files that needed to be downloaded, maintaining the folder structure was impossible. While every file still exists, the images were required to be compressed into .001 files themselves to allow them to be downloaded and that is why in the below figures they are outside of the zip file. All the files are intact, complete and forensically sound. They are just displayed differently to how they are originally.

Each of the associated files for the drones contains three datasets, denoted by an identifier. That being “df” followed by three numerical values. These datasets contain slightly different versions of the same drone, where values for dates or GPS coordinates have been changed. As well as containing different media data All three datasets will be tested during the analysis.

### 3.3. Mavic Pro

DJI released this model of drone in late 2016 and has since risen to one of their bestselling devices. The files provided for the ‘Mavic Pro’ are as shown in Figure 2.






	SDCard_External-003.001		05/08/2022 17:45	001 File	15,646,720 ...
	df019_external_microSD-004.001		05/08/2022 17:44	001 File	15,558,144 ...
	df020_external_microSD-009.001		05/08/2022 17:44	001 File	15,558,144 ...
	df021_external_microSD-007.001		05/08/2022 17:44	001 File	15,558,144 ...
	df019_flight_android_physical-005.001		05/08/2022 16:21	001 File	5,165,056 KB
	df020_flight_android_physical-008.001		05/08/2022 16:21	001 File	5,165,056 KB
	df021_flight_android_physical-010.001		05/08/2022 16:21	001 File	5,165,056 KB
	intact_sdcard_internal-006.001		05/08/2022 16:02	001 File	3,872,225 KB
	SDCard_Internal_Intact-002.001		05/08/2022 16:02	001 File	3,872,225 KB
	DJI_Mavic_Pro-20220805T133806Z-001		06/08/2022 16:43	Compressed (zipp...	0 KB
	DJI_Mavic_Pro-20220805T133806Z-011		06/08/2022 16:43	Compressed (zipp...	0 KB

Figure 2

The three different datasets for The Mavic Pro are 019, 020 and 021. Within the ‘DJI\_Mavic\_Pro’ folders lie three more files, one for each of the datasets (Figure 3). Then, within 019 and 020, there are two files: ‘August\_2017’ and ‘June\_2018’. 021 only contains a file for August. Each of these contains at least three files which house the images (Figure 4). Those being Android images, IOS backups and an image of the SD card. The exception to this is 020, where there is no IOS file and instead two SD card images (internal and external) and an export from DJI Assistant. Contained within the folders are also a number of txt files titled “README” followed by an identifier to distinguish. Finally, there are also .md5 and .sha1 (Figure 5) files for the images and txt files to validate that their integrity has been maintained while they are being examined.

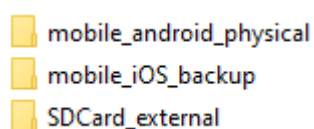


Figure 4

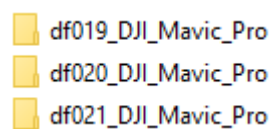


Figure 3

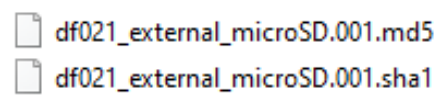


Figure 5

### *3.3.1. Method*

The method used to analyse these files is based upon the method proposed in (Yousef et al., 2020). While a 'DJI Mavic 2 Pro' was used for their study, the difference between the two models is small as it is just an upgraded version of the Mavic Pro. It will also be worthwhile to determine whether the same analysis techniques are transferable between the two models. This method will be performed on all of the datasets.

- Firstly, SHA1 and MD5 values will be used to validate the files in Autopsy.
- The internal memory images (SD card) will be reviewed with the primary aim of locating recorded media files (JPEG and MP4).
- Use EXIF data from the JPEG images to determine when and where the photos were taken.
- Analyse the contents of both iOS backups and Android images to find relevant data on the drone model and flight logs.
- Review the 'DJI Assistant' export data and decrypt them if necessary.
- Analyse any extra files and locations to determine whether there is more forensically important data available on any of the devices.
- Use this to recreate the flight path taken by the drone and compare with the values shown on the .txt files.
- Finally, the hash files will be used to ensure that data has not been edited on any of the files during the process of the investigation.

### *3.3.2. Hash Generation*

Each of the images that were provided came with hash values located within the README txt files (Figure 6) that can be used for each of the file. They contain details about each file, including name and size (Figure 7) and have unique MD5 and SHA1 values.



Figure 6

```

Filename: df020_external_microSD.001
Size: 15,931,539,456
MD5: 04bdb53daa784bc210354f5bcbf270f7
SHA1: d9334ed9dc418533429bb281e20b6e4261067704
Released: 2017-09-03

```

Figure 7

When creating the case in Autopsy and choosing a data source, there are optional text entries where these associated hashes can be added (Figure 8).

Hash Values (optional):	
MD5:	<input type="text" value="04bdb53daa784bc210354f5bcbf270f7"/>
SHA-1:	<input type="text" value="d9334ed9dc418533429bb281e20b6e4261067704"/>

Figure 8

Using such values allows each of the data sources to be verified individually. Throughout the investigation, Autopsy will calculate a given hash for each dataset, based on the file, and compare this file against the one that has been given (SleuthKit, 2022). If the two values are the same, then the data source has not been edited.

### 3.3.3. SD Card Analysis

The first set of images to view are the SD cards of each dataset. To do this, a case was made in Autopsy and each of the images were added (Figure 9). Each of these sources contains a number of files and folders.

df019_external_microSD-004.001_548 Host
df020_external_microSD-009.001_632 Host
df021_external_microSD-007.001_721 Host
intact_sdcard_internal-006.001_1 Host
SDCard_External-003.001_455 Host
SDCard_Internal_Intact-002.001_231 Host

Figure 9

Each of the ‘external’ SD card images contains two volumes of data. The first of which spans sectors 0 – 8192 and appears to be unallocated. This is true for each of the images. The second volume in each of the sources that begin with “df” contain seven items (Figure 10). The only difference between them at this level is the number of files inside the “\$Unalloc” folder. The remaining external SD card image contains an extra file titled “System Volume Information” which is used to determine system settings should the system be rebooted.

\$OrphanFiles			0000-00-00 00:00:00
\$FAT1	1		0000-00-00 00:00:00
\$FAT2	1		0000-00-00 00:00:00
\$MBR	1		0000-00-00 00:00:00
\$Unalloc			0000-00-00 00:00:00
DCIM			2017-05-26 13:24:48 BST
MISC			2017-05-26 13:24:48 BST

Figure 10

The internal images contain data and files that vary drastically from the external images. Most notably, they contain a number of DAT files which appear to be flight logs for the device. The two also have slightly different folders within them when compared to the external ones as well as each other. The contents of ‘006’ can be seen in Figure 11 and ‘002’ is shown in Figure 12. The carved files are files which have been ‘carved’ from unallocated space on the device.

intact_sdcard_internal-006.001_1 Host
intact_sdcard_internal-006.001
\$OrphanFiles (0)
\$CarvedFiles (36)
\$Unalloc (3)

Figure 11

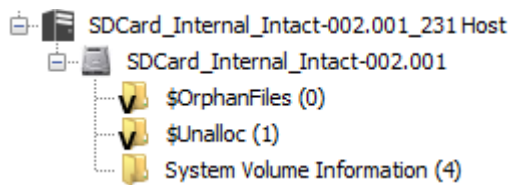


Figure 12

#### 3.3.4. DCIM Folder

According to the literature, many of the DJI devices store recorded media in a folder named 'DCIM'. This is a folder common to many different camera bearing devices. This naming scheme is defined as part of the Design Rule for Camera File Systems (DCF) specifications which are a set of standards many camera makers have adopted (Fisher, 2022). DCIM itself stands for 'Digital Camera Images' and contains all media files captured by the camera.

In the case of the Mavic Pro, this file is located on each of the external images. For each of the images, this contains another folder named "100MEDIA" which itself contains the various image and video files recorded by the device. An example of the file pathing can be seen in Figure 13 below.

`/img_SDCard_External-003.001/vol_vol2/DCIM/100MEDIA`

Figure 13

Between all four of the images that contained media; four .JPG images, fourteen .MOV videos and two carved .SWF videos were located. The image files and their locations are displayed in figures 14 and 15. Similarly some of the video files are displayed in figures 16 and 17. JPG and MOV files are standard file extension formats for image and video files respectively, with MOV being a video format developed by Apple. SWF files are an Adobe Flash format containing videos and vector-based animations (VideoStudio, 2022) which may contain interactive content. Unfortunately, since this format relies on Adobe Flash Player, which is now defunct, analysing the contents of the video may prove harmful to an analyst's device.



Name	S	C	O	Modified Time	Location
DJI_0004.JPG			0	2018-06-21 14:53:54 BST	/img_SDCard_External-003.001/vol_vol2/DCIM/100MEDIA/.
DJI_0002.JPG			0	2017-08-29 12:27:08 BST	/img_df020_external_microSD-009.001/vol_vol2/DCIM/100.
DJI_0003.JPG			0	2017-08-29 12:27:18 BST	/img_df020_external_microSD-009.001/vol_vol2/DCIM/100.
DJI_0005.JPG			1	2017-08-29 13:00:04 BST	/img_df021_external_microSD-007.001/vol_vol2/DCIM/100.

Figure 14

Figure 15

Name	S	C	O	Modified Time	Location
f0658287.swf		▼	1	0000-00-00 00:00:00	/img_intact_sdcard_internal-006.001/.\$CarvedFiles/f0658...
f0658287.swf		▼	1	0000-00-00 00:00:00	/img_intact_sdcard_internal-006.001/.\$CarvedFiles/f0658...
DJI_0001.MOV		▼	0	2018-06-19 18:55:36 BST	/img_SDCard_External-003.001/vol_vol2/DCIM/100MEDIA/...
DJI_0002.MOV		▼	0	2018-06-21 11:14:50 BST	/img_SDCard_External-003.001/vol_vol2/DCIM/100MEDIA/...
DJI_0003.MOV			0	2018-06-21 14:53:46 BST	/img_SDCard_External-003.001/vol_vol2/DCIM/100MEDIA/...

Figure 16

Figure 17

The photos appear to be images captured by the drone during a flight as three of the four consist of elevated shots of field land and markers. The final image appears to be a photograph taken of the researchers who piloted the drone. The video files contain similar content, consisting of short flight recordings or captures taken while the device is hovering in place. The landscape across all the media files remains relatively consistent and suggests that all the recordings were taken in the same area.

After attempts to analyse the contents of the SWF files, it would appear they are remnants of video files which did not save properly or became corrupted. This would seem to be the case as none of the contents for this file could be recovered or viewed. However, this may also be due to the unfamiliar file format and lack of software capable of reading it. The tool ‘SWF File Player’ was used to open and play the content, but nothing was recognised.

### 3.3.5. Image Data

Autopsy provides a number of different ways of analysing content found on an image, including file hex values and text as well as meta data and analysis (Figure 18).

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

Figure 18

The application tab shows the file as it is intended to be viewed, an image. For example, the image “DJI\_0003.JPG” is displayed in Figure 19 below. Neither the hex nor text tabs are particularly relevant for this investigation as all the information they contain can be found in the other tabs (date and image information). Viewing the file metadata, the timestamps of when the image was created, modified time, access time and changed time can be seen as well as size and hash values. Most importantly however, the GPS coordinates from when the image was taken can be viewed under ‘Analysis Results’. The displayed coordinates of “DJI\_0004.JPG” are shown in Figure 20. It is also possible to view this information by extracting the image from Autopsy and viewing its properties through a file explorer (Figure 21). However, these values are not the same as those displayed in Autopsy and, when compared to the given flight coordinates, appear to be less accurate or listed in a different format. Details about the camera the drone used can also be viewed in this way (dimensions, model, focal length and other technical details). For example, the camera model that is listed ‘fc220’ is the camera model for the Mavic Pro.



Figure 19

Analysis Result 1	
Score:	Not Notable
Type:	EXIF Metadata
Configuration:	
Conclusion:	
Altitude:	2510.613
Date Created:	2018-06-21 14:53:53 BST
Device Make:	DJI
Device Model:	FC220
Latitude:	39.96120180555556
Longitude:	-106.21647752777778

Figure 20

GPS	
Latitude	39; 57; 40.32649999999957...
Longitude	106; 12; 59.3191000000022...
Altitude	2510.613

Figure 21

The data recovered from the four images is displayed in the table below.

	DJI_0004.JPG	DJI_0002.JPG	DJI_0003.JPG	DJI_0005.JPG
Image	SDCard_External-0003.001	df020	df020	df021
Date Created (BST)	2018-06-21 14:53:53	2017-08-29 12:27:09	2017-08-29 12:27:19	2017-08-29 13:00:04
Latitude	39.96120180555556	39.96489022222222	39.964900472222226	39.960807833333334
Longitude	-106.2164775277778	-106.21823922222222	-106.2182275277778	-106.21696722222222

Table 1

The location of these coordinates is roughly as shown in Figure 22. This image was produced at (<https://www.findlatitudeandlongitude.com/l/39+N+106+W/3166882/>), with coordinates 39, -106. The displayed location is near VTO Labs' location in Colorado. Therefore, it can be said that this is the general location which the images were captured.

