

Article

Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro

Ziyu Zhao *, Yongquan Wang and Genwei Liao

School of Law and Criminal Justice, East China University of Political Science and Law, Shanghai 201620, China; wangyongquan@ecupl.edu.cn (Y.W.); hzjd88@sina.com (G.L.)

* Correspondence: 2221110088@ecupl.edu.cn

Abstract: With the frequent occurrence of drone-related criminal cases, drone forensics has become a hot spot of concern. During drone-related criminal investigations, the implicated drones are often forcibly brought down, which poses significant challenges in conducting forensic analysis. In order to restore the truth of criminal cases, it is necessary to extract data not only from the external TF card but also from internal chip memory in drone forensics. To address this issue, a drone data parser (DRDP) is proposed to extract internal and external data from criminal-implicated drones. In this paper, we present comprehensive forensics on the DJI Mavic 2 Pro, analyzing the main file structure and encryption model. According to its file structures, three case studies are conducted on various file types (DAT files, TXT files, and default files) to verify the effectiveness and applicability of the designed procedure. The results show that the encrypted data of the implicated drone, such as GPS information, flight time, flight altitude, flight distance, three velocity components (x, y, z) and other information can be extracted and decrypted correctly, which provides evidence for the identification of the case facts.

Keywords: digital forensics; drone forensics; DJI Mavic 2 Pro; file structure; file analysis; drone data parser (DRDP)



Citation: Zhao, Z.; Wang, Y.; Liao, G. Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro. *Drones* **2024**, *8*, 281. <https://doi.org/10.3390/drones8070281>

Academic Editor: Abdessattar Abdelkefi

Received: 30 April 2024

Revised: 15 June 2024

Accepted: 18 June 2024

Published: 22 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the development of drone technology, drones have proliferated around the world. The embedded device of the drone, equipped with wireless communication capabilities and tethered to the controllers, ascends into the sky to perform aerial tasks, earning the moniker “Mobile Internet of Things” [1]. Nowadays, drones are useful across diverse domains encompassing law enforcement [2], public safety operations [3], search and rescue missions, agricultural practices, and recreational pursuits. Projections indicate that, by the year 2025, the drone market is poised to yield a revenue stream of \$18 billion, underscoring the significance and commercial viability of this transformative technology.

However, it is crucial to note that drones, while possessing significant potential for beneficial applications, are not immune to exploitation for fewer benign purposes. The small size and remote operability of drones allow them to access otherwise inaccessible places, a feature that has been useful in military operations and conflicts. The increase in commercial drones has raised significant concerns regarding their misuse in criminal activities. It has gained urgency due to several notable incidents. For instance, in July 2021 [4], an Italian prisoner shot at fellow inmates with a weapon believed to have been smuggled in by a drone through the bars of their cell. In April 2022 [5], a tourist-operated drone crashed onto the roof of Rome’s historic Palazzo Venezia. The drone was seized during search measures, and the tourist now faces potential criminal prosecution. In June 2022 [6], a drone was reported to have hindered the approach of a passenger plane to the capital’s BER airport. The litigants in these cases all used DJI drones, which are the same series studied in this paper. Due to the proliferation of commercial drones and the

surge in criminal activities involving them, there is an urgent need to develop reliable drone forensics technology. We anticipate a growing need as drones become more readily available and used in various criminal activities. In the above cases, investigators need to analyze drone-related data to restore the facts, which is crucial for preventing illegal activities and ensuring flight safety.

In criminal cases, such as drug smuggling and contraband transportation, law enforcement officials may choose to forcibly shoot down the drone. However, identifying the drone user can be a significant challenge for forensic analysis. During the past 15 years, there has been a growing interest in digital forensic research to anticipate the potential misuse of drones in different criminal contexts. Drones possess several data interfaces, including internal, external, wired, and wireless [7], which makes them vulnerable to external attacks. The vulnerabilities enable attackers to obtain access to a drone's internal data either physically or through remote means. Consequently, attackers can forge and inject messages that may influence the decision-making processes and control of the drone's internal system potentially causing drone accidents. For instance, suspects might orchestrate drones in restricted airspace or deviation from designated flight routes. As intricate electronic systems with networking capabilities, drones and their associated apparatuses store data encompassing flight patterns, GPS coordinates, and user profiles. In adjudicating criminal proceedings, legal authorities are tasked with amassing evidentiary material and subjecting it to thorough scrutiny to ascertain the veracity of allegations.

The process of digital forensics involves investigators uncovering the truth in criminal cases by examining data in digital systems. According to the National Institute of Standards and Technology (NIST), the digital forensic investigation is typically structured into four main phases: collection, examination, analysis, and reporting [8]. On the other hand, drone forensics focuses on scientifically analyzing flight data, user information, and other relevant data stored in drones and associated equipment to establish evidence. In January 2022, the NIST and the Scientific Working Group on Digital Evidence (SWGDE) introduced the Best Practices for Drone Forensics [9]. This publication defines system requirements for the storage, processing, equipment, extraction, and analysis of drone data. Conversely, in October 2023, the Ministry of Public Security of China issued a technical specification for examining digital data in civil drones [10]. The guidelines outline the requirements for extracting, analyzing, and identifying data from civil drones, with the standard coming into effect in December. Despite ongoing advancements in the field of digital forensics, numerous challenges remain to be addressed.

This work presents a comprehensive study of the forensic methods for the DJI Mavic 2 Pro, including an analysis of its internal structure and working mechanism. The main contributions of this research are as follows:

1. We first conduct an analysis of the internal storage structure of the DJI Mavic 2 Pro small drone system to highlight the forensic challenges it presents. Subsequently, we review existing forensic methods and evaluate their applicability while clarifying the data sources for drone forensics. Moreover, we propose a model for extracting data from drones.
2. Using the DJI Mavic 2 Pro as a case study, we analyze the structure of the extracted file and proceed to conduct three case studies on different file types (DAT files, TXT files, and default files). Subsequently, we design the parsing process of extracted files and further develop a specialized forensic tool known as the drone data parser (DRDP).
3. Finally, we verify the applicability of evidence-collection methods and tools through experiments. Notably, we successfully parse encrypted data from the drone in question, which emphasizes the effectiveness of the proposed forensic methods and tools.

