



INTERPOL

FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT

For First Responders and Digital Forensics Practitioners



January 2020

This Framework was prepared by the Digital Forensics Laboratory of the INTERPOL Innovation Centre,
Singapore.

Any inquiries, suggestions, and feedback can be directed to:

INTERPOL Global Complex for Innovation

18 Napier Road

Singapore 258510

Email: dfi@interpol.int

Tel: +6565503462

© INTERPOL Global Complex for Innovation, 2019

FOREWORD BY THE INTERPOL SECRETARY GENERAL

INTERPOL FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT

Drones are becoming less expensive while the technology behind them continues to develop rapidly. As such, we are seeing an increase in their use not only recreationally and commercially but also for criminal purposes.

Inevitably, this has given rise to serious challenges for the law enforcement community globally. Drones have become a permanent fixture in the current policing operating environment, and one that can only grow in scale and impact in the future.

However, many law enforcement officers still lack awareness and understanding of drone technologies. Drones pose a significant threat to public safety and security if abused. It is therefore crucial that officers are equipped with the necessary knowledge and training to respond to drone incidents safely and effectively. Furthermore, drones contain valuable data which need to be extracted and analysed to provide evidence to support an investigation.

INTERPOL engages with drone experts drawn from law enforcement, the private sector and academia across the world. This network was the driving force behind the creation of the *INTERPOL Framework for Responding to a Drone Incident – For First Responders and Digital Forensics Practitioners*.

This document is designed as a reference tool for law enforcement worldwide and illustrates INTERPOL's continuous efforts to promote innovation and enhance best practices among our member countries.

This framework is part of our ongoing commitment to making the world a safer place, and I would like to thank everyone who contributed to it.

Jürgen Stock

INTERPOL Secretary General

LETTER FROM THE INTERPOL INNOVATION CENTRE DIRECTOR

On a global level, many pre-existing crimes are developing into a significant global threat by taking advantage of advances in technology and the borderless nature of our interconnected world. Further to this, we are witnessing unprecedented types of criminal activities suddenly appearing on the radar of law enforcement. These developments are adding another layer of complexity to the challenge.

Against this backdrop, INTERPOL created its Innovation Centre in Singapore in 2017, with a view to fostering innovation in global law enforcement. The Digital Forensics Lab (DFL) within the Innovation Centre has been leading the effort to increase the level of innovative technology education, and enhance digital forensics capabilities, within the INTERPOL member countries.

I truly believe that the work of digital forensics laboratories is a crucial part of policing, particularly in the investigation of crimes such as drone incidents. Indeed, digital forensics practitioners are obliged to constantly learn and to develop their expertise, especially in the context of the emergence of innovative technologies such as drones.

To this end, the DFL has been organizing Drone Expert Group Meetings annually for the past three years, bringing together drone experts in law enforcement, industry, and academia to share information, knowledge, and best practices. Maintaining this global network of experts in drones has been tremendously rewarding and useful in serving our member countries more effectively. Building on our continued collaboration with the drone expert community, I am pleased to present the INTERPOL Framework for Responding to a Drone Incident – For First Responders and Digital Forensics Practitioners.

This Framework provides an overview of drones and associated devices, first responder guidance for responding to a drone incident, and guidance for digital forensic practitioners responsible for the acquisition, examination, analysis, and presentation of drone digital evidence. This framework will hopefully contribute to closing the gap in knowledge of global law enforcement on drones, as well as increase the capacity of global law enforcement – particularly first responders and digital forensics practitioners – to safely and effectively respond to a drone incident.

In the hope of creating momentum for the digital forensics field to become a very solid and important area of policing, the INTERPOL Innovation Centre will be at the forefront of instilling innovative spirit into the activities of digital forensics laboratories in the member countries, with the aim of contributing to overcoming complex global security challenges.

Anita Hazenberg

Director, INTERPOL Innovation Centre

Acknowledgement

There were many parties involved in constructing this INTERPOL Framework for Responding to a Drone Incident. First and foremost, INTERPOL would like to thank the participants of the Drone Global Expert Group that inspired the creation of this document. In November 2018, 6 countries and 4 US agencies gathered in Denver to explore the challenges and issues that Law Enforcement face in response to a drone incident. The outcome of this meeting is this framework in which we hope to guide member countries' Law Enforcement on how to respond to a drone incident.

This framework also features extracts from fundamentals of crime scene management and processing that are taken from the Crime Scene Responder Guide published by the United States National Institute of Justice.

INTERPOL would like to extend a special thanks to Steve Watson, who hosted the INTERPOL Drone Responder and Digital Forensic Examination Workshop, which explored and created the working space for this framework to be constructed. This workshop enabled 9 INTERPOL member countries to work together to create the structure and content of this document and enable us to ensure the content and data in this document applies to the community.

Also, we would like to thank: Harry Blackie, University of South Wales, for providing the information on drone file locations which was derived from Steve Watson's Drone Datasets, Matt Service for creating the Introduction to Drones content which has been used as a reference source in this document, and Dronelogbook.com for allowing us to include their drone geometry diagram.

Finally, we would like to thank the peer reviewers of this document, which greatly assisted in adding invaluable contributions and additional insights for this framework, filling in the knowledge gaps as well as helping with the final polishing of this document:

Alexandra Clare Alder, Jamie Allan, Priscilla Cabuyao, Christopher Church, Taurean Dennis, Greg Dominguez, Albert Drijfhout, Daniel Halliwell, Graeme Horsman, Bruce Keeble, David Kovar, Alan McConnell, Alan McDevitt, Joseph Majersky, Geoff Moore, Michal Naglowski, Alan McConnell, Vincent Olsthoorn, Dale Richards, Fahad E Salamh, Alan Tan, and Antonio Sousa Lamas.

We also want to take this moment to thank the drone community and law enforcement practitioners who may not be mentioned but have helped shape and form this framework.

Contents

FOREWORD BY THE INTERPOL SECRETARY GENERAL	3
LETTER FROM THE INTERPOL INNOVATION CENTRE DIRECTOR	4
Acknowledgement	5
1. Introduction	11
1.1 Document Purpose	11
1.2 Intended Audience.....	11
1.3 Applying the Document	11
2. Overview of Drones.....	12
2.1 Drones in the Modern World	12
2.2 Drone Incidents.....	12
2.3 Categories of UAVs.....	13
a) Recreational UAVs	13
b) Commercial UAVs	14
c) Bespoke UAVs	14
2.4 UAV Components.....	15
2.4.1 Physical Components	15
2.4.2 Software	15
2.5 Drone Payloads	16
a) <i>Camera and Video Payloads</i>	16
b) <i>Thermal, Infrared (IR), and Forward-looking Infrared (FLIR) Payloads</i>	16
c) <i>Delivery Payloads</i>	16
d) <i>Weapon Payloads</i>	17
2.6 Understanding Drones and Other Associated Evidence Sources	17
a) <i>Remote Controller</i>	17
b) <i>Mobile/Tablet Device</i>	18
c) <i>First Person View (FPV) Goggles</i>	18
d) <i>Memory Cards</i>	18
e) <i>Cloud Storage</i>	19
2.7 Drone Data	19
2.8 Possible Offences using Drones	22
2.9 Drone Legislation Overview	23
2.10 Guidance on Safe Drone Operation	24
3. First Responder Guidance	31
3.1 Initial Response/Receipt of Information	31

3.2 Safety Procedures	32
3.3 Emergency Care	33
3.4 Secure and Control Persons and Potential Evidence at the Scene	34
3.5 Turn Over Control of the Scene and Brief Investigator(s) in Charge.....	35
3.6 Document Actions and Observations	35
3.7 Establish a Command Post (Incident Command System) and Make Notifications.....	36
3.8 Manage Witnesses	37
3.9 Conduct Scene Assessment	37
3.10. Boundaries: Identify, Establish, Protect and Secure	38
3.11 Conduct Scene Walk-Through and Initial Documentation	40
3.12 Note-Taking and Logs.....	41
3.13 Drone Seizure.....	42
3.14 Process of Investigation	48
4. Digital Forensics Overview and Principles	50
4.1 Overview	50
4.2 Principles of Electronic Evidence	50
4.3 Digital Forensic Lab Overview	51
4.3.1 Receive Request.....	52
4.3.2 Register Case.....	52
4.3.3 Register Exhibit	52
4.3.4 Photograph Exhibit.....	53
4.3.5 Conduct Analysis	53
4.3.6 Return Exhibit.....	53
4.3.7 Close Case	53
5. Drone Digital Forensics	53
5.1 Overview	53
5.2 Acquisition	55
5.3 Examination	64
5.4 Analysis	65
5.5 Presentation.....	68
6. Drone Data Examples.....	70
6.1 Flight Logs	70
6.2 Media File Locations	70
6.3 Companion Mobile Phone Applications.....	71
6.3.1 DJI Mobile Application	72
6.3.2 Parrot Mobile Application.....	73

6.3.3 Yuneec Mobile Application	75
6.3.4 Yuneec Mobile Application for the Drone Camera	77
6.4 Note on Storage Locations on Drones	78
7. Common Tools Used in Drone Forensics	79
7.1 Cellebrite/MSAB XRY/Oxygen/CFID	79
7.2 CsvView and DatCon	79
7.3 DRone Open source Parser	79
7.4 Google Earth Pro	79
7.5 ST2Dash and Dashware.....	79
7.6 DJI Assistant	80
7.7 FTK Imager	80
7.8 VLC Player.....	80
8. Useful Web Resources	80
Appendices	82
Appendix A: Types of Drones	82
Appendix B: Drone Incident First Responder Scene Log.....	85
Appendix C: Drone Incident Record Sheet.....	88
Appendix D: Drone Examination Log	91
Appendix E: LiPo Battery Safety Reference Card	98
Appendix F: Checklist for a Basic Drone Response Kit	100
Appendix G: Core Competencies for First Responders and Digital Forensic Specialists.....	101
Appendix H: Core Competencies for First Responders	103
Appendix I: Core Competencies for Non-Technical First Technical Responders	104
Appendix J: Core Competencies for First Technical Responders	105
Appendix K: Core Competencies for Advanced First Technical Responders	106
Glossaries	107
Glossary I: General Aviation Abbreviations	108
Glossary II: Technical Abbreviations	111
Glossary III: UAV Digital Forensics Glossary.....	112
Glossary IV: UAV Glossary of Terms.....	118

List of Figures

Figure 1: Crashed Drone with Drugs Payload	12
Figure 2: Recreational UAVs.....	13
Figure 3: Commercial UAVs.....	14
Figure 4: Bespoke UAVs	14
Figure 5: Drone Remote Controllers	17
Figure 6: Drone Remote Controllers with Phones/Tablets Attached	18
Figure 7: First Person View (FPV) Goggles	18
Figure 8: Micro SD Memory Card.....	18
Figure 9: Cloud Storage Icons.....	19
Figure 10: Fingerprint.....	19
Figure 11: Singapore Aviation Authority Infographic on Safe Drone Usage	25
Figure 12: US Federal Aviation Authority Infographic on Unmanned Vehicle Classification	26
Figure 13: Integrated Drone Remote Controller	27
Figure 14: Overview of Quadcopter Components	27
Figure 15: Overview of Fixed Wing Drone Components	28
Figure 16: Drone Remote Controller without Screen	28
Figure 17: Drone Remote Controller with Mobile Phone Attachment.....	29
Figure 18: Mobile Application for Drone Controller	29
Figure 19: Drone Mission Planner	30
Figure 21: Precautions before Approaching a Drone at an Incident	44
Figure 21: Safety Precautions When Handling a Drone	45
Figure 22: Drone Handling Flowchart	45
Figure 23: LiPo Battery Safety Warning	46
Figure 24: Preservation of Digital Evidence	46
Figure 25: Collection of Digital Evidence.....	47
Figure 26: Documentation at Incident Scene.....	47
Figure 27: Investigation Process Overview	48
Figure 28: Digital Forensic Examiners Examining a Drone	50
Figure 29: Digital Forensic Lab Process	51
Figure 30: Digital Forensics Laboratory Analysis Model	54
Figure 31: Drone undergoing Examination	56
Figure 32: Extraction Process for Drones and Drone Remote Controllers.....	57
Figure 33: Drone Identification Label.....	58
Figure 34: Drone Examination Flowchart.....	62
Figure 35: Drone Controller Examination Flowchart	63
Figure 36: Other Sources of Evidence	64
Figure 37: Yuneec Remote Controller	78
Figure 38: Yuneec Typhoon Q500 4K Data Locations	78

List of Tables

Table 1 - Drone Investigation Data Considerations	22
Table 2 - Safe Drone Operation Guidance	24
Table 3 - Crime Scene Processing Sequence	31
Table 4 - Initial Response/Receipt of Information Procedure.....	32
Table 5 - Safety Procedure	33
Table 6 - Emergency Care Procedure	34
Table 7 - Procedure for Securing and Controlling Persons at the Scene.....	34
Table 8 - Procedure for Turning over Control of the Scene and Briefing Investigator(s) in Charge.....	35
Table 9 - Procedure for Documenting Actions and Observations.....	35
Table 10 - Procedure for Establishing a Command Post (Incident Command System) and Making Notifications.....	36
Table 11 - Procedure for Managing Witnesses	37
Table 12 - Procedure for Conducting Scene Assessment.....	38
Table 13 - Boundaries Procedure: Identify, Establish, Protect and Secure.....	39
Table 14 - Procedure for Conducting Scene Walk-Through and Initial Documentation.....	40
Table 15 - Note-Taking and Logs Procedure	42
Table 16 - Drone Seizure Process.....	43
Table 17 - Drone Hazards.....	44
Table 18 - Three Considerations for Further Investigations.....	49
Table 19 - Basic Digital Evidence Principles	51
Table 20 - Types of Data held on Drone Remote Controllers	55
Table 21 - Methods to Isolate Drones/Remote Controllers.....	59
Table 22 - Drone/Remote Controller Storage Media.....	59
Table 23 - Possible Data Traces held on a Drone/Remote Controller.....	60
Table 24 - General Criteria for the Admissibility of Electronic Evidence.....	68
Table 25 - Flight Log Locations for some Popular Drones.....	70
Table 26 - Multimedia Locations for some Popular Drones.....	71
Table 27 - DJI Go 4 Mobile Application	73
Table 28 -Parrot Freeflight Mobile Application Overview	75
Table 29 - Yuneec Mobile Application Overview	76
Table 30 - Yuneec Camera Mobile Application Overview.....	77

1. Introduction

1.1 Document Purpose

This INTERPOL Framework for Responding to a Drone Incident provides guidelines for First Responders and Digital Forensics Practitioners on how to respond to a drone incident. The framework is intended to provide technical guidance in managing and processing an incident.

The objective of these guidelines is to ensure that a member country has the relevant information needed in order to most appropriately respond to a drone incident. The advice given is intended to be used as a reference for both strategic and tactical levels. These guidelines should only be used as a template document that can be referenced by countries when developing their response to a drone incident. They should be modified or changed in line with the member country's local legislation, practices and procedures to best suit the country's needs.

1.2 Intended Audience

The document is intended for the use of INTERPOL member countries. The Framework has been developed to focus on two core audiences; the First Responders and Police Officers who attend incidents, and the Digital Forensics Practitioners who process the electronic evidence post incident.

Prosecutors, Judges, and Lawyers may also gain benefit from this document through attaining a better understanding of drones, and the drone incident process. This may be useful for understanding drone-related cases and their unique aspects.

1.3 Applying the Document

The Framework is not intended to impose limits on the First Responders or Technical Staff that have to follow their national legal framework's requirements. The advice given in the Framework is not intended to contradict with any national legislation or guidance.

2. Overview of Drones

2.1 Drones in the Modern World

Drones are now very popular; from recreational use by children, to adoption by experienced criminals for the distribution of illegal items. Whether you are interested in using the technology or not, it is impossible to escape the continual presence of drones in our everyday lives - whether as a recreational pastime in the park, in mainstream media, footage on social media platforms, or on television and in films. There are regularly news stories, both positive and negative, about the use of drones, and the opportunities, risks and threats they can pose to leading industries as well as the general public.

Changes in public perception, increases in manufacturers and available models, falling commoditised pricing, and rapidly advancing technology have all served to put drone devices in possession of many people around the globe. Whilst commonly and regularly referred to by the public and mainstream media as 'drones', many law enforcement agencies around the globe use differing terms – i.e. unmanned aerial vehicle (UAV), unmanned aerial system (UAS), small unmanned aerial system (sUAS), and remotely piloted aircraft system (RPAS). This document will use the terms drone and UAV interchangeably.

The combined increase of recreational and commercial UAV adoption around the globe highlights that interaction with these devices, and their owners and operators, will continue to become more common for police forces and law enforcement agencies in the coming years.

2.2 Drone Incidents

Drones come in many shapes and sizes and can be used for a variety of operations, ranging from aerial photography and videos to transporting goods from one place to another. Drones have been increasing in availability and use by the public over the last few years. This, in turn, has led to utilization by criminals to aid in illicit acts such as: invasion of privacy, drug smuggling, terrorist operations, and the disruption of critical infrastructure. Common examples include:

- Transporting contraband into prohibited areas, such as prisons.
- Flying in restricted areas to take photographs or videos for personal use, or to gather intelligence.
- Using the drone as a menace to disrupt daily life such as flying a drone above or near an airport.



Figure 1: Crashed Drone with Drugs Payload

Several drone incidents have transpired globally in the past few years. For example, a serious UAV incident occurred at Gatwick Airport, United Kingdom, in December, 2018, when an unauthorized UAV was flying on airport property and on the airport flight path. This incident disrupted airport operations for approximately three days, impacting thousands of people, and costing millions of pounds. Further, Singapore's Changi

Airport experienced two drone incidents in one week in June 2019, disrupting the busy airport for several hours, affecting approximately 65 flights, and impacting numerous people.

Additional drone incidents have affected numerous industries and people globally in recent years. For example, in the first 6 months of 2019 alone, reports of drone incidents affecting airports and prisons in the following countries were found in the media.

Airports:

- Singapore, England, Ireland, Scotland, Canada, Germany, Italy, Dubai, USA, Mexico, New Zealand, and Norway.

Prisons:

- USA, Italy, Scotland, Ireland, England, and Canada.

However, while the above occurrences make regular headlines, the potential user cases for UAVs in both the commission and prevention of crime are almost endless. As UAV technology continues to develop and prices continue to diminish, adoption will increase and present new challenges for first responders, through to digital investigation subject matter experts, across the law enforcement community.

2.3 Categories of UAVs

The sheer volume of UAVs available on the market, along with the drastic variations in pricing, can make it difficult to understand the different types of devices available. Our research has demonstrated that UAVs can be effectively summarised into three categories:

a) **Recreational UAVs**

Recreational UAVs are designed for use by amateur enthusiasts, hobbyists, and children, and tend to be low in price. Recreational UAVs start at the lower end of the specification spectrum, and can be purchased for less than £20. They are generally intended to be used outdoors, and possess a very limited battery life. UAVs are often classified as ‘recreational’ when weighing under 250 grams. There are now thousands of recreational UAVs available in the marketplace from a range of technology stockists and toy stores, as well as endless online shops.

Given that UAV legislation is governed by intended usage rather than the device capability, there is no limit on the upper end of recreational UAV specification. Hence some very expensive devices fall into this category; varying in price up into the thousands of pounds.



Figure 2: Recreational UAVs

b) Commercial UAVs

Commercial UAVs are designed to be used in commercial practices. These UAV devices usually carry a payload depicting their usage purpose - such as a camera, used for professional photography, industrial inspection, or land survey. Like their recreational counterparts, commercial UAVs are not governed by device capability but by the intention of the user, thus even the cheapest device could be classified as 'commercial' if an operator was to deploy the UAV with a commercial intention. Nonetheless, internationally there are many manufacturers of UAVs intended primarily for commercial rather than recreational use, and most commercially intended UAVs cost many thousands of pounds.

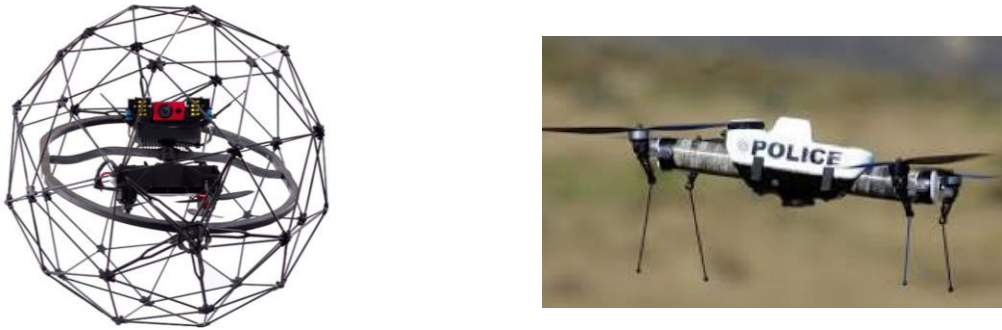


Figure 3: Commercial UAVs

c) Bespoke UAVs

Bespoke UAVs are engineered by the owner using component parts that are purchased individually and then put together, rather than purchased as a complete off-the-shelf system. Whilst recreational and commercial UAVs offer great functionality in an 'off-the-shelf' combination of UAV and controlling software, the market for bespoke UAVs has expanded at a rapid rate in recent years as a wider selection of component parts have become available and commoditised, driving down costs.

Bespoke UAVs enable a user or trader to purchase disparate component parts of a UAV from different sources, and then build and configure the device according to their individual requirements or available budget. These systems are only limited in capability by the capacity of available components and the knowledge and skill of the people building them, which are both increasing exponentially.

Bespoke configurations can be built very cheaply as recreational UAVs designed as toys for children, but can conversely be designed, specified, and constructed by UAV enthusiasts and experts to compete in capability with even the leading commercial manufacturers, comprising component parts costing into the thousands of pounds.

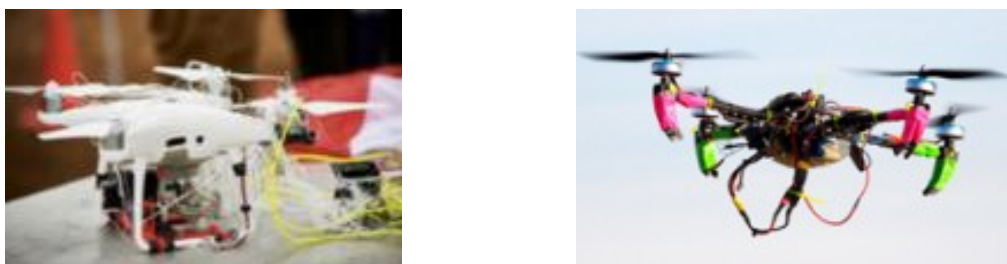


Figure 4: Bespoke UAVs

2.4 UAV Components

Any UAV will consist of the following two types of components:

2.4.1 Physical Components

The physical components of any UAV which make up the body and flight mechanisms can be broken down into the following categories. Not each and every UAV encountered will contain all outlined component parts, but each element on any UAV can be identified as one of the following:

i) Drone Body

The core fuselage of the UAV used to house all other components.

ii) Flight Controller

Used to control flight. This device will stabilize the UAV and generally accept navigation input from a radio control device. In more sophisticated systems the flight controller can both be controlled remotely in real time and be pre-programmed for autonomous flight.

iii) Motors, Rotors/Propellers/Wings, and Speed Controllers

These component parts combined provide the lift and propulsion for the UAV. Different designs exist, for example, specializing in increased speed or flight duration.

iv) Protective Casing

This protection securely encases the motors and propellers (the most vulnerable component of any UAV) to prevent collision and loss of control, and subsequent damage to the system.

v) GPS Receiver

Not essential in all UAVs, but common in the leading solutions. This component is used to effectively manage UAV position, return to home functionally, and autonomous flight routes.

vi) Radio Receiver (RX)

Used to receive control input signals received from the ground based transmitter.

vii) Transmitter (TX)

Transmits manual input from the operator on the ground to the UAV.

viii) LED Lights

Some UAVs come equipped with LED lights (usually green and red) which can be used to aid the pilot of the orientation of the drone, and help other airspace users to identify the drone.

2.4.2 Software

All UAVs include an application or software that is used to control the system when it is operational. While each recreational or commercially intended UAV will tend to come with its own configured software or control solution, for bespoke UAVs the responsibility is on the person constructing the device to build or integrate a component which works effectively. In support of this model, there are now many open source flight control and ground control applications available online that can be freely downloaded and easily modified to perform any number of tasks.

No matter which system is used or how the software components are configured, UAV software solutions can be classified into two core categories:

a) Flight Management Software

This software is uploaded to the flight controller within the UAV at one end, and also within the remote control of the user at the other end. When operational, it is used to control the UAV during takeoff, flight, and landing. Typical functions which are controlled by the flight management software solution include UAV flight, device stabilization, and manual navigation input.

b) Ground Control Software

This software is used to control pre-determined navigation and effectively plan flight schedules, and is best used by a pilot when the UAV is grounded in planning and preparation for flight. Ground control software additionally facilitates enhanced live monitoring to remote users other than the pilot when the UAV is in flight - either directly to their computers or smart devices such as a tablets or mobile phones.

Whilst offering significant innovation and supporting technical development of skills, consideration should be given to the fact that bespoke UAVs may potentially propose increased risks and more dangerous use, as they are likely to be configured with convenience and cost, rather than safety, in mind. This may result in them lacking core safety features and functionality that are built into many of the leading commercial off-the-shelf (COTS) systems, such as restricted area control, obstacle avoidance, and fail-safe management. These features lessen risk to persons and property in the event of a pilot error or a system failure.

