



LEEDS
BECKETT
UNIVERSITY

Citation:

Thornton, G and Bagheri Zadeh, P (2022) An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis. *Forensic Science International: Digital Investigation*, 41. p. 301379. ISSN 2666-2817 DOI: <https://doi.org/10.1016/j.fsidi.2022.301379>

Link to Leeds Beckett Repository record:

<https://eprints.leedsbeckett.ac.uk/id/eprint/8675/>

Document Version:

Article (Published Version)

Creative Commons: Attribution 4.0

The aim of the Leeds Beckett Repository is to provide open access to our research, as required by funder policies and permitted by publishers and copyright law.

The Leeds Beckett repository holds a wide range of publications, each of which has been checked for copyright and the relevant embargo period has been applied by the Research Services team.

We operate on a standard take-down policy. If you are the author or publisher of an output and you would like it removed from the repository, please [contact us](#) and we will investigate on a case-by-case basis.

Each thesis in the repository has been cleared where necessary by the author for third party copyright. If you would like a thesis to be removed from the repository or believe there is an issue with copyright, please contact us on openaccess@leedsbeckett.ac.uk and we will investigate on a case-by-case basis.



Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis

Greg Thornton, Pooneh Bagheri Zadeh*

Leeds Beckett University, United Kingdom Leeds Beckett University, United Kingdom



ARTICLE INFO

Article history:

Received 24 June 2021
Received in revised form
8 February 2022
Accepted 26 March 2022

Keywords:

Drone forensics
Mobile forensics
Unmanned aerial vehicle (UAV)
Ground control station (GCS)
Digital forensics investigation framework
ACPO guidelines
Digital forensics

ABSTRACT

Recent developments of drone technologies have shown a surge of commercial sales of drone devices, which have found use in many industries. However, the technology has been misused to commit crimes such as drug trafficking, robberies, and terror attacks. The digital forensics industry must match the speed of development with forensic tools and techniques. However, it has been identified that there is a lack of an agreed framework for the extraction and analysis of drone devices and a lack of support in commercial digital forensics tools available. In this research, an investigation into the extraction tools available for drone devices and analysis techniques has been performed to identify best practices for handling drone devices in a forensically sound manner. A new framework to perform a full forensic analysis of small to medium sized commercial drone devices and their controllers has been proposed to give investigators a plan of action to perform forensic analysis on these devices. The proposed framework overcomes some limitations of other drone forensics investigation frameworks presented in the literature.

© 2022 Elsevier Ltd. All rights reserved.

1. Introduction

With advances in the digital technology world in the 21st century, Digital Forensics (DF) sciences and its applications are at the heart of the criminal justice system, from triage and incident response stage at the crime scene and analysing the evidence to finally presenting the evidence to a court of law. Recent improvements in drone technology have significantly increased the commercial drone sales and usage amongst the public. It is estimated that the global drone market may reach \$127 billion by 2020 (Jain, 2017). However, the availability and ease of access to drones has created new issues for society in relation to drone misuse, such as invasions of privacy, disturbances at airports and transporting illegal goods (Attoe, 2018; Azhar, 2019; Shafi, 2019). Law enforcement has encountered difficulties such as in Washington Township, Pennsylvania where drones were being used by an individual to disperse homemade bombs and nails in a suburban Neighbourhood (Swales, 2019). Suffolk Police have identified that drones were being used by criminals to survey residential areas to identify targets, in which one drone was directly linked to a burglary in Suffolk (How Drone Technology Is B, 2015).

A drone, also referred to as an Unmanned Aerial Vehicle (UAV) (Clark et al., 2017) is defined as a remotely controlled aircraft, which is capable of capturing images and videos, with the ability to transfer the data to a remote server or Ground Control Station (GCS) (Kamoun et al., 2019; Singh, 2017). A GCS is the device that is used to operate the drone and could manifest as a mobile device such as a smartphone, tablet or laptop controlled by a user (Kovar et al., 2016). An Unmanned Aerial System (UAS) is made up of all components used to operate a drone device and includes but is not limited to; the drone or UAV, the GCS, the owner of the aircraft (UAS operator) and the person who is operating the aircraft (remote pilot), as they all play a role in operation of the drone and therefore are all sources of data (Civil Aviation Authority). A significant aim of drone forensics is to establish a link to the owner of the device (Gulatas, 2018a). Drone forensics presents new challenges to the digital forensics industry due to the customisability and amount of drone devices available to the public (Miller, 2018). Forensic tools and techniques are required to collect data while preserving the original state of the device as best as possible (McFarland, 2017).

The National Institute of Standards and Technology (NIST) have compiled a dataset of drone extractions as part of the CFReDS (Computer Forensic Reference Data Sets) project, which can be used as “simulated digital evidence for examination” (Livelsberger and Fed, 2018). This may be used as a way of validating forensic software as part of laboratory accreditations such as ISO:17025 (The

* Corresponding author.

E-mail addresses: greg.thornton@md5.uk.com (G. Thornton), P.bagheri-zadeh@leedsbeckett.ac.uk (P. Bagheri Zadeh).

CFReDS Project, 2019). The drone images were created by VTO Labs as part of a contract from the Department of Homeland and Security, with the primary aim of allowing investigators to perform a “dry run” on a drone extraction before working on high profile cases. Teardown instructions for drone devices are also included as part of the dataset (Press, 2018). Three of each drone model were acquired and a different extraction method was performed on each drone. One drone was extracted while remaining intact, one by extracting directly from the circuit board and one by removing and extracting from the chips directly (Leonard, 2018).

The lack of a comprehensive framework for handling, extracting from and analysing drones means that differing methods are used across industry and during research processes. As a result, it is likely that the outcomes of investigations have high variance in the successes and failures relative to each other without the knowledge of what the best practices are for handling UAVs that are seized by police. If a comprehensive framework were created which attempted to cover all aspects of the forensic procedures, it could create a basis for all digital forensic practitioners to follow, resulting in more consistent results from drone investigations. Current forensic principles such as ACPO (Association of Chief Police Officers) guidelines provide a good basis for forensic examinations but are generic and possibly not applicable in some cases, as can be found for mobile device forensics. Performing a full analysis on a mobile device such as a smartphone or a drone may not be possible without booting the device or loading software onto the device to successfully extract data from the device (Al Mutawa et al., 2012). This would contradict principles 1 and 2 of the ACPO guidelines, as you must modify data on the device and access live data to perform these actions (Good Practice Guide, 2012). Although practitioners should aim to follow these principles, it is not always possible.

In this research, a digital forensics investigation framework for the data extraction and data analysis of drone devices and related devices is proposed. Four drones and four drone controllers were used to create datasets which simulate the use of a drone, which were extracted using Cellebrite UFED and Oxygen Forensic Detective forensics tools. Extracted data from the devices was used to identify what artefacts are available during an investigation based on which device is seized. The extractions performed were also compared with extractions provided by the NIST, as a method to validate the results of the experiment and identify how different extraction methods can yield different results. Drones were extracted using forensic tools where possible, but alternatives were considered if forensic tools did not provide support. More advanced and destructive methods such as chip removal were possible, however they are not included in the scope of this research due to cost constraints. The new digital forensics investigation framework is proposed based on the created results.

2. Background

There are several identified issues facing digital forensics practitioners who are tasked with retrieving data from drone devices and their GCS, such as identification of the suspect, the links between the drone and the controller, and establishing ownership of the devices. It is possible that the controller of the drone is not always recovered with the drone as they can be operated from distances of 10 km away using devices such as the DJI Smart Controller (mart Controller - De) making it difficult to pinpoint the location of the controller at the time of the flight. The lack of a standard for drone file systems and logging features means the capabilities of a drone can vary depending on the model of the drone, as well as any customisations that may have been made to the drone. Bouafif et al. (Bouafif et al., 2018) found that the ownership of a Parrot AR drone could not be established from the

drone alone and required the GCS to prove ownership, despite being able to fully extract the file system from the device via serial connection.

Yousef and Iqbal (2019) identified the importance of retrieving all components which are used to operate a drone, mainly the devices used to control the drone and the destination of any backups of the drone or the controller. An investigation was performed on a DJI Mavic Air and an iPhone 6 that was used to control the drone. The microSD card of the drone was removed and imaged using FTK Imager Lite, then verified using Autopsy. The iPhone data was extracted using Apple iTunes Backup. Data relating to the drone was successfully retrieved from the drone and the controller, such as multimedia (Images and Video) on the SD card and the DJI GO 4 app plist files from the controller. Several file paths and file naming conventions were identified for DJI drone files. The main source of data identified was the log files created by the drone, which were saved on the drone in.DAT and.TXT formats. The TXT files were visible in clear text, but the DAT files were encrypted and required decryption to view the data.

The importance of the drone controller was also emphasised by Hamdi et al. (2019), as they state that an extraction on the controller used can prove a link to the drone through multimedia or app data relating to the drone. A DJI Phantom 4 was analysed as well as a set of smartphones used to control the drone (Android and iOS). Both operating systems contained application data relating to the DJI GO application which was used to operate the drone. Personally Identifiable Information (PII) could be identified from the app such as any email addresses used to log into the application as well as the username of the account. Similar to the study by Yousef and Iqbal (2019), log files in.DAT and.TXT formats were found to be the best source of data which could then be converted into visualisations showing flight routes that the drone took. However, forensically sound tools were not used in either of these investigations to retrieve data from the controller as they both used iTunes backup. Although standard methods will create backups which appear like an iTunes backup, the device may be modified if the correct settings are not altered in iTunes. For example, if iTunes sync is not disabled this may alter data on the device. In addition, creating a backup without a password may result in more sensitive data not being recovered such as the keychain, call logs or browsing history (Katalov, 2020).

Analysis performed on a DJI Phantom 3 and a Parrot AR Drone by Barton and Azhar (Barton and Hannan Bin Azhar, 2017) found that similar artefacts and metadata can be found from drones made by different manufacturers but the format for each of these artefacts is proprietary. Both drones also stored data on the smartphone that was used to control the device and used removable storage to store multimedia captured during flights. However, the extraction methods for internal storage were different. The Phantom 3 was put into “flight data mode” via the DJI GO application which enabled it to be extracted via the drone’s micro-USB port. The AR drone did not have this capability and was required to be powered on and accessed via Wi-Fi as it had no hardware ports that allowed access to the internal storage. It was identified that this may not be forensically sound as powering on the device and enabling network capabilities could change data on the drone. Chip-off was identified as the most forensically sound option to extract data, however it does impair the drone’s functionality. The applications found on the devices contained several artefacts which could be used to identify the owner such as the account name associated with the application and the email address used to download the application.

Salamh, Mirza and Karabiyik used a chip-off extraction method and other extraction methods to extract data from a DJI Phantom 4 and Matrice 210. They found that a chip removal produced the most comprehensive method to extract data from the drone, but this

meant that the drone could not be repaired to its original state. A key point that they identified from the investigation was that a range of tools should be used during the investigation of a drone as different tools can provide better results when decoding and parsing the extracted data. It was found that DatCon was the most reliable tool for parsing DJI DAT files, and was more effective than forensic tools such as Autopsy, Magnet AXIOM or Cellebrite UFED. AXIOM could not decrypt the DAT files, while Autopsy could but would display incorrect timestamps for the first few entries of the log files. DatCon could decrypt the DAT files successfully and provided additional data such as the roll, pitch and yaw and allowed the results to be exported to CSV files for easier analysis using further tools such as Google Earth. Although they acknowledge the GCS as part of the system, they do not incorporate this into the investigation and do not identify or follow a framework for the investigation (Salamh et al., 2021b).

Kao et al. (2019) also found that the internal and external drone storage as well as the controller were all required to perform a full analysis on a drone. A DJI Spark was analysed and it was found that this device records logs internally but stores multimedia to an external SD card. The DJI GO 4 application was used to control the drone using a smartphone, therefore it is important that the controller is also analysed. It was found that the application data on the controller contained log files and multimedia on the controller. The DJI GO application allows the user to take snapshots while the drone is in flight, which will only be stored on the controller and were not found on the drone and they had less precise GPS coordinates in the EXIF data. It was found that the same video files that were found on the SD card were also on the controller but had slightly different timestamps. This was found to be due to the network delay for the data to be transferred via QUIC (Quick UDP Internet Connections). A key principle of the investigation was the Locard exchange principle that states when two objects come into contact there will be traces of this contact, or communication in terms of digital forensics. The Locard exchange principle was proven by the data found connecting the drone, the controller and the SD card as matching multimedia files, device metadata and user accounts were found on one or more of the devices showing a link between them. Some examples of this are the drone make and serial number, flight logs and multimedia timestamps or GPS coordinates. Although some multimedia files metadata differed slightly this was explained by the network delay for sending files between the drone and the controller. Analysis of entries in the log files resulted in no data that could be linked to the SD card or the controller.

Some non-smartphone controllers may contain a storage capacity which stores telemetry and logging data; however, they would not contain an internal storage capacity for user data such as multimedia files. In some cases, this data can be extracted from the controller by directly connecting to a forensic workstation, but more advanced methods such as JTAG or chip-off may be required to extract from the controller, which would likely result in destroying the controller (Interpol, 2019). However, Salamh, Karabiyik and Rogers identified that some controllers such as that of the Yuneec Typhoon H could be connected to and contain a file structure on an internal IC chip. They emphasized that it was important to use forensically sound methods to extract data, suggesting Autopsy as a forensic tool to use to extract data. Autopsy is a well-known forensic extraction and analysis tool, but is an open-sourced tool that does not have the range of capabilities of other forensic tools such as MSAB XRY or Cellebrite UFED (Salamh et al., 2019).