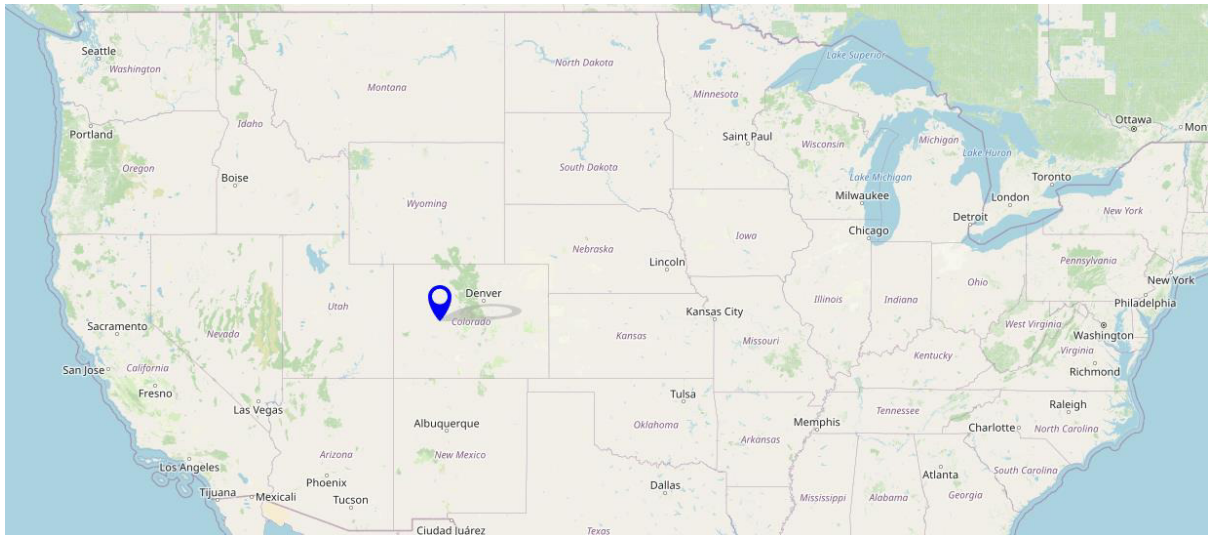


Figure 22

These values appear to be accurate when compared to the values provided in the text files. As an example, the salted coordinates for the flight saved in dataset 020 (Figure 23) are within the established boundaries. This is applicable to the coordinates recovered from each of the images which implies accuracy within this technique. While this is valuable information, a concrete flight path could not be recreated from this information alone unless a considerable number of photos were taken at regular intervals of a flight. For example, no photographs were recovered from dataset 019 and therefore no information can be garnered from viewing EXIF data. Therefore, it would be necessary to use the flight logs to recreate a path and then match this against the images.

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

Figure 23

There are a number of uses for the data that can be recovered from the images and EXIF data:

- Comparing the camera specifications of the recovered images against those of the seized drone
- Determining the GPS coordinates that the images were taken
- Any incriminating content in any of the photographs that were taken

- Determining whether the photographs were taken at the time of the suspected incident and if they have been edited in any way

### 3.3.6. Android Images

A new case was created in Autopsy titled “MavicAndroid” to view the three Android images. Each of the images were added to the case as data sources. Each of the file systems has an identical file structure. The files on the Android device are depicted in Figure 24.

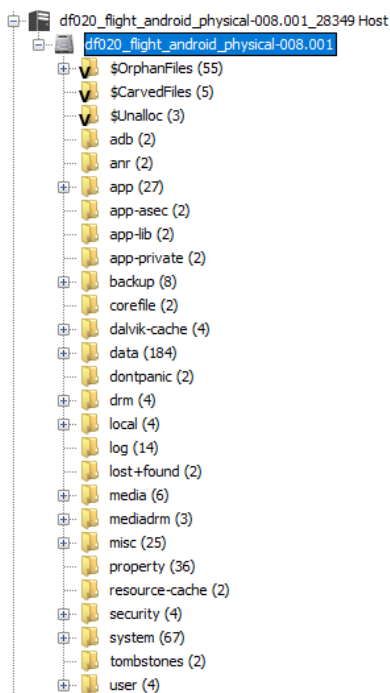


Figure 24

Each of the images contains these files. However, the contents vary slightly between the images. As an example, in df020's (as shown above) there are 27 items within the 'app' folder, whereas, in df019 there are only 21. This difference has no forensic importance as the location of important files remains the same regardless of the number of items within each file. There are a large number of files present on the device, many of which have no relation to the drone. For the purposes of this analysis, only those which are directly related to the drone and its operation will be discussed.

The first of the relevant files can be found within the app folder. This lists a number of files for different apps installed on the device. The last of these apps is “dji.go.v4-1”. It contains a number of .SO files which contain program functions and logic that the DJI application requires in order to run. The second location is within the data folder, where app data for

DJI Go is stored. Most of the data stored here appears to be configuration information about the drone, such as logs and regional data. However, there are some pieces of evidence that may be valuable. Within the DJI Go folder an array of crash reports can be accessed from flights the linked device has undertaken (Figure 25). This could be used to explain how a device came to be damaged. There are also details on the user that can be found. User ID and the user profile picture were both found here (figures 26 – 27).

Name	S	C	O	Modified Time	Change Time
[parent folder]				2017-08-29 19:45:13 BST	2017-08-29 19:45:13 BST
[current folder]				2017-08-25 18:01:08 BST	2017-08-25 18:01:08 BST
1004			2	2017-08-29 19:46:43 BST	2017-08-29 19:46:43 BST
1002			2	2017-08-29 19:46:43 BST	2017-08-29 19:46:43 BST

Figure 25

Name	S	C	O	Modified Time
uniqueUserId.txt			1	2017-08-30 16:38:09 BST

Figure 26

Name	S
user_avatar.png	

Figure 27

The most valuable data that was found on the Android images is located within the media folder. Flight records, recordings and images are all saved here. The DJI application used on this device created a folder here named “DJI” which stores the content sent from the drone. This is where the three images differ slightly, each of the images contain a folder named “dji.go.v4” but the ‘020’ image has an extra folder named “dji.pilot”. These files maintain a similar structure, with a few different files (figures 28 and 29) but they appear to store the same sorts of data. The flight logs displayed in figures 30 and 31 were taken from the ‘020’ image, one from each folder. As the figures show, the logs are for different flights. As with

the SD card images, the content of these flight records is encrypted. The final image also contained an extra folder in flight logs which had a .DAT version of the flight record in addition to a txt file.

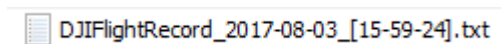
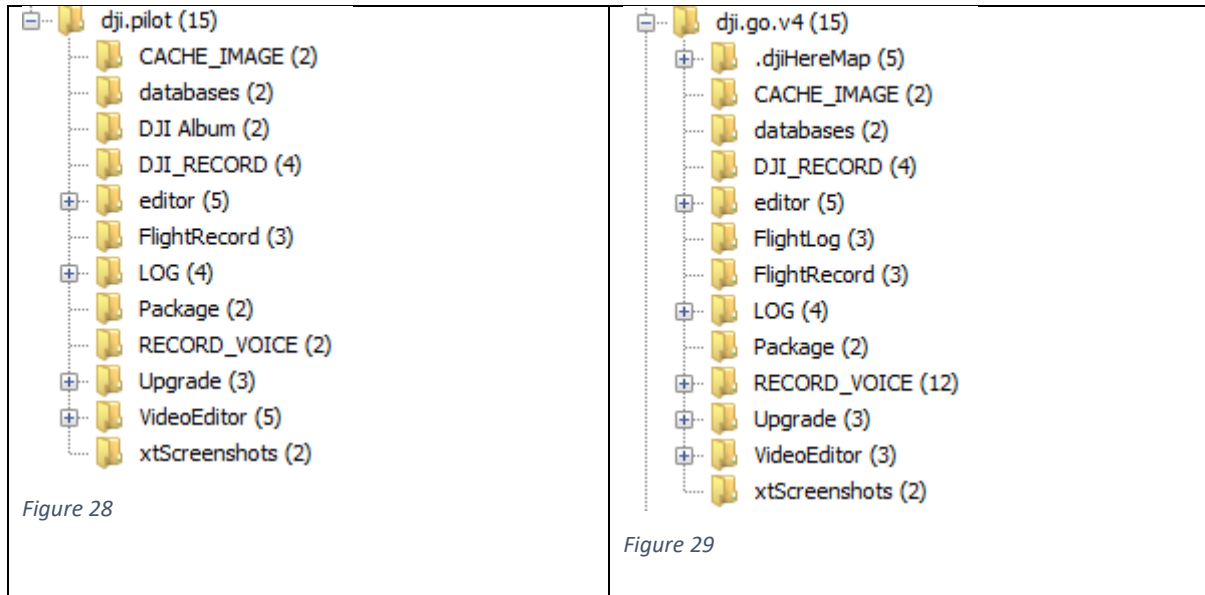


Figure 30

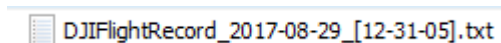


Figure 31

By feeding these txt files into an online converter (PhantomHelp, 2022). These txt files were decrypted. The results are shown in Figure 32.

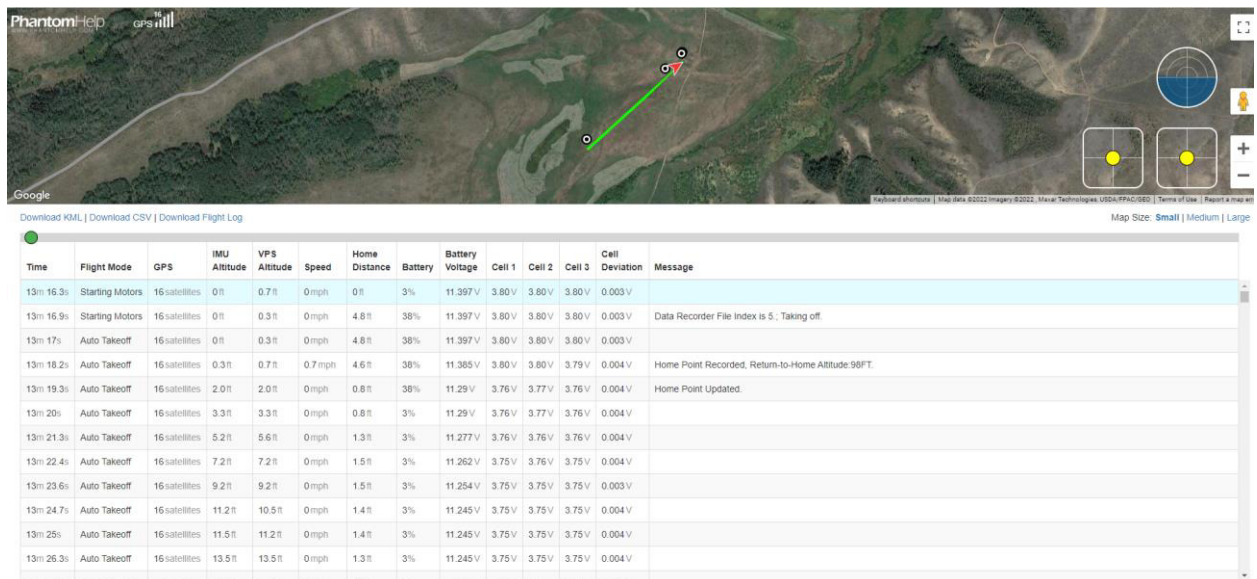


Figure 32

According to the figure, the drone flew just over 1,000 ft from its start location and then turned around and followed the same path backwards. When the flight location was compared to the one displayed in Figure 22, they were found to be in roughly the same area (Figure 33). This suggests that the flight data stored in the Android device is accurate. However, the flight log files found as part of the Android image were harder to locate than those found in the SD card.



Figure 33

As previously mentioned, images and flight recordings can also be found within the media folder. Each of the media files found here matched files found in the analysis of the SD card images. However, they were of noticeable lower quality. It appears that detail was lost in the data transfer between the drone and mobile device. It is possible that packets of data were lost due to an unstable connection. Each of these files are once again stored in the sub-folder for DJI Go. Video recordings were found in the path file shown in Figure 34. They could also be found in the dji.pilot folder, still under DJI\_RECORD. Images were found under



the file path shown in Figure 35. However, only two images were recovered during this process.

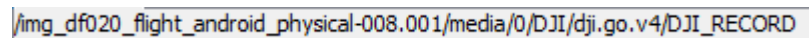


Figure 34

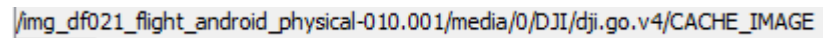


Figure 35

Nothing else of note was recovered from these images.

### 3.3.7. IOS Backups

The IOS backups that were used for this analysis were recovered using iTunes' backup feature. When a backup is created this way, the file names are encoded in a SHA-1 hash (Fitzpatrick, 2022). This process renders the names of the files indecipherable, a seemingly random string of letters and numbers. However, these strings do follow a set of rules and tend to be the same between different backups. For example, it is known that the SMS database is stored under the backup file name "3d0d7e5fb2ce288813306e4d4636395e047a3d28". Knowing this, it is possible to find the location of known key files.

For the Mavic Pro, four backups were provided. The contents of each of the backups are similar to each other. They consist of a number of folders, each with a name two-digit hexadecimal number, three PLIST files and one database manifest. The contents of each folder correspond to the hexadecimal numbering e.g., for the folder "ec", all of the files within will start with those characters. Figure 36 shows the previously discussed SMS database file.

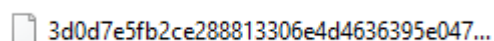


Figure 36

In (Yousef et al., 2020) they found that a file named "com.dji.go.plist" was stored in a backup as "47e664a75e84bdd13572bfc258139304fba32b96". Through navigating the backups in this study, this file was found (Figure 37). Suggesting that the backups provided

used this application. Another file was found at this location, suggesting it was possibly related (Figure 38).

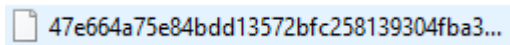


Figure 37

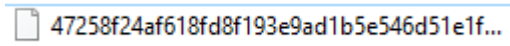


Figure 38

Unfortunately, the tools that were recommended as part of Yousef et al.'s study proved ineffective at recovering data. This may be due to them requiring a MAC OS to run. Regardless, by following their method, no further data could be recovered from the IOS backups.