A multi-pronged research approach is deployed to ensure a comprehensive understanding of drone forensics and validation of the forensic process. This approach combines a literature review, empirical examination, and case study analysis. The study's results have the potential to significantly impact academic research and practical applications. Furthermore, they may provide law enforcement agencies with effective tools for investigating

drone-related incidents and contribute to the advancement of research on drone forensics technology within the field of drone forensics.

This paper is organized as follows: Section 2 starts with a summary of previous research on drone forensics. Following this, Section 3 details the experimental setup and the data extraction model used for analyzing drones. In this section, the analysis of data retrieved from storage devices is presented, along with an explanation of the drone's proprietary file structures. Additionally, the development of the drone data parser (DRDP), a tool used for drone forensics, is described. The findings and constraints identified in our analysis are discussed in Sections 4 and 5.

2. Related Work

Drone forensics is a hot topic for drone data forensics and analysis; the existing drone forensics method can be divided into theoretical forensics and data-driven forensics [11].

Theoretical forensics focuses on model construction and data extraction. In terms of forensic model construction, Arafat al-Dhaqm et al. (2022) [12] proposed a comprehensive forensic model for theoretical forensics, and the proposed model can investigate different types of drone data adaptively. Fahad Mazaed Alotaibi et al. [13] proposed a comprehensive collection and analysis forensic model for drone forensics. By data-interdependent processes and evidence reconstruction, the proposed drone forensics model outperforms other forensics models in terms of standardizing evidence collection. However, the aforementioned forensic models are not directly connected with forensic procedures, leading to performance degradation in drone forensics and providing limited assistance in real cases.

In terms of data extraction, Qingyi Tian and Baoshun Li (2017) [14] extracted and analyzed the flight data of the DJI Phantom 3 from the internal TF card, mobile terminal APP, and external TF card. The flight data could be obtained directly since the DJI drone data from the mobile terminal APP were not encrypted or encoded. Therefore, this study is not applicable to encrypted data scenarios. Zijun Yan, Mingyu Fan, et al. (2017) [15] have proposed solutions for identifying drone users and monitoring their behavior, including a triple identity verification mechanism and a user threat decision model. The drone data used in this research was also not encrypted. Therefore, these solutions have not yet been applied to actual cases due to the process of drone data extraction being based on unencrypted data.

Data-driven forensics focuses on extracting data from drones and related devices. In terms of drone data forensics, Maryam Yousef et al. [16] used iOS-based smartphone devices to conduct a forensic investigation of Unmanned Air Systems, specifically the DJI Mavic Air. Hana Bouafif et al. [17] conducted forensic analysis on the Parrot AR drone version 2.0 and found that the internal file system of the drone can be connected and accessed through the FTP protocol, which is the commonality between drone forensics and other equipment forensics, and summarized the differences of drone forensics. Maryam Yousef [18] analyzed data extracted from four types of drones. The applicability and related functions of several commercial and open-source forensic tools are also compared. Ravin Kumar et al. [19] extracted and analyzed GPS data from three different families of drones and visualized the location information. This work introduced a new utility called FlyLog Converter Tool, which can process and convert the Parrot drone's flight log from a ".txt/.json" format to an easy-to-understand ".csv" format. Moreover, Thomas Edward Allen Barton et al. compared the operational variations of the Drone DJI Phantom 3 and the AR Drone 2.0. They discovered that log information and flight logs are commonly stored in the data of the controller application.

In addition to investigating and analyzing drone data, the data from relevant devices also need to be analyzed. Farkhund Iqbal et al. [20] used a variety of smartphone devices, to conduct the forensic analysis of unmanned aerial systems in different operating systems. In addition, the author utilized various DJI tools and software to perform logical backups of the specified mobile phone models. They then conducted forensic analysis on the drone data within the backup files, revealing a substantial amount of forensic data within the DJI

Phantom 4 APP. Graeme Horsman et al. [21] extracted and analyzed data from the Parrot Bebop drone and FreeFlight3 mobile terminal control software, providing acquisition and analysis instructions for the internal storage of the device, as well as on-board flight data, media data, and operating system-related information.

The existing data-driven forensic methods have analyzed the flight logs of drones and other devices. They rely on existing forensics tools to analyze GPS data and visualize the flight path. However, these studies have not delved into the specific file structure and encryption methods of drones, which hinders further research. In conclusion, there is an urgent need to address the research problem of extracting and analyzing the file structure and encryption methods of drones. Therefore, we propose a drone data parser (DRDP) to extract data from the drones involved in criminal cases and conduct three case studies on the structure and encryption method of DAT, TXT, and default files, which provide detailed guidance for decrypting drone data and technical support for restoring the truth of drone cases in the future.

3. The Drone Forensics Tool: A Drone Data Parser (DRDP)

Before collecting evidence, it is important to ensure that the investigation focuses on the drone's trajectory and user information. The drone has several associated devices that store data related to it. Forensic investigators can extract and analyze data in drone investigations, providing police with essential reference material to solve cases. This section describes the data extraction method for current domestic drone forensics. The method consists of five stages [22]: device reset, data creation, model construction, data collection, and tool creation. Table 1 lists the equipment and tools used during the research process.

Table 1. The equipment, tools, and software used in the research.

Device	Name	Description
Flight system	DJI Mavic 2 Pro	Quadcopter with serial number "08RDE4E00102YL"
	Drone internal TF card	Originally used to store flight data, this function is no longer available
	Drone external TF card	Used to store pictures and video files generated during the flight
	DJI remote control	DJI Mavic 2 Pro matched remote control for flight control
	Redmi 6 Pro	Android 7.0, GPS navigation, used as a display
	DJI GO 4	Synchronizes flight records in real time
Forensic equipment and tools	Forensics workstation	The corresponding environment has been configured for Windows10
	Memory card reader	This is used to read the data of the internal and external TF card of drone
	FTK imager	TF card image production
	Android backup tool	Used for backup extraction and image production of Android phones
	Ida Pro 7.0	For software disassembly research, analysis of user data information
	DRDP Tool	Used for drone flight data and user data analysis
	DJI Assistant 2	For the export of volatile storage data of drone
	JD-GUI 1.6.5	Decompiler tool for reverse engineering analysis of DJI GO 4

3.1. System Reset

To ensure that the drone and Android phone meet the necessary forensic investigation requirements, the initial step involves performing a factory reset on both devices. Subsequently, the Android phone should be updated to Android 7.0. To restore the drone to its factory settings, DJI Assistant 2 [23], a parameter adjustment software for drones, should be installed on a forensic workstation. DJI Assistant 2 supports multiple DJI models, including DJI Mavic Air, DJI Mavic Pro, and DJI Goggles. This software enables users to quickly adjust the parameters of DJI drones and update product firmware. It also allows partial drone control from a computer and extraction or deletion of flight data and media files from the internal storage device.

