

Digital Forensic Analysis of UAV Flight Data Using Static and Dynamic Methods in Coal Mining Area

Muhammad Yusuf Halim¹, Ahmad Luthfi²

¹Master Program in Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

²Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

Email: ¹muhammad.halim@students.uii.ac.id, ²ahmad.luthfi@uii.ac.id

Abstract

Unmanned Aerial Vehicles (UAV) have become vital tools in industrial sectors such as coal mining for site inspections and operational monitoring. However, unauthorized UAV flights present security risks that necessitate forensic investigation. This study examines a forensic case involving a DJI Mini 3 UAV suspected of crossing company boundaries. Using the Conceptual Digital Forensics Model for the Drone Forensic Field, both static and dynamic forensic acquisition methods were applied. Static acquisition recovered 53 photographs, 11 videos, 11 audio files, 10 deleted photos, 4 deleted videos, and 3 unidentified log files. Dynamic acquisition yielded 64 media files including 63 photographs (.JPG and .jpg) with 10 deleted, 14 videos (.MP4, .MOV, .SWF) with 6 deleted, 11 audio files, 4 plain text files, 31 deleted files, 3 EXIF metadata records containing GPS coordinates, and 3 unidentified log files. The GPS data from EXIF metadata was visualized in Google Earth to map flight paths and confirm boundary violations. These findings demonstrate that dynamic acquisition retrieves a more comprehensive artifact set than static acquisition. This study highlights the importance of UAV digital forensics in supporting security investigations and ensuring compliance with industrial UAV policies.

Keywords: UAV Forensics, DJI Mini 3, Static and Dynamic Acquisition, EXIF Metadata, Flight Path Analysis

1. INTRODUCTION

Unmanned Aerial Vehicles or UAVs have evolved from exclusive military tools into widely used platforms across various civilian and industrial domains [1]. These devices offer versatile functionalities such as aerial photography, environmental monitoring, infrastructure inspection, and security surveillance [2], [3]. Their ability to capture high-resolution imagery and real-time data has transformed how organizations gather and process spatial information [4]. According to data from Statista, UAV sales reached five million units globally in 2020 and are projected to climb to 9.6 million units by 2030, reflecting their increasing relevance in modern workflows [5].

In Indonesia, UAV adoption continues to expand, particularly in the coal mining sector. Companies utilize UAVs for tasks such as road mapping, surveying, and site monitoring. These applications improve operational accuracy, reduce time and cost, and enhance worker safety [6], [7]. However, as UAV usage becomes more prevalent, so does the potential for misuse. Unauthorized UAV flights beyond designated areas pose risks to security, privacy, and compliance [8]. In simulated mining scenarios, employees assigned to conduct aerial mapping may unintentionally or deliberately breach operational boundaries without authorization, prompting the need for reliable forensic investigation [9].

To address such incidents, this study applies the Conceptual Digital Forensics Model for the Drone Forensic Field as its analytical framework. This model consists of four core stages: preparation, acquisition, analysis, and documentation [10]. Additionally, this study employs both static and dynamic forensic methods, using FTK Imager for data acquisition and Autopsy for artifact analysis. By introducing the framework and tools early, the research establishes a solid technical foundation from the outset.

Several previous studies have explored UAV forensics, such as investigations on the DJI Phantom 3 [11] and DJI Mini 2 [12]. While these studies demonstrated the potential of flight log analysis and GPS extraction, many lacked a consistent forensic model or failed to simulate real-world violation scenarios. Moreover, to the best of our knowledge, no forensic research has previously focused on the DJI Mini 3, making it a relevant subject of investigation in this study. This study aims to identify and analyze digital artifacts or digital evidence on existing possibilities, such as media and GPS [13] from UAV DJI Mini 3 to support investigations of UAV flight violations in sensitive industrial environments such as coal mining areas.

2. METHODS

This research is carried out by applying a methodology composed of a series of systematic steps that serve as a guide in the process of identifying, analyzing, and solving problems faced throughout the research. This methodology also includes an approach to address various obstacles that may arise during the research process. Thus, the steps taken are designed to produce a comprehensive solution. The details of the stages taken in this study can be seen more clearly in Figure 3.

2.1. Literature Review

Literature Studies is a stage where information is searched from various scientific sources, such as journals, conference proceedings, and other publications, with the aim of enriching the theories that support writing. This step is important so that

writing remains consistent with existing theories. In the introduction, several studies related to UAV forensics have been explained, and the fundamental differences between this study and previous studies have been described, both in terms of methodological approach and analysis focus.