### 3.3.8. DJI Assistant Export

The exported data from DJI Assistant came in the form of two compressed zip folders. The files found within this folder follow the same structure and naming scheme. A number of text files containing encrypted data of DAT formatting. Figure 39 displays the content recovered from dataset 019.

cp_assert	✓	24/08/2022 11:41	Text Document	16 KB
crash_counter	✓	24/08/2022 11:41	Text Document	1 KB
fatal	✓	24/08/2022 11:41	Text Document	59,224 KB
fatal.log.1	✓	24/08/2022 11:41	1 File	65,537 KB
kernel00	✓	24/08/2022 11:41	Text Document	1,715 KB
kernel01	✓	24/08/2022 11:41	Text Document	2,049 KB
kernel02	✓	24/08/2022 11:41	Text Document	2,079 KB
kernel03	✓	24/08/2022 11:41	Text Document	2,086 KB
kernel04	✓	24/08/2022 11:41	Text Document	2,049 KB
kernel05	✓	24/08/2022 11:41	Text Document	2,049 KB
upgrade00	✓	24/08/2022 11:41	Text Document	936 KB
upgrade01	✓	24/08/2022 11:41	Text Document	2,475 KB
upgrade02	✓	24/08/2022 11:41	Text Document	2,086 KB
upgrade03	✓	24/08/2022 11:41	Text Document	2,151 KB
upgrade04	✓	24/08/2022 11:41	Text Document	2,761 KB
upgrade05	✓	24/08/2022 11:41	Text Document	13,450 KB
upgrade06	✓	24/08/2022 11:41	Text Document	2,263 KB
wifi00	✓	24/08/2022 11:41	Text Document	1,685 KB
wifi01	✓	24/08/2022 11:41	Text Document	2,059 KB
wifi02	✓	24/08/2022 11:41	Text Document	2,115 KB
wifi03	✓	24/08/2022 11:41	Text Document	2,094 KB
wifi04	✓	24/08/2022 11:41	Text Document	2,110 KB
wifi05	✓	24/08/2022 11:41	Text Document	2,097 KB
wifi06	✓	24/08/2022 11:41	Text Document	2,121 KB
wifi07	✓	24/08/2022 11:41	Text Document	2,098 KB
wifi08	✓	24/08/2022 11:41	Text Document	2,082 KB

Figure 39

As the files were encrypted, they needed to be passed through DatCon. However, as they were stored as text files the program cannot convert them into readable CSV. In order to convert the files, they were opened and saved with the extension.dat. This resulted in a copy of the data that could be used by the application. These files were saved in a new folder where they would not affect the originals (Figure 40).

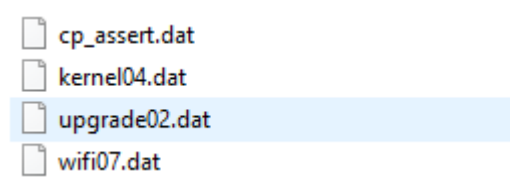


Figure 40

Then, using DatCon, the files could be selected, and a CSV file created (Figure41). The resulting .csv file would be output next to the original (Figure42).

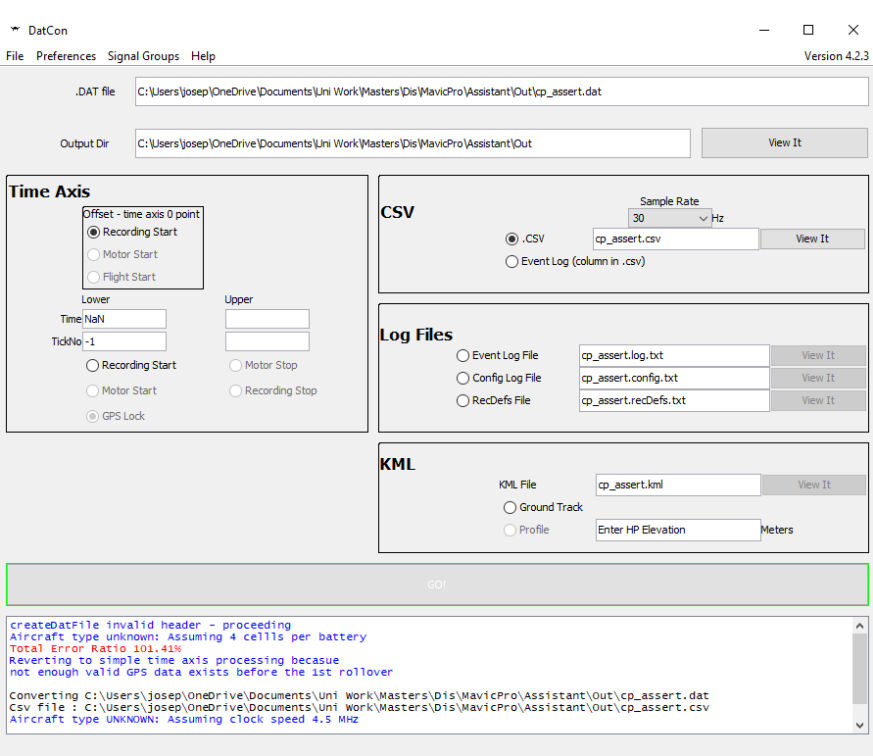


Figure 41

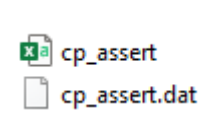
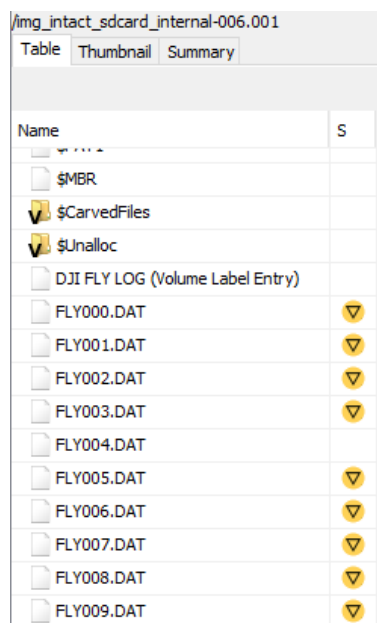


Figure 42

Unfortunately, the data recovered from these files was not of much use. Information regarding the number of crashes and the time which they occurred could be recovered. However, much of the contents appear to be encrypted and a key would be required to access all of the data that the application stores.

### 3.3.9. Flight Logs

As was discussed when observing the SD card images, a number of flight logs were found. The logs found within the first internal image can be seen in Figure 43. These files came in a natural .DAT format and could be extracted from the image using Autopsy. These files can then be converted into readable CSV using DatCon. Between the two images, over fifty records were located. Files from both the internal images were then exported in order to recreate a flight path.



The screenshot shows the Autopsy file browser interface. At the top, the path is '/img\_intact\_sdcard\_internal-006.001'. Below the path are three tabs: 'Table', 'Thumbnail', and 'Summary'. The 'Table' tab is selected. The table has two columns: 'Name' and 'Size'. The 'Name' column lists various files and folders, including '\$MBR', '\$CarvedFiles', '\$Unalloc', 'DJI FLY LOG (Volume Label Entry)', and a series of 'FLY000.DAT' through 'FLY009.DAT' files. The 'Size' column shows the size of each file, with most files being 0 bytes. The 'FLY000.DAT' through 'FLY009.DAT' files have a yellow triangle icon next to them, indicating they are selected or highlighted.

Name	Size
\$MBR	0
\$CarvedFiles	0
\$Unalloc	0
DJI FLY LOG (Volume Label Entry)	0
FLY000.DAT	0
FLY001.DAT	0
FLY002.DAT	0
FLY003.DAT	0
FLY004.DAT	0
FLY005.DAT	0
FLY006.DAT	0
FLY007.DAT	0
FLY008.DAT	0
FLY009.DAT	0

Figure 43

Once exported, the files become accessible in Autopsy's export folder for the created case. These DAT files can then be inputted into DatCon, resulting in readable flight logs in .csv format. In the case of this study, these files were then viewed using Microsoft Excel. The flight logs contain large quantities of data regarding:

- Clock Tick and Offset
- Altitude and Gyro Calculations from the IMU (Inertial Measurement Unit)
- GPS Data

- Controller and RC information
- Calibrations
- Battery Status
- Motor Status
- Air Speed

All of these values are calculated and stored regularly during a flight, resulting in thousands of values being recorded for even short flights. In order to recreate a flight path from this data, two columns are needed. "GPS:Long" and "GPS:Lat". They are stored in columns BV and BW. These values were then entered into Google Earth, resulting in a flight path. Due to the sheer volume of entries stored in the flight log, values were taken at intervals. The first log, "FLY002.DAT" was taken from the image "intact\_sdcard\_internal-006.001". Once the file was converted, the GPS coordinates were entered, and the flight path was recreated (Figure 44). The first and final coordinates were taken first and then points were plotted between them.

This flight appears to be 'point-to-point', from the top of one building to another. These buildings are the VTO Labs' listed location for their headquarters in the US. This would imply that the recovered data is correct.



Figure 44

Figure 45 shows the flight path of the second flight log that was extracted, “FLY005.DAT”. This was recovered from the second internal SD image. Again, this was a short flight that went from a start point to an end point in a line. The location of this flight appears to match with some of the images and recordings that were captured by the device in flight.



Figure 45

Both of the flights also matched with the coordinates that were salted onto the drones by VTO Labs and displayed in the txt files that were provided. While analysing the various flights, it appears that some of the logs were either corrupted or records of the device being powered on as they contained null values for many of the attributes. For example, “FLY010.DAT” had values of 0 for Latitude and Longitude when it was converted to CSV. However, a number of usable records were present.

#### 3.3.10. Validity

Once the investigation was complete, each of the images were checked in Autopsy to ensure that there were no integrity errors. For each image, the hash values calculated remained the same as the ones that were given for each of the images.

#### 3.3.11. Summary

The analysis of the Mavic Pro resulted in the recovery of images, videos, flight logs and system data. The analysis of which could place the drones’ location at the time of flight and of recording said media. An accurate flight path could be recreated that was backed up by this evidence. By viewing the contents of the Android and IOS devices, a connection between them and the drone could be established. Details about the drone and device

could also be found there. A detailed analysis of the IOS backup and DJI Assistant backup could not be performed due to encryption techniques present. However, use of a DJI product could be proven on the IOS device. These statements remain true across each of the datasets.

### 3.4. DJI Inspire 2

Released one month after the prior device, the ‘DJI Inspire 2’ was regarded as a ‘benchmark’ at release (Juniper, 2022). While it is no longer one of the best options available, it remains in the market and can be bought second hand. The provided files for this model are as shown in Figure 46.





















	df025_external_microSD-005.001		06/08/2022 00:40	001 File	15,646,720 ...
	df025_flight_android_physical-008.001		05/08/2022 23:46	001 File	5,165,056 KB
	df025_internal_microSD-009.001		06/08/2022 00:08	001 File	7,761,920 KB
	df026_flight_android_physical-004.001		05/08/2022 23:47	001 File	5,165,056 KB
	df027_external_microSD-006.001		06/08/2022 00:40	001 File	15,646,720 ...
	df027_flight_android_physical-003.001		05/08/2022 23:44	001 File	5,165,056 KB
	df027_flight2_android_physical-002.001		05/08/2022 23:45	001 File	5,165,056 KB
	DJI_Inspire_2-20220805T210232Z-001		05/08/2022 22:53	Compressed (zipp...	2,060,606 KB
	DJI_Inspire_2-20220805T210232Z-010		05/08/2022 22:33	Compressed (zipp...	1,060,224 KB
	intact_sdcard_internal-007.001		06/08/2022 00:08	001 File	7,761,889 KB

Figure 46

Similar to the Mavic, due to download constraints, there are two compressed folders. They follow the same structure here as for the Mavic, where the files in “010” reflect those in “011”. The datasets for the inspire 2 model are 025, 026 and 027, as shown in the figure above. The file system format is structured the same way the Mavic, within the zip folder are three more folders, one for each dataset (Figure 48). Within these files is at least one dated file “2017\_August” exists, while 027 contained “June\_2018” as well (Figure 49). This is very similar to the files found for the Mavic model. However, there are less files present at the roots of the directories than within the Mavic. The 026 dataset contains a “flight\_android\_physical” file as well as a zipped file containing iOS backups. At the root of 025, internal and external images of the SD card can be found as well as iOS backup and an Android image (Figure 50). Finally, dataset 027 contains two subfolders. Starting with August there are two files, another Android physical image and another iOS backup folder.

These are also present in the July folder, however, there are also two more SD card images (external and internal) as well as a zipped file named “flight\_log\_data” (figure 47).

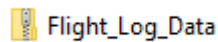


Figure 47

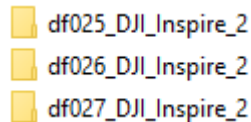


Figure 48

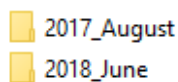


Figure 49



Figure 50

Like the Mavic, there are also a number of hashing files (md5 and sha1) for validation. Contained within are also similar ReadMe files containing specifications and information on the salted data (Figure 51).

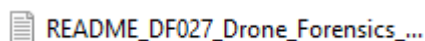


Figure 51

### 3.4.1. Method

The method for analysing the ‘Inspire 2’ will be developed based on the findings of (Marcella, 2021). However, due to the nature of the paper, only the data itself was covered and a method of extracting said data was not provided. As such, the method for this investigation will be based on the one proposed for the Mavic (as they are both DJI models and share similar make-ups), with some changes to relate to the Marcella’s findings. Each of the available datasets will be examined using this process.

- First, to ensure the validity of the investigation, the SHA1 and MD5 hash files will be used to ensure the values are the same as those provided.



- The images of the SD cards will be viewed using Autopsy to locate relevant flight logs and media files.
- EXIF data from any recovered images will be analysed with the aim of establishing when and where they were taken.
- Any recovered flight logs, along with the ones that were provided, will be decrypted and analysed so that a rudimentary flight path will be established.
- Analyse the contents of the Android and iOS devices, searching for any traces of the DJI applications used to control the drone as well as any other relevant data.
- Review any remaining files for forensically relevant data.
- Finally, the values of the hash files will be compared again to ensure data has not been edited during the investigation.

### 3.4.2. Hash Generation

Like the Mavic Pro, the hash values for each of the Inspire 2's provided data can be located within the txt files provided. Figure 52 shows the values for each of the files in dataset 027, June 2018.

```

Filename: Flight_Log_Data.zip
Size: 1,940,024,308
MD5: 97d7787cf044ddb630ff272d979bc316
SHA1: 79a2e04074e1b347e1096f3128596fbf9a9bc899
Released: 2018-10-10

Filename: Android_Logical.zip
Size: 163,229,401
MD5: e26543f2ca2fe639e86e86e3f4b49233
SHA1: 8377226d8bef26bfa2092cd63badfd03e2a44682
Released: 2018-10-10

Filename: ios_backup.zip
Size: 402,683,578
MD5: 848aa61f100e93d7217e33ca64284eca
SHA1: b605f267fc4377ac42b81cd92011b0074c34141d
Released: 2018-10-10

Filename: df027_external_microSD.001
Size: 16,022,241,280
MD5: 81658a05a04d4ed49566527f772aa916
SHA1: 17544c169692de3d6873f63c3f8849743ede7a89
Released: 2018-10-10

Filename: intact_sdcard_internal.001
Size: 7,948,173,824
MD5: 00a103d78104cf406cc72879fe87ec79
SHA1: 1b5d03a1515ce80d78dda389a378c778c8c1893c
Released: 2018-10-10

```

Figure 52

Each of the SD card and Android images were loaded into Autopsy with their corresponding hash values. Just like the investigation for the Mavic Pro, two cases were created. The first for the SD card images and the second for the Android ones. Figure 53 displays the first SD card image, along with the corresponding hashes, in Autopsy.