3.2. Data Creation

The DJI GO 4 [24] application was installed on an Android phone and utilized with the DJI remote control for multiple drone flights. The phone was used to monitor the flight status and capture photos and videos for future use.

3.3. Model Building

Data extraction from drones involves retrieving data from the drone's onboard storage, the mobile terminal control device, and the payload system. Drones establish communication with mobile terminals through WiFi, enabling the mobile app to exhibit the drone information and manage its flight, thereby facilitating user interaction. Additionally, DJI drones store flight data in the cloud, which can be synchronized through the mobile app. The drone's body includes internal chips for storing flight data, in addition to built-in and external TF cards. Using the DJI Mavic 2 Pro as an example, we analyze the operational principles of the drone and associated terminal devices. We have distilled a data extraction model for drones, which is illustrated in Figure 1.



Figure 1. Drone data extraction model.

3.4. Data Acquisition

According to the extraction model, data extraction is carried out on drones and related equipment, which includes four storage devices: the drone's internal memory chip, the Android phone connected to the mobile terminal, and the internal and external TF cards.

3.4.1. Drone Internal Memory Chip

The flight log is stored in the drone's internal chip. To obtain the internal data, we connect the powered drone to the forensic workstation and use DJI Assistant 2, the official software, to export multiple DAT files. These files are saved with the naming convention "DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT". Upon initial examination, we observed that the DAT files exported through DJI Assistant 2 were compressed using zlib. After decompression, the DAT file sheds the 283-byte zlib header and is then stored in little-endian mode. The decompressed file follows the naming

convention “FLY###.DAT”, where “###” denotes a sequential number. Notably, this file type hosts a wealth of drone attribute data and flight information.

3.4.2. Mobile Terminal Android Phone

Upon analysis, it was found that multiple TXT files, which contain flight data, are located in the “/DJI/dji.go.v4/FlightRecord” path on the mobile device. The files are named following the convention of “DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt”, with the DateTime in the file name matching the start time of the drone’s flight record. The contents of these records encompass details such as longitude, latitude, altitude, flight status, and battery power. Furthermore, the DJI GO 4 mobile application also writes flight data to the “/DJI/dji.go.v4/MCDatFlightRecords” directory on the mobile terminal. The naming convention for these files is “YY_MM_DD_[HH-MM-SS]_FLY###.DAT”, with “###” representing a sequential number. The timestamp in the DAT file name corresponds to the commencement time of the drone’s flight record, containing a substantial volume of flight data. Additionally, a reverse engineering analysis was performed on the DJI GO 4 application, which was decompiled using JD-GUI. The user information is found in the “mmkv.default” file of the mmkv structure, located in the /data/dji.go.v4/files/mmkv directory.

3.4.3. Internal TF Card

After turning off the drone and remote controller, we removed the internal TF card and used FTK Imager to create an image of the card with a hash check. We then formatted the TF card and analyzed the image file of the internal TF card from multiple flights. It was discovered that the device did not store any data. Before formatting, the internal TF card contained multiple files that followed the naming rule “FLY###.DAT”. The files were created around July 2017, with consecutive numbers denoted by “###”. It has been confirmed that, since the July 2017 update of the DJI drone firmware, the internal TF card ceased to be used as a storage device. Instead, the flight data is now stored on the drone’s internal chip.

3.4.4. External TF Card

The external TF card is used to store media files, such as pictures and videos, captured during the flight. These files are located in the “/DCIM/100MEDIA” directory and follow the naming rule of “DJI_####.JPG” and “DJI_####.MOV”, where “####” represents a series of consecutive numbers. The file metadata includes information such as shooting latitude and longitude, altitude, time, and camera model.

3.5. Tool Creation: Drone Data Parser (DRDP)

Important forensic data were obtained through the extraction of relevant files of the DJI Mavic 2 Pro. The process of analyzing relevant files is shown in Figure 2.

The drone data parser (DRDP) was developed based on the outlined analysis procedure. It is a tool designed to analyze DAT files in DJI Mavic 2 Pro, as well as TXT files, DAT files, and default files on mobile terminal devices. The tool is compatible with Python 3.7 and is primarily built on the principles of reverse engineering from DatCon. DRDP enables the processing of individual DAT, TXT, and default files, with the parsing target determined by the input parameters provided during execution. To use DRDP, users can execute the following command: `python main.py [-d] [-t] [-u]`. The command options include using -d to parse DAT files in the specified folder, -t to parse TXT files in the specified folder, and -u to parse the default file in the specified folder. The tool can be accessed at <https://github.com/EveZzy/DRDP> (accessed on 1 May 2024).

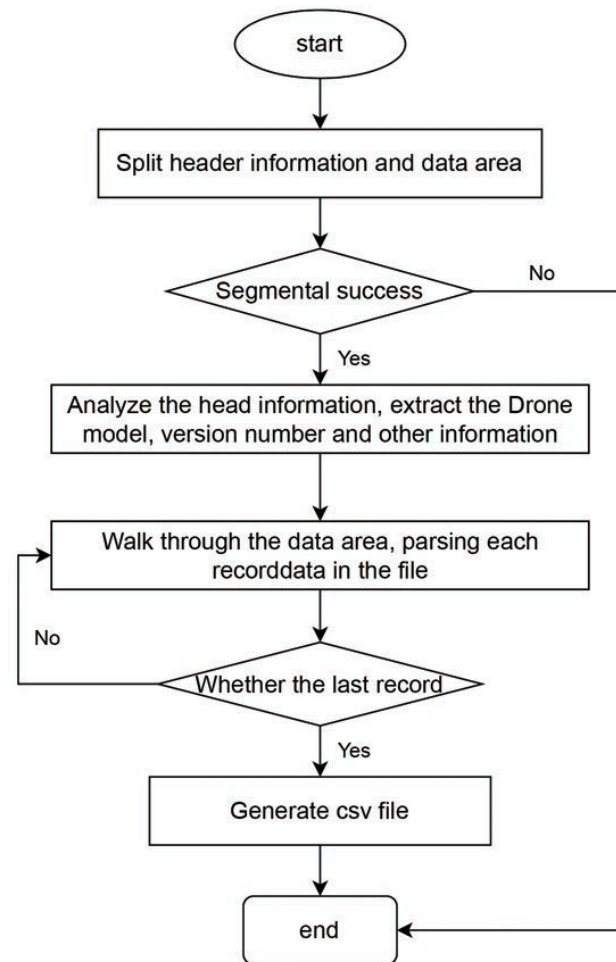


Figure 2. Drone-related file parsing process.

