



## LJMU Research Online

**Al-Room, K, Iqbal, F, Baker, T, Shah, B, Yankson, B, Mac Dermott, A and Hung, P**

**Drones Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models**

<http://researchonline.ljmu.ac.uk/id/eprint/9945/>

### Article

**Citation** (please note it is advisable to refer to the publisher's version if you intend to cite from this work)

**Al-Room, K, Iqbal, F, Baker, T, Shah, B, Yankson, B, Mac Dermott, A and Hung, P (2021) Drones Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. International Journal of Digital Crime and Forensics (IJDCF). 13 (1). ISSN 1941-6210**

LJMU has developed [LJMU Research Online](#) for users to access the research output of the University more effectively. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LJMU Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain.

The version presented here may differ from the published version or from the version of the record. Please see the repository URL above for details on accessing the published version and note that access may require a subscription.

For more information please contact [researchonline@ljmu.ac.uk](mailto:researchonline@ljmu.ac.uk)


<http://researchonline.ljmu.ac.uk/>

# Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models

Khalifa Al-Room, Zayed University, UAE

Farkhund Iqbal, Zayed University, UAE


Thar Baker, Liverpool John Moores University, UK

 <https://orcid.org/0000-0002-5166-4873>

Babar Shah, Zayed University, UAE

Benjamin Yankson, University of Ontario Institute of Technology, Canada & Sheridan College, Canada

Aine MacDermott, Liverpool John Moores University, UK

 <https://orcid.org/0000-0001-8939-4664>

Patrick C. K. Hung, University of Ontario Institute of Technology, Canada

## ABSTRACT

Drones (a.k.a. unmanned aerial vehicles – UAV) have become a societal norm in our daily lives. The ability of drones capture high-quality photos from an aerial view and store and transmit such data presents a multi-facet problem. These actions possess privacy challenges to innocent users who can be spied on or drone owner's data which may be intercepted by a hacker. With all technological paradigms, utilities can be misused, and this is an increasing occurrence with drones. As a result, it is imperative to develop a novel methodological approach for the digital forensic analysis of a seized drone. This paper investigates six brands of drones commonly used in criminal activities and extracts forensically relevant data such as location information, captured images and videos, drones' flight paths, and data related to the ownership of the confiscated drone. The experimental results indicate that drone forensics would facilitate law enforcement in collecting significant information necessary for criminal investigations.

## KEYWORDS

Bebop Parrot, DJI Phantom3, DJI Phantom4, Drones, Forensic.Syma x5c, Xiang Yu

## 1. INTRODUCTION

Recently there has been a rapid growth in the interest of UAV technology. Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, are aircraft with no pilots that can be controlled either remotely or autonomously based on a pre-programmed flight path. Due to the varied uses in civil life, the technology once reserved for military use has evolved greatly. Such uses include area

DOI: 10.4018/IJDCF.2021010101

This article, published as an Open Access article on February 4, 2021 in the gold Open Access journal, International Journal of Digital Crime and Forensics (IJDCF) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

surveillance, inspection, surveying, unarmed cargo, and aerial photography. As airspace becomes more congested, the risk of collisions increases. Safeguards against drone incidents are likely to be considerably more challenging than for conventional aircraft. This increased congestion can result in high levels of signal interference, and hence generating unreliable and intermittent data and control-streams. In controlled airspace, drones create new challenges for the interactions between pilots and air traffic controllers (Matyszozyk, 2016).

Drones are becoming a popular thing to see in shared use space or whenever visiting public events. To most people, a drone is one of two very different types of pilotless aircraft: a toy, or a weapon. It is either a small insect-like device flying around in parks or on beaches or a large aircraft spying on civilians equipped with a weapon. The first category '*recreational drones*' is aimed at consumers. There were around two million items sold around the world in 2014, and this is increasing swiftly (Clarke & Moses, 2014). The second category, '*military drones*', accounts for nearly 90% of the worldwide sales of drones (Clarke & Moses, 2014).

The DJI Phantom 4, is one of the most popular drones on the market. The DJI Phantom 4 weighs 3 pounds in total and can fly at least 4 miles away from its operator without losing its video stream or remote controls. While the Phantom can carry just over 1 pound while in flight, its beefier brother, the DJI S900, has a maximum payload of just under 7 pounds. Anyone looking to spend about \$2000 dollars to purchase one can likely fly over a prison yard, and deliver a sizeable illicit contraband package to their friends on the inside (Fox News, 2017). Drones allow their users to accomplish certain tasks such as taking in aerial views, or hard to access spaces; which in the past has proven difficult due to physical restriction or barrier. The main motivation behind using drones in this manner is to explore a new way of gaining access to uncharted environments to capture (filming or taking pictures) or deploy resources.

The unique features of drone application are its' capacity to be deployed almost anywhere (in theory) to conduct reconnaissance, retrieve data or resources, deploy resources, and its flexibility in carrying different payloads. These functionalities explain why different agencies and organizations have looked towards implementing the use of drones within their services. For example, the American Red Cross is looking toward using drones in their search and rescue missions (McFarland, 2015; Preston, 2015). In the state of Virginia (USA), fire departments are considering the use of drones in the essence of spotting emerging fire and locating lost tourists (Preston, 2015).

With the ability to reach places that cannot be accessed physically, and in a stealthy manner, the drone can be used to perform criminal activities for reconnaissance. For example, an enemy military intelligence can use drones to take pictures of sensitive local territories. Someone could use a drone to violate the privacy of other people by taking pictures of their own home backyard. On January 26<sup>th</sup> in 2015, a drone crashed on the White House lawn but the incident was ruled as an accident (Sanchez, 2015). This incident highlighted a clear vulnerability that a terrorist could have used the function of the drone, such as a camera to breach privacy. The matter is not only limited to the camera being used but also the drone could have been carrying a payload to commit the malicious act on the White House grounds. Such notable issues for the US government is drug smuggling using drones is an issue for the American and Mexican border since 2010 (Sanchez, 2015).

Several law enforcement agencies across the globe have identified the drone as the go-to machinery to infiltrate jails and drop contrabands. Small commercial drones are being used to lift packages containing illicit goods such as guns, to synthetic drugs into jails in Canada, USA, Russia, Australia, Greece, and England; where they threaten the security of the jail (Milmo, 2015) (Fox News, 2017). Recorded incidents include a 2011 incident where staff at a Moscow prison confiscated 700 grams of heroin dropped by a drone. In 2016, a riot broke out over a package dropped by a drone at Mansfield Correctional Institution (a prison in the state of Ohio, USA). The same year a drone was discovered dropping mobile phones, drugs, hacksaw blades, and other materials into a prison in the state of Oklahoma. The threat of drones is not just limited to prisons; countries across the globe are

on the lookout for terrorists and other criminal groups using this evolving technology to carry out deadly attacks (DroneShield, 2017).

The adverse use of drone technology to commit a crime is growing in prominence. With the recent overwhelming increase use of drones, the need for drone digital forensic analysis has become a necessity. Sparse research has been conducted in the field of digital forensic analysis on drones and much more work is required to create tools and techniques that will aid law enforcement in their investigation in drone-related crime in order to ensure public safety. If a crime is committed, and a drone is seized at the crime scene, the following questions need to be answered: Can we prove ownership? Can we link the drone to the crime or previous crimes? What activities has the device been involved in flight take-off information, in-flight information, and landing information? What information could be extracted from that specific drone to help law enforcement to relate it to the owner? For example, in 2016, two crewmembers of Canadian base airline Porter airways flying from Ottawa to Toronto Canada were injured, as they had to evade a drone. A similar incident occurred in May of that year which resulted in NORAD scrambling a pair of CF-18 fighter jets to intercept a drone on a flight path in Ottawa, Canada (Seymour, 2016). Both these examples show crimes been committed with drones, which should be investigated with the help of advances in drone forensics, and the culprit brought to justice; rather than current situation where most criminals are emboldened by

Although it is hard for the legislation to keep abreast with the current drone technologies changes and landscape. The use of drones is not yet regulated to ensure individual property rights and safety. Currently available information from most countries points to government effort in establishing laws that can control the rapid use of drones by civilians. There is more than one stakeholder involved in this process: the government at the federal, state and city/town levels, drone manufacturers, software vendors, and end-users all have their own motivations. As with any other emerging new technology, businesses want to manufacture and sell products unhindered by regulations, but regulators or law enforcement are interested in drafting regulation and enforcing compliance of the regulation to provide assurance to citizens (Strandage, 2017). For example, the United Arab Emirates (UAE) possesses some of the strictest drone laws; which includes requirements for drone operator: registering the drone, testing skill level of drone operator, and attaching a “sky commander” tracking device that records the height and speed of flight; which allows authorities to automatically check for offenses. Failure to register drone involves stiff fines of Dh20, 000. At the time of this research, fifty-seven commercial drone operators and about 1,000 hobbyists are registered with the Dubai Civil Aviation Authority (Badam, 2017).

