Drone Forensics: The Impact and Challenges

ATKINSON, S., CARR, G., SHAW, C. and ZARGARI, Shahrzad
<http://orcid.org/0000-0001-6511-7646>

Citation:

ATKINSON, S., CARR, G., SHAW, C. and ZARGARI, Shahrzad (2020). Drone Forensics: The Impact and Challenges. In: MONTASARI, Reza, JAHANKHANI, Hamid, HILL, Richard and PARKINSON, Simon, (eds.) Advanced Sciences and Technologies for Security Applications. Springer International Publishing, 65-124. [Book Section]

Drone Forensics: the impact and Challenges

Atkinson S.[1], Carr G.[1], Shaw C.[1] and Zargari S.[1]

[1]Sheffield Hallam University, Faculty of Science, Technology and Arts

sianatkinson15@gmail.com georgecarr97@gmail.com callumshaw12@hotmail.co.uk S.Zargari@shu.ac.uk

Abstract

Unmanned aerial vehicles (UAV) have surged in popularity over the last few years. With this, crime involving drones has also dramatically increased. Therefore, there is a dire need of successful Drone programmes that significantly would lower the amount of crime being committed involving Drone devices.

Drone forensics is a concept that is less well known or documented. Research has shown that there have been Drone Forensic programmes to support the forensics investigations, however, many have failed for a few reasons such as the lack of understanding of the technology or other limited resources. It is also known within the Digital Forensics community that Anti-Forensics techniques are constant threats and hinder investigations, resulting in less convictions.

This study aims to ascertain exactly what data can be extracted from UAV devices (Drones), the usefulness of this data, and whether consumers are able to obfuscate the data in efforts to evade detection (i.e. Anti-forensics techniques).

A number of primary and secondary datasets have been utilised in this research. Primary data includes carrying out a flight using a UAV device and consequently analysing the resulting data and an interview with a qualified Digital Forensic Analyst. Secondary data was gained from VTO Labs, recommended by NIST which was able to be interrogated in order to deliver interesting results.

This study found that Drones have the ability to hold a wealth of evidence that could potentially be very useful to assist forensics investigations. This included the flight path of the Drone, date and time of flight, altitude, home-point and alerts to inform whether the Drone was near restricted airspace such as airports (No Fly Zones).

Moreover, it was found that it is possible for the manufacturers to build in Anti-Forensics software into their devices, but it would not be possible for a consumer to utilise such techniques.

Keywords: Digital Forensics, Drones, UAV, Anti-Forensics, Mobile forensics, Drone Forensics.

Section 1 Introduction

An Unmanned Aerial Vehicle (UAV) or drone, is a pilotless aircraft that is controlled via flight software and a remote pilot. The first UAV was a quadcopter built in 1907 [17]. By 1917 developments were being made to create the Ruston Proctor Aerial Target, which is used by the army to fly bombs into enemy territories [17]. Such developments resulted in military drones that are used today. The use of unmanned aerial vehicles (drones) has soared in recent years across the UK. PWC recently reported that by 2030 there could be up to 76,000 drones operating in the UK's skies, with 628,000 jobs created within the UK economy involving drones [37].

However, this increased availability has resulted in tremendous growth of drone crime over recent years [32]. Even as far back as 2014, there were 283 drone crimes reported in the UK [43]. Some of these criminal acts include drug and weapon delivery into prisons, as well as being used to stake out homes for burglaries [13]. Drone technology is continuously evolving and is 'part of a complex digital ecosystem' [32]. This is due to the use of controllers and connected devices, meaning that it can be challenging to keep up with their many uses. This correlated with the lack of understanding within law enforcement agencies [46] about the technology.

Drones provide quick aerial views via remote pilot. The functionality and accessibility of drones has increased drone usage in various sectors such as construction, filming, photography, and estate agents who are more frequently hiring drone operators to help in commercial activities.

There has also been an increase in the recreational use of drones by hobbyist's [22]. Users fly drones remotely to capture aerial images, create films and record their experiences. Recreational drones can be purchased for approximately £400 in the UK and can be used immediately by the user after unpacking and charging the drone [42].

Due to the accessibility and usability of drones, criminals have taken advantage of their abilities to commit a vast range of crimes. In 2018, police forces across the UK reported that they had received 2,435 reports of incidents involving drones [34]. This was up 2% from previous year and a dramatic 42% higher than incidents reported in 2016 [34]. Perhaps the most high-profile case involving drones occurred in December 2018, whereby Gatwick airport closed in response to drone sightings within the surrounding airspace [22]. Flights were cancelled and delayed during the 36 hours of the closure of the airport, EasyJet reported that in total the cost of compensation reached £15m and a total of 82,000 customers were affected [22].

1.1 Unmanned Aerial Vehicles

Rouse [40] defines a drone as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UAS)[10]. Rouse [40] also states that essentially, a drone is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS.

Recently, UAVs were most often associated with the military, where they were used initially for anti-aircraft target practice, intelligence gathering and then, more controversially, as weapons platforms [40]. Drones are now also used in a wide range of civilian roles ranging from search and rescue, surveillance, traffic monitoring, weather monitoring and firefighting, to personal drones and business drone-based photography, as well as videography, agriculture and even delivery services [40].

There are various brands and designs of drones which have different components to fit the job they have been created for. Drones generally have the same or similar components to be able to function, some of which are:

- Propellers (Can be made of plastic or carbon fibre depending on the specific drone)
- Motor (The better the motor, the better that battery life of the drone)
- Receiver (Radio signals to the drone through the controller)
- Transmitter (Radio signals from the controller to the drone)
- GPS Module (Responsible for longitude, latitude, and elevation points)
- Battery (Allows the drone to fly)
- Camera (Can be inbuilt or detachable)
- Electronic Speed Controllers (Controls the speed of the drone) [1]

Similarly, any data gathered from the drones can be stored differently depending on the drone. Some drones have internal storage which varies in size from 4GB to 8GB. It is worth noting that the internal drone data will be overwritten when it has reached capacity, so it is wise to regularly check the memory and extract any data you may need. Drones also use SD or Micro SD cards, giving the user more storage capacity. There are also options such as extracting drone data to an external hard drive or even the cloud, depending on whether the data is something the pilot wants to keep.

1.2 Current Threats and Impact of UAVs

The misuse of drones poses threats to public safety, organisations, and national security due to such incidents where drones have been flown in no-fly zones. Such threats are reasons why drone forensic programs are essential in aiding the understanding of drone technology and in reducing the crime rate, especially when successful in gathering evidence for a case. However, even with the benefits a drone forensics program will bring to law enforcement agencies, this is still an area that remains relatively unexplored [5]. Drone crime can vary in threat levels, and there needs to be a more precise understanding by the public as well as law enforcement about these threats posed by drones, as drone crime is 'only limited by the imagination of the criminal' [24].

UAVs are getting more popular and accessible with consumers which makes it easier for criminals to take advantage of the technology for nefarious reasons. Drones have been used for a range of crimes from smuggling, spying/stalking, criminal damage, and even theft of card details from ATM's [34]. With all technology there is always the potential for misuse, leading to issues and negative impacts on individuals but also the community as people start to fear what the technology is capable of. With drones being adaptable and so varied, it makes the job of law enforcement even harder as they must tackle newly emerging crimes and disruptions, possibly without the necessary legislation in place for guidance.

1.3 Legal Implications

Depending on the context the drone is to be used for, there are legislations in place to outline the correct use of the drone and rules to be adhered to such as ensuring the correct licences are held for a drone. As drones were never designed for criminal use, it is impossible to create legislation to cover all possible drone crimes, as there are endless possibilities. What can be done, is to create legislation to cover the general misuse of drones; anything that causes harm or distress to the person, property, or community. This way there is a clearer line of what is unacceptable by law, therefore likely to lead to consequences. The NPCC's lead for drone crime said, 'those who choose to use drones for a criminal purpose should be in no doubt that they face serious consequences and police will use all available powers to investigate and prosecute them' [34].

Current regulations of drone fall under the Civil Aviation Act 1982 and the Air Navigation Order 2016 (amended in 2018), covering appropriate drone usage with flight restriction zones [28]]. In 2019, it was proposed that registration of all drones be mandatory with possible competency tests. The idea being that law-abiding citizens would register their drones making it easier for law enforcement to track down criminal drone use [28]]. Whilst this concept proves successful with newly registered drone users, it is not possible to ensure all drones purchased prior to the new regulations will be registered. Unfortunately, with all technology and the regulations put in place, there will be a loophole found by criminals to continue with their criminal activities.

1.4 Motivation

With the influx in use by the public, there have been reports of Drone devices being involved in criminal activity. Therefore, this study will carry out research into various crimes that have been recorded that involve such devices and how evidence gained from them aided the investigation. Additionally, this project will examine Drone devices in order to ascertain exactly what data/ evidence can be extracted from these devices and how useful they could be to an investigation.

Additionally, Anti-Forensics techniques are in existence and are at times used on devices such as PCs. This study will also look into the various techniques that are available and ascertain whether or not these techniques can be used on Drone devices.

1.5 Research Aims and Objectives

There are various aims and objectives to this study due to the collaboration of multiple projects. The research objectives are as follow:

1- Gain access to Drone data and extract using popular forensics extraction software to ascertain the usefulness of evidence.
2- Gain in-depth drone knowledge to carry out successful drone data analysis.
3- Gain information regarding the current processes used by Police Forces and other authorities to analyse the data and prevent drone crimes and how they are investigated.
4- Gain Knowledge of the various Anti-Forensics techniques that are currently available and in use by users who want to obfuscate data and determine whether these methods can be used on Drone devices.

Section 2 Existing Research

This section focuses on multiple elements relating to drones to provide a broad coverage of how technology, tools, crime, and devices affect drone technology. There are more and more research topics relating to drones, therefore, this section provides a small insight into what route the research can take into the technology. There will also be an emphasis on challenges facing the technology, whether by legislation in place, restrictions or nefarious means.

2.1 The Internet of Things (IOT)

The internet of things is described as a world where many otherwise ordinary devices are uniquely identifiable, addressable, and contactable via the internet [23]. Hegarty et al. [23] split IOT challenges into four stages: Identification, Preservation, Analysis and Presentation. Whilst Hegarty et al. [23] identify the issues IOT forensics faces, their paper does not provide insights how to deal with challenges. A further limitation of Hegarty et al. [23] paper is that it only covers the basic challenges of IOT forensics in 2014 and thus the findings are likely to be outdated. However, their study does suggest that more frameworks need to be introduced for forensic examinations of the internet of things [23].

The findings presented more recently by Conti et al. [11] are congruent with preceding work conducted by [23]. Conti et al. [11] claim the main challenges which IOT forensics face are: Evidence Identification, Collection and Preservation, Analysis and Correlation and Attribution. However, they fail to propose a framework to meet the requirements of IOT which states the challenges that forensic examiners are facing in 2018.

A review of the literature has indicated there are gaps in the knowledge surrounding IOT frameworks and procedures and thus, more work needs to be done to present a framework which considers a range of IOT devices.

2.2 UAV Devices

Whilst the definition of a drone remains constant, there are several different types of drones, which vary in size, weight, capabilities, appearance, brand, and features.

Flynt [18] breaks drones down into size; ranging from very small drones, small drones, medium drones and large drones. Additionally, Flynt [18] states drones vary with the range at which they can be flown with from some drones only being able to be flown from 5km away whereas others can be flown from as far as 650km. Drones vary in size and shape depending on their function as a drone, for whom they are targeted to be used for and the tasks they can complete.

- Quadcopters – The most popular model on the market uses four rotors positioned in each corner of the square body. This type of drone will be considered in this study as it resembles a popular choice for smuggling contraband into prisons and is used for lots of other criminal activities.
- GPS Drones – Drones which are linked to satellites via GPS, the flight direction of the drone will depend on the satellite.
- Photography Drones – These are drones which have a camera attached to the main body, they are used to take HD pictures and videos and are popular among hobbyists.
- Racing Drones – Small, fast and agile which are streamlined for speed and free of excess weight that can reach speeds of up to 60mph.

2.3 UAV Offences

The UK Civil Aviation Authority (CAA) set the rules for drone use in the UK [45].

1. Always keep your drone in sight.
2. Stay below 400ft (120m) to comply with the *drone code*.
3. Every time you fly your drone you must follow the manufacturer's instructions.
4. Keep the right distance from people and property – 150ft (50 metres) from people and properties and 500ft (150 metres) from crowds and built up areas.
5. You are responsible for each flight.
6. Stay well away from aircraft, airports and airfields when flying any drone – It is illegal to fly inside the airport's flight restriction zone without permission.

Drone crimes generally are carried out by repurposed larger drones [48] that have longer flight times, transmission distance as well as have self-adaptive flight systems that adjust flight parameters based on different payloads, such as the DJI Matrice 600 [15].

Smuggling contraband into prisons is not a new concept, however, as drones provide an effective way to smuggle more dangerous and larger items into prison grounds. Many prisons have taken an approach of non-technical solutions such as barbed wire and perimeter nets, and there are the technical solutions of installing jammers inside and on the perimeter of the prisons [41]. Agencies that have a drone forensics program will be able to use their skills to see if they can determine if any suspect drones found near prison property were carrying any contraband.

UAVs have provided criminals with new ways to carry out their crimes, such as spying and scoping potential houses to burgle [6]. Not only are drones able to store the camera footage onto a connected SD card, but there is also the option for live streaming footage, which could lead to further distress to the victim(s). An investigator needs to be able to know how to read the data they are presented with in order to provide enough evidence to support claims of the crime taking place, especially for sensitive cases.

2.4 Data Storage in Drones

Due to the various brands and designs of drones, there are different storage methods. The two main areas are the drone's internal memory, which varies in capacity depending on the drone, and SD or Micro SD slots on the drone. Depending on the drone, there is also the potential for data to be stored on the remote controller and the connected mobile devices. The descriptions below are based on the DJI Spark drone.

Drones Internal Memory - To extract the data from the drone itself, the drone needs to be connected to the laptop/virtual machine via the USB connector or the UFED Device Adapter depending on the software used for extraction. The software can either be DJI Assistant 2 or UFED 4PC. To carry out the analysis on the drone's internal memory, UFED Physical Analyser, Csv View and DatCon were used.

External SD Card - The SD that was inserted into the drone during the flight was copied to the laptop via NUIX Evidence Mover and analysed through FTK imager, where a physical image of the SD card was taken.

Remote Controller - Looking at the controller data that is held in the .DAT files, it is clear to see that there are only slight changes to the data depending on whether the drone was flown when connected to the RC or a connected mobile device. The data provided when the drone was connected to the RC provides information regarding the 'Rudder' and 'Throttle' as well as a 'Connected' identifier. The RC does not hold data that would be useful in an investigation. The examiners would need to have access to either the drone itself or the connected mobile device to collect adequate evidence to aid their investigation.

Connected Mobile Devices - For the extracted data held on the connected mobile device, the mobile device was connected to the laptop via a USB connector. This allows for viewing the file structure within the DJI GO 4 App.

2.5 Process of Drone Forensics

Drone forensics consists of various elements that allow law enforcement/private agencies to build a larger picture of how drones have been used, what evidence they hold and even make new discoveries about drone data. There are three evidence categories which need to be considered during the drone forensic process. The first category being the physical evidence, such as the aircraft, mobile devices, battery, radio controller and laptop/computer. This can relate to sensors, data links to ground stations and the flight controller. The second category is the digital evidence that relates to a drone, such as the SD/Micro SD cards, the drone itself, laptop/computer and mobile device OS (e.g. Linux, Windows, Android). This category includes file systems, media storage and firmware. The third category can be classed as miscellaneous to cover all other evidence artifacts which relate to the forensic process. This category includes social media, purchase records and even fingerprints [49].

2.5.1 Forensics Tools

Below are descriptions of various tools/software that can be used to extract and analyse drone data. Some tools/software are recognised forensic tools whereas others are free offline apps.

DJI Assistant 2 - Upon opening the DJI Assistant 2 software, there is an information box, which informs the examiner that the data will be uploaded to DJI's server before starting your data extraction. With DJI Assistant 2 the flight log data can be uploaded to a local drive, which is uploaded as .DAT files. These files are unintelligible and need to be converted to a .CSV file via DatCon to read the data.
DJI Assistant 2 has a section that provides the examiner with data held in the drone black box. When extracted, this data is encoded and can only be decoded by the DJI Company. This is due to the security of the data. The type of data held in the Black Box is used by DJI regarding user enquiries leading to investigating any issues they had during their drone flights. The data being encoded means that it will not be tampered with to affect an investigation taking place by DJI themselves.

DatCon - DatCon has the option to convert any .DAT files into a .CSV file or a .LOG file. Once the .DAT flight logs from the drone internal memory are converted into a .CSV file, it will open as an excel workbook with readable data. This data output is the most detailed flight log format found during the extraction of all the components. The data provided as part of the flight log include the 'GPS', 'Motor' and 'AirCraftCondition'.

DJI GO 4 App - The DJI GO 4 App is required to be able to control the drone from a smartphone. The app itself does provide some details about the flight taken, however not as much as that found in the drone's internal memory. The app provides the pilot with a series of interchangeable screens. It was found that the DJI GO 4 App cache held the most data out of all the components analysed. Within the mobile phone, the DJI cached files were contained in 'My Files > Internal Storage > DJI > dji.go.v4'. While the app cache holds useful data, there is a significant amount of data that is encoded. Some files can be decoded by simply converting the file format, while others are unable to be decoded. Further examination and research would be needed to determine why this is the case.

CsvView - CsvView allows .DAT, .txt, .csv or .tsv files to be uploaded into the software to identify the data held within these files. This is particularly helpful when the original files are encoded. For example, when a 'FlightRecord.txt' file is uploaded to the software the user is able to see the initial upload page, which provides data regarding the 'droneType', 'aircraftName', 'appType' and more specifically the 'aircrafSn' (serial number). This information is useful for verifying what type of drone the investigators are looking for, matching the drones given name to those held in DJI's databases and determining that an android phone is a connected device related to the drone.

Cellebrite (UFED 4PC) - The UFED 4PC software comes with a kit containing the cables and connector tips that may be needed to extract data from a range of sources. To be able to carry out the extraction, the examiners will need a Cellebrite Device Adapter as well as the Cable A with the back-tip T-100 for a DJI Spark drone.

Cellebrite (UFED Physical Analyser) - Once the extracted files are uploaded into the software, it took approximately 2 minutes for all the data to be processed and decoded. The timings will vary depending on the amount of data extracted from the drone. UFED Physical Analyser displays the data in a way that lets the examiner know where the data was found. The most crucial evidence found during the analysis of a DJI Spark drone was the battery and the aircraft serial numbers. From this small amount of evidence, the investigators would be able to get in contact with DJI to request access to any data linked with the found serial numbers, providing they have identified enough evidence to support the claim of a crime. Physical Analyser also creates a timeline of the flight. This is the first time during the analysis that a timeline has been identified; however, the timeline only displays the latest flight that was conducted, meaning that potentially important data is not detected.

2.6 Challenges in Drone Forensics

This section discusses some of the current challenges in drone forensics.

2.6.1 Anti-Forensics

As the digital age is in constant development and is an essential part of modern life, it is easy to assume that it is difficult to carry out a crime without the involvement of a digital device somewhere along the timeline. Thus, the community of digital forensics has become an integral part of criminal investigations in recent years. However, individuals have come across and created a number of applications and methods of erasing/ hiding data over the years. Such methods are referred to as 'Anti-Forensics Techniques'. Kesler states in their paper [31] that the term 'Anti- Forensics' is defined as *'Viewed generically, anti-forensics (AF) is that set of tactics and measures taken by someone who wants to thwart the digital investigation process'.* As of the time of writing this chapter there are a number of different methods of carrying out Anti- Forensics; listed below are some examples:

- **Artifact Wiping**
    - Using tools such as 'Eraser' and 'BC Wipe' to clear the slack/ unallocated space
- **Data Hiding**
    - Relocation of data- transferring data to portable device
    - Steganography
    - Altering file extensions
        - Signature analysis catches this out
- **Trial Obfuscation**
    - Modification of Metadata
        - Altering timestamps
- **Attack on Computer Forensics Tools (CFT) and processes**
    - Forensic tools are well known and well documented
        - An attacker could gain a copy of the tool and learn the ins and outs of the software, also learn its flaws
    - DoS attack

For a number of years there have been techniques used by criminals to try and obfuscate or delete evidence from devices in order to avoid detection. Jaon and Chhabra constructed a paper on the analysis of anti-forensic techniques [29] in which they document a number of well-known and widely used techniques with the intent of delaying or the destruction of investigations. The paper describes in detail each technique and gives examples of how it could be used by criminals and what types of data/ evidence can be tampered with. Techniques such as Artefact Wiping, Data Hiding, Trial Obfuscation and Attacks on Computer Forensics Tools are all thoroughly described.

