Article

UAV Forensics: DJI Mini 2 Case Study

Miloš Stanković [1,†] , Mohammad Meraj Mirza [1,2,*,†] and Umit Karabiyik [1]

1   Department of Computer and Information Technology, Purdue University, West Lafayette, IN 47907, USA; mstankovic@purdue.edu (M.S.); umit@purdue.edu (U.K.)
2   Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
*   Correspondence: mmmirza@purdue.edu
†   These authors contributed equally to this work.

Abstract: Rapid technology advancements, especially in the past decade, have allowed off-the-shelf unmanned aerial vehicles (UAVs) that weigh less than 250 g to become available for recreational use by the general population. Many well-known manufacturers (e.g., DJI) are now focusing on this segment of UAVs, and the new DJI Mini 2 drone is one of many that falls under this category, which enables easy access to be purchased and used without any Part 107 certification and Remote ID registration. The versatility of drones and drone models is appealing for customers, but they pose many challenges to forensic tools and digital forensics investigators due to numerous hardware and software variations. In addition, different devices can be associated and used for controlling these drones (e.g., Android and iOS smartphones). Moreover, according to the Federal Aviation Administration (FAA), the adoption of Remote ID is not going to be required for people without the 107 certifications for this segment at least until 2023, which creates finding personally identifiable information a necessity in these types of investigations. In this research, we conducted a comprehensive investigation of DJI Mini 2 and its data stored across multiple devices (e.g., SD cards and mobile devices) that are associated with the drone. The aim of this paper is to (1) create several criminal-like scenarios, (2) acquire and analyze the created scenarios using leading forensics software (e.g., Cellebrite and Magnet Axiom) that are commonly used by law enforcement agencies, (3) and present findings associated with potential criminal activities.

Keywords: DJI Mini 2; forensic case study; forensic practices; mobile forensics; UAV forensics; UAV forensics challenges

1. Introduction

According to [1], there have been dramatic advancements in the drone industry, and it is estimated that the market will reach nearly USD 60 billion by 2025. Moreover, it is predicted that shipments of consumer drones will grow to USD 29 million by 2021. Additionally, the increased demand for drones in the public and private sectors is predicted to be worth around USD 100 billion in the future. To put it in perspective, in 2020, consumer drones in the United Stated sales were over USD 1.25 billion [1].

On the other hand, 367 illegal activities were reported between October 2020 and December 2020 in the USA alone by the Federal Aviation Administration (FAA) [2]. Considering that the reported number is only what was reported by the FAA, it is safe to assume that the number is much greater than noted. As there are many types of drones that are involved in many of the incidents, the FAA has reported that they are working closely with law enforcement to investigate and identify these incidents [2].

Previous research has looked into multiple variations of DJI drones (e.g., DJI Phantom series and Spark) as well as some other well known manufacturers. The studies were comprehensive and provided a body of knowledge with an adequate amount of relevant content, which contributed to the unmanned aerial vehicle (UAV) forensic community.

However, there was a lack of literature supporting drones weighing less than 250 g (e.g., DJI Mini 2).

Our research aims to address the lack of comprehensive forensics methods on the DJI Mini 2 drone and its necessary operational software and controllers by performing extensive experiments with multiple criminal-like scenarios. Additionally, our conducted experiments consist of related mobile software (e.g., DJI Fly app) used to operate the drone, which is populated and then forensically analyzed.

The contributions of this research are as follows:

- Providing a comprehensive forensic investigation across multiple devices (e.g., drone body, SD cards, and mobile devices) associated with the drone.
- Analyze several criminal-like scenarios for the DJI Mini 2 drone in the real world, utilizing multiple devices.
- Testing the carrying capabilities of the DJI Mini 2 to evaluate its transporting performance for criminal activities, such as terrorist attacks and smuggling.

This paper is structured as follows: Section 2 discusses other researches and work that have already been done in the field of UAV/drone forensics. Section 3 demonstrates our methodology and the experiment design that was followed throughout the study. Section 4 highlights our findings, while Section 5 presents the discussion on the importance of our results. Finally, Section 6 concludes this research and provides direction for future work.

2. Related Work

As highlighted in [3], an ever-growing concern regarding UAVs would be the easy confiscation or loss of technology, as seen by drones being confiscated and thus privacy violations occurring due to the extraction of data from the device. Drones have been used as a mode of recreation, but there are many uses that companies and governments have found. Just as UAVs have the capability for good, such as collecting information to be used as evidence in lawsuits, they are easily used for malicious purposes, such as violating no-fly zones, illegal usage by criminals, or launch of areal missiles [3]. At the conclusion, the researchers were able to access the data on the Parrot AR Drone 2.0 used in their study and access the file system via multiple connection methods. This resulted in retrieving the controller's phone ID [3]. Based on the results shown in the paper, it was proposed to take the Parrot AR Drone 2.0 and other drones and analyze further to extrapolate the differences in the accessibility of data.

Moreover, researchers in [4] experimented using a DJI Spark drone in a criminal-like scenario while it is being controlled and linked to a mobile device. In this study, the mobile device utilized by the researchers was Android OS-operated, and they used DJI GO 4 application (app) v4.3.11, which was downloaded from the Android Play Store to control the drone. They found that the mobile device kept the flight data files under two recorded versions; the first is *.DAT*, and the other is in *.txt* files. Both formats along with media files taken during the flight were preserved under the DJI GO 4 package folder named *DJI/dji.go.v4*. They also were able to find a connection between all components they used for the study, including the drone, SD card, and smartphone, using temporal rules to determine their linkage [4].

Another recent study [5] has demonstrated a comprehensive forensic study on DJI Mavic Air 2, utilizing multiple devices and case scenarios in which the last was a crash landing. Researchers have dealt with the damaged drone and performed digital acquisition from different components that were used in the case study (e.g., smartphone, laptop, and drone body). In addition, the researchers took into consideration two possible acquisition methodologies, the first being chip-off and the second being chip-on techniques. As a result, they were able to discover a board serial number that is treated as Personal Identifiable Information (PII), which can be linked to the drone owner/operator [5].

Security issues continue to rise with the popularity of UAVs, and it is ever necessary for investigators to be able to forensically analyze devices used for malicious purposes [6]. As presented in [6], one of the primary obstacles comes from the complex and individualized

structure of the drone when performing forensics analysis. One proposed solution to the challenge was creating a framework that could aid forensics investigators by providing twelve steps of systematic analysis [6]. During the creation of the framework, five different models from multiple manufacturers were utilized. Once created, the researchers tested their proposed framework and found that it could be used for each model in the study to aid in an investigation.

In addition, researchers of [7] have highlighted some UAV forensic challenges that are associated with the tools and guidelines/frameworks used by investigators. To tackle some of the challenges they discussed, they have proposed a process that consists of 20 steps while demonstrating it using DJI Phantom 3 as a case study. Moreover, the proposed framework integrates the probability that the UAV is used in an illegal operation, whereas researchers of [8] have a proposed drone technical forensic investigation process that can be used in some cases. The authors have demonstrated the proposed investigation process using a Yuneec Typhoon H drone.

A recent study [9] that further explains the analysis of drones is known as the Drone Forensics discipline. This discipline is necessary due to the need for specialized tools and analysis as drones have many enhancements that create barriers during digital forensic analysis. Information can be lost if the examiners are not properly educated or equipped. The study [9] focused only on one manufacturer (DJI) but utilized various models to test and compare forensics tools. The methodology behind the approach was to discover which standards and procedures are best used in an investigation with DJI drones [9]. Tools of analysis were limited to Autopsy, Paraben's E3: Universal, and CsvView/Datcon. Despite the paper utilizing two web tools for additional data extraction at the end, it was not recommended due to the vulnerabilities and lack of reliability. It was found that file systems in different models of DJI drones contain the same standards for media files, EXIF data, spatial movement, metadata, and location [9].