Metadata	
Name:	/img_df025_external_microSD-005.001
Type:	Raw Single
Size:	16022241280
MD5:	da330ae0d0015d9481989402eec632f1
SHA1:	0155b8bb2f9d9452277c056409dd99cf9d29fcd

Figure 53

### 3.4.3. SD Card Analysis

As previously mentioned, a new case in Autopsy was created which contained each of the four SD card images (Figure 54). Of the four, none are from dataset 026. Instead, external and internal images were found for 025 and 027. The contents of these images are very similar to those that were found in the Mavic Pro. Both the external images contained two volumes, the first spanning sectors 0-8191 of unallocated space. The second volume contains the content of the image and spans the remaining sectors. The main difference between these images and the Mavic's is that the internal image 'df025' also contains two volumes. However, the first only spans sectors 0-62. This is unallocated space. While the second internal image lacks this, its contents, along with the contents of the second volume of the other internal image, follow the same structure.





Name
 df025_external_microSD-005.001_1 Host
 df025_internal_microSD-009.001_97 Host
 df027_external_microSD-006.001_293 Host
 intact_sdcard_internal-007.001_392 Host

Figure 54

The internal images contain three main folders each (Figure 55). 'Unalloc' appears to contain a number of unallocated files. Carved files can be found in the 'CarvedFiles' folder. Orphan files are files which no longer serve a purpose due to the application they are associated with being moved or deleted. One such file was present in the internal image for 'df025'. More notably, flight logs can be found in these images, in DAT format, along with a "PARM.LOG" which appears to note the creation of new flight logs (Figure 56). The flight logs could be found in the same location as those found in the Mavic Pro. No other files of notice were found in these two images.

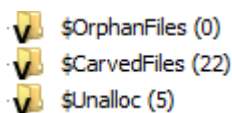


Figure 55

```
<3.007339>(1-0)----->New fly data created"FLY001.dat"
<16.971451>(1-1)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
<17.171477>(1-2)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
<17.371478>(1-3)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
<17.571514>(1-4)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
<17.771470>(1-5)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
<3.006459>(2-0)----->New fly data created"FLY002.dat"
<16.923053>(2-1)[sdk_activation]-&(FMU_CFG_GET(CFG_API_EN ,api_entry_cfg_t)->authority_level)-"g_config.api_entry_cfg.34"
```

Figure 56

The external images also had identical file structures to each other. These files can be seen in Figure 57 below. The only difference at this level is the number of unallocated files. As discussed in the research, the DCIM folder contains a subfolder named "100MEDIA" which is where all the media files recorded by the device are located. In this case, no photographs were recorded between the two datasets, but nine videos were found. Four in the first image (Figure 58) and five in the second. The "MISC" folder contained a further four subfolders. Within these, what appears to be a log of when the camera was used could be found (Figure 59) as well as copies of the video files found in the DCIM folder. These copies appear to be of lower quality.

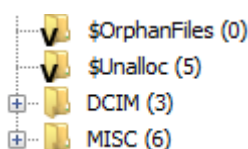


Figure 57

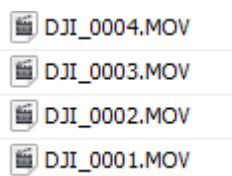


Figure 58

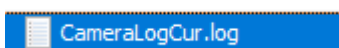


Figure 59

Two carved video files were also found on the second internal image. This suggests that they were deleted or became corrupted, and this is where such files are stored.

#### *3.4.4. Media Analysis*

Unfortunately, as there were no image files present on the SD card images, there is less information that can be gathered as EXIF data cannot be viewed. However, a number of video files were found which contain forensically relevant data.

The content of the videos is similar to those found in the Mavic Pro images. The area that the flights take place in appears to be a hilly, grassland region. Figures 60 and 61 are still captures from two of the video files that were recovered. “DJI\_0004.MOV” from df025 external and “DJI\_0005.MOV” from df027 external respectively. One of the recordings also appears to capture an operator of the drone and their trailer which they were operating the drone from. Should such a recording exist in a criminal case, it could be used to effectively incriminate the suspect.



*Figure 60*



*Figure 61*

Each of the recordings have a listed “Accessed”, “Created” and “Changed” time listed in Autopsy. Figure 62 depicts these values for the file “DJI\_0003.MOV” in the df027 image.

```
Directory Entry Times:
Written: 2017-08-29 14:08:20 (GMT Daylight Time)
Accessed: 2018-06-20 00:00:00 (GMT Daylight Time)
Created: 2017-08-29 14:04:08 (GMT Daylight Time)
```

Figure 62

Should the file be exported and viewed in Windows File Explorer, the creation time of the file is listed as the Autopsy accessed time. According to the txt file, the flights recorded took place from the 19/06/2018 – 21/06/2018 which suggests that the file existed from a previous flight recording and was updated or viewed when the new data was salted. The videos that were stored in the MISC folder do not have an updated accessed time; this value is the same as when it was created.

As mentioned above, no images were recovered using Autopsy so EXIF data, including GPS coordinates of where an image is taken, could be recovered. According to the literature, any images should be found in the DCIM folder along with the video recordings. Autopsy also allows an examiner to view deleted files on an image, there were no images here either. This suggests that no photographs were taken during the flight.

#### 3.4.5. Flight Logs

Between the two internal images, over fifty flight logs were recovered using Autopsy. The first of these logs are dated August 2017 and the latest are from July 2018. A range of these logs were exported and converted to CSV files using DatCon. Using the information found in these files, a flight path was then reconstructed.

The files produced by DatCon match the ones that were produced for the Mavic Pro in terms of structure and content. As with the logs recovered from the Mavic Pro, the values in some logs are set to zero. However, these are from logs that were outside of the time boundaries set by the txt files. Example GPS data recovered can be seen below (Figure 63). These figures are consistent with the ones that were salted onto the device.

GPS:Long	GPS:Lat
-106.216	39.9612
-106.216	39.9612
-106.216	39.9612

Figure 63

Using Google Earth, flight paths were recreated using these files. Each file contained thousands of values, even for flights where only a short distance was travelled. As such, each value cannot be added to a flight path. Instead, values were checked and key points in the journey were marked down. Figure 64 shows the first reconstructed flight path from file “FLY030.DAT”.

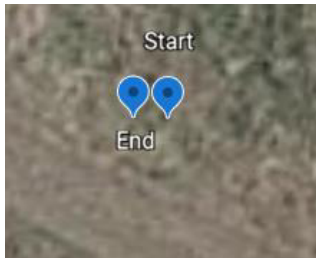


Figure 64

This flight was recorded on the 20/06/2018 and shows that the device only flew a short distance. The location matches the salted coordinates, and the terrain also matches the captured videos. Figure 65 depicts a much longer flight taken from “FLY001.DAT”.



Figure 65

This flight starts and ends behind VTO Labs’ headquarters in Colorado US. Each of the marked points on the map indicate points on the flight, numbered in order of travel. The flight itself shows that the drone travelled from the start to P1, in a straight line, before looping back around via P2 and P3 before stopping close to where it started. As the flight takes place at the building owned by the organisation who recorded the flights, it would appear that the flight data is most likely valid.

### 3.4.6. Android Images

A second case, named “InspireAndroid” was created in Autopsy using the four Android images that were provided for the Inspire 2. These images, displayed in Autopsy, can be seen in Figure 66 below.



Figure 66

Each of the images contain a number of files relating to various Android applications or functions (Figure 67). Each of the images have this structure. These files match with the ones discovered when investigating the Mavic Pro. Likewise, important data can be found in the same locations. This is likely due to both devices using “dji.go.v4”, which results in data being stored in the same method regardless of which drone model is used. As such, images, videos, app data and flight records can all be recovered from the same locations.

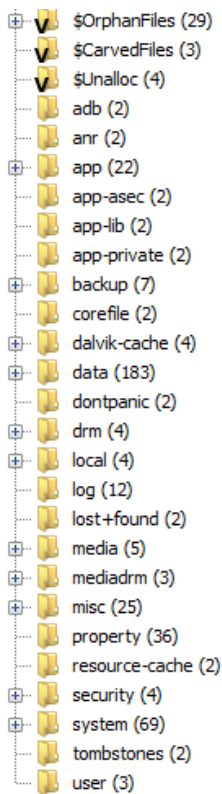


Figure 67

Within the app folder, a number of encrypted files can be found which are used for setting up and establishing functionality of the DJI GO application. Similarly, within the data folder are a number of property files that display information such as the region codes for each region (Figure 68). User avatar can also be found here. More importantly, a number of encrypted databases that show the history of the application can be found. While this data is useful, the contents of the media folder are where the most important data can be found.

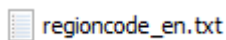


Figure 68

By navigating the media folder, the area where images, videos and flight logs are located can be found. In this case, it was under the path depicted in Figure 69.

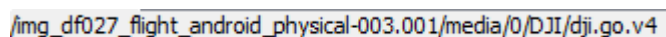


Figure 69

At this location, a number of folders can be found (Figure 70). LOG, FlightRecord, DJI\_RECORD and CACHE\_IMAGE are worth noting for their contents.



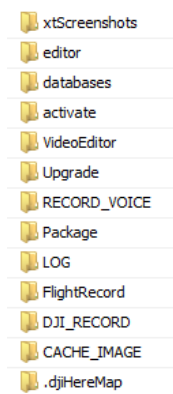


Figure 70

The LOG file contains a number of text files that contain updates and changes the drone undertook while powered on. This includes Wi-Fi connections, errors and the connection status between the drone and the application on the mobile device. Figure 71 shows the contents of one of these logs stored within the folder “UP\_WIFI\_PR”.

```
e: 11:26:02 isOfflineServerInfo getDevice1=wm620
e: 11:26:02 isOfflineServerInfo getDevice2=unknow
e: 11:26:02 isOfflineServerInfo deviceType1=rc001 deviceType2=wm620
e: 11:26:29 固件升级状态设置
e: 11:26:50 固件升级状态reset
e: 16:26:34 固件升级状态reset
e: 16:26:34 isOfflineServerInfo getDevice1=rc001
e: 16:26:34 isOfflineServerInfo getDevice2=wm620
e: 16:26:34 isOfflineEnableMode false
e: 16:27:02 startCollect
e: 16:33:38 WifiPrLogic getFail pid=rc002 reason:getUrlList -- onFailure unknownHostException:can't resolve host
e: 16:33:38 isOfflineEnableMode false callBack.exec()
e: 16:33:38 WifiPrLogic getFail pid=wm100 reason:getUrlList -- onFailure unknownHostException:can't resolve host
e: 13:17:34 isOfflineServerInfo deviceType1=rc001 deviceType2=wm620
e: 13:18:05 固件升级状态设置
e: 13:23:49 固件升级状态reset
```

Figure 71

DJI\_RECORD contains video recordings sent from the drone to the mobile device. Two recordings were found on these images, one from 025 and one from 026. These recordings appear to match the footage found within the SD card analysis. While the image quality of these recordings was on par with the ones stored on the drone’s SD card, the recording appears to be corrupted in places, ‘jumping’ frames of the video and occasionally losing picture. Unfortunately, this makes the recordings less valuable on their own as they are of lesser quality. However, when used in conjunction with the files found on the SD card, they can be used to establish a connection between the two devices.

Images that can be found in the CACHE\_IMAGE folder are in a similar situation. They appear to be images captured by the drone but of a vastly lower quality. The only images that were found are present on the 025 image (Figure 72). The images here are low in quality, appearing blurred. The first of these images can be seen in Figure 73.

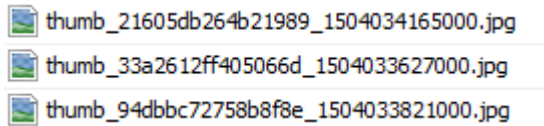


Figure 72

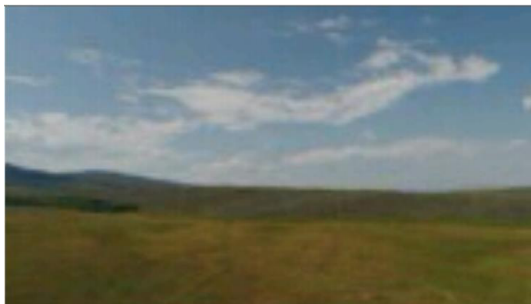


Figure 73

While no images were found on the SD card during analysis, the video recordings that were found appear to match the images found on the Android device. Figure 74 is a capture from one of the video files found on the SD card. The two images are nearly identical to each other. Each of the three images that were found match sections of flight recordings in this way. This would suggest that the images corrupted/were not saved on the SD card.



Figure 74

The loss of quality on images and videos present within the Android device is likely due to connection issues between the drone and mobile device, resulting in packet loss in transit.

Finally, the folder 'FlightRecord' contains .DAT flight records, along with the date that they were recorded (Figure 75). These records were found in the 026 image, but records can be found in each of the images.

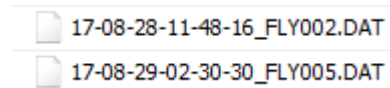


Figure 75

These logs can be exported and subsequently converted to CSV using DatCon. After doing this, a flight path can be reconstructed. Figure 76 shows the flight path for "FLY002.DAT", reconstructed in Google Earth. The flight path matches the data found within the corresponding file found on the SD card image. However, the flight log on the SD card appears to have far more coordinate values stored within it, providing a more detailed version of the flight. That being said, the flight log found on the Android device does still match the same path and is not incorrect. The flight itself shows that the drone flew in a straight line before turning around and following the same path backwards. Coming to a stop shortly before the point which it started.

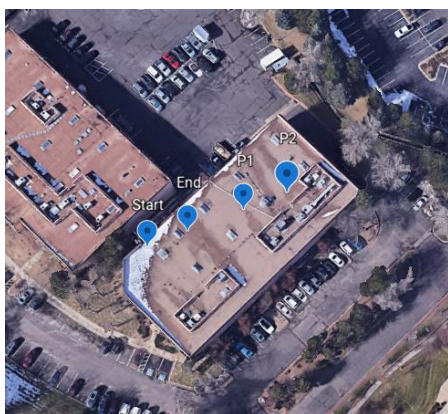


Figure 76

The locations where data can be found remained constant between each of the images that were investigated. Some differences in the naming of folders were present, such as image 026 having the folder "DJI\_SPLASH" within the media folder, but none of these folders appeared to contain any forensically relevant files or information.

