FORENSIC APPROACH TO DATA EXTRACTION FROM UAV

Tamás Nagy [1*], Imre Zsolt Kovács [1], Veronika Kozma-Bognár [2], József Berke [2]

[1] Rapid Response Police National Bureau of Investigation, Cybercrime Division, Forensic Department, Hungary
[2] Drone Technology and Image Processing Scientific Lab, Dennis Gabor University, Hungary
[*] Correspondence: nagy.tamas.pont@gmail.com

DOI: 10.66538/DH.2025.1.1.38

Abstract

The use of unmanned aerial vehicles (UAVs) has become widespread across various fields, proving to be an extremely useful tool in military operations, law enforcement, disaster management, agriculture, commerce, logistics, and many other areas. At the same time, drones can also serve as instruments for committing various offenses or crimes, either directly or indirectly. The most common illegal uses include invasion of privacy, operations in restricted airspace, and endangering air traffic. Organized crime also frequently utilizes drones for smuggling contraband across borders and delivering illicit items into prisons, such as drugs, mobile phones, or even weapons. In digital forensic data acquisition and processing, it is a fundamental professional requirement that the data stored on UAVs and their associated devices remain intact and that their use as evidence is ensured beyond any doubt. Data from the device must be extracted to an independent storage medium using certified and standardized procedures. This study focuses on key aspects of drone data extraction. It includes the identification of information relevant to investigations, along with the detailed documentation of these processes. Furthermore, the study presents and compares various software tools used in this context, highlighting their functionalities, advantages, and limitations.

Keywords: digital forensics, data extraction, drone, unmanned aerial vehicle, UAV

1. Introduction

The growing prevalence of drone usage is increasingly evident across a wide range of sectors, including agriculture, forestry, industry, transportation and logistics, security, cartography, law enforcement, disaster management, and defense. Unmanned Aerial Vehicles (UAVs) produce substantial volumes of electronic data during operation, the analysis of which is essential for monitoring operational conditions and for the investigation of unforeseen incidents. Furthermore, UAVs may function as instruments of, or be directly involved in, criminal activities. A core objective of forensic analysis is to determine what happened, when, where, and under what circumstances [1].

In the context of modern warfare, drones have also acquired significant strategic importance. The ability to extract and analyse data from adversarial UAVs may even prove decisive in the outcome of military operations.

In light of the above, the aim of this study is to provide a comprehensive examination of the possibilities for forensic data extraction, processing, and analysis from drones. The term "forensic" is understood here as pertaining to judicial investigations, specifically the collection, analysis, and interpretation of evidence for legal proceedings. In this context, it is applied within the domain of digital forensics, which encompasses the examination of information systems, devices, and digital data.

The research is guided by the central question: To what extent do the selected software solutions satisfy the methodological requirements of forensic drone data extraction?

2. Material and Methods

2.1. Theoretical and practical significance of the study, objectives

Drone forensics is a subset of mobile and wireless forensics, which falls under the broader category of digital forensics [2]. A fundamental professional requirement in forensic data extraction and processing is to ensure that the data on the drone and its

associated devices remain intact, making their use as evidence indisputable. Data from these devices must be recorded on an independent storage medium using certified and standardized procedures. It is generally recognized that adherence to the ACPO guidelines is essential in forensic investigations to preserve the integrity of the examined device and to ensure the reliability of the evidence obtained [3].

Due to the vast number of manufacturers and differing systems, this study primarily focuses on DJI-manufactured devices. The extraction of telemetry and metadata in their native format is a critical aspect of forensic processing. Data preparation includes recovering deleted files, making log files, encrypted, encoded, or compressed data readable, and applying techniques such as reverse engineering, steganography, interpolation, and even AI-based object detection and recognition. After this stage, the extracted data undergoes analysis, which, besides requiring IT expertise, also demands specialized knowledge of drone technology to ensure investigative relevance. The analysis aims, among other things, to unequivocally identify and link the examined device to its user.

2.2 Legal and methodological principles

In Hungary, forensic data extraction follows the methodological guidelines set by the Hungarian Institute for Forensic Science, particularly the General Procedures for the Examination of Digital Storage Devices [4] and the General Procedures for the Examination of Mobile Communication Devices [5].

The Digital Forensics Research Workshop (DFRWS) first established a procedural model for handling digital data in its 2001 conference. Over time, this model has been expanded and refined. To ensure scientific and professional alignment with international and applied forensic standards, Table 1 presents the methodological designations adopted by the DFRWS in 2001 as a foundational reference for the study's content.

Table 1. Operations performed in forensic activities

Identification	Identification of the digital data carrier
Preservation	Preservation and safeguarding of digital data
Collection	Collection of digital data carriers
Acquisition	Extraction of digital data
Examination	Examination of digital data
Analysis	Analysis of digital data
Presentation	Presentation of digital data
Decision	Decision-making based on digital data

Source: Methodological letter issued as an annex to the Director General's Circular 4/2019. (XII.17.) Hungarian Institute for Forensic Science

The methodological letter references numerous international standards on the subject, which serve as essential and indispensable scholarly sources for activities related to the forensic methodology of digital data acquisition, processing, and analysis [6].

Beyond these, the Scientific Working Group on Digital Evidence (SWGDE) and the European Network of Forensic Science Institutes (ENFSI) have published several recommendations on best practices concerning digital evidence [7].