4. Three Cases of Digital Forensics on DJI Mavic 2 Pro

Since the firmware update in July 2017, data on the DJI drone system, including the drone body and related mobile terminal apps, have been stored in encrypted form. The data cannot be displayed directly, and the file structure is also different from before updating. Drone flight data originate from two main sources: the DAT file in the drone's internal storage chip and the DAT, TXT, and default files in the mobile terminal application DJI GO 4. The drone's internal chip allows communication and data exchange with external networks, while the mobile terminal application DJI GO 4 controls drone flight and stores data on the mobile device, which is essential in drone-related cases. The encrypted and encoded files can be decrypted and decoded to extract GPS data, motor information, flight status, and other relevant information. Additionally, the DJI GO 4 app provides relevant information about drone users, such as username, nickname, phone number, and other data. To showcase the utility of the developed procedure, three case studies were conducted using different file types (DAT files, TXT files, and default files), with the DJI Mavic 2 Pro serving as the illustration [25].

4.1. Case 1: DAT Files Extracted from Drone and Mobile Device

1. DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT

The DAT file was analyzed, and "DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT" was decompressed using zlib. The 283 header bytes were removed, and the remaining content was segmented into 256-byte DAT header information and N flight records, each referred to as a record. The structure of the DAT file repeats until all records are concluded. It is important to note that records can have multiple data interpretations

depending on the type. The length of each DAT file varies depending on the written data type, but they all follow a common structure. Each record begins with a fixed starting value of 0×55 and ends with the last 2 bytes of check digits. After analysis, we determined that the length of a record can range from 14 to 245 bytes. In summary, the structure of the export DAT file is shown in Figure 3.

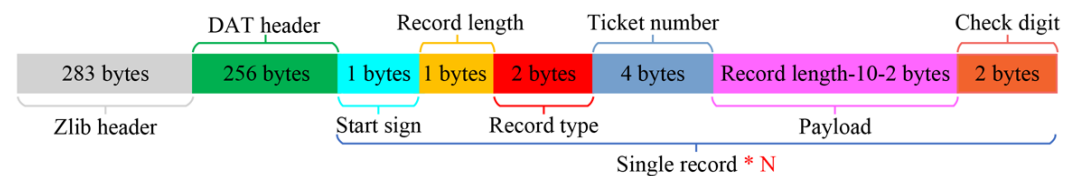


Figure 3. “DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT” file structure. The “DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT” file consists of a 283-byte zlib header, a 256-byte DAT header, and N records.

Each record begins with $0x55$. The second byte represents the record length, while the fifth and sixth bytes indicate the record type. The seventh to tenth bytes are the serial number, referred to as the ticket_number. The last two bytes are check digits, and the remaining bytes make up the XOR-encrypted data, known as the payload. Upon analysis, it was discovered that the payload is encrypted using the XOR encryption algorithm. XOR encryption is a cryptographic technique that uses XOR calculations in computing. The XOR calculation principle states that identical values yield 0, and differing values yield 1. In other words, false is returned when the two values are the same; otherwise, true is returned. The XOR operator is used to determine whether two values are different, and it is commonly used for information encryption [26]. In this case, we need to decrypt the XOR encryption algorithm used in the payload to reveal the plaintext information.

Through reverse analysis, it was discovered that each hexadecimal value of the payload in every record of the DAT file is XOR-encrypted with the value of “ticket_number%256” (hereinafter referred to as the key). We select one of the records for analysis; the specific structure of the record is shown in Figure 4.

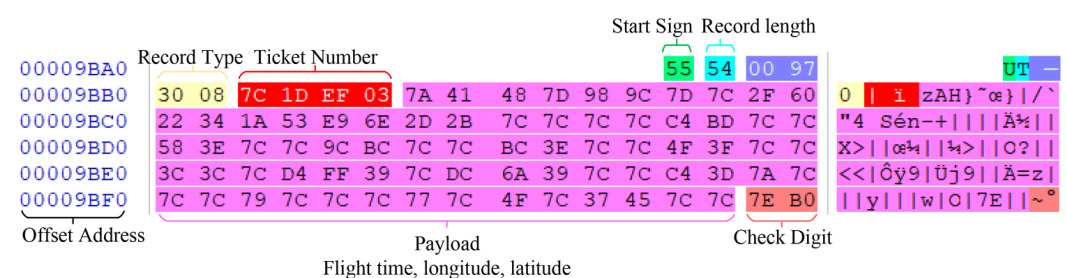


Figure 4. The structure of a specific record in DAT file.

The length of this record is $0x54$, and the record type is $0x0830$, which stores information such as flight time, longitude, latitude, height, and velocity components (x, y, z). The ticket_number is $0x03EF1D7C$, and the payload encryption information ranges from $0x9BB4$ to $0x9BFD$, with the check digit being $0xB07E$. Upon calculation, this record's ticket_number value is $0x7C$. The result was obtained after XOR decryption:

payload Cipher text: 7A 41 48 7D 98 9C 7D 7C 2F 60 22 34 1A 53 E9 6E 2D 2B 7C 7C 7C 7C C4 BD 7C 7C 58 3E 7C 7C 9C BC

each payload Cipher text $\oplus$ ticket_number%256 ($0x7C$)

payload in plaintext: 06 3D 34 01 E4 E0 01 00 53 1C 5E 48 66 2F 95 12 51 57 00 00 00 b8 c1 00 00 24 42 00 00 e0 c0

The payload plaintext is XOR decrypted first, then the initial 32 bytes are grouped in sets of 4 bytes and read in little-endian order. The results obtained are shown in Table 2.

Table 2. DAT file payload description result.