Another very recent study [10] conducted on common drone models utilized in criminal activities demonstrates what information could be gathered to better inform a law enforcement investigation. From the six brands, investigators gathered such information as media files in the form of pictures and videos, flight patterns, locations, and owner identifications. This study continued to indicate the use of drones autonomously or by an operator. This information can dictate the form of data gathered. Illegal activities via drone use come in many forms, such as drug drops over foreign borders, contraband drops over prison fences, and unsolicited surveillance. The scenario provided in the study is based upon the before-mentioned instances of illegal use of drones and law enforcement, engaging forensic analysis to determine such information as ownership and link to crime [10]. The study maintains that state and federal legislation has not managed to regulate drone technology and thus leaves most stakeholders vulnerable. In the end, it was concluded that due to the lack of a universal drone structure or forensic tools, continued research must be completed to determine the method of data extraction. Lastly, the researchers left more invasive methods, such as chip-off, as a last resort due to the possibility of damage.

Yousef and Iqbal [11] used the DJI Mavic Air drone and the iPhone 6 mobile device for the basis of the experiment in pursuit of determining examiner procedures, extrapolating files that could be used as court evidence. The researchers denoted limitations regarding their process being applied to various kinds of drones and found a challenge in the duration of time allotted for drone examination. Due to time constraints, they could not find the DJI's *.DAT* and *.txt* files that would have provided flight information.

Hamidi et al. [12] focused primarily on the DJI Phantom 4 Standard drone to determine a specific procedure for analyzing the *.DAT* file and extracting data from storage sources that could be used in a criminal case. The study resulted in the researchers finding considerable relevant information, which accomplished this study's goal, but in conclusion, it was recommended to continue research on other drone types and a greater research emphasis on *.DAT* and *.txt* file structures based on their complexity [12].

On the other hand, researchers in [13] have developed Drone Open source Parser (DROP), which is an open-source parser for DJI Phantom 3 flight logs that are encrypted in the special format of *.DAT* files. It takes each of the unreadable *.DAT* files format, which represents a flight log, and decrypts them into *.CSV* readable format. Moreover, to validate their results, they have compared their tool with the outcome of the decrypted and parsed *.txt* using http://healthydrones.com/ (accessed on 31 May 2021), which is now https://airdata.com/ (accessed on 31 May 2021). As a result, they found that the decrypted outcome of the DROP tool in a CSV file format is almost identical to the outcome of the flight logs that are decoded and decrypted from the *.txt* format. In contrast, researchers of [14] used DJI Phantom 3 Advanced as a case study to test the ability to recover GPS data as digital evidence using DatCon tool v2.3.0, enabling them to decrypt the *.DAT* files recovered from the digital forensic image of the Android smartphone used in the study.

Furthermore, in a recent case study [15], researchers have assessed and highlighted important differences in the capabilities of widely used UAV forensic software and tools (e.g., Autopsy, Cellebrite, and Datcon). Although they found that the DatCon tool was able to decrypt the *.DAT* file and convert it to a readable CSV file format, other tools used in the study have varied results regarding decryption of the *.DAT* files even though some were using the DatCon module. The study highlights the importance of validation and cross-checking results using multiple tools.

Many developments have been integrated into forensics software to detect and acquire drone equipment. For instance, Cellebrite now supports the acquisition of many DJI types (e.g.., Inspire 2, Mavic Pro, Mavic Pro 2, Mavic Air, Phantom 3 and 4, and Spark) but not the Mini 2. Despite the efforts and previous research, many questions remain unanswered regarding drone forensics, particularly the new models, such as DJI Mini 2.

3. Methodology

Malicious drone usage can be conducted in many ways, and based on the given scenario, the investigation will differ. This is due to drones varying in manufacturer, technical capabilities, version, and even size. In addition, when it comes to drone investigation techniques during real-life crimes, the drone might not be the only place to look for evidence. Applications used to operate, set up, and even update the drones can supplement and complement the existing evidence found on the device or used as primary evidence if deemed appropriate. This is to aid in finding possible connections between the software and the drone to help future investigations.

3.1. Experiment Design

During real-life crimes, when the digital evidence is involved and the devices are ceased, very rarely, only information populated on those devices will be related to the crime. Filtering through the information presents challenges, especially when it comes to large storage capacities and unknown file structures. For this study, we decided to eliminate unwanted information not related to the case study by controlling the environment as much as our resources allowed us. This ensured that the data populated during the study would be easier to filter through and unwanted cross-contamination from another unrelated action was eliminated, providing comprehensive research from the beginning of the case to the end without any additional steps.

The logic behind the selected devices for the study came from the extensive prior research conducted. The research has shown that these devices are most commonly used, available to the general public without any restrictions or prior requirements, and they are reasonably inexpensive. An additional reason for particularly choosing the DJI Mini 2 drone was the lack of research in the literature and digital forensics investigations. A full list of the devices utilized to create the case study scenarios and conduct the experiment for the research is listed in Table 1. Moreover, to find valuable information, this study and research followed best practices to acquire and examine the forensic images of the associated devices. For the two smartphones used in this study, we followed the data

population and examination guidelines suggested by the National Institute of Standards and Technology (NIST) [16].

In addition, Figure 1 shows the complete methodology involving all the processes and components utilized. Each of the phases will be discussed in detail to outline the steps that were taken into consideration.

Table 1. Full device list used in the study.

Device Name	Model/Version	Device ID
DJI Mini 2	M: MT2PD	3Q4CHBN3A3B1FX
Remote Controller (Hardware)	M: RC231	396CHBR00194WJ
Drone Battery	M: BWX161-2250-7.7	3QFPHPCA50A1P
Flight Controller (Software)	3NZCHBS003C5MF	NA
Drone Camera	FC7303	1SFLH870AB0K6X
Drone Gimbal	NA	3QCCHC3P23EKJK
FlySafe Database	01.00.01.19	NA
SD card	C10 and U3	TBM5C4004DGE
iPhone 7	A1660/iOS 13.3.1	IMEI: 355343080118768
Samsung Galaxy s7	SM-G930U/Android 8.0.0 OS	IMEI: 358512071203717
Cellebrite UFED memory card reader	A-CRD-01-005	1025056
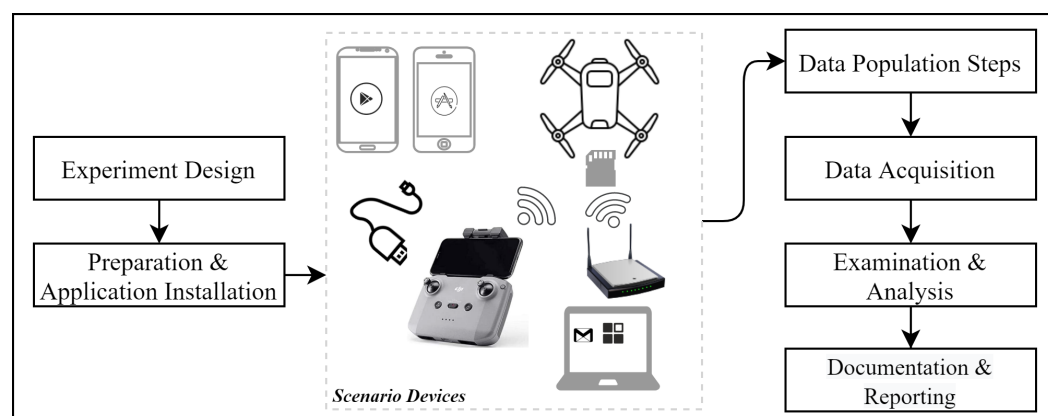
Figure 1. Methodology process followed in this research.