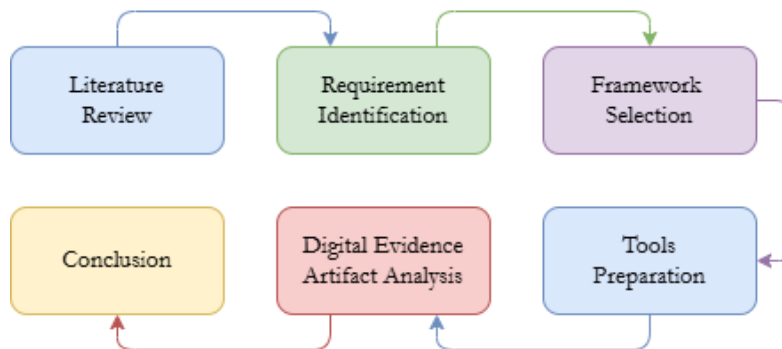


Figure 1. The flow of the research process.

2.2. Requirement Identification

At this stage, the needs needed for research are identified, so that a work environment can be built in accordance with the research objectives. The elements identified included the research location, UAV and UAV's storage, applications, and computers used as research tools. This research was conducted in one of the villages in Kutai Kartanegara Regency, East Kalimantan Province. The selection of this location is based on the existence of a coal mining area that is relevant to the case study scenario in this study.

The UAV used in this study is the DJI Mini 3. DJI Mini 3 was chosen because it has specifications suitable for the purposes of this research, including 4K/30fps video recording capabilities, flight time of up to 38 minutes, and a weight of less than 249 grams which makes it ideal for operation in various conditions. The UAV is also equipped with an O3 (OcuSync 3.0) transmission system that allows remote control of up to 10 km, as well as safety features such as three-way obstacle detection and a Return to Home (RTH) system. In addition, the DJI Mini 3 has a 1/1.3-inch CMOS sensor that can produce 48MP images, which is very useful for mapping and surveying purposes in this study [14].

The UAV is also equipped with an OcuSync 2.0 transmission system that allows remote control of up to 10 km, as well as safety features such as three-way obstacle detection and a Return to Home (RTH) system.



Figure 2. DJI Mini 3 [15]

Furthermore, the acquisition and analysis will be carried out on the UAV memory card. The type of memory card used is SanDisk Micro SD Extreme PRO 32GB. The selection of this memory card is based on several scientific considerations, namely high-power transfer speed, adequate capacity, and resistance to extreme environmental conditions. The SanDisk Micro SD Extreme PRO 32GB offers read speeds of up to 95 MB/s and write speeds of up to 90 MB/s, which is essential for supporting 4K resolution video recording without interruption or data loss. In addition, the card has good resistance to temperature extremes, vibrations, and impacts, making it suitable for use in UAV operational environments that often encounter unpredictable outdoor conditions. This memory card is perfectly compatible with the DJI Mini 3 UAV, which also supports video recording with 4K resolution [15].

2.3. Framework

This research adopts the Conceptual Digital Forensics Model for the Drone Forensic (DR0046) Field as the analytical framework, as it is considered suitable and relevant to the phenomenon and case scenario examined in this study. Flow framework Conceptual Digital Forensics Model for DRF field can be seen in Figure 3.

Based on Figure 3, the research flow will start from the Preparation Stage. The location of the research area is in a former coal mining site in a Village, East Kalimantan Province. UAV was flown over the area, here are pictures of the location of the research area can be seen in Figure 4 and Figure 5.

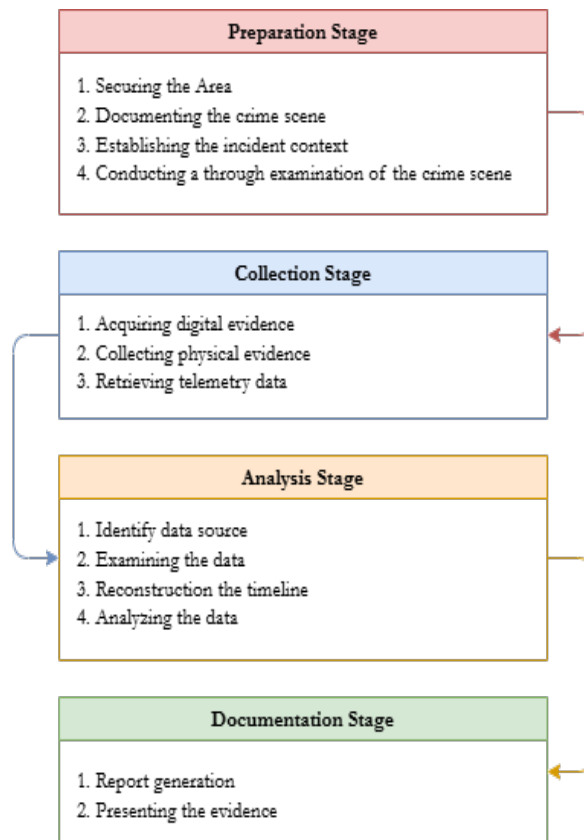


Figure 3. Framework Conceptual Digital Forensics Model for DRF Field [10]



Figure 4. Location of the research area



Figure 5. The location of the research area appears close

Then, at the collection stage, the UAV is flown over the designated research area to capture the necessary data for survey and mapping purposes, such as aerial photographs and videos. In this stage, data acquisition is also performed using two different methods: static and dynamic. The static acquisition is conducted by removing the microSD card from the UAV and connecting it to the forensic workstation using a memory card adapter. Meanwhile, the dynamic acquisition is carried out while the UAV is powered on and directly connected to the workstation using a USB cable. Both methods aim to retrieve as many digital artifacts as possible from different states of the device. To enhance clarity, the step-by-step comparison of both methods is summarized in Table 1.