One other thing of note that was found on each of the images was a deleted file named "com.parrot.freeflight3". This was found in the media file for user "obb". This application is

used to control Parrot drones on Android devices, similar to how DJI GO is used for DJI products. While this is not related to the Inspire 2, its presence indicates that whoever owned the Android device may have used more than one drone.

3.4.7. IOS Backups

As with the Android images, four IOS backups were provided (Figure 77). One for each of the images, plus an extra for image 027. This also matches the Android images, where two flights were recorded in the one dataset. The contents of these backups mimic those found when examining the Mavic Pro. A number of folders with hexadecimal naming, some PLIST files and one database file. Therefore, it can also be inferred that these backups were created using iTunes. Just as was done for the Mavic Pro.





 DF025 MC07 iOS		31/08/2022 16:51	File folder
 DF026 MC08 iOS		31/08/2022 16:52	File folder
 DF027 MC09 iOS		31/08/2022 16:50	File folder
 ios_backup		31/08/2022 16:52	File folder

Figure 77

The files found within also follow the same scheme as those found on the Mavic Pro. The first two characters are the same as the name of the folder they are found in, followed by more hexadecimal values. Likewise, the files that were found in that analysis were also present within these images. Those being the SMS database file (Figure 78) and “com.dji.go.plist” (Figure 79). The later Indicating that the device was used to pilot a DJI device.

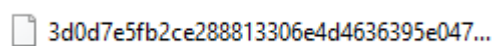


Figure 78

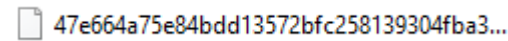


Figure 79

As the method used to analyse these files was derived from an article that only briefly mentions what may be found during the analysis of an Inspire 2, much of the process of analysis was helped by the previous investigation. Unfortunately, this meant that the same issue was present when analysing these backups. The lack of a tool or OS capable of reading

these files meant that analysing them didn't lead to any more discoveries, while using the established method.

#### *3.4.8. Flight Log Data*

The zipped file "Flight\_Log\_Data" found within dataset 027 contains a number of flight logs. These flight logs appear to match the ones recovered during the analysis of the SD cards. For example, "FLY030.DAT", found in the file and the SD card, have identical coordinates. Both start at 39.9612, -106.216 and end at 39.96119, -106.216. This applies for all of the flight logs found within the file. However, the SD card had one more file "FLY042.DAT". This is not present within the folder, perhaps because it was recorded after this file was created.

No further files of interest could be found across the datasets.

#### *3.4.9. Validity*

Each of the images were checked again in Autopsy, ensuring there were no integrity errors. Each of the hash values remained the same as they had been at the beginning of the investigation, so no data had been changed.

#### *3.4.10. Summary*

Each of the files and images that were analysed during this investigation were much the same as those investigated for the Mavic Pro. This was expected, to an extent, as the two models are created by the same company. Almost all data that can be found within the Inspire 2 and associated devices is in the same location as those for the Mavic Pro. Even the file structure of the SD cards is the same. The only substantial differences are within the properties of files such as images, describing the type of camera that was used to record media and within the files which define the drone itself.

Recordings, flight logs and system information could be recovered from the SD card images. Corresponding flight logs could be recovered from the Android device as well as images and recordings that further established a link between the drone and mobile device. A link between the IOS device and a DJI product could also be established. Flight paths could be accurately recreated using the data that was recovered.

### 3.5. Parrot Bebop

The oldest of the chosen devices, the Bebop 2 was released late 2015. The files that were provided for the ‘Parrot Bebop 2’ are displayed in figure 80.











	df022_flight_android_physical-003.001		05/08/2022 14:31	001 File	5,165,056 KB
	df023_flight_android_physical-001.001		05/08/2022 14:31	001 File	5,165,056 KB
	df024_flight_android_physical-005.001		05/08/2022 14:31	001 File	5,165,056 KB
	mtdblock0-004.dd		05/08/2022 14:37	DD File	7,634,944 KB
	Parrot_Bebop_2_plus_SkyController-2022...		05/08/2022 13:52	Compressed (zipp...	995,403 KB

Figure 80

As is implied in the above figure, the Parrot Bebop 2 datasets contained the fewest files of the drones considered during this investigation. Despite this, it also contains data for the SkyController which is a custom-built remote control for the drone (Parrot, 2021). Unlike the two previous devices, only one compressed folder was produced when downloaded. The entirety of the original file pathing is found within. As shown in the figure above, 022, 023 and 024 are the three datasets used for the Bebop 2. The general file structure found within the zip folder is near identical to those found in the Inspire 2, at least until the files found at the end of each path. The contents within the zip are as shown in Figure 81. Then, within those are dated files named in the same convention as both the other models. Similar to the Inspire 2, the first two files (022 and 023) contain only the August file (Figure 82) while 024 contains another for June 2018. Each of the ‘August’ files contains physical images of the Android device and a zipped backup for iOS. The “2018\_June” folder in 024 contains slightly different files, the IOS backup remains the same, but instead of an Android image, there is a logical extraction of the file system instead. There is also a physical image of the drone; “mtdblock0-004.dd” which is contained within “ABD\_Physical” (Figure 83). Like both the previous drones, at each step in the file chain there are ReadMe files explaining the data. It also has hash files for each of the actionable data files/images, in the same way the previous two did.

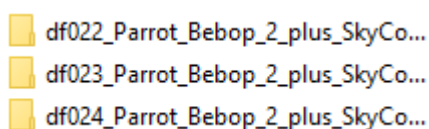


Figure 81

Figure 82

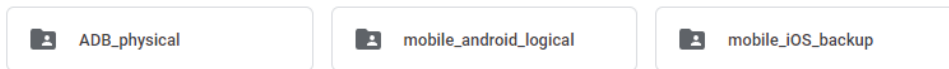


Figure 83

### 3.5.1. Method

The method that will be used to analyse the contents of the 'Parrot Bebop 2' will be based on the one put forward by (Kumar & Agrawal, 2021).

- The MD5 and SHA1 hash values will be compared for each of the files to ensure they have not been edited after being downloaded.
- The image "mtddblock0-004.dd" will then be searched for any trace of the application 'Parrot FreeFlight', establishing the link between drone and mobile device.
- Then the analysis of the Android images using Autopsy will take place. This is done with the aim of finding the Parrot app and recovering the flight logs it stores.
- Then the Android logical extraction and IOS backups will be viewed to find any relevant data.
- Any recovered flight logs will then be decrypted and analysed.
- Other potentially relevant files will then be searched.
- The data gathered will be compared to that which was salted onto the device to authenticate the findings.
- Finally, the hash values will be compared again to ensure that the files were not modified during the investigation.

### 3.5.2. Hash Generation

As with each of the drone datasets provided by VTO labs, each of the files has a corresponding MD5 and SHA1 hash. These were then entered when adding each of the images into cases in Autopsy. Figure 84 below displays this step for the Android image from dataset 023.

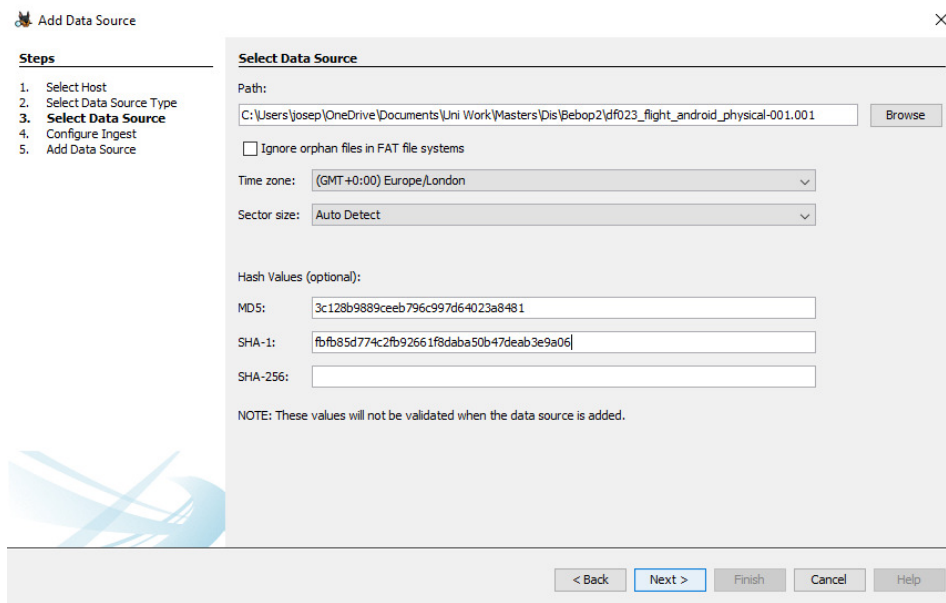


Figure 84

### 3.5.3. Mtdblock0-004.dd Analysis

Unlike the previous drone, the datasets for the 'Parrot Bebop 2' only contained one drone image to view. In order to analyse this file, a new case was created in Autopsy and the image was added as a data source. As only one data source exists, the results of the analysis may not account for any variation in structure found on other devices. However, as was found on the images for the other two drones, any differences between images tend to be minor and do not affect the process of data acquisition in a meaningful way.

Once the image was loaded in Autopsy, it could be viewed. Figure 85 displays the contents of the image.

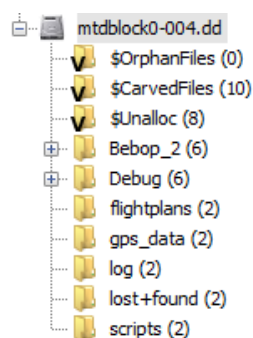


Figure 85

According to (Parrot, 2015), 'Flight Plans' are a feature of the 'Parrot FreeFlight 3' app that allow a user to create a flight plan in advance that the drone will follow once activated. It is



likely that the folder “flightplans” is where such data is stored, if there is any saved. None were recovered from this image but based on the name, it seems likely. Similarly, no files were found within the final four folders on the image. The files “gps\_data”, “log” and “scripts” each have similarly named folders in both the Inspire 2 and Mavic Pro, suggesting they serve a similar purpose. The file “lost+found” appears to be a common folder found on Linux and Unix devices. It is used to store data fragments that have lost their corresponding filename, where they can potentially be recovered (Baeldung, 2021). The debug folder contained archive and crash report data, along with what appears to be an area for deleted or completed flight plans. A number of flight plan related files that had been deleted were found in this area. The final folder, “Bebop\_2”, contained another set of folders (Figure 86). These folders contained no further data.

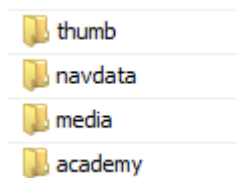


Figure 86

The presence of the “flightplans” folder was the only substantial data recovered from this image. If presence of the related application on the mobile device can be verified, it establishes a link between the two devices.

#### 3.5.4. Android Images

Each of the three datasets included an Android physical image. These were loaded into a new case in Autopsy (Figure 87). The contents of the second image are displayed in Figure 88. The contents of each image remain consistent with each other at this level.

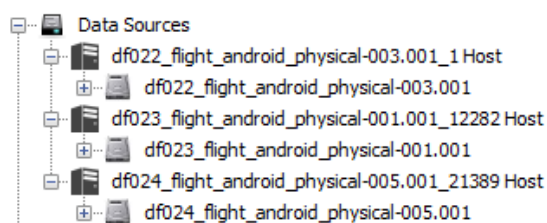


Figure 87

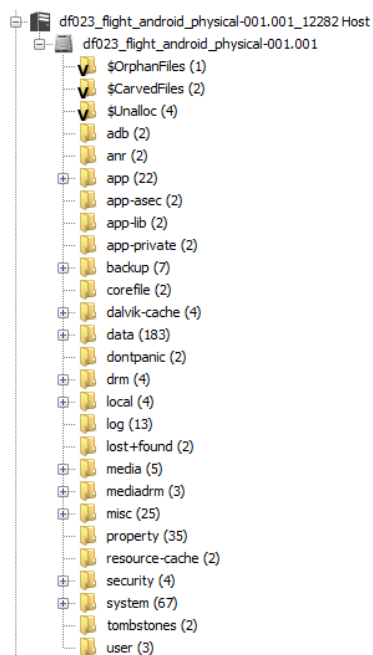


Figure 88

Of these folders, three were found to hold data relating to the Parrot drone. Those being “app”, “media” and “data”. Within the app folder is a number of folders, each for different applications on the device. “com.parrot.freeflight3-1” was one of them. This helps to verify the connection between drone and mobile device as there was evidence of this application present on the SD card image. The folder itself contains a number of Android files (Figure 89) which appear to be used for launching and running the application on the device.

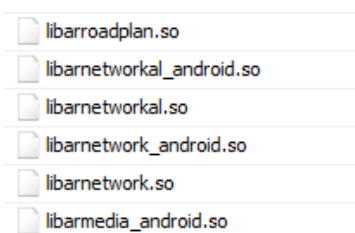


Figure 89

Within the media folder were two references to the drone. The first was found under the file path displayed in Figure 90.

`/media/0/DCIM/Bebop 2`

Figure 90

Based on the name of this folder, this could be the location where any recorded media from the drone is stored. However, none was recovered across all three of the images. This

matches the findings from the analysis of the drone image. It can be assumed this would be where media is stored as the folder name directly references the drone and DCIM is the common folder name for media storage. The second location's path is shown in Figure 91.

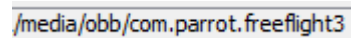
A screenshot of a file path displayed in a text field or document. The path is `/media/obb/com.parrot.freeflight3`.

Figure 91

This area appears to contain a number of update files for various plugins used by the application. It contains some .PLF files (Figure 92), which are commonly used to store information about screen layouts (Lepage, 2015). Therefore, it seems likely that these files are for updating certain aspects of the application's layout.

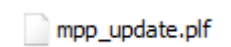
A screenshot of a file icon and name. The file is named `mpp_update.plf`.