The rapid evolution of drones for civilian applications has created several challenges: regulatory, safety, privacy, security, and the uncertain landscape for new business models. For a digital forensic investigation of drones, a few research papers have investigated the burden of exploring the drones from a technical perspective to the definefile system embedded on these devices; in order to help establish forensic liability in retrieving data from drones. As these laws are not consistent and have a challenge/gap in identify owner to the device, it is clear that there is a need for the ability to develop digital forensic analysis techniques with drones used in crime in a real-time scenario, which can significantly improve law enforcement. By performing digital forensic analysis on different types of drones commonly encountered by law enforcement, the aim is to establish a clear framework to follow when investigating and solving crimes aided by drones. The paper also discusses the legal efforts taken by authorities around the world to minimize the possibility of using drones in criminal activities and discuss further considerations in that regard.

The rest of the paper is organized as follows: the next section discusses the problem domain including the challenges facing digital investigators in drone forensics. Section 3 provides a detailed discussion on the novel methodological approach for the digital forensic analysis of a seized drone. The evaluation of the proposed model is discussed in Section 4. The paper concludes the research with future works in Section 5.

## **2. PROBLEM DOMAIN**

### **2.1. Drone Layout**

The main components, and the layout, of any drone found on the market today, are the same (i.e., the remote controller, the battery, and the storage device), however, some cutting-edge commercial drones will have some additional advanced components such as a remote control application. It is crucial to explore it works; and challenges an investigator my experience during forensic analysis of the various component.

### **2.2. Forensic Challenges**

To date, digital investigation processes have been dictated by the technology being investigated and the availability of tools to extract electronically stored information (ESI). The rise in drone usage and drone-related crimes poses a fundamental challenge to digital forensic investigations due to lack of well established procedures or framework for investigating drones. As per (Shrivastava, Approaches of network forensic model for investigation., 2017), it has become difficult to analyze crime that is related with technology due to multiplicity due to fast pace development and functionality. Most of the existing drone investigation procedures have been adopted from methodologies developed for tackling forensic analysis of other technologies, and investigators have to act under the assumption that the devices would store data in a similar manner. As a result, when the underlying technology of the target device changes, new procedures must be developed to ensure that the evidence being collected and analysed is done so in a forensically sound manner, and that all avenues of potential evidence are established. Many questions need to be answered before establishing the forensic framework to investigate and forensically analyse ESI of a technology such as a drone. Drones are considered a new challenge that has been added to the field of digital forensics. Comparing to traditional digital forensics, there is less certainty in where data originated from, and where it is stored, so data persistence may be a problem. Therefore, digital investigators need to spend more effort to understand every aspect that surrounds the drone. For instance, questions can relate to how, what, who, and where data is stored inside the drone. In considering drone forensics, the major questions that must be answered includes:

1. How could the data be acquired and captured?
2. Can the flight data be extracted?
3. Can the media files be taken by the drone be retrieved?
4. How to prove the ownership of the drone?

### **2.3. Data Acquisition**

One of the crucial steps in the field of digital forensics is acquiring the data in a forensically sound manner and determining the admissibility of such evidence in the court of law. Based on National Institute of Standards and Technology (NIST) guidelines, the method in which the data is acquired should be repeatable and authentic and maintain integrity. However, sometimes, the nature of the device cannot provide this opportunity due to the way it is built. There are various types of drone and each type differs than the other in the way possible to connect to this drone. Some may be via certain protocols FTP, Telnet, and others using a direct USB cable. Additionally, the permissions granted when accessing the drone differs from a brand to another, and often access is restricted to the media folder or to the system files as well. This means there are no current consistent means of conduct acquisition on drones and as such, each drone may need to be handled differently. Using innovative technologies, alongside the knowledge acquired from these studies as starting points for understanding drone infrastructures will help in answering these questions and guiding more knowledge of drone forensics.

## 2.4. Flight Data

To determine the flight path of the seized drone, or to prove if a drone has entered a restricted area, the flight data must be retrieved. Reconstructing the flight path of the drone can create a timeline of events but is challenging in practice as each drone type differs from the other in the way it records flight data. In addition, some may record flight data and others may not. To add to the complexity, there is an interest in some manufacturers heading towards encrypting their flight data; and restricting access to everyone except their technical team members who have the encrypting keys. Encryption and other anti-forensic techniques are commonly used by criminals trying to hide their ownership or to prevent digital investigators possessing their data. The main challenge here is not the complexity of accessing encrypted data, but rather where the drone lacks the ability to record flight data. This is the main reason why Grest calls for a GPS tracker to be installed on all drones used by the people (Grest, 2015). As per (Shrivastava, 2018), the changing scope of information processing at independent locations has made it more difficult to maintain confidentiality, integrity, and availability; while conducting an investigation and such in our view can be applied to drones.

## 2.5. Media Took by the Drone

The essence of violating the law is not restricted to the flight path of the drone; it may also include the photos and videos taken by the drone in which case it violates the privacy of others. Such privacy violation is well documented across the globe. For example, a man in Kentucky USA shot a drone with a shotgun because it was flying above his house and he saw that as a violation of his privacy (Frank, 2016). He was arrested for endangerment and criminal mischief, but later the judge dismissed all charges saying the drone was an invasion of privacy (Matyszozyk, 2016). Gair (Gair, 2015) also discusses an incident in Sydney, Australia, where a drone was hovering around the beach taking photos of people; but no one can identify the drone operator (Gair, 2015). Additionally, media content on the drone as a predictor of a privacy violation can provide a clue as to which the owner of the drone is, as within the photos resides some EXIF data that stores the location of the photo. This EXIF data can replace the essence of reconstructing the flight path from the flight data by reconstructing from the metadata stored in the photos.

## 2.6. Proving Ownership

In some cases, even when a drone involved in a crime is confiscated by an investigator, it is difficult to physically tie the drone to the owner of it; without plausible deniability by the owner, leaving the digital investigator with no choice but to forensically prove ownership. Another possible case is finding a drone at a crime scene - what digital forensic approach could be followed to find the owner of the drone? The ability to prove ownership of the drone depends on the way the drone is built (whether it records the information of the ground control station device or not). Sometimes, however, it is the other way around where the ground control station records the information of the drone. For some manufacturers, this feature is not available, because there is no mobile application to be used to control the drone and everything is restricted to the remote controller. The concept of proving the ownership of the drone is very crucial, therefore the importance of that was illustrated in one of the hearings in the House of Lords in the UK (House of Lords, 2015).

## 3. RELATED WORK

Based on the identified challenges illustrated in the section above, this reinforces the need to establish a comprehensive digital forensics methodological approach; which will allow investigators to secure, analyse, and present facts when drones are involved in a crime. Such '*facts*' includes determining whether a seized drone did cross into a restricted area via identification of GPS data; flight path analysis; study of any stored recorded media; determining ownership of the device. Part of this includes:

how do investigators gain consistent process of identifying and understanding of the forensically sound process for extracting and analyzing data to reconstruct drone-related events and possible identification of flight path and drone ownership. Kuchler (Kuchler, 2016) provided astonishing evidence about how attackers can fly drones closed by corporate buildings to intercept Wi-Fi signals, to intercept communication to launch an attack against a corporation network (Kuchler, 2016). This case that information security environmental control such where companies can landscape or housing data canters in hard to access spaces are now vulnerable to this new threat. In cases such as these, authorities must have the ability to confiscate drones and conduct a forensic analysis to identify and locate the owner of the drone used in such a malicious act.

Horsman (Horsman, 2015) demonstrates processes involved in conducting a digital forensic investigation on a Parrot Bebop 1 drone and the controller. Results from Horsman's work demonstrated the potential to conduct data acquisition from both the drone itself and the controller after it has been confiscated; and conducted analysis to identify flight path, date of recording, etc. Unfortunately, this research work provides no information about establishing drone ownership in cases where the drone has been abandoned without the controller (Horsman, 2015). In addition, this work is limited in scope as the focus was only on a single type of device and there is no guarantee the findings are transferable to other drone models.