Table 1. Comparison of Static and Dynamic Acquisition Methods

Step	Static Method	Dynamic Method
1	Power off the UAV and remove the microSD card	Power on the UAV and connect it to the workstation
2	Insert the microSD card into adapter	Establish connection between the UAV and the laptop using a USB Type-C cable
3	Use FTK Imager to acquire a forensic image from the microSD	Use FTK Imager to capture data with the UAV powered on
4	Analyze the acquired image using Autopsy	Analyze the acquired image using Autopsy
5	Extract and interpret media files	Extract and interpret media files and EXIF metadata containing GPS coordinates, which can be visualized using Google Earth

After the collection stage is complete, the analysis stage begins. In this stage, the acquired forensic image files from both methods are examined using forensic analysis tools to identify, extract, and interpret relevant digital artifacts. These may

include media files, metadata, and deleted content. The final stage is documentation, where all findings from the analysis are compiled and presented as digital evidence in accordance with the case scenario.

2.4. Tools Preparation

At this stage, the hardware and software components required for the research have been clearly defined. The hardware setup includes the DJI Mini 3 UAV, which serves as the primary subject of forensic analysis. For conducting forensic tasks such as data acquisition and analysis, an Acer Aspire E14 laptop equipped with an Intel Core i5 8th generation processor is utilized. The UAV stores flight data on a 32GB SanDisk Extreme PRO microSD card, which functions as the main storage medium for this study.

On the software side, the system operates on Microsoft Windows 11 and employs the latest version of the DJI Fly application. The UAV is controlled using a VIVO V19 smartphone running Android version 12, which serves as the RC-N1 remote controller. Forensic acquisition is performed using FTK Imager version 4.7.1, while data analysis is carried out with Autopsy version 4.21.0. A detailed summary of the hardware and software configuration used in this study is presented in Table 2.

Table 2. Summary of Tools and Environment

No	Component	Specification/Description
1	UAV Device	DJI Mini 3
2	Storage Media	SanDisk Extreme PRO 32GB MicroSD
3	Acquisition Tool	FTK Imager version 4.7.1
4	Analysis Tool	Autopsy version 4.21.0 and Google Earth
5	Workstation	Acer Aspire E14, Intel Core i5 8 th Gen, 8GB RAM
6	Operating System	Windows 11
7	RC-N1	VIVO V19 Android Smartphone with DJI Fly Application

2.5. Digital Evidence Artifact Analysis

It was simulated that an employee of a coal mining company, who was responsible for the UAV operator, was given the task of conducting aerial surveys and road mapping in the designated mine area. However, in carrying out its duties, the operator flew the DJI Mini 3 UAV outside the boundaries of the company's operating area without permission. Furthermore, this incident was seen by others, then reported to superiors that there was a UAV flight outside the allowed zone. The company's security team immediately responded by halting the UAV's operations and securing the device for further analysis. The UAV was confiscated for forensic investigation to obtain digital evidence. The results of the acquisition

and analysis on the UAV will be used to compile a report that will be used in disciplinary action against operators who violate the company's rules. Based on the presentation of the simulation, the following is an overview of the flow diagram of the simulation of flight violations that occurred on UAVs, which can be seen in Figure 6.