Raw Value	Data Type	Little-Endian Value	Calculation Method	Result	Description
06 3d 34 01	int	0x01343d06	Little-endian value	10 July 2020	YYYY-MM-DD
e4 e0 01 00	int	0x0001e0e4	Little-endian value	12:31:08	HH:MM:SS
53 1c 5e 48	int	0x485e1c53	Little-endian value/ 10^7	121.4127099708	Longitude
66 2f 95 12	int	0x12952f66	Little-endian value/ 10^7	31.17670558106	Latitude
51 57 00 00	int	0x00005751	Little-endian value/ 10^3	22.353	Height
00 00 b8 c1	float	0xc1b80000	Little-endian value/ 10^2	−0.23	X-velocity
00 00 24 42	float	0x42240000	Little-endian value/ 10^2	0.365	Y-velocity
00 00 e0 c0	float	0xc0e00000	Little-endian value/ 10^2	−0.07	Z-velocity

The check value of each record is located in the last two bytes and is generated using the “crc16-ccitt” check method. A Cyclic Redundancy Check (CRC) is a form of channel coding that generates a compact verification code based on data such as network packets or computer files. It is primarily employed to identify errors that could occur after data transmission or storage. The “crc16-ccitt” is used to verify the DAT file and determine whether its data has been altered.

2. YY_MM_DD_[HH-MM-SS]_FLY###.DAT

The file “YY_MM_DD_[HH-MM-SS]_FLY###.DAT” has identical information and structure to the “DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT” file after decompression and removal of the 283-byte zlib header. The plaintext result can be obtained using the decryption method mentioned above, and further details will not be provided.

4.2. Case 2: The TXT File Extracted from Mobile Device

The file “DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt” is generated by the software DJI GO 4 [24]. Its structure includes header information, record, and drone attribute details. The 100-byte header information includes the start and end positions of the record, detailed information, and the file version number. Apart from the 100-byte header information and the trailing N-byte (variable length) detailed information, the central part is referred to as a record, structured similarly to a DAT file. This contains flight record time, latitude and longitude, flight altitude, and various serial numbers of the drone. The detailed information includes attributes of the drone flight, such as the model, serial number, location city, and the number of pictures and videos taken during the flight. Some attribute information is presented in plaintext. It is possible to obtain a lot of information directly from the last N bytes of the TXT file, such as the aircraft serial number, battery serial number, and camera serial number.

The flight data saved as TXT files using DJI GO 4 is organized by record type. Record type 0x01 includes information such as longitude, latitude, and flight altitude, while record type 0x05 contains data on current flight time, speed, and distance. Similar to the DAT files, the data are encrypted and encoded. Although the verification method employed may vary, the underlying principles remain consistent. Figure 5 illustrates the file structure of the TXT file.

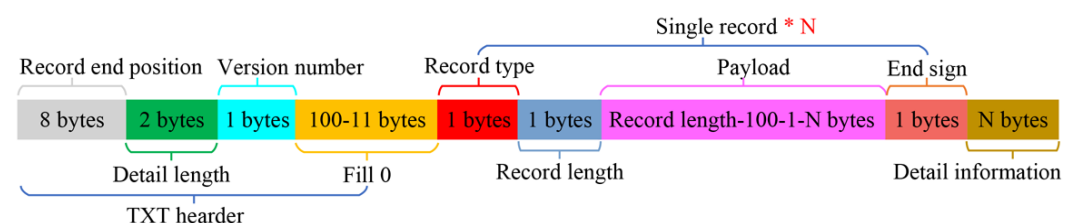


Figure 5. “DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt” file structure. (The “DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt” file consists of 100 byte header, N records, and N bytes of detailed information.

Each record begins with either 0x01 or 0x05, denoting the record type (hereafter referred to as recordType). The second byte in the record signifies the record’s length, while the final byte is always 0xFF, indicating the end of the record. The remaining bytes contain XOR-encrypted data (referred to as the payload). After conducting a retrospective analysis, it was discovered that the data in the TXT file is encrypted using the recordType and the first byte of the payload (referred to as keyByte) to

generate the crc64 check value (named scrambleBytes). Following this, an XOR encryption operation is carried out on each hexadecimal value in the payload and scrambleBytes. We select one of the records for analysis; the specific structure of the record is shown in Figure 6.

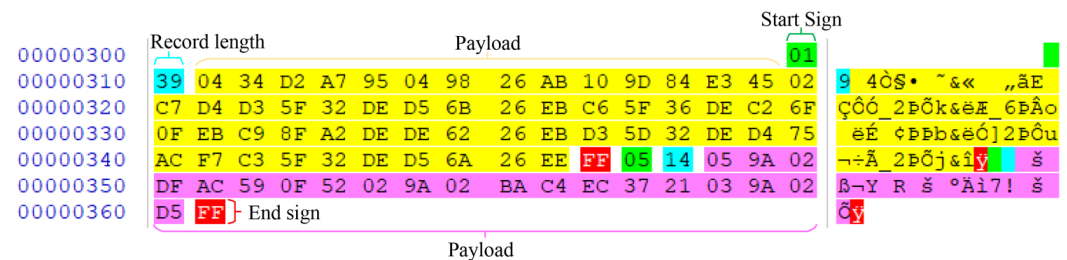


Figure 6. The structure of a specific record in TXT file.

The first record type is 0x01, which stores information such as longitude, latitude, and flight altitude. The length of the record is 0x39, with the keyByte being 0x04. The payload encryption information for this record spans from 0x034E to 0x0361. Upon calculation, the scrambleBytes for this record are 0x9A02DFAC590F5202. The final result is obtained after XOR decryption:

payload Cipher text: 34 D2 A7 95 04 98 26 AB 10 9D 84 E3 45 02 C7 D4 D3 5F

scrambleBytes: 0x9A02DFAC590F5202

each payload Cipher text $\oplus$ 0x9A02DFAC590F5202

payload in plaintext: E7 8D 95 4B D1 F3 00 40 C3 C2 B6 3D 90 69 E1 3F 00 00

The second record type is 0x05, which stores information such as flight time, flight speed, and flight distance. The length of the record is 0x14, with the keyByte being 0x05, and the payload encryption information spans from 0x0312 to 0x0349. Upon calculation, the scrambleBytes of this record are 0xD35F32DED56B26EB. The result is obtained after XOR decryption:

payload Cipher text: 9A 02 DF AC 59 0F 52 02 9A 02 BA C4 EC 37 21 03 9A 02

scrambleBytes: 0xD35F32DED56B26EB

each payload Cipher text $\oplus$ 0xD35F32DED56B26EB

payload in plaintext: 00 00 00 00 00 00 00 00 00 00 00 65 68 B5 38 73 01 00 00

After XOR decryption, the plaintext payload can be formatted into groups of either 8 + 8 + 2 bytes or 4 + 4 + 2 + 8 bytes. Interpreting each data type individually, the plaintext payload information can be extracted. The results are presented in Table 3.