Any drone can also be subject to an attack, and therefore being able to conduct an audit and forensic analysis of the internal workings of any drone is essential. The drone can be subjected to different types of attacks. In (Javaid, Sun, Devabhaktuni, & Alam, 2012), "*Cyber Security Threat Analysis and Modelling of an Unmanned Aerial Vehicle Systems*", three categorizations of different attacks which can be launch against drones is identified. As per the categorization provided by the author, confidentiality attacks span from unauthorized access to information by compromising or intercepting data sent between the drone and its controller (Javaid, Sun, Devabhaktuni, & Alam, 2012). Integrity attacks generally can be made possible through the modification of existing data on the drone or create new data onto the drone storage (Javaid, Sun, Devabhaktuni, & Alam, 2012). Availability attack includes jamming signal, falsifying signals, and Denial of Service (DoS) attacks.

The authors (Vattapparamban, Guvenc, Yurekli, Akkaya, & Uluagac, 2016) discuss the common cyber-attacks against drones including, but not limited to, de-authentication attacks, GPS spoofing attacks. In the de-authentication attack, the authors carried out a process using an attackers' machine and known the IP address of the drone controller. They showed a setup where the attacker's machine will send disassociated packets to the drone's controller to disconnect it from the drone, hence losing control of the drone. In such a situation, the attacker will have full control of the drone and can breach drone data confidentiality, integrity, availability, and where possible use the drone as attack machine on other entities (Vattapparamban, Guvenc, Yurekli, Akkaya, & Uluagac, 2016). Similarly, the authors' demonstrated GPS spoofing attack, by transmitting fake GPS coordinates to the control system of the drone, thereby allow the attacked or hijack the drone (Vattapparamban, Guvenc, Yurekli, Akkaya, & Uluagac, 2016). Iqbal et al. (Iqbal, et al., 2018) examine the Parrot Bebop 2 drone and the possibility of establishing ownership during a criminal investigation. The authors also proposed a small-scale drone ontology for modelling drone context data during a forensic investigation. However, the work was only limited to the Parrot Bebop 2 drone. Similarly, Bouafif et al. (Bouafif, Kamoun, Iqbal, & Marrington, 2011) present important results of a forensic investigation analysis performed on a test Parrot AR Drone 2.0. The authors present new insights into drone forensics to access the digital containers of an intercepted drone and retrieving all the information that can help digital forensic investigators establish ownership, recover flight data and acquire the content of media files. However, the authors failed to propose any standardized method or framework for conducting the digital forensic analysis.

Table 1. Drone brands

Drone Name	Manufacturer
DJI Phantom 3	DJI
DJI Phantom 4	DJI
Bebop Parrot Drone 1	Bebop
Bebop Parrot Drone 2	Bebop
Xiang Yu	Xiang Yu (Chinese)
X5c	Syma (Chinese)

#### 4. METHODOLOGY

To understand ESI extraction and analysis of drones, we have to keep in mind real-life crimes, and scenarios that will be encountered by law enforcement agencies. Drones can differ in technical specification, and identification. During -drone-related criminal investigation, the state of the drone at the crime scene can vary: from running state, crashed state, to an operational state. Each of these states requires investigation processes that differ from the other. Other than drone operation states and types, our examination will also cover the components of drones, such as camera, radio controller, and ground station device.

Drones have complicated structures; many innovative technologies can be embedded within, e.g., high-resolution zoom-able cameras, wireless RF antenna, recording devices, etc. Sensors come in many forms - sensors can be a camera, GPS sensor, temperature sensor, and other variations depending upon the device. The collected data can be saved on an SD memory card, or stored locally on the device. All these scenarios will be examined to find the possible extracted information.

In confiscating a drone, which is in an operational state, law enforcement can use a device such as DroneShield, which can be used to track the drone back to its pilot. Other devices such DroneGun jammer (in the RF-only mode) can trigger the drone to fly back to its point of origin, enabling whoever is flying the drone to be tracked. Additionally, DroneGun can also be used to bring drones out of the sky, making it easy for law enforcement to confiscate the device and conduct a required investigation (Matyszozyk, 2016). Table 1, presents a list of different drone brands and related manufactures. The main aim behind this technical exploration is to answer the following questions:

- Is it possible to retrieve the photos taken by the camera on the drone?
- Can the flight data be reconstructed to present the drone flight path?
- Will it be possible to link a drone to a suspect C&C device?

Answering the above questions is crucial in developing a robust digital forensic method to solve crimes committed using drones and provide timeline data. For example, if the photos taken by the drone could be retrieved, depending upon the scenario, law enforcement authorities can decide whether the pictures are a breach of privacy of other people, or even indicative of pictures taken of sensitive/restricted areas. The collected flight data (if available) can confirm if this specific drone was used to fly over a drone no-fly zone; hence the owner will be proven guilty. The last question addresses the case of finding a drone in a prohibited place. If the suspect C&C's device, in the hands of the forensic investigators, links him with that specific drone; it can serve as evidence in the proofing the suspect is guilty of the offense. Thus, he will be held accountable for his actions.

The components that will be examined are as follows:



- Drone (Aircraft)
- C&C device (Mobile or Laptop)
- Radio Controller
- Battery
- Wi-Fi Range Extender

The target exploration will be as follows:

- Flight Data
- Media stored in the drone
- Ownership of Data
- Communication between the remote controller and the drone

To address the problem of diversity in drones' brands, this paper will focus on more than one specific brand. The targeted brands due to their inherent popularity are presented in Table 1.

## 5. ANALYSIS AND RESULTS

It is essential to understand the features and specifications of each identified drone. This helps prepare an investigator to be ready to effectively work on its real-world drone crime related scenario. Table 2 presents specific attributes, generated from each drone documentation, of each device that could provide vital details to the digital forensic analyst and/or law enforcement.

The attributes to consider includes:

- **Max Flight Time:** Can help the law enforcement officials to understand and approximate the maximum time the drone can spend in the air, during flight.
- **Max Transmission Distance:** The maximum distance will help predict the location of the drone operator, hence setting a perimeter to search for the operator.
- **Operating Frequency:** In a scenario where disrupting the drone flight is the only viable option, it is essential to know the frequency. This knowledge will allow the authorities to disrupt those frequencies causing the drone to crash.
- **Connection With The Controller:** The connection between the ground control system and the remote controller can be via either Wi-Fi or direct cable connection. If connection via Wi-Fi is possible, the drone could be hijacked by the law enforcement officer, which will allow him to land it ending up the problems caused by that drone.
- **Mobile Application:** Some drones may have their designated application in which acquiring the application files synced with the ground control system (iPhone, tablet, iPad, etc.) will help retrieve some valuable information.
- **Storage:** In some instances, the issue with the drone could be the photo taken by it that exploits the privacy of others. Hence, knowing the location of storing the photo is vital. Moreover, photos taken by the drone camera most of the time will have EXIF information, including the longitude and latitude of the picture.
- **Flight Record:** One of the most important aspects, as mentioned before, is the flight record or the log which will allow the investigator to reconstruct the drone flight path and prove whether it was flying on a restricted area or not.

Table 2. Drone specification

Drone Type	DJI Phantom 3	DJI Phantom 4	Bebop Parrot Drone 1	Chinese Toy: Syma x5c	Chinese Toy: Xiang Yu
Max Flight Time	23 min	28 min	11 min	7 min	8 min
Max Transmission Distance				50 m	100m
Connection with the controller	Direct Cable	Direct Cable		None	None
Operating Frequency	2.400 GHz-2.483 GHz	2.400 GHz-2.483 GHz	2.4-5 GHz	2.4 GHz	2.4 GHz
Mobile Application	DJI Go	DJI Go		None	None
Storage	SD Card	SD Card	Internal Memory	SD Card	SD Card
GPS Mode	Yes	Yes	Yes	No	No
Flight Record	Yes	Yes	Yes	No	No

## 5.1. DJI Phantom 3

### 5.1.1. Targeting the flight data of UAV

Using the DJI GO app (DJI, 2018), any mobile device can be connected to the remote controller and extract the flight data stored in the drone, as shown in Figure 1 and 2. The drone keeps the data in a micro SD card installed under its hood. After connecting to the aircraft and opening the DJI GO application, an option “entering flight data mode” is found under Settings → Advanced Settings → Enter Flight Data Mode. The application will prompt the user to connect the aircraft to his/her computer device and extract all the flight data that was stored in this drone.

The drone will appear as a “DJI FLY LOG” drive on the user’s computer; where flight data can be extracted. All data recorded by the drone will be extracted unless the flight recorder was formatted.

The file extracted is a DAT file, as shown in Figure 3, which can be opened using WnHex editor. Analysis of the extracted data shows a retrieved the flight data, as well as the images taken through the flight, Figure 4.