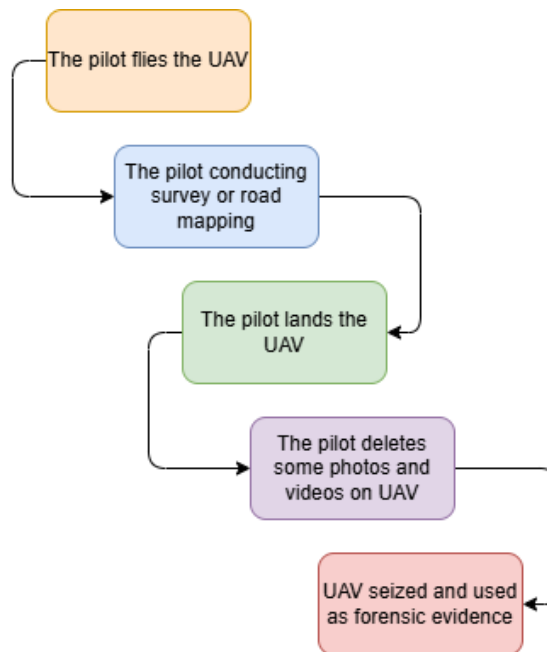


Figure 6. UAV flight violation simulation scenario process flow

Based on Figure 6, the first stage is for an employee to fly a UAV at the border location of the mining area that has been determined to conduct a survey and road mapping. However, while doing this, there were other employees who saw and reported that the UAV was flying outside the company's regional boundaries. So that the UAV was landed. However, after the UAV was landed, the employee in charge of operating the UAV deleted the data on the UAV. The deleted data is in the form of photos and videos of the flight. After that, the UAV was confiscated to be used as evidence for forensics. The forensic activity was carried out to obtain artifacts or data that could be obtained on the UAV. The analysis process on files contained within the file.dd from the acquisition results is conducted using the FTK Imager tool to identify data that contains information as digital evidence. The primary focus of the analysis is on the .001 UAV file, which consists of storage media containing image and video database files from the UAV. In general, the workflow of this research will be presented in the form of a flowchart in Figure 7.

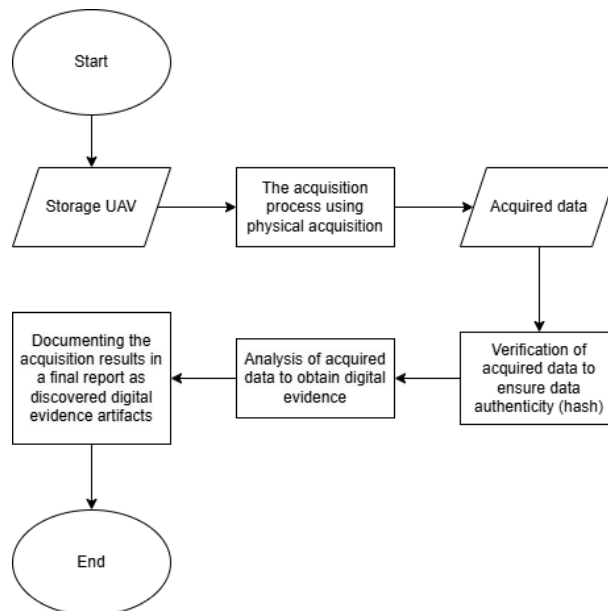


Figure 7. UAV Acquisition and Analysis Workflow

Figure 7 illustrates the steps required to secure and analyze digital evidence from a UAV, from start to finish. The process begins with identifying the storage used as the data source. This initial step ensures that all relevant storage and control components have been identified and are ready for access. Afterward, the acquisition process is conducted physically on the UAV, meaning that data is extracted directly from the UAV using the FTK Imager tool. This physical acquisition is crucial to ensure that all data on the UAV is accurately copied without alterations or data loss.

Once the acquisition process is complete, the result is a file with the .001 extension, which serves as a forensic image of the UAV's storage media. The next step is to verify the .dd file to ensure data authenticity. This verification is performed by comparing the hash value of the .dd file with the original data's hash value, ensuring that the data remains unchanged throughout the acquisition process. To ensure the integrity and authenticity of the acquired digital evidence, hash validation techniques were employed. MD5 and SHA1 hash algorithms were used to generate hash values of the forensic images, allowing verification that the data remained unchanged during acquisition and analysis processes. Maintaining data integrity is crucial because any alteration, intentional or accidental, can compromise the reliability of the evidence and undermine its acceptance in legal proceedings. This step is critical to upholding evidentiary standards and ensuring the legal admissibility of digital forensic findings [16], [17].

3. RESULTS AND DISCUSSION

This section outlines the results and discussion derived from the digital forensic acquisition and analysis conducted on the DJI Mini 3 UAV. The findings are organized based on the stages defined in the DRF Field framework, which include preparation, acquisition, analysis, and reporting.

3.1. Preparation Stage

In the preparation stage of this research, several important steps were taken to ensure that the data collection and analysis process could run well. This research aims to obtain digital evidence based on the phenomena and case studies that have been described earlier. Table 1 has explained the combination of hardware and software used to ensure that the data acquisition and analysis process can run smoothly.

The research location was chosen in the former mining area, considering the difficulty in obtaining official permits to conduct research in active mining areas. Although the former mine area provides easier access, challenges remain, especially with the limited condition of facilities and infrastructure. Frequent on-site power outages are one of the main obstacles, considering that the acquisition and analysis process requires a stable supply of electricity for equipment such as laptops and UAVs. In addition, weather conditions at the research site also added to the challenge, with rainfall high enough to limit UAV flights. UAVs cannot be flown when it rains, so researchers must carefully arrange flight schedules according to weather conditions with all these preparations and considerations, researchers must also be flexible in adjusting their schedules and data collection strategies to minimize the impact of these obstacles

3.2. Collection Stage

During the collection stage, data acquisition is conducted using two approaches, namely static acquisition and dynamic acquisition, in line with standard practices in digital forensic research. The static acquisition method involves removing the microSD card from the UAV and connecting it to a laptop or forensic workstation using an adapter. In this approach, all data stored on the microSD card is extracted in detail to identify digital artifacts relevant to the research objectives. This includes media files, metadata, and other flight-related records captured during UAV operation. The acquisition process is performed using the FTK Imager application, and the results are presented in Figure 8. Furthermore, the integrity of the acquired data has been verified through hash value validation, with both MD5 and SHA1 hash values successfully matching, confirming the authenticity and completeness of the forensic image.