3.2. Application Installation and Preparation

Prior to working with the mobile phones and the drone, a brand-new WiFi Service Set IDentifier (SSID) was created for the devices to use during the study. Setting up a new wireless network further ensures control of the environment. The device used as a wireless router was a TP-Link (TL-WR1043N v5) with OpenWRT (19.07.5 r11257-5090152ae3). To set up the case study scenario and ensure no previous data were present, SD cards and smartphones were wiped and restored to factory settings. DJI Mini 2 was not susceptible to this process since the drone and its associated remote controller were new and never used previously. Additionally, Google Inc. Gmail service was used as the email provider and a primary account to set up iCloud, Apple Appstore, Google Play Store, and an associated user account for DJI-related applications (apps). Next, the software necessary to operate the drone during the flight (i.e., DJI Fly) was installed on both phones running Android and iOS.

Various digital forensics software tools were used to acquire and analyze the data. In this research, we used resources that included open-source tools (i.e., Autopsy [17]) that

were complemented with proprietary tools such as Magnet AXIOM, and Cellebrite UFED 4PC, which are used worldwide by law enforcement agencies and practitioners [18,19]. These tools were also used for cross-validation. Table 2 lists all tools that are used in all phases of the experiment (i.e., data population, acquisition, and analysis).

Table 2. Tools and applications used.

Software Name	Version	Usage	Availability
DJI Fly on Android	1.3.0	Flight Operation	Freeware
DJI Fly on iPhone	1.3.1	Flight Operation	Freeware
Autopsy	4.18.0	Examination and Analysis	Open-source
Magnet AXIOM Process	4.11.0.24063	Acquisition	Proprietary
Magnet ACQUIRE	2.37.0.24776	Acquisition	Freeware
Magnet AXIOM Examine	4.11.0.24063	Examination and Analysis	Proprietary
Cellebrite UFED	7.42.0.82	Acquisition	Proprietary
Cellebrite Physical Analyzer	7.42.0.50	Examination and Analysis	Proprietary
Cellebrite Reader	7.42.0.50	Examination and Analysis	Freeware
Binwalk	2.2.0	Entropy measurement	Open-source
ExifTool	12.25	Reading meta information	Open-source
DatCon	4.2.0	Decryption of the *.DAT* files	Freeware

3.2.1. iOS Setup

The iOS mobile device used for the study was an iPhone 7 with iOS version 13.3.1. After connecting to the WiFi network we created, we logged into the App Store using a previously activated Gmail account and downloaded the DJI Fly app (Version 1.3.1 (440)). Upon download, we opened the app and followed the default options. The DJI Fly application initially presented a video and then asked for enabling Bluetooth, location, and notification service. We selected "only while using the app". The next prompt was if we wanted to participate in the DJI product improvement, and we selected "not now". Lastly, upon logging into the DJI Fly application using the Gmail account, we were notified about geo-zone restrictions and selected "agree". After the previous process, the app was ready for the connection with the drone.

3.2.2. Android Setup

The Android device used in this study was a rooted Samsung Galaxy s7 running Android 8.0.0. The DJI Fly app had no official version available in the Android Play Store, so v1.3.0 was downloaded as an APK file and then installed on the phone. As a connection to the internet, the phone was connected to the WiFi access point created for this study, acquiring the time and accurate GPS location. Upon opening the DJI Fly app, the prompted messages asked for several permissions (e.g., notification and location services, and access to photos), which were all agreed to. The app on the Samsung Galaxy S7, similarly to the iPhone 7, asked us to either log in or create an account, where we chose to log in, since we already had the account credentials used when we downloaded the iPhone's app.

3.2.3. Laptops

Three laptops were used during the experiment, Lenovo G570 (Model 4334), HP Pavilion dv6 (dv6-7003em), and MacBook Pro (15-inch, 2018 running 2.9 GHz 6-core Intel i9). The Lenovo laptop had a Windows 10 Home (10.0.19042) operating system, used to set up the accounts, manage the WiFi network, and root the android phone. The HP Pavilion laptop with Linux Kali (Release: 2020.4) was set up to look for any interaction between the drone and the controller. For this, we utilized the monitor mode capability allowing the wireless card (Intel AC7260) to see 802.11 management frames and Wireshark (v3.2.7) capturing the frames on different channels. Although there was no need for the iPhone 7 to be jailbroken when acquiring the iPhone device using Cellebrite, there is a need for the device to be jailbroken using Magnet ACQUIRE because it does not offer jailbreaking for the investigator. Therefore, we needed the MacBook Pro laptop to jailbreak the iPhone using the Checkra1n app (beta 0.12.2).

3.2.4. Drone

The DJI Mini 2 drone used for this study was a brand new unit. Therefore, we made sure that it was fully charged and equipped with an empty external SD card. To simulate an attacker opening the drone and testing it before the deployment, we logged on to the app and operated once before the data population scenarios using the iPhone 7. All associated applications to operate the drone were installed on the phone used in this study.

Devices used in this study are presented in Figure 2. Moreover, the figure includes additional items, which will be explained in detail further in the paper.

Figure 2. Devices and other components used in the study.

3.2.5. Machines Used for Investigations

In this study, two forensic workstations equipped with the same tools were used across all phases of the study to validate the results and eliminate any known software limitations. Additionally, to prevent any software bias, all acquired data were examined with at least two different software solutions if applicable. The first machine was equipped with Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz, with 16 GB RAM, Windows 10 Education 20H2, while the second was equipped with Intel i9-10900K processor, NVIDIA GeForce RTX™ 3070 graphics card, and 32GB of RAM memory running X version of Windows 10 Pro. Note that this study does not consider the performance of the forensic processes performed on different workstations.

3.3. Data Population

Following the initial setup of the DJI Mini 2 and confirming the proper functionality (i.e., operating and flying it once), the drone was taken out to a location for the data population. The data population consisted of flying the drone in various patterns and altitudes while gathering images, videos, and other data. The process was completed on both iPhone 7 and Samsung Galaxy s7 utilizing the DJI Fly application for drone controlling and flying.

During travel from the setup location of the drone to the location of the data population, we left the drone powered on. In addition, two phones were utilized to navigate to the location using native map apps (i.e., Google Maps for Android, Apple Maps for iPhone).

Upon reaching the location, we flew the drone in 4 different scenarios on the first test day and additional flights for testing weight carrying capabilities on another day (i.e., Scenario 5). We discuss these scenarios in detail in the following Sections 3.3.1–3.3.5. Moreover, Table 3 illustrates the scenarios in detail. Note that all times used in this study are based on Eastern Time.

Table 3. Scenario times and actions.

Scenario	Start Time	End Time	Actions Taken While Flying
1	26 March 2021 15:45	26 March 2021 15:51	Video and Photos
2	26 March 2021 15:55	26 March 2021 15:58	Video and changing mode to sport
3	26 March 2021 16:06	26 March 2021 16:12	Video
4	26 March 2021 16:17	26 March 2021 16:20	Video
5	9 April 2021	9 April 2021	Multiple Flights

3.3.1. Scenario 1

This scenario was designed to portray a criminal-like action where a malicious user would purchase a drone that does not require any prior paperwork, and it is widely used. The user sets up the drone using a personal mobile device (i.e., iPhone 7) to make it operational. The user first tests the drone to make sure that it is working as expected for the action. Once the test is completed, the user leaves for the location where the drone will be flown from. Once arrived, the user prepares the drone and confirms the home location before the flight. The user flies the drone to the desired location and flies it back. During the flight, the user was able to take videos and photos of the flight.

This type of scenario can be applied to many different real-life situations where malicious users utilize the drone to drop off payloads and perform reconnaissance, etc.