Although the study provides examples and clear descriptions of various anti- forensics techniques, unfortunately there is no mention of UAV devices within the paper; instead simply stating 'Computers' and 'Digital Devices'. This is a weakness of the paper as it does not go into depth of anti-forensics in different devices, instead simply 'computers'. The term 'computers' in technical terms refers to anything electronic that carries out a calculation, so the authors could be talking about any device. However, due to the references they make (e.g. 'different files in computer are identified by their file extensions'), it is assumed that they are referring to PCs. It is unfortunate that the study does not include a section dedicated to UAV anti- forensics techniques as it would have been very useful to be included within this study.

While this paper does have flaws, it does include a lot of interesting and very useful information regarding the various anti- forensics techniques that can be utilised by the general public.

A Digital Forensic Analyst was interviewed on their knowledge regarding Digital Forensics and UAV forensics. In relation to Anti-Forensics in UAV devices, the analyst felt that it was unlikely that users would be able to implement Anti-Forensics techniques on such a device, unless the manufacturers installed one as default. A feature such as encrypting all data on a UAV device, which would mean the data could not be extracted and analysed by the investigations team. Nonetheless, a lot of the data captured and analysed when investigating a UAV device is extracted from the mobile app used to control the device. Flight paths for example are stored there. It is possible to download a scheduler on Android devices that wipes the data from apps at designated times. Thus, it could be possible for a user to install such an app and set it to delete everything from the drone app if it has not been opened in ‘x’ amount of days. This would count as an Anti-Forensic technique and is something that could be carried out by an end user. Nevertheless, it is unlikely that a standard or computer illiterate user will know about advanced features such as this; it would take an advanced ‘tech savvy’ user to carry out the technique. However, this can be said for almost any Anti-Forensic technique. The user would have to be aware of the presence of data in order to hide/ delete it.

2.7 UAV Legislation

Due to the popularity of UAV devices, it is important that their use is governed, and guidelines are set to ensure that they are used safely and securely without endangering others. The CAA [9] have issued such guidelines within The Air Navigation Order 2016 (amended March 2019) [44] in which all UAV device users must comply. The CAA collaborated with NATS [7] to develop a website called ‘Drone Safe’ [8]. The site includes an array of features including a copy of the ‘Drone Code’ (the guidelines that must be adhered when flying such devices) [9], information regarding training opportunities for beginner fliers and general resources regarding UAV devices such as the names of approved retailers and safety checklists.

In addition to the CAAs efforts, UAV device manufacturers such as DJI offer guidance on global and regional legislation [14]. The ‘Fly Safe’ page of their site allows users to select a region and country e.g. Europe, United Kingdom and information regarding current legislation will be displayed.

2.7.1 No Fly Zones

As a result of the continued disruption being caused by UAV devices around airfields, authorities have made the decision to extend the no fly zones to a total of three miles, as opposed to the previous 0.6 mile radius. Therefore, from 13th March 2019 it will be a criminal offence to fly a UAV device within three miles of an airport [4]. Failure to comply with the new law may result in the end user being charged and sent to prison for up to five years [7]. The 'Drone Code' on the Drone Safe UK site has been updated to include the updated law regarding the extension of the no fly zone surrounding airports.

In addition to the 'Drone Code' document on the site, there are other available features that can be utilised to help end users with locating restricted/ no fly zones.

It has been reported that in the U.S, drone manufacturers such as DJI have hard coded 'No Fly Zones' into their devices [47]. In the referenced example from 2017, a TFR (Temporary Flight Restrictions) had been established around an area where President Trump was to be residing. In addition, it is stated in the article that various airport airspaces have also been hard coded into the devices meaning that they would be unable to fly in that airspace; the device would either stop in its tracks and hover or would descend automatically. Nevertheless, there are reports of the existence of software constructed by Russian developers that modify a device's GPS software in order to gain access to 'no fly zones' [30]. CopterSafe is the name of the company that is able to provide members of the public with such modifications, currently a modification board for a DJI Phantom 4 stands at $200 [12]. In addition to CopterSafe, another company has been found to provide similar services when an internet search was carried out [36]. NLD appear to offer a software client that will permit users access to a number of modifications that are compatible for an array of models. However, this company charges significantly less money than the CopterSafe hardware counterpart, only requesting $34.99.

2.7.2 Airfield Restrictions Maps

Present on the Drone Safe site is a page which displays a Google map of the UK with pinpoints of the unauthorized flying zones (Figure 2.1) [8]. In addition, there are smaller maps present which display the 'no fly zones' surrounding the major airports of the UK, such as Heathrow and Manchester (Figures 2.2 and 2.3). This is a very useful resource for any UAV device flier, especially a beginner as they may not be aware of all the no fly zones and may accidently get into trouble. Trouble which would be much greater after March 2019 with the introduction of the new heavier sentences. Nevertheless, it is not only the Drone Safe UK site that offers these maps, there are a variety of other sites online that offer similar services. UAV manufacturer DJI for example offer such a service [14] along with other sites such as 'No Fly Drones' [21], however these are not governed by a professional body such as the CCA like the data from Drone safe UK; however according to the 'Contact' page of the 'No Fly Drones' site [20], the sources of information regarding the rules and airspace must be obtained from the CAA directly [22].

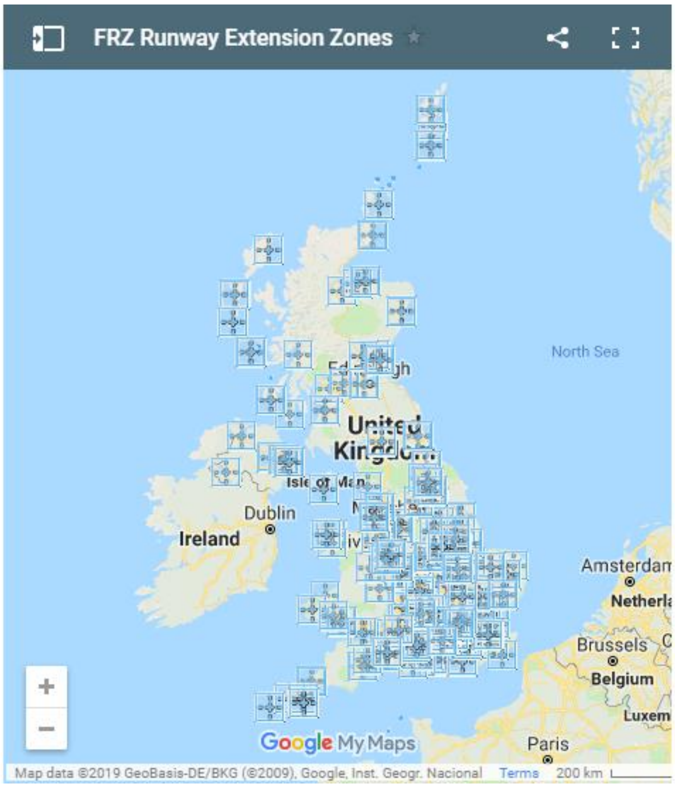
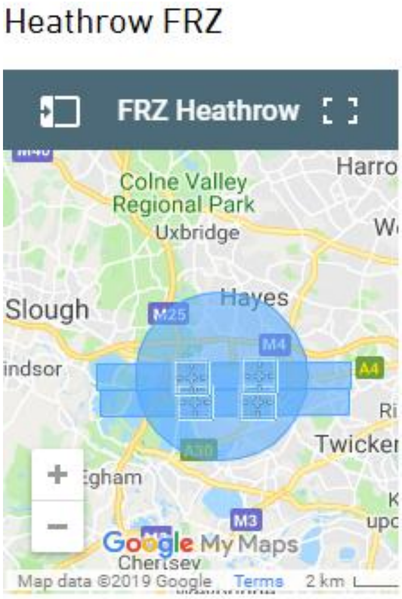


Figure 2.1- UK Flight Restrictions Map



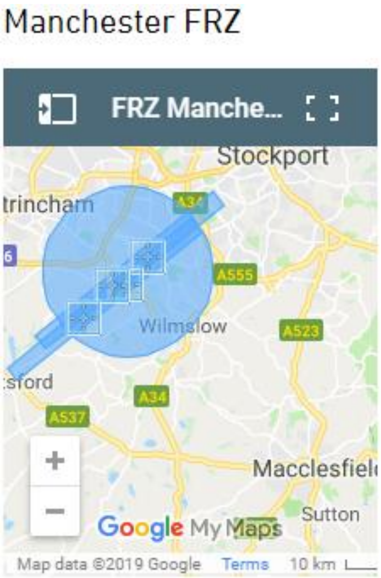


Figure 2.2- DroneSafeUK no fly zone- Heathrow Airport

Figure 2.3 DroneSafeUK no fly zone- Manchester Airport

2.7.3 Useful Mobile Safety Apps

A further feature present on the DroneSafeUK site is the description of a mobile app developed by NATS named ‘Drone Assist’ [45]. This app acts in a similar manner to the maps feature present on the website but it has enhanced features such as ‘Area Report’, to inform the user of an overview of the risks associated with flying in a specific area. Also present in the app is a feature that provides the user with weather information. This is very useful to ensure that the flight remains safe and lowers the risk of an incident.

Furthermore, the application allows users to collaborate with each other in the form of the ‘Fly Now’ feature. By utilising this function users are able to share the current location of their UAV device with other users of the app. Naturally this reduces incidents as users are aware of other UAV traffic in the vicinity [45].

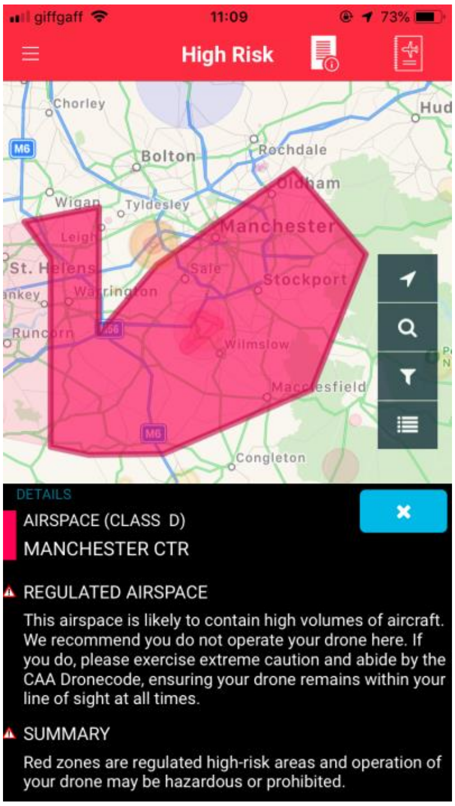
As stated, the app allows its users to gain detailed information regarding no fly zones. Figure 2.4 is an example of a 'High Risk' zone as it is surrounding Manchester Airport which naturally contains a lot of air traffic. Usefully available is a description of why the area is classified as 'High Risk'. In this figure the reason being the air space is in the vicinity of Manchester Airport. There are a number of different classifications of 'zones' (Figure 2.5) is a screenshot taken from the app which clearly describes each zone.

As useful as this application is, it does have some issues that should be addressed in the near future. It has been discussed earlier in this chapter that UAV legislation has been scrutinised and new laws will come into place from March 2019. However, this app does not make any mention to this. Upon loading the app for the first time, a message box appears stating a change in law, in July 2018 (Figure 2.6). The new laws being that it is an illegal act to fly a drone device above 400 feet without prior permission from the CAA, and that it is now illegal to fly a drone device closer than 1 kilometre from the boundary of aerodromes. As the new laws surrounding the extended 'no fly zones' does not come into place until March 2019, the content of this message box is factually correct. However, stating that from March 2019 there will be a further change in the law regarding 'no fly zones' would be a good addition; also, that higher penalties will be enforced.

2.8 Summary

In summary, there exists vast amounts of legislation and laws that must be adhered to when flying UAV devices. These laws ensure the safety of members of the public by restricting the areas where UAV device flying is permitted. It is also demonstrated in this chapter how easy the information relating to these laws and legislation are made available to UAV pilots. By distributing the free to download ‘Drone Assist’ app and the Drone SafeUK website, fliers simply have to quickly check online before flying to ensure they are not about to break any legislation/ no fly zones quickly and easily. In essence, with the relatively easy access to this information there is not really any excuse for fliers to accidentally break laws/ legislation.

In addition, it has also been stated within this chapter that UAV devices have been commercially sold in the U.S with hard coded ‘No Fly Zones’ included as default. Areas such as airports etc. The article in question was published in 2017. If this technology had been applied to all devices in the U.K at the same time, it is a possibility that the disruption to airports in 2018 would not have occurred. It is unknown by this study why the devices have not been distributed with such technology in the U.K.



AIRSPACE (CLASS D)

MANCHESTER CTR

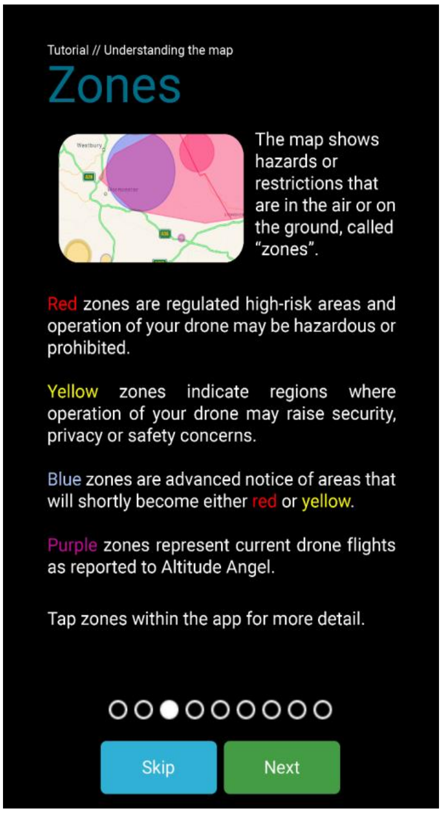
REGULATED AIRSPACE

This airspace is likely to contain high volumes of aircraft. We recommend you do not operate your drone here. If you do, please exercise extreme caution and abide by the CAA Dronecode, ensuring your drone remains within your line of sight at all times.

SUMMARY

Red zones are regulated high-risk areas and operation of your drone may be hazardous or prohibited.

Figure 2.4- Drone Assist app 'High Risk' area over Manchester Airport


Tutorial // Understanding the map

Zones

The map shows hazards or restrictions that are in the air or on the ground, called "zones".

Red zones are regulated high-risk areas and operation of your drone may be hazardous or prohibited.

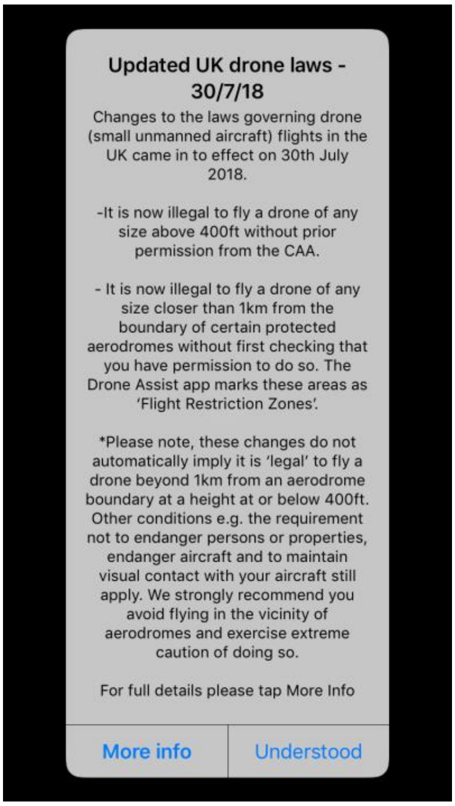
Yellow zones indicate regions where operation of your drone may raise security, privacy or safety concerns.

Blue zones are advanced notice of areas that will shortly become either red or yellow.

Purple zones represent current drone flights as reported to Altitude Angel.

Tap zones within the app for more detail.

Figure 2.5- The different classification of 'Zones' on the Drone Assist app


Updated UK drone laws - 30/7/18

Changes to the laws governing drone (small unmanned aircraft) flights in the UK came in to effect on 30th July 2018.

-It is now illegal to fly a drone of any size above 400ft without prior permission from the CAA.

- It is now illegal to fly a drone of any size closer than 1km from the boundary of certain protected aerodromes without first checking that you have permission to do so. The Drone Assist app marks these areas as 'Flight Restriction Zones'.

*Please note, these changes do not automatically imply it is 'legal' to fly a drone beyond 1km from an aerodrome boundary at a height at or below 400ft. Other conditions e.g. the requirement not to endanger persons or properties, endanger aircraft and to maintain visual contact with your aircraft still apply. We strongly recommend you avoid flying in the vicinity of aerodromes and exercise extreme caution of doing so.

For full details please tap More Info

Figure 2.6- Information on updated Drone laws

Although it is clear that authorities and manufacturers are attempting to restrict users in how and where they fly their devices, it is demonstrated in this chapter that roguish beings will try their hardest to combat these efforts and break the law.

Due to the expanding nature of drones and the constant updating and release of new models, this study will focus on the examination of the DJI Phantom 4 [16] of which no current research papers could be located. A review of the literature has indicated there are limited studies which focus on the examination of drone forensics. Thus, this study will focus on the examination of the DJI Phantom 4 to contribute to further understanding regarding drone forensics. As a result of this study, a process of examination on a DJI Phantom 4 will be proposed, in an attempt to streamline investigations. There is currently limited research relating to how drone data to proving crimes despite the rise in crimes committed with drones.

Due to the increase of drone technology, it is vital for government agencies to be able to deal with the increasing demands of the devices and have the knowledge of how to use and gather evidence from UAVs, which would benefit in investigations as well as become a useful tool to be used by the agencies. There have been several Drone Forensic Programs in the USA and UK, and while some have been successful, there have been a vast majority that have been terminated, even though drone programs would increase public safety [19]. There are two types of the programs; the first being the use of UAVs as a tool by law enforcement to aid their work, the second being where law enforcement agencies have departments dedicated to extracting evidence from UAVs used in criminal activity.

The use of UAVs as a tool by law enforcement is outside the scope of this work as it excludes essential evidence extraction and analysis skills that would be relevant to a police investigation. Therefore, this study will focus on drone data used as evidence for a police investigation. One of the reasons for these programs failures is due to a lack of understanding of UAV technology. This study will highlight a first-hand drone extraction and analysis on a DJI Spark to determine the complexity behind these processes as well as data interpretation. The study will also highlight some of the ways that drones are used for criminal activities to show how the data can support or refute criminal claims. As there is a lack of understanding in this field, there needs to be a real-life application to the analysis, to allow law enforcement agencies to know how to correctly interpret the data gathered to be successful in their investigation.

Section 3 Research Methodology

This section focuses on the research methods used as part of the projects, to show the different ways drone data can be used to draw varying conclusions. There will be focus on the questionnaire and experimental work.

3.1 Research method

As there are a vast amount of UAV device models currently on the market, it is not feasible to gain primary flight data from all of them. However, NIST (National Institute of Science and Technology) allow access to a total of thirty-two UAV images created by VTO Labs [36]. This allows for the analysis of a much wider range of devices in order to gain a clear understanding of any differences that may be present in different models and manufacturers.

Nevertheless, in order to gain a clear and concise understanding of what forensic investigators are challenged with; it is important that evidence from at least one UAV device is manually examined and analysed. Therefore, a UAV device (DJI Spark) will be taken on a number of test flights in an array of locations in order to generate good quality data to analyse. Cellebrite UFED 4PC will then be used to extract data from the device and Cellebrite Physical Analyser used to examine the data. As the UFED 4PC software houses features that exclusively extract data from UAV devices, it seems the perfect software to use for the extraction and analysis.

In addition to the use of Cellebrite software, IEF will also be used to analyse data by means of a comparison between the two tools. The comparison being an experiment of the amount of data returned by each toolkit and whether one of the tools appears to have missed some data during the extraction or decoding processes.

The extraction experiments are scheduled to take place after the interview with the forensic investigator; the reasoning being that the outcome of the interview will provide an understanding of how forensic investigation units deal with UAV devices and which methods are utilised to extract evidence from them. Thus, the extraction and handling of the test flight data as well as the data set evidence would mirror that of a real life scenario. Due to the experiments using both the VTO Labs datasets and the manual test flight data, a mixture of both primary and secondary data will be used during analysis.

During the examination of the images, it will be deduced exactly what types of evidence can be obtained from UAVs, how useful this evidence could be in given scenarios as well as ascertain if one tool is superior to another regarding analysis.

