Explanatory Case Study: Digital Forensics Investigation on DJI Spark Drone

*

P Shashank Kumar
Center for Cyber Security Systems and Networks
Amrita Vishwa Vidyapeetham Amritapuri
Kollam, India
kumarshashank813@gmail.com

Sriram Sankaran
Center for Cyber Security Systems and Networks
Amrita Vishwa Vidyapeetham Amritapuri
Kollam, India
srirams@am.amrita.edu

***Abstract*—Drones are now widely used and have grown in popularity in recent years. However, as a result of their greater use, there have been more crimes involving drones. In this explanatory case study, digital forensics methods are used to analyze a DJI Spark drone discovered at a crime scene. The purpose of this inquiry is to obtain vital data that might help with the investigation of drone-related crimes. The drone's memory card and remote controller, which have flight records, pictures, and videos on them, have important details about the crime and how the drone was used. We gather and examine this material using digital forensics techniques. Investigative personnel will then be able to recognize potential suspects and comprehend the drone's participation in the crime. Important details, such as the drone's flight path, the location of the murder scene, and the identities of the people involved, are revealed by the recovered data. This explanatory case study emphasizes the importance of digital forensics in the analysis of drone-related crimes. Drones will probably be employed more frequently in criminal acts as they become more prevalent in society. Investigators may keep ahead of the curve and efficiently use drones as a source of priceless evidence in criminal investigations by using competent digital forensics techniques.**

***Index Terms*—Explanatory case study, Digital Forensics Investigation, DJI Spark Drone, Data Recovery, Evidence Analysis, Cybercrime, Aerial Photography.**

I. Introduction

Over the past few years, the use of drones has increased substantially in both private and professional contexts, as well as in illegal operations such as corporate espionage. Consequently, the field of drone digital forensics has become a burgeoning area of study. This explanatory case study examines the methods used in digital forensics to investigate a DJI Spark drone involved in a corporate espionage case, highlighting the particular difficulties and factors involved in drone forensics.

Data recovery from the drone's storage medium is one of the primary difficulties in drone forensics. In this instance, the forensic team accessed data from the drone's memory card and remote controller using specialized tools. The file Identifies the applicable funding agency here. If none, delete this. System analysis techniques extract pertinent data, including flight logs, pictures, and videos. Analyzing metadata, which is frequently crucial in investigations, is another challenge in drone forensics. In this case, the forensic team used metadata analysis techniques to analyze the GPS data found in the drone's flight logs. This makes it possible to pinpoint the location of the drone at various points during its flight as well as the location of the corporate espionage. Data carving and recovery techniques are used to analyze drone data. These methods enabled the forensic team to recover deleted data that was essential for locating the culprits behind the industrial espionage.

This explanatory case study analyses the storage media as well as the methods and procedures applied to analyze drone data. To extract and analyze pertinent data from the drone, the forensic team used a range of techniques, including keyword searches, metadata analysis, and file carving. This explanatory case study highlights the need for digital forensics in drone investigation projects. Drone forensics will likely confront new obstacles as drone technology develops but with the creation of new methodologies and tools, digital forensics experts will be able to efficiently employ drones as a source of priceless evidence.

Identify applicable funding agency here. If none, delete this.

II. Related Work

Several studies have recently concentrated on the examination of digital forensics on DJI drones. M. P. Gupta et al. examined the DJI Phantom 4 drone using digital forensics, while Y. Li and L. Li looked into the DJI Phantom 3 and Mavic Pro drones. While M. Shariatmadari et al. concentrated on the DJI Inspire 1, A. Kumar and P. Singh examined a DJI Phantom 4 Pro drone. This research investigated drone forensics and offered insightful information on the digital forensic examination of DJI drones, especially the DJI Spark drone.

The papers included various file carving, GPS analysis, image analysis, and data extraction methods and tools utilized in the forensic study of drones. These methods assisted researchers in pinpointing the drone's flight path, the places it

visited, and the information it gathered while in the air. The investigations also offered suggestions for enhancing the precision and dependability of the digital forensic examination of drones, including safeguarding the reliability of the evidence and tracing the course of analysis.

The results of these investigations might be used as a beneficial resource when doing an explanatory case study on the digital forensics examination of the DJI Spark drone. The case study will offer a thorough analysis of the digital evidence obtained from the drone and offer insightful information regarding its behavior and mode of operation. The outcomes of this case study will improve forensic investigators' expertise and help them better grasp the capabilities and constraints of the DJI Spark drone.