3.3.2. Scenario 2

In this scenario, the same device was used as in Scenario 1 but only to perform a one-way flight. The reason behind designing a one-way flight is that we tried simulating the drone being captured or destroyed, hence not returning back. While catching the drone in this scenario, we tried shutting the drone by force clicking and holding the turn-off button; however, we could not turn it off while flying. During the process of capturing, the drone was turned off immediately by rotating it 180 degrees (i.e., top of the drone facing the ground).

3.3.3. Scenario 3

The scenario follows a similar process and the idea behind the malicious use as in Scenario 1 with few differences. First, instead of iPhone 7 as a mobile device connected to the controller, the device used was Samsung Galaxy 7. Second, the timestamps of the flight were different, as well as the flying path.

3.3.4. Scenario 4

This scenario follows the methodology of Scenario 2 except using Samsung Galaxy S7 instead of iPhone 7 as a mobile device. Just like other scenarios, this one has different timestamps of the flight and flying path.

3.3.5. Scenario 5

In this last scenario, we decided to test the carrying capabilities of the DJI Mini 2 drone using the iPhone 7 with multiple flights. This scenario was conducted at a separate location and on a different day than the previous four scenarios. The reasoning behind the test was to see the maximum carrying capacity and any difference between carrying payloads using multiple methods. The exact times of this flight scenario were not recorded in Table 3 due to multiple short flights; while trying to determine the maximum carrying capacity, only the date of the flight was recorded.

This scenario shows the capabilities of the drone and what potential malicious items that are similar to the size and weight the drone can carry. Maximum carrying capacity can play a big role during the malicious act where dangerous items can be transported, dropped, and deployed.

3.4. Acquisition

To ensure that we made the most out of the two smartphone devices and gain privileged status, we performed jailbreak and rooting operations for the iPhone and Samsung devices, respectively, as previously discussed. This was required to create physical forensic images using Cellebrite UFED, Magnet AXIOM Process, and Magnet Acquire. The SD card used in the case scenario was acquired using Cellebrite's Memory Card Reader with write blocker capability (see Figure 3).

Figure 3. Cellebrite UFED memory card reader.

Additionally, Table 4 presents the devices and tools used, the version of the tools, and image creation date and time in detail.

Table 4. Detailed acquisition process.

Device	Acquisition Tool	Image Time	Description
iPhone	Cellebrite UFED	03-31-2021 09:42	After Scenarios 1 and 2
iPhone	Magnet ACQUIRE	04-07-2021 15:03	After Scenarios 1 and 2
iPhone	Magnet ACQUIRE	04-10-2021 12:15	After Scenario 5
Samsung	Cellebrite UFED	03-31-2021 10:36	After Scenarios 3 and 4
Samsung	Magnet Process	04-05-2021 14:34	After Scenarios 3 and 4
SD card	Cellebrite UFED	03-31-2021 16:17	After Scenarios 1, 2, 3 and 4

4. Analysis and Findings

In this phase of the experiment, we gathered, analyzed, and compared the previously populated data. The comparison of the collected data was achieved by utilizing multiple digital forensics tools. We started by analyzing the images created by the acquisition tools. Table 5 explains the symbols used in Table 6, which illustrates the findings from our analysis using the three initial forensics tools utilized for this study.

Table 5. Explanation of the symbols used in Table 6.

Symbol	Explanation
Y	Artifacts were found
N	Artifacts were not found
*	Artifacts were partially recovered, and it is missing relevant data
E	Artifacts were found but encrypted
A	Recovered by Autopsy tool
C	Recovered by Cellebrite tool
M	Recovered by Magnet AXIOM tool

Table 6. Tool evaluation assessment.

Artifacts		PII			Flight Logs			Media Files		
Tools		A	C	M	A	C	M	A	C	M
	iPhone	Y	Y	Y	E	E *	E	Y	Y	Y
Component	Samsung	Y	Y	Y	E	E	E	Y	Y	Y
	SD card	N	N	N	N	N	N	Y	Y	Y

4.1. iOS Analysis

Following the first acquisition that was done after the first day of our experiment, we were able to find two *.DAT* and three *.txt* files; however, all the files discovered were encrypted. The reason that there are only two *.DAT* files compared to three *.txt* files is because it goes back to the difference in how these files were written. We believe that each *.txt* file represents a complete flight from take-off to land operation, where each *.DAT* file represents data when the drone is connected to a smartphone and is turned on to the drone shot-off. For instance, the first *.DAT* file represents the initial flight conducted before the scenarios, and the second *.DAT* file represents Scenario 1 and Scenario 2 where we did not turn the drone off between these two scenarios, resulting in one *.DAT* file.

The encrypted *.txt* files were recovered from the *DarArchive\root\private\var\mobile\ Containers\Data\Application/38FA31DB-9A11-4365-9083-8657C089F83D\Documents\Flight Records* folder on the iPhone, where the encrypted *.DAT* flight logs can be recovered from the following path *DarArchive\root\private\var\mobile\Containers\Data\Application\38FA31 DB-9A11-4365-9083-8657C089F83D\Documents\FlightRecords\MCDatFlightRecords*. Unfortunately, none of the digital forensics tools (i.e., Autopsy, Cellebrite, and Magnet Axiom)

were able to decrypt the *.DAT* or *.txt* files that store the flight records. One major difference in the comparison of the tools is that Cellebrite was able to extract four *.jpg* images from each of the *.txt* flight logs. These images represent what possibly could be high-quality thumbnails or images showing the location at the beginning of the flight. Figure 4 illustrates the screenshot taken from Cellebrite.

Figure 4. Embedded *.JPG* images from each of the *.txt* flight records.

Moreover, we were able to recover significant PII that can help in investigations. First, we were able to recover the location of the first time that the iPhone was used to connect to the drone (i.e., in our study, it was the setup location) from *Application\38FA31DB-9A11-4365-9083-8657C089F83D\Library\.space_db\flysafe_dji_flight_dynamic_areas.db* database inside a table named *dynamic_geofence_amba_record*. We believe that this location was acquired from the phone and not the drone because the first time we operated the drone was inside a building, and the drone was not able to detect GPS signals. Figure 5 illustrates the user geolocation finding.

amba_uid	lat	lng	amba_tfrs_data
94db55821a2039bdb4415381f6de2c4f	40.4276428222656	-86.9108137988894	AAAAShpFDip52WzAF5SEVOmhM6f5 +zIDvfyTAB69mgFPG0Y=

Figure 5. User setup location recovered using Magnet Axiom.

Other PIIs, such as the email that is used for app login, activation timestamp, DJI model name, last connected time, uptime, and aircraft camera serial number were recovered from *Application\38FA31DB-9A11-4365-9083-8657C089F83D\Library\Preferences\com.dji.golite.plist*. Figure 6 shows flight controller serial number, camera serial number, product name, last connect time, and the drone serial number. Moreover, Figure 7 displays the last connected email used to fly a drone, and Figure 8 shows the first time the iPhone was connected to the drone after the user finished with the activation process.

Another finding worth mentioning, in the scenario where the drone was captured, is that the camera on the drone kept recording for another 20 s even though it was flipped upside down, and the propellers were not spinning.

Although we compared the acquisition after the first day that consisted of the first two scenarios for the iPhone (see Sections 3.3.1 and 3.3.2) and the acquisition after Scenario 5 (see Section 3.3.5), the uptime did not change. On the other hand, the last connection recorded has changed and updated following the second acquisition that was performed after Scenario 5 to when the drone was last connected to the application using this iPhone.

In addition, in \private\var\mobile\Containers\Data\Application\38FA31DB-9A11-4365-9083-8657C089F83D\Documents\Tmp\DJISyncLog_2021-03-26_[13-36-13].txt file, we found records stored that convey the DJI drone sync with the phone/server, and the timestamps are similar to the scenarios.