3.1.1 Freedom of Information request

The literature has indicated that the crimes committed by drone usage has increased due to the rise in drone accessibility and functionality. A freedom of information request was made to West Yorkshire Police which asked for the number of incidents made by unmanned drones. Quantitative data was attained which was categorised by incident type since the data began being recorded and the calendar year the crime was committed. As a result, the data provided an understanding as to whether there had been an increase in the number of incidents year on year, what type of categories these incidents were classified as and whether there was a need for further research in this area (Appendix a).

3.1.2 Ethical Consideration

Due to the nature of this project, the subject of ethics must be considered. Two main forms of methodology are used to gain suitable research and test data: Interviews and UAV Extractions.

In relation to the interview methodology, it is absolutely vital that the name(s) of all participants are not revealed along with the name of the police force they are associated with. As several of the questions that are to be asked are 'open ended' and open to interpretation, it is important that this is adhered to avoid any repercussions.

Concerning to the examination of the UAV data, it is important that privacy and confidentiality is maintained. As a feature of most UAV models is that of a high resolution camera, it is more than likely that individuals may have been inadvertently captured by the device. As it is more than possible for permission not to have been granted by these individuals, it is vital that any content analysed is not to be made public and be used in a purely academic manner. Nevertheless, the possibility of capturing a criminal event using the on board camera has to also be considered. Although it is highly unlikely for a criminal act to be inadvertently captured on video, it is a serious issue. Although by providing officials with the footage would be a breach of privacy, it could be a major advantage to a current investigation. If a crime such an indecent assault on a minor was captured on the device, although it would have to be reported to the Police, it could be seen as distributing child pornography. However, if the footage were not reported to the Police, the owner of the footage could be tried for the creation and possession of indecent images of minors. Nevertheless, this theory is quashed by the content of the various related legislations. Although the Protection of Children Act 1978 states that it is an offence 'to distribute or show indecent images' and 'have in his possession indecent images' [26], the Sexual Offences Act 2003 furthers the content of the 1978 act and creates a defence to this 'offence' by stating in Section 46.1A that 'the defendant is not guilty of the offence if he proves that it was necessary for him to make the photograph or pseudo- photograph for the purposes of prevention, detection or investigation of crime, or for the purposes of criminal proceedings' [27].

Therefore if a member of the public were to take content from their UAV device to a Police official stating the content and their wish for it to be investigated, it is unlikely that they would be prosecuted as they would be seen as 'distributing' the images they 'made' in the public interest and their intent to get the crime investigated. In addition to this, it would be the CPS (The Crown Prosecution Service) who would prosecute such offences and only do so if prosecution against an individual is in the public interest. It is unlikely that prosecution of an individual such as the one in this example would not be in the public interest.

3.2 Questionnaire

In order to gain a good and relevant understanding of how investigators examine UAV devices and the current protocols associated with such examinations, conducting an interview with a qualified forensic investigator from a police force is a worthy way to gain an insight into the workings of a forensic investigation unit. A mixture of qualitative and quantitative approaches will be used during the interview. By answering the questions asked, the interviewee will be able to provide a clear and concise impression of the depth of their knowledge on the subject and how useful their input will be to this study.

Before the interview with the forensic investigator commences, the interviewee must complete, sign and date the consent form to ensure that they are fully aware of the nature of the project, the risks and benefits as well as the fact that their answers and opinions would be completely anonymous.

3.2.1 Wording of Questions

In order to gain quality information from the interview, it is important that open-ended questions are asked as well as closed questions. By utilising this approach, it will allow the interviewee to provide clear, factual information such as statistics and information regarding current protocols used within forensic investigation units as well as being able to expand and express their own opinions regarding the current situation regarding the use of UAV devices and the way that the digital forensic community is adjusting to include such devices into the various protocols and investigation methods used.

3.3 Experimental work

The initial flights that took place were to be used for the primary analysis. These flights are used to identify the extraction and analysis techniques that need to be used by the examiner, as well as to determine what different data can be identified with varying methods of control. A flight was carried out via the connected mobile device, and the following flight was conducted via the DJI controller. Forensic tools and the free offline apps were installed on a LENOVO Laptop to carry out the analysis. The extraction processes were conducted through a virtual machine. By using first-hand data and not using secondary data ensures more control over the reliability of the results, as well as accounting for any variables that may have affected the data.

The main experiments were focused around two main drone crimes: smuggling and spying. The first experiment regarding smuggling was to determine how the motor data and battery data may be affected by various payloads. And how the drone movements and gimbal directions can be used in support of a ‘spying’ claim.

3.3.1 Experiment One

There have been many cases where drones have been used to smuggle phones, weapons, and drugs into prisons. Therefore, the payload tests are to determine whether it is possible to identify whether a drone has had a payload during a flight. For this scenario, various payloads were added to the drone to see what effect the added weight had on the drone’s motor and battery data. The payloads of 146g, 18g and 10g will be compared to that of a flight without a payload. The flights conducted consisted of take-off and hovering at the default take-off height of 2m for a desired time of 3 minutes.

3.3.2 Experiment Two

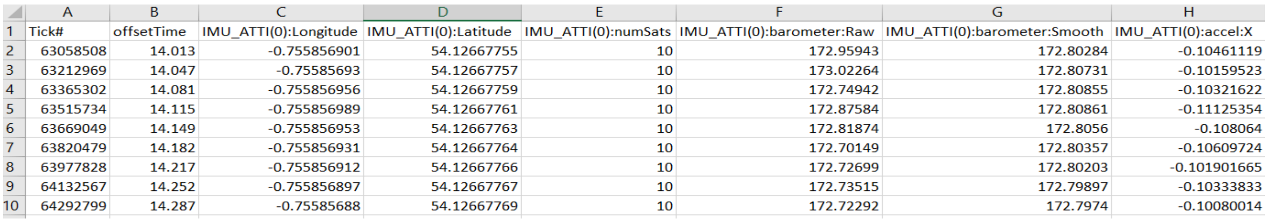
In an investigation where a claim has been made by a victim that they have been spied on by a drone, investigators want to be able to look at the data extracted from the drone and find the evidence to support or refute the claims made. For this scenario, the focus will be on the rotor movements and the camera. For the DJI Spark, the camera is located at the front of the aircraft with the gimbal having an 85° tilt range. When looking at the rotor movements, it can be determined which direction the camera was facing. The only issue is that currently, it is not possible to determine whether the camera was facing forward or tilted by the gimbal. This likely would only be determined by actual camera footage if it was taken and kept by the suspect or looking at the gimbal settings in DJI GO 4 app, which only provides limited details, provided that the settings haven’t been changed since the flight in question.

Similarly, when there is evidence to show that the suspect's drone was in fact in the area of the crime but not necessarily the suspect themselves, there can be claims that there was no footage taken, or that the camera wasn’t facing towards the victim or property. The SD containing the .jpg and .mp4 files from the camera can be examined to determine if this was the case. In the instance that the camera files have been deleted, the investigators need to be able to determine whether the camera was facing the victim or property.

3.4 Data Analysis

This section looks at how the free offline apps were used to carry out the analysis of the drone data. There will be a focus on two data components: the drone internal memory and the connected mobile device.

Internal Drone Memory - Using DatCon, the .DAT flight logs from the drone’s internal memory are converted into .CSV files, which opens as an excel workbook. This data output is the most detailed flight log format found during the extraction of all the components. Below is an example of the data from the workbook.



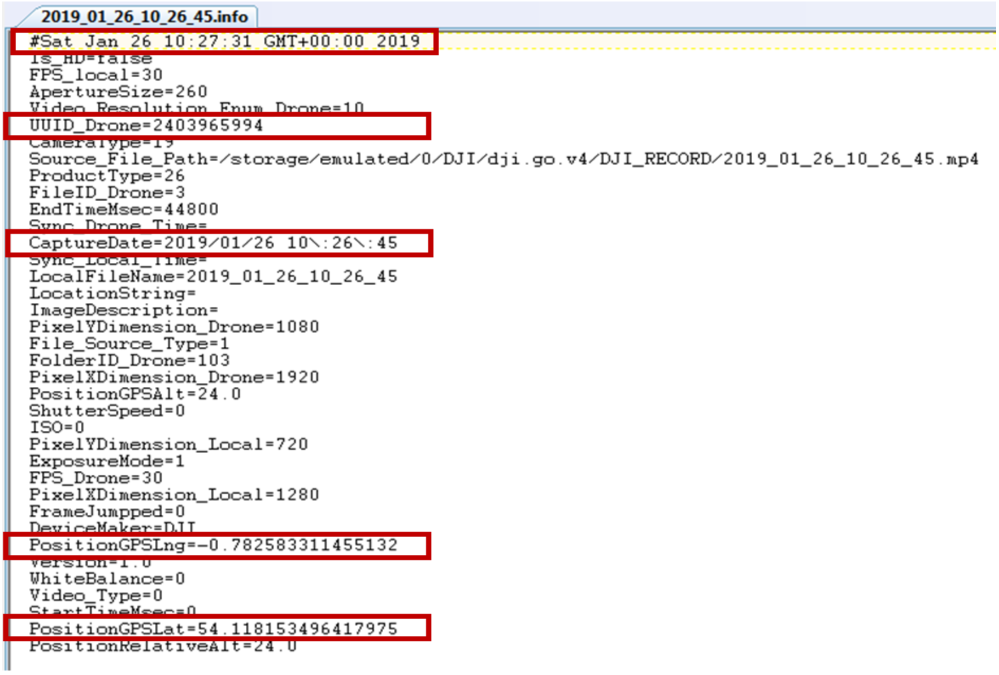
	A	B	C	D	E	F	G	H
1	Tick#	offsetTime	IMU_ATTI(0):Longitude	IMU_ATTI(0):Latitude	IMU_ATTI(0):numSats	IMU_ATTI(0):barometer:Raw	IMU_ATTI(0):barometer:Smooth	IMU_ATTI(0):accel:X
2	63058508	14.013	-0.755856901	54.12667755	10	172.95943	172.80284	-0.10461119
3	63212969	14.047	-0.75585693	54.12667757	10	173.02264	172.80731	-0.10159523
4	63365302	14.081	-0.755856956	54.12667759	10	172.74942	172.80855	-0.10321622
5	63515734	14.115	-0.755856989	54.12667761	10	172.87584	172.80861	-0.11125354
6	63669049	14.149	-0.755856953	54.12667763	10	172.81874	172.8056	-0.108064
7	63820479	14.182	-0.755856931	54.12667764	10	172.70149	172.80357	-0.10609724
8	63977828	14.217	-0.755856912	54.12667766	10	172.72699	172.80203	-0.101901665
9	64132567	14.252	-0.755856897	54.12667767	10	172.73515	172.79897	-0.10333833
10	64292799	14.287	-0.75585688	54.12667769	10	172.72292	172.7974	-0.10080014

Figure 3.1 - Drone Internal Memory, Flight Log Example

Connected Mobile Device - The DJI GO 4 App is required to be able to control the drone from a smartphone. The app itself does provide some details about the flight taken, however not as much as that found in the drone’s internal memory. The app provides the pilot with a series of interchangeable screens. In the case of a drone forensics program, the app would not be as helpful to an investigation as to have access to the data the mobile device needs to be connected to the drones WIFI. To protect the integrity of the data, the drone needs to remain disconnected to any external devices, until safe in the lab for analysis. If law enforcement were to attain the mobile device and not the drone, they would be missing the data from the app. However, the examiners would also be missing the data that is provided in the DJI GO 4 App’s cache on the connected mobile device.

The DJI GO 4 App cache held a large amount of useful data. The ‘DJI_RECORD’ folder holds any video recording taken during the flight (.mp4). The folder contains ‘.info’ files for each recording within the cache folder, which provides relevant information that would be helpful in an investigation, such as the UUID for the drone.

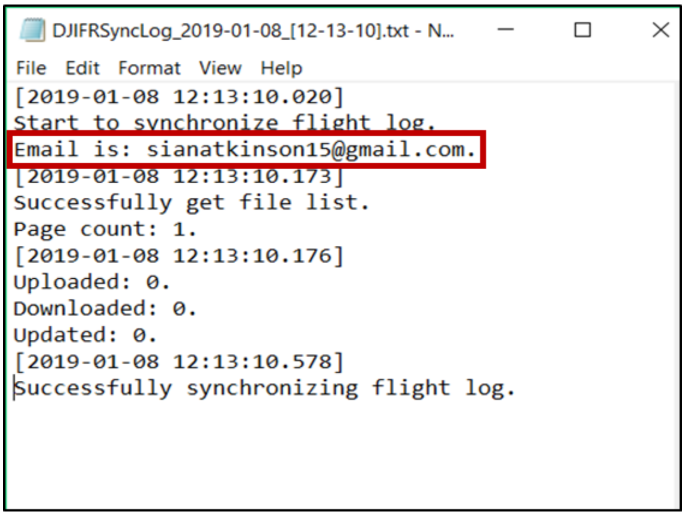
The UUID is the Unique User Identification code related to each drone pilot's DJI account, as well as the pilot’s identification and flight information. The ‘.info’ file also holds the GPS longitude and latitude locations of where the recording was taken, again providing the evidence to prove the suspect's location at the recorded time and date at the top of the .info file.



```
#Sat Jan 26 10:27:31 GMT+00:00 2019
Is_HD=false
FPS_local=30
ApertureSize=260
Video_Resolution_Enum_Drone=10
UUID_Drone=2403965994
CameraType=19
Source_File_Path=/storage/emulated/0/DJI/dji.go.v4/DJI_RECORD/2019_01_26_10_26_45.mp4
ProductType=26
FileID_Drone=3
EndTimeMsec=44800
Sync_Drone_Time=
CaptureDate=2019/01/26 10\:26\:45
Sync_Local_Time=
LocalFileName=2019_01_26_10_26_45
LocationString=
ImageDescription=
PixelYDimension_Drone=1080
File_Source_Type=1
FolderID_Drone=103
PixelXDimension_Drone=1920
PositionGPSAlt=24.0
ShutterSpeed=0
ISO=0
PixelYDimension_Local=720
ExposureMode=1
FPS_Drone=30
PixelXDimension_Local=1280
FrameJumpped=0
DeviceMaker=DJI
PositionGPSLng=-0.782583311455132
Version=1.0
WhiteBalance=0
Video_Type=0
StartTimeMsec=0
PositionGPSLat=54.118153496417975
PositionRelativeAlt=24.0
```

Figure 3.2 - DJI_RECORD .info File Content

The 'FlightRecord' folder also holds the sub-folder of 'SyncResults' which holds .txt files. As expected, this file contains the data for each synchronisation that took place. However, this file also holds the email address linked with the drone's pilot account, providing investigators with evidence of proof of ownership, as they will be able to see if the email matches that in the DJI database.



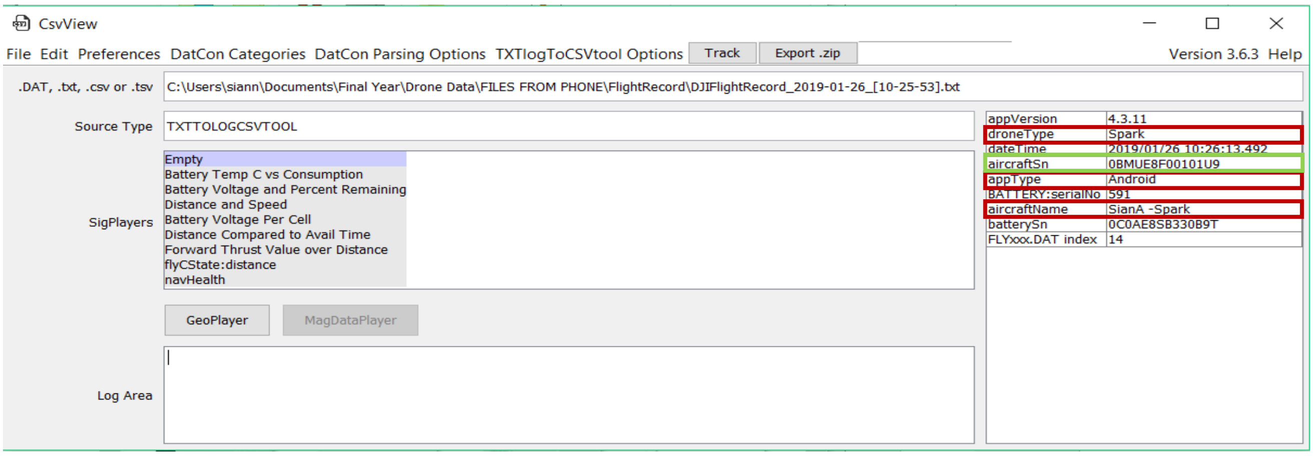
DJIFRSyncLog_2019-01-08_[12-13-10].txt - N...
File Edit Format View Help

```
[2019-01-08 12:13:10.020]
Start to synchronize flight log.
Email is: sianatkinson15@gmail.com.
[2019-01-08 12:13:10.173]
Successfully get file list.
Page count: 1.
[2019-01-08 12:13:10.176]
Uploaded: 0.
Downloaded: 0.
Updated: 0.
[2019-01-08 12:13:10.578]
Successfully synchronizing flight log.
```

Figure 3.3 - DJI 'FlightRecord' > 'SyncResults' File Content

The 'FlightRecord' folder also holds individual .txt files which are unintelligible. These .txt files were uploaded to CsvView to convert to a .CSV file to read the data. The initial upload page provides data regarding the 'droneType', 'aircraftName', 'appType' and more specifically the 'aircrafSn' (serial number). This information is useful for verifying what type of drone the investigators are looking for, matching the drones given name to those held in DJI's databases as well as determining that an android phone is a connected device related to the drone.

The option ‘GeoPlayer’ opens a new window showing a map of the flight path (Figure 3.5).


CsvView
File Edit Preferences DatCon Categories DatCon Parsing Options TXTlogToCSVtool Options
Track
Export .zip
Version 3.6.3 Help
GeoPlayer
MagDataPlayer
Log Area

.DAT, .txt, .csv or .tsv: C:\Users\siann\Documents\Final Year\Drone Data\FILES FROM PHONE\FlightRecord\DJIFlightRecord_2019-01-26_[10-25-53].txt

Source Type: TXTTOLOGCSVTOOL

SigPlayers:
Empty
Battery Temp C vs Consumption
Battery Voltage and Percent Remaining
Distance and Speed
Battery Voltage Per Cell
Distance Compared to Avail Time
Forward Thrust Value over Distance
flyCState:distance
navHealth

appVersion	4.3.11
droneType	Spark
dateTime	2019/01/26 10:26:13.492
aircraftSn	0BMUE8F00101U9
appType	Android
BATTERY:serialNo	591
aircraftName	SianA -Spark
batterySn	0C0AE8SB330B9T
FLYxxx.DAT index	14

Figure 3.4 - CsvView .txt Flight Log Upload

The map has highlighted options that link with different aspects on the map. ‘AC Path’ refers to the path taken by the drone itself (RED). ‘Tablet/RC’ refers to the path taken by the RC and we can assume the pilot (GREEN). ‘HomePoint’ is used to identify the take-off point of the drone (H).

The ‘AC Attitude: Yaw’ refers to the direction the drone is facing; this is displayed by the small green beam linked to the ‘A’.