Fundamental Principles of Storage Device Handling:

- The extent of access must be minimized.
- All modifications must be documented and justified.
- The rules for handling evidence and examination objects must be strictly followed.
- When moving examination devices, the continuity of the Chain of Custody must be maintained through proper documentation.

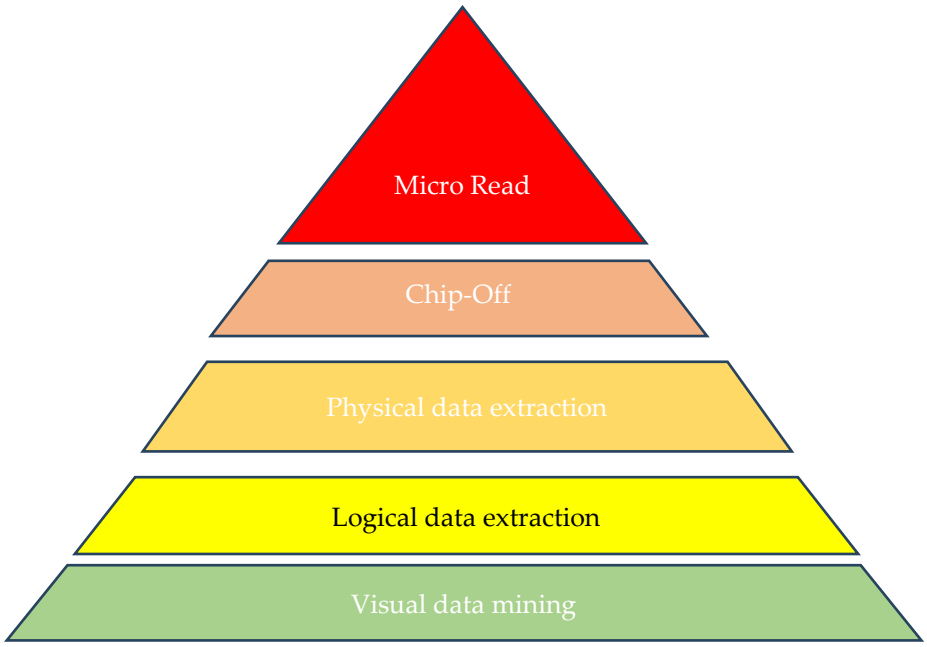
The methodological guidelines include specific principles for handling electronic data storage devices, such as handling powered-on and powered-off storage devices, performing logical, physical, and targeted data extraction from storage devices, documenting data extraction procedures, types of data that can be extracted from storage devices (hard drives, memory cards, USB drives, optical media, mobile devices), and methods for validating extracted data.

However, the methodological guidelines do not specifically address the collection of digital evidence from unmanned aerial vehicles. Therefore, the general principles applicable to conventional data carriers and storage devices should be considered as the guiding framework in this context.

2.3. Main types of data extraction

The fundamental principle of data extraction from storage devices is to minimize any modifications to the source data as much as possible by using hardware and/or software components that allow handling the data without altering it.
Figure 1 illustrates the types of data extraction, ranging from the simplest method at the base of the pyramid to the most complex procedure.

Figure 1. Types of data extraction



Source: Methodological letter issued as an annex to the Director General's Circular 5/2019. (XII.17.) Hungarian Institute for Forensic Science

Table 2. Types of data extraction, their main features and disadvantages

	Features	**Disadvantages**
Visual data mining based on external observation	Recording the data on the storage device and on the display with a camera or camcorder. Especially recommended when other forms of data extraction are not possible.	Recovering deleted data is not possible. May be time-consuming. May cause data to be modified. A damaged display prevents the process.
Logical data extraction	Reading data from the target device via wired or wireless means.	Recovery of deleted files is limited.
Physical data extraction	Extracting raw data that requires further processing (HexDump). Extracting data with full root access. Extracting data by breaking the target device (JTAG) through its test points.	Encryption on the storage device may prevent interpretation of the read data.
Chip-off	Data extraction based on storage circuit disassembly.	This involves dismantling the structure, and in many cases, restoration is not possible.
Micro Read	Direct Observation of the Logical Gates of Storage Devices The states of the logical gates in NAND or NOR circuits can be directly observed using specialized tools, allowing for the reconstruction of stored information.	The procedure is extremely costly and requires highly specialized equipment.

Source: Edited by the author

For extracting data from the drone and the RC controller, I used DJI Assistant 2 [8], FTK Imager [9], Cellebrite UFED Touch, Cellebrite UFED 4PC [10-12] , CFID SCG [13] and DJI Battery Killer [14-15].
For chip-level data extraction, the PC-3000 tool provides forensic experts with the necessary capabilities [16-17].