Key	Type	Value
kDJICareDeviceManagementHistoricalConnectedProductInfoKey	ARRAY	
	DICTIONARY	
aircraftFlightControllerSerialNumber	STRING	3NZCHBS003C5MF
aircraftCameraSerialNumber	STRING	1SFLH870AB0K6X
totalMileage	NUMBER	0.0
productType	NUMBER	76
remoteControllerSerialNumberFromServer	STRING	
productName	STRING	DJI Mini 2
activationTime	NUMBER	0.0
remoteControllerSerialNumber	STRING	
useDurationFromServer	NUMBER	0
flightDuration	NUMBER	0.0
accountName	STRING	
lastConnectTime	DATE	Fri Apr 09 13:52:46 EDT 2021
flightTimes	NUMBER	0
careStatus	NUMBER	0
aircraftSerialNumber	STRING	3Q4CHBN3A3B1FX
remoteControllerChipSerialNumber	STRING	
DJIHTTPLastLogFile	STRING	HTTP_Log2021-04-09[11][31][38](170).log

Figure 6. PII recovered using the Autopsy tool.

```
[19] DJIACCOUNTMANAGER_LASTUSEREMAIL = Pete.purdue.cnit525@gmail.com
[20] __TIMESTAMP__
    [0] Timestamp = 1616780077.929
    [1] Uptime = 3801.491394
[21] DJICareProductSn = 3NZCHBS003C5MF
[22] UserDefaultKey_IsChineaseUser = False
[23] __DEVICE_ID__ = 2b5c9b32-20e9-4985-978b-7cfc1b76a299
```

Figure 7. Email recovered using the Magnet Axiom tool.

kDJIFinishActivationInfoKey	DICTIONARY	
kDJIFinishActivationInfoTimeKey	DATE	Fri Mar 26 14:44:38 EDT 2021
kDJIFinishActivationInfoProductKey	NUMBER	76

Figure 8. User activation timestamp recovered using the Autopsy tool.

4.2. Android Analysis

Similar to iOS analysis, we were able to discover both *.txt* and *.DAT* file types in an encrypted form. The *.txt* files containing flight logs were recovered from \data\media\0\DJI\dji.go.v5\FlightRecord folder, and the *.DAT* files were recovered from the \data\media\0\DJI\dji.go.v5\FlightRecord\MCDatFlightRecords\ folder.

Regarding PII, the location of the first time that the phone connected to the drone was recovered from the table named *dynamic_geofence_amba_record* inside the following database \data\data\dji.go.v5\databases\flysafe_dji_flight_dynamic_areas.db. Other similar PII to the ones recovered from iPhone (e.g., DJI model name, and aircraft camera serial number) can be recovered from the \data\data\dji.go.v5\databases\dji.db database. Figure 9 demonstrates the geolocation values (longtitute and latitute) recovered from the *dynamic_geofence_amba_record* table, where Figure 10 shows the drone serial number along with other valuable information.

Moreover, we were able to recover a thumbnail image showing an image captured from when the iPhone was controlling the drone; the image recovered from the following path *data\media\0\DJI\dji.go.v5\CACHE_IMAGE\ImageCaches*. On the other hand, the video captured during Scenario 4 (see Section 3.3.4) was cut off and not complete, whereas for the iPhone (see Section 3.3.2), it was complete. Additionally, it appears that Cellebrite was not able to extract any images embedded inside the *.txt* flight logs on Android.

Table dynamic_geofence... ∨	1 entries	Page 1 of 1 ← →	Export to CSV
amba_uid	lat	lng	amba_tfrs_data
94db55821a2039bdb4415381f6de2c4f	40.22470559974725	-87.00357270936411	AAAAShpFDip52WzAF5SEVOmhM6f5+zlDvfyTAB69mgFPG0Y=

Figure 9. User location recovered for the first time connected to the drone using the Autopsy tool.

Table dji_component_acti... ∨	1 entries	Page 1 of 1 ← →	Export to CSV				
mc	LeftTime	checkTime	IsBuy	GimbalSN	CraftSN	Slug	productT...
3NZCHBS003C5MF	167271	1616789803	0	3QCCHC3P23EKJK	3Q4CHBN3A3B1FX	dji-care-refresh-mini-2	76

Figure 10. Drone identification information and the activation timestamp recovered using the Autopsy tool.

4.3. SD Card Analysis

Analyzing and examining the external SD card revealed that the SD card is storing media files taken during the flight and some encrypted logs. Although these logs are not the flight path logs, we were unable to decrypt them despite our efforts. On the other hand, all recovered videos have locations associated with them (see Figure 11). In addition, we were able to access media files from both phones and all four scenarios where the SD card was used. Even the video recorded during Scenario 4 (see Section 3.3.4) is found to be complete. Both the pictures and videos stored in the SD card can be recovered from the *img_Dump_001.bin\vol_vol2\DCIM\100MEDIA* folder.

F/2.8, SS 435.23, ISO 100, EV 0, GPS (-87.0032, 40.2248, 18), D 0.00m, H 15.50m, H.S n/a, V.S n/a
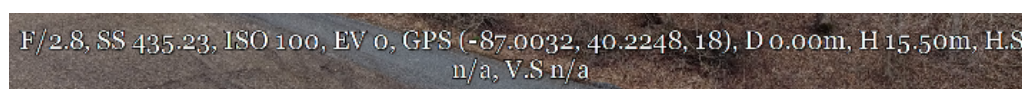
Figure 11. GPS location of the video frame displayed on top of the video using the Autopsy tool.

In addition, we were able to use ExifTool to recover the camera serial number from the pictures taken. Figure 12 demonstrates the recovered camera serial number and plenty of other information.

```
Serial Number                     : 1SFLH870AB0K6X
GPS Version ID                    : 2.3.0.0
GPS Latitude Ref                  : North
GPS Longitude Ref                 : West
GPS Altitude Ref                  : Above Sea Level
XP Comment                        : Type=N, Mode=P, DE=None
XP Keywords                       : v01.32.0047;0.0.1;v1.0.0
Compression                       : JPEG (old-style)
Thumbnail Offset                  : 18432
Thumbnail Length                  : 10518
About                             : DJI Meta Data
Format                            : image/jpg
Absolute Altitude                 : +42.40
Relative Altitude                 : +42.40
Gimbal Roll Degree                : +0.00
Gimbal Yaw Degree                 : +0.00
Gimbal Pitch Degree               : +0.00
Flight Roll Degree                : -2.70
Flight Yaw Degree                 : -117.60
Flight Pitch Degree               : -3.40
```

Figure 12. Recovered camera serial number using ExifTool.

4.4. Carrying Capacity Analysis

The first step of the carrying capacity drone analysis was to determine the overall weight of the drone. The drone was placed on the scale (Perfect Portion) and measured at 240 g ($\pm$3 g) compared to the 249 g of marketed weight. Next, the fishing line measuring 60cm was tied to the bottom of the drone with an attached plastic box where the weights were added. The weight of the plastic box with the fishing line added up to 36 g, making the overall weight of the drone and box 276 g. Weights were added between each flight until the drone was not able to take off. The maximum capacity that the drone was able to lift was around 300 g (including the plastic box, weight, and the line). Although the drone was able to lift that amount of weight during the take-off and flight, it could not maneuver easily. Therefore, the next step was to determine the optimal capacity that the drone could carry and maneuver without any problems.

For this experiment, we started removing weights (starting at 300 g) until we were satisfied that the drone operations were restored to normal. The weight we determined in which the drone can restore its normal flight was around 250 g. It is important to note that during the flight, we were experiencing high winds and that it is quite possible that the carrying capacity can vary during different flying conditions.

As our last experiment, we decided to place the weights and the box on top of the drone. The drone was able to carry and fly with 250 g attached to it. Moreover, we observed more responsiveness from the drone when the weights were attached on top of the drone compared to hanging and swinging below it. Figure 13 depicts the setup used during this analysis.