Whilst some of these proposed categorizations of UAVs can become blurred, for example – in cases where wealthy recreational users purchase higher end UAVs that are intended for commercial purposes, this categorization approach is recommended when defining UAVs and considering their respective capabilities.

2.5 Drone Payloads

There are many payloads available at different price points that can be carried by commercial UAVs. These typically fall in to one of the following categories.

a) Camera and Video Payloads

Whilst most UAVs are designed to carry some sort of camera, commercial UAVs will carry far more sophisticated imaging devices with enhanced features that could include: first person view (FPV), 4K video, optical zoom for commercial inspection applications, and GPS tagging for 3D mapping. More sophisticated camera systems may have camera gimbals which hold the camera in a level and stabilized position, eliminating any flight movement to produce a superior stabilized image and video output.

b) Thermal, Infrared (IR), and Forward-looking Infrared (FLIR) Payloads

Traditionally reserved for higher end systems, thermal imaging can be employed in a variety of user cases, including: agricultural surveying, health and safety, law enforcement, and digital search and rescue applications. Infrared payloads can be particularly useful for effective operation of UAVs during dark or night time flying conditions. FLIR uses a thermographic camera that senses the slightest of variances in infrared radiation. FLIR can see different frequency ranges, and hence can detect chemical compounds using light detection and ranging (LiDAR) to capture the exact location and distance between objects.

c) Delivery Payloads

The use of UAVs to provide timely and efficient deliveries has become an ever-increasing area of investment in recent years, with Amazon most notably making headlines for their Prime Air service.

While commercial and retail deliveries provide one opportunity for mainstream adoption, radio deployment and delivery technology could also significantly enhance other sectors, such as healthcare, with UAVs able to transport time-critical services including defibrillators on demand. However, the use of UAVs for delivery also offers opportunities to criminals, providing them with innovative solutions for transporting drugs, weapons, and other items. This tactic has been encountered in prisons internationally.

d) Weapon Payloads

UAVs possess the ability to transport weapons for distribution, or to conduct attacks using the UAV itself. This is now seen regularly in military user cases where devices are chosen as the attack method due to the increased precision and reduced risk of loss of life posed in comparison to traditional human-led combat methods. To equate the risk in an operational user case, a medium specification UAV has the capability to carry a payload of 3kg for 16 minutes at 16 meters/second. This could equate to an autonomous vehicle that can effectively carry and deploy 3kg of explosives to a range of 16 kilometres.

e) Communications Payloads

Communications payloads are not yet commonly used, but may become more common with the introduction of 5G networks. UAVs can carry communications payloads that might be used to monitor, interrupt or mimic legitimate private wireless communications – for example, through spoofing cell towers or wireless access points.

2.6 Understanding Drones and Other Associated Evidence Sources

Drones, unlike many other electronic devices, require supporting devices for appropriate operational capability. These associated devices could include the following components:

a) Remote Controller

These are used to control the drone remotely.



Figure 5: Drone Remote Controllers

b) *Mobile/Tablet Device*

These devices are used to view the camera/video feed from the drone.



Figure 6: Drone Remote Controllers with Phones/Tablets Attached

c) *First Person View (FPV) Goggles*

FPV goggles are used to view the camera/video feed of the drone, and may also control the drone by head movements or associated controls.



Figure 7: First Person View (FPV) Goggles

d) *Memory Cards*

Removable media may be utilized to hold pictures and videos taken using the drone. They may also contain flight path data, as well as geotagging of photographs by using exchangeable image file (EXIF) data within the photographs.



Figure 8: Micro SD Memory Card

e) Cloud Storage

The drone may utilize the associated mobile handset to store photographs or video in cloud storage services such as iCloud or Google Photos.



Figure 9: Cloud Storage Icons

f) Wet Evidence

Like any other piece of physical evidence, a drone and its associated devices may hold wet evidence such as fingerprints, DNA etc.



Figure 10: Fingerprint

While the drone will be the primary source of evidence, it is vital that secondary sources of evidence such as the controller, mobile phone/tablet, and memory cards are secured to ensure that the most comprehensive picture of the event and associated intelligence is collated.

When responding to a drone incident, it is important to capture as much information on the incident and the associated events, such as identifying key witnesses, locations and environmental conditions. Some of these identifiers may seem superfluous at first, but as the investigation unfolds it may become a critical factor.

2.7 Drone Data

Like all other digital solutions and devices, the use of a UAV will inevitably result in a digital footprint with the creation and storage of data - whether intended by the user as part of the core service capability or as a by-product of the use of the UAV, such as historical usage logs.

2.7.1 Types of Data

There are various types of data which assist the investigation of drone incidents. These include:

a) Audio Visual Content

In most cases, the primary and largest source of data stored by either recreational or commercial UAVs will consist of digital imagery or video footage. Most operators now strive to record the highest quality of footage possible to give them a unique selling point and business advantage over their competitors, which can result in significant volumes of data and required storage capacity, even in short bursts of filming or capturing imagery.

b) Flight Schedules

Where the UAV control system offers the capability to plan advanced flight schedules and offers a degree of autonomy to the user, this data is regularly retained and can be revisited by the user to review previous activity, repeat an existing flight schedule, or amend previous flight schedules. Often, data that is captured during flight and retrospectively downloaded into a control system or flight schedule review platform will also be intentionally retained by the user for an audit and review of usage overlaid with mapping, so users can track the UAV's activity and progress.

c) Other Payload Created Content

Where other payloads are integrated into a UAV, these too are very likely to capture and record their own data sources and present them back to a user or organization. The type of data will vary depending on the payload in question, but one example is UAVs that are used as delivery assets. These will be required to audit times, locations, and results of their respective missions.

d) Automated Usage Logs

UAVs are no different to most other digital devices in that when in use they routinely create and retain digital data that helps them continue to function as intended. While this data is not intended to be read by the user, and in fact will be unbeknown to most, some UAVs will routinely create and store usage logs that can include details such as mission details, time and date of operations, and navigational waypoints during use. This data will generally consist of GPS positions, motor speeds, altitude, and directional information.

2.7.2 Accessing Different Data Storage Mediums

Multiple devices/evidence sources present significant opportunities to investigators who, if required to do so, may have the opportunity to access vast volumes of rich data about an owner or user's usage of a device from multiple data storage sources. Our research has demonstrated that the storage and retention of data change dramatically depending on the manufacturer and specification of the UAV in question. This can range from very little, if any, digital recovery opportunities available from low-end recreational devices, right up to vast volumes of complex data that can be accessed from commercial and bespoke UAV configurations.

In addition to varying volumes of data, the location of data can also vary significantly depending on the specifications of the device, and the chosen configuration of the user. It is therefore crucial when considering data from UAVs that the principle of Digital Profiling is adopted to review: the wider technical profile and digital competency of the user, the specification of the UAV in question, any payloads in use, and the flight control configuration in place for the specific UAV. Once each of these factors has been considered, then an informed assessment can be made as to where the relevant data relating to an enquiry may be retained.

There are several locations where data may reside during an investigation. These include:

a) On-board Data Storage

Some UAV devices will store and retain information within memory and processors built into the UAV frame or flight controller. Depending on the specifications of the UAV and its associated ports, the method of extracting this data may vary from relatively simple methods such as 'plug and play', to advanced destructive forensics techniques such as 'chip-off'.

b) Removable Storage Devices

Given the size of the associated files, most UAVs designed to capture high resolution images and video will offer the capability to integrate a removable storage device. Given micro SD cards are now available with up to 2 TB in storage, this range offers the most value and capacity while taking up little space, and is the leading data storage solution in UAVs. It should be taken into consideration that while the primary purpose of external storage may be to retain multimedia files, other types of data may also be available on the device.

c) Mobile Devices and Applications

Many UAVs offer the ability to fully or partially control the device or payload via a web connection or native application on a smart device. This should not be overlooked as a potential source of UAV data. When conducting digital profiling, consider which applications the subject has on their mobile device, and what the presence of a UAV-related application may offer to the investigation.

d) Remote Controllers

Most drones require a specific remote controller. This remote controller may hold residual data that may assist in helping identify the drone it is paired with, as well as any phones or tablets used to view the drone's footage.

e) Ground Stations

Control systems that have a ground link for route planning, FPV, or visual monitoring can also record their data or live footage onto a local storage device such as a computer hard drive. Access to this rich data can be obtained through the use of integrated software to view the data in its intended source or, if this is not available, through computer triage or traditional digital forensic techniques.

f) Cloud-Based Data Platforms

The continual commoditization of and increased access to cloud-based storage means that it cannot be overlooked as a potential source of UAV data. Cloud data could be intended by the user to reduce local storage demand, or a by-product of a UAV cloud-hosted platform which retains data on behalf of its customers.

g) Network Packet Data

Wireless controllers often issue commands to the drone and communicate through wireless networks. This network packet data is an additional source of forensic evidence. The introduction of 5G will likely lead to an increase in drone control over cellular networks, making cellular network data a potentially invaluable evidentiary source.

2.7.3 Drone Investigation Data Considerations

Due to the nature of drone data, and the fact that drones utilize additional supporting devices, the following should be considered:

Drone Investigation Data Considerations
<ul style="list-style-type: none">• The data can be scattered in several physical locations, sometimes across countries.
<ul style="list-style-type: none">• The data can be transferred across jurisdictional borders effortlessly and in split seconds.
<ul style="list-style-type: none">• The data is highly volatile – it is easily altered, overwritten, damaged or destroyed by a single stroke of a key.
<ul style="list-style-type: none">• The data can be copied without degradation.
<ul style="list-style-type: none">• The lifespan of electronic evidence, unlike any other discipline of forensic evidence, is short before it is rendered useless. After five years the device may not be able to be switched on or function properly.

Table 1 - Drone Investigation Data Considerations

Therefore, based on these facts, drone evidence must be processed and handled with due care.

Additional information and advanced considerations regarding the identification, acquisition, analysis and interpretation of data from UAVs will shortly be available in an advanced INTERPOL Drone Forensics Module - which is currently under development.

2.8 Possible Offences using Drones

In response to the emerging threat of UAVs, and the risk they pose to the public and property if not used in accordance with their regulations and licence procedures, a number of offences have recently been created. Drone offences vary across jurisdictions, hence first responders should have at least an appreciation of the applicable drone laws.

Drone offences can include any of the following:

- Failure to maintain direct visible contact with the UAV.
- Flying above the locally permitted altitude (e.g. the maximum permitted altitude in the UK and US is 400 feet).
- Flying in an airspace without permission.
- Flying in restricted airspaces, such as: an airport, military base or critical infrastructure installation such as a nuclear power station.
- Flying when it is unsafe to do so (e.g. bad weather conditions).
- Unauthorized use of a surveillance aircraft (e.g. use UAV for surveillance/invasion of privacy).
- Endangering a civil aircraft (e.g. flying too high, or within an airport or restricted airspace).

Additionally, in some jurisdictions it is illegal to fly over people - particularly crowds, to carry a payload that the drone has not been designed to carry, and to release cargo from a drone.

With drone offences, the following points should be considered:

- What are the facts you want to establish?
- Location of offence.
- Time and date of offence.
- Have the pilot and other suspects been identified and detained?
- What was the purpose of the drone flight?
- Was there an intended target? If so, who/what was it and what was the intention of the drone operator?

One further important aspect that needs to be considered is that even though the drone is the perceived threat, the actual target for apprehension should be the pilot and associated suspects.

2.9 Drone Legislation Overview

Although approaches to drone regulation differ dramatically across the globe, some elements of regulation are largely the same from country to country. Most countries have adopted a safety-first approach, and may require registration of either the drone or the pilot, or both. Even within countries with existing drone legislation, laws are constantly being re-evaluated. There may be regulation of the drone itself and also of the airspace you are flying the drone in. Most legislation and regulation is made by the country's Civil Aviation Authority. Some countries have banned drones completely, so if you travel to one of these countries you are liable to having your drone confiscated at customs, or if you are caught flying a drone this may result in huge fines or imprisonment.

Countries that have banned drones (as of August, 2019) include:

Algeria, Barbados, Brunei, Cote d'Ivoire, Cuba, Iran, Iraq, Kyrgyzstan, Madagascar, Morocco, Nicaragua, Senegal, and Syria.

As a law enforcement officer, you are encouraged to know the current laws within your country. A majority of countries have appointed their Civil Aviation Authority to create the required legislation for drones.

The absence of drone legislation does not necessarily mean you can fly a drone wherever or however you like. In fact, this could mean that the authorities are generally opposed to the use of drones in their country, especially by tourists. The same cautionary note applies when bringing a drone through customs. Sometimes, when a country has no drone-specific laws, some customs officials choose to confiscate drones, and some choose not to. For countries that do have drone/UAS legislation, the country's national or civil aviation authority typically sets and enforces drone regulations.

If you are unsure of your country's drone legislation, we recommend contacting the national aviation authority to check the latest guidance. Many countries now have mobile apps that are available through mobile app stores such as Google Play for Android, and the Apple App Store for iPhone, that can be used to verify the relevant local regulations, and view maps of areas in which it is permissible to fly drones.

2.10 Guidance on Safe Drone Operation

At a minimum, when flying a drone in a country where there is no known drone legislation, it would be wise to follow the following guidance (this guidance has been taken from the United States Federal Aviation Administration’s Drone Advisory, and the United Kingdom Civil Aviation Authority’s Drone Code):

Safe Drone Operation Guidance	
1	Keep the drone within visual line-of-sight.
2	Fly within the drone manufacturer’s specified weather parameters.
3	Stay 150 feet away from people and properties. Do not fly directly over people.
4	Stay 500 feet away from crowds and built-up areas.
5	Fly at or below 200 feet (Singapore)/400 feet (US).
6	Fly during daylight or civil twilight.
7	Fly at or under 100 mph.
8	Yield right of way to manned aircraft.
9	Do not fly from a moving vehicle.
10	Do not fly within 5 km of an airport or critical infrastructure installation such as nuclear power station, military base or restricted area - as designated by the country.

Table 2 - Safe Drone Operation Guidance

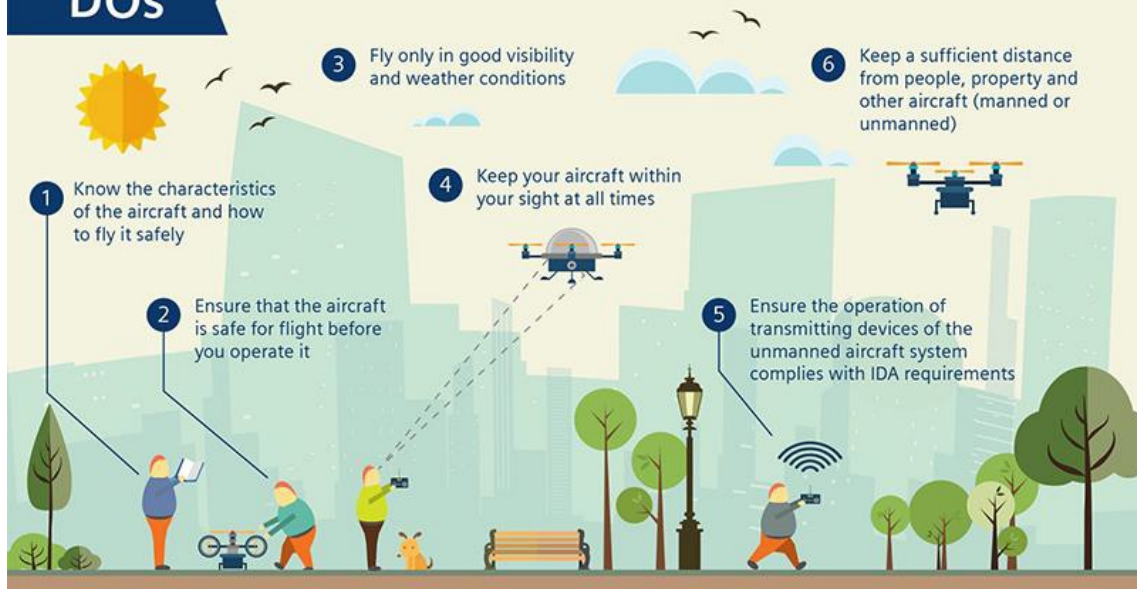
If in doubt, seek advice from your Civil Aviation Authority.

Further recommendations for the safe operation of UAVs can be seen below in Figures 11 and 12.

FLY IT SAFE

Advisory on the Safe and Responsible Operation of Unmanned Aircraft
(For recreational and private uses only)

DOs



DON'Ts



Figure 11: Singapore Aviation Authority Infographic on Safe Drone Usage

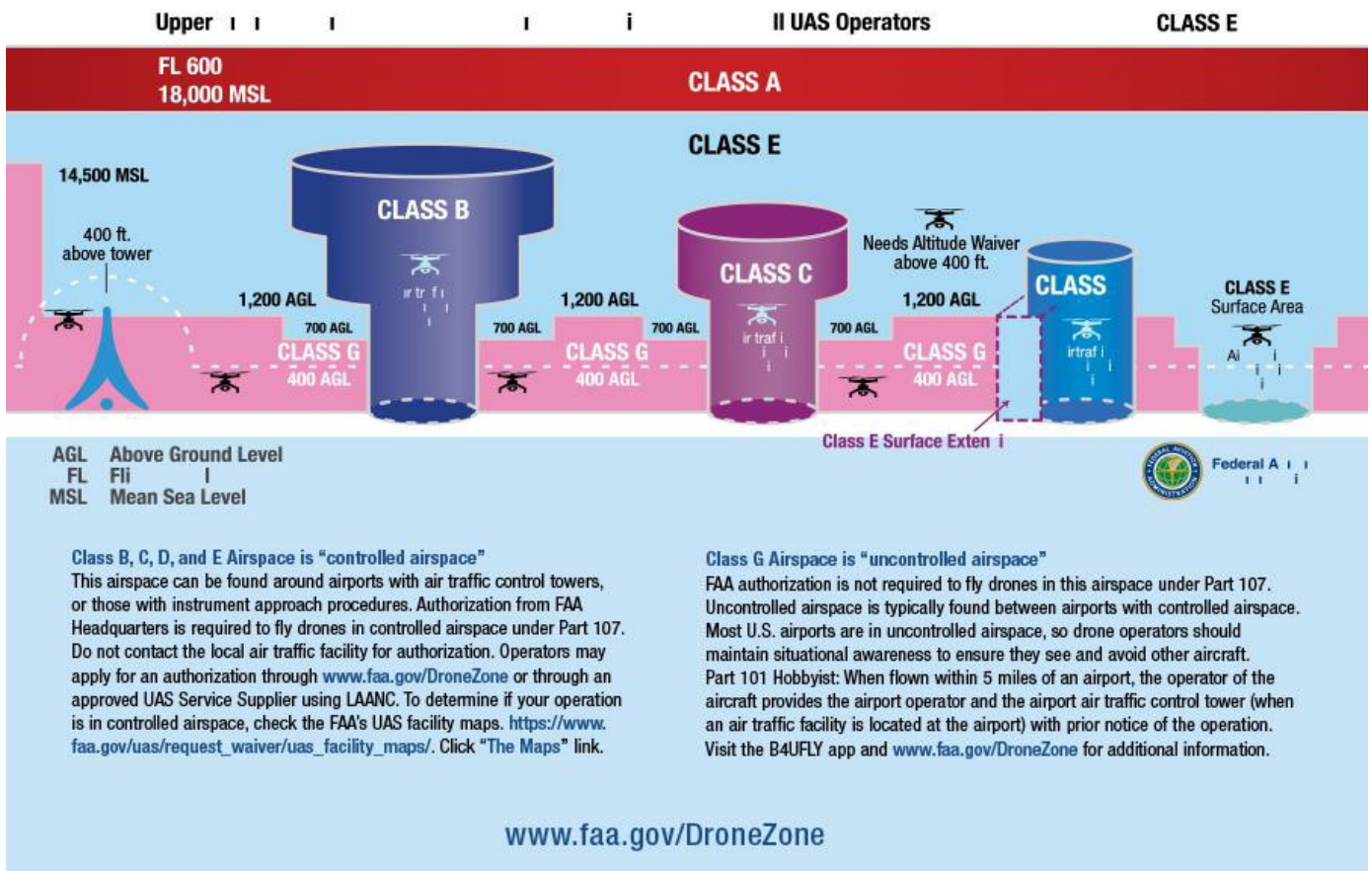


Figure 12: US Federal Aviation Authority Infographic on Unmanned Vehicle Classification