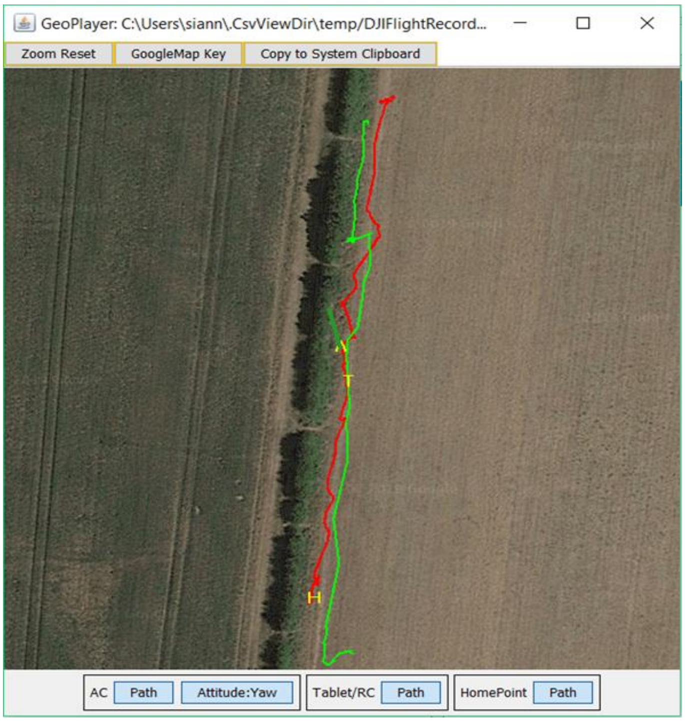
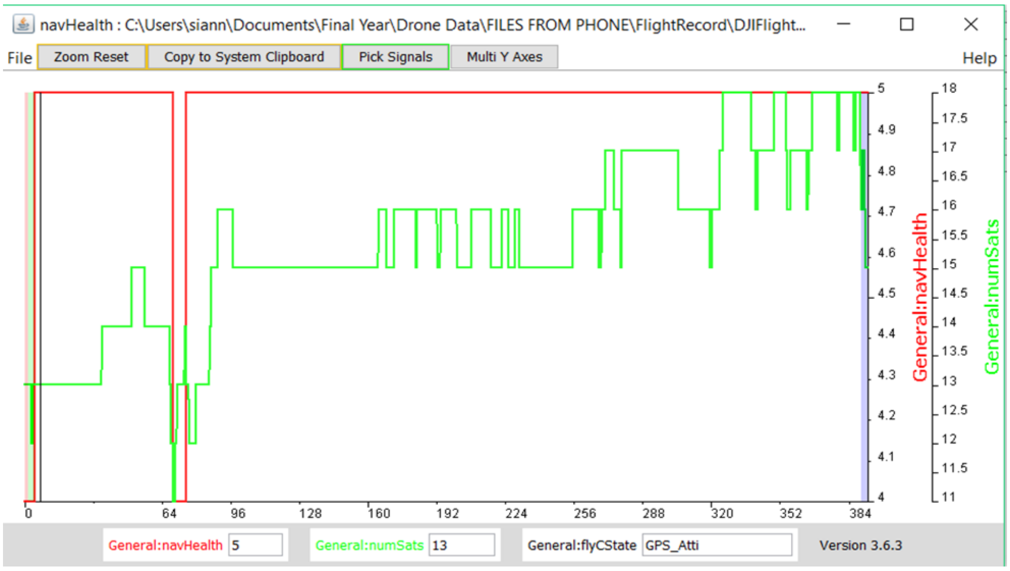


Figure 3.5 - Csv Geo Player Flight Map

The section for ‘SigPlayers’ (Figure 3.6) displays a graph of the flight ‘General:navHealth’ and ‘General:numSats’. The ‘T’ and ‘A’ on the ‘GeoPlayer’ map will move with the corresponding actions on the ‘SigPlayers’ graph. By going to the ‘Pick Signals’ option on the graph, it will open a new window of signals that can be displayed on the graph when uploaded. There are two types of signals to choose from; these are ‘StateSignals’ and ‘TimeSeriesSignals’.



General:navHealth 5

General:numSats 13

General:flyCState GPS_Atti

Version 3.6.3

Figure 3.6 - Csv Sig Players Default Graph

Section 4 Results and Discussion

This section focuses on the results from both the questionnaire and experimental work and what can be interpreted from the results.

4.1 Questionnaire Result

In order to gain a good and relevant understanding of how investigators examine UAV devices and the current protocols associated with such examinations, conducting an interview with a qualified forensic investigator from a police force is a worthy way to gain an insight into the workings of a forensic investigation unit. A mixture of qualitative and quantitative approaches will be used during the interview. By answering the questions, the interviewee will be able to provide a clear and concise impression of the depth of their knowledge on the subject and how useful their input will be to this research.

4.1.1 Interview with Digital Forensic Analyst

In order to gain a clear understanding of the current protocols, procedures and knowledge surrounding UAV devices in a forensic investigation environment, an interview was sought from a Digital Forensics Analyst working for a regional police force. By coincidence, as well as being employed by a regional police force, the interviewee is an associate lecturer at an institution teaching a module called 'Investigative Forensics'. By attending their lectures, a good idea of their capabilities and knowledge of the subject of digital forensics was gained. It was clear from these sessions that the interviewee was extremely well informed and was more than capable of providing quality responses to the questions provided. Although the digital forensics analyst stated that they did not house a vast amount of knowledge on UAV devices, it was clear that their input would be extremely valuable to this project. The interview took place on 27th February 2019 and took approximately one hour to complete.

In the interview, a range of questions surrounding UAV/ Drone devices were asked to the analyst using both open and closed question methodology. The analyst has not had a terribly long career in digital forensics, having only worked in the sector for a total of approximately four years, but in that time has gained a lot of knowledge and experience in the field. However, it is stated in the interview that they are not an expert in the field of drone forensics. In fact, it is so rare that the department get such a device in for analysis, it is an exciting occurrence for all members of the digital forensics team. Thus, it is not an everyday occurrence. As stated, the analyst has worked in a Digital Forensics environment for approximately four years and is currently only aware of around three devices ever coming in for data extraction/ analysis. On average, maybe one per year.

When asked about the types of crime that UAV devices are involved in, it is stated that every one of the cases they are aware of have been involved in drug related crimes. An example of such a case would be the investigation of a drone device that was found crashed in the vicinity of a prison. Officials wanted to ascertain where the device was flying from, when it did so and whether or not a payload was attached. In essence, whether or not the device was being used in a malicious manner i.e. delivering contraband into prisons, or just simply happened to be flying within the area of the prison. Both of which are illegal acts. The result being the latter. A second case example is also drug related, but the analyst did not work closely on the case, but simply knew about it; as stated previously it is a culture within the department to be up to date regarding the process of extraction and analysis of drone devices.

In addition to these questions, queries regarding knowledge of current legislation were also asked. As stated previously, there are vast amounts of laws and legislation being implemented surrounding UAV devices and as of the time of writing, the lack of appropriate laws surrounding drones is a very current issue. Therefore, it was a surprise to learn that the analyst did not have a lot of knowledge on these devices and even less on legislation. When asked about the area of legislation, the analyst was not able to provide distinctive answers regarding the legislation currently in place or due to be implemented. This was a surprise as it was thought when constructing the questions to ask that it would be a requirement by Digital Forensics department for all personnel to keep up to date with current legislation of digital devices to ensure they are aware of them. Nevertheless, this was proved to be a false assumption. It was deduced that investigation personnel are not required to keep up to date on laws and legislation but ‘learn them as they go’. Although they are aware of legislation such as RIPA (Regulation of Investigatory Powers Act) [25], it is not something that is used every day.

However, it is also stated that in a lot of cases that do, or in the future, will involve drone devices, they will be dispatched straight away to the CAA for investigation at their specialist forensic investigation department. In addition to this, the analyst stated that by the time devices get to their department, whichever type of device it may be, issues relating to legislation are generally already dealt at the beginning of the evidence chain. Therefore, it is understandable why the force may not be willing to spend public funds sending its personnel on training courses when it is not viable with the amount of tasks they are asked to carry out which include legislation.

Although it seems forensic investigators/ analysts are not required to know legislation relating to their devices, they are required to adhere to the four ACPO principles. It is suggested by [38] that these principles are not up to scratch for examination of modern devices and are not applicable in the slightest to UAV devices. Consequently, this was put to the analyst during the interview to gain their personal views on the theory and recommendation. The outcome of this question was a contradiction to the paper. The analyst's personal view is that the ACPO guidelines are still very relevant to modern investigations. One argument that was agreed was that on modern mobile devices, data is changed as soon as the device is powered on; therefore, breaking the first rule in the set of guidelines. Nevertheless, it was reasoned that the second rule of 'if original data must be changed, the investigator must be competent to do so', and that if the investigator is not competent, they should not be carrying out an examination in the first place. The third rule of 'make notes' is also still a very current and necessary task to undertake. However, they stated that they would remove or amend the final rule of 'the officer in charge is in charge' as it does not make much sense. A very well-made argument in favour of the ACPO guidelines was made by the analyst during the interview. However, if this rule were to be removed or altered drastically, it could result in the investigating personnel becoming solely responsible for the law and principles being followed. Although investigators should always be anally retentive in ensuring this, the removal of the final ACPO principle may lead to investigators becoming lacks in enforcing them.

In relation to the section of the said conference paper where it is recommended that UAV devices gain their own set of principles/ guidelines; the analyst disagreed with the recommendation. Stating that it was a 'slippery slope' as almost every device is different, in particular mobile devices, and could lead to having hundreds of different sets of ACPO principles. This is a valid point as mobile devices can be seen to 'break' the guidelines just as much as UAVs. Therefore, it could lead to a set of guidelines for mobile devices, of which many operate differently which could lead to a set of principles for every model of device which would be unsustainable by DFUs.

Finally, the analyst was questioned about Anti-Forensics techniques. According to the interviewee, Anti-Forensics techniques are encountered at regular intervals when investigating devices, especially PCs. Popular techniques used by end users are apparently tools such as 'CCleaner', 'BitLocker' and 'VeraCrypt'. These tools have the ability to forensically wipe everything or encrypt the data from storage to make extracting data from them near to impossible for investigators. Although it is possible for investigators to gain a RIPA 49 order (essentially forces the suspect to reveal their password or face a two year custodial sentence), it is not an easy task as the order has to be signed off by a judge in court who has to be satisfied that everything has been done by investigators to attempt to gain the data from the device. The consequences of not complying with a RIPA 49 order, although could act as a deterrent and 'scare' suspects to reveal their credentials, could also act as a means of lowering the suspect's sentence. The reasoning behind this being that if the entire prosecution case relied upon the content of the 'locked' device, the suspect could simply take the two years' imprisonment instead of revealing the content of their device and risk gaining a longer custodial sentence.

In relation to Anti-Forensics in UAV devices, the analyst felt that it was unlikely that users would be able to implement Anti-Forensics techniques on such a device, unless the manufacturers installed one as default. A feature such as encrypting all data on a UAV device, which would mean the data could not be extracted and analysed by the investigations team. Nonetheless, a lot of the data captured and analysed when investigating a UAV device is extracted from the mobile app used to control the device. Flight paths for example are stored there. It is possible to download a scheduler on Android devices that wipes the data from apps at designated times. Thus, it could be possible for a user to install such an app and set it to delete everything from the drone app if it has not been opened in ‘x’ amount of days. This would count as an Anti-Forensic technique and is something that could be carried out by an end user. Nevertheless, it is unlikely that a standard or computer illiterate user will know about advanced features such as this; it would take an advanced ‘tech savvy’ user to carry out the technique. However, this can be said for almost any Anti-Forensic technique. The user would have to be aware of the presence of data in order to hide/ delete it.

4.2 Experimental work

As well as analysing drone data, multiple experiments were conducted to create a link with 2 main drone crimes. This is to show how the drone data can support or refute claims of a crime. For these experiments, smuggling and spying were the drone crimes chosen. Below explains the outcome of the experiments.

4.2.1 Smuggling Contraband

The flight logs provide data showing changes to the battery and motor data. The most significant changes to that data come from the 146g payload flight. This outcome is to be expected due to the fact the payload was just under half the weight of the DJI Spark drone itself, therefore, to fly with the excess weight, the drone motors needed to use more power. The expectation for this flight was that the payload would be too much extra weight meaning the drone would not be able to take off.

However, this was not the case. Looking at the data for the motor speeds it's clear to see how the drone used the motors to balance out the added weight to gain altitude. Some of the data didn’t show any considerable differences from the no payload flight and the 18g and 10g payload flights, such as the ‘motor voltage_output’, which remained in the range of 9.3 to 9.6. The 146g payload ‘motors voltage_output’ ranged from 31.3 to 87, showing significant difference to the amount of power needed to adapt to the added weight of the payload.

4.2.2 Spying Claims

By examining the flight log in CsvView, it’s clear to see the flight path, as well as the path taken by the RC/pilot. For the spark drone, the maximum transmission distance from the drone to the controller is 1.2 miles. For this experiment, the pilot isn’t in the vicinity of the drone when the flight ends, meaning there is a possibility the accused would remain a suspect of the crime.

The DJI Spark drone has a 2-axis mechanical stabilisation system (pitch and roll), as well as a controllable gimbal range of -85° to 0° (pitch). Pitch, yaw and roll are based on the drone’s rotor movements and can be useful to determine the location the drone’s camera was facing at this time of the crime. The yaw axis shows the investigator the direction the drone was facing during the flight, which in turn indicates the direction the camera was facing due to the camera on the Spark drone being located at the front.

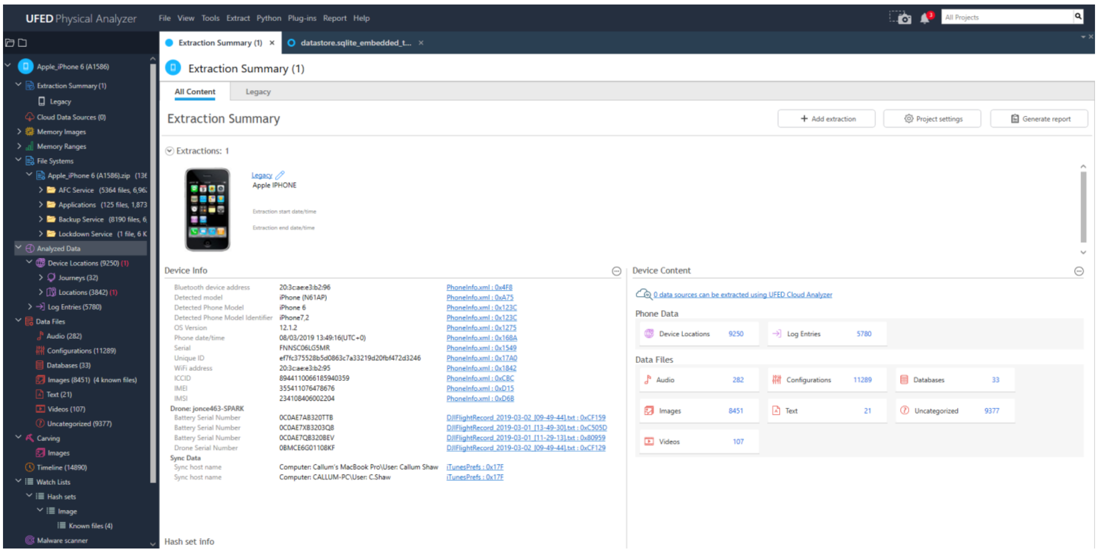
Using CsvView, the investigators can determine which direction the camera was facing at the time of the reported crime. In this experiment the yaw axis is facing in a different direction to where the drone is being flown.

4.3 Data Analysis

As mentioned previously, a mixture of both Primary and Secondary data was gained in relation to UAV devices. This includes flight data, logs, contents of on board storage etc. This data has been processed and analysed in order to ascertain what types of data is available on the devices and how useful this data could be to an investigation. Also, as the data includes varying device models of UAV, it is interesting to see whether the amount of data exported from these devices differs by manufacturer and/ or model.

4.3.1 Drone DJI Go 4

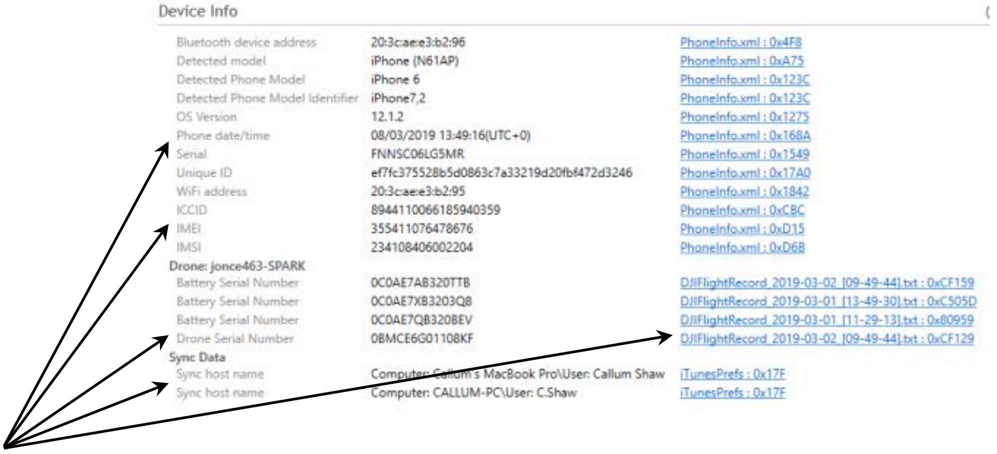
Below are screenshots of location logs and maps that have been extracted from the DJI GO 4 app of the mobile device used to fly the device. Cellebrite Physical Analyser is used to extract the data from the mobile device. This is the data relating to the UAV device that was flown personally and was not gained from the NIST dataset.



Device Info

Bluetooth device address	20:3c:ae:e3:b2:96	PhoneInfo.xml : 0x4F8
Detected model	iPhone (N61AP)	PhoneInfo.xml : 0xA75
Detected Phone Model	iPhone 6	PhoneInfo.xml : 0x123C
Detected Phone Model Identifier	iPhone7,2	PhoneInfo.xml : 0x123C
OS Version	12.1.2	PhoneInfo.xml : 0x1275
Phone date/time	08/03/2019 13:49:16(UTC+0)	PhoneInfo.xml : 0x168A
Serial	FNNSC06LG5MR	PhoneInfo.xml : 0x1549
Unique ID	ef7fc375528b5d0863c7a33219d20fbf472d3246	PhoneInfo.xml : 0x17A0
WiFi address	20:3c:ae:e3:b2:95	PhoneInfo.xml : 0x1842
ICCID	8944110066185940359	PhoneInfo.xml : 0xCBC
IMEI	355411076478676	PhoneInfo.xml : 0xD15
IMSI	234108406002204	PhoneInfo.xml : 0xD6B
Drone: jonce463-SPARK		
Battery Serial Number	0C0AE7AB320TTB	DJIFlightRecord_2019-03-02_[09-49-44].txt : 0xCF159
Battery Serial Number	0C0AE7XB3203Q8	DJIFlightRecord_2019-03-01_[13-49-30].txt : 0xC505D
Battery Serial Number	0C0AE7QB320BEV	DJIFlightRecord_2019-03-01_[11-29-13].txt : 0x80959
Drone Serial Number	0BMCE6G01108KF	DJIFlightRecord_2019-03-02_[09-49-44].txt : 0xCF129
Sync Data		
Sync host name	Computer: Callum's MacBook Pro\User: Callum Shaw	iTunesPrefs : 0x17F
Sync host name	Computer: CALLUM-PC\User: C.Shaw	iTunesPrefs : 0x17F

*Figure 4.1 STYLEREF 1 \s 5. SEQ Figure * ARABIC \s 1 1- Extraction summary of mobile device.*

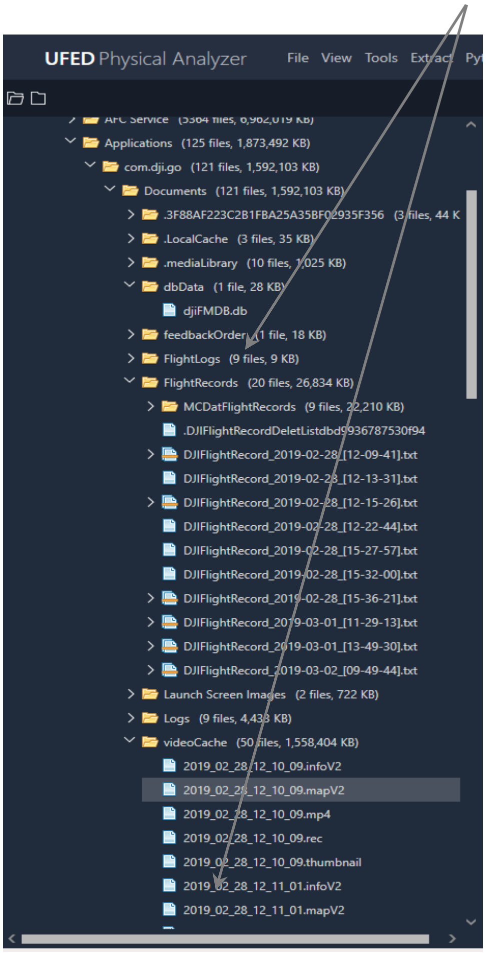

Device Info

Bluetooth device address	20:3c:ae:e3:b2:96	PhoneInfo.xml : 0x4F8
Detected model	iPhone (N61AP)	PhoneInfo.xml : 0xA75
Detected Phone Model	iPhone 6	PhoneInfo.xml : 0x123C
Detected Phone Model Identifier	iPhone7,2	PhoneInfo.xml : 0x123C
OS Version	12.1.2	PhoneInfo.xml : 0x1275
Phone date/time	08/03/2019 13:49:16(UTC+0)	PhoneInfo.xml : 0x168A
Serial	FNNSC06LG5MR	PhoneInfo.xml : 0x1549
Unique ID	ef7fc375528b5d0863c7a33219d20fbf472d3246	PhoneInfo.xml : 0x17A0
WiFi address	20:3c:ae:e3:b2:95	PhoneInfo.xml : 0x1842
ICCID	8944110066185940359	PhoneInfo.xml : 0xCBC
IMEI	355411076478676	PhoneInfo.xml : 0xD15
IMSI	234108406002204	PhoneInfo.xml : 0xD6B
Drone: jonce463-SPARK		
Battery Serial Number	0C0AE7AB320TTB	DJIFlightRecord_2019-03-02_[09-49-44].txt : 0xCF159
Battery Serial Number	0C0AE7XB3203Q8	DJIFlightRecord_2019-03-01_[13-49-30].txt : 0xC505D
Battery Serial Number	0C0AE7QB320BEV	DJIFlightRecord_2019-03-01_[11-29-13].txt : 0x80959
Drone Serial Number	0BMCE6G01108KF	DJIFlightRecord_2019-03-02_[09-49-44].txt : 0xCF129
Sync Data		
Sync host name	Computer: Callum's MacBook Pro\User: Callum Shaw	iTunesPrefs : 0x17F
Sync host name	Computer: CALLUM-PC\User: C.Shaw	iTunesPrefs : 0x17F

Figure 4.2- Extraction Summary of mobile device used during test flight

The above screenshots (Figure 4.1 & 4.2) show the 'Extraction Summary' of the mobile device used to carry out the test flight of the obtained UAV device. The extraction summary tab itself contains a lot of useful information regarding the related devices. For example, it is easy to ascertain uniquely identifiable information such as the mobile device's Serial Number and IMEI number. Also visible is the name(s) of the computer(s) used to sync data. However, most importantly, information relating to the UAV device used is displayed. The Serial Number of the UAV device and the batteries used are displayed. Very useful information for investigators. Also present are the files that the data was found in, more useful information for investigators.