A wireless connection is required to connect to the full file system of a Parrot Bebop according to Horsman (2016), as only a media folder is visible when connected to a computer. As a result of

this, typical forensic tools such as FTK Imager cannot be used to obtain a physical image of the drone. To access the whole device storage, a connection must be made to the drone via Telnet or FTP. Using an FTP connection results in restricted access to the "internal_000" folder, whereas connection via Telnet allows access to the complete system. As the Bebop drone uses a Linux file system, standard tools such as the dd command is applicable. This does however mean that a user may be able to access the drone's internal storage using the same methods and modify the internal storage of the drone using standard Linux tools. However, it may be possible to identify commands used on the device via the ".ash_history" file, which logs commands that are run via SSH provided that this has not been tampered with VCONNECT-IT (vconnectit). The bash logs can also be reviewed, which show commands that are run by regular users and is a feature on most Linux platforms (Hoffman). Every time a connection is established to the drone, a ".pud" file is created which contains details of the connection such as the date and time of the flight and the serial number of the UAV. These ".pud" files contain data relating to the movements of the drone and its controller during a flight. The results of the experiment found that it was not possible to establish ownership of the drone if the controller is not also obtained. However, if the controller were to be retrieved the Freelight 3 application that is used to control the drone would contain metadata such as the drone serial number embedded in XML (Android) or Plist (iOS) files based on the operating system (Horsman, 2016).

Salamh et al. used wireless connections to connect to a drone, but performed this on a VTI Phoenix and DJI Matrice 210 in order to gain access to the drone. A common vulnerability on the telnet port was used to perform a brute force attack using Kali Linux and gain access to the drone while it is in operation. From this the drone's internal memory could be accessed and transferred. DAT files were recovered from the drone, which were then decrypted using DatCon and visualised using Google Earth. An eight-stage framework was created with the purpose of gaining unauthorized access to a drone in order to disrupt the use of the drone and to recover data from the drone. Although flight logs were recorded, the methods used for the extraction were intrusive and not forensically sound. This method may also compromise the drone if an attack is detected by the drone, initiating security features such as auto-shut down or wiping the device when an intrusion is detected (Salamh et al., 2021a).

It is widely accepted that the ACPO guidelines should always be followed during forensic investigations to maintain the integrity of the device and the reliability of the evidence provided from the investigation. Although simplified statements, the four principles of ACPO guidelines create a basis for digital forensics investigators to follow when handling digital evidence to maintain its integrity and therefore its admissibility in a court. This is because the same laws are applied to all digital evidence, so it should have the same underlying principles for preserving the integrity of the evidence (Good Practice Guide, 2012). It is important that a chain of custody is maintained from when an exhibit is seized and is always accounted for while in possession. This is used to prove that the evidence seized at a crime scene is the same evidence and has not been tampered with (Badiye et al., 2020) and that it has been preserved (Saleem et al., 2016). Continuity forms are maintained to identify who has had access to the evidence and at what times and dates they have had access, which can be used to create a timeline of where the evidence has been after seizure, in addition to sealed exhibit bags which preserve evidence and prevent tampering (Obbayi). If the chain of custody is not maintained, it cannot be proven beyond reasonable doubt that the evidence relates to the suspect or has not been tampered with in any unexpected way, resulting in evidence potentially being inadmissible in court (FutureLearn).

A good practice for data verification was identified by Stanković, Mirza and Karabiyik, who used two separate workstations to perform extractions in order to eliminate any software bias or limitations. The forensic tools Autopsy, Magnet AXIOM and Cellebrite UFED were used for extractions on the drone and the GCS, which are industry standard tools that offer a range of extraction and analysis features. An Apple iPhone and a Samsung smartphone were used as a controller for the drone, to identify sources of data from the two major smartphone controller operating systems. It was identified that smaller drones have significantly less extraction support options, and emphasised that it is essential to extract from the controller whenever possible. An extraction of the drone's external memory card was performed; however, no extractions of the drone's internal memory were extracted as they were not detected by the forensic workstation (Stanković et al., 2021).

Yousef, Iqbal and Hussain identified that a DJI drone could not be detected via a Tableau physical hardware write blocker, but extractions could still be performed by connecting it to the workstation through non-write blocked methods. They identified that it is essential to extract from all components of the system as they all contain rich sources of information relating to the operation of the drone. Extractions were successfully performed on the drones internal and external memory using FTK Imager, while the iPhone controller was extracted using iTunes backup. Yousef et al. suggested that investigators should not rely on only one tool, but should have multiple tools available for various purposes. It was also identified that the difficulty of extracting from and decoding data from drones is becoming more difficult due to improvements in the security of the devices, and suggest that more novel methods may be required for these. No forensic framework appears to have been followed for the investigation or suggested for future investigations, which could be implemented to aid the repeatability and consistency of similar future investigations (Yousef et al., 2020).

Al-Samman et al. (Al-Samman and Al-Hadhrami, 2021) reviewed the current drone forensics investigation models and identified challenges and potential approaches to mitigate the current issues using the Design Science Research method. They proposed a generic investigation model, however, the model has not been tested against any UAVs or drone datasets to evaluate the performance. Mistry and Sanghvi (2021) discussed how digital forensics investigation techniques perform from drone acquisition, evidence collection, data analysis to the reporting phase, which then led to suggesting a general legal procedure to collect and analyse drones from the crime scene and then investigate them inside the lab.

Jain et al. (2017) suggested a 12-step methodology which aims to cover all processes during the recovery, extraction, analysis and presentation of data from drone devices, which are to be followed in a waterfall styled process. A large emphasis is placed on identifying the hardware features of a drone as they are typically modular allowing for a large amount of customisation. The range of features available in drone devices means an excellent knowledge of drone hardware is required to identify and classify the drone as well as identify tools and techniques required for future processes. However, little emphasis is placed on the extraction tools and techniques, as well as the need for them to be forensically sound.

A more granular 20-step methodology is proposed by Roder and Choo (2018) which places emphasis on creating an action plan based on the circumstances of the crime and the devices available. This methodology also includes other forensic practices such as wet forensics and ballistics to identify if any evidence can be found which can later be associated with a suspect, such as fingerprints or DNA on the device. Multiple steps involve the classification and identification of the drone using observations and open-source

tools to determine the capabilities of the drone such as storage medium locations and the payload or modification capabilities of the device. Forensic copies of data, including the GCS (smartphone or tablet) are then created and interrogated using traditional digital forensics methods. This data is then output in the form of a report or statement.

Renduchintala et al. (2019) developed a forensic framework for drone forensics which includes processes for hardware forensics and digital forensics of drones. A software application was created which interprets log files created by DJI or Yuneec drone devices, which creates summaries of the device metadata, flight routes and device diagnostics such as battery life or roll, pitch and yaw. A key issue identified was the additional difficulties created when a drone is recovered without the controller, however no processes for controller forensics are produced. It was identified that there is a need for interpretation software to convert bespoke log file and multimedia formats to a uniform output, which can then be used in visualisation software such as Google Maps or the application created during the project. An illustration of the framework outline is shown below in Fig. 1. Although this framework outlines the key processes of drone forensics and some best practices, little is provided in relation to the physical handling of the drone and the extraction methods and tools that are available as well as the reliability of these tools in forensic investigations.

Gülataş & Baktir (Gulatas, 2018b) suggested a framework that consists of 7 stages: Preparation, Scene Control, Customisation Detection, Data Acquisition, Evidence Authentication, Evidence Examination and Presentation. It is suggested that many widely accepted principles such as prevention of data loss, chain of custody and avoiding adding data are followed where possible to maintain the integrity of the data. The importance of hashing and creating working copies are also included, which proves the integrity of data extracted from devices is maintained, while also working from copies of the data rather than the original source. This is to maintain that evidence is authentic and will be admissible in court. An important aspect of the framework is that it includes all components used to operate the drone and the whole system is referred to as a UAS. This includes the GCS (Ground System Controller) which could be a smartphone or tablet, as well as any remote storage locations such as a computer or cloud service. These components can be crucial in a digital forensic investigation as a link between the devices can prove ownership and usage of the drone. The framework suggests that data should be verified using hash values, which is effective for devices which have removable storage, but devices which have internal storage this is not often possible, such as the GCS. This is because data is altered slightly when the device is powered on and when extraction tools are loaded onto the device to perform an extraction. This would mean that a hash value may be used for individual files but not the acquired image of the controller

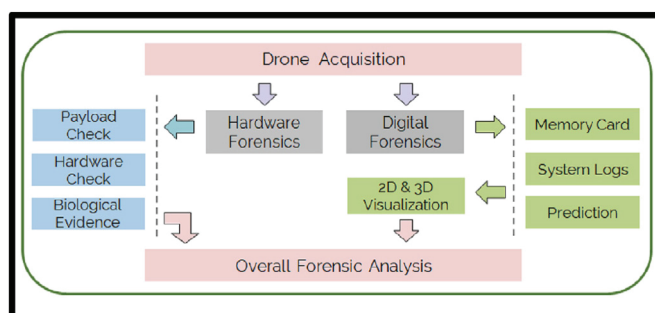


Fig. 1. Drone Forensic Framework Proposed by Renduchintala et al. (Renduchintala et al., 2019).

as this is likely to be different every time an extraction is performed. An alternative to this for the GCS would be to perform a manual review of data and dip sample the extracted data against data found on the GCS.

Flight logs were identified as the main artefact retrievable from drones by Renduchintala et al. (2017) and a framework was created for analysing drone flight logs. The three key stages were identified: During Flight, Extraction and Details of Logs and finally Visualisation using JavaFX. Log files will start recording data as soon as the drone powers on, so they capture all events that the drone will perform. These logs are then extracted from the device and converted into visualisations using JavaFX. It was found that the formatting and storage locations of the drones was proprietary and differed for every manufacturer. The lack of a standardised logging format presented the challenge of interpreting multiple different formats of log files. In addition to this, some log files were stored on the GCS or were encrypted. It is also possible that cheaper drones may have basic logging capabilities only, or no logging features at all. An illustration of the framework suggested for interpreting log files is shown in Fig. 2. Although the framework produced by Renduchintala et al. is excellent for performing an analysis of log files recovered from drones, this framework does not include other data sources such as multimedia and EXIF data, user data from the GCS or finding connections between the drone and the GCS.

In 2018, Iqbal et al. (2018) performed an investigation on a Parrot Bebop 2 drone and a basic framework for drone forensics was created. It was found that Bebop 2 drones had a vulnerability with its FTP port being open to all devices, which was shown to be compromised by an external Linux system. Access was gained to the drone, which was used to disconnect the GCS and power off the drone while in use. It was proposed that this could be used as a method to disable a drone in a no-fly zone and seize the drone. The four stages of the framework are: Confiscate UAV, Process UAV, Forensic Analysis and finally Document, Report and Present. This provides a generic overview of the forensic processes that will be performed on the drone but does not consider the GCS or any other associated devices which would be of high evidential use. This method was only tested on one drone and could be unsuccessful for drones with different manufacturers or security techniques.

A framework is required for UAS forensics due to the recent developments in the drone device products available to the public, which has resulted in more cases of criminal misuse of the

technology in small-scale and large-scale issues. In addition to this, there is a lack of a widely accepted methodology in place to handle drone devices when seized, such as how to extract data from the device, what artefacts are available to investigators and the significance of the recovered artefacts. The next section of the article provides a detailed analysis of drone devices used in the experiment and suggests a proposed framework for the analysis of drone devices while also outlining any issues, controversies and problems encountered.

3. Main FOCUS OF the ARTICLE

In order to develop a digital forensics investigation framework, the drones listed in Table 1 below were used to create a set of artifacts. All drone devices were flown around a sports hall at Leeds Beckett University. A number of images and videos were captured during the flight for further analysis and investigation purposes. None of the devices were jailbroken at the time of the experiment. To follow the forensically sound manner in the seizure stage of the experiment, the drone and GCS were powered off and isolated from any networks and wireless connections by disabling any Wi-Fi and Bluetooth settings and enabling Flight mode if supported.

3.1. GT/1 - DJI phantom 4

GT/1 is a DJI Phantom 4 drone which was purchased second hand and was extracted before the experiment to identify whether the drone was factory reset or wiped before being sold. If the drone were factory reset, this would give an insight into what data is removed from the drone and what data remains after a wipe or

Table 1
Drones and smartphones used during the project.

Reference	Make	Model	Type
GT/1	DJI	Phantom 4	Drone
GT/2	Apple	iPhone 8	Controller (Smartphone)
PBZ/1	DJI	Mavic Pro	Drone
PBZ/2	Apple	iPhone 8	Controller (Smartphone)
PBZ/3	DJI	Mavic Mini	Drone
PBZ/4	Samsung	Galaxy S9	Controller (Smartphone)
PBZ/5	Yuneec	Mantis Q	Drone
PBZ/6	Samsung	Galaxy S10	Controller (Smartphone)

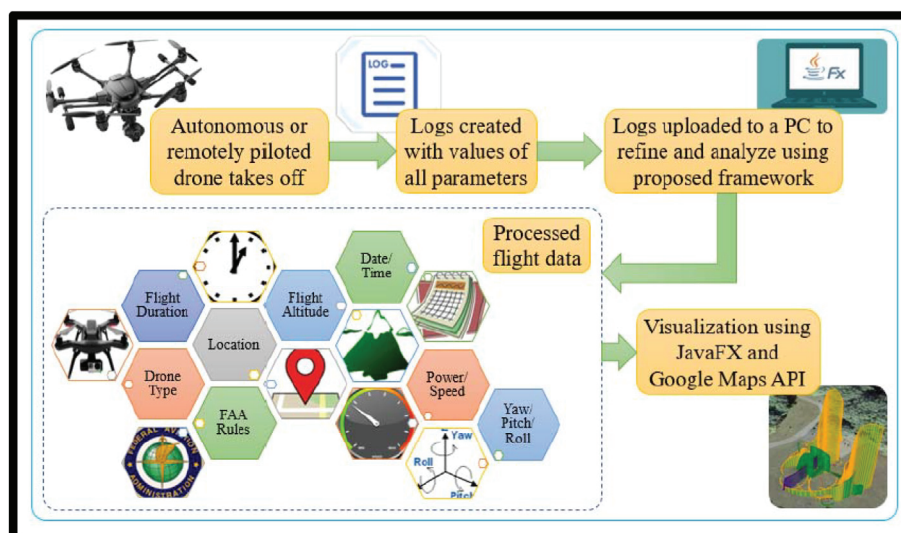


Fig. 2. Proposed framework for analysing drone log files (Renduchintala et al., 2017).

factory reset. A 32 GB MicroSD card was included with the drone, which would also be extracted and analysed. The drone was factory reset before it was flown using the DJI Assistant 2 application. Several supported extraction methods were successfully performed in Cellebrite UFED and Oxygen Forensic Detective before and after being factory reset, as well as after the experiment. It appeared that the drone had not been factory reset when purchased and data from previous flights performed by the previous user(s) were recovered. Log files, location data, videos and configuration settings were recovered from the drone and the provided memory card. A minimal quantity of metadata was recovered from the drone which was limited to the serial number of the drone and the serial number of batteries used in the drone. This metadata may be useful if the user were to attempt to remove the serial numbers which are physically printed on the drone and the batteries; however, they do not directly provide any link to the GCS or the owner of the drone.