Table 3. TXT file payload description result.

Raw Value	Data Type	Interpretation Value	Calculation Method	Result	Description
e7 8d 95 4b d1 f3 00 40	Double	2.1190515427604057	Interpretation value $\times 180/\pi$	121.412709970857	Longitude
c3 c2 b6 3d 90 69 e1 3f	Double	0.5441361623143951	Interpretation value $\times 180/\pi$	31.1767055810603	Latitude
00 00	Unsigned short	0	Interpretation value /1000	0	Height
00 00 00 00	Float	0	Interpretation value	0	Speed
00 00 00 00	Float	0	Interpretation value	0	Distance
65 68 b5 38 73 01 00 00	Unsigned long long	1594384279653	Unix time	2020-07-10 20:31:19:653	Time

The detailed information provided includes attributes of the drone, such as its name “mavic pro se” and serial number “08RDE4E00102YL”. Additionally, it encompasses information regarding the maximum flight altitude, maximum flight speed, number of photos, and other details found in the TXT file.

4.3. Case 3: The Default File Extracted from Mobile Device

The “mmkv.default” file was examined, and it was found to use base64 encoding. Base64 encoding involves converting the ASCII code value of the original text into an 8-bit binary number. The number is grouped and converted into decimal numbers, which are matched with corresponding characters from the base64 encoding table to complete the encoding process. It is important to note that, when data length is not a multiple of 3, padding is introduced to the final encoded data using the “=” character as the padding character. A portion of the “mmkv.default” file is shown in Figure 7:

mmkv.default																
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000006A0	5A	75	61	33	49	3D	08	6D	61	70	5F	74	79	70	65	01
000006B0	01	14	6B	65	79	5F	61	63	63	6F	75	6E	74	5F	6E	69
000006C0	63	6B	6E	61	6D	65	0D	0C	5A	47	70	70	64	47	56	7A
000006D0	64	41	3D	3D	16	44	4A	49	43	6F	6D	70	6F	6E	65	6E
000006E0	74	4D	61	6E	61	67	65	72	5F	72	63	01	0A	14	6B	65
	ANSI ASCII															
	Zua3I= map_type															
	key_account_ni															
	ckname_ZGppdGVz															
	dA== DJICcponen															
	tManager_rc ke															

Figure 7. Part of the “mmkv.default” file.

By parsing the “mmkv.default” file in the key-value storage format, during the decoding process, the value part was base64 decoded. Following the attribute record storage structure, the drone account nickname was located in the file, as highlighted in the yellow section of Figure 4. Specifically, the value “key_account_nickname” is represented by 0x06B2 0x06C5, while 0x06B1 indicates the length of the value 0x14. Furthermore, the hexadecimal value 0x06C7 indicates the length of the value 0x0C. The encoded value from 0x06C8 to 0x06D3 is encoded in base64 as “ZGppdGVzdA==”, which decodes to “djitest”. By decoding the contents of the “mmkv.default” file systematically and interpreting them in key-value format, user information such as user ID, nickname, phone number, and region can be extracted.

The extraction analysis of DJI Mavic 2 Pro retrieved useful forensic data, including GPS data, user details, dates, and other information, which were obtained from various sources and encrypted using different methods. Forensically relevant drone information is summarized in Table 4. To facilitate a clear and concise illustration of the recommended data acquisition process for investigators, we advocate utilizing the flow diagram presented in Figure 8.

Table 4. Artifact list containing drone pairing information.

Forensic Object	Target Data	Protection
Internal chip	DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT	Encryption XOR
Internal TF card	No longer used as a storage device	-
External TF card	/DCIM/100MEDIA/DJI_####.JPG /DCIM/100MEDIA/DJI_####.MOV	-
Flight log file	/0/DJI/dji.go.v4/FlightRecord/DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt	Encryption XOR
Flight data	/DJI/dji.go.v4/MCDatFlightRecords/YY_MM_DD_[HH-MM-SS]_FLY###.DAT	Encryption XOR
User information file	/data/dji.go.v4/files/mmkv/mmkv.default	Encryption Base64
Media file	/DJI/dji.go.v4/DJI Album/org_####_Unixtime000.jpg /DJI/dji.go.v4/CACHE_org_####_Unixtime000.jpg	-
Media file caching	/DJI/dji.go.v4/CACHE_screen_####_Unixtime000.jpg /DJI/dji.go.v4/CACHE_thumb_####_Unixtime000.jpg	-

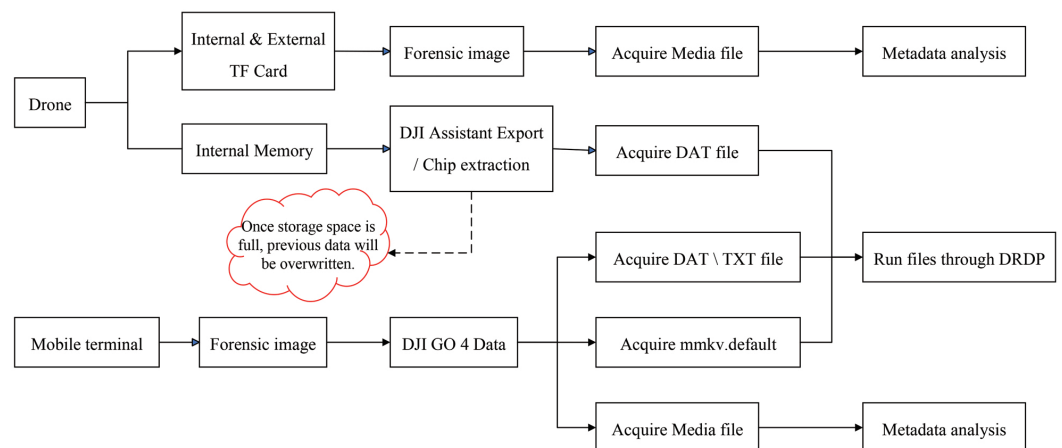


Figure 8. DJI Mavic 2 Pro data analysis process.