III. Contemporary literature

With a particular focus on examining DJI drones, Data extraction, and criminal investigation have been the focus of drone forensics research on DJI drones. Case studies on DJI drones like[21][22] Spark, Mini 2, and Mavic Air 2 use DatCon and CSVView to extract data. DJI drone data extraction[23], user identification, flight path reconstruction, and criminal investigation data recovery are highlighted. Drone[24][25] forensics standardization improves incident analysis. This study enhances forensic investigators and shows DJI drone forensics' potential in criminal investigations.

Pathak et al. (2019) offer a 99 percent accurate remote user authentication [26]technique for IIoT and embedded device security and privacy using PRNU and fingerprint biometrics. Their approach tackles IIoT deployments' heightened susceptibility during the COVID-19 pandemic, improving privacy and attack defense. In embedded device [27]forensic investigations, Nimmy et al. (2022) propose the SMART strategy to protect criminal suspects' data and privacy. They also propose a PRNU-based smart home authentication strategy for [28]resource-constrained IoT devices without passwords or smart cards. These researches advance drone forensics and IIoT and embedded device security.

IV. Methodology

In this case study, it was found that a DJI Spark drone had received sensitive data from a business, raising questions about a security breach. After noticing strange drone activity close to its protected facilities, the business launched a digital forensics investigation. As soon as the drone was discovered on the company's property, it was confiscated, and a forensic photograph was taken for examination. According to the information stored on the device, which included pictures, movies, and metadata, the drone had taken pictures and videos of the company's private facilities and data. The research team was able to pinpoint the time and place of data gathering by using the GPS metadata that was attached to the photographs and videos. Digital forensics analysis showed that the DJI Spark drone had definitely recorded the business's confidential information, possibly resulting in a security breach.

This incident emphasizes how crucial it is to put in place strong security measures to protect sensitive data, especially in view of the fast-advancing state of drone technology. Organizations need to be on the lookout for drone-related security breaches since hostile actors can utilize drones to collect sensitive data secretly. To avoid such occurrences, businesses are advised to create and enforce thorough drone security policies. These regulations should specify how to use drones, where they are permitted to fly, and how to spot and respond to any potential security incidents involving drones. Additionally, it's crucial to guarantee that staff members receive sufficient training in drone security procedures and are aware of any potential hazards posed by drones. Organizations must also keep up with the most recent developments in drone technology and security protocols if they want to safeguard themselves against security breaches.

A. Drone

Fig. 1. DJI Spark Drone With Remote Controller

1) Hardware:

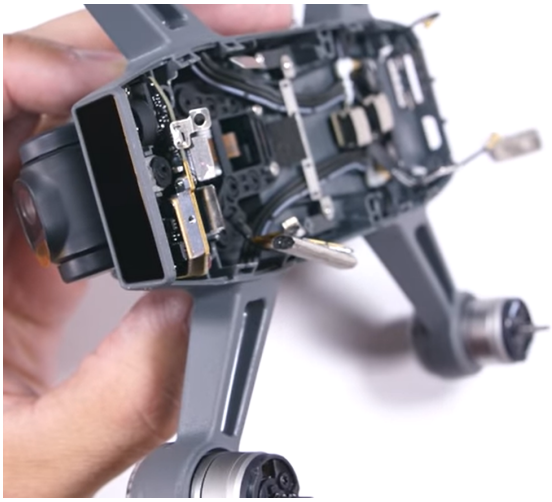

Fig. 2. Camera, Propellers, Battery, Light bridge

Camera: The Spark has a 12-megapixel camera that is capable of capturing still photos and 1080p videos (Fig. 2).

GPS module: A GPS module allows the drone to know its location and fly accurately (Fig. 3).

Motors: The Spark has four brushless motors that power its flight (Fig. 3).

Propellers: The drone is equipped with 2-blade plastic propellers (Fig. 2).

Flight control system: A flight control system monitors and manages the drone's flight (Fig. 2).

Battery: A rechargeable lithium-ion battery powers the drone (Fig. 2).

Sensors: The Spark has various sensors, including a 3-axis accelerometer, a 3-axis gyroscope, and a barometer (Fig. 3).

Remote control: A remote control or mobile device can be used to control the drone (Fig. 1).

Light bridge: Light bridge technology provides a high-quality video feed from the drone to the remote control or mobile device (Fig. 2).

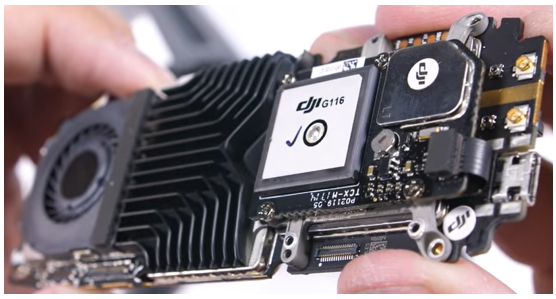

Fig. 3. GPS module, Motors, Sensors

2) Software:

DJI GO 4 app: The DJI GO 4 smartphone app lets DJI drone owners alter their drone's settings. The software lets users control their drones' flight, status, camera, and gimbal settings. Users may also see their drone's surroundings via the app's real-time camera stream. Battery life and GPS signal quality may be checked on the DJI GO 4 app. Altitude, speed, and flying mode are controlled through the app's simple UI. The app's intelligent flight mode lets users shoot footage as their drone follows a path. The DJI GO 4 software gives DJI drone customers unprecedented access to their aircraft's settings and a multitude of options for filming and recording stunning aerial footage.