Location data, log files and TXT files were found on the drone's internal memory. It appears that the location data was not recorded correctly by the drone, potentially caused by interference from the sports hall metal roof. Despite being factory reset, log files from previous flights were found on the drone, which appear to match the data identified from extractions before the drone was wiped. The log files were stored in.DAT format in the file path "NO NAME/FLYXXX.DAT". The file name is always in the format "FLYXXX.DAT" with "XXX" being replaced by an incrementing number e.g., "FLY141.DAT". A large number of events are logged for each flight, such as FLY141.DAT, which recorded 54,644 entries within an 18-min flight. Included in these entries are location data which stores the latitude, longitude and altitude of the drone at regular intervals (appearing to be every second if possible). Fig. 3 shows an example of a log entry decoded from GT/1.

Cellebrite Physical Analyzer successfully decrypted the.DAT files that were extracted from GT/1. All waypoints with their corresponding timestamps have been recovered, and a visualization of the flight route is provided. Fig. 4 and Fig. 5 show examples of flight routes decrypted from flight routes from previous flights of GT/1 visualized in Cellebrite Physical Analyzer.

Images, videos and configuration files were found on the drones external microSD card. Images were saved in JPG format with the

file name structure "DJI_XXXX.JPG" (XXXX being an incrementing number) in the "/DCIM/100MEDIA/" folder. Metadata was also recovered for images captured by the drone's camera, as shown in Table 2.

Video files were also recovered, which were stored in.MOV format in the same directory as the images. Minimal metadata was found in relation to images stored on the memory card, as the camera metadata was not included for this file. However, timestamps, file paths and an MD5 hash value were recovered for video files.

The NIST dataset DF006 provides an extraction of a DJI Phantom 4 which was created by removing the chip from the drone and extracting from the chip directly. This would have yielded the best results, provided that the chip is not hardware encrypted. Review of data extracted from DF006 showed that location data, multimedia, log files and configuration files were also recovered, which matched naming conventions, file paths and metadata recovered from GT/1. It appears that the forensic tools recovered the same data as what a direct extraction from the internal memory card would have but has not destroyed the device.

3.2. GT/2 - apple iPhone 8

GT/2 is an iPhone 8 (A1905) that was used to operate GT/1 using the DJI GO 4 application. Extractions were successfully performed on this device using Cellebrite UFED and Physical Analyser using an advanced logical (checkm8) extraction. It was found that a copy of multimedia files saved on the drone's memory card were also duplicated on the handset, however they contain less metadata and do not have matching MD5 values. Databases were also recovered for the DJI GO 4 application. The plist file "com.dji.go.plist" was found in the "/mobile/Containers/Data/Application/com.dji.go/Library/Preferences/" directory and contains metadata relating to the version of the application, the last user account used in the application and the serial number of the drone, as shown in Table 3. This shows that a link can be established to the drone from the GCS based on data extracted from the GCS.

The battery serial number (07JDD4W001022Z) was also identified in the plist file "bindInfo.plist", which is located in the "mobile/Containers/Data/Application/com.dji.go/Library/Application Support/bindInfo.plist" directory, as shown in Fig. 6 and Fig. 7.

The file "com.dji.assistant.plist" found in the "/mobile/Containers/Data/Application/com.dji.assistant/Library/Preferences/" directory contains the user account email and password related to the DJI assistant application, as shown in Fig. 8 and Fig. 9. The username is the email address will be the address used to create the DJI account, and may match the account used in the DJI Go application. This email address and password may provide further attribution to a suspect if this information is linked to other information, such as other user accounts with a matching email, or similarities in passwords.

The flight record "DJIFlightRecord_2020-12-11_().txt" was recovered from GT/2, which relates to the flight performed during the experiment. No location data was recorded from the flights, however all other data such as timestamps and elevation appear to have been recorded. The latitude and longitude are recorded as "0" for entries in the flight log, indicating that there may have been interference when retrieving GPS data. The metal sports hall roof blocking the signal was identified as the most likely reason for this error, as previous flights from GT/1 flight logs do contain location data, which are demonstrated in Fig. 10 and Fig. 11.

A manual review of the DJI GO application on GT/2 showed the username for the application and recent flights were visible on the handset. Some user data was available, but an internet connection was required to view the full profile details. Image and video files

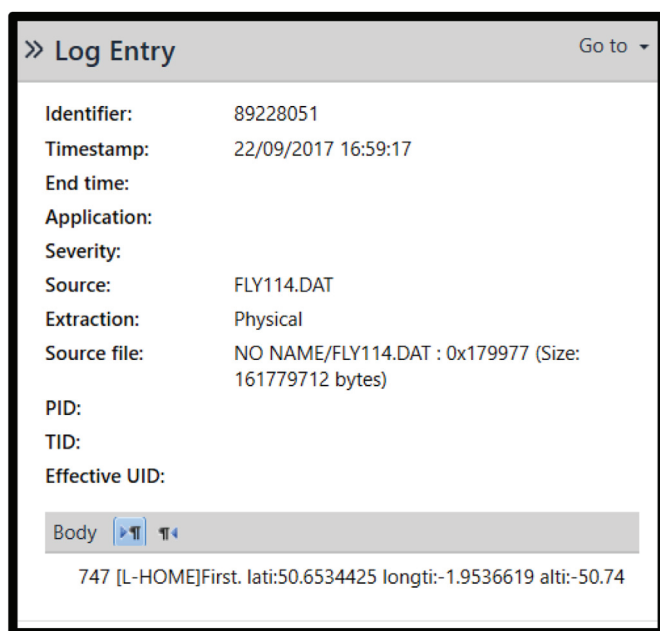


Fig. 3. A log within FLY114.DAT showing the drone's current GPS coordinates.

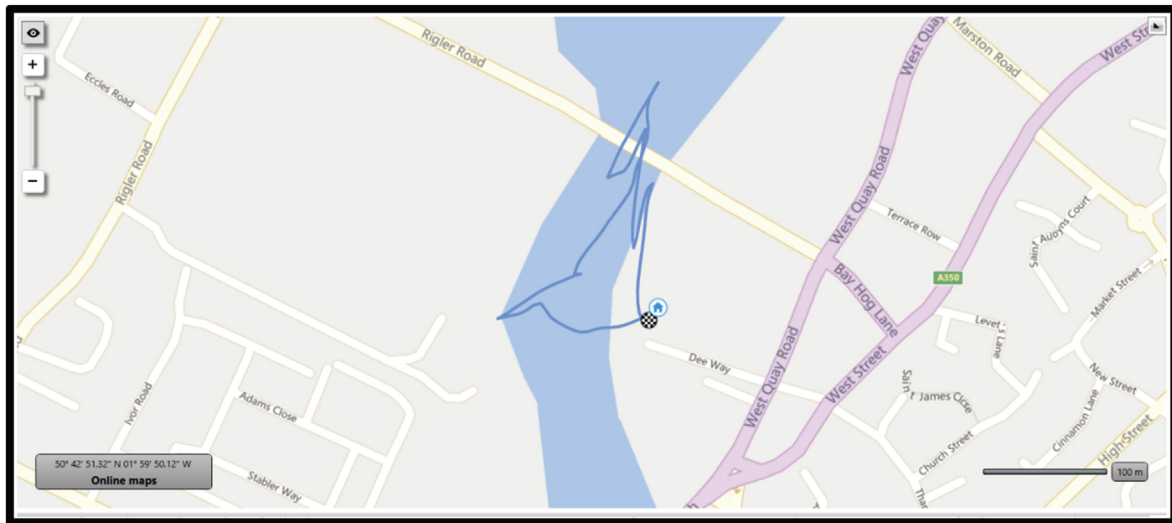


Fig. 4. The flight route recovered from the log file "FLY118.DAT".

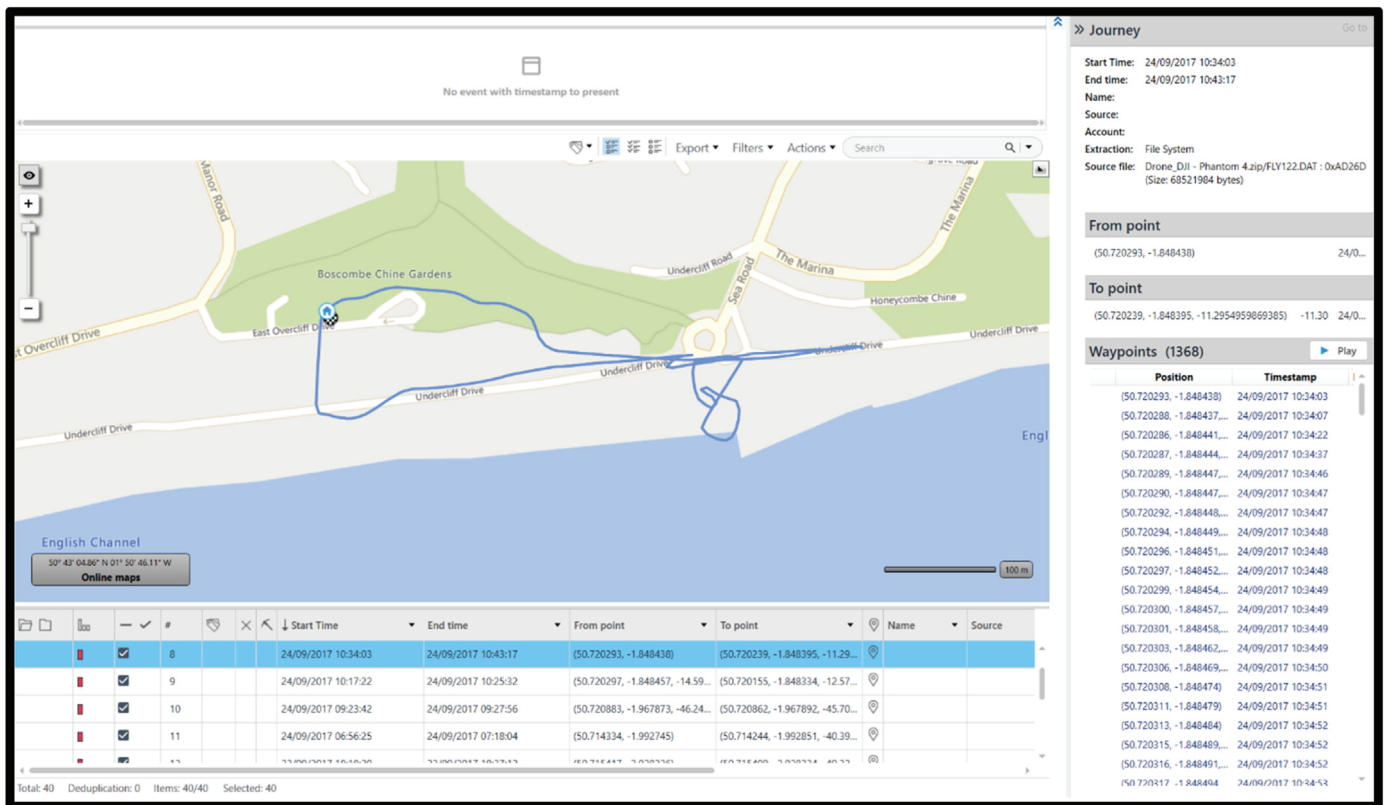


Fig. 5. The visualised flight route and corresponding data of "FLY122.DAT" from GT/1.

were found which visually match videos and images found on GT/1, however they do not contain metadata relating to the drone camera and do not have matching MD5 values. The pixel resolution of these files is 1280x720 (around the native resolution of the handset) as shown in Table 4, whereas the resolution of images on GT/1 were 4000x3000.

3.3. PBZ/1 - DJI Mavic Pro

PBZ/1 is a DJI Mavic Pro drone with microSD capacity and a

micro-USB data port, which was successfully extracted using Celebrite UFED. Location data and log files were successfully recovered from the drone, as well as minimal device information such as the drone serial number (08RDEA70010305) and the battery serial number (093AEBU03308NX). 228 log entries were recorded during a 4-min flight during the experiment, which were found in FLY051.DAT. The file paths for DAT files were "Drone_DJI - Mavic Pro.zip/flyctrl/FLY051.DAT", differing from GT/1 which is also a DJI drone but is a different model. Location data for the flight data during the experiment was not recovered, suggesting that there

Table 2
Metadata recovered relating to DJI_0034.JPG.