2.3.1. Observation-Based Data Extraction

According to forensic methodology, the initial phase of data extraction involves a thorough examination of the device, which includes visual inspection and detailed documentation thereof. The photographic documentation produced during this visual data extraction process serves to record the precise condition of the device, which is particularly important if testimony is later required regarding external or internal damage marks found on the equipment. Interpreting external or potentially hidden labels and markings on the drone can also contribute to the identification of the UAV, the determination of its manufacturer and model, or even the recognition of its firmware version.
In addition, the use of classical trace collection techniques, such as fingerprint detection, can be particularly valuable for identifying the owner of the drone or the individuals who last operated it. It is crucial to emphasize that, whenever trace collection is carried out—whether it involves fingerprint lifting or sampling of possible chemical or biological contaminants (e.g., gunpowder residue,

blood) present on the device surface—all other activities that could compromise the integrity, identification, or admissibility of such traces in subsequent investigative proceedings must be strictly avoided until trace processing is complete.
During surface observation, contaminants, scratches, or other physical traces may also be detected, potentially indicating the nature of the device's usage.
At this stage of the documentation process, precision and thoroughness are indispensable, as even the smallest detail may provide relevant information for further analysis.
During the examination, the drone serving as evidence is photographed from all angles. It should be noted that the photographs included in this thesis are presented for illustrative purposes only and are not intended to represent the full scope of the documentation.

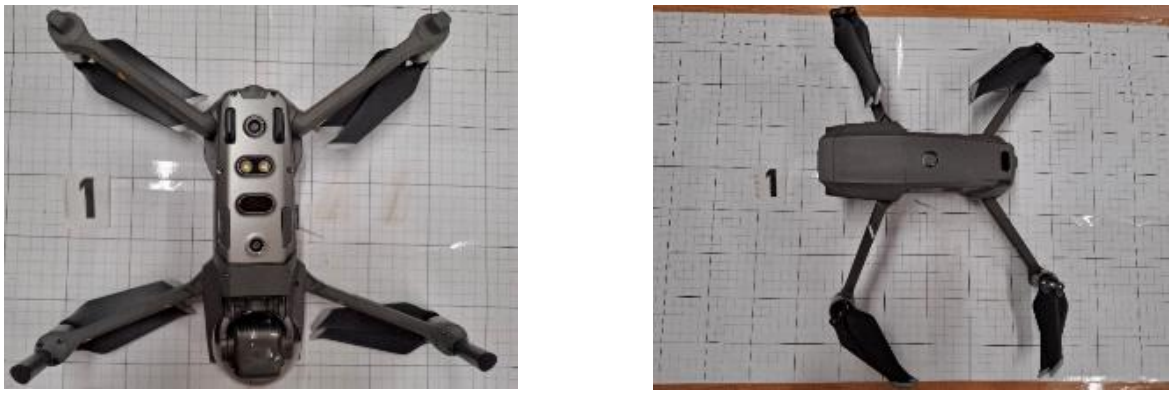
Initially, an overview photograph is taken of the examined items (drone and controller) together, followed by a frontal image of the first selected component— in this case, the drone—taken head-on, which clearly depicts the nature of the object and its main visual elements. Subsequently, profile and side-view images are captured from both the right and left sides of the device, and the rear view is also documented.
For photographic background, 10x10 millimetre grid paper was used, allowing for easy estimation of approximate dimensions and proportions. On the frontal and profile photographs, the inscriptions on the original factory labels are visible, potentially indicating the device type (Figure 2).

Figure 2. Frontal and side-view photographs of the drone

Source: Author's own photographs

For the top-down and bottom-up images, the drone was photographed from a vertical angle. These photographs clearly show the power button and various sensors (Figure 3).

Figure 3. Top and bottom-view photographs of the drone



Source: Author's own photographs

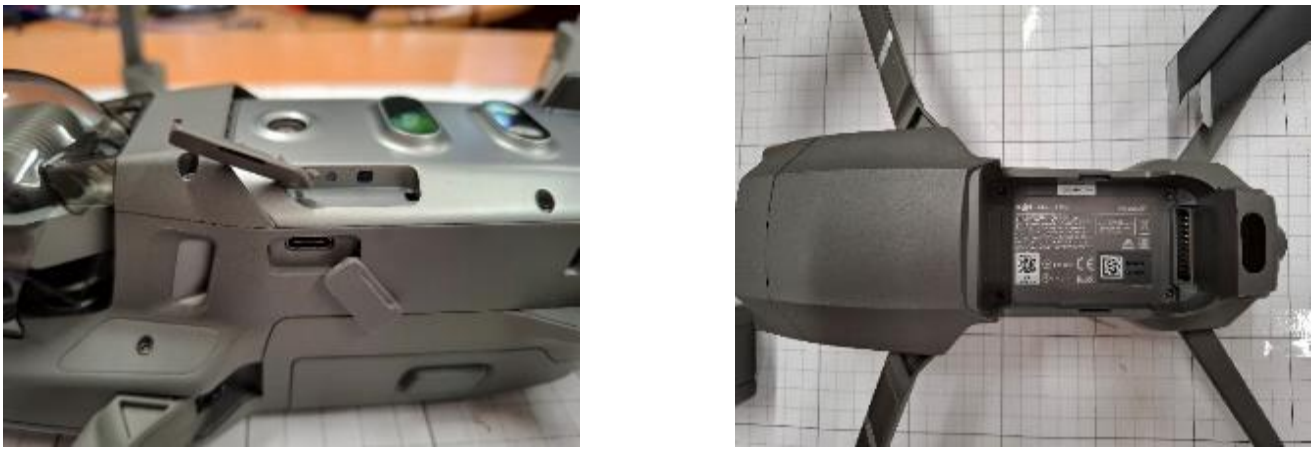
Subsequently, photographs were taken from an isometric perspective, in which the object is captured at approximately a 45-degree angle, allowing both the top and side of the drone to be visible simultaneously (Figure 4). This photographic technique enhances spatial perception. In cases where a specific damage mark needs to be documented more clearly, an oblique-angle view may also be employed to improve visibility.