Figure 92

Finally, the “data” folder contains many subfolders for each of the applications and processes that are run on the device. Within these is a folder named “com.parrot.freeflight3”. The contents of this folder are displayed in Figure 93.

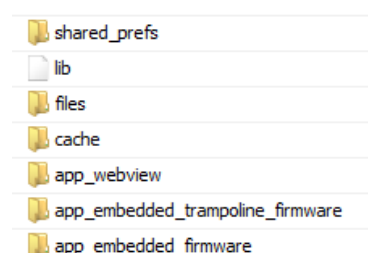
A screenshot of a folder listing. The folders are: `shared_prefs`, `lib`, `files`, `cache`, `app_webview`, `app_embedded_trampoline_firmware`, and `app_embedded_firmware`.

Figure 93

The bottom two folders notably contain matching files to those found at the location shown in Figure 91. Being a variety of .PLF files. “shared\_prefs” contains a number of xml files that appear to relate to user settings and preferences that have been selected by the user when operating the application. Both “cache” and “app\_webview” contain general information about the application. Within “files”, a variety of information is stored. This includes another version of the .PLF files that were found elsewhere, satellite data (stored in a folder named “ephemeris”) and flight information such as flight logs. These logs can be accessed at the file path shown in figure 94. There were also zipped versions of flight logs found in a folder

'data/com.parrot.freeflight3/files/ACADEMY/runDetails

Figure 94

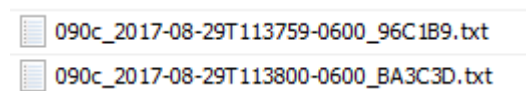


Figure 95

Only the first image contained flight logs at this location, both of the others contained nothing at this point. However, the other two images did have logs present in the Blackbox folder (Figure 96).

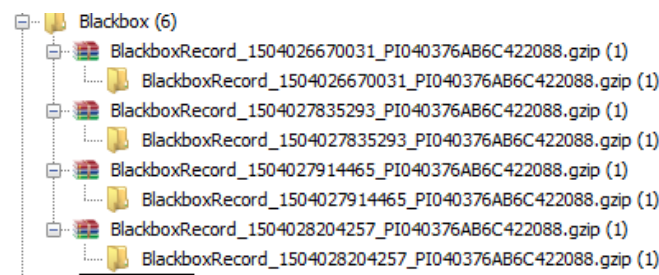


Figure 96

The text saved on these logs is confusing and difficult to understand at a glance (Figure 97).

[illegible]

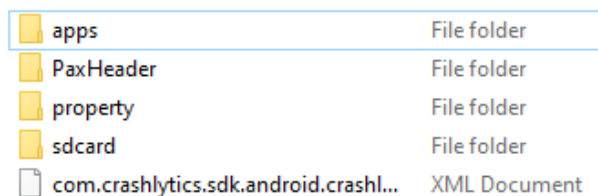
Figure 97

Logs were extracted from both locations for analysis.

Evidence of the DJI application discussed in the previous sections was also present on each of the images. However, no content was found that suggested a device had been paired and used.

### 3.5.5. Android Logical Extraction

The logical extraction provided in the final dataset is similar to the images viewed in the previous section. The main differences are where files are located. The contents of the zipped file are displayed in Figure 98.



apps	File folder
PaxHeader	File folder
property	File folder
sdcard	File folder
com.crashlytics.sdk.android.crashl...	XML Document

Figure 98

The “apps” folder contains all the file location that were found in the data folder on the image (for the Parrot application). Meanwhile, the folder “sdcard” contained the contents of what was found in the “media” folder on the image. Two zipped Blackbox flight logs were recovered from this extraction but nothing else of note was found. The flight logs were in .GZIP format.

### 3.5.6. IOS Backups

The content of the IOS backups appears to be consistent with the findings from the previous drones. Each of the backups contain a list of hexadecimal folders (Figure 99), containing files which were also named using hexadecimal characters. These files shared the first two characters of their name with the folder they are located in. As this is the case, it can be assumed they were extracted using Apple iTunes as they share the same characteristics as the previous cases. The same PLIST files were also found.

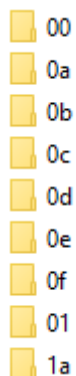


Figure 99

Unfortunately, the study that informed this analysis and method made no mention of the IOS file system and as with the previous analysis for IOS backups, the files themselves could not be viewed. This means that no data could be gathered from these backups that directly relates to the Bebop 2.

### 3.5.7. Flight logs

Two types of logs were extracted from the Android images; the .txt files found in the “runDetails” folder, and the ones found in the zipped black box files. The first of which can be converted using the tool ‘Parrot Drone Flight Log Converter’.

Each of the flight logs recovered were selected for extraction using the tool (Figure 100). Once selected, pressing the convert button will create a CSV file in the same file location that the .txt file was taken from (Figure 101). Two types of text files are stored when a flight log is recorded, the log itself and a smaller file that stores system information as well as the start location of the flight. The tool also converts these “Header” files into a more readable format.

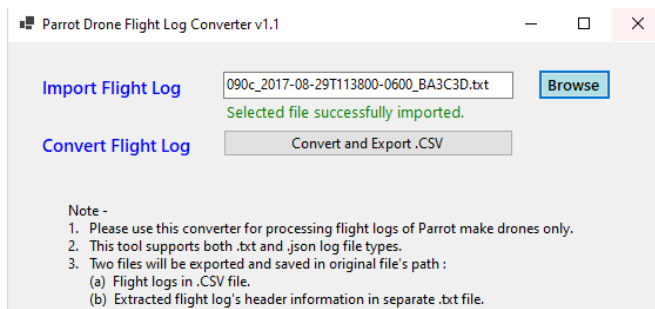


Figure 100

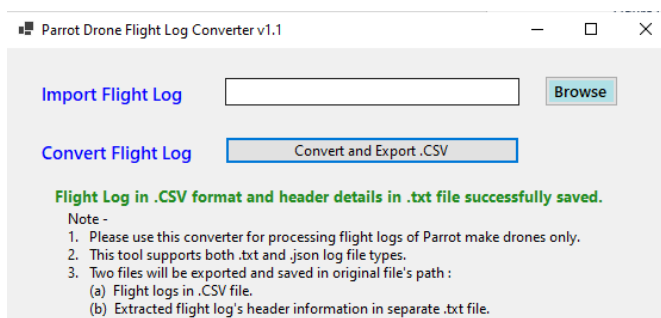


Figure 101

Figure 102 displays two text files that were recovered, along with the two files that the converter produced. The contents of the CSV and TXT files are displayed in Figures 103 and 104 respectively.

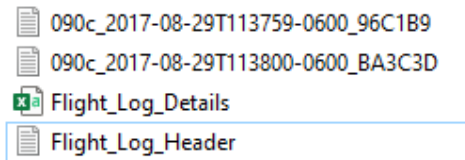


Figure 102

"time"	"battery"	"controllé"	"controllé"	"flying_st"	"alert_sta"	"wifi_sigr"	"product_"	"product_"	"product_"	"product_"	"product_"	"speed_v"	"speed_v"	"speed_v"	"angle_pl"	"angle_th"	"angle_ps"	"altitude"	"flip_type"	"speed"
62	63	-106.216	39.96124	0	0	-46	true	-106.216	39.96121	0	18	0.005853	-0.00681	0.004327	0.041976	-0.02955	0.998278	-3	0	0.009969
73	63	-106.216	39.96124	0	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042369	-0.03026	0.99571	0	0	0
74	63	-106.216	39.96124	0	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042369	-0.03026	0.99571	0	0	0
74	63	-106.216	39.96124	0	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042369	-0.03026	0.99571	0	0	0
75	63	-106.216	39.96124	0	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042369	-0.03026	0.99571	0	0	0
78	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042369	-0.03026	0.99571	0	0	0
182	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042316	-0.03021	0.995112	0	0	0
387	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042316	-0.03021	0.995112	0	0	0
391	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042316	-0.03021	0.995112	0	0	0
391	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042316	-0.03021	0.995112	0	0	0
391	63	-106.216	39.96124	1	0	-46	true	-106.216	39.96121	0	18	0	0	0	0.042534	-0.03013	0.995548	0	0	0

Figure 103

```

{"version": "1.2"
"software_version": "4.2.1"
"hardware_version": "HW_02"
"date": "2017-08-29T113800-0600"
"product_id": 2316
"serial_number": "PI040376AB6C421353"
"product_name": "Bebop 2"
"uuid": "BA3C3DBB35927B2B08228E755FA0F759"
"run_origin": 0
"controller_model": "SkyController"
"controller_application": "nap"
"product_style": -2
"product_accessory": -2
"gps_available": true
"gps_latitude": 39.961214
"gps_longitude": -106.216362
"crash": 0
"jump": null
"run_time": 315800
"total_run_time": 315970

```

Figure 104

The files display a variety of useful data including controller GPS data, drone GPS data, the model used, run time, crashes and the speed at which the device was travelling. Using the GPS data taken from the files, a flight path was reconstructed using Google Earth. Figure 105 displays the start and end points of the flight, along with the coordinates of the controller that was used (yellow). These were condensed into one point for the full flight because the coordinates of each were too close together to read on a larger map.

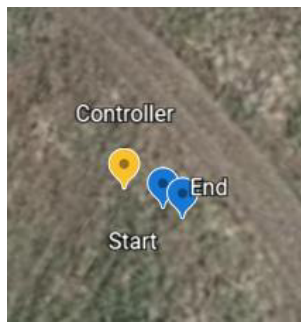


Figure 105

Figure 106 displays the flight that the drone took, based off of the coordinates found in the flight log. This flight was recreated by taking key points from the log and marking them down in order on Google Earth (Start to P1 to P2 etc...).



Figure 106

The location appears to be consistent with some of the logs recovered from both the Mavic Pro and Inspire 2, with the later having one recording on the same stretch of dirt track. The location also matches the flight that was recovered as part of Kumar and Agrawal's study in 2021. The flight path the drone took is fairly complex, appearing 'hourglass-shaped'. The flight coordinates also match closely to the ones that were provided in the readme file, suggesting that they are accurate.

Moving on to the flight logs found as part of the "BlackBox" folder, within the zipped files were text files which appear to contain similar data to the ones already discussed. The contents of one, opened in Notepad, can be seen in Figure 107.





Figure 107

Unfortunately, these files cannot be accepted by the converter tool, even when saved as txt files. Doing so displays the following error message:

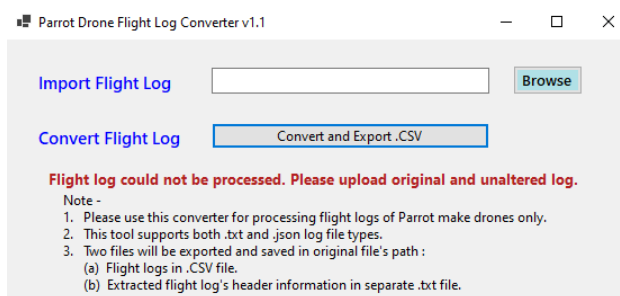


Figure 108

This is likely due to the files stored in the black box folders being a different format to those that are saved normally. It is still possible to reconstruct a flight from the data found in these files but, due to how difficult the file is to read, would take far more time than using the .txt ones. However, they appear to store more accurate coordinates for the flight. The files found in "runDetails" appear to be rounded figures, while the ones in the BlackBox folders do not. The starting point for one of these files is shown in Figure 109 below.

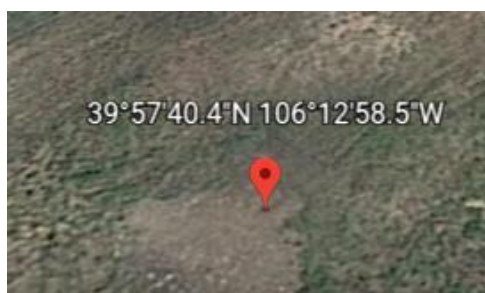


Figure 109

#### *3.5.8. Hash Validation*

Once again, the files were checked in Autopsy to ensure that no changes had been made to them. As they retain the same hash values, without error, none of them have been edited in any way.

#### *3.5.9. Summary*

In the case of the Bebop 2, almost all of the data that was recovered came from the Android images. Flight logs and a variety of system information was recovered but unfortunately there were no video recordings or photographs to extract. Through the structure of the drone file system and the details of the paired drone found on the Android device, a connection between the two could be established. However, this connection would be more concrete with images and videos to evidence. Furthermore, no evidence could be recovered from the IOS backups.

## 4. Method Analysis

### 4.1. DJI Mavic Pro

#### 4.1.1. Comparison

There were some substantial differences between this method and the one that was used in (Yousef et al., 2020). This is due to their focus on IOS devices, while this study gave more attention to the Android images. The IOS backups did not give much information during this investigation as the tools that were suggested in Yousef et al.'s work required MAC/IOS operating systems, or no longer worked.

In their work, they found that JPEG images and MP4 videos could be found in the "100MEDIA" folder of the drone's memory. They also found that these files followed a naming convention of a "DJI" prefix followed by numbers. When analysing the contents of the DJI GO application, they found that videos files could be found, but at a lower quality. Furthermore, the EXIF data from their media files showed data artifacts of the time and place they were recorded. They also found flight logs as part of their analysis of the DJI Assistant 2 on the IOS device, recreating flight paths from them.

There were a number of similarities between the findings of their report and this one. Firstly, both images and videos could be found at the location they specified. The EXIF data they contained also matched what they described. One unexpected similarity is the data found as part of the Android images, when compared to their IOS backups being near identical. This is most likely due to DJI using a similar file and storage systems between different versions of their applications. System and User information was recovered from the Android images, much the same as what was described in their study. Images and videos could also be extracted, though at lower quality. Flight logs were located in the mobile device, as part of the DJI app.

However, there were also some notable differences between the results of the method. The video files that were recovered from the drone itself were not in .MP4 format, being .MOV files instead. The Android images also have a different structure than IOS systems. There were also flight logs uncovered on the drone images themselves as part of this study, while

they only noted the ones recovered off of the IOS device. While their study focused on the Mavic 2 Pro, the two drones appear to share a lot of their structure in common.

#### *4.1.2. Strengths*

This method had a number of notable strengths:

- At the end of the investigation, a variety of evidence/information was gathered. Image, video, flight logs, EXIF data, system info and user ID were all recovered from both the drone and the mobile device.
- A solid connection could be established between mobile device and drone. This is due to the common media found between the two, as well as matching system and drone information.
- Using the tool 'DatCon', the .DAT files could be converted relatively easily and then mapped using the coordinates found.
- Their investigation provided a thorough overview of the file structure of the devices, as well as the content which was contained there. This was useful when looking through the various images and backups as knowing where content was sped up the process.