There are many log viewer tools available online to analyze the flight data, but the confidentiality of your data is not assured. Fundamentally, there is no guarantee the developer of such a tool will not share your data. Many log viewer utilities are available, free to download and use such as DJI Log

Figure 1. DJI App on iPhone



Figure 2. iOS Permission window

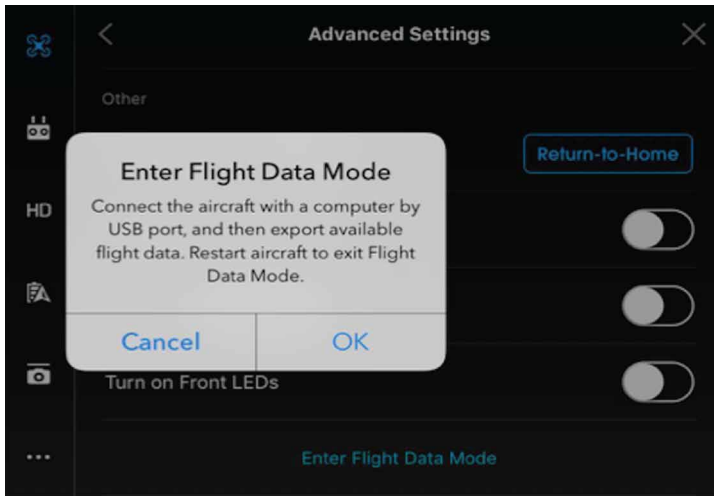


Figure 3. DJI Phantom 3 files

Name	Date modified	Type	Size
FLY065.DAT	1/23/2016 5:09 PM	DAT File	144,416 KB
FLY066.DAT	6/20/2016 3:21 PM	DAT File	21,696 KB
FLY067.DAT	6/20/2016 3:21 PM	DAT File	40,672 KB
FLY068.DAT	6/20/2016 3:21 PM	DAT File	41,568 KB
FLY069.DAT	6/20/2016 4:50 PM	DAT File	11,552 KB
FLY070.DAT	6/20/2016 4:50 PM	DAT File	16,864 KB
FLY071.DAT	6/20/2016 4:54 PM	DAT File	20,448 KB
FLY072.DAT	6/20/2016 4:55 PM	DAT File	108,320 KB
FLY073.DAT	6/20/2016 5:05 PM	DAT File	13,664 KB
FLY074.DAT	6/20/2016 5:05 PM	DAT File	67,264 KB
FLY075.DAT	7/23/2016 8:20 PM	DAT File	307,204 KB
FLY076.DAT	7/23/2016 8:20 PM	DAT File	233,120 KB
FLY077.DAT	7/29/2016 2:53 AM	DAT File	91,008 KB
FLY078.DAT	7/29/2016 3:03 AM	DAT File	8,864 KB
FLY079.DAT	7/29/2016 3:07 AM	DAT File	51,520 KB
FLY080.DAT	7/29/2016 3:16 AM	DAT File	55,008 KB
FLY081.DAT	7/29/2016 3:23 AM	DAT File	21,472 KB
FLY082.DAT	7/29/2016 3:28 AM	DAT File	29,504 KB
FLY083.DAT	7/29/2016 3:33 AM	DAT File	22,944 KB
FLY084.DAT	7/29/2016 3:51 AM	DAT File	8,512 KB
FLY085.DAT	8/15/2016 10:48 PM	DAT File	126,144 KB
FLY086.DAT	8/15/2016 10:48 PM	DAT File	3,040 KB
FLY087.DAT	8/15/2016 11:32 PM	DAT File	123,872 KB
FLY088.DAT	8/16/2016 10:25 PM	DAT File	13,420 KB

Converter and DatCon. Uploading the DAT file through DJI Log Converter can give a visualization of the drone’s flight data as is shown in Figure 4.

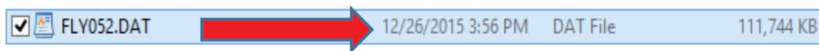
Nevertheless, the time of the flight can be identified through direct observation of the creation time of the DAT file, Figure 5.

Both the location and time of the suspected flight incident can be enough to compare to the findings mentioned above and decide whether the owner is the culprit of that specific incident.

Figure 4. Drone GIS information



Figure 5. DAT file creation date/time



### 5.1.2. Dealing With the Ground Control Station (Mobile Phone)

The above findings can be corroborated by the examination of the mobile phone used to operate the drone. The DJI GO application is used to control the drone and fly it above certain areas. This means that the application will store files on the mobile phone, analyzing those files will give us additional information. The application files related to the DJI GO app can be found on these specific locations:

- For iOS devices: Apps/DJIGo/FlightRecord
- For Android devices: DeviceStorage/DJI/dji.pilot/-FlightRecord

A phone was used to operate the drone. Post-event, using one of the dominant tools in the mobile forensic acquisition, the phone was acquired and analyzed, and the following application files were extracted.

The most important file we are concerned about when targeting the flight data is “DJIFlighRecord.txt”. As you can see above, the way the file is saved shows the data and time of the flight. For instance, “DJIFlightRecord\_2016-07-29\_ [03-28-52].txt” shows that the flight was recorded on 29/07/2016 at 3:28:52. Like the drone DAT file, the DJIFlightRecord.txt file can be analyzed by using some available tools such as DJI Log Converter, DatCon, and My Logs – Healthy Drones by Air Data UAV. Once the text file is uploaded to My Logs – Healthy Drones, the information of the flight can be presented as shown in Figure 6.

The flight related valuable information that could be obtained is flight time, location, path and duration of the flight.

### 5.1.3. Targeting the Ownership Data

When law enforcement suspects that someone is responsible for flying a drone in a restricted area, what can be done to link the suspect phone to the flying drone? The number that will relate the drone

Figure 6. Drone information visualized



to the ground control station (i.e., mobile device) could be the serial number of the remote controller used to control the drone, as is shown in Figure 7.

After identifying the remote controller serial number, it is highly probable that the serial number will be stored in one of the application files related to the app. Using any mobile acquisition tool, the application files related to the DJI GO application can be extracted, Figure 8. The file that we are concerned about is called `com.dji.pilot.plist`, which is one of the files listed in Figure 8. In this file, the serial number of the connected radio controller will be stored and by that, there is a definite link between the drone and the phone.

The following extraction, Figure 9, was completed by simply typing the serial number in the find tool within the Find tool.

However, using any *plist viewer*, you can open the `com.dji.pilot.plist` file and extract the `DJICModelName` as shown in Figure 10, where the C stands for the “controller”.

After finding the serial number of the drone’s radio controller, the phone under examination was used to control the drone. Hence, the owner of the mobile must be able to explain his link to the drone seized in the crime scene.

#### 5.1.4. Media Taken by the Drone

The media taken by the DJI Phantom 3 is simply stored on the SD card (not the same as the one that stores the flight data). By connecting the SD Card through a write-blocker device and acquiring it