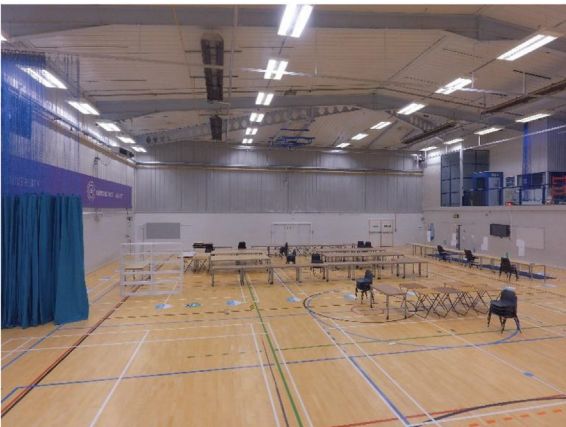
DJI_0034.JPG																											
	<table border="0"> <tr> <td>Name</td> <td>DJI_0034.JPG</td> </tr> <tr> <td>Size (bytes)</td> <td>5065353</td> </tr> <tr> <td>Path</td> <td>exFAT/DCIM/100MEDIA/DJI_0034.JPG</td> </tr> <tr> <td>Created Date</td> <td>11/12/2020 13:13:01</td> </tr> <tr> <td>Accessed Date</td> <td>11/12/2020 13:13:18</td> </tr> <tr> <td>Modified Date</td> <td>11/12/2020 13:13:02</td> </tr> <tr> <td>MD5 Hash</td> <td>2b28e49973a553cfa 527eb3884fb4144</td> </tr> <tr> <td>Camera Make</td> <td>DJI</td> </tr> <tr> <td>Camera Model</td> <td>FC330</td> </tr> <tr> <td>Capture Time</td> <td>11/Dec/20 13:13:01</td> </tr> <tr> <td>Pixel Resolution</td> <td>4000x3000</td> </tr> <tr> <td>Orientation</td> <td>Horizontal (normal)</td> </tr> <tr> <td>Lat/Lon</td> <td>0.000000/0.000000</td> </tr> </table>	Name	DJI_0034.JPG	Size (bytes)	5065353	Path	exFAT/DCIM/100MEDIA/DJI_0034.JPG	Created Date	11/12/2020 13:13:01	Accessed Date	11/12/2020 13:13:18	Modified Date	11/12/2020 13:13:02	MD5 Hash	2b28e49973a553cfa 527eb3884fb4144	Camera Make	DJI	Camera Model	FC330	Capture Time	11/Dec/20 13:13:01	Pixel Resolution	4000x3000	Orientation	Horizontal (normal)	Lat/Lon	0.000000/0.000000
Name	DJI_0034.JPG																										
Size (bytes)	5065353																										
Path	exFAT/DCIM/100MEDIA/DJI_0034.JPG																										
Created Date	11/12/2020 13:13:01																										
Accessed Date	11/12/2020 13:13:18																										
Modified Date	11/12/2020 13:13:02																										
MD5 Hash	2b28e49973a553cfa 527eb3884fb4144																										
Camera Make	DJI																										
Camera Model	FC330																										
Capture Time	11/Dec/20 13:13:01																										
Pixel Resolution	4000x3000																										
Orientation	Horizontal (normal)																										
Lat/Lon	0.000000/0.000000																										

Table 3
Metadata recovered from "com.dji.go.plist".

Data Label	Value
appVersion_pack	4.3.38
cached_sn_key	07JDD4W001022Z
DJIFirmwareReleaseDateKey	2020
DJIACCOUNTMANAGER_LASTUSEREMAIL	G.thornton7686@student.leedsbeckett.ac.uk
cached_product_name_key	P4
AIRCRAFT_FLIGHT_LOG_DEVICE_SN	07JDD4W001022Z
country	GB

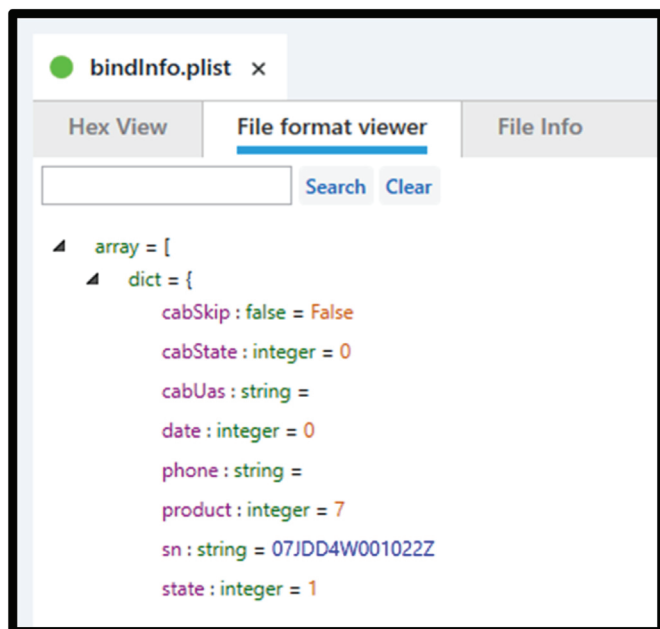


Fig. 6. GT/1 battery serial number identified in "bindInfo.plist" using Cellebrite Physical Analyzer.

may have been interference from the sports hall roof. Review of flights found on the drone before the experiment showed that the location data from "FLY049.DAT" was successfully decrypted from the DAT files by Cellebrite Physical Analyzer. A location recording is taken approximately every 15 s, which records the current time and

location of the drone, as shown in Fig. 9. The Flight Logs from FLY049.dat were input into Google Earth, which showed that the drone had been flown within a residential area. The timestamped geolocations were pinned on the map, which is shown in Fig. 12 and Fig. 13.

Configuration files and multimedia were recovered from the memory card, which were not found on the internal memory of the drone. Images files were found in JPG format in the "NO NAME/DCIM/100MEDIA/" file path with detailed metadata such as the make and model of the camera, creation, modification and access times as well as an MD5 hash value of the file. Video files were found in MOV format in the "NO NAME/DCIM/100MEDIA/" file path. Minimal metadata was found for video files on the memory card.

The extracted data was compared with NIST dataset DF0021, which showed that multimedia, location data and configuration files were recoverable from the drone. Videos and images were found in the same file paths and with the same metadata. However, there does not appear to be any device information (drone serial number and battery serial number) recovered from the device, but this may have been omitted or not available at the time of extraction. This shows that the forensic tools have extracted identical data compared to a NIST extraction which has removed the internal memory card from the drone and performed a direct extraction. As a result, the available tools are better to use than a direct extraction as they do not impair functionality of the drone or potentially damage the drone.

3.4. PBZ/2 - apple iPhone 8

PBZ/2 is an Apple iPhone 8 (A1905) which was used as the GCS to operate PBZ/1. The handset was extracted using an advanced

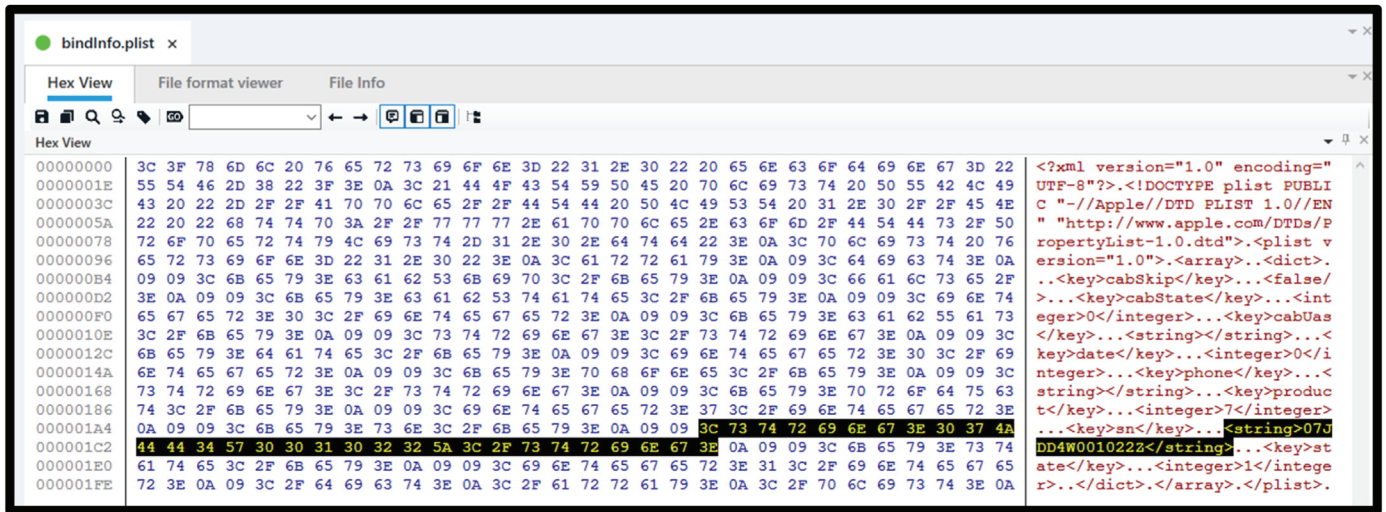


Fig. 7. Hex string relating to GT/1 battery serial number in "bindInfo.plist".

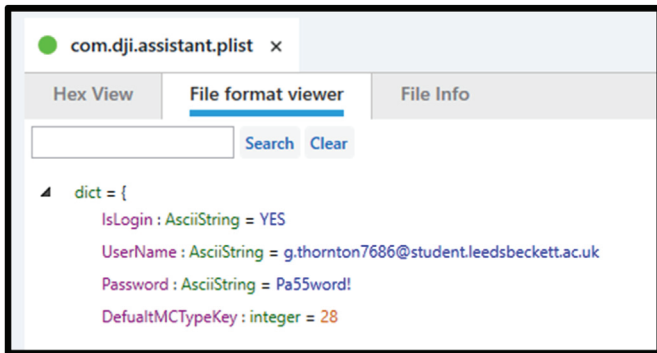


Fig. 8. User account information recovered from the plist "com.dji.assistant.plist".

logical (checkm8) method. The DJI GO 4 application was installed on this device to operate the drone. Extractions were successfully performed on the device, with multimedia, user account information, configuration files, databases and text files being successfully recovered. Device information for this drone was not recovered unlike GT/2 (drone serial number and battery serial number). Visually identical multimedia files were found on the handset which match images found on the drone memory card, however they contain less metadata and are a lower resolution. JPG images were found in the "iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/FlightRecords/DJIFlightRecord_2020-12-11_" (Miller, 2018; McFarland, 2017; Livelsberger and Fed, 2018; The

CFReDS Project (2019); Press (2018); Leonard (2018); Al Mutawa et al. (2012); Good Practice Guide (2012); mart Controller - De; Bouafif et al. (2018); Yousef and Iqbal (2019).txt" directory. Thumbnail files were found in the "iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/.mediaLibrary.Cache/Thumbnail/" file path, which have a filename which appears to be an MD5 hash value. Identical screen nail images were found in the "iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/.mediaLibrary.Cache/Screen nail/" directory, which appear to visually match the JPG images created by the drone and handset. Some images appear to only contain the screen nail and the thumbnail on the handset, while the original image is stored on the drone memory card, as shown in Table 5, Table 6 and Table 7.

For each thumbnail and screen nail image, a config file is found in the "/mobile/Containers/Data/Application/com.dji.go/Documents/.mediaLibrary.Cache/djifile" directory, with a name matching the thumbnail and screen nail image. This file contains metadata relating to the created date of the original image and the product that relates to the image. In Fig. 14 below, the product type is listed as "DJIKumquatX", this appears to be an internal product name for Mavic Pro (httpsbbs.dji.comthread-13, 1341). The config file also shows that a thumbnail and screen nail image were created for the original image.

The "com.dji.go.plist" plist file recovered from PBZ/2 shows the last user email, product key name and the version of the DJI Go application, as shown in Fig. 15. This file provides unique identifiers such as the last user email, which could be attributed to a suspect. Although no unique identifiers for the drone are provided, it is

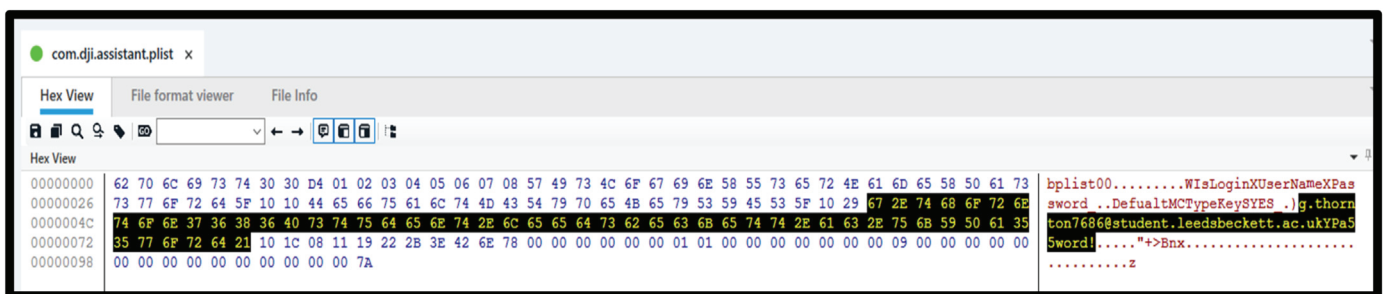


Fig. 9. User account information recovered from the plist "com.dji.assistant.plist" (Hex View).

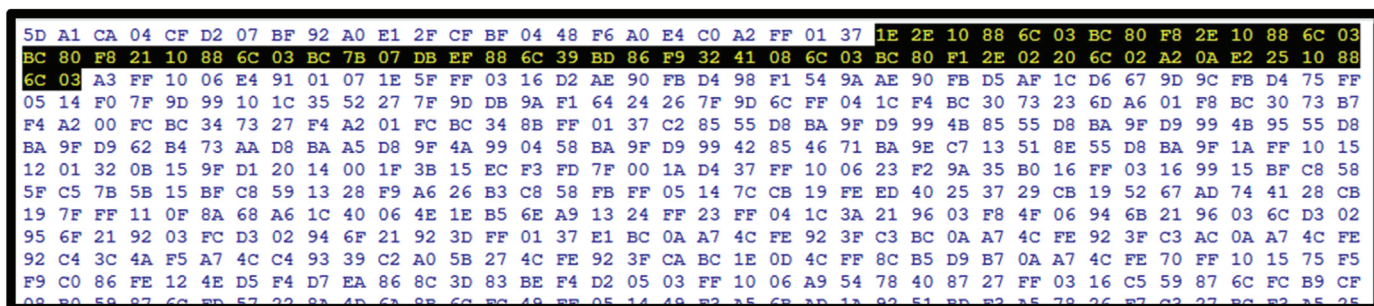


Fig. 10. Hex values for an entry in the log file " DJIFlightRecord_2020-12-11 ().txt ".