#### *4.1.3. Weaknesses*

Developing a method based on their findings also had some weaknesses:

- The tools which they suggested using did not work in this case, meaning that analysing the IOS backups became a difficult task and only a small amount of data could be recovered from them.
- A number of tools need to be used to complete this analysis. While this is not a problem unique to this method, it makes the process more complicated than it could be.
- Their method focuses on the IOS backups. While as part of this investigation, the Android images could be navigated using the same tool as for the drone image, it would be valuable to contain more information on how to access the data and what it can be used for.

#### 4.1.4. Improvements

One of the major weaknesses with this method is that the tools that were suggested to view the IOS backups would not work. In order to improve on this, other tools may be worth considering. One such tool that could be used for this is “iBackup Extractor” (Wide Angle Software, 2022). This is a tool for Windows and Mac that allows a user to view the translated contents of an IOS backup. It was capable of reading each of the backups provided in the study (Figure 110) and displayed the names of each of the files, as long as the directory was set to the backup’s location.

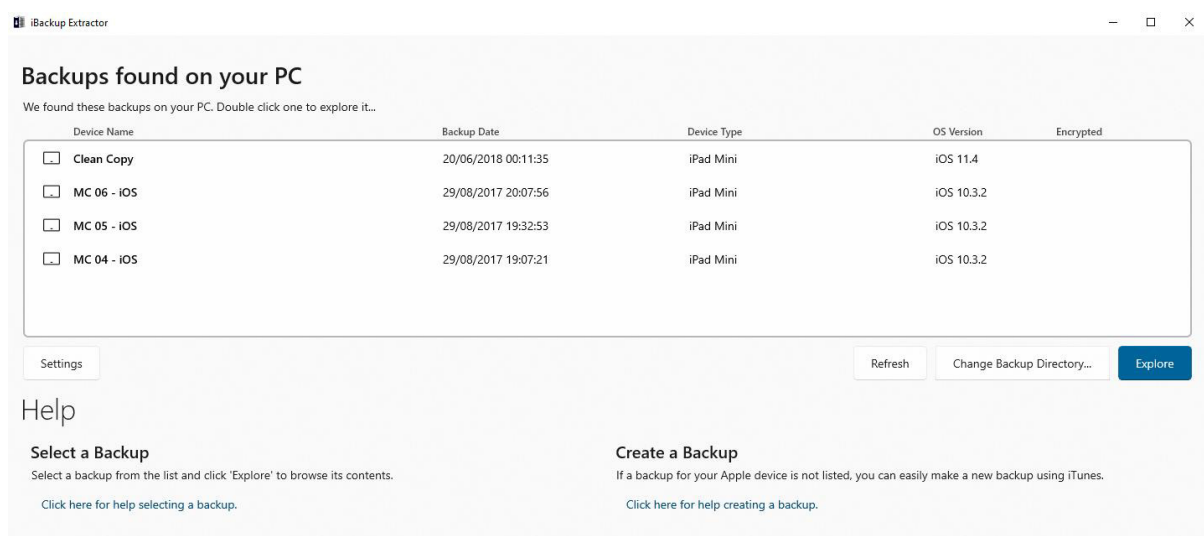


Figure 110

By using this on the backups for the Mavic Pro, a folder related to the DJI GO application could be found (Figure 111).

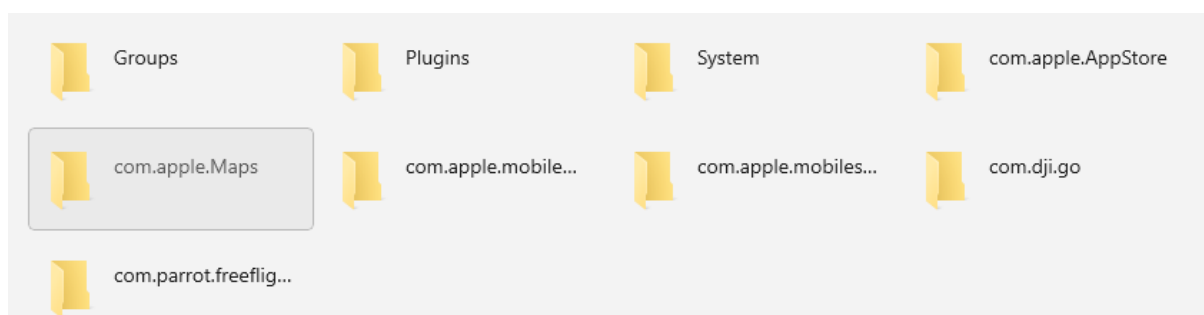


Figure 111

By navigating these folders, copies of flight logs could be found (Figure 112).

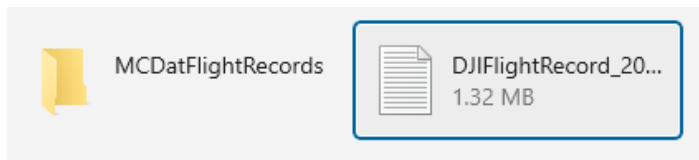


Figure 112

This would provide a far more concrete analysis of the IOS backups and could be used to provide a more detailed structure of what is contained within the backups inside the method. This would help to establish what kinds of data can be extracted from IOS devices, which is needed if a comprehensive overview of drone analysis is to be established. Unfortunately, for the full functionality of the tool, a payment is required. Despite that, using the tool is recommended as it was the only one found that could read the backups.

While a few tools are necessary, it may be possible to reduce the amount used. In their report, “ProDiscover Basic”, “Encase Imager” and “E3:Universal” are all used to display filesystem structure and media data. With the exception of “E3:Universal”, which was used for mobile device analysis, these purposes can be fulfilled by Autopsy. Although they may each have their own strengths, using too many tools for an analysis can confuse and complicate the results. Therefore, it may be of more use to only use the one.

The method itself should be updated to reflect a more detailed analysis of these backups.

## 4.2. DJI Inspire 2

### 4.2.1. Comparison

The methodology used to analyse the drone and related devices in this investigation was based on the findings Marcella’s 2021 report. However, as this report (and no others that were found) gave a descriptive method for analysing the Inspire 2, the details of the method were set based on other DJI models and what was uncovered on the Mavic Pro. As such, most of the findings of Marcella’s report are general statements that apply to any DJI device.

In the report, Marcella found that flight data could be found on TXT files on the mobile device and DAT files on the drone’s internal storage. This remains consistent with what was found on the Inspire 2. However, DAT logs could be found on the mobile device in addition to the TXT files. The described data that could be extrapolated from these logs was

consistent with the report. The report then mentions the types of data EXIF information can give e.g., data and GPS location. While no mention of where this data can be found was made in the report, when it was discovered as part of this investigation, those EXIF values were found to be present in the media. Therefore, it can be used for the same purpose as outlined in the report.

While no information that was present in Marcella's report was inaccurate, there was no mention of file structure or system specific information. As for differences between the Inspire 2 and Mavic Pro, no images were recovered from the Inspire 2. However, this is likely due to no images being captured by the drone as the file location where they are stored in the Mavic Pro was also found. The only other difference was in system information that described the device itself, such as the camera details in the EXIF information. As the structure of the Android and IOS devices are independent of drones that they are used to control, there were no significant differences found between the two investigations.

#### *4.2.2. Strengths*

As Marcella's report did explicitly state a methodology that could be followed, analysing the strengths and weaknesses of it as such would be redundant. Likewise, the method that was used in this investigation shares the strengths and weaknesses of the method followed for the Mavic Pro. Instead, the idea of using a common methodology for all DJI drones shall be considered.

- This would save a lot of time on the part of analysts, as they would only need to consider one methodology for several different models.
- Less research would need to be done to update a singular method, allowing any updates or discoveries to be added and known about faster.
- As discovered in this investigation, the Mavic Pro and Inspire 2 store their file in virtually identical ways. This is likely also true for other DJI products, meaning this idea is potentially viable.
- Any differences between models are likely small and could be included as notes at certain points in the method.

#### *4.2.3. Weaknesses*

Although this idea is the end goal, there are some issues that should be considered first.

- While the models reviewed as part of this paper were very similar, this may not be true of all models. Some older models could have very different systems to those that are more recent. Making a common method impossible.
- In order to form an all-encompassing method, a great deal of research would need to be undertaken. Each drone would need to be compared and contrasted. This would take a lot of time and effort. On top of this, a number of each model would need to be viewed to account for differences that may arise.
- If these drones have substantial differences, a wide variety of tools may be needed. This can confuse the results of an analysis as the more factors that need to be accounted for, the more likely one is forgotten or incorrectly used.

#### *4.2.4. Improvements*

To mitigate some of these potential weaknesses and ensure that such a method is effective, some things could be done. Firstly, more research. There needs to be more articles and reports that describe the contents of each device. As part of the literature review, no content regarding the forensic analysis of the Inspire 2 existed. The structure of less known models needs to be noted down and published so that they can be compared.

It would also be beneficial if there were standard tools for the analysis of these devices. As it stands, different tools are required for each of the data sources and none of them are definitively the best.

To improve upon the method established for the Inspire 2, similar steps should be taken as those outlined in the analysis of the Mavic Pro's method.

### *4.3. Parrot Bebop 2*

#### *4.3.1. Comparison*

The information and evidence gathered as part of this investigation match that which was discovered as part of Kumar & Agrawal's 2021 study, which this method was based upon. Through their investigation, they recovered flight logs from the Android images they acquired and used a tool that they developed to convert these logs into csv data that they could input into Google Earth and reconstructed a flight path out of it.

The analysis performed in this study followed the steps they took and resulted in near identical discoveries. By following a path through the folders "data",



“com.parrot.freeflight3”, “Academy” and finally “runDetails” in the Android images, flight logs were found that matched the format described in their study. Likewise, the results of using the flight log converter were also as expected, producing a CSV file with the flight’s data as well as a “header” file which contained system related artifacts. The flight that was recreated is also consistent with the one produced in their study, with matching location and general flight shape. In their study, more points were plotted on the map which resulted in slight differences. However, the general shape remains the same. This was to be expected as the data source used in their study was VTO Labs, the same as the one used in this study.

While there were no differences in the data collected, more information could be exported from the Android images than what was mentioned as part of their study. The first of these is the user data that can be found in the “shared\_prefs” folder. While not the most relevant data, it could help to establish the identity of the drone’s operator. Similarly, operation information for the app was recovered that may help further establish a connection between drone and mobile device. Finally, there were the flight logs found in the “Blackbox” folder. These logs were not mentioned in their study at all, despite there being far more of them than the regular .txt files. They also did not discuss the contents of the drone, IOS backups or Android extraction.

#### *4.3.2. Strengths*

This method has a number of strengths that make it worth considering should an analysis of this type of device need to take place:

- The information that was provided in their study allows for a thorough examination of an Android device, in regard to finding content related to a “Parrot Bebop 2”.
- As long as a connection between mobile device and drone exists, it can be proved using the method.
- The “Fly Log Converter Tool” that they created and suggest using worked very well, making the flight logs easier to understand and use.
- The data that is recovered using this method can be used to recreate a flight path relatively easily. Being able to recreate the flight path is arguably the most important

piece of evidence that needs to be recovered as it can prove that a drone was used to commit a crime.

#### *4.3.3. Weaknesses*

While the strengths of this method are considerable, there are a number of weaknesses if this method were to be all that is used for analysing the 'Bebop 2'. They are:

- The method relies heavily on having access to an Android image. If an IOS device had been recovered instead or if there was no mobile device available at all, then no information could be gathered using this method. Likewise, the study makes little mention of the drone's internal image and how to recover data from it.
- There is no consideration for the contents of an IOS device at all.
- Only the flight logs are considered. The study makes no mention on where images or videos could be recovered from. These are important pieces of forensic evidence and should not be overlooked.
- While a connection is established between mobile device and drone, it is tenuous and needs evidence such as images being present on both devices to substantiate the findings.
- Not enough evidence is recovered as part of the method to fully incriminate a suspect. Especially if there are no usable flight logs present on the devices.

#### *4.3.4. Improvements*

In order to create a more balanced investigation, some changes and additions could be made. Firstly, a method for analysing the encrypted IOS backups needs to be established. To do this, it is recommended that the tool discussed in the method analysis of the Mavic Pro is used. This would allow actual data to be recovered from the backups and, using this data, establish a connection between mobile device and drone. The tool would be used to analyse the contents in the same way that Autopsy was used for the Android images, searching the file system for data and extracting it. By using this tool on the backups that were provided, what appears to be flight logs in .JSON format were recovered (Figure 113).

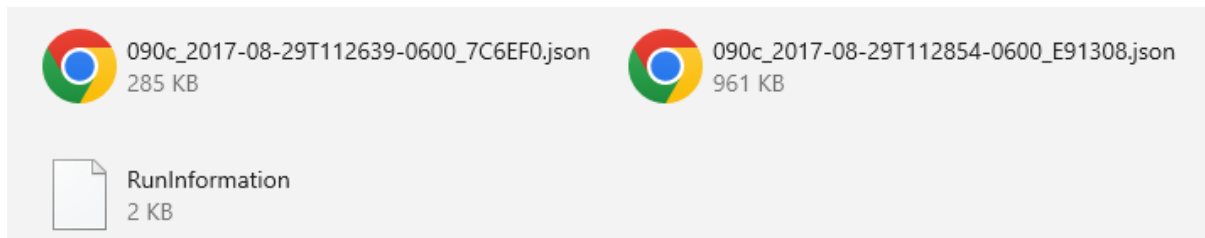


Figure 113

As with the other methods, if a tool such as this was used, further data could be recovered, and a better criminal case could be established.

To make the drone image more useful, specific artifacts should also be mentioned in the method and where to find them e.g., photos and videos. This also applies to the Android images and IOS backups. More evidence would help to strengthen any analysis and create a clearer picture of what has happened. In order to do this, more images of the Bebop 2 would need to be created for analysis to inform an updated method.

## 5. Conclusions

### 5.1. Challenges Faced

This project has come with its own set of challenges. Some were anticipated but many of them were not. Before concluding, it is important to reflect on these challenges to consider the difficulties of performing a forensic analysis on drone devices. This will help to inform any future work of these problems and develop ways of avoiding them, improving on the process set out by this paper. Eventually, through improvement, the problem posed by drone forensics may be solved.