Figure 7. Drone serial number

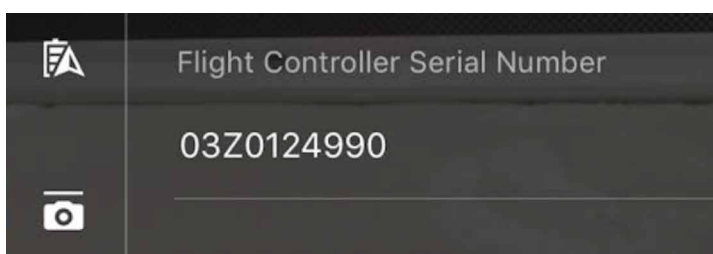


Figure 8. Drone extracted files

Name	Date modified	Type	Size
2016-08-14[14][03][26][367].txt	8/16/2016 2:31 PM	Text Document	1 KB
2016-08-15[00][17][51][308].txt	8/16/2016 2:31 PM	Text Document	1 KB
756452f888739715971a3f49027a57a	8/16/2016 2:31 PM	File	3 KB
Alvin	8/16/2016 2:31 PM	File	1 KB
archive	8/16/2016 2:31 PM	File	1 KB
BBCF6E1B939EA5AAE12F25D38AA517CA	8/16/2016 2:31 PM	File	3 KB
com.dji.pilot.plist	8/16/2016 2:31 PM	PLIST File	9 KB
com-facebook-sdk-AppEventsTimeSpent.json	8/16/2016 2:31 PM	JSON File	1 KB
com-facebook-sdk-PersistedAnonymousDJ.json	8/16/2016 2:31 PM	JSON File	1 KB
Cookies.binarycookies	8/16/2016 2:31 PM	BINARYCOOKIES ...	2 KB
datastore.sqlite	8/16/2016 2:31 PM	SQLITE File	72 KB
DJIFlightRecord_2016-07-23_[20-45-47].txt	8/16/2016 2:31 PM	Text Document	91 KB
DJIFlightRecord_2016-07-23_[20-48-42].txt	8/16/2016 2:31 PM	Text Document	18 KB
DJIFlightRecord_2016-07-23_[20-50-03].txt	8/16/2016 2:31 PM	Text Document	17 KB
DJIFlightRecord_2016-07-29_[03-17-14].txt	8/16/2016 2:31 PM	Text Document	53 KB
DJIFlightRecord_2016-07-29_[03-18-21].txt	8/16/2016 2:31 PM	Text Document	49 KB
DJIFlightRecord_2016-07-29_[03-19-29].txt	8/16/2016 2:31 PM	Text Document	62 KB
DJIFlightRecord_2016-07-29_[03-20-03].txt	8/16/2016 2:31 PM	Text Document	59 KB
DJIFlightRecord_2016-07-29_[03-24-00].txt	8/16/2016 2:31 PM	Text Document	18 KB
DJIFlightRecord_2016-07-29_[03-28-52].txt	8/16/2016 2:31 PM	Text Document	109 KB
E410B86E644AC1161D246AD8C864E2B	8/16/2016 2:31 PM	File	3 KB
IconState.plist	8/16/2016 2:31 PM	PLIST File	2 KB
JPUSHDocument	8/16/2016 2:31 PM	File	1 KB
learn_more.json	8/16/2016 2:31 PM	JSON File	2 KB

Figure 9. Discovered serial number in log file

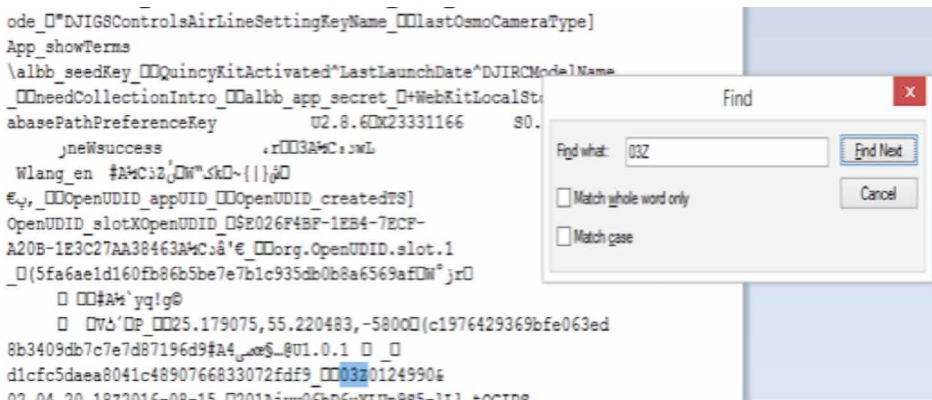
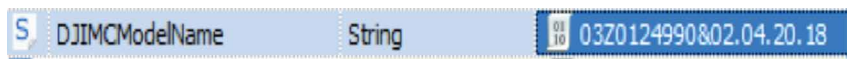


Figure 10. DJIMCModelName extraction



following simple forensic procedure, the photos and videos can be explored easily even deleted files could be retrieved using some forensic techniques.

### 5.1.5. Remote Controller Communication

In a scenario where someone is flying a drone within a restricted airspace, how can law enforcement confiscate the drone safely or crash-land it? In such a scenario, the communication between the radio controller and the drone should be targeted. In this experiment, the communication was identified to be through radio frequencies 2.4 GHz, so the convenient way to attack the drone is through disrupting the GPS signal. By using a device, which jams the GPS signal, controlling the flying drone becomes problematic and if it was flying in a windy weather, it might crash eventually.

## 5.2. DJI Phantom 4

### 5.2.1. The Drone

The first step that any law enforcement officer can do is to pinpoint the drone's serial number. Using this serial number, the authority can ask the DJI officials to identify the person whom this aircraft belongs to. The serial number could be found in the body of the aircraft as is shown below. It is important to note that a DJI aircraft cannot start flying unless it is being registered and tied to a specific account, which means that by identifying the serial number, Figure 11, the DJI officials can reveal the identity of the owner of this aircraft.

Figure 11. DJI Phantom 4 serial number



Note as well that the battery of the aircraft has its own serial number as shown in Figure 12.

Moreover, the remote controller has its own serial number as shown in Figure 13.

When connecting the drone via a USB cable, the operating system will recognize the drone as a removable media as shown in Figure 14.

Examining each media file can allow the examiner to identify the location where the media files were captured. The EXIF information embedded within the files are shown in Figure 15.

After identifying the longitude and latitude, it is a matter of plotting the numbers on the map and you will know the exact location.

There is no obvious way how to extract the flight logs, hence when connecting the aircraft to the PC, it will be recognized as a removable storage. Even when contacting the DJI support officials they have responded that there is no conceivable way of extracting the flight logs from the aircraft itself.

Figure 12. DJI Phantom 4 battery serial number



Figure 13. DJI Phantom 4 Controller serial number



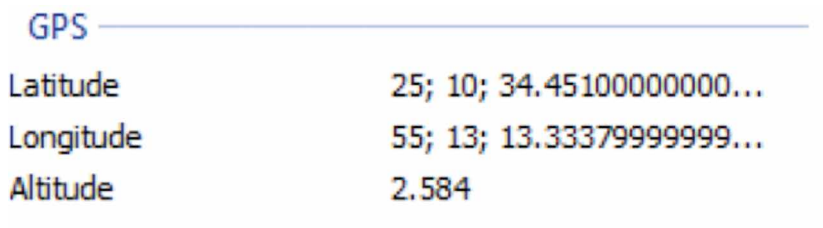
Figure 14. DJI Phantom 4 data files asa USB drive

This PC > Removable Disk (E:) > DCIM > 100MEDIA

Name	Date modified	Type	Size
DJI_0001.MOV	11/20/2016 12:02 ...	QuickTime Movie	3,469 KB
DJI_0002.MOV	11/20/2016 12:02 ...	QuickTime Movie	1,708 KB
DJI_0003.JPG	11/20/2016 12:02 ...	JPEG image	4,038 KB
DJI_0004.JPG	11/20/2016 12:03 ...	JPEG image	4,182 KB

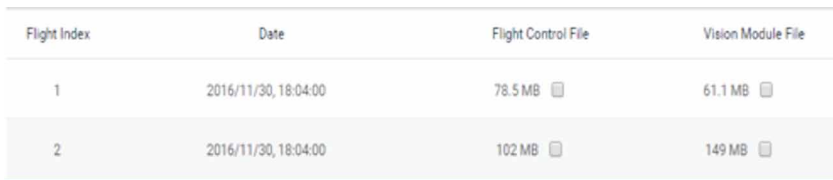


Figure 15. EXIF information



GPS	
Latitude	25; 10; 34.451000000000...
Longitude	55; 13; 13.333799999999...
Altitude	2.584

Figure 16. Flight Control file and Vision module file

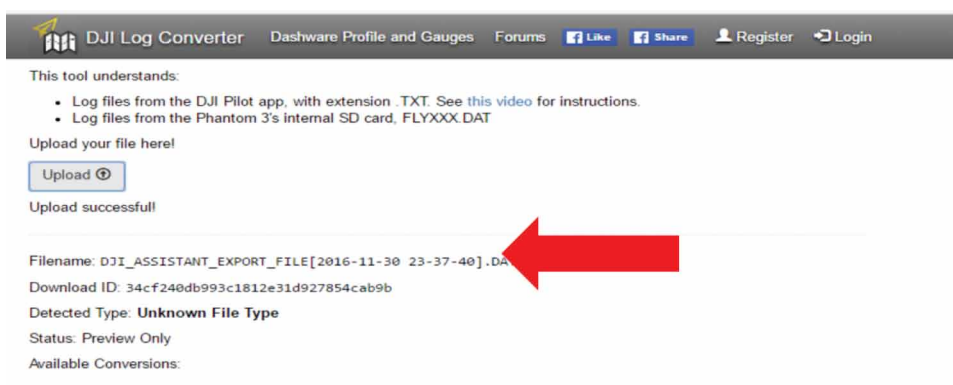


Flight Index	Date	Flight Control File	Vision Module File
1	2016/11/30, 18:04:00	78.5 MB	61.1 MB
2	2016/11/30, 18:04:00	102 MB	149 MB

However, some drone hobbyist refers to a software called DJI Assistant 2 that can help in extracting the DAT files, which store the flight log as we have experienced in the DJI Phantom 3. When connecting the aircraft through the DJI Assistant 2 tool, you can select the Flight Record tab and extract the flight log. Unlike the Phantom 3, the Phantom 4 stores two types of files, which are Flight Control file and Vision module file, Figure 16.