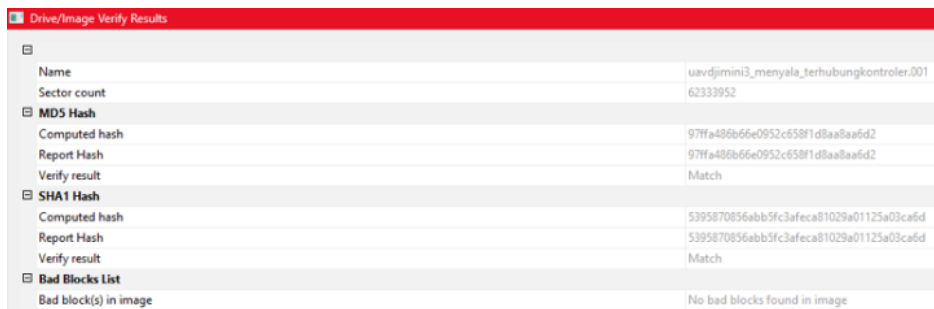
Drive/Image Verify Results	
Name	uavdjimini3.001
Sector count	62333952
MD5 Hash	
Computed hash	99ede1ed9d521f5af817c3c6a204b656
Report Hash	99ede1ed9d521f5af817c3c6a204b656
Verify result	Match
SHA1 Hash	
Computed hash	1080047c23fa4f30841c5afca5ff0914df44001
Report Hash	1080047c23fa4f30841c5afca5ff0914df44001
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 8. Hash value acquisition on SanDisk Micro SD storage using static method

The next process is acquisition using the dynamic method. In this method, the UAV is powered on and then connected to a laptop via a USB Type-C cable. Acquisition is performed using FTK Imager software to generate a forensic image file with a .001 extension. Once the acquisition process is complete, the software automatically displays the MD5 and SHA1 hash values of both the source data and the duplicated file. The verification results show that both hash values are identical, indicating that the integrity of the data was successfully maintained during the acquisition process. This procedure can be seen in Figures 9 and 10.



Figure 9. Dynamic Acquisition Process



Drive/Image Verify Results	
Name	uavdijmini3_menyala_terhubungkontroler.001
Sector count	62333952
MD5 Hash	
Computed hash	97ff4486b66e0952c658f1d8aa8a6d2
Report Hash	97ff4486b66e0952c658f1d8aa8a6d2
Verify result	Match
SHA1 Hash	
Computed hash	539587085abb5fc3afeca81029a01125a03cafd
Report Hash	539587085abb5fc3afeca81029a01125a03cafd
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 10. Hash Value Acquisition Results on DJI Mini 3 UAV Using Dynamic Method

3.3. Analysis Stage

The analysis of the UAV DJI Mini 3 image files obtained through the static method revealed 64 media files dated August 28, 2024, consisting of 53 photos, 11 videos, and 11 audio files. Additionally, deleted files were found, including 10 photos and 4 videos. Based on metadata tracing and visual content, the deleted photos depicted images of residential areas, plantation areas, and a mosque. Meanwhile, the four deleted videos, which initially could not be played through Autopsy's internal features, were successfully played after extraction. One of the playable videos showed that the UAV flew beyond the designated boundary, in line with the simulated violation scenario. The analysis also revealed three files with a .log extension; however, further investigation showed that these files did not contain any flight log information. Therefore, it can be concluded that no flight log files were found in the results of the static method acquisition.

In the dynamic acquisition process conducted on the DJI Mini 3 UAV, data analysis using Autopsy software revealed a total of 64 media files, consisting of both active and deleted items. Among them, 31 deleted files were identified, including 4 video files with .MP4 extensions, 2 with .MOV extensions, 10 photo files with .JPG extensions, 10 with .jpg extensions, 4 text files with .TXT extensions, and 1 file with a .SWF extension. Furthermore, 63 image files containing EXIF metadata were found, comprising 53 files with .JPG extensions and 10 with .jpg extensions. The EXIF data provided detailed geographic coordinates, including latitude, longitude, and altitude, indicating the exact capture locations of the images, all of which shared the same timestamp of August 28, 2024. Notably, the analysis uncovered visual evidence supporting the case scenario of a boundary violation, with one significant photo showing a farmer within a plantation area. The location of this image was verified through its EXIF metadata, confirming that the UAV had flown outside the authorized boundary of the coal mining site. This visual evidence, which reinforces the occurrence of the violation, is presented in Figure 11.