The first difficulty faced was finding existing reports and summaries of different drones. This problem had lasting effects as two of the three drones that were analysed lacked papers that established a clear method of analysis. The method for the 'Mavic Pro' was based off of a method for the 'Mavic 2 Pro' and the 'Inspire 2' was derived from a general research paper and other DJI models. This applies to a number of different models as only the more common/popular ones seem to have a significant amount of existing data on them. This is especially apparent for any drones not produced by DJI, likely due to DJI's dominance of the market. This challenge can be partially mitigated by using websites that provide collections of scientific journals and reports but even then, there are still issues. Primarily, a lot of drones simply do not have studies on them but even some that do are locked behind a paywall which severely limits their accessibility.

One challenge that was not expected was part of acquiring the datasets used. Due to their size, a stable internet connection was necessary to download them, or the download would cancel part way through. Meaning that that process would need to start again. The successful attempt alone took several hours. This remained an issue until a wired connection was established. Even then, the files needed to be downloaded individually to accommodate.

When it came to analysing the images, one problem was organising and using the various tools that were needed. As previously mentioned, each of the reports that reviewed for this investigation recommended their own tools and techniques for analysis. In some cases, this was straightforward, such as using Autopsy to open and view images. However, when it

came to viewing the IOS backups, more than five tools were used to try and find which one worked the best. Managing this across multiple investigations/drones was difficult as the needs of each had to be met.

Only having one internal image for the “Parrot Bebop 2” posed an unexpected challenge. This was mainly due to a lack of media content, meaning that any conclusions about the location of media on the drone had to be inferred from context or research. Even then, it can only be said that such conclusions were likely as there was nothing to reference on the drone itself. Analysing the Android image helped with this as the structure and content found within filled in some of the gaps. Ideally however, more, or different, images should be considered.

The most challenging of these problems was analysing the contents of the IOS backups. Before this investigation, it was assumed that this process would be the similar to the Android images. However, this proved to not be the case. This meant that a lot of time was spent on them, trying different tools and reading articles to make the backup contents readable. It did not help that most of the articles that were consulted, focused on the contents of an Android mobile device.

## 5.2. Reflection

Within this report, a number of findings were put forward. These findings are briefly summarised below:

- Flight logs could be found in .DAT format for both DJI models. These were located on the drones, found on the internal SD images. They could also be recovered from the Android images, located within the DJI application’s folders. These were converted to csv using DatCon.
- Flight logs could be recovered from the Android images of the Parrot Bebop 2. These were found in .txt format, present within the “ACADEMY” folder. These were made readable by the tool FlyLog Converter.
- Media files were found on both of the DJI devices, within the 100MEDIA folder. These files could also be found on the Android images, within the DJI application folder.

- The recovered GPS data from the flight logs could be used to recreate accurate flight path that show where the drone was at a certain time.
- Comparisons were drawn between the findings of this report and those that it was based off. Validating the findings and providing some improvements.

As previously discussed, the process of acquiring this information was long and contained many challenges. In order to successfully complete the analyses of the drones, a number of skills were acquired or developed:

- Using a variety of tools. Google Earth, DatCon, FlyLog Converter and Autopsy were all used. Knowledge of how to use these tools effectively were developed over the course of this study.
- Method writing/creation and following a scientific process when developing and following the methods for each drone.
- Essay writing and structure when writing the report.
- Analysis and evaluation when viewing the contents of each device and determining their purpose.

As well as the findings of the report and skills that were developed, there was some other general information that was learned as part of the study:

- The general structure of the drones that were analysed, as well as the contents of the Android images.
- The structure of IOS device backups, the encryption they use and how to access them.
- How to access the information present on these devices and what it means.
- How to structure investigations like the ones for each of the drones as well as the rest of the report.

Overall, a lot of information was gathered, and lessons were learned as part of this investigation. While the investigation did not yield all the results it could have (more data for each of the mobile devices and a lack of media content for the Parrot device), enough was drawn so that an informed analysis of the methods could take place. Which was what the study aimed to do.

### 5.3. Future Work

Drone forensics is an emerging field, both for research and the technology that is being used. As such, further studies are imperative. While this paper established a lot, there are a lot more drone models out there. Even for the drones that were covered within this study, more data would only be beneficial. To achieve the end goal of establishing a standard approach for drone analysis, a number of things could be done.

First, in order to get a good base understanding, studies on the analysis of each available drone model should be collected (or conducted if none are available). While this would take a lot of work, it is necessary to account for all the variables when undertaking a project such as this. These studies could then be used to inform a structured method that can be applied to all drone devices.

Another aspect that must be improved upon for such a project to work is the tools that would be used. Currently, there is no 'best' option to view and analyse these devices. This applies mostly to the mobile devices. In order to perform an in-depth analysis, a tool that can translate IOS backups and extract relevant data needs to be developed or established for non-MAC devices. Otherwise, the cost and time required may prevent researchers from completing thorough analyses. Likewise, a standard method of analysing the Android devices needs to be established on MAC systems.

Finally, the methods that were tested in this investigation should be updated for the purposes of a thorough analysis. This would include further details about the IOS backups and new image data for the Parrot device. Similarly, it would also be beneficial to test the methods put forwards by other papers for these and other drone devices. This would help to ensure that all the information gathered is accurate.

### 5.4. Conclusion

In conclusion, the methods that were put forward in this paper all had their merits. Both methods for the DJI drones allowed for a near complete review. However, some changes need to be made to improve upon the mobile analysis. Meanwhile, the method for analysing the Parrot Bebop 2 was less effective. Changes need to be made to account for media content and IOS connections. Despite this, a considerable amount of data was extracted from each of the devices. The method for the Mavic Pro was the most valuable as

it was detailed and thorough when it came to its content, making it the most viable for use in real-world scenarios. Although both the remaining methods could also be used if the suggested changes are made, and they are subsequently reviewed. While all different, these methods provide transferrable skills and teach a lot about drone forensic analysis in general which would help when reviewing any UAS. That being said, they alone are not enough to create a standard method and more research must be undertaken in the future.



## Bibliography

Abdujalil, A. (2022). *Ukraine war: Drone pilots mark targets for new offensive* - BBC News.

<https://www.bbc.co.uk/news/world-europe-62578235>

Aloft. (2022). *Aloft - Drone Fleet Management Software & UTM Services*.

<https://www.aloft.ai/>

Android. (2022). *Android Debug Bridge (adb) | Android Developers*.

<https://developer.android.com/studio/command-line/adb>

Autopsy. (2022). *Autopsy*. <https://www.sleuthkit.org/autopsy/>

Bader, M., & Baggili, I. (2010). iPhone 3GS forensics: logical analysis using apple itunes backup utility. In *Small scale digital device forensics journal* (Vol. 4, Issue 1).

<http://digitalcommons.newhaven.edu/>

Baeldung. (2021). *The lost+found Directory in Linux and UNIX | Baeldung on Linux*.

<https://www.baeldung.com/linux/lost-found-directory>

Bouafif, H., Kamoun, F., & Iqbal, F. (2020). Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0. *International Journal of Digital Crime and Forensics*, 12(1), 35–57. <https://doi.org/10.4018/IJDCF.2020010103>

Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2018). Drone Forensics: Challenges and New Insights. *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings, 2018-January*, 1–6.

<https://doi.org/10.1109/NTMS.2018.8328747>

DatCon. (2021). *DatCon Introduction*. <https://datfile.net/DatCon/intro.html>

Davis, K. (2015). *Drone smuggles heroin from Mexico into California* - The San Diego Union-Tribune. <https://www.sandiegouniontribune.com/sdut-drone-smuggle-heroin-us-calexico-drug-2015aug12-story.html>

DJI. (2022a). *DJI GO - DJI*. <https://www.dji.com/uk/goapp>

DJI. (2022b). *DJI Matrice 600 Pro - DJI*. <https://www.dji.com/uk/matrice600-pro>

- Drone Safe. (2018). *Become a Commercial Drone Pilot in 2022*.  
<https://dronesaferegister.org.uk/blog/becoming-a-commercial-drone-pilot-in-2018>
- Elands, P. J. M., de Kraker, J. K., Laarakkers, J., & Olk, J. G. E. (2016). *Technical Aspects Concerning the Safe and Secure Use of Drones*. [www.tno.nl](http://www.tno.nl)
- Fisher, T. (2022). *Why Are Photos Stored in a DCIM Folder?* <https://www.lifewire.com/why-are-photos-stored-in-a-dcim-folder-2620570>
- Fitzpatrick, A. (2022). *How do apps store data in iPhone backups: filenames and hashes*.  
<https://reincubate.com/support/how-to/iphone-backup-files-structure/>
- Florio, F. de. (2016). *Unmanned Aircraft System RW UAS are well appreciated for their discretion and ease of use in urban environment. From: Multi-Rotor Platform-based UAV Systems, 2020 Airworthiness Requirements*.
- Global Brands. (2020). *Top 10 Drone Companies in the world - 2020 - Global Brands Magazine*. <https://www.globalbrandsmagazine.com/top-10-drone-companies-in-the-world-2020/>
- GOV.UK. (2019). *Action to detect, deter and disrupt the misuse of drones - GOV.UK*.  
<https://www.gov.uk/government/news/action-to-detect-deter-and-disrupt-the-misuse-of-drones>
- Himmat, Y. (2022). *A UAV Dynamics Model Based on Machine Learning*.
- Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, 16, 1–11. <https://doi.org/10.1016/j.diin.2015.11.002>
- Iqbal, F., Yankson, B., AlYammahi, M. A., AlMansoori, N. S., Qayed, S. M., Shah, B., & Baker, T. (2019). Drone Forensics: Examination and Analysis. In *International Journal of Electronic Security and Digital Forensics* (Issue 3). <http://researchonline.ljmu.ac.uk/>
- Juniper, A. (2022). *DJI Inspire 2 review: still the pro drone choice in 2022? | Digital Camera World*. <https://www.digitalcameraworld.com/reviews/dji-inspire-2-review>
- Kao, D. Y., Chen, M. C., Wu, W. Y., Lin, J. S., Chen, C. H., & Tsai, F. (2019). Drone forensic investigation: DJI spark drone as a case study. *Procedia Computer Science*, 159, 1890–1899. <https://doi.org/10.1016/j.procs.2019.09.361>

- Kelly, P. (2022). *Criminals “using drones to scout areas”, Police Scotland warn | The National*. <https://www.thenational.scot/news/20202850.criminals-using-drones-scout-areas-police-scotland-warn/>
- Kostadinov, D. (2019). *The mobile forensics process: steps and types - Infosec Resources*. <https://resources.infosecinstitute.com/topic/mobile-forensics-process-steps-types/>
- Kovar, D. (2015). *Drone Forensics – An Overview | Integriography: A Journal of Broken Locks, Ethics, and Computer Forensics*. <https://integriography.wordpress.com/2015/03/15/drone-forensics-an-overview/>
- Kumar, R., & Agrawal, A. K. (2021). Drone GPS data analysis for flight path reconstruction: A study on DJI, Parrot & Yuneec make drones. *Forensic Science International: Digital Investigation*, 38. <https://doi.org/10.1016/j.fsidi.2021.301182>
- Lepage, M. (2015). *What is a .PLF File And How Do I Open It in Primavera P6?* <https://www.planacademy.com/plf-file-primavera-p6/>
- Marcella, A. J. (2021). *Cyber forensics*.
- Meitav, R. (2022). *Criminal organizations step up assassinations by using drones - Israel News - The Jerusalem Post*. <https://www.jpost.com/israel-news/article-712601>
- O’Kane, S. (2019). *Parrot exits the toy drone market - The Verge*. <https://www.theverge.com/2019/7/19/20699905/parrot-exit-toy-drone-market-dji-consumers>
- Parrot. (2015). *flightplanappforbeebopdrone*.
- Parrot. (2021). *Skycontroller*.
- PhantomHelp. (2022). *DJI Flight Log Viewer - PhantomHelp.com*. <https://www.phantomhelp.com/logviewer/4EIXDN2KC5OOCMBX2B2/>
- Salamh, F. E., Karabiyik, U., & Rogers, M. K. (2019). RPAS forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon H. *Sensors (Switzerland)*, 19(15). <https://doi.org/10.3390/s19153246>

- Shackle, S. (2020). *The mystery of the Gatwick drone | Gatwick airport | The Guardian*.  
<https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone>
- SleuthKit. (2022). *Autopsy User Documentation: Data Source Integrity Module*.  
[http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/data\\_source\\_integrity\\_page.html](http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/data_source_integrity_page.html)
- Stanković, M., Mirza, M. M., & Karabiyik, U. (2021). UAV forensics: DJI mini 2 case study. *Drones*, 5(2). <https://doi.org/10.3390/drones5020049>
- Statista. (2022). • *UK: drone package delivery system market share 2018-2030 | Statista*.  
<https://www.statista.com/statistics/1279194/uk-drone-package-delivery-system-market-share/>
- Taylor, D. R. (2022). *Parrot anafi drone review: A worthy investment for beginners and pros alike | The Independent*. <https://www.independent.co.uk/extras/indybest/gadgets-tech/parrot-anafi-drone-review-b2116259.html>
- VideoStudio. (2022). *SWF File: What is a .SWF and How to I Open it?*  
<https://www.videostudiopro.com/en/pages/swf-file/>
- VTO Labs. (2022). *Drone Forensics | VTO Labs*. <https://www.vtolabs.com/drone-forensics>
- Vyas, K. (2020). *A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs)*. <https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs>
- Wide Angle Software. (2022). *Premium iPhone Backup Extractor for Windows & Mac*.  
<https://www.wideanglesoftware.com/ibackupextractor/>
- Yousef, M., & Iqbal, F. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, 16, 1–11. <https://doi.org/10.1016/j.diin.2015.11.002>
- Yousef, M., Iqbal, F., & Hussain, M. (2020). Drone Forensics: A Detailed Analysis of Emerging DJI Models. *2020 11th International Conference on Information and Communication Systems, ICICS 2020*, 66–71. <https://doi.org/10.1109/ICICS49469.2020.239530>
- Ziering, J. (2018). *Kittyhawk Insights #2 — Most Popular Drone Models | Aloft*.  
<https://www.aloft.ai/blog/most-popular-drone-models/>