Unfortunately, the files are encrypted, as depicted in figures 17 and 18, and could not be converted using the previous tools. The only way to decrypt and interpret the files is by sending them to DJI support and ask for their assistance.

Figure 17. Drone encrypted files (McFarland, 2015)



### 5.2.2. SD Card

Examining an SD card will be a routine job for any forensic investigator as it takes no new techniques to approach the matter. The method followed when examining the SD card is tantamount to connect it through a write-blocker and performing a physical acquisition to obtain the logical as well as the

Figure 18. Drone encrypted files (Preston, 2015)

The screenshot shows a web application interface with several sections:

- .DAT file:** A red box with the text "Click here to specify .DAT file".
- Output Dir:** A text box containing "C:\Users\kha11fa ATRoom\Desktop" and a "View It" button.
- Time Axis:** A section with "Offset - time axis 0 point" and radio buttons for "Recording Start", "Motor Start", and "Flight Start". Below are "Lower" and "Upper" time input fields, and radio buttons for "Recording Start", "Motor Stop", "Recording Stop", and "GPS Lock".
- CSV:** A section with "Sample Rate" set to "30" Hz and a "View It" button. Radio buttons for ".CSV" and "Event Log (column in .csv)".
- Log Files:** Radio buttons for "Event Log File" and "Config Log File", each with a "View It" button.
- Dashware:** A red box with the text "Not Dashware compatible" and a "Make It Dashware Compatible" button.
- KML:** Radio buttons for "KML File", "Ground Track", and "Profile". The "Profile" option has a sub-section "Enter Home Point Elevation from Google Earth".

A red error message at the bottom of the interface reads: "Can't Go: .DAT file not specified, Lower is greater than Upper". Below this, a text box displays the error details: "C:\Users\kha11fa ATRoom\Desktop\DJT\_ASSISTANT\_EXPORT\_FILE[2016-11-30 23-04-04].DAT is not a .DAT file".

deleted data. Then, it is like the metadata extraction section mentioned above as the investigator will focus his aim to identify the location of the photos embedded within the photos itself.

### 5.2.3. Ground Control Station (Mobile Phone)

Before discussing what results could be extracted from the device used to operate the drone, it is important to note that as mentioned earlier that the application used to control DJI drones is DJI Go application. Updates designed for this application comes on a daily basis and the user is forced to update before he can fly the drone. This means that the results and findings that the forensic investigator suspects could be different after each update. During this study, the results have differed per device as they are not as expected with DJI Phantom 3.

When acquiring the mobile phone used to control the DJI Phantom 4, the application files were like the ones encountered in the DJI Phantom 3 Professional part. The location of the DJI Go application file is the same.

- For iOS devices: Apps/DJIGo/FlightRecord
- For Android devices: DeviceStorage/DJI/dji.pilot/FlightRecord

Like what was experienced in the DJI Phantom 3 case, the DJI Flight Record file, which holds the flight data, is also found as shown in Figure 19.

Uploading the DJI Flight Record to healthy drones site will present the below information in Figure 20. Once again, valuable information is extracted through this useful online tool and presented in a user-friendly way. Providing the law enforcement investigator, the opportunity to present that in a neat visualized manner to the court of law.

Figure 19. DJI Flight Record file



 DJIFlightRecord_2016-11-19_[23-51-26...	11/20/2016 6:37 PM	Text Document	79 KB
 DJIFlightRecord_2016-11-20_[00-02-15...	11/20/2016 6:37 PM	Text Document	307 KB

Figure 20. Visualization DJI Flight Record



The airmap\_flysafeplace.db file is within the application files here as well, like what has experienced in DJI Phantom 3 examinations. To establish the link between the mobile devices, which were used to control the drone, the com.dji.pilot.plist file was explored, however, the serial number was not found within the file itself (similar to the DJI Phantom 3).

What is found within the application file was the username used, which is pointed to in Figure 21, and eventually could be linked to the aircraft, as each aircraft must have a username linked to it before flying as mentioned before.

Note also that the location of the flight is logged through logging the longitude and latitude coordinates. More information could be extracted as the country name of the associated account from within the plist file, Figure 22.

#### 5.2.4. Remote Controller

To underline the possible way of hijacking a drone is to identify the way of communication between the controller and the drone. In the case of DJI Phantom 4, the mobile phone is connected through a USB cable to the remote controller; however, it is connected through radio frequencies between the controller and the drone. Analogous to the DJI Phantom 3, the DJI Phantom 4 will face flying issues if it is GPS signal becomes problematic.

Figure 21. Drone username in log file

```
oCameraType]
App_showTerms_[]needCollectionIntro_[]QuincyKitActivated
\albb_seedKey^LastLaunchDate^DJIRCMoelName_[]albb_app_secret_
[]+WebKitLocalStorageDatabasePathPreferenceKey
    U3.1.0X23331166[]80.0[]xy[] j{rWsuccess 3A[]c}>
    è[] Wlang_en_[]rakteam.zu.lab@gmail.com#A[]à[]ù[]P^[]W[]s^,[][]j[]+[]^[]%
    &[]@[]_[]OpenUDID_appUID_[]OpenUDID_createdTS]
    OpenUDID_slotXOpenUDID_[]
    $362DD31F-8C438-91B-87-9278C[] EDA04F3A[]c>
    x'[]»[]_[]org.OpenUDID.slot.0
    _[](5c964680c1a82e66f02eebb53003a46d9a9a1b26[]X0_[]_[] []
        [][]#A[]%[][]uM6r [] []X[]€^,
    ç[]_[]25.176242,55.220374,12510[](c1976429369bfe063ed8b3409db7c7
    e7d87196d9#[]A,[]
```

Figure 22. GIS Location information in-flight log file

```
è[]_[]0http://www.skypixel.com/user/rakteam/avatar/x128j*+, -z
$classnameX
$classesUNSURELç, KNSObject_[]800058805632307200WrakteamRAE_
[]United_Arab_[]
Emirates_[]rakteam.zu.lab@gmail.comRZu_[](9a4abe07763f46a2975356aa
bb29bd5f5406924978+*j_[]DJISkypixelProfileModel=9;,.
_[]DJISkypixelProfileModel_[]DJISkypixelBaseObjectXMTLModel_[]ONSK
```

### 5.3. Syma x5c Chinese Drone

Before exploring the forensic aspects of the drone, it is convenient to underline the reasons that may classify the drone as a popular drone, which make it a possible scenario to be faced by the law enforcement authorities in some concerning conditions. Syma X5c quadcopter could be purchased for a reasonable price of \$64. In addition, the quadcopter is extremely easy to use and some hobbyists refer to this drone as “the drone that could be used by your grandmother”.

#### 5.3.1. The Drone

The SYMA x5c does not store any flight data, so it would be impossible to reconstruct the flight path. The pictures and videos captured by the camera of the drone are stored in the SD card found in the drone.

#### 5.3.2. SD Card

The SD card could be examined using any forensic tool through a write-blocker device. After going through the pictures recorded by the camera, it is clear that there is no metadata stored within the picture, hence no location could be identified.

Note that the date of the picture is 2013 as shown in Figure 24 since the drone time is not accurate.

#### 5.3.3. Remote Controller

The communication between the drone and the remote controller is through radio waves. The controller operates over 2.4 GHz frequency, and through a blocking device, used to target this specific frequency the drone where not able to fly or its flight was considered problematic.