Flight control software: Flight control software is a must for any drone system to operate effectively and safely. In most cases, the drone already has the flight controller pre-installed. This device acts as the drone's brain and controls its direction, position, and movement in the air. In order to stabilize the drone and account for environmental elements like wind and turbulence, flight control software uses sensors and algorithms. This software also controls the drone's takeoff, landing, and flight stability. Modern engineering has improved drone functionality with features like GPS tracking, autonomous flight modes, and obstacle avoidance. Users can control drones effectively and easily with the use of flight control software.

Camera software: It is essential that flight control software be installed on any drone system in order to assure secure and effective drone flight operations. Usually pre-installed with the drone, the flight controller serves as its brain, steering its movement in the air and determining its orientation.The drone's takeoff, landing, and flight stability are managed by flight control software, which employs sensors and algorithms to stabilize the drone and account for environmental elements like wind and turbulence. To improve the drone's usefulness, cutting-edge technology like GPS tracking, autonomous flight modes, and obstacle avoidance are integrated into the software.The takeoff of the drone is managed by flight control software, which also allows users to operate drones quickly and efficiently.

GPS software: In order to calculate the position, height, and speed of the drone, GPS software, which triangulates signals from a minimum of four GPS satellites, is largely used for drone navigation. With the help of latitude, longitude, and altitude data, this software makes it possible to display the drone's location on user interfaces or maps. In order to ensure safe operation, it also constantly checks the drone's speed. Applications involving aerial photography or surveying, in particular, require altitude data. Geo-fencing is an advanced GPS function that deters unauthorized flights, which can further improve safety. In order to operate drones precisely and securely, GPS software is essential.

Obstacle avoidance software: Obstacle avoidance software is essential in locations with multiple obstacles including buildings, trees, and other drones. This software uses several sensors to quickly avoid obstructions. The program may change the drone's height, speed, and direction in real time. Obstacle avoidance is important in rough terrain or many obstacles. Since pilots can map their 3D environment and establish better flying pathways, drone operation is safer, more secure, and more effective. Drone safety relies on obstacle avoidance software.

Autonomous flight modes: Modern drones have autonomous flight modes like Active-Track and Quick-Shot that allow them to fly and carry out tasks without user control. These modes, such as Rocket, Drone, Circle, and Helix, use sophisticated algorithms and computer vision to track and follow moving objects or to take cinematic pictures and movies with pre-planned flight routes. Users can also guide the drone to particular destinations or regulate its movements with easy hand gestures in the Tap Fly and Gesture Control modes. These autonomous flight modes increase drone operations' inventiveness and safety while increasing consumer access to cutting-edge features and reducing the potential for human error.

Firmware: Drone firmware connects hardware and software control systems. The drone's motors, sensors, and software wouldn't work without firmware. DJI releases firmware updates to improve performance, security, and stability. Firmware updates repair bugs and prevent hacking, ensuring the drone's efficiency and security. Upgrade firmware to avoid drone mishaps. Drone owners must update the firmware to maximize

efficiency and safety.

B. Drone Crime Questions

The 5W1H questions (who, what, when, where, why, and how) are the backbone of every thorough report in a criminal investigation. Before commencing a drone investigation, it's important to carefully examine the questions being asked. Following are some goals established by the 5W1H formula:

Who: People who are suspects, witnesses, or victims in the inquiry The purpose of this investigation is to track down the drone pilot from the logs of their flights.

Where: where the crime took place and any additional places that may be important. Using GPS coordinates, this investigation creates a virtual flight plan.

What: Explain the specifics of the alleged criminal conduct.

When: When the offense is committed and any other pertinent details In this research, we look at how a drone's time stamp stacks up against a cell phone's and draw some conclusions about the two devices' respective chronologies.

Why: Why a crime is committed at a certain moment.

How: How did they pull off the crime?