In addition to these useful artefacts, Physical Analyser also has the ability to examine the device's file system (Figure 4.3). After utilising this feature, it is found that the DJI GO 4 app's folders within the file system house some extremely useful items. For example, it seems that the app caches video files recorded by the device and stores them in the 'videoCache' folder of the file system. Present also are an array of video files (.mp4) which it is assumed were recorded on the UAV device test flights, due to the file name being a date. Also present in the same folder are files with the extensions '.mapv2' and '.infoV2'. Although the description of these extensions is unknown, it is assumed that the content would contain data regarding the flight path of that particular flight. The various different information objects that could be gained from the file system could assist investigators to match the mobile device to a specific UAV device.



```
  AFC Service   (5364 files, 6,962,019 KB)
  Applications   (125 files, 1,873,492 KB)
    com.dji.go   (121 files, 1,592,103 KB)
      Documents   (121 files, 1,592,103 KB)
        .3F88AF223C2B1FBA25A35BF02935F356   (3 files, 44 K
        .LocalCache   (3 files, 35 KB)
        .mediaLibrary   (10 files, 1,025 KB)
        dbData   (1 file, 28 KB)
          djiFMDB.db
        feedbackOrder   (1 file, 18 KB)
        FlightLogs   (9 files, 9 KB)
        FlightRecords   (20 files, 26,834 KB)
          MCDatFlightRecords   (9 files, 22,210 KB)
          .DJIFlightRecordDeletListdbd9936787530f94
          DJIFlightRecord_2019-02-28_[12-09-41].txt
          DJIFlightRecord_2019-02-28_[12-13-31].txt
          DJIFlightRecord_2019-02-28_[12-15-26].txt
          DJIFlightRecord_2019-02-28_[12-22-44].txt
          DJIFlightRecord_2019-02-28_[15-27-57].txt
          DJIFlightRecord_2019-02-28_[15-32-00].txt
          DJIFlightRecord_2019-02-28_[15-36-21].txt
          DJIFlightRecord_2019-03-01_[11-29-13].txt
          DJIFlightRecord_2019-03-01_[13-49-30].txt
          DJIFlightRecord_2019-03-02_[09-49-44].txt
        Launch Screen Images   (2 files, 722 KB)
        Logs   (9 files, 4,433 KB)
        videoCache   (50 files, 1,558,404 KB)
          2019_02_28_12_10_09.infoV2
          2019_02_28_12_10_09.mapV2
          2019_02_28_12_10_09.mp4
          2019_02_28_12_10_09.rec
          2019_02_28_12_10_09.thumbnail
          2019_02_28_12_11_01.infoV2
          2019_02_28_12_11_01.mapV2
```

Figure 4.3- Extract from the mobile device's file system.

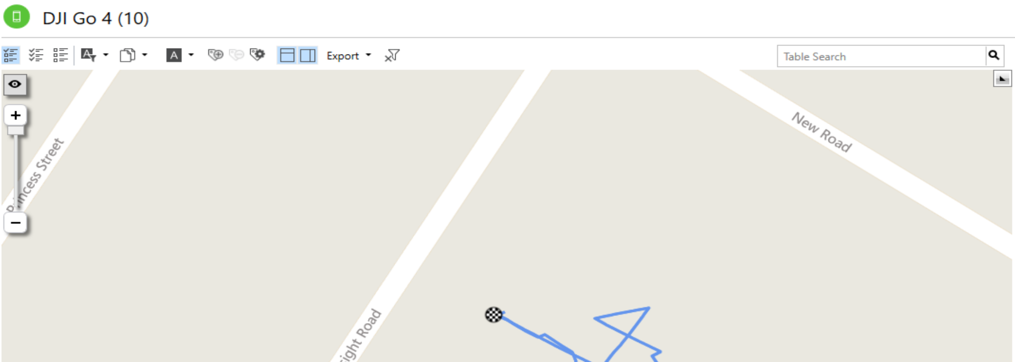
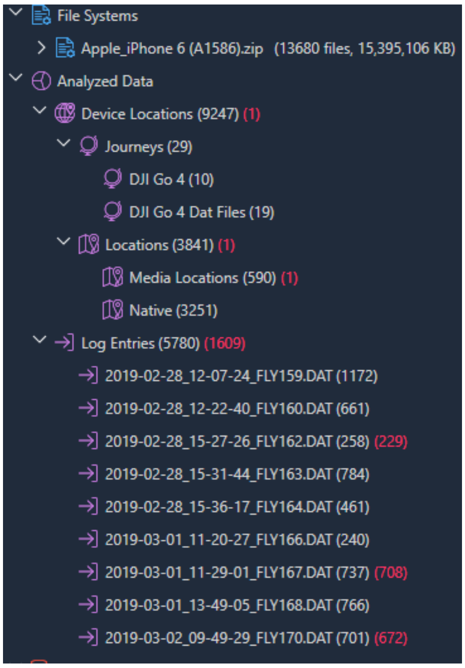


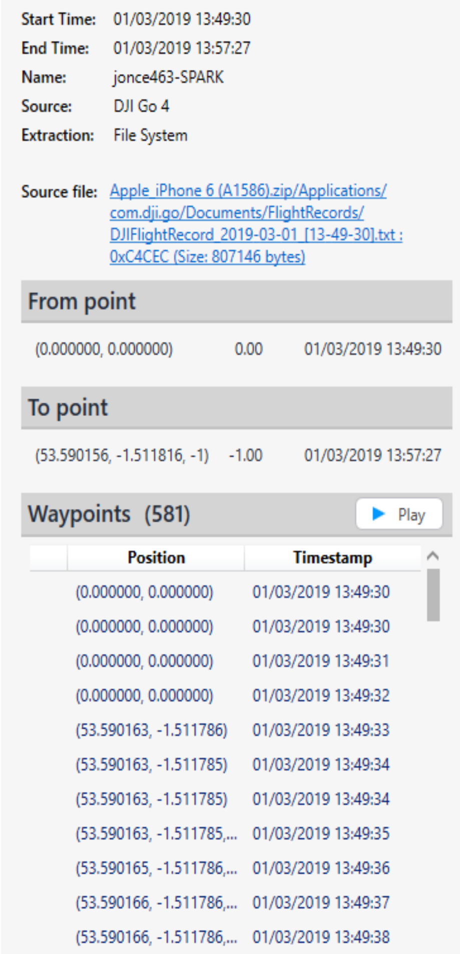
Figure 4.4- Physical Analyser map of test flight

The screenshots below display the contents of the analysed data of the DJI Go 4 app. The user is able to view logs made by the app during use.



- File Systems
  - Apple_iPhone 6 (A1586).zip (13680 files, 15,395,106 KB)
- Analyzed Data
  - Device Locations (9247) (1)
    - Journeys (29)
      - DJI Go 4 (10)
      - DJI Go 4 Dat Files (19)
    - Locations (3841) (1)
      - Media Locations (590) (1)
      - Native (3251)
  - Log Entries (5780) (1609)
    - 2019-02-28_12-07-24_FLY159.DAT (1172)
    - 2019-02-28_12-22-40_FLY160.DAT (661)
    - 2019-02-28_15-27-26_FLY162.DAT (258) (229)
    - 2019-02-28_15-31-44_FLY163.DAT (784)
    - 2019-02-28_15-36-17_FLY164.DAT (461)
    - 2019-03-01_11-20-27_FLY166.DAT (240)
    - 2019-03-01_11-29-01_FLY167.DAT (737) (708)
    - 2019-03-01_13-49-05_FLY168.DAT (766)
    - 2019-03-02_09-49-29_FLY170.DAT (701) (672)

Figure 4.4- Extract of the DJI GO 4 app's file system.



Start Time:	01/03/2019 13:49:30
End Time:	01/03/2019 13:57:27
Name:	jonce463-SPARK
Source:	DJI Go 4
Extraction:	File System
Source file:	Apple_iPhone 6 (A1586).zip/Applications/com.dji.go/Documents/FlightRecords/DJIFlightRecord_2019-03-01_[13-49-30].txt : 0xC4CEC (Size: 807146 bytes)

From point

(0.000000, 0.000000) 0.00 01/03/2019 13:49:30

To point

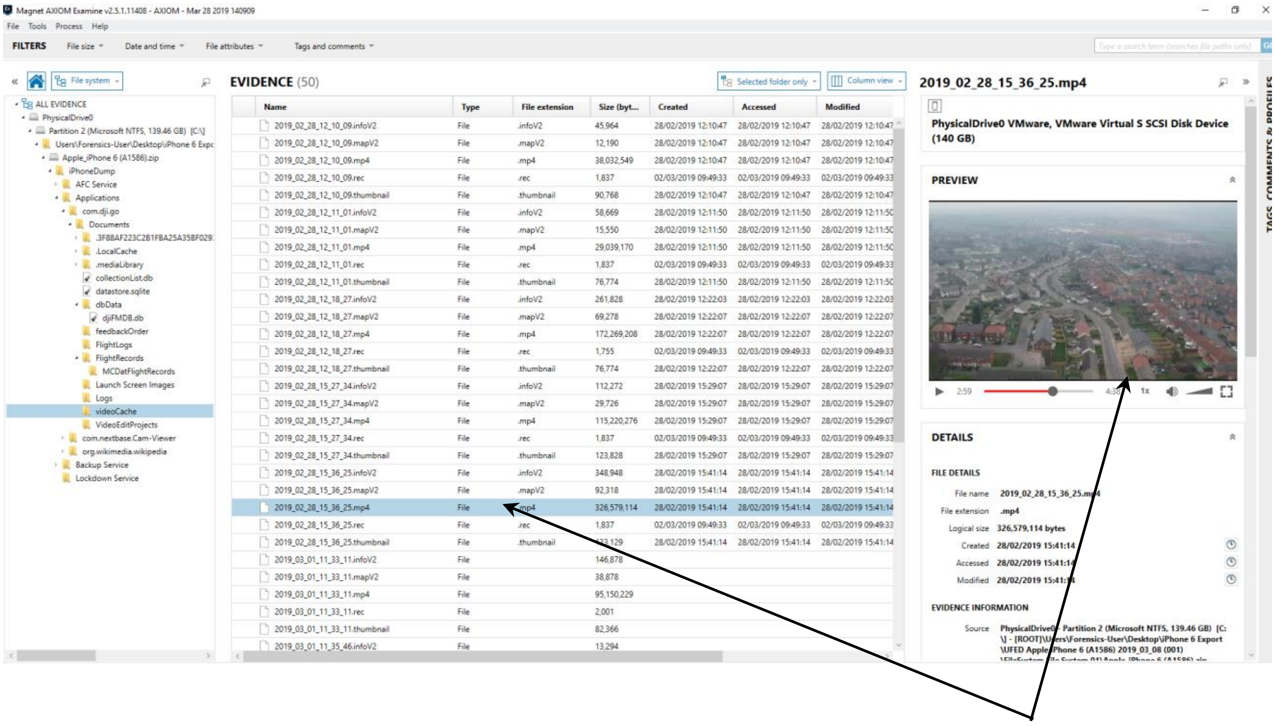
(53.590156, -1.511816, -1) -1.00 01/03/2019 13:57:27

Waypoints (581)

Position	Timestamp
(0.000000, 0.000000)	01/03/2019 13:49:30
(0.000000, 0.000000)	01/03/2019 13:49:30
(0.000000, 0.000000)	01/03/2019 13:49:31
(0.000000, 0.000000)	01/03/2019 13:49:32
(53.590163, -1.511786)	01/03/2019 13:49:33
(53.590163, -1.511785)	01/03/2019 13:49:34
(53.590163, -1.511785)	01/03/2019 13:49:34
(53.590163, -1.511785,...	01/03/2019 13:49:35
(53.590165, -1.511786,...	01/03/2019 13:49:36
(53.590166, -1.511786,...	01/03/2019 13:49:37
(53.590166, -1.511786,...	01/03/2019 13:49:38

Figure 4.5- Waypoints and timestamps of the GPS coordinates.

These logs are in .DAT format which allows the Physical Analyser software to generate a map and flight path (Figure 4.4). The user is then able to view the flight path by clicking on the 'Play/ Stop' toggle button. Once initiated, this would simulate the flight path made by the device.



EVIDENCE (50)

Name	Type	File extension	Size (byt...	Created	Accessed	Modified
2019_02_28_12_10_09.infoV2	File	.infoV2	45,964	28/02/2019 12:10:47	28/02/2019 12:10:47	28/02/2019 12:10:47
2019_02_28_12_10_09.mapV2	File	.mapV2	12,190	28/02/2019 12:10:47	28/02/2019 12:10:47	28/02/2019 12:10:47
2019_02_28_12_10_09.mp4	File	.mp4	38,032,549	28/02/2019 12:10:47	28/02/2019 12:10:47	28/02/2019 12:10:47
2019_02_28_12_10_09.rec	File	.rec	1,837	02/03/2019 09:49:33	02/03/2019 09:49:33	02/03/2019 09:49:33
2019_02_28_12_10_09.thumbnail	File	.thumbnail	90,768	28/02/2019 12:10:47	28/02/2019 12:10:47	28/02/2019 12:10:47
2019_02_28_12_11_01.infoV2	File	.infoV2	58,669	28/02/2019 12:11:50	28/02/2019 12:11:50	28/02/2019 12:11:50
2019_02_28_12_11_01.mapV2	File	.mapV2	15,550	28/02/2019 12:11:50	28/02/2019 12:11:50	28/02/2019 12:11:50
2019_02_28_12_11_01.mp4	File	.mp4	29,039,170	28/02/2019 12:11:50	28/02/2019 12:11:50	28/02/2019 12:11:50
2019_02_28_12_11_01.rec	File	.rec	1,837	02/03/2019 09:49:33	02/03/2019 09:49:33	02/03/2019 09:49:33
2019_02_28_12_11_01.thumbnail	File	.thumbnail	76,774	28/02/2019 12:11:50	28/02/2019 12:11:50	28/02/2019 12:11:50
2019_02_28_12_18_27.infoV2	File	.infoV2	261,828	28/02/2019 12:22:03	28/02/2019 12:22:03	28/02/2019 12:22:03
2019_02_28_12_18_27.mapV2	File	.mapV2	69,278	28/02/2019 12:22:07	28/02/2019 12:22:07	28/02/2019 12:22:07
2019_02_28_12_18_27.mp4	File	.mp4	172,269,208	28/02/2019 12:22:07	28/02/2019 12:22:07	28/02/2019 12:22:07
2019_02_28_12_18_27.rec	File	.rec	1,755	02/03/2019 09:49:33	02/03/2019 09:49:33	02/03/2019 09:49:33
2019_02_28_12_18_27.thumbnail	File	.thumbnail	76,774	28/02/2019 12:22:07	28/02/2019 12:22:07	28/02/2019 12:22:07
2019_02_28_15_27_34.infoV2	File	.infoV2	112,272	28/02/2019 15:29:07	28/02/2019 15:29:07	28/02/2019 15:29:07
2019_02_28_15_27_34.mapV2	File	.mapV2	29,726	28/02/2019 15:29:07	28/02/2019 15:29:07	28/02/2019 15:29:07
2019_02_28_15_27_34.mp4	File	.mp4	115,220,276	28/02/2019 15:29:07	28/02/2019 15:29:07	28/02/2019 15:29:07
2019_02_28_15_27_34.rec	File	.rec	1,837	02/03/2019 09:49:33	02/03/2019 09:49:33	02/03/2019 09:49:33
2019_02_28_15_27_34.thumbnail	File	.thumbnail	123,828	28/02/2019 15:29:07	28/02/2019 15:29:07	28/02/2019 15:29:07
2019_02_28_15_36_25.infoV2	File	.infoV2	348,948	28/02/2019 15:41:14	28/02/2019 15:41:14	28/02/2019 15:41:14
2019_02_28_15_36_25.mapV2	File	.mapV2	92,318	28/02/2019 15:41:14	28/02/2019 15:41:14	28/02/2019 15:41:14
2019_02_28_15_36_25.mp4	File	.mp4	326,579,114	28/02/2019 15:41:14	28/02/2019 15:41:14	28/02/2019 15:41:14
2019_02_28_15_36_25.rec	File	.rec	1,837	02/03/2019 09:49:33	02/03/2019 09:49:33	02/03/2019 09:49:33
2019_02_28_15_36_25.thumbnail	File	.thumbnail	123,129	28/02/2019 15:41:14	28/02/2019 15:41:14	28/02/2019 15:41:14
2019_03_01_11_33_11.infoV2	File		146,878			
2019_03_01_11_33_11.mapV2	File		38,878			
2019_03_01_11_33_11.mp4	File		95,150,229			
2019_03_01_11_33_11.rec	File		2,001			
2019_03_01_11_33_11.thumbnail	File		82,366			
2019_03_01_11_35_46.infoV2	File		13,294			

2019_02_28_15_36_25.mp4

PhysicalDrive0 VMware, VMware Virtual S SCSI Disk Device (140 GB)

DETAILS

FILE DETAILS

File name 2019_02_28_15_36_25.mp4
File extension .mp4
Logical size 326,579,114 bytes
Created 28/02/2019 15:41:14
Accessed 28/02/2019 15:41:14
Modified 28/02/2019 15:41:14

EVIDENCE INFORMATION

Source PhysicalDrive0 - Partition 2 (Microsoft NTFS, 139.46 GB) [C:\] - [ROOT]\Users\Forensics-User\Desktop\iPhone 6 Export\UFED Apple iPhone 6 (A1586) 2019_03_08 (001)

Figure 4.6- Magnet AXIOM Examine software displaying the mobile device's file system

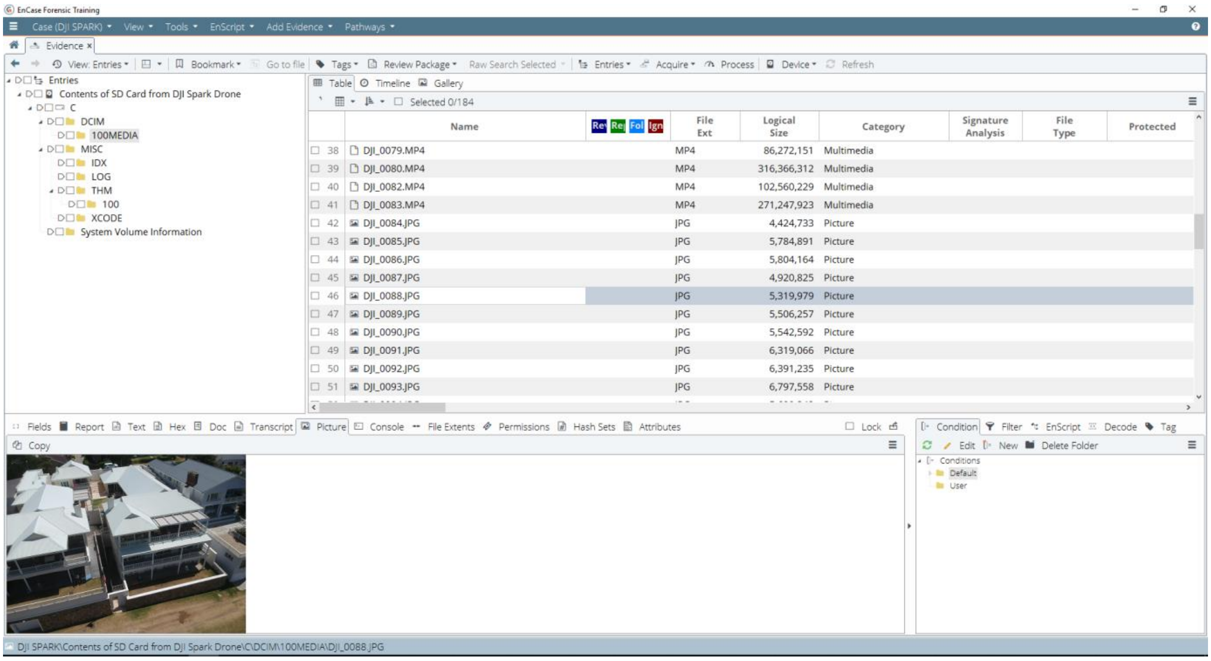
In addition to Cellebrite's Physical Analyser tool, Magnet's AXIOM Process/ Examine software was also utilised in order to analyse the mobile device data (Figure 4.6). Alike Physical Analyser, this software also allowed the user to examine the file system. Additionally, the software displays useful metadata about the current file, such as 'File Name', 'Creation Time', 'Logical Size' and 'Last Accessed'. All these examples, albeit present in the Cellebrite software, are very useful to investigators.