2.11 Sample of Drones and Associated Equipment



Figure 13: Integrated Drone Remote Controller

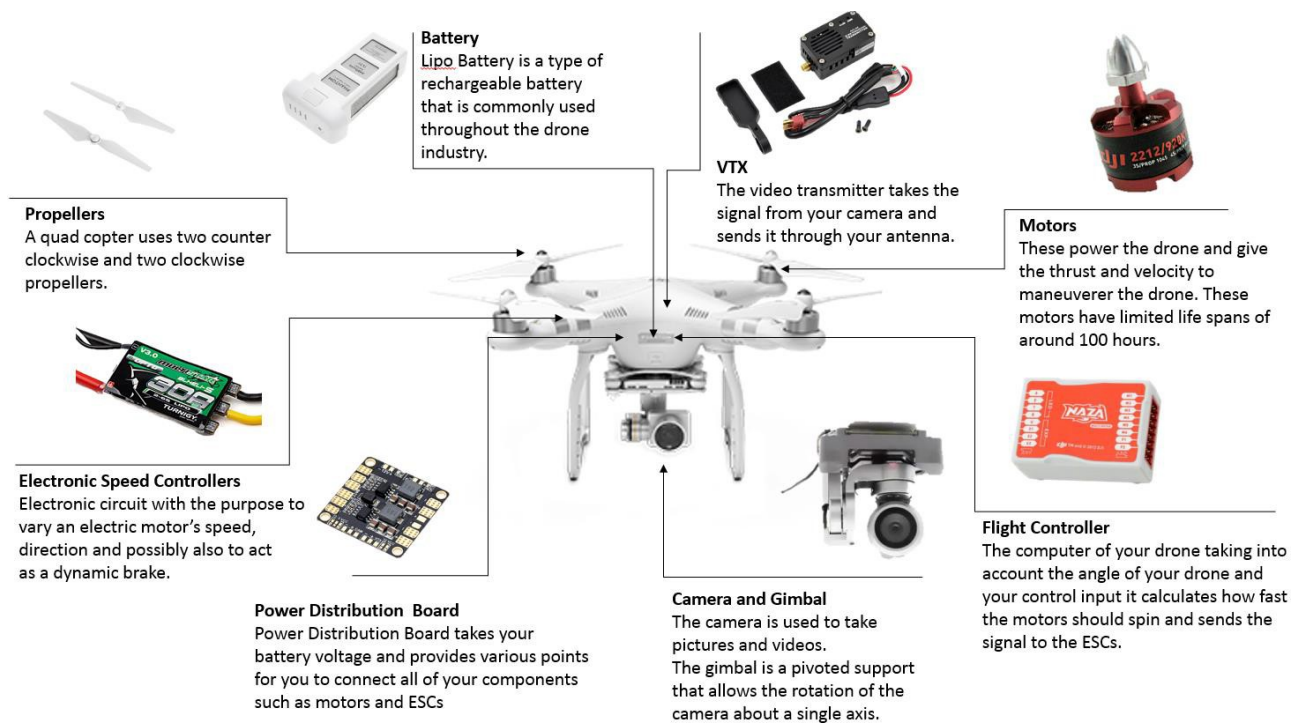


Figure 14: Overview of Quadcopter Components

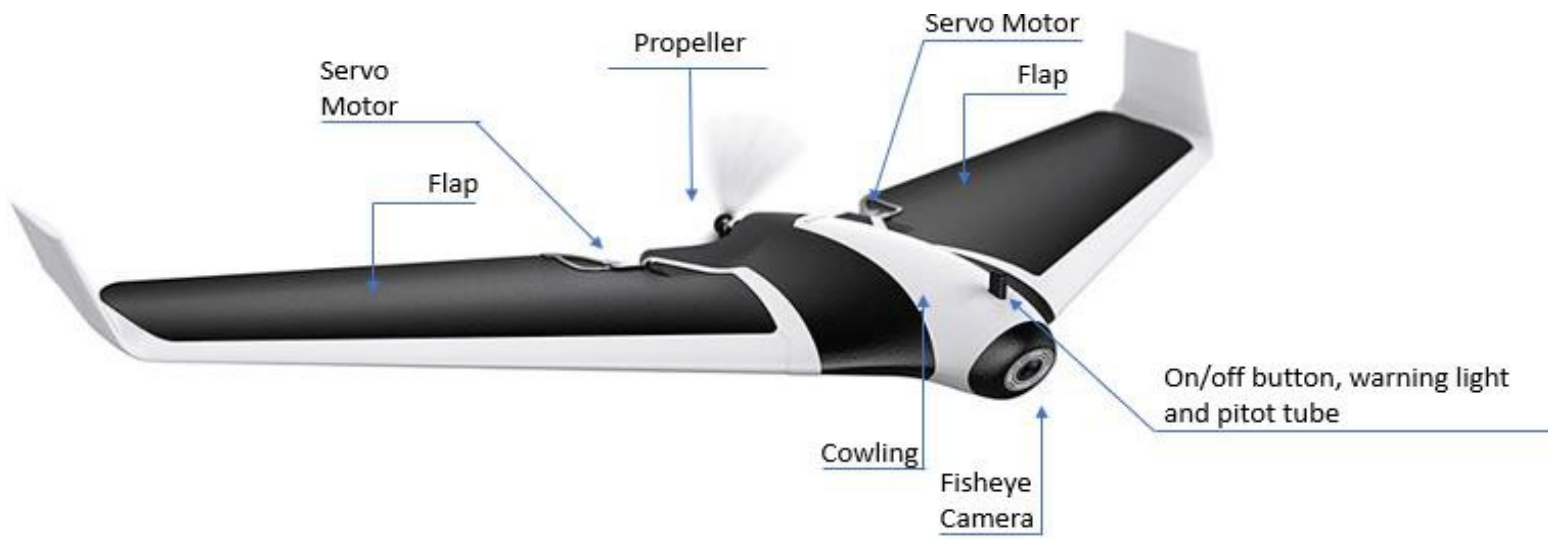


Figure 15: Overview of Fixed Wing Drone Components



Figure 16: Drone Remote Controller without Screen



Figure 17: Drone Remote Controller with Mobile Phone Attachment



Figure 18: Mobile Application for Drone Controller

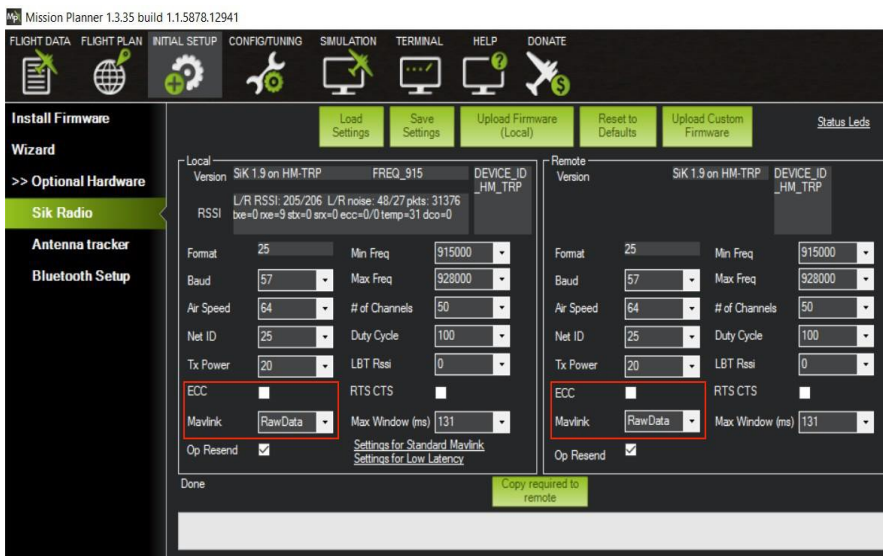
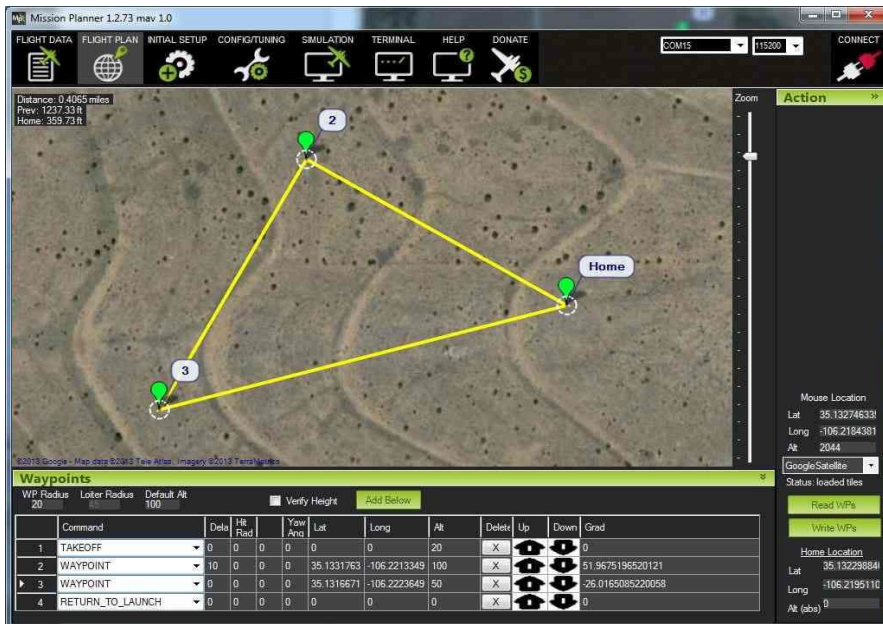


Figure 19: Drone Mission Planner

3. First Responder Guidance

This guidance has been created to maximize potential investigational avenues, and ensure the safety of the investigator and general public.

Crime Scene Processing Sequence	
1	Initial Response/Receipt of Information
2	Safety Procedures
3	Emergency Care
4	Secure and Control Persons at the Scene
5	Boundaries: Identify, Establish, Protect and Secure
6	Turn Over Control of the Scene and Brief Investigator(s) in Charge
7	Document Actions and Observations
8	Establish a Command Post (Incident Command System) and Make Notifications
9	Manage Witnesses
10	Conduct Scene Assessment
11	Conduct Scene Walk-Through and Initial Documentation
12	Note-Taking and Logs

Table 3 - Crime Scene Processing Sequence

3.1 Initial Response/Receipt of Information

Principle: One of the most important aspects of securing the crime scene is to preserve the scene with minimal contamination and disturbance of the physical evidence. The initial response to an incident should be expeditious and methodical.

Policy: The initial responding officer(s), upon arrival, shall assess the scene and treat the incident as a crime scene. They shall promptly, yet cautiously, approach and enter the crime scene, remaining observant of any persons, vehicles, events, potential evidence, and environmental conditions.

Procedure:

The initial responding officer(s) should	
a	Note or log dispatch information (e.g. address/location, time, date, type of call, parties involved).
b	Be aware of any persons or vehicles leaving the crime scene.
c	Approach the scene cautiously, scan the entire area to thoroughly assess the scene, and note any possible secondary crime scenes.
d	Be aware of any persons and vehicles in the vicinity that may be related to the crime. Make initial observations (look, listen, smell) to assess the scene and ensure officer safety before proceeding.
e	Remain alert and attentive. Assume the crime is ongoing until determined to be otherwise.
f	Treat the location as a crime scene until assessed and determined to be otherwise.
g	Safely direct additional responding units into the area

Table 4 - Initial Response/Receipt of Information Procedure

Summary: It is important for the initial responding officer(s) to be observant when approaching, entering, and exiting a crime scene. The initial responders should ensure the safety of law enforcement personnel and the general public located in or near the crime scene.

3.2 Safety Procedures

Principle: The safety and physical well-being of officers and other individuals in and around the crime scene are the initial responding officer(s') priority.

Policy: The initial responding officer(s) arriving at the scene shall identify and control any dangerous situations or persons.

Procedure:

The initial responding officer(s) should	
a	Ensure that there is no immediate threat to other responders; scan the area for sights, sounds, and smells that may present danger to personnel (e.g. hazardous materials such as payloads that contain IED or biohazards). If the situation involves a payload, biological weapons, or radiological or chemical threats the appropriate personnel/agency should be contacted before entering the scene.
b	Approach the scene in a manner designed to reduce the risk of harm to the officer(s), while maximizing the safety of victims, witnesses, and others in the area.

c	Survey the scene for dangerous persons and control the situation.
d	Notify supervisory personnel and call for assistance/backup.

Table 5 - Safety Procedure

Summary: The control of physical threats will ensure the safety of officers and others present.

3.3 Emergency Care

Principle: After controlling any dangerous situations or persons, the initial responding officer(s') next responsibility is to ensure that medical attention is provided to injured persons while minimizing contamination of the scene.

Policy: The initial responding officer(s) shall ensure that medical attention is provided with minimal contamination of the scene.

Procedure:

The initial responding officer(s) should	
a	Assess the victim(s) for signs of life and medical needs and provide immediate medical attention.
b	Call for medical personnel.
c	Guide medical personnel to the victim to minimize contamination/alteration of the crime scene.
d	Point out potential physical evidence to medical personnel and instruct them to minimize contact with such evidence (e.g. ensure that medical personnel preserve all clothing and personal effects without cutting through bullet holes, knife tears etc.). Document movement of persons or items by medical personnel.
e	Instruct medical personnel not to clean up the scene, and to avoid removal or alteration of items originating from the scene.
f	If medical personnel arrived first, obtain the name, unit, and telephone number of attending personnel, and the name and location of the medical facility where the victim is to be taken.
g	If there is a chance the victim may die, attempt to obtain a 'dying declaration'. In some instances, fingerprint and shoe impressions of medical personnel may need to be taken for elimination purposes.
h	Document any statements/comments made by victims, suspects, or witnesses at the scene.

i	If the victim or suspect is transported to a medical facility, send a law enforcement official with the victim or suspect to document any comments made, and to preserve evidence. (If no officers are available to accompany the victim/suspect, stay at the scene and request medical personnel to preserve evidence and document any comments made by the victim or suspect).
j	Safeguard evidence, such as a payload that is taken into custody. Follow chain-of-custody procedures as soon as the evidence is confiscated.

Table 6 - Emergency Care Procedure

Summary: Assisting, guiding and instructing medical personnel during the care and removal of injured persons will diminish the risk of contamination and loss of evidence.

3.4 Secure and Control Persons and Potential Evidence at the Scene

Principle: Controlling, identifying, and removing persons at the crime scene, and limiting the number of persons who enter the crime scene is an important function of the initial responding officer(s) in protecting the crime scene.

Policy: The initial responding officer(s) shall identify persons at the crime scene and control their movement.

Procedure:

The initial responding officer(s) should	
a	Control all individuals at the scene - prevent individuals from altering/destroying physical evidence by restricting movement, location and activity while ensuring and maintaining safety at the scene.
b	Identify all individuals at the scene, such as: <ul style="list-style-type: none"> • Suspects: Secure and separate. • Witnesses: Secure and separate. • Bystanders: Determine whether they are a witness. If so, treat as above; if not, remove from the scene. • Victims/family/friends: Control while showing compassion. • Law enforcement, medical and other assisting personnel: Identify.
c	Exclude unauthorized and non-essential personnel from the scene (e.g. law enforcement officials not working the case, politicians, media).

Table 7 - Procedure for Securing and Controlling Persons at the Scene

Summary: Controlling the movement of persons at the crime scene and limiting the number of persons who enter the crime scene is essential to maintaining scene integrity, safeguarding evidence, and minimizing contamination.

3.5 Turn Over Control of the Scene and Brief Investigator(s) in Charge

Principle: Briefing the investigator(s) taking charge assists in controlling the crime scene, helps establish further investigative responsibilities, and assists with the managing of resources.

Policy: The initial responding officer(s) at the scene shall provide a detailed crime scene briefing to the investigator(s) in charge of the scene.

Procedure:

The initial responding officer(s) should	
a	Brief the investigator(s) taking charge.
b	Assist in controlling the scene.
c	Turn over responsibility for the documentation of entry/exit.
d	Remain at the scene until relieved of duty.

Table 8 - Procedure for Turning over Control of the Scene and Briefing Investigator(s) in Charge

Summary: The scene briefing is the only opportunity for the next in command to obtain initial aspects of the crime scene before subsequent investigation.

3.6 Document Actions and Observations

Principle: All activities conducted and observations made at the crime scene must be documented as soon as possible after the event to preserve information.

Policy: The initial responding officer(s) shall maintain documentation as a permanent record.

Procedure:

The initial responding officer(s) should	
a	Document observations of the crime scene, including the location of persons and items within the crime scene, and the appearance and condition of the scene upon arrival.
b	Document conditions upon arrival (e.g. lights on/off; shades up/down, open/closed; doors and windows open/closed; smells; ice, liquids; movable furniture; weather; temperature; and personal items).
c	Document personal information from the witnesses, victims, suspects, and any statements or comments made.
d	Document the actions of witnesses, victims, suspects, and others.

Table 9 - Procedure for Documenting Actions and Observations

Summary: The initial responding officer(s) at the crime scene must produce clear, concise, documented information encompassing their observations and actions. This documentation is vital for later investigation and court processes.

3.7 Establish a Command Post (Incident Command System) and Make Notifications.

Principle: Setting up a location where crime scene investigation activities can be co-ordinated, media meetings can be held, and team meetings can occur is very valuable. This command post provides a central location for crime scene investigation activities and an assessment of resources. Establishing a command post also helps to ensure that other key investigative participants are told of the investigation and included in activities as needed.

Policy: The investigator(s) in charge shall set up a location where crime scene investigation activities can be coordinated, media meetings can be held, and team meetings can occur.

Procedure:

The initial responding officer(s) should	
a	Set up a temporary command post in a location where media can take necessary photographs without jeopardizing the scene (and evidence) security.
b	Notify investigators or appropriate department(s) (such as Homicide) of information gathered at the crime scene. Discuss the details of the scene during this step.
c	Notify the Communications Department (Dispatch) of phone numbers at the command post.
d	Ask the Communications Department (Dispatch) to notify surrounding agencies and send teletypes regionally and nationally when a suspect has fled the scene. These alerts should include a description of the suspect, any vehicles involved, and contact information for the person these agencies should contact if they locate the suspect.
e	Brief the supervisor as required.
f	Debrief with first responders and officers/investigators.
g	Make necessary assignments, recording each on a formal assignment sheet.
h	Use the assignment sheet to record assignment updates throughout the investigation. Make this assignment sheet available to personnel working on the case. Assign evidence recorder, entry/exit recorder (who is also responsible for keeping an event timetable).
i	Establish the status and locations of victims and suspects.
j	Establish the status of bulletins that have been broadcast regarding victims and suspects. Ensure that missing suspect alerts are broadcast. Establish a schedule for investigative team meetings (including all uniformed officers), during which status will be given, assignment updates will be made, and other key information will be shared.

Table 10 - Procedure for Establishing a Command Post (Incident Command System) and Making Notifications

Summary: The establishment of a command post is critical to the communication among the crime scene responders, Dispatch and others providing information to the crime scene responders.

3.8 Manage Witnesses

Principle: The timely interviewing of witnesses is crucial to the solution of a crime.

Policy: The investigator(s) in charge shall identify and secure witnesses to crimes, interview them at the scene, if applicable, and process them according to departmental regulations.

Procedure:

The initial responding officer(s) should	
a	Interview any witnesses at the scene separately to best use their reported experiences to benefit the overall investigation.
b	Transport each witness to the police station separately from other witnesses or suspects.
c	Obtain written/recorded statements from each witness at the police station.
d	When possible, the following tasks should be performed by the Supervising Officer: <ul style="list-style-type: none">• Establish the status and locations of each victim and suspect.• Establish the status of bulletins that have been broadcast regarding each victim and suspect. Ensure that any necessary missing suspect alerts are broadcast promptly.

Table 11 - Procedure for Managing Witnesses

Summary: The timely separate interviewing of witnesses is important to obtain information about any crime.

3.9 Conduct Scene Assessment

Principle: Assessment of the scene by the investigator(s) in charge allows for the determination of the type of incident to be investigated and the level of investigation to be conducted.

Policy: The investigator(s) in charge shall identify specific responsibilities, share preliminary information, and develop investigative plans in accordance with departmental policy, and local, state, and federal laws.

Procedure:

The initial responding officer(s) should	
a	Converse with the first responder(s) regarding observations/activities.
b	Evaluate safety issues that may affect all personnel entering the scene(s) (e.g. blood-borne pathogens, hazards).
c	Evaluate search and seizure issues to determine the necessity of obtaining consent to search, and obtain a search warrant.
d	Evaluate and establish a path of entry/exit to the scene to be utilized by authorized personnel.
e	Evaluate initial scene boundaries.
f	Determine the number/size of the scene(s) and prioritize.
g	Establish a secure area within proximity to the scene(s) for consultation and equipment staging.
h	If multiple scenes exist, establish and maintain communication with personnel at those locations.
i	Establish a secure area for temporary evidence storage by rules of evidence/chain of custody.
j	Determine and request additional investigative resources as required (e.g. personnel/specialized units, legal consultation/prosecutors, equipment).
k	Ensure continued scene integrity (e.g. document entry/exit of authorised personnel, prevent unauthorised access to the scene).
l	Ensure that witnesses to the incident are identified and separated (e.g. obtain valid ID).
m	Ensure the surrounding area is canvassed, and the results are documented. Ensure preliminary documentation/photography of the scene, injured persons, and vehicles.

Table 12 - Procedure for Conducting Scene Assessment

Summary: Scene assessment allows for the development of a plan for the co-ordinated identification, collection, and preservation of physical evidence and identification of witnesses. It also allows for the exchange of information among law enforcement personnel and the development of investigative strategies.

3.10. Boundaries: Identify, Establish, Protect and Secure

Principle: Defining and controlling boundaries provides a means for protecting and securing the crime scene(s). The number of crime scenes and their boundaries are determined by their location(s) and the type

of crime. Boundaries are established beyond the initial scope of the crime scene(s) with the understanding that the boundaries can be reduced in size if necessary but cannot be as easily expanded.

Policy: The initial responding officer(s) at the scene shall conduct an initial assessment of the extent of the crime scene(s) and then establish and control its boundaries.

Procedure:

The initial responding officer(s) should	
a	Establish boundaries of the scene(s), starting at the focal point and extending outward to include: <ul style="list-style-type: none"> • Where the crime occurred. • Potential points and paths of exit and entry of suspects and witnesses. • Places where the victim/evidence may have been moved (be aware of trace and impression evidence while assessing the scene).
b	Secure the scene. Set up physical barriers (e.g. ropes, cones, crime scene barrier tape, available vehicles, personnel, other equipment) or use existing boundaries (e.g. doors, walls, gates).
c	Document the entry/exit of all people entering and leaving the scene, once boundaries have been established.
d	Protect the scene. Control the flow of personnel and animals entering and leaving the scene to maintain the integrity of the scene.
e	Institute measures to preserve/protect evidence that may be lost or compromised (e.g. protect from the elements (rain, snow, wind) and footsteps, tire tracks, sprinklers).
f	Document the original location of the victim or any objects that you observe being moved.
g	Consider search and seizure issues to determine the necessity of obtaining consent to search, and obtaining a search warrant.

Table 13 - Boundaries Procedure: Identify, Establish, Protect and Secure

Note: Persons should NOT smoke, use the telephone or bathroom, eat or drink, move any items from the scene including weapons (unless necessary for the safety and well-being of persons at the scene), adjust the thermostat or open windows or doors (maintain scene as found), touch anything unnecessarily (note and document any items moved), reposition moved items within the established boundaries of the scene. Do not allow a suspect to use bathroom facilities, or to alter his/her appearance, including brushing hair or washing hands.

Summary: Establishing boundaries is a critical aspect of controlling the integrity of evidentiary material.

3.11 Conduct Scene Walk-Through and Initial Documentation

Principle: The scene walk-through provides an overview of the entire scene, identifies any threats to scene integrity, and ensures the protection of physical evidence. Written and photographic documentation provides a permanent record. A walk-through should only be completed if there will be no disturbance of the evidence. There may be the need for the immediate documentation and collection of evidence before the walk through.

Policy: The investigator(s) in charge shall conduct a walk-through of the scene. The walk-through shall be conducted with individuals responsible for processing the scene.

Procedure:

The initial responding officer(s) should	
a	Avoid contaminating the scene by using the established path of entry.
b	Consider whether personal protective equipment (PPE) should be used.
c	Prepare preliminary documentation (e.g. notes, rough sketches) of the scene as observed.
d	Identify and protect fragile and perishable evidence (e.g. consider climatic conditions, crowds/hostile environment). Ensure all evidence that may be compromised is immediately documented, photographed, and collected.
e	When involved in the initial walkthrough, note the condition of the scene. Record relevant observations, which may include things such as: <ul style="list-style-type: none"> • Outdoor fixtures such as lamp posts, sign posts, and benches. • Entrances and exits from surrounding buildings and local environmental conditions. • The crash site: is there any damage to localized buildings or environment. • Street lights: on or off? If on, which lights were on? • Weather conditions: time of day, local weather, wind speed etc. • Ground conditions. • Exterior lighting conditions. • Odours: cigarette smoke, gas, powder, perfume, etc. • Description of the perpetrator (when present). • Description of crime-related people present. • Description of emergency medical or search-and-rescue personnel present. • Weapons observed. • Furniture present, including location relative to the victim, and overall scene. • Develop a general theory of the crime.

Table 14 - Procedure for Conducting Scene Walk-Through and Initial Documentation

Summary: Conducting a scene walk-through provides the investigator(s) in charge with an overview of the entire scene. The walk-through provides the first opportunity to identify valuable and fragile evidence, and

determine initial investigative procedures, providing for a systematic examination and documentation of the scene. Written and photographic documentation records the condition of the scene as first observed, providing an important permanent record.

3.12 Note-Taking and Logs

Principle: Note-taking and logs provide a permanent record of crime scene activities.

Policy: All personnel assigned to the crime scene investigation shall maintain notes and logs of their activities.

Procedure: Detailed entry/exit logs should be created. An entry/exit log is used to document the people who come to and go from a crime scene during the investigation. People who were at the crime scene before the investigation began are also noted in this log.

The initial responding officer(s) should	
a	The officer who is monitoring the log, the “Log Officer,” is assigned the task by the Supervising Officer and is responsible for completing this task and monitoring the log at all times. The Log Officer is responsible for ensuring that the log is filled out thoroughly, and that anyone entering the scene has a stated purpose there.
b	<p>Position the log so that it is clearly visible. Set up the log for people to use when arriving to and departing from the scene. Record the following information about the crime scene:</p> <ul style="list-style-type: none"> • Crime scene location. • Name of witnesses. • Name of victims. • Name of persons taken into custody. • Name of first responders and approximate arrival times. • Name of Supervising Officer and approximate arrival time (approximate time should be used if arrival time was before the log was established).
c	<p>Record the information listed below for each person at the scene. If not using an official log book or forms, leave spaces where this information can be recorded:</p> <ul style="list-style-type: none"> • Arrival date. • Time of arrival. • Name. • Identification and Unit numbers. • Organization (if not with the investigating department). • Reason for being at the scene (log information should include the arrival and departure times of all personnel at the crime scene, including the Coroner or Digital Forensic Specialist or other essential personnel). • Information about who is at the crime scene and why they are there; incident number; first responder names, Log Officer and Supervising Officer

names, shield numbers, unit numbers, location of crime scene, name of victims, suspects, witnesses etc.

- Before making it available to crime scene visitors, record logistical data (time, crime scene location, names of victims, suspects, and witnesses etc.) in the entry/exit log.
- Ensure that the departure time for any person departing from the scene is recorded before that person actually leaves.
- If someone exits the scene without reporting to the Log Officer, that officer can enter an estimated departure time along with a note stating the rationale for it being estimated.
- Store the log in a secure location, and as mandated by departmental regulations.

Table 15 - Note-Taking and Logs Procedure

Summary: Note-taking and an entry/exit log record the persons present at a crime scene for investigative and prosecutorial purposes.

3.13 Drone Seizure

The following guidance is provided to ensure that the majority of UAV seizures are conducted following recognized best practice.

Prior to any interaction, where possible take steps to identify the make and model of the UAV and complete research so that you are informed of the capability of the device that you have encountered, and the respective data storage locations and digital intelligence or evidential opportunities available. Prior to any interaction with the user or the UAV device, consider how to achieve the best evidence for the offence that you have witnessed occur or that you have been called to respond to.

If, having completed this step, you believe there is a benefit in seizing the UAV device and you wish to do so then this should be completed following the steps below:

Drone Seizure Process	
1	Consider wet forensic (DNA and Fingerprint) opportunities prior to any physical interaction with the UAV and RC. Ensure all handling of the devices is mindful of the preservation of such opportunities when considering seizure and packaging options. For example, wear gloves, consider wet forensic hot spots (power buttons, cable areas, joysticks etc), and package carefully.
2	Rapidly consider the proximity of connected or associated devices that the UAV may be connected with or being controlled by. Most UAVs have a short control range and so controllers/antennae are usually within close proximity. Attempt to locate the pilot.
3	If possible, approach the drone from behind and obscure any cameras to prevent the drone pilot seeing you approach. Assess whether the device is on (usually indicated by lights or noise on the unit) or off. Document the power state of the device and whether or not you have witnessed it powered on since arrival. If the device is on, review and record any information instantly available on any of its screens. Disable

	the flying ability of the device (using a non-tampering measure - such as putting a coat or net over the device, or tipping it over), until confident on how to safely shut down the specific drone make/model without causing data corruption.
4	Record key identifiers of the UAV including the make, model, and serial number of the device. Identifiers may appear in different locations depending on the model being handled. Some UAVs have QR codes which can be scanned to facilitate identification.
5	If the UAV has a removable battery, remove this from the device. If there is a non-removable battery, power down the device by pressing the power button once, then pressing again and holding for two seconds (for DJI models), or switch to 'off' (depending on the model). Record the time at which any one of these steps is completed. CAUTION – If battery has any signs of damage or leakage do not remove or tamper as the battery could cause injury or explosion.
6	Record any readily identifiable modifications to the UAV, or additional solutions and payloads which may offer additional functionality, located on the device/in the proximity of the device.
7	Package the UAV and RC independently in separate faraday enclosures/bags to prevent over the air contamination and remote wiping. Package additional connected/associated devices in separate faraday bags, but record that they were found in proximity. Devices linked but located separately/a distance from the device should be treated as independent exhibits and packaged accordingly.