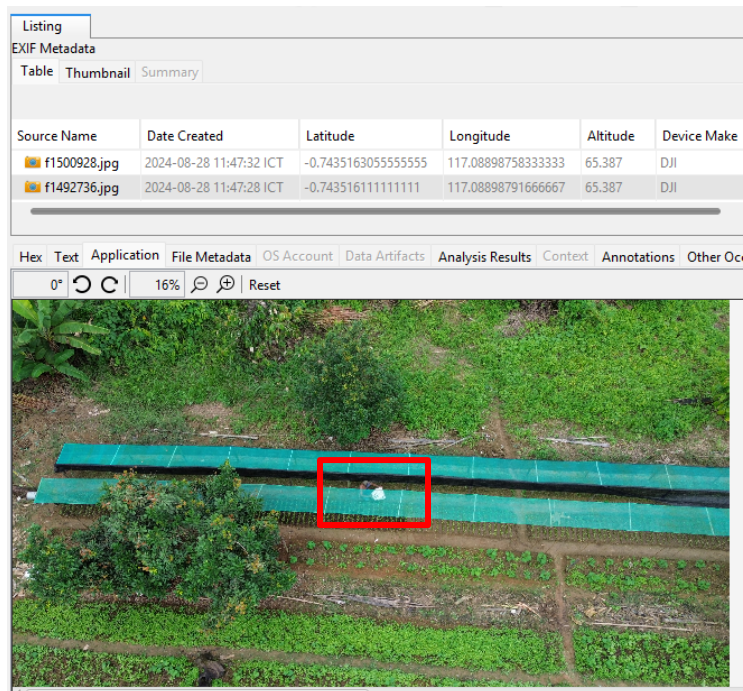


Figure 11. A Farmer in Plantation Area

Following the extraction of EXIF metadata containing geographic coordinates for each image, the researcher conducted a spatial analysis by plotting selected photo artifacts onto the Google Earth platform. This process was carried out to identify and mark the specific locations where the UAV had flown, based on the visual evidence derived from the coordinate information embedded in the metadata. These mapped locations provided clear indications of flight path violations, as illustrated in Figure 12.



Figure 12. UAV Flight Coordinate Points Based on EXIF Metadata

Figure 12 displays the Google Earth interface used for geospatial analysis in this study. In the visual representation, blue markers indicate the designated coal mining area, red markers correspond to the residents' plantation zones, and yellow markers represent the residential area, including public facilities such as a mosque. The plotted data confirms that the UAV had crossed the official boundary of the coal mining site. However, it is important to note that the satellite imagery available on Google Earth had not yet been updated at the time of analysis, resulting in the area still appearing as undeveloped green forest rather than an active mining zone. This research was conducted in a rural area located in Kutai Kartanegara Regency, East Kalimantan. The results of the analysis indicate that the dynamic acquisition method yielded a richer set of data compared to the static method. This includes a greater number of media files, as well as more detailed metadata, particularly EXIF information containing GPS coordinates, which were not fully captured through the static acquisition process.

3.4. Documenting Stage

The documentation phase represents the final stage in the digital forensic process based on the DRF Field Framework. At this stage, all investigative findings are systematically compiled to provide a comprehensive overview of the forensic activities conducted. The results are presented in tabular form to facilitate the identification of data, interpretation of findings, and correlation between extracted digital artifacts. Specifically, Table 3 summarizes the results obtained through the static acquisition method, while Table 4 presents the findings from the dynamic acquisition method. Both tables display the types of artifacts recovered, associated metadata, and digital evidence that support the simulated case of airspace violation involving the UAV.

Table 3. Static Method Artifact Report of the DJI Mini 3 UAV

Artifact Types	Number of Files	Information
Photograph	53	Photo creation date on August 28, 2024
Video	11	Video shooting date on August 28, 2024
Audio	11	Audio can't be played
Deleted Photos	10	Contains pictures of grades, residential areas, and mosque.
Deleted Videos	4	Cannot be rotated, but can be rotated after extraction
File .log	3	Cannot be identified
Evidence of Violation	Yes	Based on photos and videos that contain areas other than coal mining

Table 4. Dynamic Method Artifact Report of the DJI Mini 3 UAV

Artifact Types	Number of Files	Information
Media Files	64	Media file found on August 28, 2024, according to the case study
Photograph	63	.JPG (53), .jpg (10), and deleted files .JPG (10)
Video	14	.MP4 (11) deleted 4, .mov (2), and .swf (1)
Audio	11	Audio can't be played
Plain Text	4	.txt
Deleted Files	31	.MP4 (4), .mov (2), .JPG (10), .txt (4), and .swf (1)
EXIF Metadata	3	Shows GPS info (latitude, longitude, and altitude) and can be analyzed on Google Earth website
File .log	3	Cannot be identified
Evidence of Violation	Yes	Based on photos and videos that contain areas other than coal mining