After analysing the evidence extractions in two different software, it seems that no crucial evidence/ data has been missed by either. The device used to carry out the test flights is a DJI Spark device. The reasoning behind choosing this particular device is purely due to the fact that it is the most assessable. DJI is the largest UAV manufacturer (Unmanned Aircraft Systems (UAS)[10]: Commercial Outlook for a New Industry, 2015) and the Spark model being relatively low priced at approximately £449 (DJI, 2019), it is assumed that this is the model most assessable to the general public and would be more likely to be involved in criminal activities due to this.

4.3.2 DJI SPARK SD Card

Due to unforeseen issues regarding the Cellebrite UFED 4PC software see Appendix B, FTK Imager had to be used to create an E01 evidence file of the internal SD card of the UAV device. The E01 file format is widely supported within forensic toolkits, which make it an ideal candidate.

In order to analyse the contents of the E01 file, EnCase was used. Below is a screenshot of the contents of the SD card (Figure 4.7). A high volume of both video and image files are present on the card which can be viewed by the user.

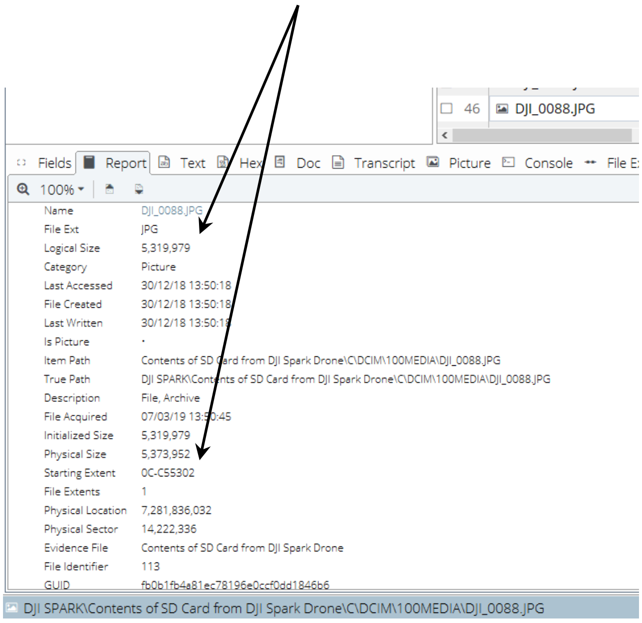

EnCase Forensic Training
Case (DJI SPARK) View Tools EnScript Add Evidence Pathways
Evidence
View: Entries Bookmark Go to file Tags Review Package Raw Search Selected Entries Acquire Process Device Refresh
Entries
Contents of SD Card from DJI Spark Drone
C
DCIM
100MEDIA
MISC
IDX
LOG
THM
100
XCODE
System Volume Information
Table Timeline Gallery
Selected 0/184
Fields Report Text Hex Doc Transcript Picture Console File Extents Permissions Hash Sets Attributes
Lock
Copy
Condition Filter EnScript Decode Tag
Edit New Delete Folder
Conditions
Default
User

	Name	Rev Rej Fol Ign	File Ext	Logical Size	Category	Signature Analysis	File Type	Protected
38	DJI_0079.MP4		MP4	86,272,151	Multimedia			
39	DJI_0080.MP4		MP4	316,366,312	Multimedia			
40	DJI_0082.MP4		MP4	102,560,229	Multimedia			
41	DJI_0083.MP4		MP4	271,247,923	Multimedia			
42	DJI_0084.JPG		JPG	4,424,733	Picture			
43	DJI_0085.JPG		JPG	5,784,891	Picture			
44	DJI_0086.JPG		JPG	5,804,164	Picture			
45	DJI_0087.JPG		JPG	4,920,825	Picture			
46	DJI_0088.JPG		JPG	5,319,979	Picture			
47	DJI_0089.JPG		JPG	5,506,257	Picture			
48	DJI_0090.JPG		JPG	5,542,592	Picture			
49	DJI_0091.JPG		JPG	6,319,066	Picture			
50	DJI_0092.JPG		JPG	6,391,235	Picture			
51	DJI_0093.JPG		JPG	6,797,558	Picture			

DJI SPARK\Contents of SD Card from DJI Spark Drone\C\DCIM\100MEDIA\DJI_0088.JPG

Figure 4.7- EnCase loading the contents of the UAVs on board SD Card

Also, the user is able to view an array of metadata regarding the artefact. Metadata such as the item path, creation date and last accessed. This is very useful information that could be pertinent in a case. In addition to this, the physical location of the file within the file system is also displayed. By using this data to locate the physical location on the drive it may make the case more solid.


46 DJI_0088.JPG
Fields Report Text Hex Doc Transcript Picture Console File E
100%

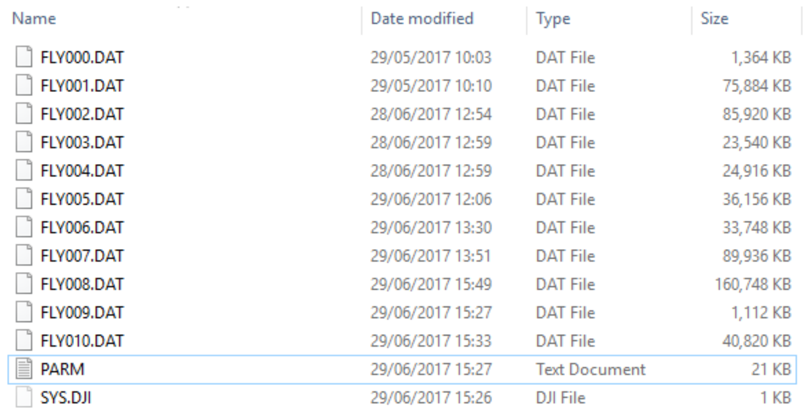
Name	DJI_0088.JPG
File Ext	JPG
Logical Size	5,319,979
Category	Picture
Last Accessed	30/12/18 13:50:18
File Created	30/12/18 13:50:18
Last Written	30/12/18 13:50:18
Is Picture	·
Item Path	Contents of SD Card from DJI Spark Drone\C\DCIM\100MEDIA\DJI_0088.JPG
True Path	DJI SPARK\Contents of SD Card from DJI Spark Drone\C\DCIM\100MEDIA\DJI_0088.JPG
Description	File, Archive
File Acquired	07/03/19 13:50:45
Initialized Size	5,319,979
Physical Size	5,373,952
Starting Extent	0C-C55302
File Extents	1
Physical Location	7,281,836,032
Physical Sector	14,222,336
Evidence File	Contents of SD Card from DJI Spark Drone
File Identifier	113
GUID	fb0b1fb4a81ec78196e0ccf0dd1846b6

DJI SPARK\Contents of SD Card from DJI Spark Drone\C\DCIM\100MEDIA\DJI_0088.JPG

Figure 4.8- EnCase extraction showing the true path of file

4.3.3 DJI Phantom 4

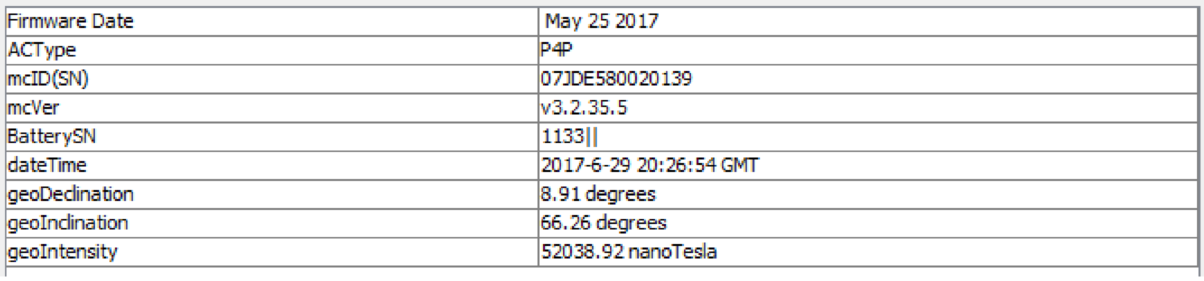
Whilst investigating the Internal SD card a total of 11 flight of logs were located, alongside a text document titled 'PARM.LOG' and SYS.DJI (Figure 4.9).



Name	Date modified	Type	Size
FLY000.DAT	29/05/2017 10:03	DAT File	1,364 KB
FLY001.DAT	29/05/2017 10:10	DAT File	75,884 KB
FLY002.DAT	28/06/2017 12:54	DAT File	85,920 KB
FLY003.DAT	28/06/2017 12:59	DAT File	23,540 KB
FLY004.DAT	28/06/2017 12:59	DAT File	24,916 KB
FLY005.DAT	29/06/2017 12:06	DAT File	36,156 KB
FLY006.DAT	29/06/2017 13:30	DAT File	33,748 KB
FLY007.DAT	29/06/2017 13:51	DAT File	89,936 KB
FLY008.DAT	29/06/2017 15:49	DAT File	160,748 KB
FLY009.DAT	29/06/2017 15:27	DAT File	1,112 KB
FLY010.DAT	29/06/2017 15:33	DAT File	40,820 KB
PARM	29/06/2017 15:27	Text Document	21 KB
SYS.DJI	29/06/2017 15:26	DJI File	1 KB

Figure 4.9 - File's located within internal SD card directory

By using the CsvView application, data was able to be obtained from the flight logs and data was able to be extracted that could otherwise not have been seen by opening the .dat file manually. FLY008.DAT was inputted into CsvView and the following information was presented as shown in Figure (4.10).



Firmware Date	May 25 2017
ACType	P4P
mcID(SN)	07JDE580020139
mcVer	v3.2.35.5
BatterySN	1133||
dateTime	2017-6-29 20:26:54 GMT
geoDeclination	8.91 degrees
geoInclination	66.26 degrees
geoIntensity	52038.92 nanoTesla

Figure 4.10 - Flight details of FLY008.DAT from CsvView

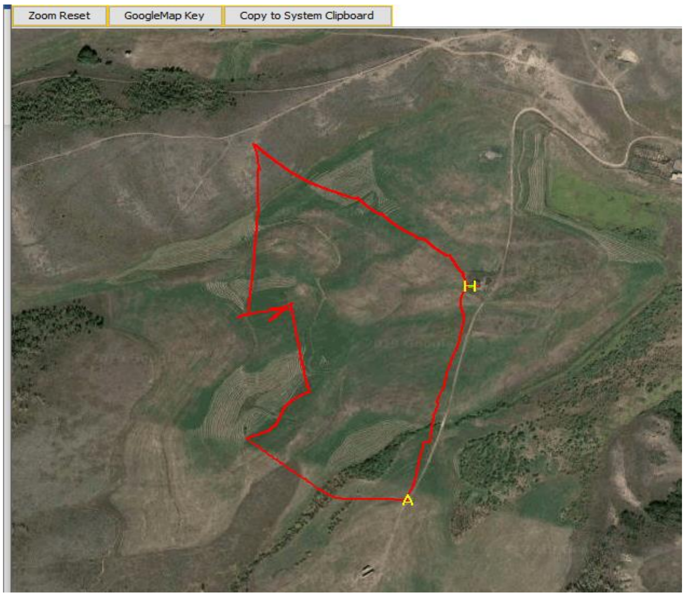


Figure 4.11 - Flight path obtained from FLY008.DAT

Using the feature GeoPlayer within CsvView allows for the user to see both the flight path which was taken by the drone and the home-point which was set at the start of the flight by the user. This home point is represented by the 'H' on the maps, whilst the flight path is shown as a red continuous line. Figure 4.11 shows the specific flight path of the file 'FLY008.DAT'.

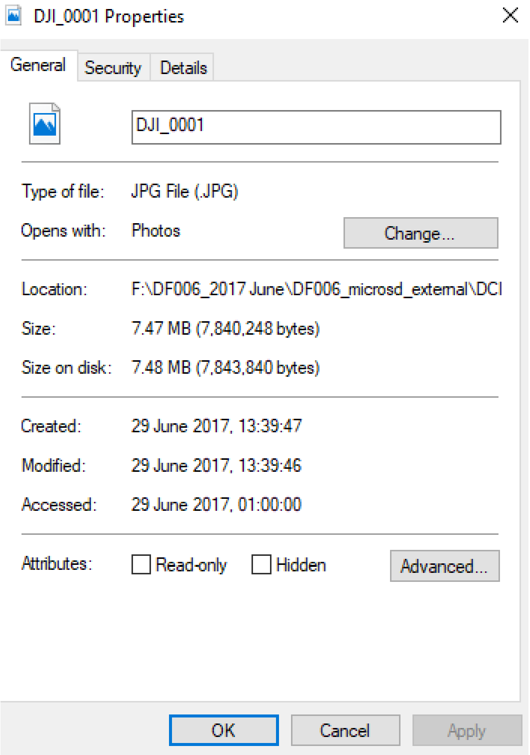
Upon further examination of flight log ‘FLY008.DAT’, a number of graphs were able to be created showing a range of signals which are recorded by the drone at the point of flight. By extracting specific signals (Appendix C).

4.3.4 External and Internal SD Card

Whilst examining the external SD card a number of files were located inside both a folder titled ‘DCIM’ and a hidden folder titled ‘MISC’ (Appendix C).

Within the DCIM folder there was another folder titled ‘100Media’ and within this there was a number of .JPG files and .mov files. In total 17 images were stored on the external SD card and a further 6 videos were also stored (Appendix C).

Upon further investigation into the image files via the image properties key points of interest were located. The date of creation, modified date and accessed date were all available for the user to view (Figure 4.12).



DJI_0001

Type of file: JPG File (.JPG)
Opens with: Photos

Location: F:\DF006_2017 June\DF006_microsd_external\DCI
Size: 7.47 MB (7,840,248 bytes)
Size on disk: 7.48 MB (7,843,840 bytes)

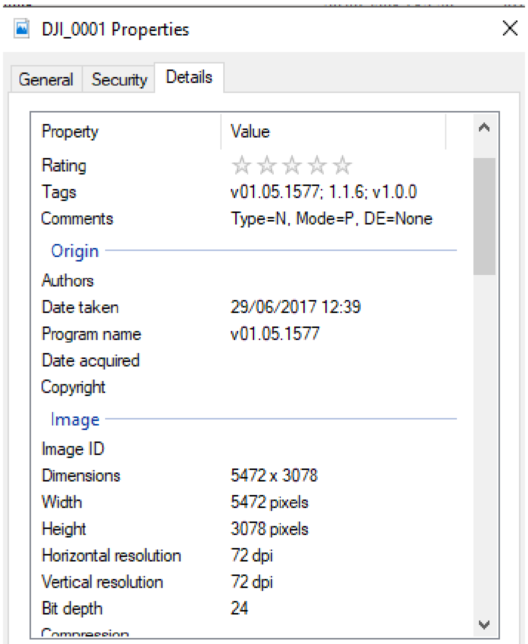
Created: 29 June 2017, 13:39:47
Modified: 29 June 2017, 13:39:46
Accessed: 29 June 2017, 01:00:00

Attributes: □ Read-only □ Hidden

Figure 4.12 - Properties of DJI_0001 image

When viewing the details tab within the properties, further data was able to be acquired. The date taken was located as 29/06/2017 12:39. Details regarding the size of the image, resolution and dimension can also be viewed (Figure 4.13).

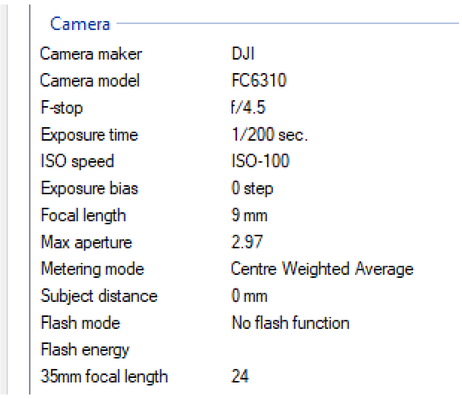
Information regarding the camera which has taken this image can also be located in the details tab. Furthermore, GPS co-ordinates of the image can also be viewed, providing an insight as to where the drone was located when the image was taken (Figures 4.14 and 4.15).



DJI_0001 Properties

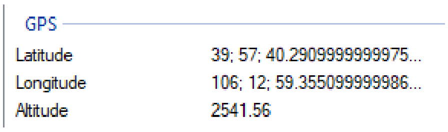
Property	Value
Rating	☆☆☆☆☆
Tags	v01.05.1577; 1.1.6; v1.0.0
Comments	Type=N, Mode=P, DE=None
Origin	
Authors	
Date taken	29/06/2017 12:39
Program name	v01.05.1577
Date acquired	
Copyright	
Image	
Image ID	
Dimensions	5472 x 3078
Width	5472 pixels
Height	3078 pixels
Horizontal resolution	72 dpi
Vertical resolution	72 dpi
Bit depth	24
Compression	

Figure 4.13 - Image details in properties of DJI_0001 image



Camera	
Camera maker	DJI
Camera model	FC6310
F-stop	f/4.5
Exposure time	1/200 sec.
ISO speed	ISO-100
Exposure bias	0 step
Focal length	9 mm
Max aperture	2.97
Metering mode	Centre Weighted Average
Subject distance	0 mm
Flash mode	No flash function
Flash energy	
35mm focal length	24

Figure 4.14 - Camera details in properties of DJI_0001 image



GPS	
Latitude	39; 57; 40.2909999999975...
Longitude	106; 12; 59.355099999986...
Altitude	2541.56

Figure 4.15 - GPS details in properties of DJI_0001 image

Through viewing the images that have been found on the external SD the user can view what the drone has been taking pictures of. This can provide evidence of specific crimes regarding spying and reconnaissance. A selection of the pictures extracted from the external SD provide an insight as to what the drone operator was taking photos of and whether they were legal or illegally taken (Figures 4.16 and 4.17).