Figure 13. Items used during carrying capacity analysis.

4.5. Data Analysis

As discussed earlier, *.DAT* and *.txt* flight logs/records were not recognized by the forensics tools used in this study because they were encrypted. Therefore, we ran an entropy analysis using the Binwalk tool (v2.2.0) [20] to calculate each file's entropy score. Figure 14 illustrates the outcome of the tool after running it on both files for Scenario 1 (see Section 3.3.1). As shown in Figure 14, the results showed very high entropy scores throughout both files.

Following the literature review, many resources suggested using different tools in an attempt to decrypt the *.DAT* files generated during the scenarios. The most used freeware tool to decrypt *.DAT* files is the DatCon [21]. Even though the website stated the model of our drone was not supported, we tested it regardless. It turned out to be true, and the *.DAT* files could not be decrypted. As an alternative solution to examine the contents of the *.DAT* files, we found the website airdata.com. Airdata helps pilots and others (e.g., researchers) by providing fleet drone management, as well as crash-prevention information [22]. After the registration of a free account, we were able to upload our *.DAT* files and decrypt them successfully.
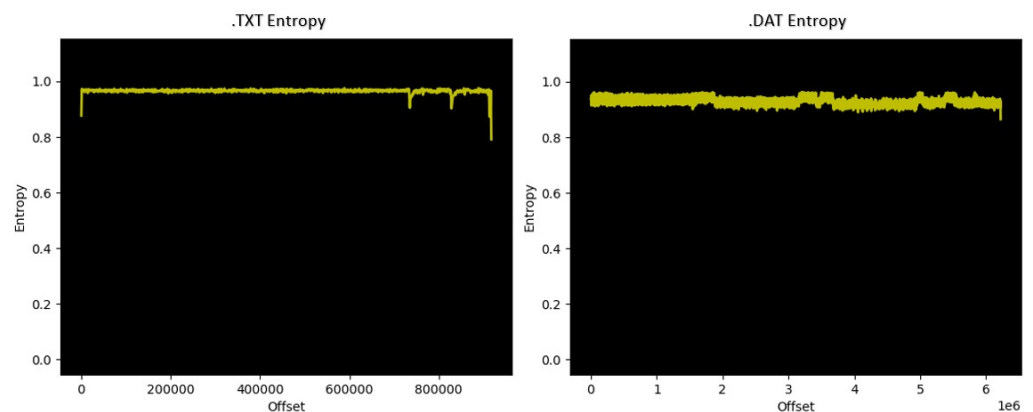
Figure 14. Scenario 1 entropy analysis for *.txt* and *.DAT* files.

Despite the ability of airdata.com to decrypt the *.DAT* files, we also tried to decrypt *.txt* files; however, the process was not successful. Moreover, airdata.com allows the user

to download the decrypted *.DAT* files in KML, GPX, CSV, and original formats. Therefore, to ensure data integrity, we compared the outcome of the downloaded CSV file once after the decryption, the second time after deleting the file and enabling the web tool to decrypt it again. Interestingly, we found that the checksum values using the MD5 hashing algorithm of the two downloaded CSV files match, meaning that the tool provides consistent decryption results.

While the main motive behind the website (airdata.com) was not to provide digital forensic services to the end-users but to give pilots crash-prevention information and manage large fleets of drones, we found this website very beneficial during our study [22]. Its intuitive user interface and detailed analysis of the log files allowed us to visualize flight patterns, altitudes, battery levels, controls sent to the drone, error codes, and many more. A screenshot in Figure 15 shows the user interface of the airdata.com web tool during the analysis process of Scenario 1 and Scenario 2. Moreover, Figure 16 illustrates the weather tab that contains wind speed faced during one of the flights in Scenario 5.
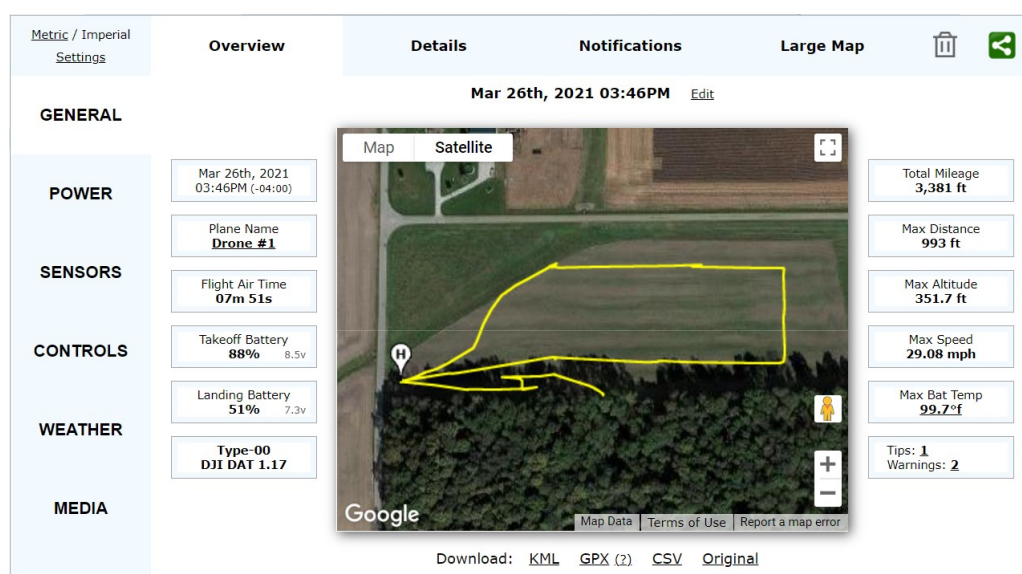
Figure 15. User interface of app.airdata.com.

One important finding is we could not have a matching location (i.e., drone flight location and iPhone cached location) from the cached locations recovered from the iPhone in the first acquisition using Magnet Acquire. However, we were able to find matching locations for the drone and the iPhone after the second acquisition using Magnet Acquire. This is due to the fact that the iPhone keeps the cached locations for a certain time (approximately one week), and our first Magnet acquisition was more than seven days apart from the day we flew the drone. However, we were able to find the matching location in the second acquisition because it was performed within seven days. In addition, in the first Cellebrite acquisition for Scenarios 1 and 2, we were able to match the user location with the cached locations on the drone flight records because it was less than a week from the scenario. We recovered the iPhone cached locations from the *ZRTCLLOCATIONMO* table located in the *\private\var\mobile\Library\Caches\com.apple.routined\Cache.sqlite* database.
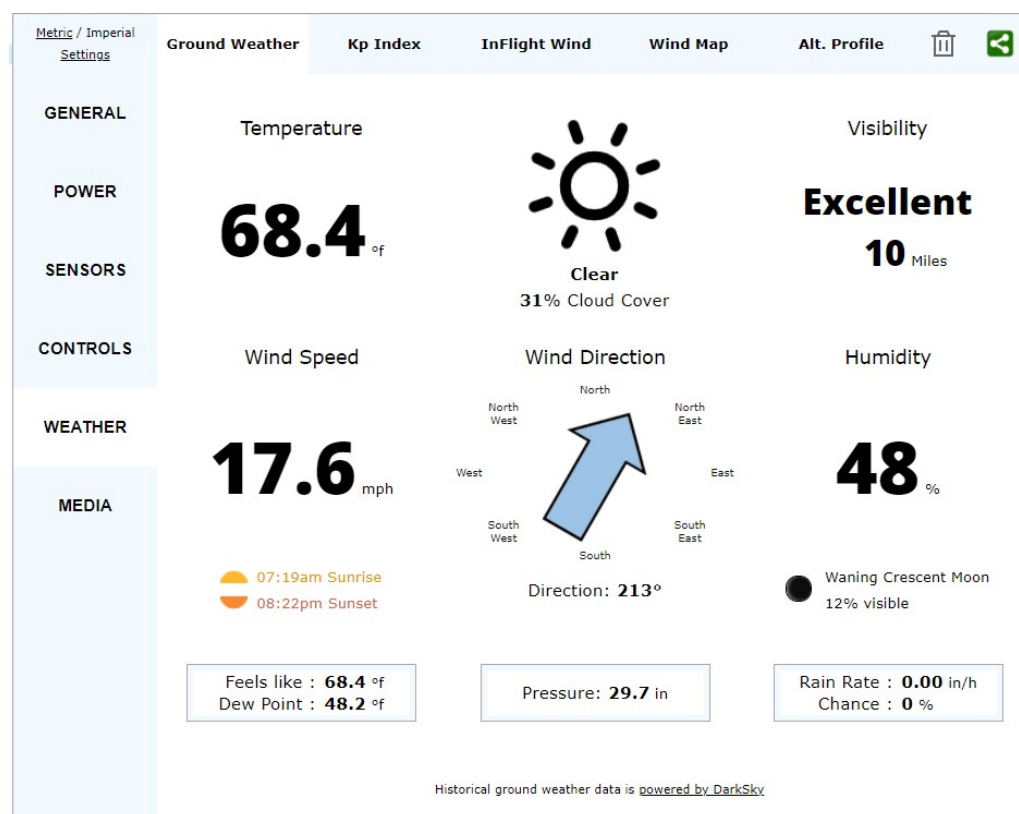
Figure 16. Weather section at app.airdata.com after analyzing one of the *.DAT* files in Scenario 5.