3.5. Discussion

A key finding from the analysis of the DJI Mini 3 UAV is the presence of EXIF metadata within the image files obtained through dynamic acquisition. This metadata includes geographic information such as latitude, longitude, and altitude, which is highly valuable for tracking UAV flight paths. In contrast, the static acquisition method did not yield similar metadata, and the overall artifacts retrieved were significantly more limited. Interestingly, the dynamic acquisition also revealed duplicate image files with differing extensions, specifically .JPG and .jpg, indicating the need for precision in managing and categorizing forensic artifacts. Additionally, three log files were discovered, camera_log.log, fc_log.log, and linux_log.log. Various tools were employed to interpret these files, including DatCon, Airdata.com, Phantomhelp.com, and AI-based. However, none of the files could be successfully parsed. Even after converting the extensions to .txt, the file contents remained unreadable. Based on their filenames, it is assumed that camera_log.log relates to camera activity, fc_log.log to the flight controller, and linux_log.log to the UAV's operating system. Notably, no recognizable flight log artifacts were recovered from the device. Another unique finding was the discovery of 11 audio files, which is unexpected given that the DJI Mini 3 does not support audio recording. Further inspection revealed that these audio tracks were embedded components of video files stored in separate formats.

This analysis highlights several common challenges faced in UAV forensics. The inability to parse critical log files suggests that such data may be stored in

unreadable or proprietary formats, complicating forensic retrieval efforts. The presence of duplicate image files with differing extensions further complicates artifact management and validation. Moreover, the volatile nature of UAV data, especially those captured through dynamic acquisition, necessitates prompt forensic action to preserve transient information that could be lost once the UAV is powered off.

To improve forensic readiness for UAV models similar to the DJI Mini 3, it is essential to implement systematic data logging and secure storage protocols within both the UAV and its ground control systems. Firmware updates and design standards should prioritize forensic accessibility, allowing authorized investigators to retrieve comprehensive flight data, including telemetry and control commands. Collaboration between regulatory bodies, UAV manufacturers, and law enforcement agencies is vital to establish standardized forensic frameworks that ensure digital evidence integrity and facilitate legal proceedings related to UAV violations.

From a legal standpoint, although this research does not involve a real court case, it is relevant to consider the admissibility of UAV-based digital evidence within the context of Indonesian law. Referring to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), along with the Indonesian Criminal Procedure Code, digital evidence such as images, GPS metadata, and other electronic records can be accepted in court if acquired through proper forensic procedures. This legal framework has undergone several amendments, most recently through Law Number 1 of 2024, which introduced changes to various provisions in Law Number 11 of 2008 as amended by Law Number 19 of 2016 [18]. These changes reinforce the legal recognition and admissibility of electronic evidence in judicial processes. In this study, the integrity of digital data was preserved using hash verification techniques with MD5 and SHA1, thereby supporting the authenticity and reliability of the evidence. In addition, UAV operations in Indonesia are regulated under the Minister of Transportation Regulation Number 63 of 2021, which prohibits drone flights beyond designated areas or within restricted zones without permission [19]. The forensic findings in this study, particularly the detection of UAV flight beyond the operational boundary based on GPS data, clearly demonstrate the practical relevance of such regulations. Therefore, UAV forensics not only supports technical investigations but also plays an important role in enforcing compliance with aviation safety laws.

4. CONCLUSION

This study demonstrates that the application of the Conceptual Digital Forensics Model for the Drone Forensic Field, supported by the use of FTK Imager and Autopsy, is effective in extracting and analyzing digital forensic artifacts from the

DJI Mini 3 UAV. The findings reveal that most of the digital evidence available on this device consists of media files such as images and videos, along with EXIF metadata. The EXIF metadata is particularly valuable as it contains GPS coordinates including latitude, longitude, and altitude, which are essential for mapping UAV flight paths and identifying potential boundary violations. Notably, these GPS data were obtained through the dynamic acquisition method, which provides more comprehensive forensic information than static acquisition. Critical data such as flight logs and detailed telemetry information were not found within the UAV itself.

Based on this limitation, future research is encouraged to conduct forensic analysis not only on the UAV but also on the ground control station or controller device, which is likely to store essential operational data including flight paths and control logs. In addition, employing alternative forensic tools may offer comparative insights that enhance the diversity and depth of artifact analysis. Beyond its technical contribution, this study also highlights the practical relevance of UAV forensics in supporting security enforcement within industrial environments. The ability to extract digital evidence related to boundary violations can serve as a valuable resource for companies to develop stricter UAV operation policies, improve internal compliance protocols, and align with national airspace regulations to prevent unauthorized drone activities in restricted zones.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Ministry of Research, Technology, and Higher Education of the Republic of Indonesia for the financial support provided through the Student Thesis Research Grant (PTM) scheme, under Contract Number: 052/DirDPPM/70/DPPM/PFR-KEMDIKBUDRISTEK/VI/2024.