Figure 4. Isometric view photographs of the drone

Source: Author's own photographs

After photographing the object from all angles, it becomes necessary to highlight individual components, to remove detachable elements for separate photographic documentation. This method allows access to manufacturer labels, inscriptions, as well as to the data communication ports and removable storage media (e.g., microSD cards). By removing the battery, the data on its factory label, including identifying serial numbers, can also be recorded (Figure 5).

Figure 5. Photographs Showing the Locations of Communication Ports and Labels



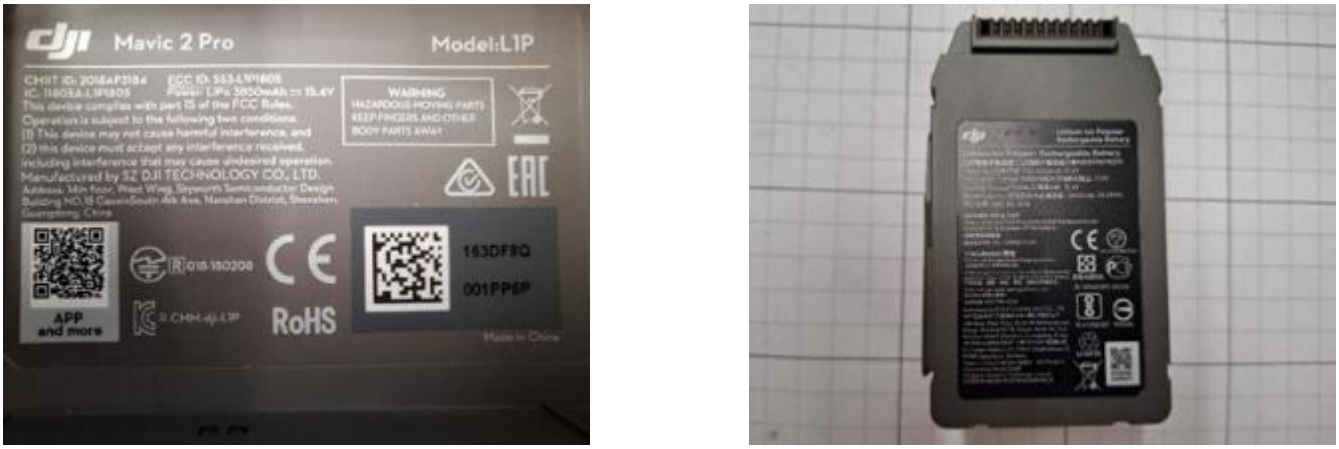
Source: Author's own photographs

The drone's label contains various data points that are essential for accurate identification. Typically, the label includes the manufacturer's name, the model designation, and the type number, which allow for a straightforward determination of the device's technical specifications. Additionally, the serial number enables unique identification of the unit.

The manufacturing date can provide insight into the operational lifespan of the drone, while the firmware version indicates the specific software build running on the device-information that may be relevant for security or functionality assessments.

Labels often feature compliance markings such as CE or FCC, indicating conformity with applicable standards. Some labels may also display power specifications, including required voltage and current levels. Moreover, the maximum take-off weight and the country of origin may also be listed, offering further contextual details regarding the drone's provenance (Figure 6).

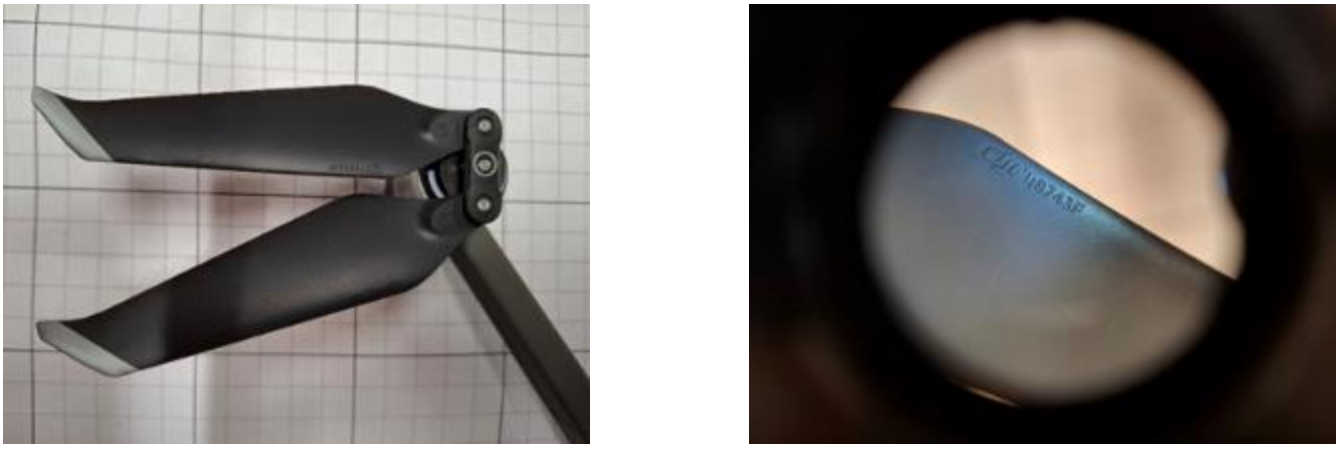
Figure 6. Label information of the drone and its battery