5. Result Testing and Discussion

This section outlines the tests performed to verify the feasibility of the forensic program DRDP. Nine sets of “DJI_ASSISTANT_EXPORT_FILE_YYYY_MM_DD_HH-MM-SS.DAT” files were exported and then chosen for testing. Correspondingly, nine “YY_MM_DD_[HH-MM-SS]_FLY###.DAT” and nine “DJIFlightRecord_YYYY_MM_DD_[HH-MM-SS].txt” files were extracted from the mobile terminal for joint testing. The DRDP successfully parsed nine data sets. Table 5 presents part of the

parsing results from the CSV file. The velocity components (x, y, z) were not found in the TXT file and Table 6 displays the DAT-parsed results from the CSV file.

Table 5. Analysis results of various drone-related files in Part 1.

Drone DAT					Android DAT				Android TXT			
Time	Longitude	Latitude	Height	Distance	Longitude	Latitude	Height	Distance	Longitude	Latitude	Height	Distance
20:31:40	121.4140	31.17631	83.865	137.1404	121.4137	31.17645	83.865	137.1611	121.4140	31.17633	74.1	129.8784
20:31:41	121.4142	31.17626	88.930	149.7040	121.4138	31.17640	88.930	149.8093	121.4141	31.17628	79.5	143.8932
20:31:42	121.4143	31.17622	93.835	161.7168	121.4139	31.17636	93.835	161.7943	121.4142	31.17624	84.1	154.9510
20:31:43	121.4144	31.17617	98.871	172.8596	121.4140	31.17631	98.871	172.9213	121.4143	31.17619	89.0	166.5772
20:31:44	121.4145	31.17612	104.776	185.9019	121.4142	31.17626	104.776	185.9697	121.4144	31.17614	94.4	178.5248
20:31:45	121.4146	31.17608	108.724	194.3239	121.4143	31.17622	108.724	194.4079	121.4145	31.17610	99.4	189.3292
20:31:46	121.4147	31.17604	113.670	204.3065	121.4144	31.17617	113.670	204.5189	121.4146	31.17606	103.8	198.6641
20:31:47	121.4148	31.17601	118.637	214.2771	121.4145	31.17612	118.637	214.4884	121.4147	31.17601	109.2	209.6367

Table 6. Analysis results of various drone-related files in Part 2.

Drone DAT				Android DAT		
Time	X-Velocity	Y-Velocity	Z-Velocity	X-Velocity	Y-Velocity	Z-Velocity
20:31:40	−5.31	11.65	−5.01	−5.31	11.65	−5.01
20:31:41	−5.31	11.34	−5.12	−5.31	11.34	−5.12
20:31:42	−5.32	10.68	−4.98	−5.32	10.68	−4.98
20:31:43	−5	9.72	−5.04	−5	9.72	−5.04
20:31:44	−4.87	9.66	−4.99	−4.87	9.66	−4.99
20:31:45	−4.71	9.4	−4.96	−4.71	9.4	−4.96
20:31:46	−4.45	9.01	−5.02	−4.45	9.01	−5.02
20:31:47	−4.47	8.9	−4.98	−4.47	8.9	−4.98

The flight record is obtained by processing the last N bytes of information from the TXT file through the `rstrip()` function and transcoding it into a string. This record contains important information such as the flight start time, starting GPS location, total distance and duration of the flight, maximum altitude reached, and number of photos taken.

The DRDP tool executes the command “python main.py -u” to parse user information. It accurately extracts the user ID, nickname, phone number, and region of drone users, as shown in Table 7.

Table 7. “mmkv.default” file parsing result.

Name	Description	Parsing Result
key_account_nickname	Nickname	djitest
key_account_id	User ID	djiuser-oruxe8p9vnkr
key_account_phone	Phone number	18817707586
key_account_uid	User uid	1272083171242541056
key_account_phone_area	Register area	86(China)

User information is analyzed to enhance the completeness of the evidence chain and provide additional insights into suspects. This information can be corroborated and reinforced by other evidence. Additionally, the author made a significant discovery. Upon analyzing the drone DAT data, it was observed that the earliest flight record file was incomplete, retaining only a limited amount of information. After conducting multiple export and analysis tests, it has been determined that the drone continuously writes new flight data when powered on. Once the storage space is full, previous data are overwritten and cannot be recovered. Therefore, in practical forensic activities, forensic personnel should promptly export the data and power down the drone equipment to prevent the overwriting of flight data and potential data loss.

The research is restricted to the DJI Mavic 2 Pro, and therefore does not provide a comprehensive understanding of all consumer drone forensics. Although some scholars are conducting relevant research on drone user information, the specific decryption algorithms and file structures have not been announced; we make up for this and serve as a solid foundation for subsequent drone forensics. Due to the significant time and energy costs associated with forensic analysis research, it is impractical to cover all or even most consumer drones. Our ongoing efforts involve continuous research in the field of drone forensics and collaboration with governments to encourage drone manufacturers to establish agreed-upon data standards for flight recordings. The forensic tool DRDP faces a major limitation due to the specialized data formats of DAT and TXT files. This work acknowledges the

inability to capture the full spectrum of potential data for exhaustive parsing from relevant files and recognizes the limitation of achieving exhaustive parsing for all data.

By comparing the drone's flight data with those of the mobile device, we can verify that the flight data originate from the Android phone controlling the DJI drone. However, the altitude value in the TXT file significantly differs from the value in the DAT file, and the specific reason for this discrepancy remains unclear. This discrepancy will serve as the starting point for our next phase of research. Our future work will focus on further exploring the structures of the DAT and TXT files, as well as related files on the device, such as "mmkv.default", which may contain important information. Additionally, we have attempted to reverse engineer the drone's firmware, but more work is needed to illuminate data that cannot be parsed in the current analysis. In the future, further research should be conducted in other areas related to drones where reliable data can be obtained.

6. Conclusions and Future Work

In this paper, a drone data parser (DRDP) was designed to analyze the file structure and encryption method of the DJI Mavic 2 Pro. The proposed method can parse GPS information, flight time, altitude, distance, and velocity components (x, y, z) effectively, enabling the accurate analysis of the drone's flight status and providing robust support for the truth of cases. The proposed DRDP is verified on real-world drone data files to confirm its effectiveness, including DAT files, TXT files, and default files. The experiments show that the proposed DRDP can successfully parse the internal and external data of drones.