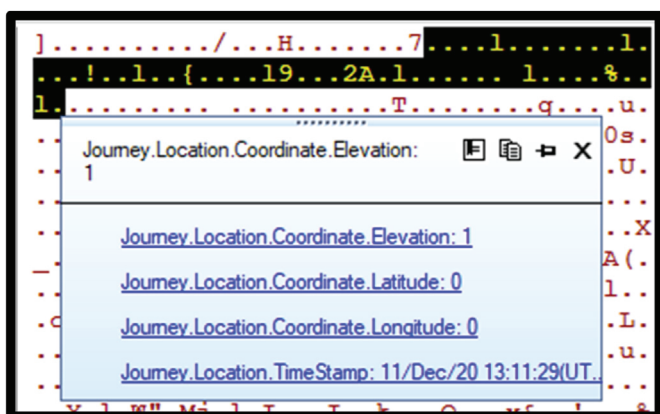


Fig. 11. ASCII and decoded entry from Fig. 10.

shown that the handset was connected to a DJI Mavic Pro drone. If the drone could not be located, the "com.dji.go.plist" file also contains the last known GPS location of the drone, as shown in Fig. 16. As the locations of the last flight were not recorded, the latitude and longitude are recorded as "0".

3.5. PBZ/3 - DJI Mavic Mini

PBZ/3 is a DJI Mavic Mini (MT1SD25) with an external microSD card. This drone was not supported in Cellebrite UFED or Oxygen Forensic Extractor. No extraction was performed on the drone. An extraction was successfully performed on the MicroSD card which was inserted in the drone. As this drone was only released in 2020, it is likely that support for this drone may be unavailable until tools have been created, tested, and verified as forensically sound. This

may present an issue to investigations as the need for the data must be weighed against the cost and risk of performing more advanced or less forensically sound procedures such as chip removal, which is also seen in mobile device forensics. The memory card inserted in this drone was previously used in GT/1 and was not formatted to identify whether this would affect data capture on the drone. It was found that no additional data was captured from the flight, but data from previous flights still remained on the memory card. As a result, no data was successfully captured for this drone. No NIST extraction was available at the time of analysis for this model of drone and a comparison of extracted data could not be performed for this device.


3.6. PBZ/4 – Samsung Galaxy S9

PBZ/4 is a Samsung Galaxy S9 smartphone which was used to operate PBZ/3. A decrypting physical boot loader extraction was used to extract data from the handset. The DJI Go application was installed on this device to operate the drone. As no data was successfully recovered from PBZ/3, it is vital that a connection can be found to the drone and the operator of the drone. Images and videos were successfully recovered from the handset which were taken during the operation of PBZ/3; however, they cannot be directly linked to the device from the metadata available. Video files were found in the "data/Root/media/0/DJI/dji.go.v5/DJI FLY/Video/" directory and images were found in the "data/Root/media/0/DJI/dji.go.v5/DJI FLY/Photo/" directory. Table 8 shows an example of an image recovered from the flight of PBZ/3.

3.7. PBZ/5 – Yuneec Mantis Q

PBZ/5 is a Yuneec Mantis Q drone with a 32 GB external memory card. This drone was not supported in Cellebrite UFED or Oxygen Forensic Extractor, therefore no extraction could be performed on

Table 4 Metadata relating to "DJIFlightRecord_2020-12-11_().txt_embedded_3.jpg".

DJIFlightRecord_2020-12-11_().txt_embedded_3.jpg	
	<p>Name DJIFlightRecord_2020-12-11_().txt_embedded_3.jpg</p> <p>Size (bytes) 160603</p> <p>File Path Greg's iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/FlightRecords/DJIFlightRecord_2020-12-11_().txt/DJIFlightRecord_2020-12-11_().txt_embedded_3.jpg</p> <p>MD5 7b6a92cc5f766b9f bc6d17a3f1de22f0</p> <p>Source File DJIFlightRecord_2020-12-11_().txt: 0x81BEE</p> <p>Pixel 1280x720</p> <p>Resolution</p> <p>Orientation Horizontal (normal)</p>

#	Origin	Timestamp	End time	Position
1	Device	19/Apr/20 12:10:15		(53.851894, -1.523449, 53.690802)
2	Device	19/Apr/20 12:10:30	Latitude	(53.851894, -1.523449, 53.512438)
3	Device	19/Apr/20 12:10:46	Altitude	(53.851894, -1.523449, 53.202703)
4	Device	19/Apr/20 12:11:02	Longitude	(53.851894, -1.523449, 53.190618)
5	Device	19/Apr/20 12:11:17		(53.851894, -1.523449, 53.400915)
6	Device	19/Apr/20 12:11:33		(53.851894, -1.523449, 53.312231)
7	Device	19/Apr/20 12:11:49		(53.851894, -1.523449, 53.847924)
8	Device	19/Apr/20 12:12:04		(53.851894, -1.523449, 53.922375)
9	Device	19/Apr/20 12:12:20		(53.851894, -1.523449, 53.918481)
10	Device	19/Apr/20 12:12:36		(53.851894, -1.523449, 53.912939)

Fig. 12. Location recordings found in "FLY049.DAT".

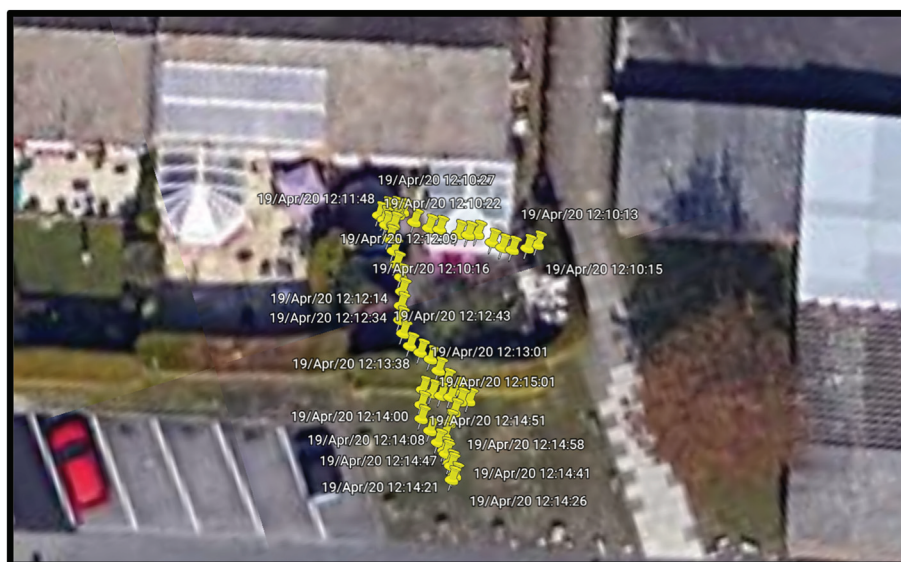


Fig. 13. Google earth visualisation of FLY049.DAT.

the drone itself. Advanced methods could have been attempted; however, they were not performed due to the likeliness of damaging the drone. An extraction was successfully performed on the MicroSD card which was inserted in the drone using FTK Imager.

Images, videos and documents were successfully extracted from the memory card; however, no log files were present. The documents recovered all appear to be quick start guides for the Mantis Q. Images recovered from the memory card were in.JPG format with the file name "YUNXXXXX.JPG" (XXXXXX being an incrementing number e.g., YUN00002.JPG). These files were found in the "NO NAME/DCIM/100MEDIA/" file path, and contained metadata relating to the drone camera make and model. A duplicate for each JPG image was found in.THM format, which appear to be used as thumbnails on camera memory cards (File Recovery Central). The THM files appear visually similar but are significantly smaller, lower quality and contain less metadata. Table 9 and Table 10 show a comparison of JPG and THM images.

Video files were found in MOV format in the "NO NAME/DCIM/100MEDIA/" directory, with an additional smaller video file created for every MOV file, which is in .2nd format. This file appears to be a thumbnail file of the original video, as it is visually identical, but is a significantly smaller file size and lower quality, but contains the same metadata, as shown in Table 11 and Table 12.

No NIST extraction was available at the time of analysis for this model of drone. As a result, a comparison of extracted data could not be performed for this device.

3.8. PBZ/6 – Samsung Galaxy S10 lite

PBZ/6 is a Samsung Galaxy S10 Lite smartphone which was used to operate PBZ/5 and the operating system for this device was Android 10. The Yuneec Pilot app was installed on the device to operate the drone. As only the memory card was extracted from PBZ/5, it would be ideal to recover log files from the flight of PBZ/5 and be able to link them to the drone, in addition to identifying data

Table 5
Original image found on PBZ/1 memory card.


Original (PBZ/1 Memory Card)		
	Name	DJI_0011.JPG
	Size (Bytes)	6222680
	File Path	NO NAME/DCIM/100MEDIA/DJI_0011.JPG
	Created Date	11/12/2020 13:22:54
	Accessed Date	11/12/2020 00:00:00
	Modified Date	11/12/2020 13:22:54
	MD5	daef5482c0a028d44db 6cb5b8a6436f5
	Camera Make	DJI
	Camera Model	FC220
	Capture Time	11/Dec/20 13:22:54
	Pixel Resolution	4000x3000
	Lat/Lon	0.000000/0.000000

Table 6
Screen nail image recovered from PBZ/2.



Screen Nail Image (PBZ/2)		
	Name	BBC339FFBD06B6270 0AFE4DE111D8AC7
	Type	Image
	Size (Bytes)	128019
	File Path	iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/.mediaLibrary.Cache/Screen nail/BBC339FFBD06B6 2700AFE4DE111D8AC7
	Created Date	11/12/2020 13:23:07(UTC+0)
	Modified Date	11/12/2020 13:23:07(UTC+0)
	MD5	e32b58be935dbedb6 6c4de0a47bb59ba
	Pixel Resolution	960x720

Table 7
Thumbnail image recovered from PBZ/2.

Thumbnail Image (PBZ/2)		
	Name	BBC339FFBD06B62700 AFE4DE111D8AC7
	Type	Image
	Size (Bytes)	34540
	File Path	iPhone/mobile/Containers/Data/Application/com.dji.go/Documents/.mediaLibrary.Cache/Thumbnail/BBC339FFBD06B62700A FE4DE111D8AC7
	Created Date	11/12/2020 13:23:06(UTC+0)
	Modified Date	11/12/2020 13:23:06(UTC+0)
	MD5	3c7bb640970b861a8badd3 1e752bd152

relating to the multimedia captured during the flight of PBZ/5. Table 13 shows metadata recovered relating to PBZ/6.

No images or videos were found on the handset which were related to the operation of PBZ/5. The text file "configs.xml" was found in the "/data/data/com.yuneec.android.z/shared_prefs/

configs.xml" directory, which contains the username, nickname, app version and drone version, as shown in Fig. 17. This data can be attributed to a suspect as the nick name user name and password will be unique to the user and will be used to log into the Yuneec Pilot app. The drone version shows that a drone has been connected

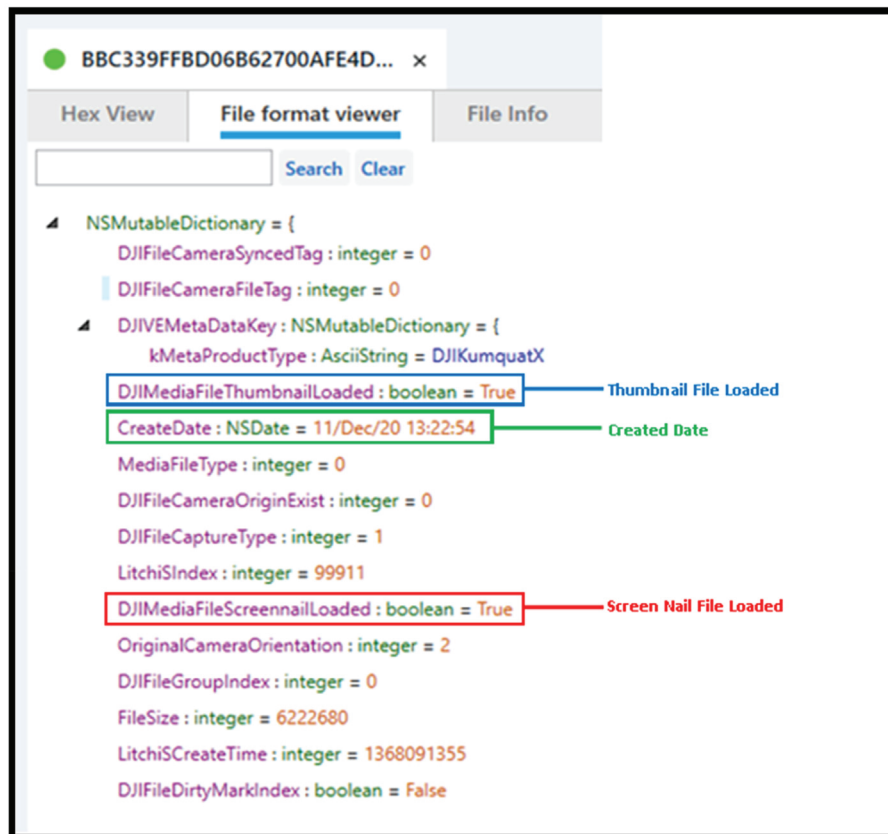


Fig. 14. File view of the config file "BBC339FFBD06B62700AFE4DE111D8AC".

to the handset, and the specific version of the drone is displayed. Although this is not unique, it will show that a drone with the matching make and model has been operated using the handset.

Databases were recovered, which appear to contain logs of events captured during the operation of PBZ/5, however a link could not be made to PBZ/5 based on data found in the logs. The database "Yuneec.db" found in the "/data/com.yuneec.android.z/databases/yuneec.db" directory, contained the table "running_log" which contains logs which were created during the operation of a drone. A sample of data found in the "running_log" table is shown below in Fig. 18. The database "Yuneec_flight_log.db" contained the last user email address that was used to operate the Yuneec Pilot application.

A review of data found that evidence of a drone being used during the timeframe was found, but a direct link to PBZ/5 could not be established. It was clearly identified that a Yuneec drone was used during the timeframe, but no model numbers or unique identifiers were recovered which would link the GCS to PBZ/5 uniquely.

Table 14 shows a summary of data extracted from the devices used during the experiment.