Table 16 - Drone Seizure Process


It is crucial that the drone and associated equipment should be recovered with minimal data loss to ensure that the potential for historical data and user identification is maximized. To aid first responders at a drone incident, INTERPOL has created a UAV First Responder Scene Log that enables the first responder to record and document the offence and the associated events - See Appendix C.

When attending a drone incident, it is crucial that the following aspects are taken into consideration.



Your first priority is safety of you, other emergency services and the public.

Upon arrival at the scene you must assess the scene and ensure that nobody is at risk from injury or death. When considering approaching the drone you have to decide, why is the drone there?



- Did it crash or did it land on its own?
- Can you identify the intended target?
- Can you locate the pilot of the drone?
- Does the drone have a payload, if so is there an associated risk such as IED or Biohazard?





REMEMBER



Drones can be wiped remotely. Disable power or isolate from outside signals if possible. Damaged batteries may leak battery acid or catch fire.

Wet forensics (Biological, DNA, Fingerprint, etc) are often the best source for the identification of an individual.
Handle all evidence with gloves to preserve this evidence.

If the drone has a payload – is it a BIO hazard or IED hazard?

Do not forget to try to locate the pilot. Drones are generally controlled by other devices – i.e. remote controller, phone, tablet – locate these devices and isolate from the network.

Figure 20: Precautions before Approaching a Drone at an Incident

Once the on-scene assessment has taken place and you are confident that there is no risk to you, other emergency service personnel or the public, you can consider approaching the drone.

When approaching the drone, if you can approach the drone from behind so that the drone pilot cannot see you approach the drone through a camera feed, then do so.

The main hazards will be from the drone propellers if they are still rotating. If the drone is still on, it may suddenly try to take off when you approach. To ensure this does not happen, you can either cover the drone with a heavy jacket or blanket so as to prevent the drone taking off, or you can just tip the drone over which will impede its ability to take off.

Your priority here is to secure the scene and any possible digital evidence that may assist in identifying the individual responsible for this incident.

Drone Hazards
<p>Propellers – If still rotating, place blanket or heavy jacket over drone to prevent drone from taking off and injury to personnel. If propellers are not rotating either turn drone over or remove propellers to prevent the drone from taking off.</p>
<p>Batteries – Drones are powered by LiPo batteries that can become unstable if damaged or are not handled correctly. If battery is still intact and no visible sign of damage or leakage then remove battery if you are able and confident to do so. If in doubt seek advice.</p>

Table 17 - Drone Hazards

SAFETY FIRST

Drones pose a unique set of safety hazards for first responders

- If the drone is still powered on, the rotors can spin and the propellers can cause damage to an individual who attempts to handle the device.
- If a device is powered on and the rotors are spinning, attempt to disable the device by throwing a large mesh or heavy blanket on top of the device to prevent it from taking off, and to disable the rotors.
- LiPo batteries used to power drones can be highly unstable and any impact or exposure to liquids may cause a fire or explosion.
- Payloads may potentially be dangerous or hazardous to those who come into contact or in the vicinity.
- When handling or approaching a drone at a scene, safety should be the number one concern.



Figure 21: Safety Precautions When Handling a Drone

The main hazards on drones are the propellers and the LiPo batteries that power the drone. Each of these elements require special handling to ensure you do not put yourself or others at risk from harm.

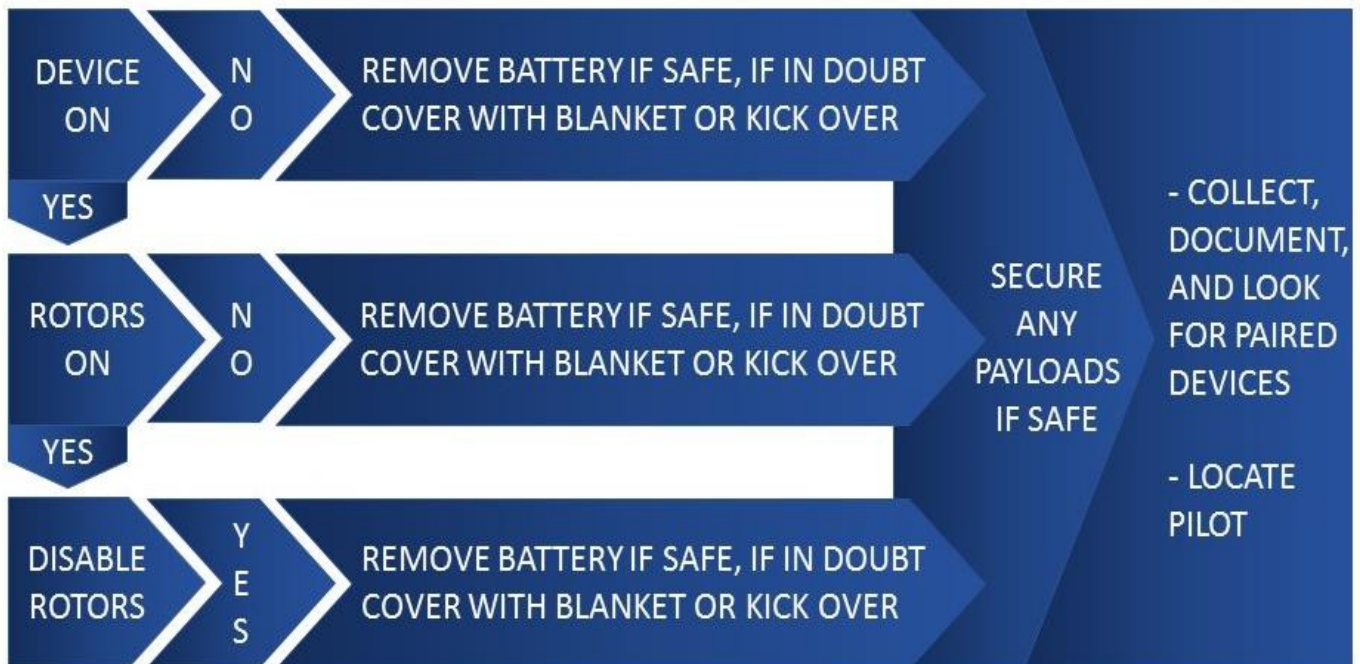


Figure 22: Drone Handling Flowchart

SAFETY FIRST

Drones pose a unique set of safety hazards for first responders



- Once the rotors have stopped spinning, remove the battery from the device (if safe to do so) or flip the device upside down
- Only remove the battery if there is no sign of damage or compromised cells to the battery. Handling a damaged batter may result in serious burns or injury.
- Once a battery is removed, store in a dry separate container or a [LiPo](#) transportation container.
- Damaged batteries can be very unstable, and any moisture or impact may cause the cell to rupture Or ignite.
- Once device is disabled from flight, consider removing the propellers if safe to do s

Document the times when any of the above are conducted



Figure 23: LiPo Battery Safety Warning

PRESERVATION

PRESERVE ANY DIGITAL EVIDENCE THAT MAY RESIDE ON THE DEVICE.

THE DEVICE MAY STORE DATA ON AN SD CARD OR INTERNAL CHIP ON THE MOTHERBOARD INSIDE THE DEVICE. IT IS IMPORTANT TO KEEP THE DEVICE AS INTACT AS POSSIBLE.

WHEN PACKAGING AND TRANSPORTING, KEEP SAFE FROM IMPACT AND SHOCK DAMAGE. IF ANY DAMAGE IS INFLICTED PRIOR TO OR POST SEIZING - DOCUMENT.

CONSULT DIGITAL FORENSIC EXAMINERS FOR PRESERVATION, HANDLING, AND TRANSPORT OF ANY OTHER ELECTRONIC DEVICES BEING SEIZED.

IF IN DOUBT, SEEK GUIDANCE FROM TRAINED PERSONNEL.



Figure 24: Preservation of Digital Evidence

COLLECTION

TAKE EVERYTHING

DRONES GENERALLY REQUIRE OTHER DEVICES TO CONTROL AND VIEW THEIR CONTENT, SUCH AS: CONTROLLERS, MOBILE PHONES, FPV GOGGLES, TABLETS, LAPTOPS, ETC.

- Data of evidentiary value may be found on the drone, controller, mobile devices, computer, and cloud for each drone.
- Collect any device that may have been paired with the drone (controllers, mobile phones, laptops, computers, memory cards, USB sticks etc.)
- When collecting associated equipment especially controllers and mobile phone – SWITCH OFF. This is to prevent remote wiping of data and prevent data loss.



IF IN DOUBT SEEK ADVICE

Figure 25: Collection of Digital Evidence

DOCUMENT

Note the state of the drone when found

- Is it ON/OFF?
- Are the propellers still rotating?
- Are the drone indication lights flashing or on?
- Is there a payload?
- Can you identify the intended target?
- Is there any damage or indication of why the drone crashed?
- Can you identify the pilot or associated suspects?

What are the drone identifiers?

- Serial Numbers (drone, batteries), Model Numbers, Aviation Authority Serial Numbers.



PHOTOGRAPH:

- ALL PARTS OF THE DRONE AND SURROUNDING AREA.
- ANY DAMAGE OR MODIFICATIONS TO THE DRONE.
- ANY ASSOCIATED EQUIPMENT THAT IS FOUND.
- IF ASSOCIATE EQUIPMENT IS ON, PHOTOGRAPH THE DISPLAY AND LOG DATE AND TIMES.

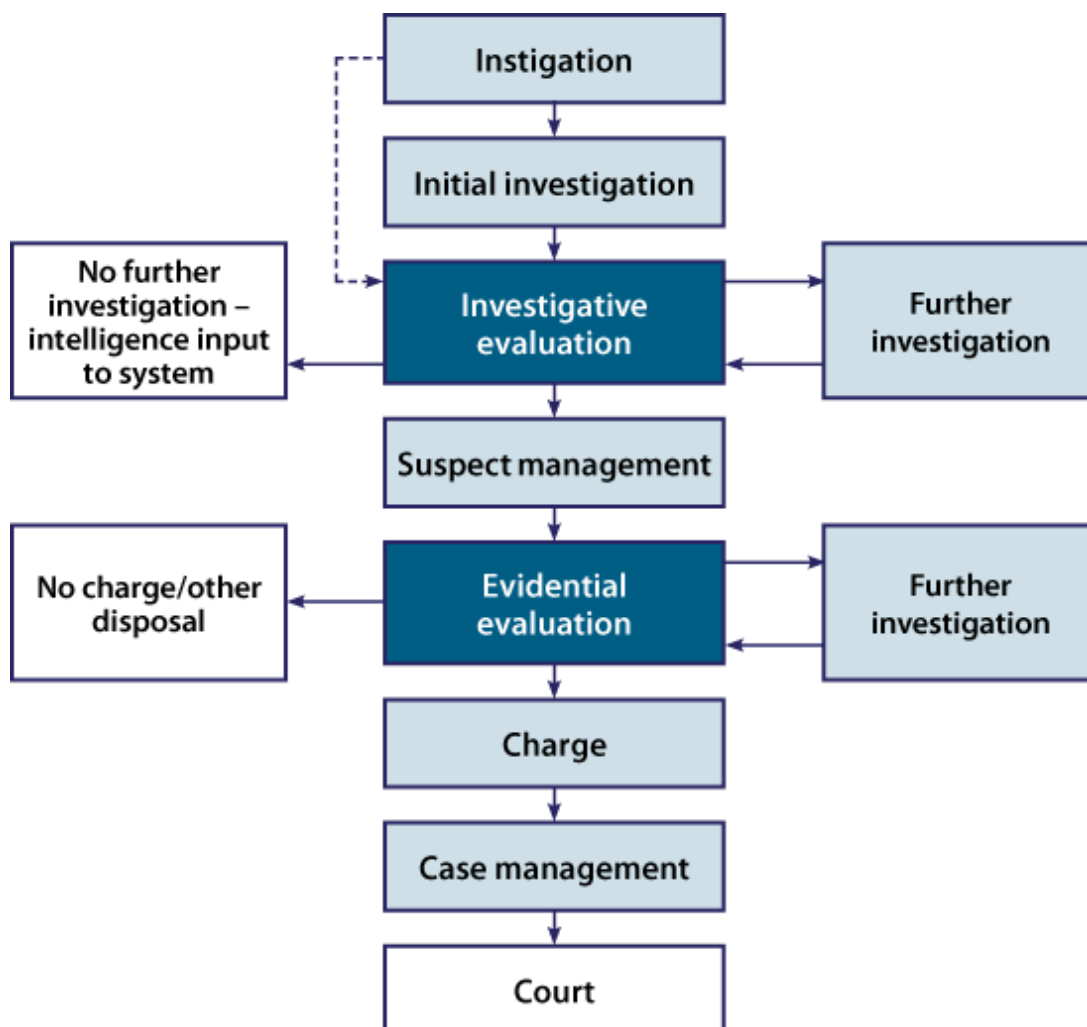
Figure 26: Documentation at Incident Scene

3.14 Process of Investigation

Once the crime scene has been analysed and all appropriate actions have been taken at the scene, the focus of the investigation will shift from the response, to the need to prove who, why, where, and when, which will help prove the reasons and identify the suspects behind the incident.

The type of activity investigators engage in and the material gathered varies depending on whether investigations use the reactive or proactive method. However, they all go through similar stages, as shown in the Investigation Process Overview diagram below.

Every investigation is different and hence may require a different route through the process. For example, in some cases the identity of the offender is known from the outset, and the investigation quickly enters the suspect management phase. In others, the identity of the offender may never be known, or is discovered only after further investigation.



Light blue sections represent activities from investigative strategies, the dark blue sections represent the main decision points and the white sections are the outcomes that can be achieved.

Figure 27: Investigation Process Overview

The initial investigation phase is concluded when some actions have been completed. These include:

- First responder or investigator obtaining an account from the victim and any witnesses who are immediately available.
- Immediate needs of the victims and witnesses have been met.
- A crime scene examination has been instigated.
- All fast track actions indicated by the material on hand have been taken.
- All records required under local policy have been completed and reviewed.
- All intelligence gathered during the initial investigation has been submitted.

Force policy guides call takers, public counter staff, and patrol officers on the information that they need to gather, and subsequent action to take. When receiving reports, staff should ensure that they record, retain and reveal all material, and pass it to the investigating officer. Investigators should be familiar with the investigative strategies relating to victims and witnesses, as this enables them to exploit early opportunities to gather material by questioning the person reporting the crime.

Comprehensive records are required to be completed, as this enhances the overall investigation by:

- Assisting the investigator in carrying out an investigative evaluation.
- Contributing to the intelligence picture of the crime areas.
- Enabling supervisors to assess the quality of the investigation.
- Facilitating the handover of the investigation if it is allocated to another investigator.

3.14.1 Further Investigation

When a crime is allocated for further investigation, investigators should develop a clear plan for how they intend to bring the investigation to a successful conclusion. The investigation plan should be based on a rigorous evaluation of the material that has been gathered to date, and should include the following factors:

Three Considerations for Further Investigations
• The specific objectives of the investigation.
• The investigative strategies to be employed to achieve those objectives.
• Resource requirements of the investigation, such as: investigator, crime scene examiner, digital forensic specialist, and intelligence analyst.

Table 18 - Three Considerations for Further Investigations

The above considerations are not exhaustive, but they are meant to guide the investigator. This framework is not intended to cover investigative strategies, as this is beyond the scope of this document.

As you can see from the Investigation Process Overview diagram, thus far this framework has covered the initial investigation and evaluation stages. The following sections will cover the evidential evaluation and associated processes that will assist a drone incident investigation. The next section of the framework will detail the digital forensic strategy and processes for drone data analysis to enable first responders and digital forensics practitioners to understand the digital forensic process.

4. Digital Forensics Overview and Principles

4.1 Overview

Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital device or other digital storage media. The goal of digital forensics is to extract data from electronic evidence, process the data into useful information, and present the findings in court. All processes involved therefore shall utilize sound forensic techniques to ensure that all findings are admissible in court.

The aim of carrying out digital forensics on drones and associated equipment is to identify flightpaths, user data, and associated pictures and videos contained within the devices that will assist in understanding the drone and its usage.

The nature of the cases in which digital evidence is involved are generally borderless and happen in split seconds. Hence the findings derived from electronic evidence must follow a standard set of guidelines to ensure that it is admissible not only in a specific country's court of law, but also in the international criminal justice system.

The following chapters will outline best practice for handling UAV devices - applicable across the existing range of recreational, commercial and bespoke devices and flight controller systems. Each chapter will contain its own relevant content, including clear and concise step-by-step guidance on the legislation and offences that govern UAVs. In addition, it includes a section that outlines how to manage and preserve the integrity of a UAV device from the first point of contact through to triage or forensic examination.

It is crucial for a digital investigator to understand that whilst digital intelligence and evidential opportunity must be treated differently, the overarching principles of digital intelligence and evidence apply throughout the case management process, from the initial seizure through to the court stage.

4.2 Principles of Electronic Evidence



Figure 28: Digital Forensic Examiners Examining a Drone

When dealing with electronic evidence, one must ensure that the following principles are adhered to:

Digital Evidence Principles	
Principle 1	Electronic evidence shall be obtained in a legal manner.
Principle 2	Staff involved with examining electronic evidence shall receive an appropriate training program prior to handling electronic evidence.
Principle 3	All actions taken on the electronic evidence shall not change its data. If there is a need to access the original data or change the system setting, it is recommended that only competent staff to do so, and that staff must be able to justify those actions.
Principle 4	A record of all actions taken when handling electronic evidence shall be created and preserved so that they can be audited. An independent third party should be able to repeat those actions and achieve the same result.

Table 19 - Basic Digital Evidence Principles

Therefore, the seizure of the drone and associated equipment is crucial to ensure the maximum exploitation of digital evidence is possible.

4.3 Digital Forensic Lab Overview

When the drone and associated equipment is submitted to a DFL then the lab should have an established procedure for case management. Generally, there are seven steps in managing a case as is illustrated in the following figure and further explained in the subsequent sections. Prior to conducting a case, the DFL shall ensure that it is following and complying with the legislation. The manager or the examiner shall ensure that permission for processing the evidence exists through warrants or official documents. The goal of conducting Digital Forensics work is to use evidence to prove or disprove disputed facts, hence electronic evidence must be obtained in compliance with the legislation. At the end of the Digital Forensics work, it must be ensured that the electronic evidence is admissible and the forensic report is acceptable in court.



Figure 29: Digital Forensic Lab Process

4.3.1 Receive Request

The DFL work starts upon receiving a formal request from a requestor. This formal request can come in the form of a letter, email or fax. The information supplied in the formal request include the crime involved, the related act, electronic evidence details, the case objective and possibly the warrant.

The lab manager or appointed staff shall then review the request and determine whether the case is feasible, based on the following criteria:

- a. The case is within the scope of digital forensics, i.e. the evidence is related to electronic evidence and not otherwise - such as DNA and fingerprint
- b. Method and tools are available
- c. Staff is available to conduct the case
- d. The legal requirement is fulfilled

The DFL shall then respond to this request formally whether or not they accept the case. If the decision is to accept, the DFL shall provide a date for delivery of the electronic evidence to the requestor.

4.3.2 Register Case

Once the DFL decides that the case is feasible, the requestor shall come to the DFL with the electronic evidence. The DFL shall create a unique running case number for that case and fill out a case registration form.

In order to effectively examine electronic evidence, examiners need to be supplied with a clear and specific case request by the requestor. Due to large and various types of data in a device such as documents, videos, communications, health monitoring data, locations, etc., it is impossible for an examiner to examine data in a digital device without a clear and specific request.

Based on that information the Examiner can plan the methods and tools to be used to process the evidence.

Both parties, the requestor and the DFL staff, shall sign the form. The work has now officially commenced. Next the DFL shall create a folder in a storage media to store all logical data related to the case in this folder.

4.3.3 Register Exhibit

When electronic evidence (exhibit) is received, it is important that the exhibit is sealed before it can transfer custody to the DFL. To eliminate any reasonable doubt on the integrity of the evidence, both the requestor and the examiner must be able to demonstrate that no one else has gained access to the evidence during the process of transfer from one party to another. Although this practice is new and costly for some agencies, the DFL will nevertheless provide constant awareness and provide a firm timeline to start practicing this procedure with the agencies.

Each piece of electronic evidence that is submitted, shall be registered and assigned a unique exhibit label which is documented with the exhibit's details in the registration form.

This registration includes each exhibit's sub-items such as sim cards and memory cards. The labels shall be able to track the sub-items to the parent item. For example, should a mobile phone is labeled as 20190105(2)-MP01, then the sim card may be labeled as 20190105(2)-MP01-SIM01.

It is important to note that any defects on the exhibit must be documented in the exhibit registration form. This is to protect the DFL from any negative claims in the future.

Any forms of softcopy related to the exhibit shall be uploaded to the case folder.

Now the chain of custody of the exhibits has started, and the form shall be filled in by the staff receiving the exhibit.

4.3.4 Photograph Exhibit

A photograph of the exhibit is conducted for the following reasons; to record the state of the exhibit and to effectively identify the exhibit in future. Photograph the overall view of the exhibit as well as the close-up view. If the screen is active, photograph its screen display also. The pictures shall then be uploaded to the case folder. It is advisable that the exhibit is photographed before returning it back to the requestor as a future reference of its conditions.

4.3.5 Conduct Analysis

The analysis shall be conducted in accordance to the DFL Analysis Model. Refer to Section 5 for the details of conducting the analysis. During the process, Examiners shall maintain communication with the requestor and communicate any deviations or limitations that may arise during the examination. Some examiners have years of knowledge in digital forensics, and so they are able to allocate the right data when effective communications between examiners and requestor take place.

4.3.6 Return Exhibit

Once the analysis has been completed, the DFL shall contact the requestor to pick up the evidence. Common practice in the DFL, is to return the exhibit along with the forensic report to the requestor to save traveling time. Before returning the exhibit, the DFL must seal it. The seal shall have the staff's initial, the exhibit's label and the date and time it has been sealed.

4.3.7 Close Case

After this, the process is complete and the DFL can close the case. To close the case, both parties shall agree that the work is complete and the report has been delivered to the requestor. This can be done by signing a form.

5. Drone Digital Forensics

In this section we shall look at the digital forensic process for drones and drone controllers. If there are associated devices such as laptops, mobile phones or tablets this examination process is covered in the INTERPOL Global Guidelines for Digital Forensics Laboratories.

5.1 Overview

This chapter covers the procedure for conducting digital forensic analysis on drone-related electronic evidence in digital forensics lab (DFL). A chronological process model is presented to provide a comprehensive overview of the main processes involved in drone digital forensics.

There are typically four phases involved in the analysis of electronic evidence in the DFL: acquisition, examination, analysis, and presentation. Throughout the process, the chain of custody of the evidence must

always be updated whenever it changes hands and its integrity must be secured at all times. Examination and analysis phases may be repeated until the work satisfies the case request.

It is commonly understood that conducting digital forensics work generally involves these four phases, however, not all cases will require all the phases. In certain cases, the acquisition phase can be skipped in order to conduct triage straight away during the examination phase. An example of such a case is when there are large sets of data, and hence conducting acquisition on each item of evidence may be not feasible.

The following figure shows the laboratory analysis model:

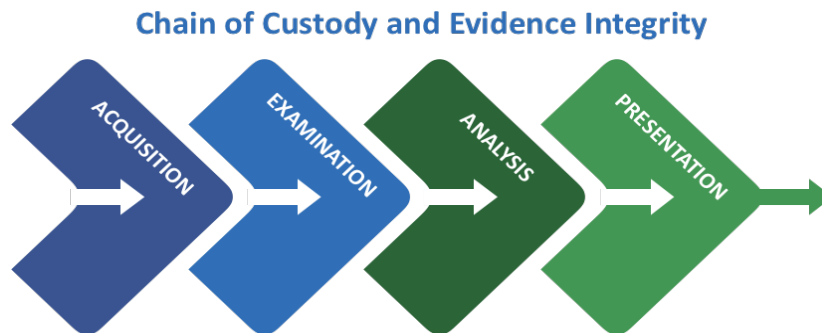


Figure 30: Digital Forensics Laboratory Analysis Model

5.1.1 Drone Devices

The next section of this document will explain in detail each phase involved in the DFL Laboratory Analysis Model. This document explains the process of conducting acquisition, examination, and analysis on two types of devices:

- (I) Drones
- (II) Drone Remote Controllers (RC)

As identified in Section 2.5 of this document, there are several different types of drone data, which are stored on different data storage mediums, including the drone itself, removable storage mediums, mobiles devices, the cloud, and so on. It has been seen that there is sometimes residual data held on the drone RC. If necessary, the examiner should try to recover data from the RC. This data could include:

Types of Data held on Drone Remote Controllers	
Telemetry	This data will hold data related to the drones flights such as GPS, time and date (from GPS signal), velocity, direction, altitude, motor speeds, and user inputs.
Associated Devices	Any devices that have been paired or connected to the controller such as mobile handset or tablet. This may be the IMEI of the handset or unique hardware ID of the device.
Registered User Accounts	The user account may be a registered email address or registered account name that has been created with the drone manufacturer.