Moreover, we wanted to confirm that the drone or the controller was not beaconing any management frames during the flight. We matched the channels by setting the same channel and frequency on the app and the wireless card on the laptop. We then opened Wireshark (v3.2.7) and filtered DJI's Media Access Control (MAC) address. Since we did not want the filter for a specific MAC address, we created a byte-offset capture filter for the first three octets unique to each manufacturer, such as DJI. The filters did not show any MAC addresses related to the DJI. The probable reason for this is because the drone is using OcuSync 2.0, which is a wireless transmission protocol used in these newer types of drones when transmitting video feeds over long distances.

Although the user interface on both iOS and Android devices looked similar, one major difference we spotted was the password character limitation when accessing the accounts before the flight.

Lastly, during the capturing scenarios of the drone operations on both iOS and Android mobile devices, we tried shutting off the drone first while in flight by pressing and then holding the power button. However, this method did not work. When we flipped the drone upside down, the propellers stopped, and we were able to suspend the drone operations. This illustrated how this drone can be best captured without causing damage to the drone.

5. Discussion

During the course of this study, we experienced several difficulties with the digital forensic tools when it came to decrypting the flight records. Therefore, we can safely conclude that there is no one tool that would be superior in drone forensics, as discussed in Section 4 in detail. It is important to note that during these types of investigations, the investigators need to utilize multiple techniques and sources to find and examine data. As we have shown, the tool that was able to decrypt the *.DAT* files was not intended for digital forensics investigations; however, it was able to decrypt and then analyze the flight logs.

Moreover, current digital forensics tools could not recognize the drone when connected directly to the forensics machine. This is because this model of the drone is new, and it is

found that this model is not equipped with storing data internally. However, that does not imply that the internal memory of some sort does not exist. This leaves the door open for further analysis, such as chip-off analysis, which is out of the scope of this research.

As it was discussed in Section 4.4, the carrying capability of the DJI Mini 2 drone was more than we expected. The ability to carry more than its weight should be very concerning when thinking about malicious activities that can be performed easily without being detected. Furthermore, another consideration is that this type of drone does not require any previous paperwork or registration, which leaves law enforcement agencies with no ability to track back to the owner or a malicious actor. At the time of this writing, there are no major changes expected in FAA rules regarding micro drones (e.g., DJI Mini 2) at least until 2023 [23], leaving room for malicious activities.

Security concerns arose when the DJI Fly app was not in the official Android Play Store, and it had to be downloaded as an APK file and then installed on the mobile device. This presents great security concerns since the owner of the device does not always have the latest version (i.e., updated version) of the app. In addition, the app can contain malicious code placed by accident or on purpose. It is also possible that malicious code can be introduced or hard-coded into the APK file, which leads to vulnerable mobile devices used by the end-users.

During the initial setup of the drone, we were able to fly the drone without a GPS signal successfully, further indicating anti-forensic challenges to hide any PII related to the location. As a result, these challenges will make the investigation challenging, even if they consist only of the phone and the drone with the controller.

The error codes were found during the examination of the *.DAT* files via the airdata.com website. These errors showed a possibility to discover if the drone was carrying a load while operating. The error code: "Not Enough Force/ESC Error" was repeated continuously during the weight testing flights. Figure 17 shows the definition of this error code according to the *airdata.com* wiki page for notification [24]. Moreover, Figure 18 demonstrates the error code while the drone is being captured in Scenario 2 (see Section 3.3.2).
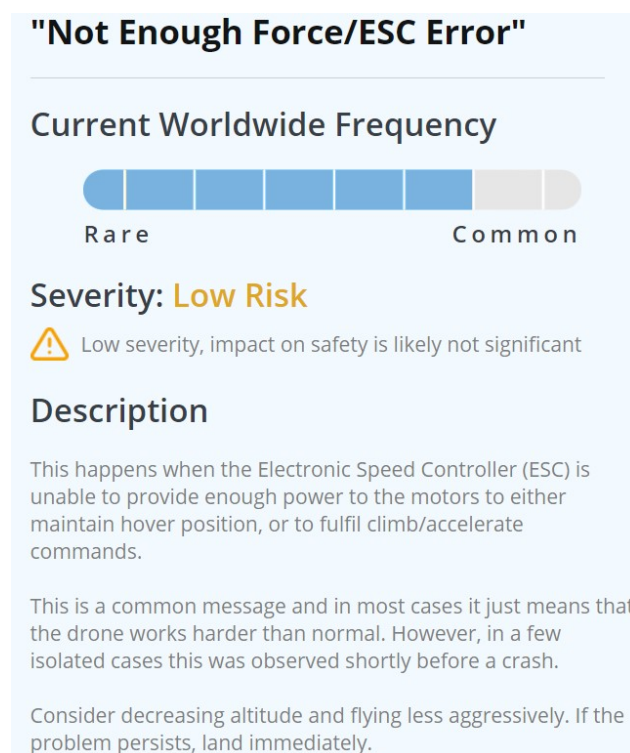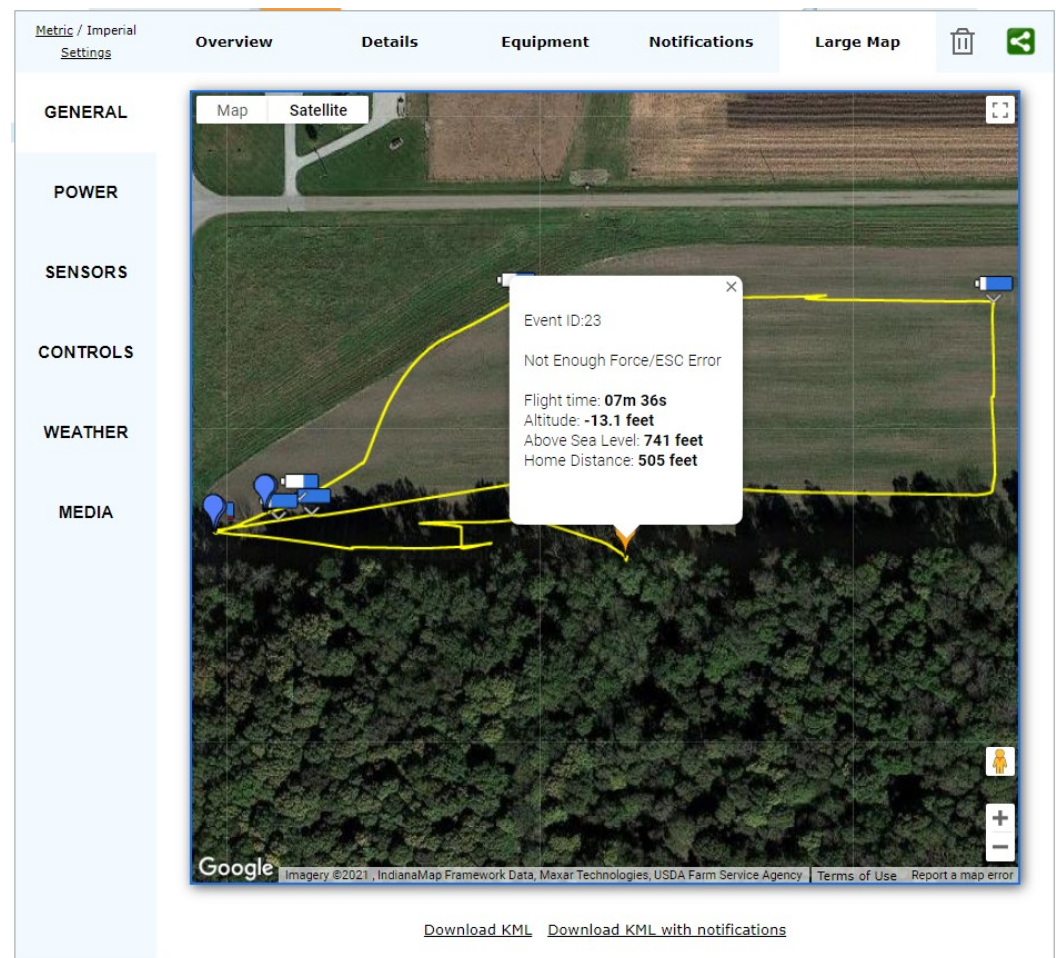