C. DJI Drone Crime Questions

When conducting a digital forensic investigation into crimes involving DJI drones in secure facilities, the following questions may be relevant:

a. What type of data is stored on the drone?

b. What is the origin and destination of the drone flight?

c. What is the drone's flight path and altitude?

d. Who had control over the drone during the flight?

e. What type of data is transmitted from the drone to the remote controller or other devices?

f. Was any unauthorized access attempted or made to the drone or its stored data?

g. Was the drone's firmware or software altered or modified in any way?

h. Can any relevant video or photo footage be recovered from the drone or its storage media?

i. Can any flight logs or other relevant data be recovered from the drone or its storage media?

V. Processes for experiments

A. Problem Statement

A digital forensics examination found that the DJI Spark drone took pictures and videos of the firm's secure data centers and other locations. If hostile actors use these images and videos to their advantage, the company may suffer catastrophic financial and brand harm (Fig. 4). The GPS data that was included with the media was essential for monitoring the drone's flight route, pinpointing the exact place and moment when the material was collected, and possibly even identifying any suspects who may have flown the drone over the corporation's property.

This emphasizes how crucial it is to capture and protect digital evidence in forensic investigations since it can be used to pinpoint likely suspects and reenact the sequence of events leading up to a security breach. This information can only be provided by the GPS metadata associated with the media, making it a crucial component of forensic investigations.

B. Steps - Digital Forensics on DJI Spark Drone

a. Seize the DJI Spark drone as well as any linked storage devices, such as SD cards or mobile devices used to operate the drone, and turn them over to the appropriate authorities.

b. Create a forensic image of the storage devices with the use of specialist software in order to get an identical, bit-for-bit replica that can be analyzed.

c. Conduct an analysis of the forensic picture to get any metadata and GPS data that may be associated with the photographs and videos that are at issue.

d. Check that the data that is extracted is genuine and hasn't been tampered with.

e. Conduct an analysis of the GPS data to establish the location and time of the sensitive facility, as well as the data collection carried out by the drone.

g. To construct a comprehensive picture of the occurrence, it is necessary to correlate the findings with other pieces of information that are at your disposal, such as the records kept by the firm.

h. Give a presentation on the findings and a full report on the procedure that was used for the study and the conclusions.

C. Steps followed for DJI Spark Drone

The following information may be gathered by digital forensics from the crime scene where a DJI Spark drone is used to acquire confidential data:

Physical evidence: In order to get insight into the crime, it is important to thoroughly search for any physical evidence, such as the drone, storage devices, and any other pertinent equipment.

1. DJI Spark Drone
2. Pen Drive
3. Apple Laptop
4. Hard Disk
5. Remote Controller (Mobile Phone)

Network information: If the drone is used in conjunction with other devices or linked to a network, the source and destination of any data transfers can be deduced by analyzing the network logs and IP addresses associated with those devices.

Log files: Log files from the drone, the software that controls the drone, or any other relevant equipment can offer useful information on the activities and use history of the drone.

User data: Extraction of user data such as login passwords, emails, and chat logs might help identify the people involved and their motivations for engaging in the activity.

NOTE: It is essential to keep in mind that the particulars of the case and the condition of the evidence will determine the kind of information that may be gleaned from the crime scene. The process of digital forensics is intricate and meticulous, and in order to acquire the correct findings, one needs both specialist expertise and specialized instruments.

VI. Analysis and Findings

A. Steps for the Data Collection from the Drone

a. There are two methods you can use to retrieve a DJI drone's flight logs, notably if you're using an iPhone or iPad that runs the iOS operating system. The first choice entails using a USB connection to attach the device to a computer and the iTunes program to gain access to the file-sharing options on the device. The user can then choose the DJI Go 4 app and save the log files right to their computer from there.

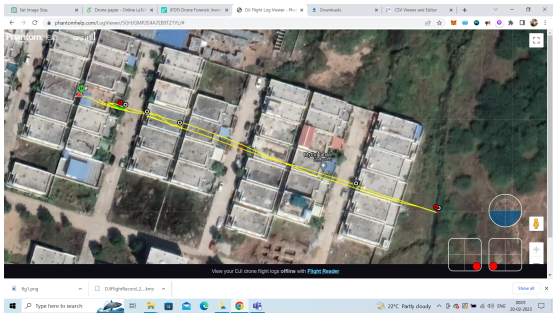

Fig. 4. Flight path

b. To extract the logs, go to the website Phantom-Help.com (https://www.phantomhelp.com/Phantom-4/) (Fig. 5). Download logs from the website directly using the DJI Go 4 app by connecting the device to a computer and choosing it.

c. If we don't know how to use iTunes or don't have access to a computer, this solution might be better.

d. PhantomHelp.com also provides a variety of tools for DJI Spark drone owners, such as instructions on how to operate the device, answers to frequently asked issues, and access to a log file analysis service.

e. This service is able to upload their log files for a thorough examination of their flight data, which includes crucial information like GPS accuracy and flying performance. The main purpose of this research is to assist users in locating and fixing any problems they might be having with their DJI drone.