Communication Signal Parameters Between Drone and RC	These logs should contain signalling data which logs the signal strength between the drone and the RC
---	---

Table 20 - Types of Data held on Drone Remote Controllers

For specific guidance on digital forensic analysis of other drone-associated devices, such as mobile phones and computers, please refer to the INTERPOL Global Guidelines for Digital Forensic Laboratories.

5.2 Acquisition

Acquisition or, as it is better known, data acquisition, is the process of creating a forensic copy of the electronic evidence (exhibit) such as the drone, controller, mobile phone, or laptop, in the form of an image file or files. The image file/s will then be used in the analysis phase. The acquisition is made in order to preserve the integrity of the electronic evidence. It is to produce an identical copy of the data without changing the content of the electronic evidence in any way. It is good practice to create two copies – one to keep as the master file, and one to use for forensic analysis.

Electronic evidence needs to be acquired in a forensically sound manner. The intangible nature of data and information stored in electronic form makes it easy to manipulate and more prone to alteration than traditional forms of evidence. It is therefore important to have a defined and tested acquisition procedure.

Once an image file has been created, both the hash value of the exhibit and the image file must be recorded. Hashing is used to prove that the image file is exactly the same as the content of the exhibit. There are many hashing algorithms used in digital forensics, such as Sha-256. Most forensic software and hardware offer the hash-generating feature.

Examination and analysis must only be done on a forensic copy of the original evidence, unless circumstances prevent examiners from doing so. This is important in order to preserve the integrity of the evidence. The forensic copy of the electronic evidence must be stored on other storage media, never on the evidence itself. The forensic copy must be clearly labelled to ensure it is not mixed up with the original evidence or with forensic copies from other cases. The digital forensic laboratory must therefore prepare some storage media before receiving cases.

The following gives details of data extraction on drones. The extraction method is very similar to mobile phones, as there are commonalities between drone and mobile phone examinations.

5.2.1 Types of Data Extraction

Before commencing the digital forensic work, the examiner must review the case paperwork obtained from the requester in order to ascertain the types of data required from the exhibit. This can assist the examiner in deciding the best extraction method for the case.

There are four different levels of data extraction for drones, which are described below starting with the level where most data can be extracted, and ranging down to the level where the least data can be extracted.



Figure 31: Drone undergoing Examination

a) Physical Extraction

A physical extraction is the acquisition of raw binary data from the media storage of the device. This raw data then needs to be analysed and processed at a later stage by forensic software. This method typically allows the examiner to access live and deleted data, operating system files and areas of the device that are not normally accessible to the user.

b) File System Dump (FSD)

The File System Dump (FSD) is a hybrid of physical extraction and logical extraction. FSD retrieves the device's file system and interprets the data during the processing stage. This allows the examiner to retrieve, for example, databases holding deleted telematics/media data that may not be available at a logical extraction and may not be accessible during a physical extraction. However, a limitation of FSD is that it does not retrieve all deleted data the way a physical extraction is able to do.

c) Logical Extraction

Logical extraction involves receiving information from the drone and allowing the device to present the data for analysis. This is often the equivalent of accessing the data on the device itself. This method makes only live data available to the examiner. Most drone device forensic software offers this type of feature if the data is not contained on a removable media card. The issue with logical extractions is that there is no way of verifying the data on the drone itself as most drones do not have displays to view or examine the data contained within the drone.

d) Chip-Off

For drones that have on-board memory or are damaged, Chip-Off methods can be used to extract the data. Chip-Off also allows the extraction of raw binary data from the device's storage, but it requires the permanent removal of the device's memory chip from the memory board. When the examiner conducts Chip-Off, the device could potentially be damaged and can no longer be used. In addition, expectations on the use of Chip-Off for drones must be moderated. Recent devices store encrypted data on their memory chip.

Regarding drone remote controllers, the examiner will need to identify the memory chip on the remote controller board and acquire the data using USB connection, JTAG, or chip-off methods. There may also be removable media cards used in the remote controller and these should be treated the same as any normal removable media.

The order of attempted extractions is important. Examiners should strive to conduct the examination method that is least destructive but yields the most data. This allows examiners to capture areas that might be damaged or overwritten at later stages. Methods of extraction such as Chip-Off should only be considered as a last resort, especially with Chip-Off, as the process can be destructive and unrecoverable.

The use of JTAG to recover data from drones has been seen to cause issues especially with popular makes of drones. This method should be tested on a test device before utilizing on the evidential exhibit, because this may brick the microcontroller and prevent the examiner from any data recovery from this module.

5.2.2 Extraction Tools

Analysis of drones typically requires the use of dedicated software, power cables and data cables. More advanced examination techniques, such as Chip-Off, require further tools. These include desoldering/reballing equipment, and specialist jigs to read raw data from the device's memory chips. Also, when examining drones, it may be necessary to use manufacturer software suits, even those these are not considered forensic software, if these are the only acquisition avenues available to the examiner to acquire the data.

5.2.3 Extraction File Format

Due to the requirement to use dedicated tools to extract data, drone data is often extracted in a proprietary format. These formats can often be transferred between different tools to leverage the strengths of different decoding abilities. Other non-proprietary formats include bin files and raw files.

5.2.4 Process Flow



Figure 32: Extraction Process for Drones and Drone Remote Controllers

a) Identify the Exhibit and Storage Media

The examiner observes the exhibit at hand, before proceeding to the next process.

i) Drone

The exhibit's label should be affixed to the drone, on the inside of the drone, or printed on the back of it. The label may include manufacturer, model number, serial number and connection IDs - such as WiFi Mac Address.

ii) Drone Remote Controller

The exhibit's label should be affixed on the back of the controller, or inside the battery compartment. The label should include the device make and model, serial number, and pairing ID. Also the remote

controller may use an operating systems such as Android and if this is the case then the principles of mobile device examinations should be used



Figure 33: Drone Identification Label

Next, a storage media should be prepared to store the extracted data.

b) Isolate Exhibit from Network

When conducting extraction, the device needs to be switched on.

i) Drone

To prevent any attempt to connect to a network and subsequently risk changes to any data, the exhibit needs to be isolated from a network or associated connections such as the mobile phone that was used with the exhibit.

ii) Drone Remote Controller

To prevent any attempt to connect to GPS satellites or paired devices such as the drone or associated mobile handsets which subsequently risk changes to any data, the exhibit needs to be isolated from GPS Satellites and other devices to ensure that GPS/WiFi/Network signals are not picked up and new data/files are created that will reveal the location of the digital forensics' lab.

Depending on budget, isolation can be achieved through different methods, such as:

Methods to Isolate Drones/Remote Controllers	
Network Shielded Room	A laboratory installed with Faraday shielding to prevent network signals. However this is a very expensive solution and the use of smaller Faraday bags can be considered as an effective alternative.
Wireless/Signal Jamming Equipment	This equipment blocks incoming mobile network/GPS/WiFi signals. In some jurisdictions, it is illegal to use. This will also interfere with other equipment that require WiFi/Mobile Network/GPS signals to send and receive data.
Manual Method	This is the cheapest and most easily configured method. This involves using aluminium foil placed over the drone/remote controller antennas to restrict satellite signals being received by the exhibit. This method is not fool proof as the examiner has to ensure the antennas and surrounding area of the drone/remote controller is fully covered.

It is important to note that when the drone is switched on it will initially try to receive a GPS signal to verify its position, and time and date. This data may then be used to verify authenticity of drone datasets such as No Fly Zone Database etc. Hence every time the drone is switched on this may result in a new data file being created in the drones file system, and may show up in any examination of the drone.

Table 21 - Methods to Isolate Drones/Remote Controllers

c) Extract Relevant Data

Due to some specific extraction techniques, rooting devices, and some drones/drone remote controllers utilizing software similar to mobile operating systems (particularly Android OS), it is not always possible to implement write-blocking to a drone or drone remote controller. Where possible, write-blocking should be implemented, for example on memory cards. However, it is widely acknowledged that the write-blocking method is not always possible or practical for drones/controllers. For this reason, it is imperative that the examiner is fully aware of the consequences of their actions when handling drones/controllers, and is able to explain and justify their actions.

Drones/controllers are presented with two distinct media storage types that require separate handling techniques, as in the following table:

Drone/Remote Controller Storage Media	
Media	Description
Memory Cards	These can be examined as a computer hard disk. Both logical and physical extraction can be conducted on these cards, as long as the forensic tools support this feature. The examiner has to access the card, extract the data, and then put it back into the device before switching it on. Some devices store data in the memory card, and if it detects that the card is not available, it could cause data loss from the drone/controller. If time and resources allow, a bit-to-bit clone of the memory card should be created and that clone inserted into the handset.
Internal Memory	This requires drone/mobile compatible manufacturer/forensic tools. Some devices are supported by forensic tools for a physical extraction. The forensic tools will boot the device in a particular way and conduct physical extraction without making any changes or alterations to the user data on the device.

Table 22 - Drone/Remote Controller Storage Media

Possible Data Traces held on a Drone/Remote Controller	
Artefacts that are stored on the drone/controller by default. The probability of finding such traces is high, even if a suspect tries to cover his or her tracks. Some of the discoverable traces:	
Standard Digital Exhibit Artefacts: <ul style="list-style-type: none"> • Slack space. • Unallocated space. • Thumb caches. • Log files. 	Drone Specific Artefacts: <ul style="list-style-type: none"> • Update history. • Diagnostic logs. • Registered email accounts. • Paired devices. • Multimedia files. • Flight/telematics Logs. • Drone media thumbnail caches. • Map artefacts such as geo coordinates, waypoints, and home locations. • Drone specific software such as manufacturers' drone management software. • Emails that show new registration of drones or update notifications from the manufacturer. • CSV files that contain telematics, diagnostics, or GPS coordinates.

Table 23 - Possible Data Traces held on a Drone/Remote Controller

The extraction process will vary depending on the extraction tool chosen. Most forensic tools have a guide explaining the procedure that must be followed for a successful extraction. In some cases, examining and analysing the drone/controller requires modification to the system files or the operating system in order to extract the data. This process can cause some data to be irrecoverably lost. However, it affects only the system files with little evidential value. Knowledge of what is altered by any of these processes can be gained by holding appropriate training certifications, such as training provided by the manufacturers of drone/mobile forensics software, or practical experience involving the testing of drone/mobile device extraction.

Another rich source of forensic evidence is the drone's backup, telemetry, and diagnostic files. Some drones and associated devices will create backups or copies on other devices, such as in a laptop/computer or on the cloud. These backups can assist in building a timeline of evidence, and can also be used to gain access to historical data not present on the drone. It is also possible to analyse some backups as if they were a physical device.

Due to the nature of drones/controllers, standard forensic tools may not support the extraction and analysis of data from the drone. It may be necessary to utilize off-the-shelf software to extract and analyse the data. If this is required then it is advised that adequate checks and quality assurances are completed to ensure that the data recovered is verified, and the impact on the exhibit is assessed before commencing the use of such a solution. Also, when using manufacturer-specific software, it needs to be considered that the application may send data or copies of recovered files to the manufacturer's data servers for reference.

d) Verify the Exhibit and the Extracted Data

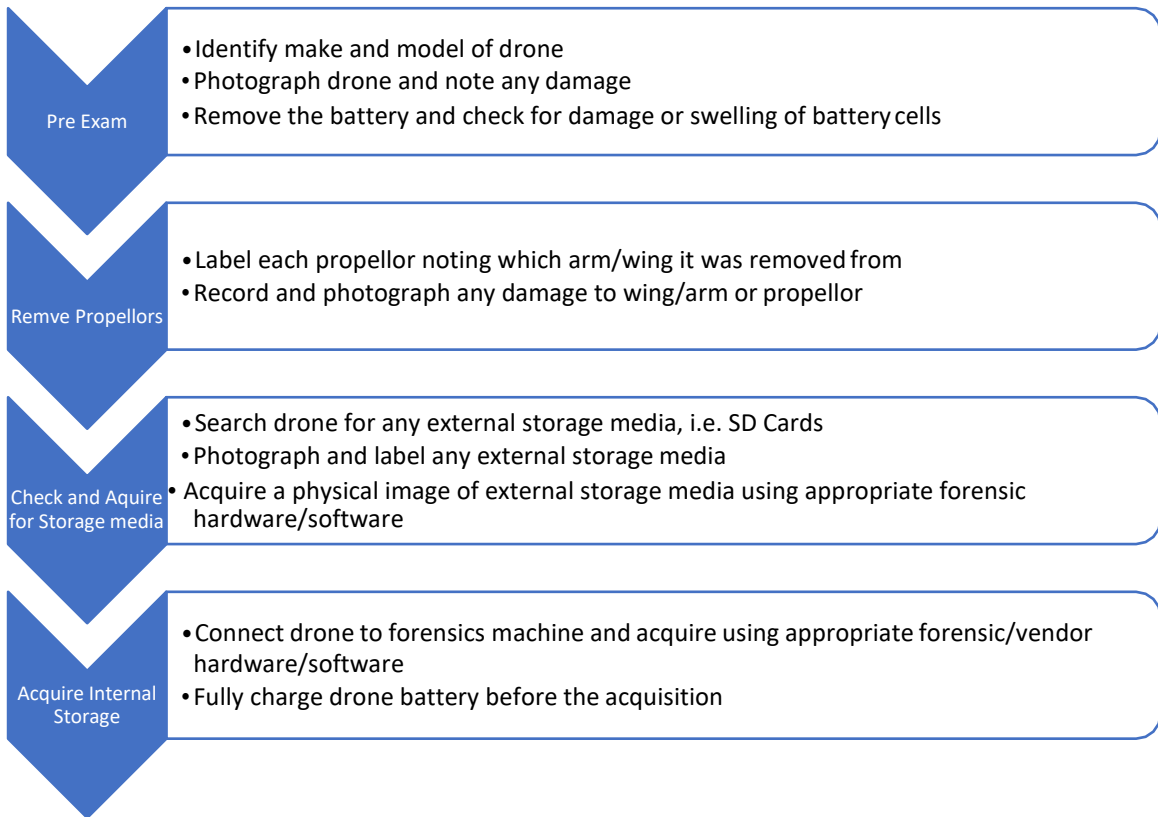
Once the data has been extracted, the examiner must verify the data collected against the data on the exhibit. Information such as date and time, geo coordinates, and user/system information must be cross-checked by the examiner, as sometimes it is converted to another format during the extraction process. Due to drones not having a user interface where the data can be verified on the device, it is recommended that if possible, the extracted data should be acquired and analysed by at least two forensics tools. This is known as dual tooling.

e) Document All Actions

The last step in a drone/remote controller data acquisition is to ensure that the process is documented. The examiner should make case notes during the acquisition, noting date and time of examiner actions, forensic and associated software utilized in the acquisition, and any errors or abnormalities that occur during the process. This is essential for chain of custody, and will also be required if the evidence is used in court. The examiner should remember that there may be a huge gap of time between acquisition, examination, analysis, and prosecution, thus notes should be as comprehensive as possible.



DRONE



Acquisition Methods

USB Cable	JTAG	ISP	CHIP OFF
<ul style="list-style-type: none">• Connect to PC• Acquire using appropriate hardware/software	<ul style="list-style-type: none">• Identify JTAG pin outs• Connect to JTAG acquisition box and retrieve data	<ul style="list-style-type: none">• Locate ISP connection points• Acquire data through appropriate method	<ul style="list-style-type: none">• Identify memory chip• Remove chip, clean and reball if required• Image using appropriate chip adaptor and programmer

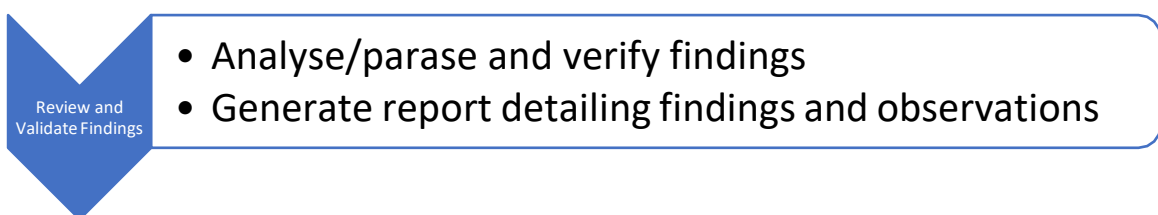
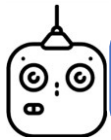


Figure 34: Drone Examination Flowchart



Controller

Pre Exam

- Identify make and model of controller
- Photograph controller and note any damage/modifications
- Remove the battery and check for damage or swelling of battery cells

Check and Acquire for Storage Media

- Search controller for any external storage media, i.e. SD Cards
- Photograph and label any external storage media
- Acquire a physical image of external storage media using appropriate forensic hardware/software

Acquire Internal Storage

- Connect controller to forensics machine and acquire using appropriate forensic/vendor hardware/software
- Fully charge controller battery before the acquisition

Acquisition Methods

USB Cable

- Connect to PC
- Acquire using appropriate hardware/software

JTAG

- Identify JTAG pin outs
- Connect to JTAG acquisition box and retrieve data

ISP

- Locate ISP connection points
- Acquire data through appropriate method

CHIP-OFF

- Identify memory chip
- Remove chip, clean and reball if required
- Image using appropriate chip adaptor and programmer

Review and Validate Findings

- Analyse/parase and verify findings
- Generate report detailing findings and observations

Figure 35: Drone Controller Examination Flowchart

5.2.5 Other Sources of Evidence

With a drone there could be many associated devices ranging from payloads, ancillary electronics, VR/FPV Goggles as well as modifications or additions to the drone. The investigator and forensic examiner should keep an open mind as to what exhibits are relevant or required to fully investigate the case.

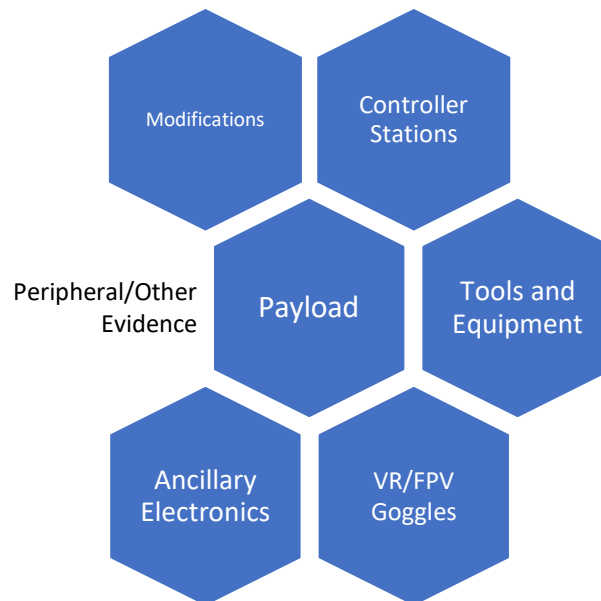


Figure 36: Other Sources of Evidence

Sometimes it has been known that the vital electronic data that is required for the investigation has resided on associated device such as a mobile handset or laptop. If you are unable to carry out full examinations of devices then at least a triage of the device and the data stored within the device should be attempted and documented.

5.3 Examination

Examination of original evidence should be avoided, where possible. The examiner must always work on the forensic copy (image file) of the evidence. If this is inevitable, access to the data must be protected using a write blocker.

In certain cases, examiners need to use an isolated environment or pre-set environment to conduct the examination. For example, conducting the simulation on a database system or gaming software. To achieve this, examiners may use virtualization technology and encapsulate the case in a working container. When the examination is complete, the examiner may revert the workstation to its previous state using a known image, or using a feature offered by the operating system.

For more information on examination methods for digital evidence, see Section 5.2 of the INTERPOL Global Guidelines for Digital Forensics Laboratories.

5.4 Analysis

5.4.1 Analysis Procedures for Digital Traces

Just as a criminal leaves physical traces behind at a crime scene, a drone utilized by a criminal to commit a crime will leave traces and indications of its locations and actions leading up to its confiscation on the drone and other associated devices.

Data and information that need to be extracted from a drone/remote controller depends on the type of case.

a) Pictures and Videos

To conduct analysis on pictures and videos, the examiner first needs to have a clear idea from the requestor of what to look for. Is the investigator looking for multimedia created on the device, or indication by analysing the pictures and videos for a criminal act? Reviewing the stored pictures and video will assist the examiner in understanding the nature of use of the drone, and also the areas that the drone has been operating in.

Analysis of pictures typically starts with signature analysis. Next, the examiner may sift through pictures in the gallery by using the thumbnail view.

For video analysis, some software offer the feature of extracting still pictures from videos. For example, Y pictures, in every X second/minute. These extracted pictures can then also be viewed in a gallery view. This allows for the much more efficient previewing of video files.

In cases where location or production details of pictures and video files are important, the examiner should consider extracting the metadata of those files. Metadata are sets of data that describe and give information about other data, for example, GPS coordinates where the picture was taken, creation date and time, as well as the device used to capture the picture. If the multimedia was taken on the drone, then there will be geo tags as this would automatically be initiated by the drone unless the user has changed the configuration of the drone.

Some exhibits may have thousands of photos and videos, and it is impossible for the examiner to sift through and locate one specific video or pictures file. The best way of doing this is by extracting all pictures and then passing them to the requestor. Also, there may be multiple copies of the same video or photograph on the drone, as these may be used to enhance user experience by utilizing thumbnails and compressed videos of the original footage.

The simple task of viewing the contents of the pictures/videos does not require any digital forensic expertise and hence could be carried out by the requestor. When the relevant photos/videos have been

identified, further analysis can be conducted by the examiner to extract more meaningful data, such as GPS coordinates and creation or modification data.

b) Flight Logs

Drone flight logs are of evidential value in many cases. They typically contain the following artifacts:

- GPS position
- Time and date
- Data parameters (i.e. rotor speed, altitude, and direction)
- Drone telematics
- Diagnostic error codes
- Associated media logs

Analysing drone flight log artifacts can be important for suggesting purpose or intent. An example is the position of the drone at a certain point, which could illustrate the drone user's intent to enter a restricted or protected airspace.

Most analysis forensic software offers flight log parsing. However, due to evolving technology where some drones are frequently being updated, some forensic software may take some time to update their database. Therefore, it is important for examiners to understand the underlying structure of flight logs. Since most drones utilize SQLite database or CSV files, the examiner may consider parsing the artifact manually by using appropriate software to display the data.

This not only allows examiners to be independent of a particular software, but also allows them to cross-check the results of the software against the flight logs.

c) Applications/Software

Although there are no standard procedures for how to analyse all artefacts due to their diversity, analysis is commonly done by conducting information gathering on reliable and trusted sources on the software artefacts or application installed. The findings can then be verified by conducting a simulation or installing the application on a test device and conducting tests to understand the functionality and data collection of the application. This will also give the examiner a better understanding of the user rights of the applications and if what registration data is required to use the app.

d) User Activity

The drone operating system tracks user activity at many different places. Examples include:

- Drone power on and shutdown times
- Drone settings
- Device usage
- User logins/accounts
- Wi-Fi/device connections
- Telematic logs

Analysing this user activity helps to get a better understanding of the user's behaviour and can even prove evidential activities. Depending on the operating system, the artefacts are stored in various files and locations.

e) Unallocated Space

Unallocated areas can contain artefacts of all of the types of evidence mentioned above. Searching and extracting certain file types in unallocated areas can be automated by using carving software. The Examiner should specify what kind of files they are searching for because data carving is a very time-consuming task. Data carving does not work well on fragmented files. Most of the time data found in unallocated areas cannot be associated with a certain user, time stamps, or even a location within a folder structure.

f) Cloud and Remote Storage

When an examiner discovers traces of cloud services in a drone, it could indicate either of the following:

- Data is stored locally on the drone and remotely on the cloud; or
- Data is stored fully on the cloud. The drone may not contain any data at all.

In fact, the data that are stored remotely may not just be stored on a single server, but can be stored on multiple servers in the cloud. Most of the time, even the provider of a cloud service cannot tell on which particular server, data-centre or in which country certain parts of the data are stored.

Although technically it is easy to make a forensic copy of the virtual machine which resides in the cloud, there are some legal matters that need to be considered. Depending on the applicable legislation, identifying and obtaining the appropriate legal authorization for intercepting such data may pose an issue. It may also be challenging to ensure that the data have been acquired in compliance with the legal procedures in the requesting country.

Another disadvantage is that there is likely to be far less recoverable data to be extracted. Indeed, if a suspect created a temporary virtual machine to commit his or her crimes and then deleted that machine, there may be no evidence at all to recover.

The possibility of acquiring and analysing remotely stored data is dependent on the legislation and jurisdiction. In some jurisdictions, for example, under certain circumstances the examiner is allowed to connect to the remote storage using the suspect's credentials from the drone in order to acquire the data. Other jurisdictions may not accept such an acquisition. In these cases, official channels can be used to request preservation and access to the data from the provider.

5.5 Presentation

The presentation phase requires putting together findings in a presentable and understandable way for stakeholders. When the analysis phase is completed, the examiner needs to put the findings and results in a forensic report. The examiner should illustrate and translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand. They may also be expected to interpret those facts, and to express an opinion on their meaning. In some cases when a large number of exhibits are analysed, it will be difficult for the examiner to present the outcome to the investigation team. It is recommended to adopt an analytic software, to facilitate matching digital evidence with other data from the investigations. This kind of tools can also be used to index and search all the exhibits, providing the investigation team with a global overview of the case.