The experiment suggests it is difficult to establish a strong link between the GCS and the drone in most cases, as a drone device does not appear to contain metadata relating to the controller used during operation. This would pose a great difficulty for investigators if the GCS were not recovered from a crime scene, as attribution to a suspect may not be possible using the data available for extraction from a drone unaccompanied with a GCS. However, if the GCS is recovered, evidence such as log files, multimedia, location data and configuration files are an excellent source to find data which is very similar to data found on the drone and have a much

greater likelihood of attributing the usage of the devices to a suspect. There is a lack of support for smaller or newer drone devices in the forensic tools used, showing that alternative techniques may need to be researched and used as an alternative if support is not available. Although two drone devices could not be extracted, it was identified that advanced methods such as chip removal could have enabled data extractions of the devices, but this would likely destroy the device. As this was not included in the scope of the experiment, advanced methods were not utilised, however they were identified as a possibility.

4. Proposed digital forensics investigation framework

Based on the experiments presented in the previous section, a framework has been created which has identified the key processes of UAS forensics and proposed a workflow for processes that will be performed during the investigation. The aim of the framework is to cover all aspects of data capture and analysis from small to medium sized commercial drones, while also maintaining the integrity of any data captured and preserving the original condition of the device when seized. The framework consists of five generic stages, which aim to break the investigation down into clear and distinct stages, each with their own objectives and guidelines. Multiple devices are combined to make a UAS such as an UAV and GCS, which means that different processes are required to examine all the different devices. Using a top-level approach enables all devices to be examined during the same investigation, whereas a low-level framework would require the investigation to be split into several sub-investigations. Fig. 19 shows the framework proposed for UAS forensic investigations.

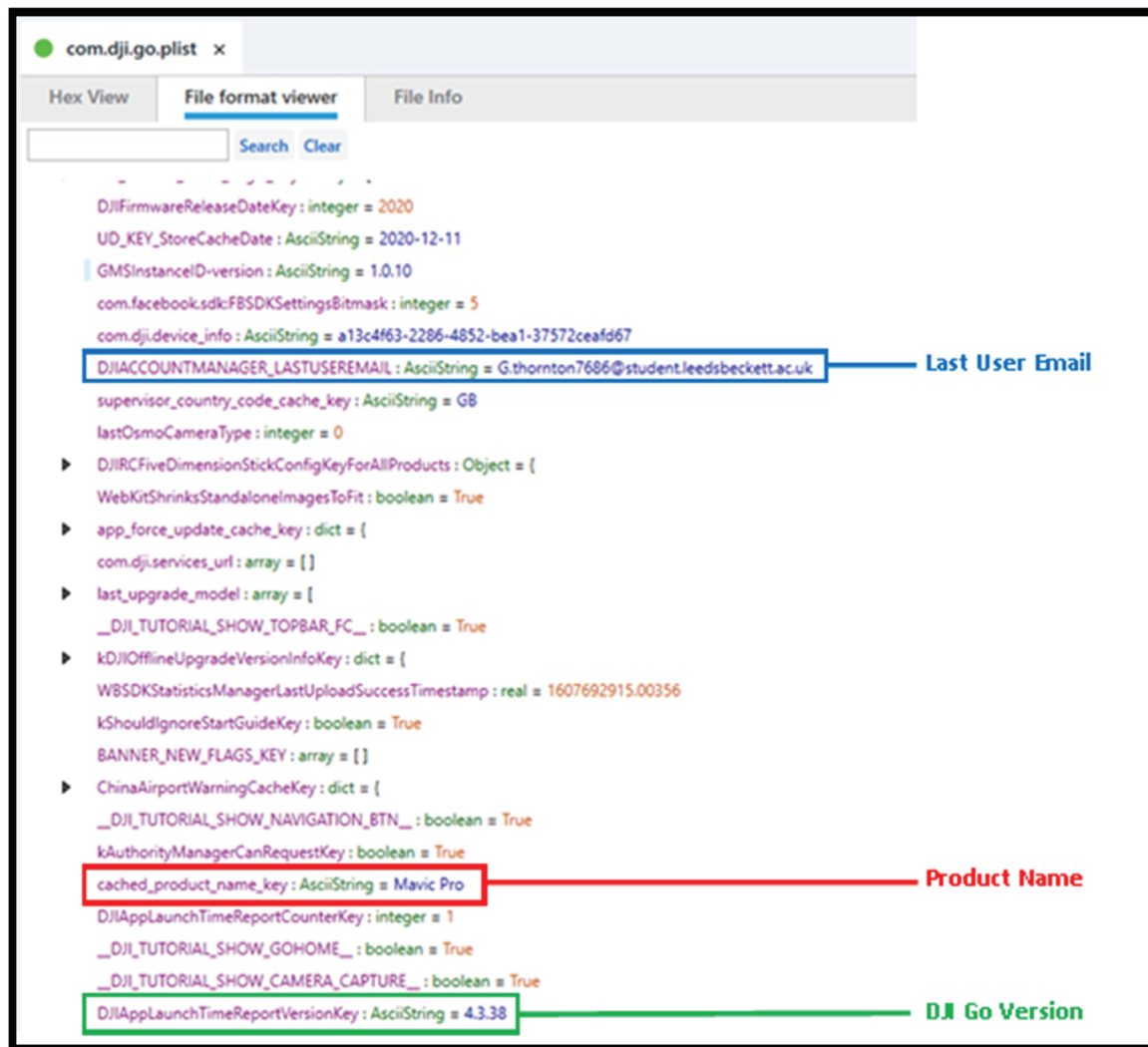


Fig. 15. Sample data from "com.dji.go.plist" file recovered from PBZ/2.

4.1. Seizure

The seizure stage relates to how the device is secured from a crime scene or from a suspect. The primary objectives should be to successfully obtain the drone in the same condition that it was found in and prevent any further damage or modifications. If a drone is found in a powered-on state, it should be powered off and isolated from any networks or wireless connections by disabling Wi-Fi, Bluetooth, and mobile data settings, if possible, then enabling flight mode or airplane mode if available. In the event the GCS (Ground Control Station) e.g., smartphone or tablet is recovered, this should also be powered off and isolated from any networks and wireless connections. To prevent the drone from being operated, it can be turned upside down to prevent it from starting another flight. GCS devices may be required to remain powered on if they are PIN locked or encrypted but should be isolated from any networks as soon as possible. If possible, the devices should be handled using gloves to preserve any fingerprints or DNA evidence that may reside on the drone as this could provide a link to the suspect(s). A chain of custody should be established to track where the devices are physically stored and who is in possession of the devices at any given time.

Seizure Stage Objectives:

1. Seize the drone and any other related devices from the crime scene.
2. Isolate the device(s) from the environment using exhibit bags and preserve the device(s) for fingerprints/DNA examinations.
3. Isolate the device(s) from any network connections by enabling Flight mode and disabling any wireless connections such as Wi-Fi or Bluetooth.

4.2. Physical examination & planning


The physical examination and planning stage consists of a thorough examination of the devices seized and to identify a suitable plan for extraction and analysis. A physical examination should be performed on all devices while situated in a forensically sound environment such as a laboratory to assess the current condition of the devices, such as any damage, distinctive markings, modifications, or other notable features. Attention should be paid to the condition to the data port(s) on the devices to determine whether a standard extraction can be performed. If the data ports are damaged, options for advanced procedures should be considered and weighed against the monetary cost and the likeliness of damage to the device with what data may be recovered from the



Fig. 16. Last known aircraft location from "com.dji.go.plist".

Table 8

Image metadata relating to flight image found on PBZ/4.

go_photo_1607693612528.jpg		
	File Name	go_photo_1607693612528.jpg
	File Type	Image
	Size (Bytes)	471807
	Path	data/Root/media/0/DJI/dji.go.v5/DJI FLY/Photo/go_photo_1607693612528.jpg
	Created Date	11/12/2020 13:33:32(UTC+0)
	Accessed Date	11/12/2020 13:33:32(UTC+0)
	Modified Date	11/12/2020 13:33:32(UTC+0)
	MD5	47085f650225fd95566d1dba160409de

device and how vital this is to the case. Any removable media such as memory cards or SIM cards should be identified and removed from the devices to prevent further alterations such as overwriting data if the device were to be powered on. Background research

should be performed to identify what data would typically be recovered from the device and what extraction and analysis tools are available. For example, if a DJI Phantom 4 is seized, the manufacturers website will list the capabilities of the drone and datasets

Table 9

JPG image recovered from PBZ/5.


YUN00002.JPG	
	<p>Name YUN00002.JPG Size (Bytes) 7610894 File Path NO NAME/DCIM/100MEDIA/YUN00002.JPG Created Date 11/12/2020 13:16:26 Accessed Date 11/12/2020 00:00:00 Modified Date 11/12/2020 13:16:26 MD5 8305eceb76fb21d b1b5d1f0446aecb9 Camera Make Yuneec Camera Model Mantis Q Capture Time 11/Dec/20 13:16:26 Pixel Resolution 4160x3120 Lat/Lon 0.000000/0.000000</p>

Table 10

THM image recovered from PBZ/5.



YUN00002.thm	
	<p>Name YUN00002.thm Size (Bytes) 11648 File Path NO NAME/DCIM/100MEDIA/YUN00002.thm Created Date 11/12/2020 13:16:26 Accessed Date 11/12/2020 00:00:00 Modified Date 11/12/2020 13:16:26 MD5 f428e575e8cae0026109e6666c2663b1</p>

Table 11

Metadata recovered relating to YUN00001.MOV.

YUN00001.MOV	
	<p>Name YUN00001.MOV Size (Bytes) 158423117 File Path NO NAME/DCIM/100MEDIA/YUN00001.MOV Created Date 11/12/2020 13:15:20 Accessed Date 11/12/2020 00:00:00 Modified Date 11/12/2020 13:16:22 MD5 4ccc5f039c4f27d992613363938420b7 @too {Mantis_0.0.10_E} AE:1,EV:-1.5,FLICK:1,WB:1,IQ:1,VOL:30</p>

from NIST can be used to show examples of what data is recoverable and the file paths of these artefacts. The specifications of controllers should be researched, as some non-smartphones may contain an internal storage capacity which can be extracted using standard tools or may require more advanced methods of extraction.

Physical Examination & Planning Stage Objectives:

1. Conduct a physical examination of device(s) to identify unique identifiers, damage or notable features.

2. Research the model of device(s) and identify storage capabilities of the device(s).
3. Identify extraction options for the device(s).

4.3. Extraction

The extraction stage will be used to prepare and extract data from the device(s). Traditional forensic standards such as ACPO guidelines should be adhered to whenever possible as they provide solid

Table 12
Metadata recovered relating to YUN00001.2nd.


YUN00001.2nd	
	<p>Name YUN00001.2nd Size (Bytes) 16019337 File Path NO NAME/DCIM/100MEDIA/YUN00001.2nd Created Date 11/12/2020 13:15:20 Accessed Date 11/12/2020 00:00:00 Modified Date 11/12/2020 13:16:22 MD5 76cc01be6e8c67ed3a1027dd25549fc2 ©too {Mantis_0.0.10_E} AE:1,EV:-1.5,FLICK:1,WB:1,IQ:1,VOL:30</p>

Table 13
Device information recovered from PBZ/6.

Device Information	Value
Advertising ID	4ca11bb2-8dc0-44c5-8c74-903d0ebd165f
Android ID	666355bbcea9314e
Android ID	8bfd112a87c2c72
Detected model	SM-G770F
Phone date/time	14/Dec/20 15:32:39
Phone revision	Phone revision
Bluetooth MAC Address	70:CE:8C:B4:2C:1C
Bluetooth device name	Galaxy S10 Lite
Factory (Serial) number	RF8N20AETVM
Mac Address	70:ce:8c:b4:2c:1d

principles for the investigation making handling devices and extracting from them as forensically sound as possible and using standardised practices to make results more reliable and repeatable. It is common for drones to contain both internal and external storage with memory card slots, as well as GCS devices containing internal storage, external storage and SIM cards. It is important that any removable media such as SIM cards or memory cards are removed from the device and extracted individually, as this will reduce the risk of the media being written to or gaining a wireless connection and therefore will be more forensically sound. Removable media can be connected to a forensic workstation using write-blockers which will prevent the data on the media from being altered. If non-smartphone

controllers are identified to contain an internal storage capacity, then extractions should also be attempted on the controller.

If a smartphone GCS is found rooted or jailbroken, then this can provide further extractions for the handset, such as a rooted physical extraction for Android devices, or “checkra1n” extractions for iOS. This could result in a higher yield of data extracted from the GCS. Typical extractions for iOS and Android may load a small client application onto the handset to perform the extractions or may boot the device into another mode, such as a “checkm8” extraction, which would be uninstalled after completion.

After extractions of the GCS have been performed a manual review of data on the GCS should be performed, while taking screenshots of the data present on the handset. The data extracted from the GCS should be compared with the data visible on the handset to confirm that the data has extracted correctly and represents the data as it is found on the handset.