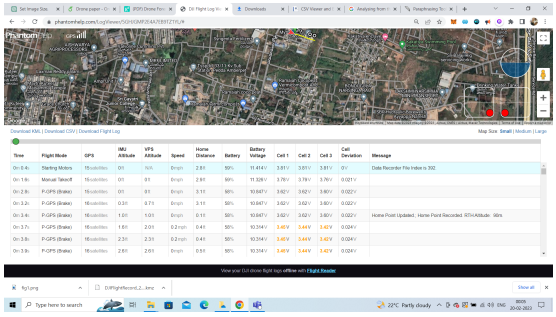

Fig. 5. Flight Logs,GPS(Global Positioning System) data

VII. DGCA's(Directorate General of Civil Aviation) Guidelines

All drone operators are expected to adhere to the rules established by the Directorate General of Civil Aviation (DGCA), the regulatory authority in charge of managing drone activities in India. These rules are intended to ensure the responsible and safe usage of drones as well as to stop prohibited actions like privacy invasion.

In this incident, a DJI Spark drone is found and taken into custody while allegedly invading privacy and obtaining sensitive information from a local firm. Under Indian law, such behavior is prohibited, and the operator may face legal repercussions.

Drone use for unauthorized surveillance or the collection of private data without the necessary authority is a crime in India, according to the country's legal system. Depending on the seriousness of the infraction, these actions may result in fines or even jail time.

As a result, the drone operator in this event is probably going to be held accountable for their acts, which might result in fines and/or jail time. The DGCA and other governing agencies in India take drone security and safety very seriously and will not put up with any unlawful or reckless drone use. All drone operators must make sure they are abiding by the rules established by the DGCA and that they are not using their drones for any illegal purposes.

Sections under which a drone operator may be booked, specifically

1. The information obtained is determined to be proprietary or sensitive information belonging to the company under Section 408 of the Indian Penal Code (IPC), which deals with criminal breach of trust. A fine, up to three years in prison, or both are possible penalties for criminal breach of trust.

2. The Information Technology Act of 2000's Section 66E addresses how privacy violations are punished and lists fines for taking, disseminating, or transmitting someone else's photograph without their permission. A fine, a term of up to three years in prison, or both are possible penalties for this offense.

3. The Official Secrets Act of 1923 protects information that is collected, and the drone operator could be charged with violating this law. A 14-year prison sentence is the maximum penalty for breaking this law.

4. If the drone is operated in a restricted area, such as a military installation or another sensitive place, the drone operator could be charged with criminal trespass under Section 447 of the IPC. A fine, a term of up to three months in jail, or both are possible penalties for this offense.

NOTE: In order to prevent any legal concerns, it is crucial for drone operators to abide by all rules and regulations established by the DGCA and to obtain the necessary authorization prior to undertaking any drone operations.

VIII. Experiment Results

A digital forensics examination was carried out after a drone was seen flying suspiciously close to a company's secure facilities, and the findings were disturbing. The organization's private facilities and sensitive data were discovered to have been photographed and recorded by a DJI Spark drone. The breadth of the breach was determined by [12], [14], [13], [7],

[17], and the investigative team's painstaking analysis of the data, including metadata, saved on the drone. Investigators were able to determine the position and time of capture with the use of GPS metadata, which also allowed them to determine the extent of the incident and any affected personal data. The results of the inquiry point to a possible security lapse and highlight the necessity of appropriate security measures to safeguard private data in the face of developing drone technology.

In order to prevent unauthorized drone use in close proximity to sensitive places, strong policies and procedures must be put in place. Security breaches are now more likely due to the rising availability and capabilities of drones. To find any present rogue drones, detection technology might also be needed. Additionally, it is critical for businesses to educate staff members on drone security protocols and potential risks, such as data privacy violations. The DJI Spark drone mishap emphasizes the significance of putting in place proper security procedures to protect crucial data (Fig. 6). The need for data protection measures as drone technology develops is shown by the investigation team's use of GPS metadata to pinpoint the place and time of capture when analyzing drone data.