5.5.1 Admissibility of Electronic Evidence

The criteria for the admissibility of electronic evidence may differ from jurisdiction to jurisdiction. Generally, the examiner should consider the following criteria when evaluating electronic evidence for trial:

General Criteria for the Admissibility of Electronic Evidence	
Authenticity	The evidence must establish facts in a way that cannot be disputed and be representative of its original state.
Completeness	The analysis of, or any opinion based on, the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.
Reliability	There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
Convincing	The evidence must be persuasive as to the facts it represents, and must be able to convince the stakeholder of the truth in court.
Proportionality	The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e. the level of intrusion or coercion) caused to the rights of any party should not outweigh the probative value of the evidence (i.e. its value as proof).

Table 24 - General Criteria for the Admissibility of Electronic Evidence

5.5.2 Report Writing

A forensic report must be written in clear and understandable language. The result must be properly summarized and it must also provide a concise answer to the case request, supplied by the requestor.

It is recommended that all technical details be listed in the appendix section, rather than put in with the main content. This is to facilitate the layman's understanding in reading the report.

The examiner must also refrain from providing a statement that cannot be proven. For example, "The suspect has altered File A". An appropriate sentence would be "File A found in Computer B has been altered".

Due to the complexity of the case, sometimes it is difficult for the examiner to express the findings in the report. The use of visual aids and visual representation such as animation, slides, pictures and live demonstrations are good methods of facilitating understanding.

5.5.3 *Expert Witness*

In some jurisdictions, a submitted forensic report is sufficient in court, in lieu of the examiner attending the court session. However, in other jurisdictions, the examiner is required to attend a court session and present his/her expert testimony related to the case.

An expert witness is a person who, by virtue of education, training, skill, or experience, has an expertise and specialized knowledge beyond that of the average person. The witness's knowledge is sufficient that others may officially and legally rely upon his/her specialized (scientific, technical or other) opinion about evidence or a fact within the scope of his/her expertise, referred to as the expert opinion.

In some jurisdictions, expert status is decided on each and every case by the trial judge and the person is only an expert in that case. In other jurisdictions, expert status is appointed by the legal institution, and the person is responsible for any case within his/her expertise.

The rights and duties of an expert witness differ from country to country. It is important for examiners to familiarize themselves with their legislation, their court procedures, their role and their rights and duties in that role.

For more information on ensuring the quality and admissibility of electronic evidence produced in a DFL, see Sections 6.1 and 6.2 of the INTERPOL Global Guidelines for Digital Forensics Laboratories.

6. Drone Data Examples




In the below tables we show the common locations for flight logs and multimedia of some commonly used drones currently on the market.

6.1 Flight Logs

Drone Make/Model	Data Location	File Type	Default Name
DJI Phantom 3	Internal SD	.dat	FLYXXX
DJI Phantom 4 Pro	Internal SD	.dat Two additional logs generated named 'PHARM.LOG' and 'USER.LOG'	FLYXXX
DJI MAVIC 2	INTERNAL eMMC	.dat	
YNEEX Q500 4K	SD CARD (when saved on Controller)	.csv	Remote/RemoteGPS/Telemetry
Parrot ANAFI	External SD (or iPhone when used with controller)	.bin (.json)	Log.bin (XXDate&TImeXX.json)

Table 25 - Flight Log Locations for some Popular Drones

6.2 Media File Locations

Drone Make/Model	Location	File Path	File Type	Default Name
 DJI Phantom 3				
 Photos	External SD	\DCIM\	.jpg/.dng	FLYXXX
 Video	External SD	\DJI\dji.pilot\DJI_REC ORD\	.mp4/.mov	FLYXXX













				
DJI Phantom 4				
 Photos	External SD	\DCIM\	.jpg/.dng	FLYXXX
 Video	External SD	\DCIM\	.mov/.mp4	FLYXXX
				
DJI MAVIC 2				
 Photos	Internal eMMC/External SD	\DCIM\	.jpg/.dng	FLYXXX
 Video	External SD	\DCIM\	.mov/.mp4	FLYXXX
				
YUNEEC Q500 4K				
 Photos	Camera SD	\DCIM\	.jpg/.dng	
 Video	Camera SD	\DCIM\	.mp4	
				
Parrot ANAFI				
 Photos	External SD	\DCIM\100MEDIA	.jpg/.dng	
 Video	External SD	\DCIM\100MEDIA	.mp4	
*Additional footage may be found on the controller micro SD card at the directory \FPV-Video\Local\ using the extension .avc for video footage.				

Table 26 - Multimedia Locations for some Popular Drones

6.3 Companion Mobile Phone Applications

The majority of drones come with companion mobile applications to either pilot the drone or view the camera feed and location of the drone overlaid on a map. These apps generally require the user to register a valid email account to access the application but it also may be possible to use your Facebook, Google, Apple or Outlook account with some of these applications. All applications have to be installed by the user via the application store such as Google Play Store and Apple Store and require particular user permissions to access some functions of the handset. In the tables below we list an overview of DJI, Parrot, and Yuneec drones.


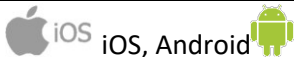
The examiner should be aware that it may be possible to utilize a third-party application to control or monitor the drone so when examining the mobile phone, laptop or tablet the examiner must verify the functionality

of installed applications to ensure that none of the applications are related to the drone being examined. Also, analysis of the application may show information related to other registered drones within the application.

For specific guidance on digital forensic analysis of mobile phones, please refer to the INTERPOL Global Guidelines for Digital Forensic Laboratories.

6.3.1 DJI Mobile Application

DJI have companion mobile applications for all their drones. The most utilized mobile application is the DJI Go 4.

Application Name	DJI Go 4	
Application Icon		
Publisher	DJI Technology	
Supported Platforms	 iOS, Android	
Publishers Description	<p>Capture the world from above. DJI GO 4.0 has been optimized for all of DJI's latest products. These include the Phantom 4, Mavic Pro, Phantom 4 Pro, and Inspire 2. It provides near real-time image transmission and camera settings adjustment, as well as editing and sharing of aerial imagery.</p>	
Features:	<ul style="list-style-type: none"> • All-new Homepage and UI. • Near Real-time HD Image Transmission. • Camera Settings Adjustment. • Updated playback interface. • Updated Editor with improved UI. • More templates and music tracks in Editor. • Convenient video downloading, editing and sharing. • Integrated live streaming. • Near real-time flight data recording. 	
Screenshots		
Application Home Screen	In-Flight Controls	

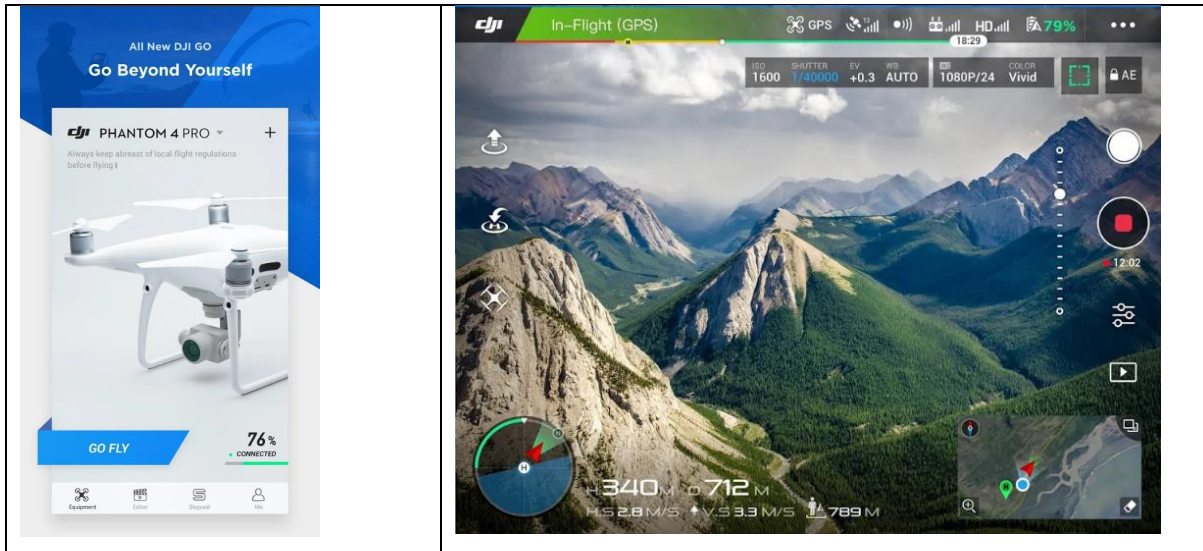





Table 27 - DJI Go 4 Mobile Application

6.3.2 Parrot Mobile Application

Application Name	Free Flight Pro
Application Icon	
Publisher	Parrot SA
Supported Platforms	 iOS,  Android
Publishers Description	<p>The official piloting application for Parrot drones.</p> <p>PILOT YOUR DRONE VIA SMARTPHONE OR TABLET.</p> <p>Download FreeFlight Pro, the free app that allows you to access advanced flight settings and pilot your Parrot Bebop, Bebop 2 and Disco drones.</p> <p>To pilot ANAFI please use the new Freeflight 6 app. Please note that Freeflight 6 cannot be used with the Parrot Bebop 2 and Parrot Disco range.</p> <p>INTUITIVE PILOTING</p> <p>FreeFlight Pro's touch controls make flying Parrot drones easy for all pilots, both beginner and advanced. The app's interface can be customized to suit each individual's skill level. If you are looking for a more precise piloting experience, connect your smartphone or tablet to the Parrot Skycontroller 2.</p>

IMMERSIVE FLIGHT

Get onboard with the new First-Person View (FPV) Parrot Cockpitglasses! FreeFlight Pro now includes an immersive piloting mode that works with the Parrot Cockpitglasses for high thrills and amazing sensations. To activate, simply insert your smartphone into the glasses, take-off, and experience the magic of flight. When immersive flight mode is in use, live telemetry data is shown on your screen to ensure a successful session.

ADVANCED PHOTO AND VIDEO

FreeFlight Pro comes equipped with advanced photo and video settings. Photo Mode allows you to capture high quality images in professional formats like RAW / DNG. You can also record Full HD 1080p videos at 30Mb/s and customize white balance, exposure, and the refresh rate. Time-lapse mode lets you take pictures at scheduled intervals for breath-taking accelerated video footage. Lastly, enjoy real-time video streaming on your smartphone/tablet while in flight.

PARROT CLOUD

By becoming a member of Parrot Cloud, you can keep track of all your adventures and connect with other drone pilots. Share your photos, videos and data sessions with other pilots and instantly upload to YouTube, Google Photos or Twitter. In addition, you get a free backup of all the data shared on Parrot Cloud.

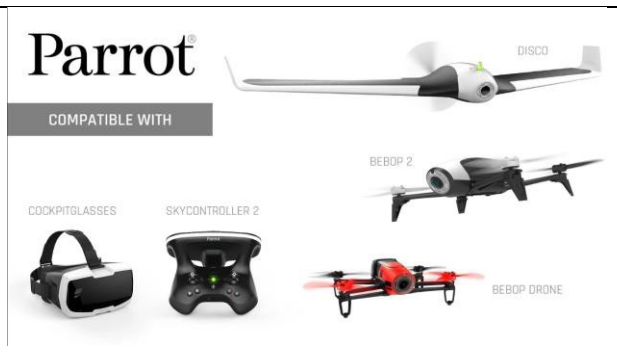
FLIGHT PLAN (in-app purchase)

Prepare pre-programmed autonomous flights from your smartphone or tablet using Flight Plan (in-app purchase). Create customized routes for your drone easily by selecting GPS waypoints on your screen. Hit take-off and watch your drone do the rest! Capture incredible video footage with this intelligent flight modes, including Point of Interest (POI), which allows you to focus your flight session around one object.

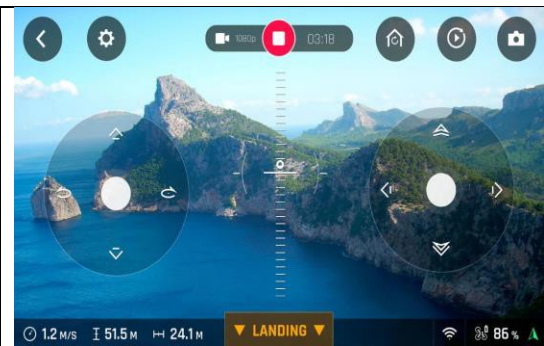
ACROBATICS, LOOPS & TURNS

The FreeFlight Pro application also includes fun features like one-touch flip. Make your Bebop drone flip, loop and turn with a single tap on the piloting home screen. For more piloting tips, tricks and useful video tutorials, please visit Parrot.com before taking off. Have a great flight!

Screenshots



Application Compatibility



Application being used as a Flight Controller



	
App in Cockpit Glasses	

Table 28 -Parrot Freeflight Mobile Application Overview

6.3.3 Yuneec Mobile Application

Application Name	Yuneec Pilot
Application Icon	
Publisher	Yuneec International Co.,Ltd
Supported Platforms	iOS, Android
Publishers Description	<p>Yuneec Pilot application is specially developed for Mantis Q, a compact and robust travel drone that can do more than just capture beautiful moments as unique pictures and 4K videos. The Mantis Q is guaranteed to be good fun thanks to its innovative voice control, rapid Sport Mode, long flight time, automatic flight modes, practical face recognition, and integrated Social Sharing Function. Designed to be an uncomplicated travel companion that can be taken anywhere, it is ideal for outdoorsy people, gadget lovers, and adrenaline junkies.</p>
Screenshots	

<p>User Account Screen</p>	<p>Social Media Integration</p>
<p>App Features</p>	<p>App Features</p>

Table 29 - Yuneec Mobile Application Overview

6.3.4 Yuneec Mobile Application for the Drone Camera




Application Name	CG03
Application Icon	
Publisher	Yuneec International Co.,ltd
Supported Platforms	iOS, Android
Publishers Description	
<p>CG0 is a Ground Control Station for Android Devices. It has these functions, control of the exposure, adjust the sensitivity, white balance, shutter time, and so on. CG0 is in active development, if you have some doubts, please visit our website: http://www.yuneec.com.</p>	
Screenshots	
	
Main Application Screen	
	
Video Settings Screen	

Table 30 - Yuneec Camera Mobile Application Overview

Yuneec also utilize the Android platform on the display that is built into the remote controller.



Controller utilises Android OS

Figure 37: Yuneec Remote Controller

6.4 Note on Storage Locations on Drones

Yuneec allows the user to store drone-generated data in up to three locations:

- Camera Gimble
- Drone
- Remote Controller



Figure 38: Yuneec Typhoon Q500 4K Data Locations

In the example above, the drone package may contain an SD Card in the drone, camera, and remote controller. This is why it is important for the examiner to thoroughly inspect the drone and associated devices to ensure that all storage media is located and analysed, as deemed necessary.

Also, if there is a mobile phone or tablet paired with the drone then there maybe artefacts contained within the parent application found on the mobile handset.

7. Common Tools Used in Drone Forensics

The market for drone forensics tools is in its infancy and a majority of commercial tools for drone forensics are part of a bigger suite of tools for mobile or computer forensics. The capability of these tools can change month to month so when selecting the right software tool to extract drone data you should always check the manufacturers supported devices list alongside what data types they extract from that supported device.

7.1 Cellebrite/MSAB XRY/Oxygen/CFID

- Capable of mounting and parsing data extracted from drones. Supports a limited number of drones but this should be utilized where appropriate as this simplifies the processing of drones and the associated data. It should be considered to use at least two tools to ensure that data verification is made over the extracted data.

7.2 CsvView and DatCon [<http://datfile.net/>]

- DatCon is an open source tool capable of parsing and converting DJI .dat files into various formats such as .kml, .csv. It also has the ability to strip out certain data into a separate log file, such as configuration and event logs.
- CsvView is a similar tool, by the same developer, that can be used for parsing log data. Despite the name, it is not limited to CSV files and can accept original .dat logs. Although both tools are similar they have different capabilities and features.

7.3 DRone Open source Parser (DROP) [<https://github.com/unhcfreg/>]

- DROP Developed by Devon Clark with the UNH Cyber Forensics Research & Education Group. This open source tool can be used for parsing and converting flight logs from DJI Phantom 3 drones. The program also includes an incomplete breakdown of the data structure within logs, reversed engineered from DatCon.

7.4 Google Earth Pro [<https://www.google.co.uk/earth/versions/#download-pro>]

- May transmit data online. This mapping tool can be used for viewing flight data extracted from logs. It was successfully tested with both CSV and KML files.

7.5 ST2Dash and Dashware [<https://github.com/ajpierson/st2dash> ; <http://www.dashware.net/>]

- May transmit data online.
- ST2Dash is an open source tool designed for converting ST10+ controller and Q500 flight logs in to a format usable by Dashware. Dashware is a free editing suite for overlaying telemetry data on to video footage. In testing it seemed impractical for forensic use as synchronizing the data was time consuming and it did not provide information that was not already available. But it be useful under some circumstances.

7.6 DJI Assistant

- This may be used to acquire data held on a DJI drone, and will also parse recovered flight logs into csv files.

7.7 FTK Imager

- This can be used to create images of SD cards for analysis. Note: a media write blocker should be used.

7.8 VLC Player

- A multifunctional multimedia player that supports multiple video formats and codecs. This can be used to view the multimedia generated by the drone being examined.
- Since both internal and external SD cards can be either FAT32 or exFAT, they can be easily examined with forensic suites such as FTK and Autopsy.

8. Useful Web Resources

There are many websites that demonstrate or highlight drones and the associated forensic process. Below are some useful sites for reference that will aid you in understanding the issue and challenges in drones.

Drone Forensics [<https://www.droneforensics.com/>]

The Drone Forensics program seeks to identify digital forensic data on consumer and professional drones to aid law enforcement and government in investigations. The program is run by VTO Inc. of Broomfield, Colorado, USA.

Forensic Focus [<https://www.forensicfocus.com/>]

This is a website that has very active forums discussing digital forensics as well as informing you of the latest developments in digital forensics.

RPAS Forensic Validation Analysis Towards a Technical Investigation Process: A Case Study of Yuneec Typhoon H

(<https://www.mdpi.com/1424-8220/19/15/3246>)

Analyse drone images using the Computer Forensics Reference Datasets (CFReDS) and present results for the Typhoon H aerial vehicle manufactured by Yuneec, Inc. Furthermore, this paper explores the availability and value of digital evidence that would allow a more practical digital investigation to be able to build an evidence-based experience






Directory of National Civil Agencies

(<https://www.icao.int/pages/links.aspx>)

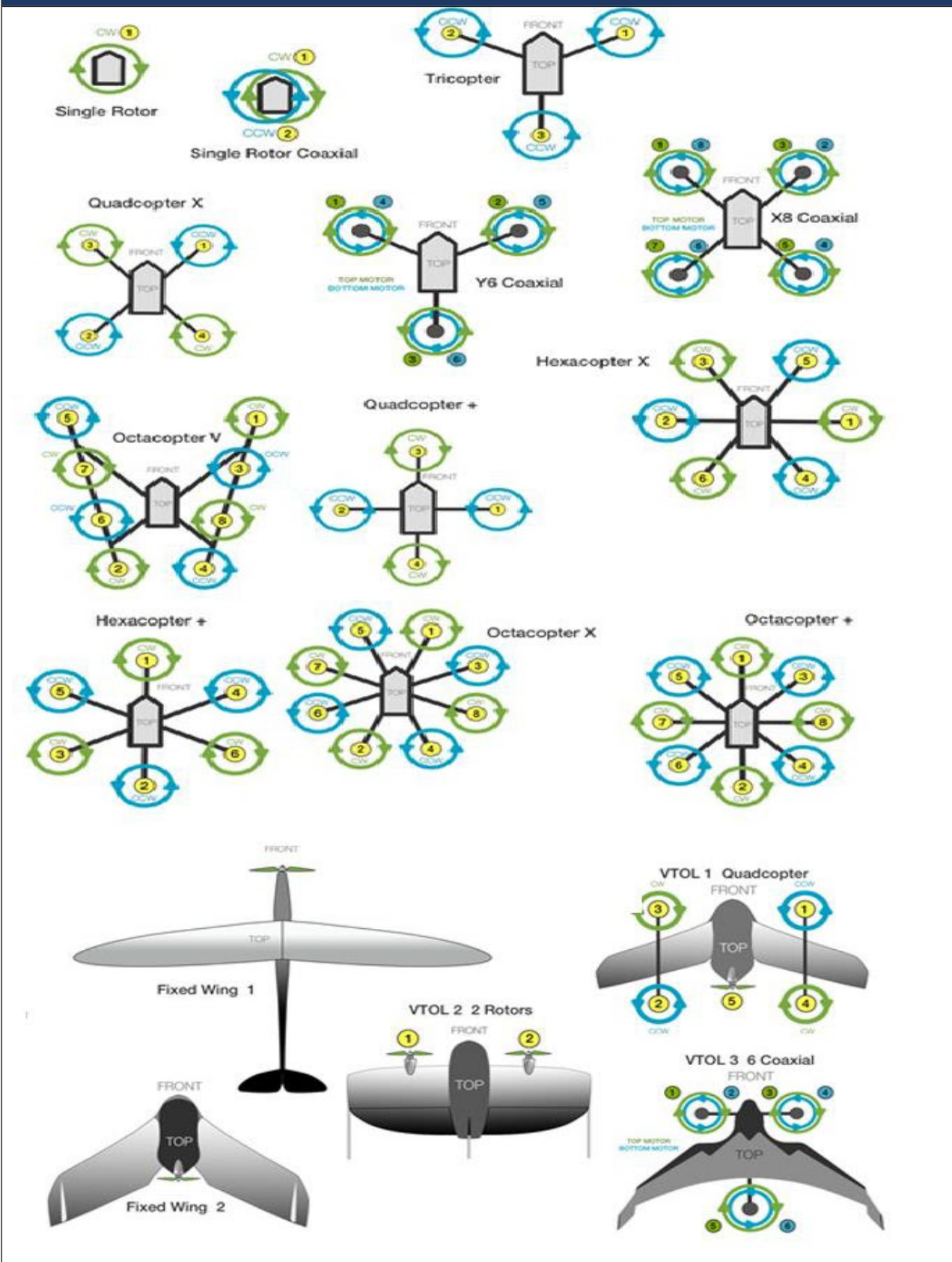
This directory contains details of all national aviation agencies. These agencies may be useful to contact when dealing with a drone incident.

Appendices

Appendix A: Types of Drones

Drone Type	Pros	Cons	Typical Uses
Multi-Rotor 	<ul style="list-style-type: none"> • Accessibility. • Ease of use. • VTOL and hover flight. • Good camera control. • Can operate in a confined area. 	<ul style="list-style-type: none"> • Short flight times. • Small payload capacity. 	Aerial photography and video aerial inspection
Fixed-Wing 	<ul style="list-style-type: none"> • Long endurance. • Large area coverage. • Fast flight speed. 	<ul style="list-style-type: none"> • Launch and recovery can require a lot of space. • No VTOL/hover. • Non-autonomous are harder to fly, more training needed. • Expensive. 	Delivery, aerial mapping, and pipeline and power line inspection
Single-Rotor 	<ul style="list-style-type: none"> • VTOL and hover flight. • Long endurance (with gas power). • Heavier payload capability. 	<ul style="list-style-type: none"> • More dangerous. • Harder to fly, more training needed. • Expensive. 	Aerial LIDAR laser scanning
Fixed-Wing Hybrid 	<ul style="list-style-type: none"> • VTOL and long-endurance flight. 	<ul style="list-style-type: none"> • Not perfect at either hovering or forward flight. • Still in development. 	Delivery
Elios 	<ul style="list-style-type: none"> • Collision tolerant. • Designed for indoor/confined space operation. • Dust and splash resistant. 	<ul style="list-style-type: none"> • Expensive. 	Accessing the inaccessible, and indoor/confined space inspection

Types of Multi-Rotor/VTOL Copters



Types of Drone Batteries



Sealed LiPo Batteries



Hobby

Types of Controllers



Dedicated



Companion Controller



Enhanced Companion Controller

Appendix B: Drone Incident First Responder Scene Log

Officer Actions
<p>Record incident</p> <p>Take photographs or video of the system in flight including surroundings. i.e. over a crowd, built up area etc.</p> <p>Any flight in a restricted or no fly zone airport, military base, nuclear power station, prison or specially designated zone should be considered a threat to public safety.</p>
<p>Identify the pilot</p> <p>The pilot will be most likely to be located where they have a good vantage point, allowing them to maintain control of the drone. They will most likely be using two hands on a controller (which may be a conventional controller, smartphone or tablet etc.) and their focus will be on controlling their device - they will be looking toward the device and rarely changing their orientation. The pilot may be static or walking slowly. These behaviours are likely to be significantly different from others around them.</p>
<p>Engage with the pilot and ascertain:</p> <p>What are they doing?</p> <p>What are they filming?</p> <p>Do they have the appropriate license for operating the drone?</p>
<p>Ascertain nature of the offence:</p> <p>Examples include:</p> <p>Public Nuisance</p> <p>Assault</p> <p>Criminal Damage</p> <p>Terrorism</p> <p>Obstruction</p>
<p>If you believe an offence is being committed, communicate to the pilot to the land system responsible and away from crowded area.</p>

Preliminary Investigation

Identify the point from which the drone took off and landed

Secure scene to ensure that no persons are placed in danger from the drone

Access incident area and evaluate the cause of the drone location:

Drone

What type of drone is it? (multicopter or fixed wing)

Did it crash or land?

Is it still on?

Is there an additional payload present?

Are there any clear and present dangers: i.e. explosive threat, moving propellers, unidentified payload?