If possible, this data should be compared with a NIST extraction performed on the same drone model if available to determine whether all available data sources have been successfully extracted. However, app versions and operating systems may differ, so may be possible to find different data. If required data is identified, but is not in the extracted data, further extractions are required, and the extraction stage should be returned to. Once it has been confirmed that data has been successfully extracted from the GCS, this should then be powered off and reassembled, but external storage or SIM card should not be reinserted in the device.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="select_product_result" value="1" />
  <string name="nick name">PilotF3Lv6pf7</string>
  <string name="user name">g.thornton7686@student.leedsbeckett.ac.uk</string>
  <string name="version_name">2.0.7</string>
  <boolean name="is login" value="true" />
  <string name="DRONE-VERSION">1.0.02_E_1097</string>
  <string name="user pwd">Pa55word</string>
  <string name="token">AD70AA2EE9B26030DB5AB06929717FAF</string>
</map>
```

Fig. 17. Contents of “configs.xml”.

id	Running_log_time	Running_log_date	Running_log_type	Running_log_text
25	1607692524367	2020-12-11 13:15:24	6	(3,11)TAKEOFF MODE
26	1607692524401	2020-12-11 13:15:24	6	Takeoff detected.
27	1607692527385	2020-12-11 13:15:27	6	(3,26)ANGLE MODE
28	1607692656799	2020-12-11 13:17:36	2	vehicle command 176 (1 4 6 0)
29	1607692656802	2020-12-11 13:17:36	6	(3,41)BEGIN TO AUTOLAND
30	1607692661981	2020-12-11 13:17:41	2	Failsafe enabled: no local position
31	1607692661986	2020-12-11 13:17:41	6	Failsafe mode on.
32	1607692661999	2020-12-11 13:17:41	6	Landing detected.
33	1607692662029	2020-12-11 13:17:42	6	(3,27)FUSE OPTICAL FLOW
34	1607692662033	2020-12-11 13:17:42	6	Failsafe mode off.
35	1607692662129	2020-12-11 13:17:42	6	Disarmed by auto disarm on land.
36	1607692662136	2020-12-11 13:17:42	6	Automated flight complete.
37	1607692662138	2020-12-11 13:17:42	6	(3,26)ANGLE MODE
38	1607692666796	2020-12-11 13:17:46	6	(3,25)SPORT MODE

Fig. 18. Sample of data found in the “running_log” table.

Table 14
Extracted data from drone and GCS devices.

	GT/1	GT/2	PBZ/1	PBZ/2	PBZ/3	PBZ/4	PBZ/5	PBZ/6
Log Files	✓		✓					✓
Images	✓	✓	✓	✓		✓	✓	✓
Videos	✓	✓	✓	✓		✓	✓	✓
Configuration Files	✓	✓	✓	✓		✓		✓
Location Data	✓	✓		✓		✓		✓
Device Serial Number	✓	✓		✓		✓		✓
Battery Serial Number	✓	✓						
NIST Extraction Available	✓	–	✓	–		–		–
Link established with Paired Device		✓		✓				
Application Databases	–	✓	–	✓	–	✓	–	✓

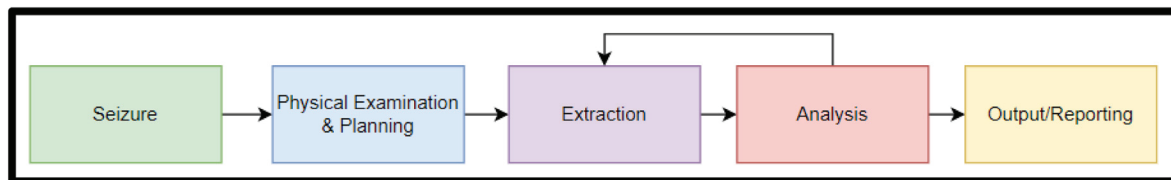


Fig. 19. Proposed framework for UAS investigations.

Extraction Phase Objectives.

1. Gain the best level of extraction possible for the device(s).
2. Maintain the integrity of the device(s) by altering the device(s) data as little as possible.
3. Verify data extracted by performing a manual review or comparing with a reliable data source such as NIST datasets and/or perform a manual review of data available on the device(s).

4.4. Analysis

During the analysis stage, the data extracted from all UAS devices will be reviewed to establish links between the devices and attribution towards the user and/or owner of the devices. Printed and electronic unique identifiers, user account information and software versions should be identified to distinguish the seized drone from other drone devices. Location data should be reviewed to prove that the drone and/or controller were used around the area of a crime scene or in a prohibited area. The GPS coordinates of the drone are recorded at regular intervals on the drone’s internal

memory and on the GCS in some cases, meaning a visualisation of a drone’s flight path can be re-created using appropriate software tools. Multimedia data should also be reviewed to attempt to identify any photos, videos or audio files that have been created during operation of the drone. It is likely that the video and image files captured using the drone will be duplicated on the GCS, meaning a link can be established between the GCS and the drone, although some of these files may only be visually identical. Timestamps for these files should match between the GCS and the drone, but may differ slightly due to transmission times, which may be dependent on the quality of connection between the drone and the GCS at the time of capture. EXIF data from any images and videos taken by the drone camera could show the location of the drone when it was taken, as well as timestamps to corroborate the location of the drone at a given time. Timestamps for multimedia on the drone’s external memory and on the GCS should have timestamps that are the same or within seconds, dependent on the transmission time between the drone and the GCS.

Log files stored on the drone’s internal storage can show location data, dates and times that the drone was in use, while also not being editable by the end user in most cases, meaning it can be a

reliable source of information. Any application data relating to applications which are used to operate the drone should be reviewed to identify if any user data can be identified within the application data, such as usernames, email addresses, or flight logs. Visually confirming that data is available on the GCS provides further evidence that the GCS was used with the drone and provides a further link between the GCS and the drone, and that this data was available to the user of the GCS. Device information such as serial numbers may be used to uniquely identify the devices and may be used to establish ownership or use of the devices. Manufacturer specifications for the devices may also give insight into the device capabilities such as the weight of a payload that can be transported using a drone.

Analysis Phase Objectives.

1. Establish links between the components of the UAS.
2. Attribute ownership and/or usage of the devices to a suspect.
3. Identify evidence which can prove that the device(s) were used to commit a crime.

4.5. Output & reporting

Finally, the results of the investigation will be output in a human readable, condensed format which will outline the key findings of the investigation. Results of analysis should be summarised to contain only data relevant to the investigation and should give a clear understanding of key findings. The main aim will be to determine whether a link can be established between the drone, the GCS and any suspects who may have used or handled any of the devices.

Output & Reporting Phase Objectives.

1. Summarise what the purpose of the investigation was and how it was carried out.
2. Summarise findings of the investigation and provide evidence that either proves or refutes the use of the device(s) to commit a crime.
3. Output results into a clear human readable format.

The main advantage of this framework is the adaptability and usability for multiple devices in one investigation package. As UAS are formed from several different devices, different processes may be needed for each device, such as a drone or a smartphone. The customisability and variability in drone device hardware and software means that an adaptable framework is required to analyse these devices in one investigation. A low-level process is not outlined as it may become obsolete as drone technology develops. Another advantage of the framework is its similarity to existing practices in digital forensics, making it somewhat familiar to digital forensics practitioners and is akin to practices which are tested and approved by digital forensic providers. However, using a high-level approach means that a specific and highly detailed process is not outlined. This may result with some variances in tools and techniques used in investigations, but this may occur regardless due to the different tools available to practitioners at the time. Although examples of data sources are outlined, it is possible that more bespoke devices will store different data in different locations, meaning that it may be difficult to identify and interpret data related to drone usage. It is likely that the framework would require modifications on a frequent basis to maintain its usefulness as technology and the tools used in digital forensics develop.

5. Discussion

A review of current literature showed a consensus that standardisation of process used in digital forensics is beneficial to the industry as it creates a standard and basis for all digital forensics investigations to follow. Officially recognised standards are implemented by the industry to allow digital forensics entities to work to a high, agreed standard resulting in accurate, repeatable, and trustworthy results from extraction and analysis procedures. Working practices such as ACPO guidelines are universally agreed as a good basis for digital forensics investigations and should be followed whenever possible ([An Explanation of Gu](#)). Industry standards such as ISO 17025 have been implemented into digital forensics to provide an officially recognised standard to follow during investigations. This means that individual forensic laboratories are outputting work to the same standard making it accurate, reliable and repeatable, hence analysis from other laboratories can be trusted to be to a high standard.

5.1. High-level vs low-level framework

A key issue with the development of a framework for UAS forensics is whether to implement a high-level or low-level methodology. Using a high-level methodology will typically involve generic processes but will have a large scope of devices that can be analysed using the framework. Alternatively, a low-level framework may be used which details specific processes for analysing a drone, but this may make the framework unsuitable for some devices and may become obsolete over time as processes and available tools develop or improve ([Du et al., 2017](#)).

The purpose of the framework created is to provide a higher-level framework which allows for more flexibility when performing investigations and to future-proof the framework, accommodating changes in technology and the tools used during investigations. This is a key feature that is not found with other forensic frameworks relating to drones, which have a large focus on specific data sources which may alter as drone technology develops. The framework accounts for all components of a GCS and the related artefacts that can be recovered from the various devices. This allows all devices to be analysed using the same processes which will improve the consistency of the investigation and allow experiments to be more repeatable and reliable. Best practices and a list of objectives for each stage are provided, which give investigators a list of best practices and expected outcomes for each stage, meaning investigators will know what to expect from each stage of the investigation. Unlike other identified frameworks, this framework suggests that once data has been extracted from the devices, a manual review of data should be performed on a GCS, or comparison with a known dataset such as NIST. The purpose of this is to validate the data from the devices and prove that the data extracted from the devices is an accurate representation of what data is available or visible on the device.

In comparison with the framework suggested by [Jain et al. \(2017\)](#), a higher-level framework has been proposed in this research work, which merges some stages such as identification/collection, identify class/category, measure weight, check for customisation and compare specification with original have been grouped into the physical examination and planning stage of the proposed framework. Although these processes outlined by [Jain et al. \(2017\)](#) are necessary, they can be merged into one process in which they can be carried out in an order found more convenient. For example, it may be necessary to check for fingerprints

and DNA first then assess the hardware to better preserve this “wet” evidence. Using the created methodology would give practitioners more flexibility in their investigations, while maintaining the low-level processes that are required. Similarly, the created model also includes low-level processes such as establishing a chain of custody, photographing devices and identifying capabilities into one combined stage. As these processes are low-level and could be completed in a different order. The proposed framework allows the investigator to complete these practices in a different order if necessary.

The proposed framework also provides more practical tasks for how to handle and analyse devices than the framework suggested by Renduchintala et al. (2019), as detailed suggestions are provided for the best practices while handling devices, what data is likely to be recoverable and how this data can be used in an investigation. The suggested framework also provides guidance on how to perform a forensic analysis of the controller used to operate the drone, which was not included in the framework created by Renduchintala et al. (2019). A similarly high-level framework is suggested for the analysis of micro-drones by Yousef and Iqbal (2019) which provides greater detail regarding tools which are good alternatives to commercial forensic tools, such as using Linux to disable a drone mid-flight and extract the data using Linux. This was not investigated during the experiment but should be considered for further development of the framework. A larger emphasis is placed on the handling of devices in a forensically sound manner in the framework created, whereas the framework created by Iqbal provides more in-depth analysis techniques of the drone devices. It appears that using a high-level framework means that it can be used on a wider array of devices but does mean some detail regarding alternative or advanced techniques is lost. However, with further research and documentation a knowledgebase of drone forensics can be created, outlining failures and successes of drone analysis and extraction techniques.

5.2. Identification and analysis of forensic artefacts

Log files created during operation of the drone were identified as a primary source of data important to drone forensics investigations. Analysis of DJI drones found that log files were stored in DAT and TXT format. It was found that the DAT files were encrypted, but the TXT files were readable. These files could be then converted into visualisations using software such as Google Earth to show the flight routes taken by the drone (Yousef and Iqbal, 2019; Hamdi et al., 2019). This was also identified during the investigation as logs were successfully extracted from GT/1 and PBZ/1, and the flight logs could be decoded and visualised by Cellebrite Physical Analyser. Applications found on the handset by Barton and Azhar (Barton and Hannan Bin Azhar, 2017) showed that user data such as the username and email addressed used in the application could be recovered to prove attribution towards the user, which was also identified during analysis of GCS devices used during the experiment.

Similar to Kao et al. (2019), it was found that the controller was required in addition to the drone to establish a link between the devices and attribute this link to the user of the drone. It was also found that multimedia was stored on the external memory card, but not the internal memory card, which was displayed by all drone devices that were extracted as part of the experiment. GCS devices were analysed by Yousef and Iqbal (2019) using iTunes backups of the GCS and showed that plist files were available on iOS devices in addition to multimedia. This was replicated during the experiment using forensic extraction tools such as Cellebrite Physical Analyser and Cellebrite UFED. Plist files containing data relating to the user account for the DJI GO application was recovered in both

investigations, however this data was also found visible on the GCS during a physical examination conducted during the experiment.