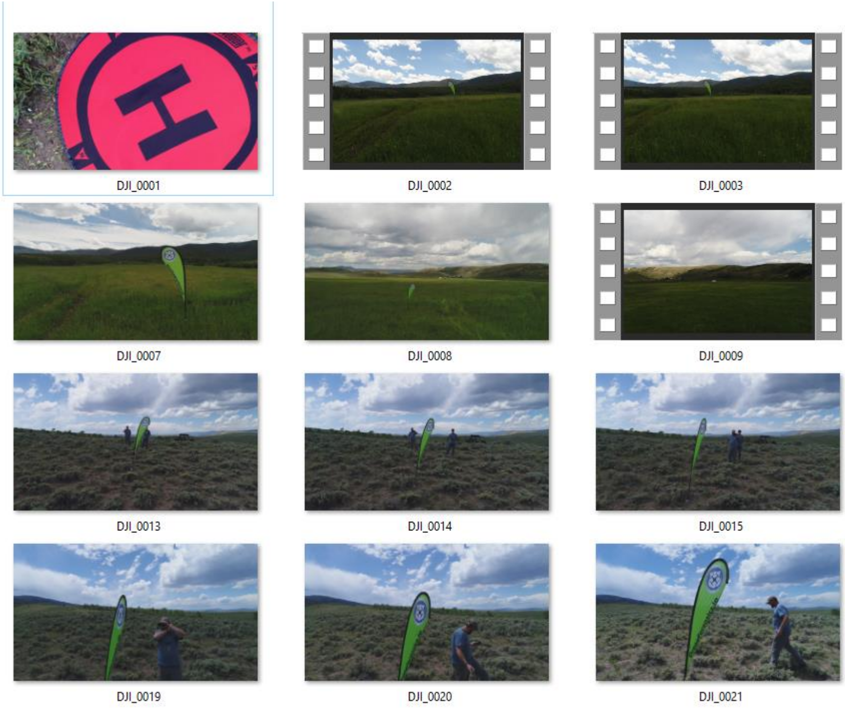


Figure 4.16 - Images and video's found on external SD

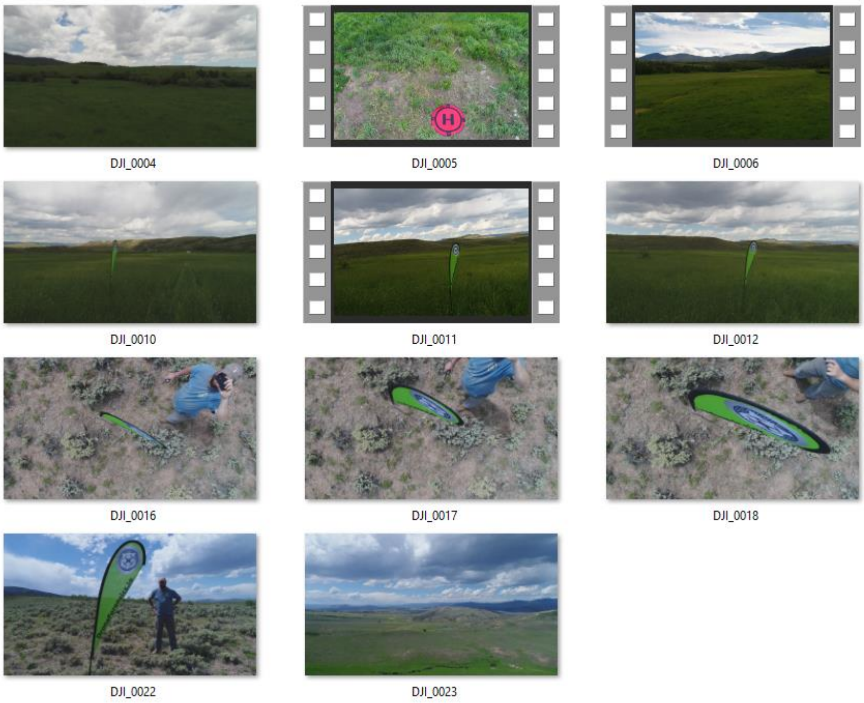
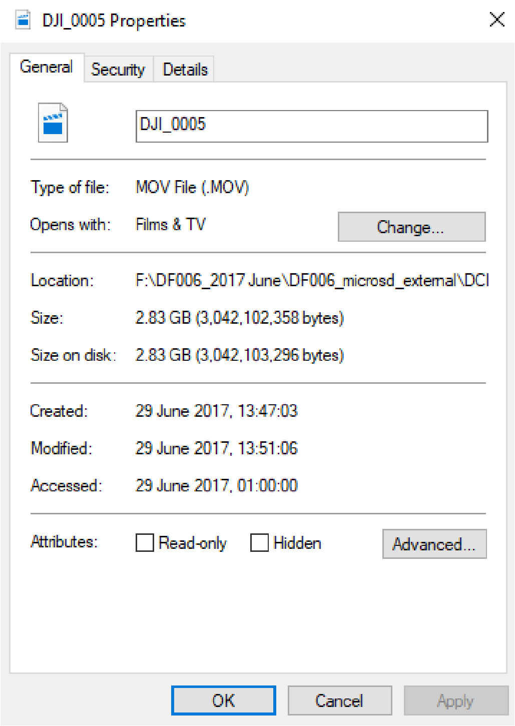


Figure 4.17 - Further image's and video found on external SD

Videos located as .mov files within the 100Media folder contain less information in the properties when compared to the still images acquired. The created, modified and accessed dates and time appear, however the accessed time appears to be before the created time (Figure 4.18). Within the details tab, the media created date and time is obtained, this time is shown as 29/06/2017 13:46 which is just before the file creation time (Figure 4.19). The video's properties do not include information regarding the location through GPS contrasting with the images that were obtained.



DJI_0005

Type of file: MOV File (.MOV)

Opens with: Films & TV

Location: F:\DF006_2017 June\DF006_microsd_external\DCI

Size: 2.83 GB (3,042,102,358 bytes)

Size on disk: 2.83 GB (3,042,103,296 bytes)

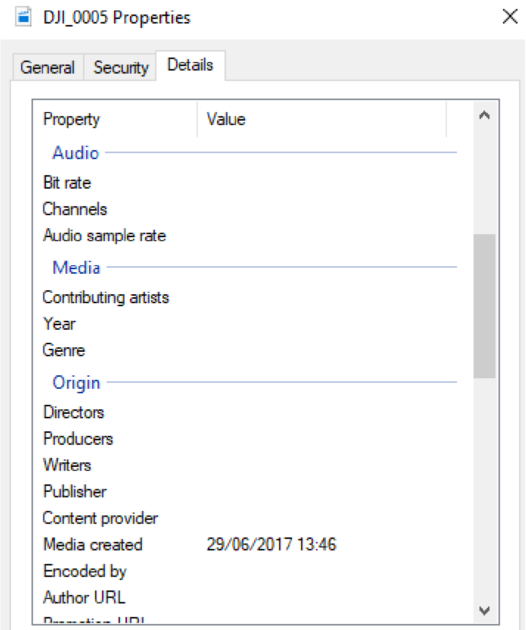
Created: 29 June 2017, 13:47:03

Modified: 29 June 2017, 13:51:06

Accessed: 29 June 2017, 01:00:00

Attributes: □ Read-only □ Hidden

Figure 4.18 - DJI_005.mov properties



Property	Value
Audio	
Bit rate	
Channels	
Audio sample rate	
Media	
Contributing artists	
Year	
Genre	
Origin	
Directors	
Producers	
Writers	
Publisher	
Content provider	
Media created	29/06/2017 13:46
Encoded by	
Author URL	

Figure 4.19 - DJI_0005.mov details

4.4 Further Discussion

In this section, any further considerations will be discussed regarding each component of this study. A lot of results have been gained from carrying out the experiments stated in this chapter; the outcome of which have fuelled various recommendations regarding the examination of UAV devices as well as thoughts on future work in this area.

In regard to the experiments, the scenarios and data interpretation are formed from the use of the DJI Spark. The outcomes are likely to vary depending on the model and brand of the drone used for criminal activity. In the case of the payloads, there would need to be further experimentation with drones that have a more intelligent stability system, to determine how the data output is affected by the additional weight.

With regards to the rotor movements and gimbal, it is important to note that at the time of experimentation, there was no data to determine the degree of the gimbal. This data would be an essential piece of evidence as the investigators would be able to determine if the camera was facing a specific direction, such as into the victim's property, rather than just facing in the general direction. This type of evidence may also aid in creating a timeline, to determine when the suspect first started observing the victim during their drone flight.

Section 5 Conclusion and Future work

5.1 Introduction

This chapter will provide the overall conclusion of the results which have been obtained through the experiment and will incorporate parts of the previous chapter discussing those results. Furthermore, this chapter will look at to what extent this project has added to the existing literature, whether the objectives and aims of the project were met and recommendations for future work within this area of research.

5.2 Summary of Findings

Based on the findings, it is shown that with the right tools, not necessarily specialist software, a drone forensics team would be able to find appropriate evidence to support their investigations. However, it is important to note that there can be challenges during the extraction and analysis, that depending on the specific case, would need to be examined to retain the integrity of the data.

Through completion of the experiment a number of key items of interest were discovered that can help forensic examiners with criminal investigations. Flight data stored on the internal SD was analysed and provided a vast range of information relating to the signals which are stored on the device itself. This analysis of results was more in-depth than previous research papers detailed in the literature review, this study provides a more detailed analysis and highlighted signals such as airport limits, emergency brakes information and whether the controller was connected to the device at all times during the flight.

Media stored within the external SD and mobile application data was also found through the experiment. This data was congruent with previous research [3],[39],[24], [33] on different models of drones, by exploring the metadata the GPS co-ordinates of where the image was taken were located as was the date and time of creation.

Ownership between the drone and the controller was explored, however due to limitations with the data which had been acquired form VTO it was not possible to provide concrete evidence that the two can be linked together. However, serial numbers of the drone were located on the internal SD flight logs and also discovered on the flight log which had been stored on the mobile application.

5.3 Limitation

It is important to note that all drones have different components and have different capabilities, depending on the range or brand, therefore each individual drone will hold unique limitations. As such, the experiments carried out with the DJI Spark drone presented a limitation of the internal memory size only being 4GB. The issue with a smaller internal memory means that the existing data, and possible evidence, is overwritten when the capacity is reached.

There is currently limited research in the field of drone forensics as found in the literature review within the chapter. This means that researchers only have a limited basis of understanding of this topic and there is a lack of unique research. Whilst this work will quickly become outdated due to the fast-growing nature of drones and their constant upgrading, this research provides a further understanding of drone forensics. However, more research needs to be carried out on a range of drones to establish common themes of data extraction and data locations. Only when many drones have been researched can a general framework for drone extraction be developed, as has been done with mobile forensics.

5.4 Recommendation and Future work

Whilst carrying out this project, a number of obstacles have been encountered. Therefore, there are a few recommendations that this study would like to make in order to make the industry more 'drone/ UAV friendly'.

Firstly, when attempting to extract data from a mobile device using EnCase software, the evidence was unable to be acquired. This is something that EnCase must work on to ensure that almost all devices are supported by their software.

Secondly it was discovered during the interview with the Digital Forensics Analyst that there is not a great amount of knowledge of UAV devices within DFUs. Although the analyst only works with one Police Force, they are in contact with people from other forces and states that views on UAV devices are very similar across all forces nationwide. The view being that it is very rare that a UAV device is brought into a Unit, so it is not worth the resources sending personnel on training courses. In addition to the lack of UAV Forensics training, DFU personnel are not required to have knowledge on current laws and legislations of any devices. Although standards such as ISO 27001 and ISO 17025 must be adhered, as well as the ACPO guidelines [2], knowledge of other legislation is not required and generally analysts/ investigators 'learn as they go' in relation to laws and legislation. This is something that this study finds astounding as having up to date knowledge of the current legalities relating to the device(s) would be very beneficial to an investigation. For example, if the use of a device were an illegal act in a specific area e.g. the use of a UAV device in the vicinity of a school and it was found that this occurred, it should be included in the final report. Nonetheless it is likely that an investigator/ analyst would look up such laws and legislation on an ad-hoc basis, but this would waste time during an investigation. Therefore, it is a recommendation of this study that DFUs at least make all of their personnel aware of relevant laws and legislation and send them on 'refresher' courses on a regular basis e.g. annually. Refresher courses would be very beneficial also for standards such as ISO 27001 and ISO 17025 to ensure that they are being continuously obeyed.

References

[1] Admin. (2017). *Drone Components_Quick List of it's Parts.* Retrieved from http://grinddrone.com/drone-features/drone-components

[2] Association of Chief Police Officers. (2012). ACPO good practice guide for digital evidence. (). Retrieved from https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[3] Barton, T. E. A., & Hannan Bin Azhar, M.,A. (2017). Forensic analysis of popular UAV systems IEEE. doi:10.1109/EST.2017.8090405

[4] BBC. (2019, February 20). Drone no-fly zone to be widened after Gatwick chaos. Retrieved from www.bbc.co.uk: https://www.bbc.co.uk/news/business-47299805

[5] Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2018). 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). In Drone Forensics: Challenges and New Insights. [Conference] Paris, France: IEEE.

[6] Brown, R. (2018). Fears burglars are using drones to case homes - as drone reports to police rocket. The Cambridgeshire Live. Retrieved from https://www.cambridge-news.co.uk/news/cambridge-news/burglars-drones-homes-reports-rocket-14785783

[7] CAA, NATS. (2019, February 19). The Drone Code. Retrieved from Drone Safe UK: https://dronesafe.uk/wp-content/uploads/2019/02/Drone-Code_March19.pdf

[8] CAA, NATS. (n.d). Retrieved from Drone Safe UK: https://dronesafe.uk/

[9] The Civil Aviation Authority. (n.d). Safety Apps. Retrieved from DroneSafeUK: https://dronesafe.uk/safety-apps/

[10] Canis, B (2015). Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry. Congressional Research Service. Retrieved from http://goodtimesweb.org/industrial-policy/2015/R44192.pdf

[11] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of things security and forensics: Challenges and opportunities. Future Generation Computer Systems; Future Generation Computer Systems, 78, 544-546. doi:10.1016/j.future.2017.07.060

[12] CopterSafe. (n.d). NFZ mod for Phantom 4 (not for PRO). Retrieved from CopterSafe: http://www.coptersafe.com/product/nfz-mod-phantom-4/

[13] Crawford, J. (2018). 10 Crimes Committed Using A Drone. Retrieved from http://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/

[14] DJI. (n.d.). FlySafe. Retrieved from DJI website: https://www.dji.com/uk/flysafe

[15] DJI. (2019). Matric 600. Retrieved from https://www.dji.com/uk/matrice600

[16] DJI. (2018). Phantom 4. Retrieved from https://www.dji.com/uk/phantom-4/info

[17] Dormehl, L. (2018). The history of drones in 10 milestones. Retrieved from https://www.digitaltrends.com/cool-tech/history-of-drones/

[18] Flynt, J. (2017). 21 types of drones. Retrieved from https://3dinsider.com/types-of-drones/

[19] Fussell, S. (2018). Who Will Police Drones? Retrieved from https://gizmodo.com/who-will-police-police-drones-1826891119

[20] H, J. (n.d.). Retrieved from No Fly Drones: http://www.noflydrones.co.uk/

[21] H, J. (n.d.). Contact. Retrieved from No Fly Drones: http://www.noflydrones.co.uk/contact

[22] Haylen, A. (2019). Civilian drones. (Briefing Paper No. CBP 7734). Retrieved from www.parliament.uk/commons-library

[23] Hegarty, R., Lamb, D. J., & Attwood, A. (2014). Digital evidence challenges in the internet of things. Paper presented at the Inc, 163-172.

[24] Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation, 16, 1-11. doi:10.1016/j.diin.2015.11.002

[25] HM Government. (2000, August 1). Regulation of Investigatory. Retrieved from Legislation.gov: https://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

[26] HM Government. (1978). Protection of Children Act 1978. Retrieved from Legislation.gov: https://www.legislation.gov.uk/ukpga/1978/37/pdfs/ukpga_19780037_en.pdf

[27] HM Government. (2003). Sexual Offences Act 2003. Retrieved from Legislation.gov: https://www.legislation.gov.uk/ukpga/2003/42/pdfs/ukpga_20030042_en.pdf

[28] House of Commons - Science and Technology Committee. (2019). Commercial and recreational drone use in the UK. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2021/2021.pdf

[29] Jain, A., & Chhabra, G. (2014). Anti-Forensics Techniques: An Analytical Review. 2014 Seventh International Conference on Contemporary Computing (IC3) (p. 7). India: IEEE.

[30] Liao, S. (2017, June). DJI drones can get past no-fly zones thanks to this Russian software company. Retrieved from The Verge: https://www.theverge.com/2017/6/21/15848344/drones-russian-software-hack-dji-jailbreak

[31] Kessler, G. C. (2007). Anti-Forensics and the Digital Investigator. Proceedings of the 5th Australian Digital Forensics Conference (p. 8). Perth Western Australia: Edith Cowan University.

[32] Kovar, D., Bollo, J. (2018). Drone Forensics. Digital Forensics Magazine, v34, 14-19.

[33] Maarse, M., Sangers, L., van Ginkel, J., & Pouw, M. (2016). Digital forensics on a DJI phantom 2 vision UAV. University of Amsterdam,

[34] Mercer, D. (2019). Revealed: Drones used for stalking and filming cash machines in the UK. Retrieved from https://news.sky.com/story/police-warn-drone-users-after-incidents-soar-by-40-in-two-years-11637695

[35] NIST. (2018, June 6). Drone Forensics Gets a Boost With New Data on NIST Website. Retrieved from NIST: https://www.nist.gov/news-events/news/2018/06/drone-forensics-gets-boost-new-data-nist-website

[36] NLD. (n.d). NLD MOD Client License Key. Retrieved from No Limit Dronez: https://nolimitdronez.com/activation-key-for-nld-mod-client

[37] PWC. (2018). Skies without limits. (). Retrieved from https://www.pwc.co.uk/intelligent-digital/drones/Drones-impact-on-the-UK-economy-FINAL.pdf

[38] Roder, A., Choo, K.-K., & Le-Khac, N.-A. (n.d). UNMANNED AERIAL VEHICLE FORENSIC INVESTIGATION., (p. 14).

[39] Roder, A., Choo, K. R., & Le-Khac, N. (2018). Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as A case study.

[40] Rouse, M. (2018). Drone (unmanned aerial vehicle, UAV). Retrieved from https://internetofthingsagenda.techtarget.com/definition/drone

[41] Rubens, T. (2018). Drug-smuggling drones: How prisons are responding to the airborne security threat. Retrieved from https://www.ifsecglobal.com/drones/drug-smuggling-drones-prisons-airborne-security-threat/

[42] SmashingDrones.com. (2019). Best camera drones for sale UK 2019. Retrieved from https://smashingdrones.com/

[43] The Daily Mail. (2017). Ten drone crimes a day: Surge in popularity sees police report for 12-fold jump in offences linked to the gadgets. Retrieved from https://www.dailymail.co.uk/news/article-4373806/Police-report-12-fold-jump-drone-offences.html

[44] The Office of the General Counsel. (2016, August). The Air Navigation Order 2016 and Regulations. Retrieved from The Civil Aviation Authority: http://publicapps.caa.co.uk/docs/33/CAP393_Fifth_edition_Amendment_13_March_2019.pdf

[45] UK Civil Aviation Authority. (2019). Drone code. Retrieved from https://dronesafe.uk/drone-code/

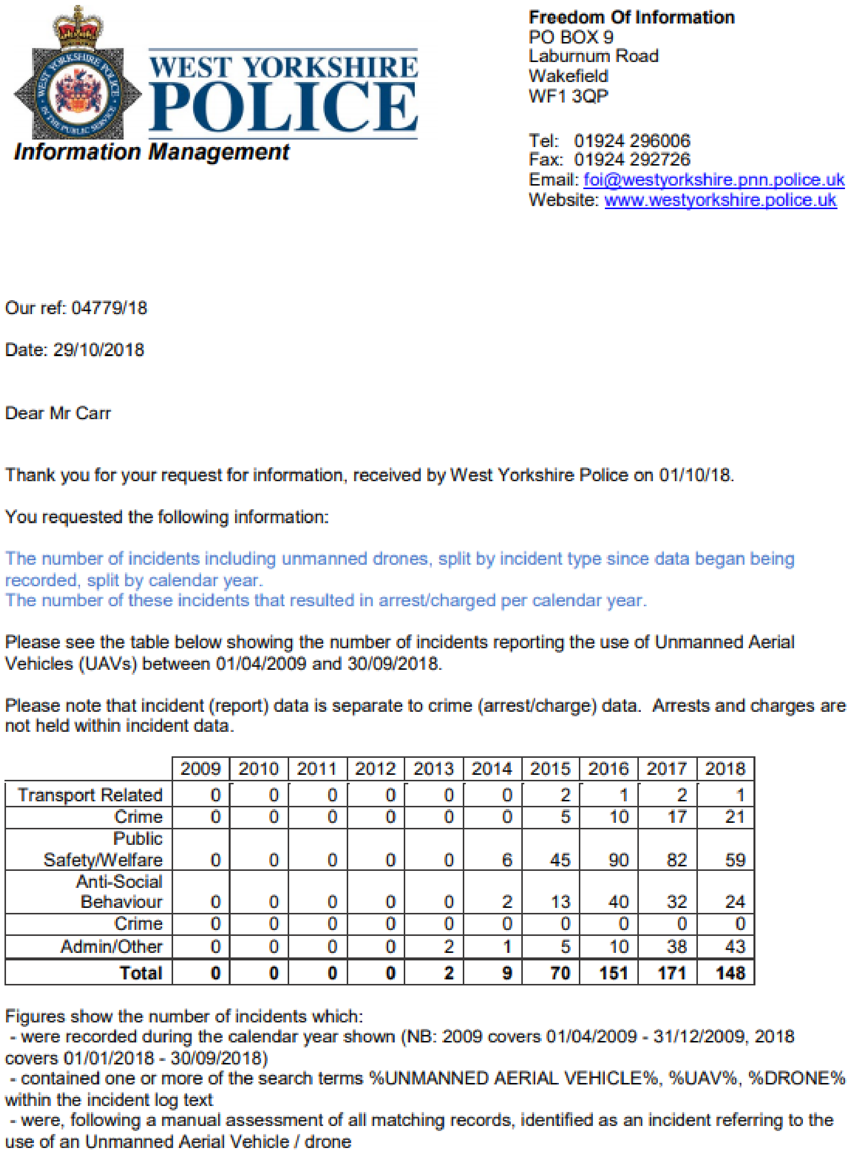
[46] Uleski, M. (2017). The Top 6 Reasons Police UAV Programs Fail. [Blog]. Retrieved from https://www.dartdrones.com/blog/top-police-uav-fails/

[47] WADDELL, K. (2017, March 2). The Invisible Fence That Keeps Drones Away From the President. Retrieved from The Atlantic: https://www.theatlantic.com/technology/archive/2017/03/drones-invisible-fence-president/518361/

[48] Watson, A. (2019). 5 Ways Commercial Drones are Pushing the Boundaries of Crime. [Blog]. Retrieved from https://www.cellebrite.com/en/blog/5-ways-commercial-drones-are-pushing-the-boundaries-of-crime/

[49] Kovar, D. (2016) UVA (aka drone) Forensics. [Slide Presentation] Cyber Security Summit. Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492184184.pdf

Appendix a



WEST YORKSHIRE POLICE
Information Management

Freedom Of Information
PO BOX 9
Laburnum Road
Wakefield
WF1 3QP

Tel: 01924 296006
Fax: 01924 292726
Email: foi@westyorkshire.pnn.police.uk
Website: www.westyorkshire.police.uk

Our ref: 04779/18

Date: 29/10/2018

Dear Mr Carr

Thank you for your request for information, received by West Yorkshire Police on 01/10/18.