Controller/Pilot

Can you identify the pilot of the drone?

Is the controller still communicating with the drone?

Are they compliant with your directions?

Are they cooperative?

What is the intended use of the drone?

Securing the Scene

Date		
Time		
Location		
GPS Coordinates	Longitude	Latitude
Check for signs damage to the drone or signs of collision in the the surrounding area.		
Notes		

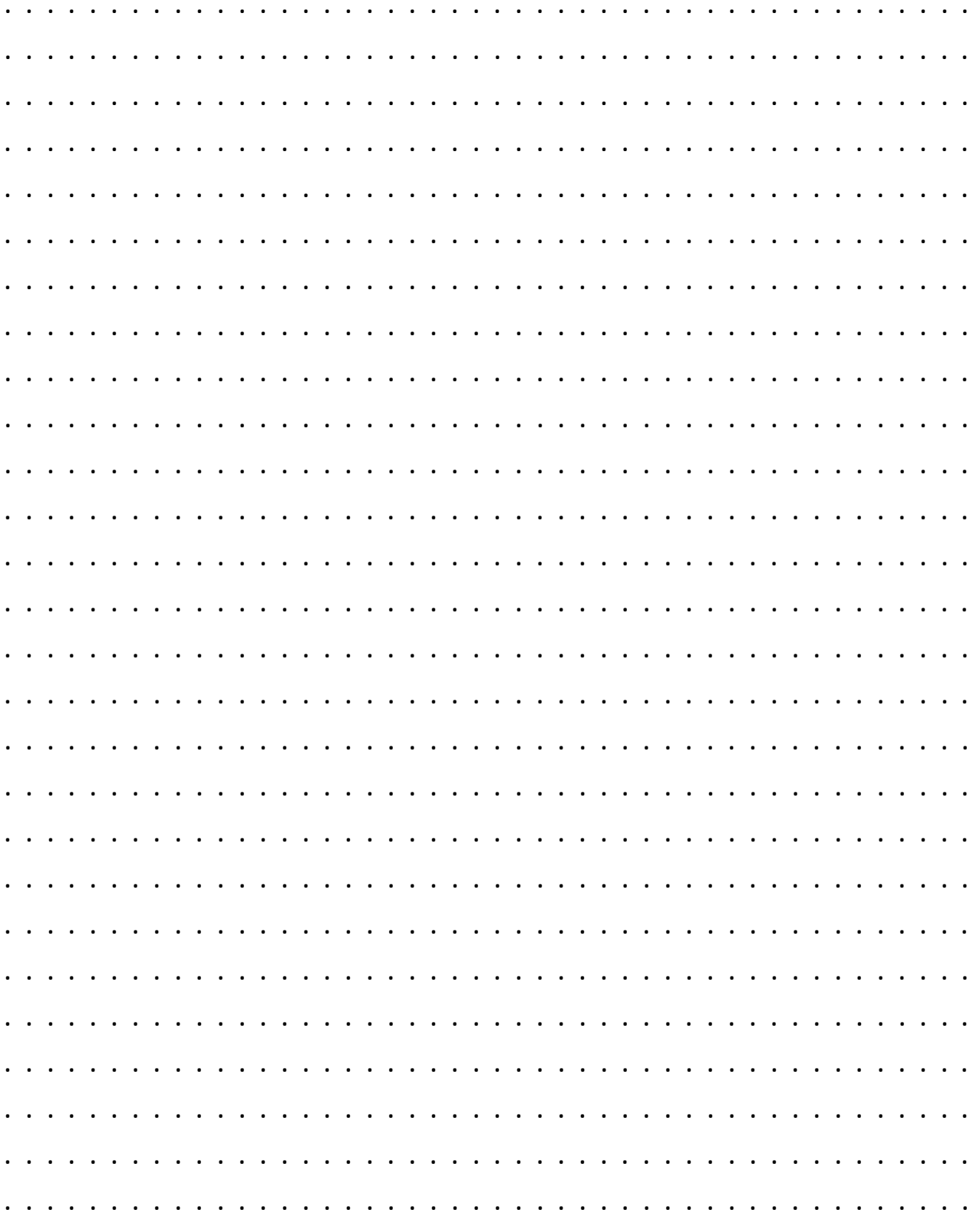
Appendix C: Drone Incident Record Sheet

Drone Incident Record Sheet

Attending Officer					
Drone Type					
Multi-Rotor	<input type="checkbox"/>	Fixed Wing	<input type="checkbox"/>	Single Rotor	<input type="checkbox"/>
Other					
Make			Model		
Is Drone Switched On?	Yes	<input type="checkbox"/>	No	<input type="checkbox"/>	
If you power off the drone, please state the method used to power off the drone					
Switched Off	<input type="checkbox"/>	Battery Removed	<input type="checkbox"/>	Other	<input type="checkbox"/>
Date	<input type="text"/>	Time	<input type="text"/>		
Weather Conditions (Is it Sunny, Cloudy, Rainy, Windy)					
Notes					

Scene Sketch

(Please use two fixed points for reference and keep to scale)



Have Photos been taken of the drone and surrounding area?					
Yes		No			
Has drone operator been identified?					
Yes		No			
Has associated equipment associated with the drone been identified and recovered?					
Yes		No			
Associated Equipment Identified					
Controller		Mobile Device		Tablet	
Batteries		Additional Media Cards		Other	
Details of Other Equipment:					
Form Completed By		Contact Number			
Signed					
Date		Time			

Appendix D: Drone Examination Log

Drone Examination Log

Examination Considerations of Drones for Digital Forensic Laboratory Examinations

1. Drones have the potential to contain both internal storage and an external SD card
 - Internal SD card can contain flight logs and may require disassembly of the drone.
 - To access the internal memory, some drones can be mounted/imaged over USB. However, some drones cannot be write blocked in order to obtain data in internal memory.
2. Drones contain different data on the device itself as well as other network connected devices (i.e. controllers, laptops, mobile phones, tablets, etc.)
 - Follow proper acquisition procedures for network connected devices
 - Remember digital forensic handling procedures for acquisitions from network connected devices.
3. Network isolation procedures when conducting examinations on drones or connected devices.
4. If there is no internal or external removable media, the examiner may need to access the flash memory chip on the device.




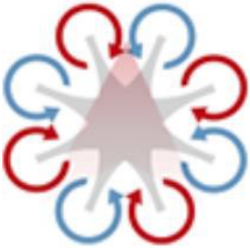



Initial Evidence Intake/Case Details

Investigator Name/ ID	
Case Identification Number	
Investigating Agency	
Full forensic exam strategy	
(Provide a brief explanation of all tests that will be performed on evidence items received to laboratory).	
<small>*This is a just a brief synopsis of planned work but it does not reflect the actual steps performed.</small>	

Initial Exhibit Assessment/Physical Description

What device is under examination?			
<input type="radio"/> UAV	<input type="radio"/> Controller	<input type="radio"/> Phone	<input type="radio"/> PC/Other
If "Other" please describe.			
Has all wet forensic work been performed? (i.e. biological, DNA, fingerprint, biohazard, etc.)	<input type="radio"/> YES	<input type="radio"/> NO	<input type="radio"/> Not applicable
What is the condition of device under examination?	<input type="radio"/> Damaged	<input type="radio"/> Modified	<input type="radio"/> No damage observed
If damaged or modified, please describe.			
Have photographs been taken of device?	<input type="radio"/> YES	<input type="radio"/> NO	<input type="radio"/> Not applicable
Examiner Notes			
(Use this section to record any information not covered within this table)			

Device Examination Notes

<p>Manufacturer</p>			
<p>Type of drone (please circle the appropriate picture)</p>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
	 <input type="checkbox"/>	<div style="border: 1px solid black; width: 100%; height: 80px; margin-bottom: 5px;"></div> <div style="border: 1px solid black; padding: 2px; display: inline-block;">Other – please draw</div>	
<p>Model Name</p>			
<p>Colour</p>			
<p>Serial Number/Part No</p>			

Is there any removable storage? (e.g. memory cards, USB drive, hard drive)	Please specify where was it located: (e.g. camera, drone, internal, display, other)	
	Removable storage type (e.g. micro SD, SD, other)	
	Memory card capacity	
	Branding/Serial numbers:	

Are there any other components with printed labels/serial numbers?
(List these components below with serial/part numbers)

--

Have photographs been taken of removable components?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Not Applicable
--	------------------------------	-----------------------------	---

Examiner Notes

Examiner Notes

<p>What types of forensic tool(s) were used for data acquisition? (Include name of forensic tool and version)</p>		
<p>How was the device connected to the forensic tool for data acquisition?</p>	<p>Cable <input type="checkbox"/> Wi-Fi <input type="checkbox"/></p>	<p>Chip off <input type="checkbox"/> JTAG/ISP <input type="checkbox"/> Other <input type="checkbox"/></p>
<p>Acquisition Source (e.g. SD card, internal memory, chips)</p>		
<p>What was data acquisition duration?</p>		

Examination Notes
(Please note any/all values obtained and any behaviour observed during extraction)

<p>Examination Completed Date</p>	
<p>Examination Completed Time</p>	
<p>Signed</p>	

Appendix E: LiPo Battery Safety Reference Card

LiPo Battery Safety

- Lithium batteries need special handling because physical damage or short circuiting them is likely to cause them to catch fire.
- Store them in a special bag when not in use or while charging and keep the bag where it could contain a fire.
- If a LiPo pack starts to expand (puff up) or if it won't take a full charge on all cells, dispose of it.
- Before disposal, a LiPo battery should be fully discharged by connecting it to a resistive load (light bulb or charger-discharge function).
- It is a good idea to keep a metal bucket filled with sand handy in case a LiPo fire needs to be extinguished.
- DO NOT put water on a burning LiPo Battery, lithium takes oxygen directly out of water and keeps on burning.
- Lithium batteries are especially likely to misbehave while charging or discharging or when dropped.

Appendix F: Checklist for a Basic Drone Response Kit

The following is a suggestion for a basic equipment list that a DFL should own. The reader shall take note that the list is non-exhaustive and may require more depending on the nature of cases received.

No	Item	
1	Laptop	<input type="checkbox"/>
2	Drone data recovery and analysis software	<input type="checkbox"/>
3	Data recovery software	<input type="checkbox"/>
4	Mobile device analysis software	<input type="checkbox"/>
5	Imaging and analysis software	<input type="checkbox"/>
6	Faraday Bag/Box	<input type="checkbox"/>
7	Camera	<input type="checkbox"/>
8	Crime Scene Tape and associated materials	<input type="checkbox"/>
9	Write blocker	<input type="checkbox"/>
10	Empty storage media – to store data extracted from electronic evidence in short term and long term: <ul style="list-style-type: none"> • Pen drive • External hard disk • Hard disk 	<input type="checkbox"/>
11	Electrical/Electronic toolkit	<input type="checkbox"/>
12	Power cable extension	<input type="checkbox"/>
13	LiPo Bag	<input type="checkbox"/>

Appendix G: Core Competencies for First Responders and Digital Forensic Specialists

The following is a suggestion for core competencies that should be considered for a Technical First Responder

1. Purpose

The purpose of this document is to describe the desired core competencies for First Non-Technical Responders, Technical, Advanced First Responders and Drone Digital Forensic Specialists that are responding to a drone incident.

Competency Level	
BASIC	Non-Technical First Responder
INTERMEDIATE	Technical First Responder
ADVANCED	Advanced Technical First Responder
	Drone Digital Forensics Specialist

2. Scope

The intended audience is for first responders who encounter drones and associated equipment in the field. These best practices should be followed if hardware or software is used to retrieve data from a drone. This document may not apply for those inside the lab setting whose interaction with the drone is to forensically retrieve the content of the drone.

3. Definitions

Drone forensics is the utilization of scientific methodologies to recover data stored by a drone and associated equipment such as remote controllers and paired mobile devices for legal purposes.

4. Limitations

Drones present a unique challenge to law enforcement due to rapid changes in technology. There are numerous models of drones in use today. New families of drones are typically manufactured every three (3) to six (6) months. Many of these drones use closed operating systems and proprietary interfaces making it difficult for the forensic extraction of digital evidence.

Drones have associated equipment which may consist of a remote controller, a heads-up display which may be a mobile phone or tablet. There may also be associated batteries and memory cards that may have been used in the drone.

Some limitations encountered are as follows:

Incoming and Outgoing Signals – Attempts should be made to block incoming and outgoing signals of a drone and associated equipment. Common methods include Radio Frequency (RF) blocking container or jamming appliances. Blocking RF signals will drain the battery, may be expensive, are not always successful and may

result in the alteration of drone data. This will also ensure that the data cannot be remotely wiped by the suspect.

Cables – Data Cables are often unique to a particular drone. Frequently cables are specific to the forensic tool to be used. Data cables often have a wide variety of connections (e.g., RJ-45, USB, or RS-232). This results in a large number of cables being required for forensic analysis of drones.

Destruction of Data – There are methods to destroy data locally and remotely on a drone.

Drivers – Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with the tool or downloaded from a website. Drivers may compete for control for the same resource if more than one forensic product is loaded on the analysis machine.

Dynamic Nature of the Data – Data on active (powered-on) drones is constantly changing. There are no conventional write-blocking methods for drones.

Encryption – Data may be stored in an encrypted state preventing analysis.

Equipment – Equipment used during examinations may not be the most recent version due to agency verification requirements of hardware, firmware and/or software.

Field Analysis – First responders should be aware of the risks associated with triaging mobile drones. Triaging mobile drones is not considered a full examination. The drone should be protected for further examination.

The Condition of the Evidence – Commercially available tools may not provide solutions to deal with physically damaged drones.

Hash Values – Individual data objects (e.g., graphics, audio, and video files) will often maintain consistency between the forensic workstation and the hash value reported by the drone application. Due to the volatility of drone operating systems, overall case file hashes of system files will typically not be consistent due to file system optimization.

Industry Standards – Manufacturers of drones lack standardized methods of storing data (e.g., closed operating systems and proprietary data connections).

Loss of Power – Many drones may lose or create data or initiate additional security measures once discharged or shut down.

Removable Media Cards – Processing these cards inside the drone poses risks (e.g., not obtaining all data including the deleted data, and altering date/time stamps).

Training – The individual copying data from a drone and associated equipment should be trained to ensure the integrity of the data.

Unallocated Data / Deleted Data – Many drone forensic tools may only provide the logical acquisition of data. Deleted data may only be recoverable from a physical acquisition.

Associated Equipment - a drone requires a controller and/or remote viewer to utilize the drone functionality and this equipment may not be local to a drone at a crime scene. There may also be associated with batteries and memory cards associated with the drone that may not be in situ to the device.

Appendix H: Core Competencies for First Responders

The following is a suggestion for a core competency that should be considered for a Technical First Responder

First Responders are defined as individuals that may be responsible for the collection and minimal examination of a drone. There are three levels of First Responders:

Level 1 First Responders are individuals that collect and/or manually examine drone and associated equipment.

Level 2 Technical First Responders are individuals that utilize a tool or software to extract data from the drone and associated equipment. The use of basic tools to download/extract data from a drone and associated equipment necessitates that proper training is completed by the individual using that tool.

Level 3 Advanced Technical First Responders are individuals that utilize a tool or software to extract data from the drone and associated equipment. The use of advanced tools to download/extract data from a drone and associated equipment necessitates that proper training is completed by the individual using that tool.

The drone and associated equipment forensics field continues to be dynamic and shares some aspects of traditional computer forensics.

A practitioner should have an overall understanding of mobile forensics analysis and can remain current by reading trade journals, taking classes, participating in professional organizations, taking continuing education, on-the-job training and hands-on experience.

An examiner must adhere to all appropriate standard operating procedures and policies. A code of ethics including neutrality in the scientific processes.

An examiner may be assigned casework that falls within one or more of the following levels and should, therefore, have the appropriate level of training to perform the examination.

Levels of analysis - The level of analysis is dependent on the request and the specifics of the investigation. Higher levels of analysis require a more comprehensive examination.

Appendix I: Core Competencies for Non-Technical First Technical Responders

The following is a suggestion for a core competency that should be considered for Non-Technical First Responder

1. Ability to Identify Basic Drone configurations.
 - a. Must identify drone types and UAS systems
 - b. Shutdown procedures appropriate for the drone and associated equipment
2. Utilize scene security: understand how to properly secure the area.
 - a. Crime scene
3. Interview people: witness, suspect people.
4. Render safe procedures.
5. Understand how to protect the evidence: collect, handle and package.
 - a. Take crime scene pictures
 - b. Label evidence with numbers
 - c. Package evidence appropriately
6. Maintain the chain of custody.
7. Understand the appropriate legal framework.

Appendix J: Core Competencies for First Technical Responders

The following is a suggestion for a core competency that should be considered for Technical First Responder

Competencies listed below outline the minimum requirements for a Technical First Responder manually analysing a drone in the field without the use of an examination tool.

- All the competencies that are listed for “Core Competencies for Non-Technical First Responders” and “Core Competencies for Technical First Responders” and:
 1. Understand proper evidence handling, labelling, preservation and seizure.
 2. Understand the consequences and risks associated with interfering with the drone.
 3. Understand that placing memory cards in different computers, mobiles or drones may modify the data.
 4. Understand the removal and replacement of a battery may cause a drone to reset.
 5. Understand applicable legal authority and case law.
 6. Identify the following types of drones: multicopters and fixed wing.
 7. Understand the importance of proper crime scene documentation.
 8. Understand the correct seizure process for drones and associated technologies.
 9. Understand the need and relevance to verify the data extracted from the drone and associated equipment.
 10. Understand the possibilities of associated equipment such as controllers and mobile phones used to view drone footage.
 11. Proper handling of drone batteries to ensure that the batteries are safely secured and handled to prevent an explosion or leakage.
 12. Potential biohazards associated with drones or associated equipment.
 13. Determine the need for wet forensics such as fingerprints, DNA etc.

Appendix K: Core Competencies for Advanced First Technical Responders

The following is a suggestion for a core competency that should be considered for an Advanced First Technical Responder

Competencies listed below outline the minimum requirements for a First Responder that uses an examination tool to analyse a drone and associated equipment. An example of a Level 2 First Responder would be a properly trained patrol officer/case agent who uses software or a hardware device to download data from a drone and associated equipment.

Examples of logical and file system examinations include using software or a hardware device to acquire user/system accessible data such as flight logs, home locations, flight telemetry registered user information, pictures, video, audio, application data, device information, stored on the drone.

All the competencies that are listed under Core Competencies for Non-Technical First Responders”, “Core Competencies for Technical First Responders” and:

1. Define important acronyms used to describe drone components and their functions.
2. Identify the following types of drones: multicopters and fixed wing.
3. Identify what information can be stored in a drone and associated equipment.
4. Identify what information can be stored on a memory card.
5. Identify other locations where information can be stored.
6. Understand the legal issues associated with drones (e.g., the scope of the warrant, consent, case law, licensing by state, and certification requirements)
7. Ability to isolate a drone from command signal by powering off the drone, using RF shielding or disabling all radio communications.
8. Ability to explain the advantages and disadvantages of powering off the drone.
9. Describe methods and tools for processing drones and associated equipment.
10. Knowledge of tool functionality, their limitations and the possible need for additional examination (e.g., logical dumps of data may not retrieve deleted data from the drones, controllers and memory cards).
11. Understand the need to perform tool testing, maintenance and validation.
12. Understand the “Best Practices for Drone Examinations.”
13. Understand that data from media cards may not be extracted using some software or hardware devices.
Ability to defend in court the use of utilized tools.

Glossaries

General Overview

1.1 It should be noted that the terminology related to UAS operations continues to evolve and therefore this Glossary is not exhaustive or definitive. The terms listed below are a combination of the emerging International Civil Aviation Organisation (ICAO) definitions, other 'common use' terms which are considered to be acceptable alternatives, and a number of 'legacy' terms. Whilst these legacy terms will continue to be recognised, in the interests of commonality the use of the following terminology is advised.

1.2 Some of the following are terms used by the Military as defined in the Military Aviation Authority (MAA) Regulatory Publications (MRP). These terms (identified by an asterisk *) are not necessarily applicable to UAS that are subject to civil regulations.

NOTE: The terms 'pilot' and 'remote pilot' are being increasingly used worldwide (including ICAO) to describe the person who directly controls an unmanned aircraft and that trend is reflected in this document. It should be noted, however, that within the United Kingdom there are many legal requirements in the Air Navigation Order 2016 applicable to 'pilots'. These references, however, apply only to pilots in the traditional sense – i.e. persons on board and flying the aircraft. There are at present no legal requirements setting out the qualifications needed to control an unmanned aircraft; this work is still to be completed.

Glossary I: General Aviation Abbreviations

COMMON ABBREVIATIONS USED IN DRONES

AAIB	Air Accidents Investigation Branch
ACAS	Airborne Collision Avoidance System
AIP	Aeronautical Information Publication
ANO	Air Navigation Order
ANSP	Air Navigation Service Provider
AOA	Aircraft Operating Authority*
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSU	Air Traffic Service Unit
BRS	Ballistic Recovery Systems
BVLOS	Beyond Visual Line of Sight
CAA	Civil Aviation Authority
CFT	Certificate for Flight Trials
CPL	Commercial Pilot Licence
CRM	Crew Resource Management
C-UAV (C-UAS)	Counter Unmanned Aircraft Vehicle (System)
DA	Danger Area
DAP	Directorate of Airspace Policy
EASA	European Aviation Safety Agency
ERF	Emergency Restriction of Flying
EVLOS	Extended Visual Line of Sight
FAA	Federal Aviation Administration
FIR	Flight Information Region
FISO	Flight Information Service Officer

FMC	Flight Management Computer
FOP	Flight Operations Policy
FRTOL	Flight Radio Telephony Operators' Licence
GCS	Ground Control Station
HALE	High Altitude Long Endurance
HMI	Human-Machine Interface
ICAO	International Civil Aviation Organization
IFR	Instrument Flight Rules
JAA	Joint Aviation Authority
MAA	Military Aviation Authority
MALE	Medium Altitude Long Endurance
MoD	Ministry of Defence
MOR	Mandatory Occurrence Reporting
MRP	MAA Regulatory Publication(s)
MTOM	Maximum Take-off Mass
NAA	National Aviation Authority
NAS	National Airspace
NOTAM	NOtice To AirMen
RA(T)	Restricted Area (Temporary)
RCS	Radar Cross Section
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System Remotely Piloted Air System*
RPAS Cdr	Remotely Piloted Air System Commander*
RPS	Remote Pilot Station
RTF	Radiotelephony
RTS	Release to Service
SARPs	Standards and Recommended Practices
SRG	Safety Regulation Group
SSR	Secondary Surveillance Radar

SUA	Small Unmanned Aircraft
SUAS	Small Unmanned Aircraft System
SUSA	Small Unmanned Surveillance Aircraft
TCAS	Traffic Collision Avoidance System
TDA	Temporary Danger Area
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System(s)
UAS-p	UAS Pilot (legacy term)
UAV	Unmanned Aerial Vehicle(s) (legacy term)
UAV-p	UAV Pilot (legacy term)
UIR	Upper Flight Information Region
VFR	Visual Flight Rules
VLOS	Visual Line of Sight

More detailed explanations of terms are provided on the following pages.

Glossary II: Technical Abbreviations

AVIATION AGENCY LIST

ACC	Accelerometer
AUW	All Up Weight
ARTF	Almost Ready to Fly
AH	Altitude Hold
mAh	milliAmp Hours.
Rx	Receive (as in receive radio signal)
Tx	Transmit (as in transmit radio signal)

COMMON DIGITAL FORENSICS TERMINOLOGY

A	
Acquisition	See "Image".
Archive Copy	A copy of data placed on media suitable for long-term storage, from which subsequent working copies can be produced.
Archive Image	Any image placed on media that is suitable for long-term storage, a bit stream duplicate of the original data placed on media that is suitable for long-term storage.
Authentication	The process of substantiating that the data is an accurate representation of what it purports to be.
C	
Capture	The process of recording data, such as an image, video sequence, flight data.
Chain of Custody / Continuity	The chronological documentation of the movement, location and possession of evidence.
Copy	An accurate reproduction of information.
D	
Data	Information in analogue or digital form that can be transmitted or processed.
Data Analysis	The assessment of the information contained within the media.
Data Extraction	A process that identifies and recovers information that may not be immediately apparent.
Data Smear	The modification of data by a running system during the data acquisition process.