CUSTOM.d	CUSTOM.u	CUSTOM.d	CUSTOM.u	OSD.flyTim	OSD.flyTim	OSD.latituc	OSD.longit	OSD.height
12/10/202	7:17:05.86	12/11/202	12:47:05.8	0m 0.4s	0.4	17.32942	78.64299	0
12/10/202	7:17:05.97	12/11/202	12:47:05.9	0m 0.5s	0.5	17.32942	78.64299	0
12/10/202	7:17:06.08	12/11/202	12:47:06.0	0m 0.6s	0.6	17.32942	78.64299	0
12/10/202	7:17:06.19	12/11/202	12:47:06.1	0m 0.7s	0.7	17.32942	78.64299	0
12/10/202	7:17:06.29	12/11/202	12:47:06.2	0m 0.8s	0.8	17.32942	78.64299	0
12/10/202	7:17:06.40	12/11/202	12:47:06.4	0m 0.9s	0.9	17.32942	78.64299	0
12/10/202	7:17:06.51	12/11/202	12:47:06.5	0m 1.0s	1	17.32942	78.64299	0
12/10/202	7:17:06.73	12/11/202	12:47:06.7	0m 1.1s	1.1	17.32942	78.64299	0
12/10/202	7:17:06.73	12/11/202	12:47:06.7	0m 1.2s	1.2	17.32942	78.64299	0
12/10/202	7:17:06.84	12/11/202	12:47:06.8	0m 1.3s	1.3	17.32942	78.64299	0
12/10/202	7:17:06.95	12/11/202	12:47:06.9	0m 1.4s	1.4	17.32942	78.64299	0
12/10/202	7:17:07.06	12/11/202	12:47:07.0	0m 1.5s	1.5	17.32942	78.64299	0
12/10/202	7:17:07.17	12/11/202	12:47:07.1	0m 1.6s	1.6	17.32942	78.64299	0
12/10/202	7:17:07.27	12/11/202	12:47:07.2	0m 1.7s	1.7	17.32942	78.64299	0
12/10/202	7:17:07.39	12/11/202	12:47:07.3	0m 1.8s	1.8	17.32942	78.64299	0
12/10/202	7:17:07.49	12/11/202	12:47:07.4	0m 1.9s	1.9	17.32942	78.64299	0
12/10/202	7:17:07.59	12/11/202	12:47:07.5	0m 2.0s	2	17.32942	78.64299	0
12/10/202	7:17:07.69	12/11/202	12:47:07.6	0m 2.1s	2.1	17.32942	78.64299	0
12/10/202	7:17:07.80	12/11/202	12:47:07.8	0m 2.2s	2.2	17.32942	78.64299	0
12/10/202	7:17:07.92	12/11/202	12:47:07.9	0m 2.3s	2.3	17.32942	78.64299	0
12/10/202	7:17:08.02	12/11/202	12:47:08.0	0m 2.4s	2.4	17.32942	78.64299	0
12/10/202	7:17:08.02	12/11/202	12:47:08.0	0m 2.5s	2.5	17.32942	78.64299	0
12/10/202	7:17:08.13	12/11/202	12:47:08.1	0m 2.6s	2.6	17.32942	78.64299	0
12/10/202	7:17:08.24	12/11/202	12:47:08.2	0m 2.7s	2.7	17.32942	78.64299	0
12/10/202	7:17:08.35	12/11/202	12:47:08.3	0m 2.8s	2.8	17.32942	78.64299	0
12/10/202	7:17:08.45	12/11/202	12:47:08.4	0m 2.9s	2.9	17.32942	78.64299	0
12/10/202	7:17:08.56	12/11/202	12:47:08.5	0m 3.0s	3	17.32942	78.64299	0
12/10/202	7:17:08.67	12/11/202	12:47:08.6	0m 3.1s	3.1	17.32942	78.64299	0.3
12/10/202	7:17:08.78	12/11/202	12:47:08.7	0m 3.2s	3.2	17.32942	78.64299	0.3
12/10/202	7:17:08.89	12/11/202	12:47:08.8	0m 3.3s	3.3	17.32942	78.64299	0.7
12/10/202	7:17:09.00	12/11/202	12:47:09.0	0m 3.4s	3.4	17.32942	78.64299	1
12/10/202	7:17:09.00	12/11/202	12:47:09.0	0m 3.5s	3.5	17.32942	78.64299	1
12/10/202	7:17:09.21	12/11/202	12:47:09.2	0m 3.6s	3.6	17.32942	78.64299	1.3
12/10/202	7:17:09.32	12/11/202	12:47:09.3	0m 3.7s	3.7	17.32942	78.64299	1.6
12/10/202	7:17:09.32	12/11/202	12:47:09.3	0m 3.8s	3.8	17.32942	78.64299	2.3
12/10/202	7:17:09.42	12/11/202	12:47:09.4	0m 3.9s	3.9	17.32942	78.64299	2.6
12/10/202	7:17:09.42	12/11/202	12:47:09.4	0m 4.0s	4	17.32942	78.64299	3.3
12/10/202	7:17:09.64	12/11/202	12:47:09.6	0m 4.1s	4.1	17.32942	78.64299	3.6
12/10/202	7:17:09.75	12/11/202	12:47:09.7	0m 4.2s	4.2	17.32942	78.64299	4.3
12/10/202	7:17:09.86	12/11/202	12:47:09.8	0m 4.3s	4.3	17.32942	78.64299	4.9
12/10/202	7:17:09.97	12/11/202	12:47:09.9	0m 4.4s	4.4	17.32942	78.64299	5.6
12/10/202	7:17:09.97	12/11/202	12:47:09.9	0m 4.5s	4.5	17.32942	78.64299	6.2
12/10/202	7:17:09.97	12/11/202	12:47:09.9	0m 4.6s	4.6	17.32942	78.64299	6.9
12/10/202	7:17:10.29	12/11/202	12:47:10.2	0m 4.7s	4.7	17.32942	78.64299	7.9
12/10/202	7:17:10.29	12/11/202	12:47:10.2	0m 4.8s	4.8	17.32942	78.64299	8.5
12/10/202	7:17:10.51	12/11/202	12:47:10.5	0m 4.9s	4.9	17.32942	78.64299	9.2