Source: Author's own photographs

During photo documentation, attention must also be paid to small details that may not be visible to the naked eye or with standard camera settings but can assist in identifying certain subcomponents. For example, inscriptions on the drone's propeller may help determine whether it is an original or aftermarket part. This information may indicate the cause of unstable flight behaviour, manoeuvring anomalies, or inconsistent flight performance. Macro photography can reveal micro-damages or hairline cracks that would otherwise remain invisible to the naked eye (Figure 7).

Figure 7. Macro shots



Source: Author's own photographs

Based on the label information and unique markings found on the drone, the following table can be compiled to assist in the identification of the device and its components, as well as the determination of certain parameters during the investigation.

The information presented on the drone's label provides detailed insight into the device's identifiable characteristics and certifications. The QR code identifier on the label, "163DF8Q 001PP6P," serves as a unique serial number.

The CMIIT ID and FCC ID are identifiers indicating regulatory approval of the drone's radio frequency (RF) components, certifying compliance with the standards of the respective countries.

The unique QR code enables precise identification of the battery and provides access to information such as manufacturing and tracking data.

Following the photographic documentation of the drone and its components (e.g., battery, Micro-SD card), similar photographic procedures must be applied to the controller and/or mobile device. After capturing frontal, profile, top, bottom, and oblique view images, attention must also be given to photographing the identification label and, if necessary, specific macro details (Figure 8).

Figure 8. RC controller

Source: Author's own photographs

A fundamental principle of the observational data collection and documentation described above is that all such data must be associated with a unique criminal case identifier. The piece of evidence and its corresponding unique evidence number are inseparably linked. During the documentation of each step of the forensic process, special attention must be paid to the consistent use of the criminal case identifier.

2.3.2. Logical and physical data extraction

DJI Assistant 2

DJI Assistant 2 is the simplest method for downloading flight logs and data from the internal storage of DJI drones. The drone can be connected to a computer via a USB cable. DJI Assistant 2 supports both Windows and macOS operating systems, ensuring broad compatibility. It is important to note that certain DJI drone models may require a specific version of the Assistant 2 software. Before initiating data extraction, the appropriate version must be selected, downloaded, and installed.

Among the available menu items in the application is "Log Export," which allows the export of log files containing telemetry data. Other menu functions should not be used, as they may modify the drone's stored data [18].

By clicking the "Save To Local" button, the selected log files can be saved locally. Due to the size of individual files, it is advisable to save them one by one to facilitate later processing.

The saving process may take anywhere from a few minutes to several dozen minutes, depending on the size and number of files. The end of the copying process is indicated by the progress bar reaching 100% and the message "Download Complete."

In the designated output directory, the saved files have a .DAT extension and are named according to the format DJI_ASSISTANT_EXPORT_FILE_DATE_TIME. The date and time in the filename reflect the moment of export and do not indicate the original creation time of the log files.

The downside of the software is that the extracted flight logs are encrypted.

Logical data copying using FTK Imager

After connecting the drone to the computer via a hardware write blocker, the Windows operating system immediately mounted it as a drive. The system assigned it a unique drive letter, and the contents of the storage became visible through the file explorer interface.

The directories labelled DCIM, LOST.DIR, and MISC, commonly found on drones and other digital devices, are standard folder names used to store various types of data and system-level operations.

If a microSD card was present in the drone, its data acquisition could also be performed using the FTK Imager software, with the application of a hardware write blocker [9].

It is important to note, however, that the commonly used E01 forensic image file can be created using other software and hardware solutions as well. These include, among others, the Paladin Forensic Suite, which is based on a Linux platform, or the dedicated hardware device Logicube Falcon-NEO 2.

One disadvantage of the software is that the extracted flight logs are encrypted, thereby limiting processing and analysis.

Cellebrite UFED Touch, Cellebrite UFED 4PC

For data acquisition, I used Cellebrite UFED 4PC version 7.7.0.180. At the time of the examination, the most up-to-date software solution developed by the company for this purpose was Cellebrite Inseyets. According to the program's login interface, data extraction from drones is natively supported.

Cellebrite Premium is a more advanced tool in Cellebrite's product line, offering extended data extraction capabilities, including the ability to acquire data from locked or damaged devices. However, during the current examination, I did not have access to the Premium version.

Figure 9 illustrates the data extraction process using the Cellebrite UFED Touch device.

Figure 9. Data acquisition using the Cellebrite UFED Touch

Source: Photo taken by the author

From the available backup types offered by the software, I first initiated the “Physical” data extraction, as this method provides the most comprehensive acquisition from the drone’s internal storage. Physical acquisition offers the possibility of recovering deleted or hidden files as well.
The file system extraction was performed subsequently. In both cases, the resulting initialization file was named EvidenceCollection.ufdx. The physical extraction data was saved in a subdirectory as a Dump_001.bin image file.
It should be noted that the data extraction primarily included media files and their associated metadata, but not the flight logs.