Although data was extracted from all devices, it was found that there was some interference with the recording of location data among all devices, as little location data related to the flight of the drones was recovered. However, this was potentially caused by interference from the sports hall roof. Data from previous flights found on the drones was used as an additional source for comparison. The forensic tools used during the experiment provided a full extraction of devices when supported, as shown by the comparison of available NIST extraction. However, it was also found that there is a lack of support for smaller drones, or newer drones in the forensic tools used. As a result, more alternative methods could have been used to extract data from the devices but could not be attempted due to time constraints.

As drones from only two manufacturers were used, the framework has been tested on only a small portion of the drones available to consumers. The inclusion of additional drones from different manufactures such as Parrot or UVify could have improved the testing of the framework and identification of data sources as well as identifying extraction or analysis issues and solutions. Additional research should have been performed on PBZ/5 as Yuneec drones were not supported by the forensics software used, so an alternative method should have been identified before the experiment and the framework were completed. Although more variety of drones would have improved the investigation, the purpose of the investigation was to identify the key components of a UAS investigation and provide a high-level framework which will encompass all small to medium sized commercial drones using best practices currently used by digital forensics identities, allowing investigators to consistently apply the same framework for all investigations.

Advanced extraction procedures such as chip removal were identified as a possible option for the extraction of devices not supported by commercial tools. As advanced procedures were not included in the scope of the project they were not attempted, but insight into the internal hardware and storage capabilities of drone devices and their controllers may give a greater understanding of the hardware components of drone devices.

Although some minor attempts were made to hide PII, a more in-depth review of anti-forensics methods using drone devices could provide greater insight into how a user may hide their identity or prevent data capture using drone devices. For example, it was identified that interference with the drone's GPS data recording may have been caused by the metal sports hall roof, but this may be caused by other factors which were not identified. Although the drone's internal storage is not accessible to the user in most cases, it was not identified whether data is overwritten when the internal storage capacity is full, or whether the drone will not operate.

6. Conclusion

A framework for forensic analysis of unmanned aerial systems was developed in this research work. Four drones and four GCS were examined using the proposed framework, which resulted in successful extraction and analysis of most devices. For devices which encountered errors, further techniques to attempt were identified, but could not be attempted due to cost and time constraints. The framework was based on a combination of existing literature and observations of existing frameworks used in digital forensics. A high-level framework has been created which aims to incorporate many devices, giving suggestions for what may be encountered and what to attempt to identify.

It was identified that it is often not possible to find data to link the drone to a GCS and a suspect based on data only extracted from

the drone. Although log files with location data, multimedia and configuration files can be found on the drone, there is little to no data which creates a direct link between the drone and a specific GCS or a specific individual. However, when the GCS is also analysed a link is much more likely to be identified between the drone and the GCS, which can then be attributed to a user of the devices. To aid law enforcement and to improve the security of drone devices, drone manufacturers could implement logging the user's details and the GCS metadata within the log files of the drone, which may act as a deterrent to criminals as data captured from the drone only could be used to identify both the GCS and the owner or user of the devices. Logging capabilities or configuration files appear to be stored on the internal memory of most drones and is not editable by the user in most cases, meaning it could prove to be a vital source of data for both law enforcement and the drone manufacturers to prevent crime using drone technology.

References

- Al Mutawa, N., Baggili, I., Marrington, A., 2012. Forensic analysis of social networking applications on mobile devices. *Digit. Invest.* 9, S24–S33. <https://doi.org/10.1016/j.diin.2012.05.007>.
- Ahmed M. Al-Samman, Tawfik Al-Hadhrani, Ahmad Al Shami and Fuad Alnajjar, 2021, Research Challenges and Opportunities in Drone Forensics Models, *Electronics*, 10(13), 1519. <https://doi.org/10.3390/electronics10131519>.
- An explanation of ACPO guidelines for digital based evidence, n.d. Athena forensics. URL <https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics>.
- Attoe, R., et al., 2018. The emerging world of drone forensics: extracting data from an [WWW Document]. AccessData. URL, 8.4.20. <https://accessdata.com/blog/the-emerging-world-of-drone-forensics-extracting-data-from-an-unmanned-aeri>.
- Azhar, D.H., 2019. Challenges and techniques in drone forensics. URL https://www.iaria.org/conferences2019/files/CYBER19/HannanAzhar_Tutorial_ChallengesAndTechniques.pdf.
- Badiye, A., Kapoor, N., Menezes, R.G., 2020. Chain of custody (chain of Evidence). Treasure Island (FL. In: StatPearls. StatPearls Publishing. URL <http://www.ncbi.nlm.nih.gov/books/NBK551677>.
- Barton, T.E.A., Hannan Bin Azhar, M.A., 2017. Forensic analysis of popular UAV systems. In: 2017 Seventh International Conference on Emerging Security Technologies (EST). Presented at the 2017 Seventh International Conference on Emerging Security Technologies (EST), IEEE, Canterbury, pp. 91–96. <https://doi.org/10.1109/EST.2017.8090405>.
- Bouafif, H., Kamoun, F., Iqbal, F., Marrington, A., 2018. Drone forensics: challenges and new insights. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). Presented at the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, Paris, pp. 1–6. <https://doi.org/10.1109/NTMS.2018.8328747>.
- n.d Civil Aviation Authority. An introduction to unmanned aircraft systems | UK Civil Aviation Authority [WWW Document]. An introduction to unmanned aircraft systems. URL, 12.26.20. <https://www.caa.co.uk/Consumers/Unmanned-aircraft/Our-role/An-introduction-to-unmanned-aircraft-systems>.
- Clark, D.R., Meffert, C., Baggili, I., Breitinger, F., 2017. DROP (DRone Open source Parser) your drone: forensic analysis of the DJI Phantom III. *Digit. Invest.* 22, S3–S14. <https://doi.org/10.1016/j.diin.2017.06.013>.
- Du, X., Le-Khac, N.-A., Scanlon, M., 2017. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service arXiv:1708.01730 [cs]. URL <http://arxiv.org/abs/1708.01730>.
- File Recovery Central, n.d. THM file - what is the purpose of a .thm file on a memory card and can I delete it? Plus, why can't I find my videos on my Canon camera? [WWW Document]. What is the purpose of a .THM file and can I delete it? URL, 1.2.21. <http://www.filerecoverycentral.com/thm-file-canon-what-is-it.html>.
- FutureLearn, n.d. Who is analysing what? Chain of custody [WWW Document]. FutureLearn. URL, 9.29.20. <https://www.futurelearn.com/courses/science-behind-forensic-science/0/steps/56559>.
- ACPO Good Practice Guide for Digital Evidence (No. 5.0), 2012. Association of Chief Police Officers of England, Wales & Northern Ireland. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
- Gulatas, I., 2018. UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION (Dissertation). Bahcesehir University, Istanbul, Turkey. URL <http://acikerisim.bahcesehir.edu.tr:8080/xmlui/bitstream/handle/123456789/1254/Unmanned%20aerial%20vehicle%20digital%20forensic%20investigation.pdf?sequence=1>.
- Gulatas, I., 2018. UNMANNED AERIAL VEHICLE DIGITAL FORENSIC INVESTIGATION (Dissertation). Bahcesehir University, Istanbul, Turkey. URL <http://acikerisim.bahcesehir.edu.tr:8080/xmlui/bitstream/handle/123456789/1254/Unmanned%20aerial%20vehicle%20digital%20forensic%20investigation.pdf?sequence=1>.
- Hamdi, D.A., Iqbal, F., Alam, S., Kazim, A., MacDermott, A., 2019. Drone forensics: a case study on DJI Phantom 4, 2019. In: IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). Presented at the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1–6. <https://doi.org/10.1109/AICCSA47632.2019.9035302>. IEEE, Abu Dhabi, United Arab Emirates.
- n.d Hoffman, C., How to use your bash history in the Linux or macOS, Terminal [WWW Document]. How-To Geek. URL, 8.27.20. <https://www.howtogeek.com/howto/44997/how-to-use-bash-history-to-improve-your-command-line-productivity>.
- Horsman, G., 2016. Unmanned aerial vehicles: a preliminary analysis of forensic challenges. *Digit. Invest.* 16, 1–11. <https://doi.org/10.1016/j.diin.2015.11.002>.
- URL How Drone Technology Is Being Used to Target Homes by Burglars, 2015. Calder Security Wakefield, 12.26.20. <https://www.caldersecurity.co.uk/theft-by-drone>. <https://www.dji.com/thread-134162-1-1.html>.
- Interpol, 2019. FRAMEWORK for RESPONDING to A DRONE INCIDENT - for First Responders and Digital Forensics Practitioners. Interpol, INTERPOL Global Complex for Innovation, 18 Napier Road, p. 258510. Singapore. <https://informaticoadomicilio.com/wp-content/uploads/2020/03/respuesta-ante-incidentes-drones-interpol.pdf>.
- Iqbal, F., Yankson, B., AlYammahi, M.A., AlMansoori, N.S., Qayed, S.M., Shah, B., Baker, T., 2018. Drone forensics: examination and analysis. *Int. J. Electron. Secur. Digital Forensics* 11, 10. <https://doi.org/10.1504/IJESDF.2019.10020543>.
- Jain, U., 2017. A drone forensics investigation framework (M.S.). ProQuest dissertations and theses. Purdue university, United States – Indiana. URL <https://search.proquest.com/docview/1948771261/abstract/C19BAAB7651A43ADPQ/1>.
- Jain, U., Rogers, M., Matson, E.T., 2017. Drone forensic framework: sensor and data identification and verification, 2017. In: IEEE Sensors Applications Symposium (SAS). Presented at the 2017 IEEE Sensors Applications Symposium (SAS). IEEE, Glassboro, NJ, USA, pp. 1–6. <https://doi.org/10.1109/SAS.2017.7894059>.
- Kamoun, F., Bouafif, H., Iqbal, F., 2019. Towards a better understanding of drone forensics: a case study of Parrot AR drone 2.0. *Int. J. Digital Crime Forensics (IJDCF)* 12, 1–23. <https://doi.org/10.4018/IJDCF.2020010103>.
- Kao, D.-Y., Chen, M.-C., Wu, W.-Y., Lin, J.-S., Chen, C.-H., Tsai, F., 2019. Drone forensic investigation: DJI Spark drone as A case study. *Procedia Comput. Sci.* 159, 1890–1899. <https://doi.org/10.1016/j.procs.2019.09.361>.
- ElcomSoft blog Katalov, V., 2020. The Worst Mistakes in iOS Forensics, URL, 8.27.20. <https://blog.elcomsoft.com/2020/01/the-worst-mistakes-in-ios-forensics>.
- Kovar, D., Dominguez, G., Murphy, C., 2016. UAV (Aka Drone) Forensics. SANS DFIR Summit June 23–24, 2016 Austin, TX USA - PDF Free Download. URL <https://docplayer.net/51276876-Uav-aka-drone-forensics-sans-dfir-summit-june-23-24-2016-austin-tx-usa.html>.
- Leonard, M., 2018. NIST builds drone forensics dataset - [WWW Document]. GCN. URL, 8.4.20. <https://gcn.com/articles/2018/06/14/drone-forensics.aspx>.
- Livelsberger, B.R., Fed, n.d., Drone Forensics and other new additions to CFRDS. URL https://www.nist.gov/system/files/documents/2018/11/14/4_livelsberger.pdf.
- DJI Smart Controller - designed to maximize your outdoor flying experience - DJI [WWW Document], n.d. DJI Official. URL <https://www.dji.com/uk/smart-controller> (accessed 8.11.20).
- McFarland, R., 2017. Digital Forensics Methodology – a Brief Overview. The Cyber Security Place. URL, 9.27.20. <https://thecybersecurityplace.com/digital-forensics-methodology-brief-overview>.
- Miller, P.C., 2018. UAS Magazine – the Latest News on Unmanned Aerial Systems - Forensic Images Help Law Enforcement Catch Drone Criminals [WWW Document]. Forensic Images Help Law Enforcement Catch Drone Criminals. URL, 8.4.20. <http://www.uasmagazine.com/articles/1872/forensic-images-help-law-enforcement-catch-drone-criminals>.
- Mistry, Nilay R., Sanghvi, Hitesh P., 2021. Drone forensics: investigative guide for law enforcement agencies. *Int. J. Electron. Secur. Digital Forensics* 13 (3).
- n.d Obbayi, L., Chain of custody in computer forensics [WWW Document]. Infosec Resources. URL, 9.29.20. <https://resources.infosecinstitute.com/category/computer-forensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics>.
- Press, R., 2018. Drone Forensics Gets a Boost with New Data on NIST Website [WWW Document]. NIST. URL, 8.4.20. <https://www.nist.gov/news-events/news/2018/06/drone-forensics-gets-boost-new-data-nist-website>.
- Renduchintala, A.L.P.S., Albehadili, A., Javaid, A.Y., 2017. Drone forensics: digital flight log examination framework for micro drones, 2017. In: International Conference on Computational Science and Computational Intelligence (CSCI). Presented at the 2017 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, Las Vegas, NV, USA, pp. 91–96. <https://doi.org/10.1109/CSCI.2017.15>.
- Renduchintala, A., Jahan, F., Khanna, R., Javaid, A.Y., 2019. A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. *Digit. Invest.* 30, 52–72. <https://doi.org/10.1016/j.diin.2019.07.002>.
- Roder, A., Choo, K.-K.R., 2018. Unmanned aerial vehicle forensic investigation process: dji phantom 3 drone as a case study. ArXiv. URL <https://www.semanticscholar.org/paper/Unmanned-Aerial-Vehicle-Forensic-Investigation-Dji-Roder-Choo/f0be824621e530d3b587506bd45408aab4c6611a>.
- Salamh, F.E., Karabiyyik, U., Rogers, M.K., 2019. RPAS forensic validation analysis towards a technical investigation process: a case study of yuneeq Typhoon H. *Sensors* 19, 3246. <https://doi.org/10.3390/s19153246>.
- Salamh, F.E., Karabiyyik, U., Rogers, M.K., Matson, E.T., 2021. A comparative UAV forensic analysis: static and live digital evidence traceability challenges. *Drones* 5, 42. <https://doi.org/10.3390/drones5020042>.

- Salamh, F.E., Mirza, M.M., Karabiyik, U., 2021. UAV forensic analysis and software tools assessment: DJI Phantom 4 and Matrice 210 as case studies. *Electronics* 10, 733. <https://doi.org/10.3390/electronics10060733>.
- Saleem, S., Popov, O., Baggili, I., 2016. A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. *Digit. Invest.* 16. <https://doi.org/10.1016/j.diin.2016.01.008>. S55–S64.
- Shafi, H., 2019. Digital Forensics Is Ready for its Latest Challenge. *Drones* [WWW Document]. Medium. URL, 8.4.20. <https://medium.com/@haniahshafi/digital-forensics-is-ready-for-its-latest-challenge-drones-936c1418e928>.
- Singh, A., 2017. Drone forensics - detailed analysis done & explained. URL, 12.26.20. <https://www.dataforensics.org/drone-forensics>.
- Stanković, M., Mirza, M.M., Karabiyik, U., 2021. UAV forensics: DJI Mini 2 case study. *Drones* 5, 49. <https://doi.org/10.3390/drones5020049>.
- Swales, V., 2019. Drones used in crime fly under the Law's Radar, 2019 N. Y. Times. URL. <https://www.nytimes.com/2019/11/03/us/drones-crime.html>.
- [WWW Document] The CFReDS Project, 2019. The CFReDS project. <https://www.cfreds.nist.gov>, 8.6.20.
- n.d vconnectit, ash_history [WWW Document]. vConnect-IT. URL, 8.27.20. https://vconnectit.wordpress.com/tag/ash_history.
- Yousef, M., Iqbal, F., 2019. Drone forensics: a case study on a DJI Mavic Air, 2019. In: IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). Presented at the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1–3. <https://doi.org/10.1109/AICCSA47632.2019.9035365>. IEEE, Abu Dhabi, United Arab Emirates.
- Yousef, M., Iqbal, F., Hussain, M., 2020. Drone forensics: a detailed analysis of emerging DJI models. In: 2020 11th International Conference on Information and Communication Systems (ICICS). Presented at the 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE, Irbid, Jordan. <https://doi.org/10.1109/ICICS49469.2020.239530>, 066–071.