Fig. 6. Battery level, Errors malfunctions, Camera settings, GPS data

IX. Conclusion

In order to find any security flaws and safeguard sensitive data, digital forensics is essential when looking into drone-related incidents. A thorough digital forensics investigation is required in cases of corporate espionage with a DJI Spark drone in order to ascertain the scope of the breach and the sensitive data that may have been revealed. Data collection, file system analysis, metadata analysis, and recovery procedures are only a few of the methods used in this inquiry. Investigators can identify the precise location and time of capture as well as the type of sensitive information that was taken by carefully examining the data stored on the drone, including photos, videos, and metadata.

A forensic photograph of the DJI Spark drone is taken to ensure that the original data is not compromised during the data collection process, which is crucial for acquiring and protecting digital evidence for investigation. Detectives can locate the sensitive data-containing documents and folders that were captured by the drone's camera by using file system analysis. The location and time of data capture are revealed through metadata analysis, and this information is crucial to the inquiry. Recovery procedures are utilized to find buried data that may have been wiped from the device, along with deleted files. This case study highlights the value of digital forensics in identifying security flaws and safeguarding private data. Digital forensics will continue to be essential in these efforts as drone technology develops and organizations are forced to be proactive in protecting their sensitive data.

X. Future Work

Digital forensics is essential to the investigation of drone-related occurrences, especially in situations of corporate espionage utilizing DJI Spark drones, because it helps to [9] spot potential security flaws and safeguards private data. Digital forensics techniques, including data collection, file system analysis, metadata analysis, and recovery procedures, are crucial for a thorough inquiry. Using these [11] techniques, investigators can gather crucial data from the drone and spot any unusual activity.

Data collection is a crucial step in the investigation process because it makes it possible to preserve digital evidence without changing or erasing any original data. In this situation, making a forensic image of the DJI Spark drone gives an accurate and thorough copy of the data kept on the device. File system analysis, which entails looking through the device's file system and locating files that the drone had access to, is also essential for finding sensitive data.

The investigation process also includes metadata analysis, which is crucial since it provides key details like the date and place of data collection. It is essential to know the precise location of the [15] drone at the moment of data collection, and GPS metadata in particular can offer accurate location data. Recovery processes are critical because they let investigators access deleted files or other hidden data on the device, potentially revealing key pieces of evidence.

Investigators are able to uncover potential security flaws, ascertain whether the DJI Spark drone accessed sensitive data [8] without authorization, and take the necessary precautions to protect sensitive data by using digital forensics techniques. Digital forensics will continue to be a crucial tool in attaining this goal as drone technology develops, making it imperative for organizations to be proactive in protecting their sensitive data.

REFERENCES

[1] Gupta, M. P., Sheth, P. B. H., and Modi, N. P. (2017). Digital forensics analysis of DJI Phantom 4 drone. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS) (pp. 345-350). IEEE.

[2] Li, Y., and Li, L. (2018). Digital forensic investigation of DJI Phantom 3 drone. Journal of Intelligent and Fuzzy Systems, 34(4), 2211-2218.

[3] Li, Y., and Li, L. (2018). Digital forensic investigation of DJI Mavic Pro drone. In 2018 IEEE International Conference on Computational Science and Engineering (CSE) (pp. 232-237). IEEE.

[4] Kumar, A., and Singh, P. (2018). A forensic analysis of DJI Phantom 4 Pro drone. In 2018 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 1856-1861). IEEE.

[5] Shariatmadari, M., Dehghantanha, A., and Ebrahimi, R. (2019). Digital forensic investigation of DJI Inspire 1 drone. Digital Investigation, 28, 47-55.