CFID

The Covert Forensic Imaging Device (CFID) is a specialized portable tool designed for the forensic acquisition and analysis of data from unmanned aerial vehicles (UAVs), particularly DJI drones. It includes a dedicated UAV Mode, which facilitates the secure extraction of flight logs and related data even from damaged or non-functional drones. This capability ensures the preservation and integrity of critical evidence in field and laboratory conditions alike.
Upon connecting a supported DJI drone or its internal microSD card, the CFID automatically recognizes the device and switches to UAV Mode. From this point, the tool performs a targeted extraction process, collecting flight-related data such as .DAT, .CSV, and .KML files. These files contain detailed information about flight activity, geolocation data, and telemetry values essential for forensic investigation. In cases where the drone is damaged and cannot be powered on, the internal microSD card can be removed and connected directly to the CFID, which will still perform a full extraction, making the device suitable for a wide range of forensic scenarios. Data extraction is illustrated in Figure 10.

Figure 10. Data extraction with CFID

Source: Photo taken by the author

One of the most significant advantages of the CFID over competing forensic imaging tools is its ability to provide immediately accessible flight log data. The extracted .CSV files are not encrypted, in contrast to outputs from some other forensic software, and can be opened directly in programs such as Microsoft Excel. This allows investigators to review and analyse the flight data without the need for proprietary decoding tools or additional decryption steps. The accessibility and transparency of this data significantly streamline the forensic workflow and enable faster, more efficient preliminary assessments in time-critical investigations.

Starting from the Phantom 3 series, CFID supports most DJI models, offering broad compatibility with commonly used consumer and professional drones. In addition, the device is accompanied by an Android application that allows the real-time visualization of extracted flight logs, even in offline environments. This makes it possible for forensic analysts to begin interpreting data immediately on-site, which can be essential during dynamic or multi-agency investigations.

Overall, the CFID's UAV Mode offers a user-friendly, and efficient solution for drone data acquisition. Its ability to extract unencrypted, analysis-ready flight logs sets it apart from other tools on the market, making it a highly valuable asset in the forensic examination of UAVs.

One of the major advantages of the software is that the extracted flight logs are unencrypted, allowing for direct processing and analysis without the need for proprietary tools or decryption, which significantly facilitates forensic evaluation.

Data extraction from RC controller

For research purposes, I performed data extraction from a DJI RC Plus controller, model number RM700B, which features a built-in display, standalone operating system, and internal storage. The controller is equipped with USB-C, USB-A, HDMI ports, as well as a removable micro-SD card.

The controller was connected to a portable computer running FTK Imager using a standard USB-C to USB-A cable. The operating system mounted the controller as a drive. A simple logical data extraction was then performed from the mounted storage device. The acquired data set was subsequently processed into an .AD1 image container using the FTK Imager software in order to ensure its integrity and authenticity. A forensic image of the 128 GB nominal capacity micro-SD card found in the RC controller was created using FTK Imager, resulting in an .E01 format image file.

Flight log files

Table 3 presents the file paths, operating systems, and file types associated with log files generated by various drone applications. These logs contain critical telemetry and flight-related data.

Table 3. File paths of LOG files for selected applications

Application name	Operating system	Path	LOG file type
DJI GO 3	Android	DJI/dji.pilot/FlightRecord	TXT
	iOS	DJI GO/FlightRecord	TXT
DJI GO 4	Android	DJI/dji.go.v4/FlightRecord DJI/dji.go.v4/FlightRecord/MCDatFlightRecords	TXT DAT
	iOS	iTunes -> Fájl megosztás -> FlightRecords -> MCDatFlightRecords	TXT DAT
DJI FLY	Android	Android/Data/DJI.Go.v5/Files/FlightRecords	TXT
	iOS	DJI FLY/FlightRecord	TXT
Litchi	Android	LitchiApp/flightlogs	CSV
Autel Explorer	Android	explorer/flightLog	-
	iOS	The log file is not available directly through iTunes.	-
DJI GS PRO	iOS	GS PRO -> Home -> FlightLog -> Export	TXT
DJI Ultimate Flight	Android	DJI_Ultimate_Flight\Tracks	CSV
Drone Harmony	Android	Drone Harmony -> Plans & Flights -> Flight Logs	-
Pix4D Capture	Android	DJI/com.pix4d.plugindji/FlightRecord	TXT
	iOS	iTunes –> file sharing -> Pix4DCapture -> SDK logs	TXT

Source: Table compiled based on information available at airdata.com

The following folders, containing relevant data, can be extracted from the folder structure of the controller (Table 4).

Table 4. Relevant data containing folders found on the RC Controller

File path	File types
DJI\com.dji.industry.pilot\FlightRecord\ DJIFlightRecord\	TXT extension files
DJI\com.dji.industry.pilot\FlightRecord\ MCDatFlightRecords\	DAT extension files
DJI\com.dji.industry.pilot\CACHE_IMAGE\	thumbnails
DJI\Mission\KML\	KMZ extension files
Android\data\com.dji.industry.pilot\files\DJI\ com.dji.industry.pilot\FlightRecord\Upload\	empty folder (in the case of the controller under test)
Controller\Movies\	MP4 extension video files
Controller\Pictures\	screenshot files with PNG extension

Source: table created by the author

2.4. Other data extraction methods

The data acquisition techniques previously presented—commonly used in standard forensic investigations—can be supplemented by additional data extraction methods. These alternative techniques often require specialized expertise and high-cost technological infrastructure.