Digital Evidence	Information of probative value that is stored or transmitted in a binary form.
Directory Listing	A list of files contained within an object. It may also contain other information such as the size and dates of the files.
Downloading / Exporting	The process of retrieving digital data, audio, video and still images and transactional data. Can be in either native or proprietary format or an open format
E	
Erased File Recovery	The process of recovering deleted files
Extraction	A method of exporting data from a source (e.g. copying data from EnCase preview, dumping data from a cell phone) See Data Extraction.
F	
File Format	The structure by which data is organized in a file.
File Slack	The data between the logical end of a file and the end of the last storage unit for that file. For the FAT file system, the data between the logical end of the file and the end of the cluster.
Forensic	The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime.
Forensic Cloning	The process of creating a bit stream duplicate of the available data from one physical media to another.
G	
GeoTag	GPS coordinates added to files as metadata.
GPX	GPS exchange format. An XML scheme designed for a common GPS format for software applications.
H	
Hash or Hash Value	Numerical values generated by hashing functions used to substantiate the integrity of digital evidence and / or for inclusion / exclusion comparisons against known value sets.
I	

Integrity Verification	The process of confirming that the data presented is complete and unaltered since time of acquisition.
L	
Log File	A record of actions, events and related data.
Logical Acquisition / Copy	An accurate reproduction of information contained within a logical volume (e.g. mounted volume, logical drive assignment etc).
M	
Media	Objects on which data can be stored.
Meta Data	Data, frequently embedded within a file that describes a file or directory which can include the locations where the content is stored, dates and times, application specific information and permissions.
Mobile Device	A portable device that has an embedded system architecture, processing capability, on-board memory and may have telephony capabilities.
Mobile Phone Forensics	For legal purposes, the utilization of scientific methodologies to recover data stored by a cellular device.
Multimedia Evidence	Analog or digital media, including, but not limited to, film, tape, magnetic and optical media and / or the information contained therein.
N	
Native File Format	The original form of a file. A file created with one application can often be read by others, but a file's native format remains the format it was given by the application that created it. In most cases the specific attributes of a file (for example, fonts in a document) can only be changed when it is opened with the program that created it.
P	
Password Recovery	The process of locating and identifying a series of characters used to restrict access to data.
PCB	Printed Circuit Board. A board used in electronics which may hold components or refer to the board itself in a bare state.
Peer Review / Technical Review	An evaluation conducted by a second qualified individual of reports, notes, data, conclusions and other documents.
Physical Copy	(c) An accurate reproduction of information contained on the physical device.

Physical Image/Acquisition	(c) A bitstream duplicate of data contained on a device.
Pixel	Picture element, the smallest component of a picture that can be individually processed in an electronic imaging system [<i>The Focal Encyclopedia of Photography</i> , 4th Edition 2007].
Playback	Recorded material viewed and heard as recorded, facilitated by camcorder, cassette recorder, or other device.
Preview	(c) A sub-process of triage where a cursory review of items is performed to assess the need for collection and/or further examination.
Primary Image	Refers to the first instance in which an image is recorded onto any media that is a separate, identifiable object. Examples include a digital image recorded on a flash card or a digital image downloaded from the Internet.
Processed Image	Any image that has undergone enhancement, restoration or other operation.
Proficiency Test	A test to evaluate analysts, technical support personnel, and the quality performance of an agency (<i>Four examples are provided</i>). 1. Open test - the analyst(s) and technical support personnel are aware they are being tested. 2. Blind test - the analyst(s) and technical support personnel are not aware they are being tested. 3. Internal test - conducted by the agency itself. 4. External test - conducted by an agency independent of the agency being tested.
Proprietary File Format	Any file format that is unique to a specific manufacturer or product.
Q	
Quality Assurance	Planned and systematic actions necessary to provide sufficient confidence that an agency's/laboratory's product or service will satisfy given requirements for quality.
R	
Reconstruction	The process of repairing damaged media in order to allow the retrieval of data.
Reference Materials	Refers to items such as published literature, hardware and software documentation, hash sets, header sets, etc.
Reliability	The extent to which information can be depended upon.

Reproducibility	The extent to which a process yields the same results on repeated trials.
Residue	(c) Data that is contained in unallocated space or file slack. (a) The residue of a filtered signal is the algebraic difference between the filter output and its signal input. [<i>Diamond Cut Users Manual</i>]
Resolution	The act, process, or capability of distinguishing between two separate but adjacent parts or stimuli, such as elements of detail in an image, or similar colors. [Taken from the <i>Encyclopedia of Photography</i> , 3rd Edition]
S	
Source Code	The list of instructions written in a programming language used to construct a software program.
Storage Media	Any object on which data is preserved.
T	
Technical/Peer Review	An evaluation conducted by a second qualified individual of reports, notes, data, conclusions, and other documents.
Timeline Sequence Reconstruction	The process of relating images, audio, or other data to one another in a chronologically ordered succession.
Track Log	A complete list of trackpoints that a GPS device has created.
Triage	The process by which items considered for collection or analysis are prioritized to determine the order in which they should be collected and/or analyzed, if at all.
U	
Unallocated Space	Data storage areas available for use by the computer. The area may already contain previously stored information. Also referred to as <i>Free Space</i> .
V	
Validation	The process of performing a set of experiments, which establishes the efficacy and reliability of a tool, technique or procedure or modification thereof.
Validation Testing	An evaluation to determine if a tool, technique or procedure functions correctly and as intended.
Verification	1. The process of confirming the accuracy of an item to its original. 2. Confirmation that a tool, technique or procedure performs as expected.

Video	The electronic representation of a sequence of images, depicting either stationary or moving scenes. It may include audio.
W	
Waypoint	A location that is stored by a GPS device based on user interaction.
Work Copy	A copy or duplicate of a recording or data that can be used for subsequent processing and/or analysis.
Write Block/Write Protect	Hardware and/or software methods of preventing modification of media content.

Note: Above definitions obtained from SWGDE (Scientific Working Group on Digital Evidence) Digital & Multimedia Evidence Glossary Version 3.0 (June 23, 2016).

Glossary IV: UAV Glossary of Terms

COMMON UAV TERMINOLOGY

0-9	
2.4GHz	The frequency used by digital (spread spectrum) radio communications in our applications, including 2.4Ghz RC, Bluetooth and some video transmission equipment. This is a different band than the older 72 Mhz band that is used for analogue RC communications. To avoid radio frequency conflict is it often a good idea to use 72 Mhz radio equipment when you are using 2.4 GHz onboard video transmitters, or use 900 Mhz video when using 2.4 GHz RC equipment. 2.4GHz is commonly within the unlicensed band.
3D Mapping	This is a software package that allows you to create 3D maps from your drone. It allows you to map large areas quickly and effectively. This enables farmers to better plan crop rotation, allows insurance companies to assess damage to buildings without endangering life. It also enables forest management companies to monitor tree crown delineation and helps architects to create an accurate 3D map of the topography of a site for planning consideration.
5.8GHz	Commonly band such as 2.4 GHz used most in microwaves, Bluetooth, drones, etc. So using your drone in this band may lead to disturbances from other wireless devices or drones. 5.8GHz is commonly within the unlicensed band.
A	
Accelerometer (ACC)	A device that measures acceleration forces in a specific direction. Used to help stabilize quadcopters, often under windy conditions.
ACRO Mode	It is also known as the "Rate Mode" where it utilizes the remote controller to control the angular velocity of the drone. Most of this is used on performing flips and rolls.
Ascent Speed	This is the speed that the drone ascends into the air. For example, the Wind 4 has an ascent speed of 4 metres per second (m/s).
ATTI Mode	Attitude Mode - In this mode the drone keeps their altitude through barometric pressure. The position will not be stabilized using GPS or Glonass. This means if the drone goes with the wind, it probably won't keep the same position, you will have to readjust the flight path of the drone.

Aircraft (ICAO)	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the Earth's surface.
Airframe	The airframe is the integral and physical structure of the UAV required to achieve controlled flight.
All Up Weight (AUW)	Total weight of the aircraft including battery and other parts.
Almost Ready to Fly (ARTF)	Sometimes also known as ARA – drone package includes everything but might require some assembly. Usually means that receiver is not included.
Altitude Hold (AH)	Height maintenance of the drone – uses Barometric Altimeter sensor.
Auto Levelling	Flight mode that allows the aircraft to stay level and it uses Accelerometer / gyroscope to achieve this.
Autonomous Aircraft	An unmanned aircraft that does not allow pilot intervention in the management of the flight. It is a subcategory of unmanned aircraft (UA).
Autonomous Flight	Flight path guided by GPS Waypoints.
Autonomous Operation	An operation during which a remotely-piloted aircraft is operating without pilot intervention in the management of the flight.
B	
Barometric Altimeter (BARO)	Altitude measurement sensor – uses barometric pressure – same as the transmitter – controls the drone/quadcopter in flight from the ground.
Battery	Various types of batteries are used on drones. An on-board battery or cartridge style battery may power the flight controller, the receiver or video transmission equipment.
BeiDou	Chinese Navigation satellite system that consists of two difference satellite constellations.
Bind	Procedure for linking the controller to the drone.
Bind aNd Fly (BNF)	Bind-N-Fly products come with everything you need except for a transmitter to control the drone. With BNF products you can use the transmitter of your own pick and bind it to the receiver included with the drone.

Brushless Motor	A brushless motor has permanent magnets which rotate around a fixed armature eliminating problems associated with connecting current to the moving part. The brushless motors are far more efficient and durable than brushed motors due to no friction thus reducing noise output, increasing reliability.
BVLoS	Otherwise known as <i>Beyond the Visual Line of Sight</i> . This refers to drone flights that are being performed beyond the pilot's visual line of sight. In most countries, this is not allowed or highly restricted without permission. The current UK rules state that drone operations must be carried out within normal visual line of sight – up to 400ft (122m) high and 500m in every direction.
C	
Centre of Gravity (CG or CoG)	The average centre balance point of your drone.
Channel	This can refer to the frequency a video transmitter is using or an assigned function linking a controller-transmitter with a drone. For instance, a channel may be assigned to control the throttle, or turning navigation lights on and off. Most drones use at least 6 channel for control.
Controlled Airspace	Airspace type of air of defined dimensions within which air traffic control service is provided to IFR flights and VFR flights by the airspace classification.
Controlled Zone (CTR)	Controlled zone of a certain area up to a certain predefined altitude.
Controller	The controller is the handheld device used by the drone pilot to control the quadcopter. Controllers are also called transmitters.
Command and Control Link (C2) (ICAO)	The data link between the remotely-piloted aircraft and the remote pilot station for the purposes of managing the flight.
Counter UAV (C-UAV)	Counter-Drone technology, also known as Counter-UAS (C-UAS) or Counter-UAV (C-UAV) technology, refers to systems that are used to detect and / or intercept unmanned aircraft. See also DTI.
D	
Descent Speed	This is the speed that the drone descends from the sky. For example the drone has a descent speed of 3 metres per second (m/s).

Detect and Avoid (ICAO)	The capability to see, sense or detect conflicting traffic or other hazards and take the appropriate action. Sense and avoid provides the functions of self-separation and collision avoidance to establish an analogous capability to “see and avoid” required manned aircraft.
Detect, Track and Identify (DTI)	A real-time method to Detect and Track moving objects, including UAVs, using a single or array of sensors and then to identify.
DJI Aeroscope	Aeroscope is DJI’s counter drone technology. By intercepting the current communications link between a DJI drone and its remote controller, Aeroscope is able to broadcast real-time identification information including UAV serial code, make and model, UAV position, speed, latitude and ground controller location.
Drone	The common term utilized to define unmanned aerial vehicles, or UAVs. These cover many different types of an unmanned aeroplane or various sizes that are made use of for multiple factors, from armed forces planes to hobbyists taking amateur digital photography. UAVs are additionally called remotely piloted aircraft, or RPA.
DSM / DSM2 / DSMX	Spektrum, an RC equipment maker, refers to their proprietary technology as “Digital Spectrum Modulation.” Each transmitter has a globally unique identifier (GUID), to which receivers can be bound, ensuring that no transmitter will interfere with other nearby Spektrum DSM systems. DSM uses Direct-Sequence Spread Spectrum (DSSS) technology.
DSSS	Direct-Sequence Spread Spectrum is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that modulates the carrier or broadcast frequency. The name ‘spread spectrum’ comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device’s transmitting frequency.
E	
Electromagnetic Interference (EMI)	Electrical interference – sometimes from outside sources.
Electronic Speed Control (ESC)	Device to control the motor in an electric aircraft, translating signals from the flight controller to the motors governing speed and rotation direction. Usually includes a BEC, or Battery Elimination Circuit (BEC), which provides power for the RC system and other on-board electronics, such as an autopilot.

Electronically Erasable Programmable Read Only Memory (EEPROM)	Electronically Erasable Programmable Read Only Memory. A type of non-volatile memory used in computers and other electronic devices to store small amounts of data that must be saved when power is removed, e.g., static calibration/reference tables. Unlike bytes in most other kinds of non-volatile memory, individual bytes in a traditional EEPROM can be independently read, erased, and re-written.
Elevator (ELEV)	Also known as “Pitch”, please refer to its definition.
EVLOS	Extended Visual Line of Sight. A form of enhanced operation above the basic rules, most commonly using a person as a spotter who is based at the maximum length of LOS from the pilot under jurisdictional rules. For example, if the LOS limit of the drone is 500m from the pilot, then a spotter stands 500m away from the pilot in the direction of the drone’s flight path, and therefore when the drone reaches 500m the spotter can effectively extend the LOS another 500m, so providing the pilot with 1km of LOS. The spotter would usually have communication with the pilot to inform of the drone’s behaviour, however, the spotter may also have a remote control to take over operation of the drone, and so the pilot may then travel 500m beyond the spotter, and so on and so forth.
F	
Field of View (FOV)	A measurement how much environment you can see through a camera lens. Usually measured in degrees.
First Person View (FPV)	Wireless connection with the drone’s camera to a screen either on the controller or an attached screen (smartphone or tablet) – you see what the drone sees. There is some debate that this also implies that an experienced pilot can let the UAV leave their line of sight, although this is debatable and caution ought to always be utilized.
Flight Controller	Microprocessor controller or “Brain” of the drone which controls flight.
Flight Envelope	Ranges of manoeuvrability where limits of roll, pitch and yaw attitude are set to protect the stability of an aircraft.
Fly Away	Fly away refers to UAV flight that’s not controlled by the operator. Fly aways can often be caused by external electronic / magnetic interference. Some UAVs are manufactured with fly away protection systems. In case of loss of control, the drones GPS position system can make it return safely to the start position.

Frame	See "Airframe".
Frequency Hopping	The transmitted signal changes frequency according to a certain hopping pattern and the advantage of this is the signal avoids the problem of failing communication on a particular frequency.
G	
Geofence	A virtual geographic boundary defined by GPS that enables the device to trigger a response when a device enters or leaves a particular area.
Gimbal	A specialized mount for a camera, which can swerve and tilt using servos. It allows the camera to stay in the same position, regardless of the drone's movement, making for a very still and smooth looking image.
Global Positioning System (GPS)	A series of satellites in close earth orbit which transmits signals that the drone, which when received, determines its position according to earth.
GLONASS	Globalnaya Navigazionnaya Sputnikovaya Sisyema or Global Navigation Satellite System. GLONASS is Russia's version of GPS (Global Positioning System).
Ground Control Station (GCS)	See 'Remote Pilot Station'. <i>Note: RPS is the preferred term as it enables the consistent use of one term with the same meaning irrespective of its location (e.g. on a ship or in another aircraft).</i>
Gyroscope	Provides an angular velocity around 3 axes of space in degrees to maintain the orientation of the quadcopter.
H	
Handover	The act of passing piloting control from one remote pilot station to another.
Heads Up Display (HUD)	A display that is shown directly in front of a pilot while flying a drone. HUD displays may include overlaid telemetry data such as altitude, speed, drone angle, compass heading and GPS coordinates. See also On Screen Display (OSD).
Hexacopter (Hexa)	A multirotor aircraft that uses six rotors for air travel.

Home Location	Home location is either the take-off location that is stored in the drone or the registered location that has been set by the user. This is utilized when the user triggers a Return to Home (RTH) command either due to low battery, failsafe RTH when a drone loses signal with the controller for 3 seconds, or Smart RTH when the user presses the Home button on the controller or the application.
Hovering Time	Hovering Time is a term used which illustrates how long the drone can hover in the sky when not in motion. The hovering time varies depending on the weight of the payload, the heavier the payload, the lesser the hovering time.
I	
IP Rating	An IP rating is used to define levels of sealing effectiveness of electrical enclosures against intrusion from foreign bodies (tools, dirt etc.) and moisture. For example; IP65 Enclosure – IP rated as “dust tight” and protected against water projected from a nozzle.
Inertial Measurement Unit (IMU)	Accelerometer plus a gyro attached to the controller for orientation and stabilization usually has at least three accelerometers (measuring the gravity vector in the x, y and z dimensions) and two gyros (measuring rotation around the tilt and pitch axis). Neither are sufficient by themselves since accelerometers are thrown off by movement (i.e., they are “noisy” over short periods of time), while gyros drift over time. The data from both types of sensors must be combined in software to determine right aircraft attitude and movement.
L	
Landing Gear	Most drones have a fixed landing gear, which will also be retractable to allow for a full 360-degree view in-flight. Fixed-wing drones don't have landing gear as they land perfectly fine on their belly.
Lithium Polymer Battery (LIPO)	Variants include Lithium Ion (Li-Ion) battery. This battery chemistry offers more power and lighter weight than NiMh and NiCad batteries.
Line of Sight (LOS)	Shorthand for the view, which is a crucial regulation in flying a UAV; if the aircraft is not in your sight, then it is prone to loss of control resulting in individual or property damage.
Lost Link (ICAO)	The loss of command and control link contact with the remotely-piloted aircraft such that the remote pilot can no longer manage the aircraft's flight.
M	

Magnetometer	Electronic compass that flight controller uses to know which direction it is pointed in.
Multicopter	The general term referring to a drone that has more than one motor and propeller dedicated to providing lift and propulsion for the vehicle. Most common drones have 4 or more rotors, but can have any number upwards to 12 for example.
N	
Nano	A miniaturized drone, usually < 8 grams and often within a toy category.
No Fly Zone (NFZ)	A term that refers to areas that have governmental restrictions denying or disabling flight (see GeoFence) of UAVs above the predetermined area.
O	
Octocopter	A multicopter aircraft that uses eight rotors for air travel.
Operator (ICAO)	A person, organization or enterprise engaged in or offering to engage in an aircraft operation. <i>Note: In the context of remotely-piloted aircraft, an aircraft operation includes the remotely-piloted aircraft system.</i>
On Screen Display (OSD)	A way to integrate data (often telemetry information) into the real-time video stream the aircraft is sending to the ground.
P	
Payload	What the drone can carry / lift / drop / deliver.
PIC	Pilot in Command. The pilot who is legally responsible by being in control of the drone at the time.
Pilot	The person in direct control of the UA - See also 'Remote Pilot'.
Pitch	The angle of drone in flight – controls which arm is higher than the others.
Point Of Interest (POI)	This is the place that a UAV is supposed to reach. Alternatively, a point of interest could be an area that the camera on the UAV is supposed to capture footage of.
Power Distribution Board	A small printed circuit board used to organize power connections and distribute power between batteries, ESCs and other on-board systems. Not required for all drones, but is more common in hobby grade drones to keep cabling tidy.

Propellers	Also known as “Props”, these are what get the drone off the ground, and into the air. They spin in correlation to the pilot’s manual controls and depending on the intensity of the spin is what creates the intensity of the drone’s movement.
Proportional, Integral, Derivative Control (PID)	PID refers to the mathematical process that is used by a flight controller to achieve a stable power / response ratio in a drone’s motors. Adjusting PIDs can make a drone more or less responsive, but can also make it less stable.
Q	
QUAD / Quadcopter	A UAV rotorcraft that is likewise called a quadrotor helicopter. These aeroplanes are made of a more straightforward layout than a similar sized remote helicopter and are pushed by 4 blades instead of two.
R	
Radio Line-Of-Sight (RLOS)	A direct, unobstructed, electronic point-to-point contact between a transmitter and a receiver.
Radio Controlled (RC)	Which is how drones receive flight instructions using radio signals. The ground-based pilot may use a hand-held unit like a game controller or, if the UAV has Wi-Fi capabilities, a computer or tablet can be used.
Ready To Fly (RTF)	Refers to drones or quadcopters that have everything you need, “in the box”, to start flying. The kit should include the drone, batteries, instruction manual, controllers, and any other equipment required to fly the drone.
Receiver	In general terms, the radio on the drone that receives commands from the operator’s transmitter. A receiver may also refer to the video / goggle setup a First Person View (see FPV) that the operator will use to receive real-time video information from the drones.
Received Signal Strength Indicator (RSSI)	The strength of radio signal from the controller to drone.
Return to Home (RTH)	Return the drone to the “home” position where it took off.
Revolutions Per Minute (RPM)	The number of times the drone’s motor shaft rotates a full cycle in 60 seconds.

Remote Pilot (ICAO)	A person charged by the operator with duties essential to the operation of a remotely-piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.
Remote Pilot Station (RPS)	The component of the remotely-piloted aircraft system containing the equipment used to pilot the remotely-piloted aircraft.
Remotely Piloted Air System*	An unmanned air system includes a number of elements such as the ground-based control unit, ground launch system and the Remotely Piloted Air Vehicle (RPAV) and all associated flight safety-critical elements.
Remotely-Piloted Aircraft (RPA) (ICAO)	An unmanned aircraft which is piloted from a remote pilot station.
Remotely-Piloted Aircraft System (RPAS). (ICAO)	A remotely-piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components as specified in the type design.
Roll	Flight term for rotation along an axis. Provides side to side motion of the drone.
Rotorcraft	An airborne car that gets its lift as well as propulsion from rotor blades, as opposed to the deal with wings that can be discovered on a plane. When a rotorcraft has two or more blades supplying propulsion, it is known as a multicopter aeroplane.
RPA Observer (ICAO)	A trained and competent person designated by the operator who, by visual observation of the remotely-piloted aircraft, assists the remote pilot in the safe conduct of the flight.
RPAS Commander*	RPAS Cdr is responsible for the conduct and safety of a specific flight and for supervising the person in direct control of the RPAS. His duties are equivalent to those of an Aircraft Commander.
RTK	RTK stands for <i>real time kinematics</i> . This is a satellite navigation technique that is used to enhance the precision of position data derived from satellite based precision systems such as GPS.
Rudder	Same as YAW – controls which direction the drone is flying.
S	
Sense and Avoid (SAA)	See 'Detect and Avoid'.

Servo	A mechanical device sometimes used on vehicles to move physical surfaces or items on the drone. Most drones do not require servos on board because their motions are controlled by changing speeds on each of the rotors. A servo is more relevant on fixed wings or servo controlled gimbals.
Small Unmanned Aircraft (SUA)	Any unmanned aircraft, other than a balloon or a kite, having a mass of not more than a specified weight limit depending on country without its fuel but including any articles or equipment installed in or attached to the aircraft at the commencement of its flight.
Small Unmanned Surveillance Aircraft (SUSA)	A small unmanned aircraft which is equipped to undertake any form of surveillance or data acquisition.
Swarm	A swarm is a technically termed as a group of UAV aircraft driven by artificial intelligence. Swarming drones communicate with each other while in flight and can respond to changing conditions autonomously. A good analogy would be a dense flock of starlings reacting to a sudden threat like a hawk. The entire flock manoeuvres like a single organism. A swarm is not to be confused with a group of UAVs flying together in formation and acting individually autonomously.
T	
Telemetry	Data referring to all aspects of a flying drones. Speed, altitude, pitch, roll, yaw, battery life, position etc.
Thermal	Thermal cameras allow you to collect thermal imaging and data. This can be used for industrial building inspections, to monitor crop defects, and more traditional methods such as tracing life in emergency situations.
Throttle	Controls the speed – revolutions (RPM) of the propellers / motors. This in turn when interpreted by the flight controller can alter the drone’s altitude or directional path for example.
Transmitter	Same as a controller – controls the drone in flight from the ground.
Trim	An adjustment used to alter the baseline of a joystick on a control transmitter. If a drone has a tendency to ‘drift’ in one direction when a joystick is left untouched, the operator may ‘trim’ the stick so that the drone will stay in place even when the operator is not touching the controller.

Tripod mode	A very slow and stable mode, ideal for shooting low to the ground, as well as close-up action shots. It's a very precise style of filming and is used frequently by cinematographers and photographers in their work.
U	
UAS-p <i>(legacy term)</i>	See 'Pilot'.
UAV Pilot/UAV-p <i>(legacy term)</i>	See 'Pilot'.
Unmanned Aircraft (UA)	<p>An aircraft which is intended to operate with no human pilot on board, as part of an Unmanned Aircraft System. Moreover a UA:</p> <ul style="list-style-type: none"> - is capable of sustained flight by aerodynamic means; - is remotely piloted or capable of autonomous operation; - is reusable; and - is not classified as a guided weapon or similar one-shot device designed for the delivery of munitions. <p><i>Note: RPA is considered a subset of UA.</i></p>
Unmanned Aircraft System	An Unmanned Aircraft System (UAS) comprises individual 'System Elements' consisting of the Unmanned Aircraft (UA) and any other System Elements necessary to enable flight, such as a Remote Pilot Station, Communication Link and Launch and Recovery Element. There may be multiple UAs, RPS or Launch and Recovery Elements within a UAS.
V	
VLoS	Otherwise referred to as <i>Visual Line of Sight</i> , and is essentially the opposite to BVLoS. This is how drone operators should operate, ensuring that their drone is well within their visual line of sight.
Vertical Take-off and Landing (VTOL)	Vertical take-off and landing is a valuable feature of quadcopters and other UAVs with multiple rotors. These aircraft can launch and vertically, which requires very little space. Fixed wing aircraft need a runway to take off and land.
Visual Line-Of-Sight (VLOS) Operation (ICAO)	An operation in which the remote pilot or RPA observer maintains direct unaided visual contact with the remotely-piloted aircraft.
W	

Waypoint	Set of three or more coordinates used to guide a drone along a predetermined flight path during autonomous missions.
Wide Open Throttle (WOT)	When the throttle stick on a controller is pushed all the way forward (full throttle).
Y	
Yaw	Flight term used to describe the rotation of a drone around its centre axis. Controls which direction the quadcopter is facing.



INTERPOL