You requested the following information:

The number of incidents including unmanned drones, split by incident type since data began being recorded, split by calendar year.
The number of these incidents that resulted in arrest/charged per calendar year.

Please see the table below showing the number of incidents reporting the use of Unmanned Aerial Vehicles (UAVs) between 01/04/2009 and 30/09/2018.

Please note that incident (report) data is separate to crime (arrest/charge) data. Arrests and charges are not held within incident data.

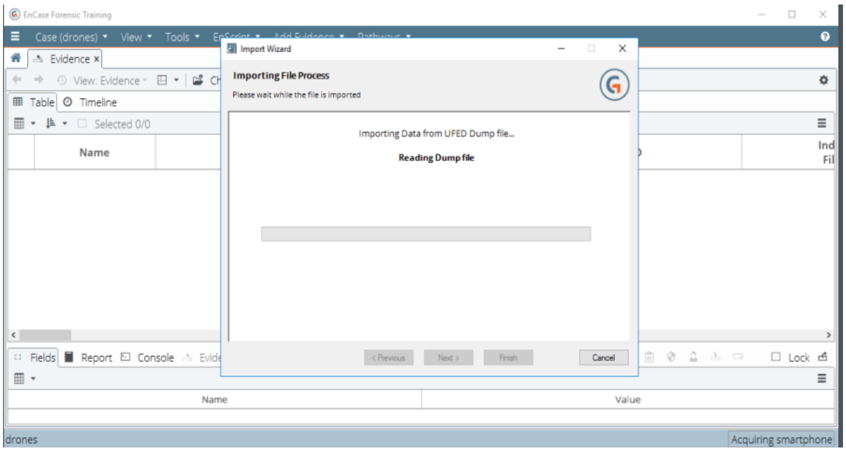
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Transport Related	0	0	0	0	0	0	2	1	2	1
Crime	0	0	0	0	0	0	5	10	17	21
Public Safety/Welfare	0	0	0	0	0	6	45	90	82	59
Anti-Social Behaviour	0	0	0	0	0	2	13	40	32	24
Crime	0	0	0	0	0	0	0	0	0	0
Admin/Other	0	0	0	0	2	1	5	10	38	43
Total	**0**	**0**	**0**	**0**	**2**	**9**	**70**	**151**	**171**	**148**

Figures show the number of incidents which:
- were recorded during the calendar year shown (NB: 2009 covers 01/04/2009 - 31/12/2009, 2018 covers 01/01/2018 - 30/09/2018)
- contained one or more of the search terms %UNMANNED AERIAL VEHICLE%, %UAV%, %DRONE% within the incident log text
- were, following a manual assessment of all matching records, identified as an incident referring to the use of an Unmanned Aerial Vehicle / drone

Appendix B

When using EnCase to acquire the data from the mobile device used to control the UAV device, issues were encountered. The data had previously been extracted using Cellebrite and a '.UFD' dump file created. EnCase is able to read the dump file in order to acquire the data. However, it was found that the software was unable to read the data; the error message stating that the task was not possible whilst being run in a Virtual Machine. As the EnCase software is not available outside of the designated Virtual Machine, it is not known whether or not EnCase is able to read and acquire the dump data from the iOS device used to control the UAV device.

The following screenshots note the process and error messages displayed when attempting to carry out this task.

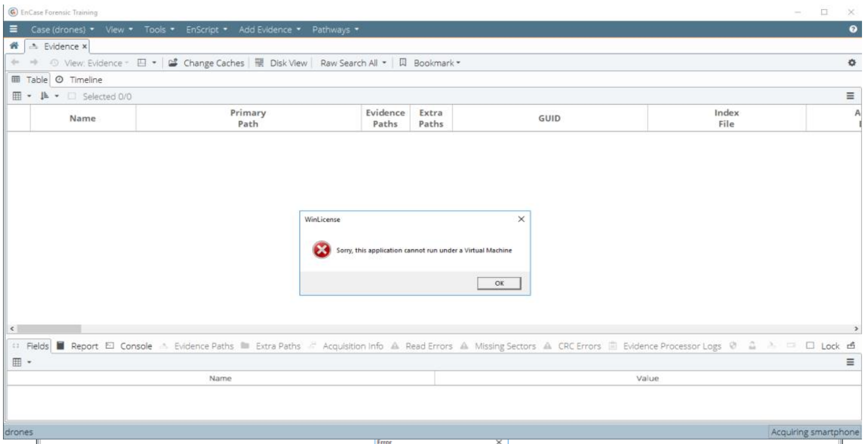


Importing File Process

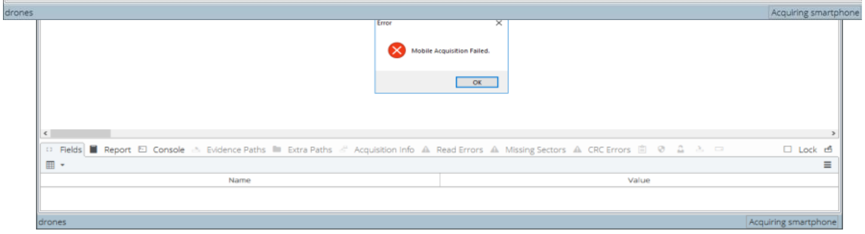
Please wait while the file is imported

Importing Data from UFED Dump file...

Reading Dump file

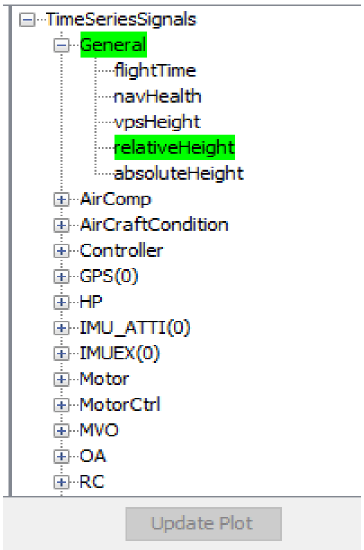


Sorry, this application cannot run under a Virtual Machine

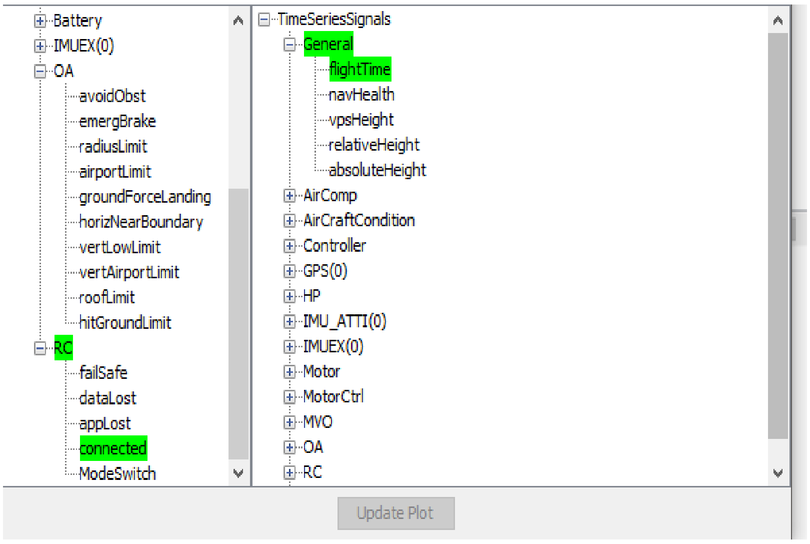


Mobile Acquisition Failed.

Appendix C



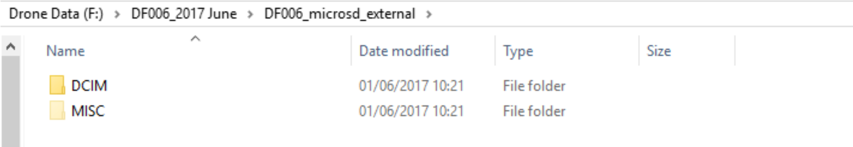
Signals used to present controller connection



```
⊞ Battery
⊞ IMUEX(0)
⊟ OA
    avoidObst
    emergBrake
    radiusLimit
    airportLimit
    groundForceLanding
    horizNearBoundary
    vertLowLimit
    vertAirportLimit
    roofLimit
    hitGroundLimit
⊟ RC
    failSafe
    dataLost
    appLost
    connected
    ModeSwitch
```

```
⊟ TimeSeriesSignals
  ⊟ General
      flightTime
      navHealth
      vpsHeight
      relativeHeight
      absoluteHeight
  ⊞ AirComp
  ⊞ AirCraftCondition
  ⊞ Controller
  ⊞ GPS(0)
  ⊞ HP
  ⊞ IMU_ATTI(0)
  ⊞ IMUEX(0)
  ⊞ Motor
  ⊞ MotorCtrl
  ⊞ MVO
  ⊞ OA
  ⊞ RC
```

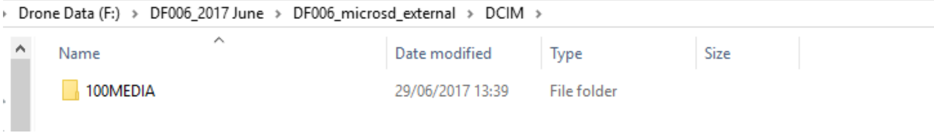
Signals used to present altitude



Drone Data (F:) › DF006_2017 June › DF006_microsd_external ›

Name	Date modified	Type	Size
DCIM	01/06/2017 10:21	File folder	
MISC	01/06/2017 10:21	File folder	

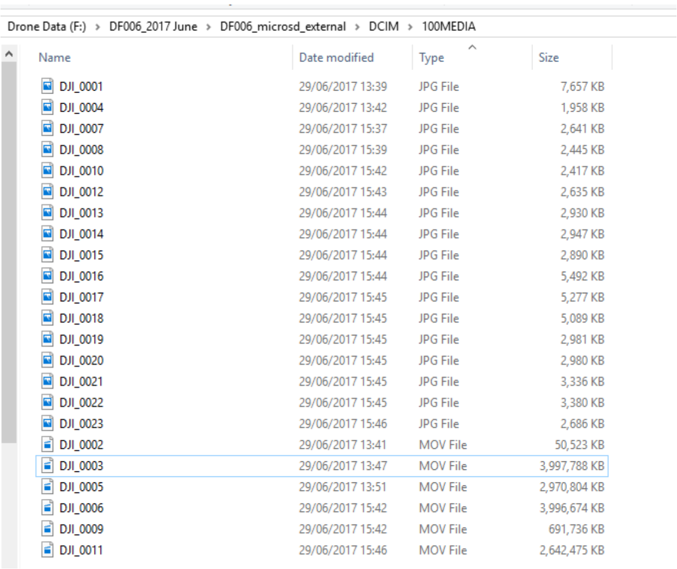
Root folder of external SD Card



Drone Data (F:) › DF006_2017 June › DF006_microsd_external › DCIM ›

Name	Date modified	Type	Size
100MEDIA	29/06/2017 13:39	File folder	

100Media Folder stored in DCIM Folder



Drone Data (F:) › DF006_2017 June › DF006_microsd_external › DCIM › 100MEDIA

Name	Date modified	Type	Size
DJI_0001	29/06/2017 13:39	JPG File	7,657 KB
DJI_0004	29/06/2017 13:42	JPG File	1,958 KB
DJI_0007	29/06/2017 15:37	JPG File	2,641 KB
DJI_0008	29/06/2017 15:39	JPG File	2,445 KB
DJI_0010	29/06/2017 15:42	JPG File	2,417 KB
DJI_0012	29/06/2017 15:43	JPG File	2,635 KB
DJI_0013	29/06/2017 15:44	JPG File	2,930 KB
DJI_0014	29/06/2017 15:44	JPG File	2,947 KB
DJI_0015	29/06/2017 15:44	JPG File	2,890 KB
DJI_0016	29/06/2017 15:44	JPG File	5,492 KB
DJI_0017	29/06/2017 15:45	JPG File	5,277 KB
DJI_0018	29/06/2017 15:45	JPG File	5,089 KB
DJI_0019	29/06/2017 15:45	JPG File	2,981 KB
DJI_0020	29/06/2017 15:45	JPG File	2,980 KB
DJI_0021	29/06/2017 15:45	JPG File	3,336 KB
DJI_0022	29/06/2017 15:45	JPG File	3,380 KB
DJI_0023	29/06/2017 15:46	JPG File	2,686 KB
DJI_0002	29/06/2017 13:41	MOV File	50,523 KB
DJI_0003	29/06/2017 13:47	MOV File	3,997,788 KB
DJI_0005	29/06/2017 13:51	MOV File	2,970,804 KB
DJI_0006	29/06/2017 15:42	MOV File	3,996,674 KB
DJI_0009	29/06/2017 15:42	MOV File	691,736 KB
DJI_0011	29/06/2017 15:46	MOV File	2,642,475 KB

Images and videos stored within 100Media Folder

Appendix D

Question	Response
● Could you please state your official job title?	● Digital Forensic Analyst
● How long have you been working in forensics and within your current role?	● Placement year in Wales and then worked there over the summer in the last two years of university ● Then worked there for 1 year before moving to SYP ● Total of around 2 ½ years at SYP
● Do you have an area of forensics that you find more interesting than the rest, or a specialism?	● Computers more than phones are his specialism, centring around the operating system, Internet artefacts etc. ● Phones are very interesting but change too often. Skills gained may change two years after you've learned them. Also there are skills/ methods that are specific for one particular phone model. ● Not disinterested in any part of forensics, but the file system and operating system is where the interest lies.
● How often would you say that you get Drone devices in your forensic department? ○ What are the types of crimes associated with these cases?	● Very rarely get a device in. Maybe one a year on average. ● The very few they have had have been drug related cases flying drugs into prisons. ● One example was a drone that had crashed in the vicinity of a prison and it had to be examined to see whether or not it had been used for the drug delivery purpose or had the drone just happen to have been flying around the prison. The outcome was the latter. ● The second case was also drug related and the suspects had been caught and the drone device seized. The investigation wanted to know where it had been used. Didn't directly work on the case but was aware of the process and outcome as the department personnel get 'excited' whenever a drone comes in. Drone was traced back to Manchester where it was being used to drop drugs to prisons.
● You worked at a Welsh constabulary before SYP, were Drone devices more popular there?	● The Welsh constabulary cases were drug related. Wanting to know the flight path etc.
● Do you see the field of Drone forensics expanding?	● Yes. Criminal cases involving drones are rare. Mainly civil cases. See it staying that way for now, staying fairly rare. ● Foresees new laws surrounding drones coming in regarding videos and images with the new laws coming in regarding upskirting. Thinks in the future that flying a drone over a beach for example and capturing images of people sunbathing will be an illegal act. ● Thought there would be a massive increase in the use of drone devices when they were commercially available. However, there wasn't really any surge in the use of them in criminal acts. Thinks that it comes down to people still delivering/ exchanging drugs by hand and using technology such as burner

	phones to suddenly buy and start flying drones to deliver goods.
● What are the current protocols that must be followed when extracting evidence from a Drone device? Are they similar to Mobile protocols?	● Pretty similar to mobile devices. Essentially just remove the SD Card and forensically image it, following the same procedures as dealing with other mobile devices and removable media. Write blocker, make an E01 etc. ● If it a more serious case, a chip off could be called for. But that takes a long time to carry out and all drones are different. It will probably land to someone with expertise in mobile phones to try and work out which pins to utilise etc. ● Drones are at the minute a bit of an unknown. ● Normal procedure is to analyse the SD card and if the officer is satisfied with the evidence located, it probably wouldn't go any further. Especially if nothing can be gained from the SD Card. The more data that can be gained from the SD Card, the more likely it is that the officer will request further analysis of the device, i.e. chip off and apps on phones. As drones can be expensive, you have to justify taking it apart and risk damaging the device. ● Tend to get more information off the phone app ● Some drone controllers store data also. colleagues in Derbyshire informed me, they have a specialist drone unit. ● Not getting enough devices in at the minute to warrant a specialised set of procedures. ● Could outsource the extraction of data if required e.g. chip offs. Never outsourced any though.
● Do you think that the ACPO principles need to be updated to be more inclusive of Drone devices as well as mobile devices? ○ Do you think there should be a separate set of principles solely for Drone devices?	● Don't think they are as outdated as they could be considering how old they are. The first principle of 'don't change data' can be an issue, especially with phones as you change data as soon as it is powered on. However, the second rule of 'if you are competent to change data, you can' is a good cover as if you are working in forensics you will generally be competent. ● If I were to change ACPO principles, it wouldn't be any of the first three. It would be point four. Maybe re-word it or something similar. ● Generally points 1, 2 and 3 are still very valid in current times. They have aged very well. ● Even relevant for drone work. ● Don't think drones justify getting their own set of principles, as then there would be a different set of principles for a lot of other types of devices and would end up with ACPO Principle 99, 125 etc.
● Do you know anything about the current legislation on Drone devices?	● Do not know very much about current drone legislation, only that it is an illegal act to fly them in the vicinity of the airport. ● It isn't a requirement of the job role to be aware of current legislation.

	● Generally if crimes involving breaking legislation rules were committed, the CAA would take the investigation not the police. It is thought that they will have their own team of forensic experts/ investigators to analyse devices.
● Does your forensics department send its staff on regular training courses regarding new methods of extracting data and changes/ additions to legislation?	● Not required to attend any courses or read new legislation on a regular basis. ● Investigators get to know a lot of the legislation whilst they are working on devices. ● Legislation is mentioned within other courses on forensics. ● Normally the process of dealing with legislation is dealt with before the artefact gets to us. We usually only have to worry about working within RIPA.
● Have you encountered any Anti-Forensics techniques when examining devices? ● Do you think that Anti-Forensics techniques could be used on a Drone device? ○ If so, which ones? ○ How difficult do you think it could be to do this, i.e. could a novice user do it or would it have to be a highly skilled technically minded user?	● Yes. It is a big issue that can cover a lot. Tools such as BitLocker and CCleaner are classed as Anti-Forensics tools. CCleaner forensically wipes (i.e. 0s everything) and encrypts and can do so on schedule. BitBleach, Eraser are also classed as Anti-Forensic tools. Tend to comment of their instillation within the final forensic report. Encryption is also seen as Anti-Forensics. BitLocker, VeraCrypt etc. Section 49 of RIPA allows officers to force suspects to disclose their password depending on the case. It is very difficult to get a RIPA 49 order. It has to go through a judge to be signed off and has to be proved that you have tried to get into the evidence. ● It depends on whether the user or the manufacturer implemented them. For example, fairly easy for the manufacturer to make every bit of data encrypted on the board. More difficult for a user of the drone to implement. Maybe set up a schedule on an Android to wipe the content of the app if it hasn't been opened in x amount of days. Standard users would find it difficult to carry out anti-forensics techniques on drone devices.