DJI drones typically operate on a Linux-based operating system that is specifically optimized for flight control and data security functions. This system differs significantly from conventional smartphone operating systems, as its design does not prioritize application versatility or broad internet connectivity. Instead, its primary focus is maintaining drone security and ensuring operational stability during flight.

When selecting the appropriate data extraction technique, it is important to consider that the operating system of DJI drones is more closed than typical mobile operating systems. Furthermore, similar or even more advanced security mechanisms than those found in mobile platforms may prevent complete data acquisition or hinder access to and interpretation of the extracted data [19-20].

Beyond the methods already discussed, it is also possible to extract data from the batteries of certain DJI drone models. One software tool that can be used for this purpose is DJI Battery Killer. Originally developed to restore malfunctioning batteries, in exceptional cases it may be utilized to extract data from the battery under investigation. However, it has significant drawbacks: the battery casing must be physically opened, and a special connector is required to interface the battery with a computer system [14].

For processing data from the drone and the remote controller, as well as analyzing flight log files, I used Cellebrite Physical Analyzer [12], Autopsy [21], FlightReader [22], AirData [23-24], CsvView, DatCon [25], Oxygen Forensics [26], BriefCam [27], Microsoft Excel and custom-developed programs /Drone Incident Parser/ [28]. This study does not cover a detailed analysis of the practical methodology of data processing.

2.5. Forensic Data Extraction from Damaged or Manipulated Drones

A further aspect worth highlighting is the forensic handling of drones that are physically damaged or intentionally tampered with. In real investigative practice, it may be the case that devices are found to have been subjected to mechanical stress, fire, or even deliberate hardware or software manipulation. In such cases, specialized tools such as the PC-3000 can provide valuable support in recovering data from partially corrupted or inaccessible storage devices, thereby ensuring that potentially crucial evidence is not lost. Moreover, the possibility of tampered or deliberately falsified flight logs must also be considered. Here, the examiner's task is to validate data integrity through cross-comparison with other sources of evidence, such as external storage media,

controller logs, or cloud-based synchronizations. This step is critical to establish the authenticity and evidential value of the acquired data.

Concerns regarding malware or intentional infection of captured drones also merit attention. In forensic workflows, data acquisition is carried out in an offline environment, which significantly reduces the risk of system compromise. Any malicious code present on the storage medium would be detected by installed security solutions, and its potential impact would remain limited to the local forensic workstation. It is important to emphasize that the primary purpose of employing a hardware write blocker is to protect the integrity of the digital evidence itself, rather than to defend the forensic system against malicious code. Nevertheless, awareness of such threats reinforces the importance of maintaining strict isolation of forensic acquisition systems from operational networks.

3. Results

Modern drones, including DJI drones, encrypt data—such as flight logs, location data, and other sensor measurements. Security protocols are embedded in the system and often synchronize with DJI's own cloud (optional), where they are also protected against unauthorized access. For mobile phones and RC controllers, data encryption is often optional, and various manufacturers apply different levels of security solutions, so the security level can vary significantly.

The data links of drones, whether Wi-Fi, OcuSync, or Lightbridge, are protected with strong encryption, minimizing the possibility of external eavesdropping or data breaches.

DJI regularly provides firmware updates that patch operating system vulnerabilities, add new features, and fine-tune flight safety. For these reasons, most of the examined software solutions are either unable to extract flight log files, or if they do, the extracted files are encrypted and cannot be read without additional processing or decryption. Due to the strong, multi-layered manufacturer encryption of the log files, decrypting them is nearly impossible, and processing and analysis may not always be feasible.

My findings suggest that none of the examined software versions are capable of independently and comprehensively meeting the investigative needs of authorities. However, their complementary use—when tailored to specific tasks—can be particularly useful and sufficient for uncovering the circumstances of a criminal offense.

4. Conclusions

In this study, I primarily sought to answer the question of how well the software examined meets the requirements set by forensic methodology in relation to drone data extracting.

Based on the results detailed in the evaluation of the primary research, it can be concluded that the software tools analyzed only partially meet the expectations set by forensic methodology. Based on the results, it can be concluded that several areas may require development in order to enforce the legal and professional principles of forensic investigations, particularly regarding the interoperability of software. In my opinion, this highlights the need to supplement the current software toolkit and develop new solutions better suited to forensic requirements for the saving, processing, and analysis of drone data according to forensic methodology.

References

1. Répás J. (2023): Examination of the Application of Drone Forensics Methodology in Expert Examination of Highly Automated Civil and Military Vehicles. p. 19. In: I. Alverad-Bánki International Cybersecurity Conference. Dr. József Répás, Online Conference Proceedings, Alverad Technology Focus Ltd. and Óbuda University Bánki Faculty, 25 October 2023. https://oda.uni-obuda.hu/bitstream/handle/20.500.14044/25368/I.%20Alverad-B%C3%A1nki%20Nemzetk%C3%B6zi%20Kiberbiztons%C3%A1gi%20Konferencia%20Konferenciak%C3%B6tet.pdf#page=22 (Accessed: 25 October 2024.)
2. Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2018): Drone Forensics: Challenges and New Insights. 2018 9th „IFIP International Conference on New Technologies, Mobility and Security (NTMS)”, pp. 1. https://doi.org/10.1109/NTMS.2018.8328747 (Accessed: 10 September 2024.)