In future work, we plan to further explore more features of drones' data from DAT and TXT files. This expanded analysis will encompass the Euler angle data (pitch, yaw, and rotation) associated with the drone to provide a detailed depiction of the drone's state. Moreover, we aim to delve into the reverse engineering of drone firmware to ascertain the potential for inferring plain data when encryption methods differ. Furthermore, we intend to extend the current research scope by exploring a wider range of drone models and manufacturers.

Author Contributions: Conceptualization, Z.Z. and Y.W.; funding acquisition, Y.W. and G.L.; project administration, G.L.; methodology, Z.Z. and Y.W.; software, Z.Z.; validation, Z.Z. and G.L.; formal analysis, Z.Z.; investigation, Z.Z. and G.L.; resources, Z.Z.; writing—original draft preparation, Z.Z.; writing—review and editing, Z.Z., Y.W. and G.L.; supervision, Y.W. and G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Key Research and Development Program of China (2023YFC3306100, 2023YFC3306103, 2023YFC3306105), Major Projects of National Social Science Foundation (20&ZD199), and the Humanities and Social Sciences Research Project of the Ministry of Education (23YJA820015).

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author/s.

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

References

1. Lee, S.; Seo, H.; Kim, D. Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller. *Sensors* **2023**, *23*, 29–34. [CrossRef] [PubMed]
2. Ikuesan, R.A.; Ganiyu, S.O.; Majigi, M.U.; Opaluwa, Y.D.; Venter, H.S. Practical Approach to Urban Crime Prevention in Developing Nations. In Proceedings of the 3rd International Conference on Networking, Information Systems & Security, Marrakech, Morocco, 31 March–2 April 2020; pp. 1–8.
3. Philomin, S.; Singh, A.; Ikuesan, A.; Venter, H. Digital forensic readiness framework for smart homes. In Proceedings of the International Conference on Cyber Warfare and Security, Norfolk, VR, USA, 12–13 March 2020; pp. 627–653.
4. Italian Prisoner Shoots at Rivals with Gun 'Smuggled in by Drone'. Available online: <https://www.theguardian.com/world/2021/sep/20/italian-prisoner-shoots-at-rivals-with-gun-smuggled-in-by-drone> (accessed on 21 September 2023).
5. Tourists Crash Drones into Italy Landmarks in Rome and Pisa. Available online: <https://edition.cnn.com/travel/article/tourist-drone-incidents-rome-pisa/index.html> (accessed on 27 July 2023).
6. Drohne über Teslas Gigafactory Behindert Flugverkehr. Available online: <https://www.golem.de/news/flughafen-ber-drohne-ueber-teslas-gigafactory-behindert-flugverkehr-2205-165376.html> (accessed on 15 November 2023).
7. Chen, Z.; Mu, Q.; Luo, W.; Yang, X.; Li, D.; Shao, X.; Liu, Y.; Zhu, H. Digital Forensics for Automotive Intelligent Networked Terminal Devices. *IEEE Trans. Veh. Technol.* **2023**, *73*, 5128–5138. [CrossRef]
8. Kent, K.; Chevalier, S.; Grance, T. Guide to integrating forensic techniques into incident. *Tech. Rep.* **2006**, 80–86.

9. Best Practices for Drone Forensics. Available online: https://drive.google.com/file/d/1CbQzf9eq2fpEVj9Bj43ID_yBcFxSgHyc/view?pli=1 (accessed on 13 January 2024).
10. Technical Specification for Examination of Digital Data in Civil Drone. Available online: <https://www.moj.gov.cn/pub/sfbgwapp/zwgk/zwgksfbhy-bz/202310/W020231020678452706562.pdf> (accessed on 7 October 2023).
11. Studiawan, H.; Grispos, G.; Choo, K.K.R. Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed. *Comput. Secur.* **2023**, *10*, 33–40. [[CrossRef](#)]
12. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D. A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field. *Comput. Intell. Neurosci.* **2022**, *2022*, 8002963. [[CrossRef](#)] [[PubMed](#)]
13. Alotaibi, F.M.; Al-Dhaqm, A.; Al-Otaibi, Y.D.; Alsewari, A.A. A comprehensive collection and analysis model for the drone forensics field. *Sensors* **2022**, *22*, 64–86. [[CrossRef](#)] [[PubMed](#)]
14. Tian, Q.; Li, B. Research on Digital Forensics Methods for Small Drones. *Inf. Netw. Secur.* **2017**, *66*, 75–82.
15. Yan, Z.; Fan, M.; Wang, G. A Forensic Scheme Research for Multirotor Drones. *Inf. Netw. Secur.* **2017**, *66*, 75–82.
16. 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, United Arab Emirates, 3–7 November 2019; pp. 1–3.
17. 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.
18. 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. 66–71.
19. Kumar, R.; Agrawal, A.K. Drone GPS data analysis for flight path reconstruction: A study on DJI, Parrot & Yuneec make drones. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 30–41.
20. Iqbal, F.; Alam, S.; Kazim, A.; MacDermott, Á. 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, United Arab Emirates, 3–7 November 2019; pp. 1–6.
21. Horsman, G. Unmanned aerial vehicles: A preliminary analysis of forensic challenges. *Digit. Investig.* **2016**, *16*, 1–11. [[CrossRef](#)]
22. Fernández-Fuentes, X.; Pena, T.F.; Cabaleiro, J.C. Digital forensic analysis of the private mode of browsers on Android. *Comput. Secur.* **2023**, *134*, 10–25. [[CrossRef](#)]
23. DJI Assistant 2 For Mavic. Available online: <https://www.dji.com/cn/downloads/softwares/assistant-dji-2-for-mavic> (accessed on 5 August 2023).
24. DJI GO 4. Available online: <https://www.dji.com/cn/downloads/djiapp/dji-go-4> (accessed on 15 July 2023).
25. Fu, Z.; Zhi, Y.; Ji, S.; Sun, X. Remote attacks on drones vision sensors: An empirical study. *IEEE Trans. Depend. Secur. Comput.* **2021**, *19*, 3125–3135. [[CrossRef](#)]
26. Choi, H.; Lee, S.; Jeong, D. Forensic recovery of SQL server database: Practical approach. *IEEE Access* **2021**, *9*, 14564–14575. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.