Table 3. Drone Overview

Name	Syma x5c Quadcopter
Price	\$64
Weight	915 Grams
Flight Time	7 minutes
Camera Resolution	2 Megapixel
Video Resolution	720p
Operating Range	50 meters
Operating Frequency	2.4 GHz
Battery Capacity	500 mA 3.7 V
Mobile Application	None

Figure 23. Drone image properties and values

Property	Value
<b>Image</b>	
Image ID	
Dimensions	2560 x 1440
Width	2560 pixels
Height	1440 pixels
Horizontal resolution	96 dpi
Vertical resolution	96 dpi
Bit depth	24
Compression	
Resolution unit	
Colour representation	
Compressed bits/pixel	
<b>Camera</b>	
Camera maker	
Camera model	
F-stop	
Exposure time	
ISO speed	

Figure 24. Drone acquired photos

This PC > Removable Disk (E:) > PHOTO

Name	Date modified	Type	Size
PICT0000.jpg	10/1/2013 12:00 AM	JPEG image	171 KB
PICT0001.jpg	10/1/2013 12:00 AM	JPEG image	242 KB
PICT0002.jpg	10/1/2013 12:00 AM	JPEG image	309 KB
<input checked="" type="checkbox"/> PICT0003.jpg	10/1/2013 12:00 AM	JPEG image	313 KB
PICT0004.jpg	10/1/2013 12:00 AM	JPEG image	312 KB
PICT0005.jpg	10/1/2013 12:00 AM	JPEG image	322 KB

Table 4. Xiang Yu drone Overview

Name	Yu Xiang 668-A3
Price	\$25
Flight Time	10 minutes
Operating Range	100 meters
Operating Frequency	2.4 GHz
Battery Capacity	380 mA 3.7 V
Mobile Application	None

#### 5.4. Xiang Yu drone (Chinese)

Similar to the Syma x5c drone, the Xiang Yu drone has many similarities with it especially the low price and the ease of use.

##### 5.4.1. The Drone

Unfortunately, the Yu Xiang drone does not store any flight data, which means that there it is impossible to reconstruct the flight path of the drone.

##### 5.4.2. SD Card

Similar to the Syma x5c drone, the pictures and videos are stored in the SD card found in the drone. The photos and videos, which are stored in the SD card, were extracted easily. However, there is no EXIF data that can find those media files.

##### 5.4.3. Remote Controller

Even the communication between the remote controller and the drone is through the radio frequency waves. Through using a device that jams radio frequency waves, the drone crashed immediately.

#### 5.5. Bebop Parrot Drone 1

##### 5.5.1. The Drone

The connection can be established to the drone through wireless via Telnet. After connecting, the flight data could be found under the academy folder in pud format. The file contains additional information in its metadata that includes the date and time of the flight and the serial number of the drone. Analysing the pud file can provide the investigator with the full flight path of the drone.

##### 5.5.2. The Ground Control Station

When dealing with the device used to control the drone, the investigator must focus on the application files associated with the application used to control the Bebop parrot drone, which is Freeflight3. Similar to the drone internal storage, the flight data is stored in the application files related to the Freeflight3 application. Depending on whether the controlling device is Android or iOS, the files could be found under these locations:

- Android: /data/data/com.parrot.freeflight3/files/academy
- iOS: /Applications/com.parrot.freeflight3/documents/academy

Similar to the drone the flight data is stored in a pud format, as well as the metadata associated with the file.

- **Media took by the drone:** In the media files (photos and videos), the ground control device has a direct access to the internal storage of the drone. The user can download or delete any media file from using the phone only. The media files can be founded by accessing the media folder.
- **Ownership Data:** To relate the ground control station to the concerning drone, the “com.parrot.freeflight3.plist” file must be examined. The file could be found in the following location:
  - Android: data/data/com.parrot.freeflight3/shared\_prefs
  - IOS: Applications/com.parrot.freeflight3/Library/Preferences

### 5.5.3. Remote Controller

The Bebop Parrot drone can be controlled using the ground control device only and without using a controller. Hence, it depends on the drone Wi-Fi network, which requires no authentication for connecting. The fact that it relies on this unsecured Wi-Fi network makes it vulnerable to any de-authentication attack, which will result in another device hijacking the drone and take control over.

## 6. CONCLUSION

With the continuing rise of drone usage within the public, the concerns including but not limited to privacy breaches, criminal and malicious usage of drones will rise. It is essential for the digital investigator to have the know-how and understand the crucial process, features and functionalities of drones to extract crucial forensic evidence about activities captured within the drone during an event involving the drone. Although different manufacturers introduce new drones constantly, as a result, some processes within this paper will need to be tweaked to meet the need of respective cases depending on the new drone model(s) the forensic investigator will need to deal with. Some drones may have the ability to record the flight data and keep the ownership data to identify the devices used to control the drone while other cheaper drones may lack this feature where the only thing that could be extracted from the drone is the media file. Those types of “cheaper” drones may replicate the idea of prepaid phones where it could be a problem to identify the owner of the device. Moreover, the location in which the drone was flying can be identified from the EXIF information founded in the media files.

To hijack the drone the investigator must identify firstly the way of communication between the controller and the drone or between the ground control station and the drone. Although, investigating and forensically processing data captured by different drones have been addressed; the lack of an already built digital forensic tool that covers all types of drones discussed and how to deal with the data extracted is an area that should be presented in the future. An open source tool could be introduced to aid digital forensics investigators in dealing with such devices. Moreover, the JTAG and chip off analysis could be explored. Hence, in the case of a damaged drone, this approach can help in reading the data more efficiently. Furthermore, more work could be done in this field to develop a tool to automate the process of examining and extracting information from the drone. The information presented from our experiments can be used to inform digital forensic investigators for future drone analysis. Future work involves collating this information and developing a clear process model for investigative processes and procedures to follow, taking into consideration the constraints identified during analysis, e.g. device condition, encrypted data, media ownership.

## REFERENCES

- Amato, A. (2014). *New Software 'Snoopy' Lets Your Drone Hack Smartphones*. Drone Life.
- Badam, R. (2017, April 11). *UAE drone users must register themselves and their device under strict new rules*. Retrieved April 22, 2017, from The National”, Thenational.ae: <http://www.thenational.ae/uae/uae-drone-users-must-register-themselves-and-their-device-under-strict-new-rules>
- Bento, M. D. (2012.). Unmanned Aerial Vehicles. *InsideGSS*, 54-61.
- Bone, E., & Bolkcom, C. (2003). *Unmanned Aerial Vehicles: Background and Issues for Congress*. Congressional Research Service: The Library of Congress.
- Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2011). *Drone Forensics: Challenges and New Insights*. ADFA.
- Bracken-Roche, C., Lyon, D., Mansour, M. J., Molnar, A., & A., S. (2014). *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles*. Kingston, Canada: Surveillance Studies Centre, Queen's University.
- Brodsky, I. (2016). 6 reasons why enterprise drones are on course. *Computerworld*.
- Cavoukian, A. (2012). *Privacy and Drones: Unmanned Aerial Vehicles*. Information and Privacy Commissioner of Ontario.
- Clarke, R., & Moses, L. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law & Security Review*, 30(3), 263–285. doi:10.1016/j.clsr.2014.03.007
- Kovar, D. (2015, December 3). *UAV (aka drone) Forensics*. Retrieved from [https://files.sans.org/summit/Digital\\_Forensics\\_and\\_Incident\\_Response\\_Summit\\_2015/PDFs/ForensicAnalysisofsUASakaDronesDavidKovar.pdf](https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/ForensicAnalysisofsUASakaDronesDavidKovar.pdf)
- DJI. (2018). Retrieved from <https://www.dji.com/phantom-3-standard/app>
- DroneShield. (2017, January 14). *How Prisons Can Combat Drone Threats*. Retrieved April 22, 2017, from <https://www.droneshield.com>: <https://www.droneshield.com/blog-content/2017/1/14/how-prisons-can-combat-drone-threats>
- Fox News. (2017, April 17). *Drones smuggling porn, drugs to inmates around the world*. Retrieved from <http://www.foxnews.com/us/2017/04/17/drones-smuggling-porn-drugs-to-inmates-around-world.html>
- Frank, M. (2016, February 10). *Drone Privacy: Is Anyone in Charge?* Retrieved from <http://www.consumerreports.org/electronics/drone-privacy-is-anyone-in-charge/>
- Horsman, G. (2015). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*.
- Gair, K. (2015, December 12). *Privacy concerns mount as drones take to the skies*. Retrieved from <http://www.smh.com.au/digital-life/consumer-security/privacy-concerns-mount-as-drones-take-to-the-skies-20151208-glijvk.html>
- Gertler, J. (2012). *U.S. Unmanned Aerial Systems*. Congressional Research Service.
- Grest, L. (2015, September 15). *Are We Ready For The Drone Revolution?* Retrieved from <http://www.smh.com.au/digital-life/consumer-security/privacy-concerns-mount-as-drones-take-to-the-skies-20151208-glijvk.html>
- Horsman, G. (2015). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digital Investigation*, 16, 1–16. doi:10.1016/j.diin.2015.11.002
- House of Lords. (2015). *Civilian Use of Drones in the EU*. Authority of the House of Lords.
- Humphries, M. (2011). *WASP: The Linux-powered flying spy drone that cracks Wi-Fi & GSM networks*. GEEK.
- Iqbal, F., Yankson, B., AlYammahi, M., AlMansoori, N., Qayed, S., Shah, B., & Baker, T. (2018). *Drone forensics: examination and analysis*. *Int. J. Electronic Security and Digital Forensics*.