3. Thornton, G., Bagheri Zadeh, P. (2021): An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis. Forensic Science International: Digital Investigation, Volume 41. https://www.sciencedirect.com/science/article/pii/S2666281722000609 (Accessed: 28 Augustus 2025.)
4. Hungarian Institute for Forensic Science. (2019): General Procedures for the Examination of Digital Storage Devices (4/2019. (XII.17.) Circular. https://www.nszkk.gov.hu/content/modszertani-leirasok/4-2019-korlevel/melleklet-4-2019-korlevel_signed.pdf (Accessed: 11 August 2024.)
5. Hungarian Institute for Forensic Science. (2019): Methodological Description of General Procedures for the Examination of Mobile Communication Devices (5/2019. (XII.17.) NSZKK Director General Circular Annex. https://www.nszkk.gov.hu/content/modszertani-leirasok/5-2019-korlevel/melleklet-5-2019-korlevel_signed.pdf (Accessed: 11 August 2024.)
6. Hungarian Institute for Forensic Science. (2020): Methodological letter on the general principles of electronic data examination. MISZK_modszertani_level_6_2020.pdf (Accessed: 11 August 2024.)
7. Szabolcsi Zs. (2022): Cyber Forensic Work in the Field. National Research, Development and Innovation Office Publication. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Szabolcsi%20Zsolt_Terepen_vegzett_digitalis_forenzikus_munka_v2.pdf (Accessed: 18 October 2024.)
8. 3D Insider (n.d.): DJI Assistant 2. https://3dinsider.com/dji-assistant-2 (Accessed: 14 September 2024.)
9. Exterro (n.d.). FTK Imager: Digital forensics software. https://www.exterro.com/digital-forensics-software/ftk-imager (Accessed: 12 September 2024.)
10. Cellebrite (n.d.): Cellebrite introduces UFED Touch2 platform. https://cellebrite.com/en/cellebrite-introduces-ufed-touch2-platform/ (Accessed: 12 September 2024.)
11. Cellebrite (n.d.): Cellebrite Reader. https://cellebrite.com/en/reader (Accessed: 15. October 2024.)
12. Cellebrite (n.d.): Physical Analyzer. https://cellebrite.com/en/physical-analyzer (Accessed: 15 October 2024.)
13. CFID (n.d): CFID User guide SSG Rev 1.8. https://cyber-ssct.com/drone/CFID_User_Guide_1.8.pdf (Accessed: 22 April 2025.)
14. DJI (2024): DJI Forum: Intelligent Battery Repair. https://forum.dji.com/thread-302619-1-1.html (Accessed: 12 October 2024.)
15. DJI (n.d.): DJI Assistant 2: Troubleshooting. https://support.dji.com/help/content?customId=en-us03400007747&spaceId=34&pbc=mF6h4ZTt (Accessed: 11 October 2024.)
16. Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S., Ghabban, F. M. (2021): Research Challenges and Opportunities in Drone Forensics Models. Electronics, pp. 1-29. https://doi.org/10.3390/electronics10131519 (Accessed: 6 April 2024)
17. Acelab (n.d.): PC-3000: A powerful tool for data recovery. https://blog.acelab.eu.com (Accessed: 14 September 2024.)
18. 3D Insider (n.d.): DJI Assistant 2. https://3dinsider.com/dji-assistant-2 (Accessed: 14 September 2024.)
19. Flack, D. (2024): Rise of the Drones. Modern Drone Forensic Opportunities. SANS Institute. https://www.sans.org/presentations/rise-of-the-drones-modern-drone-forensic-opportunities (Accessed 19 October 2024.)
20. Tamma, R. – Skulkin, O. – Mahalik, H. – Bommisetty S. (2018): Practical mobile forensics - third edition, Packt Publishing, 402 p.ISBN: 9781788839198
21. Basis Technology (2016): Autopsy 4.0 User Documentation. https://sleuthkit.org/autopsy/docs/user-docs/4.0 (Accessed: 16 October 2024.)
22. FlightReader. (n.d.): https://www.flightreader.com/ (Accessed: 20 October 2024.)
23. Airdata UAV (n.d.): Airdata Google Group. https://groups.google.com/g/airdata (Accessed: 11 October 2024.)
24. Airdata UAV (n.d.): Features. https://airdata.com/features#tab-panel-2 Accessed: 11. October 2024.)
25. Datfile.net. (n.d.): Introduction. https://datfile.net (Accessed: 20 October 2024.)
26. Oxygen Forensics (n.d.): Federal and Government Solutions. https://www.oxygenforensics.com/en/solutions/federal-and-government/ (Accessed: 18 October 2024.)
27. BriefCam (n.d.): BriefCam Training. https://www.briefcam.com/resources/briefcam-training (Accessed: 18 October 2024.)
28. Nagy T., Berke J., Fazekas I. (2024): Forensic methodology of drone data saving, processing, and analysis. In: II. Drone Technology Data Processing and Data Security Challenges Conference, Gábor Dénes University, Budapest, 15 November 2024.