Figure 17. ESC error description [24].

Figure 18. ESC error message in Scenario 2 from app.airdata.com.

6. Conclusions and Future Work

Drone usage over the last few years, especially in recreational uses, has dramatically increased in production. This increase greatly affects law enforcement agencies that are trying to battle malicious drone usage. In this case study, we had complete control over all stages of the conducted comprehensive experiment on the DJI Mini 2 drone to utilize it in creating criminal-like scenarios. Similar scenarios are likely to be committed for nefarious activities in the real world by malicious users. While the findings of this study are limited to only one UAV (i.e., DJI Mini 2), it is important to note that the availability, price, and lack of regulations for the drone make it easy to conduct criminal-like activities. That is why having a comprehensive study on the drone can help forensic investigators when faced with similar scenarios. As discovered in our analysis, the carrying capacity of the DJI Mini 2 is more than the weight of the drone itself, which might be used by malicious actors in different scenarios such as dropping contraband materials on prisons or smuggling drugs over borders, etc.

For future work, we plan to perform chip-off data extracting and analysis. This may be very useful due to the ability to acquire data from the drone body, which would reveal insightful information, as seen from previous research. Moreover, a further experiment can be performed to check how battery usage is affected when carrying various weights. Finally, an examination of OcuSync 2.0 transmission technology can be performed to experiment on communication methods between the devices by applying a UAV kill chain to identify possible intrusion vulnerabilities.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Intelligence, I. Drone Industry Analysis 2021: Market Trends & Growth Forecasts. 2021. Available online: https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts (accessed on 10 March 2021).
2. FAA. UAS Sightings Report. Available online: https://www.faa.gov/uas/resources/public_records/uas_sightings_report/ (accessed on 10 March 2021).
3. Bouafif, H.; Kamoun, F.; Iqbal, F.; Marrington, A. Drone forensics: Challenges and new insights. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–6.
4. Kao, D.Y.; Chen, M.C.; Wu, W.Y.; Lin, J.S.; Chen, C.H.; Tsai, F. Drone Forensic Investigation: DJI Spark Drone as A Case Study. *Procedia Comput. Sci.* **2019**, *159*, 1890–1899.
5. Lan, J.K.W.; Lee, F.K.W. Drone Forensics: A Case Study on DJI Mavic Air 2. In Proceedings of the 2021 23rd International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 7–10 February 2021; pp. 291–296.
6. Jain, U. A Drone Forensics Investigation Framework. Ph.D. Thesis, Purdue University, West Lafayette, IN, USA, 2017.
7. Roder, A.; Choo, K.K.R.; Le-Khac, N.A. Unmanned aerial vehicle forensic investigation process: Dji phantom 3 drone as a case study. *arXiv* **2018**, arXiv:1804.08649.
8. Salamh, F.E.; Karabiyik, U.; Rogers, M.K. RPAS forensic validation analysis towards a technical investigation process: A case study of yuneec typhoon H. *Sensors* **2019**, *19*, 3246.
9. Yousef, M.; Iqbal, F.; Hussain, M. Drone Forensics: A Detailed Analysis of Emerging DJI Models. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 066–071.
10. Al-Room, K.; Iqbal, F.; Baker, T.; Shah, B.; Yankson, B.; MacDermott, A.; Hung, P.C. Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models. *Int. J. Digit. Crime Forensics* **2021**, *13*, 1–25.
11. Yousef, M.; Iqbal, F. Drone forensics: A case study on a DJI Mavic Air. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, UAE, 3–7 November 2019, pp. 1–3.
12. Iqbal, F.; Alam, S.; Kazim, A.; MacDermott, Á.; Hamdi, D.A. Drone forensics: A case study on DJI phantom 4. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, UAE, 3–7 November 2019; pp. 1–6.
13. Clark, D.R.; Meffert, C.; Baggili, I.; Breitinger, F. DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digit. Investig.* **2017**, *22*, S3–S14.
14. Prastya, S.E.; Riadi, I.; Luthfi, A. Forensic analysis of unmanned aerial vehicle to obtain gps log data as digital evidence. *IJCSIS* **2017**, *15*, 279–285.
15. Salamh, F.E.; Mirza, M.M.; Karabiyik, U. UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies. *Electronics* **2021**, *10*, 733.
16. Mobile Devices. 2017. Available online: thelma.allen@nist.gov (accessed on 17 March 2020).
17. Technology, B. Autopsy. Available online: https://www.basistech.com/autopsy (accessed on 6 March 2021).
18. Forensic, M. Magnet AXIOM—Digital Investigation Platform. Available online: https://www.magnetforensics.com/products/magnet-axiom (accessed on 6 March 2021).
19. Cellebrite. Home—Cellebrite | Digital Intelligence for a Safer World. Available online: https://www.cellebrite.com/en/home/ (accessed on 7 March 2021).
20. ReFirmLabs. GitHub—ReFirmLabs/binwalk: Firmware Analysis Tool. Available online: https://github.com/ReFirmLabs/binwalk (accessed on 26 April 2021).
21. DatCon. CsvView/DatCon. Available online: https://datfile.net/ (accessed on 15 April 2021).
22. UAV, A. Drone Data Management and Flight Analysis | Airdata UAV. Available online: https://airdata.com/ (accessed on 23 April 2021).
23. DroneDJ. The Rules for Sub-250 g Drones Might Just Surprise You—DroneDJ. Available online: https://dronedj.com/2021/04/29/what-are-the-rules-for-sub-250-gram-drones/amp/ (accessed on 30 April 2021).
24. Airdata UAV. Not Enough Force/ESC Error | Drone Notifications WIKI | Airdata UAV. Available online: https://app.airdata.com/wiki/Notifications/Not+Enough+Force/ESC+Error (accessed on 26 April 2021).