Javaid, A., Sun, W., Devabhaktuni, V., & Alam, M. (2012). Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. In *IEEE Conference on Technologies for Homeland Security*. IEEE. doi:10.1109/THS.2012.6459914

Kovar, D. (2016, June 23). *UAV (aka drone) Forensics*. Retrieved from [https://files.sans.org/summit/Digital\\_Forensics\\_and\\_Incident\\_Response\\_Summit\\_2016/PDFs/UAV-Forensic-Analysis-Next-Gen-David-Kovar.pdf](https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2016/PDFs/UAV-Forensic-Analysis-Next-Gen-David-Kovar.pdf)

Kuchler, H. (2016, July 26). *Cyber experts warn of hacking capability of drones*, Retrieved February 2, 2017, from <https://www.ft.com/content/a06a1f5c-505f-11e6-8172-e39ecd3b86fc>

Matyszozyk, C. (2016, October 26). *Judge rules man had right to shoot down drone over his house*. Retrieved April 22, 2017, from CNET: 2017. Available <https://www.cnet.com/news/judge-rules-man-had-right-to-shoot-down-drone-over-his-house>

McFarland, M. (2015). *American Red Cross takes serious look at using drones for disaster relief, holds off for now*. Retrieved from [https://www.washingtonpost.com/news/innovations/wp/2015/04/21/american-red-cross-takes-serious-look-at-using-drones-for-disaster-relief-holds-off-for-now/?utm\\_term=.22a1dd4d98e5](https://www.washingtonpost.com/news/innovations/wp/2015/04/21/american-red-cross-takes-serious-look-at-using-drones-for-disaster-relief-holds-off-for-now/?utm_term=.22a1dd4d98e5)

Milmo, C. (2015, September 16). *Drones used to deliver illicit goods to prisons*. Retrieved April 21, 2017, from <http://www.independent.co.uk/news/uk/crime/drones-operated-by-criminal-gangs-used-to-deliver-drugs-mobile-phones-and-potentially-firearms-to-10504154.html>

Paganini, P. (2015). *Hacking drones by exploiting design flaws*. Security Affairs.

Preston, I. (2015, April 8). *Carova volunteer fire department deploying drone to help spot fires*. Retrieved from <http://wtkr.com/2015/04/08/carova-volunteer-fire-department-deploying-drone-to-help-spot-fires/>

Rao, B., Gopi, A., & Maione, R. (2016). The societal impact of commercial drones. *Technol. Soc.*, 45, 83–90. doi:10.1016/j.techsoc.2016.02.009

Sanchez, A. (2015, February 2). *Worst Case Scenario: The Criminal Use of Drones*. Retrieved from <http://www.coha.org/worst-case-scenario-the-criminal-use-of-drones/>

Seymour, A. (2016, November 14). *Near-collision with possible drone injures crew members on Porter flight from Ottawa*. Retrieved April 23, 2017, from <http://ottawacitizen.com/news/local-news/flight-crew-injured-after-near-collision-with-suspected-drone>

Shrivastava, G. (2017). Approaches of network forensic model for investigation. *International Journal of Forensic Engineering*, 3(3), 195–215. doi:10.1504/IJFE.2017.082977

Shrivastava, G. (2018). Investigating New Evolutions and Research in Digital Forensic & Optimization. *Recent Patents on Engineering*, 3-4.

Strandage, T. (2017, June 08). *Civilian Drones*. Retrieved from Economist: <https://www.economist.com/technology-quarterly/2017-06-08/civilian-drones>

Vattapparamban, E., Guvenc, I., Yurekli, A., Akkaya, A., & Uluagac, S. (2016). Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety. In *International Wireless Communications and Mobile Computing Conference (IWCMC)*. IWCMC. doi:10.1109/IWCMC.2016.7577060

*Khalifa Mohammad AlRoom has been working in the Digital Forensic Department at Dubai Police General Head Quarter in United Arab Emirates since 2013. Khalifa Mohammad graduated as an electronics engineer and has an MSc in Cyber Security from Zayed University (1st degree with honors). He has worked in different cases involving a diversity of electronic devices. Moreover, Khalifa has an interest in the field of cyber security and has participated in numerous occasions as a penetration tester. In addition to his main role as a digital forensic examiner, Khalifa has helped organize various events as part of his social responsibility toward the community.*

*Farkhund Iqbal holds the position of Associate Professor and Director Advanced Cyber Forensics Research Laboratory in the College of Technological Innovation, Zayed University, United Arab Emirates. He holds a Master (2005) and a Ph.D. degree (2011) from Concordia University, Canada. He is using machine learning and Big Data techniques for problem solving in healthcare, cybersecurity and cybercrime investigation in smart and safe city domain. He has published more than 50 papers in peer-reviewed high ranked journals and conferences. He is an affiliate professor in school of information studies, McGill university, Canada and Adjunct professor in Adjunct Professor, Faculty of Business and IT, University of Ontario Institute of Technology, Canada. He is the recipient of several prestigious awards and research grants. He has served as a chair and TPC member of several IEEE/ACM conferences, guest editor of special issues and reviewer of high rank journals. He is the member of several professional organization including ACM and IEEE Digital society.*

*Thar Baker is a Senior Lecturer in Software Systems Engineering in the Department of Computer Science at Liverpool John Moores University, UK. Dr Baker has published numerous refereed research papers in multidisciplinary research areas including Cloud Computing, Distributed Software Systems, Algorithm Design, Green and Sustainable Computing, IoT, and Autonomic Web Science. He has been actively involved as a member of editorial board and review committee for a number of peer-reviewed international journals and is on the program committee for a number of international conferences. He is a fellow member of the British Higher Education Academy.*

*Babar Shah is an Assistant Professor in the College of Information Technology at Zayed University. Dr. Babar Shah received his PhD on the topic of energy efficient wireless and mobile communication from Gyeongsang National University, where he studied at the Department of Informatics. He holds two Master degrees, Master in Computer Networks from Derby University, UK (2007) and Master in Computer Science from Peshawar University, Pakistan (2002). Dr. Babar's research interests center Wireless and Mobile Communications, Peer-to-peer Networks, Communication in 3D WSNs, IOT and smart technologies. He is also interested in other aspects of informatics and has published many articles in this area.*

*Benjamin Yankson is a Faculty member at Sheridan College's School of Applied Computing (Ontario, Canada), and currently working towards his PhD at University of Ontario Institute of Technology (UOIT). He holds a Master degree in Information Systems Security from UOIT (2013), a Microsoft Certified Professional (MCP), and a Comptia Security+ certification. His research and teaching interests includes: Security and privacy of smart connected devices; Digital forensics; Information Systems Risk Management; and Information System Security Auditing. Prior to academia, Benjamin spent 10+ years in various Technical leadership, and Security roles within Healthcare IT, and Education.*

*Áine MacDermott is a Senior Lecturer in Cyber Security and IoT in the Department of Computer Science at Liverpool John Moores University (LJMU) in the UK. She received her PhD in Network Security from Liverpool John Moores University in 2017, and a first class BSc (Hons) in Computer Forensics in 2011. Previously Áine worked as an Associate Tutor in Computing at Edge Hill University for two academic years. Academic research interests include the Internet of Things, critical infrastructure protection, computer network security, collaborative intrusion detection in interconnected networks, and digital forensics – over 20 academic papers have been published to date, presenting and exhibiting both nationally and internationally.*

*Patrick C. K. Hung is a Professor and Director of International Programs at the Faculty of Business and Information Technology in University of Ontario Institute of Technology, Canada. He currently works with the College of Technological Innovation at Zayed University on several smart city and cybersecurity research projects in the United Arab Emirates. He is also a Visiting Researcher at University of São Paulo, Brazil and National Technological University (UTN)-Santa Fe, Argentina. Patrick worked with Boeing Research and Technology at Seattle on aviation services-related research with two U.S. patents on mobile network dynamic workflow system. Before that, he was a Research Scientist with Commonwealth Scientific and Industrial Research Organization in Australia as well as he worked as a software engineer in the industry in North America. He is a founding member of the IEEE Technical Committee on Services Computing, and the IEEE Transactions on Services Computing. He is a Coordinating Editor of the Information Systems Frontiers.*