[6] Drone Forensics: The Impact and Challenges, ATKINSON, S., CARR, G., SHAW, C. and ZARGARI, Shahrzad ¡http://orcid.org/0000-0001-6511-7646¿ Available from Sheffield Hallam University Research Archive (SHURA) at: http://shura.shu.ac.uk/28441/

[7] M. Yousef, F. Iqbal, and M. Hussain, "Drone Forensics: A Detailed Analysis of Emerging DJI Models," 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2020, pp. 066-071, doi: 10.1109/ICICS49469.2020.239530

[8] U. Jain, M. Rogers, and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, 2017, pp. 1-6, doi: 10.1109/SAS.2017.7894059

[9] Towards a Better Understanding of Drone Forensics: A explanatory case study of Parrot AR Drone 2.0 Hana Bouafif, ESPRIT School of Engineering, Tunis, Tunisia Faouzi Kamoun, ESPRIT School of Engineering, Tunis, Tunisia Farkhund Iqbal, College of Technical Innovation, Zayed University, Abu Dhabi, UAE

[10] Da-Yu Kao, Min-Ching Chen, Wen-Ying Wu, Jsen-Shung Lin, Chien-Hung Chen, Fuching Tsai, Drone Forensic Investigation: DJI Spark Drone as A explanatory case study, Procedia Computer Science, Volume 159,2019

[11] Yang, Chi-Cheng and Chuang, Hsuan and Kao, Da-Yu. (2021). Drone Forensic Analysis Using Relational Flight Data: A explanatory case study of DJI Spark and Mavic Air. Procedia Computer Science. 192. 1359-1368. 10.1016/j.procs.2021.08.139

[12] Prastya, S.E., Riadi, I., and Luthfi, A. (2017) "Forensic Analysis of Unmanned Aerial Vehicle to Obtain GPS Log Data as Digital Evidence." International Journal of Computer Science and Information Security (IJCSIS) 15 (3): 280-285

[13] Roder, A.; Choo, K.K.R.; Le-Khac, N.A. Unmanned aerial vehicle forensic investigation process: DJI phantom 3 drones as a case study. arXiv 2018, arXiv:1804.08649

[14] 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)

[15] Chicago/Turabian Style Stanković, Miloš, Mohammad Meraj Mirza, and Umit Karabiyik. 2021. "UAV Forensics: DJI Mini 2 explanatory case study" Drones 5, no. 2: 49. https://doi.org/10.3390/drones5020049

[16] l-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. [Google Scholar] [CrossRef]

[17] Technology, B. Autopsy. Available online: https://www.basistech.com/autopsy (accessed on 6 March 2021)

[18] Jain, U. A Drone Forensics Investigation Framework. Ph.D. Thesis, Purdue University, West Lafayette, IN, USA, 2017. [Google Scholar]

[19] Otero, A., and Quesada, L. (2018). Digital Forensics in Drones: A Review. In C. Valli (Ed.), The Routledge Handbook of Digital Forensics and Investigations (pp. 429-444). London: Routledge. doi: 10.4324/9781315679561-24

[20] Rashid, N., Khan, A.U., and Zeb, A. (2019). Digital Forensics Analysis of Drones: A Systematic Literature Review. Digital Investigation, 28, 1-20. doi: 10.1016/j.diin.2018.12.002

[21] Drone Forensic Investigation: DJI Spark Drone as A Case Study, by Da-Yu Kao et al., published in Procedia Computer Science (2019).

[22] UAV Forensics: DJI Mini 2 Case Study, by R.A.N.S.A. Research Team, published in MDPI Sensors (2020).

[23] Drone Forensics: A Case Study on DJI Mavic Air 2, by A.K. Singh et al., published in IEEE Xplore (2020).

[24] Drone Forensics: A Comprehensive Study on DJI Mavic Air 2, by M.A. Khan et al., published in Journal of Forensic Sciences (2020).

[25] Drone Forensics: A Review of the State of the Art, by M.A. Khan et al., published in Journal of Digital Forensics, Security and Law (2020).

[26] J. Pathak, S. Sankaran and K. Achuthan, "A SMART Goal-based Framework for Privacy-Preserving Embedded Forensic Investigations," 2019 9th International Symposium on Embedded Computing and System Design (ISED), Kollam, India, 2019, pp. 1-5, doi: 10.1109/ISED48680.2019.9096232.

[27] K. Nimmy, S. Sankaran, K. Achuthan and P. Calyam, "Lightweight and Privacy-Preserving Remote User Authentication for Smart Homes," in IEEE Access, vol. 10, pp. 176-190, 2022, doi: 10.1109/ACCESS.2021.3137175.

[28] K. Nimmy, S. Sankaran, K. Achuthan and P. Calyam, "Securing Remote User Authentication in Industrial Internet of Things," 2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 244-247, doi: 10.1109/CCNC49033.2022.9700512.