REFERENCES

- [1] K. Al-Room *et al.*, 'Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models', *International Journal of Digital Crime and Forensics*, vol. 13, no. 1, pp. 1–25, Jan. 2021, doi: 10.4018/IJDCF.2021010101.
- [2] N. Y. Pinatik and F. S. Papilaya, 'Pengolahan Foto Udara UAV (Unmanned Aerial Vehicle) Menggunakan Software Agisoft Metashape', *jupeI*, vol. 6, no. 1, pp. 1–11, Feb. 2024, doi: 10.32520/jupeI.v6i1.2838.
- [3] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, 'Research Challenges and Opportunities in Drone Forensics Models', *Electronics*, vol. 10, no. 13, p. 1519, Jun. 2021, doi: 10.3390/electronics10131519.

- [4] R. Kumar and A. K. Agrawal, 'Drone GPS data analysis for flight path reconstruction: A study on DJI, Parrot & Yuneec make drones', *Forensic Science International: Digital Investigation*, vol. 38, p. 301182, Sep. 2021, doi: 10.1016/j.fsidi.2021.301182.
- [5] S. Silalahi, T. Ahmad, and H. Studiawan, 'Transformer-Based Named Entity Recognition on Drone Flight Logs to Support Forensic Investigation', *IEEE Access*, vol. 11, pp. 3257–3274, 2023, doi: 10.1109/ACCESS.2023.3234605.
- [6] M. Loli, S. A. Mitoulis, A. Tsatsis, J. Manousakis, R. Kourkoulis, and D. Zekkos, 'Flood Characterization Based on Forensic Analysis of Bridge Collapse Using UAV Reconnaissance and CFD Simulations', *Science of The Total Environment*, vol. 822, p. 153661, May 2022, doi: 10.1016/j.scitotenv.2022.153661.
- [7] I. P. Putrawiyanta, Novalisae, Noveriady, Ferdinandus, and A. Drobank, 'Pemanfaatan Teknologi Drone Untuk Pemetaan Perubahan Rona Bentang Alam Pada Wilayah Pertambangan', *AKSELERASI*, vol. 5, no. 3, pp. 50–56, Nov. 2023, doi: 10.54783/jin.v5i3.783.
- [8] V. Chamola, P. Kotes, A. Agarwal, Naren, N. Gupta, and M. Guizani, 'A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques', *Ad Hoc Networks*, vol. 111, p. 102324, Feb. 2021, doi: 10.1016/j.adhoc.2020.102324.
- [9] A. Almusayli, T. Zia, and E.-H. Qazi, 'Drone Forensics: An Innovative Approach to the Forensic Investigation of Drone Accidents Based on Digital Twin Technology', *Technologies*, vol. 12, no. 1, p. 11, Jan. 2024, doi: 10.3390/technologies12010011.
- [10] F. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, 'A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field', *Eng. Technol. Appl. Sci. Res.*, vol. 13, no. 5, pp. 11608–11615, Oct. 2023, doi: 10.48084/etasr.6195.
- [11] S. E. Prastya, S. P. Cipta, and B. Nugraha, 'Analisis Log Penerbangan Pada Unmanned Aerial Vehicle (UAV) Sebagai Barang Bukti Digital', *JTekInfULM*, vol. 5, no. 1, pp. 11–18, Apr. 2020, doi: 10.20527/jtiulm.v5i1.42.
- [12] M. Stanković, M. M. Mirza, and U. Karabiyik, 'UAV Forensics: DJI Mini 2 Case Study', *Drones*, vol. 5, no. 2, p. 49, Jun. 2021, doi: 10.3390/drones5020049.
- [13] E. Mantas and C. Patsakis, 'Who watches the new watchmen? The challenges for drone digital forensics investigations', *Array*, vol. 14, p. 100135, Jul. 2022, doi: 10.1016/j.array.2022.100135.
- [14] A. Taylor, 'A Digital Forensics Case Study of the DJI Mini 3 Pro and DJI RC', *arXiv*, p. 20, 2023, doi: 10.48550/arXiv.2309.10487.
- [15] DJI, 'DJI Mini 3', DJI Mini 3 So Fly, 2025. [Online]. Available: <https://www.dji.com/id/mini-3>

- [16] P. K C, R. Soman, and P. Honnavalli, 'Validity of Forensic Evidence using Hash Function', in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India: IEEE, Jun. 2020, pp. 823–826. doi: 10.1109/ICCES48766.2020.9138061.
- [17] P. Kr. Boyanov, 'Practical Applications of Hash Functions MD5, SHA-1, And SHA-256 Using Various Software Tools to Verify the Integrity of Files', *JSAR*, vol. 27, no. 1, pp. 120–137, Nov. 2024, doi: 10.46687/jsar.v27i1.413.
- [18] R. Indonesia 'Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik'. 2024.
- [19] R. Indonesia, 'Peraturan Menteri Perhubungan Nomor 63 Tahun 2021 tentang Peraturan Keselamatan Penerbangan Sipil Bagian 107 tentang Sistem Pesawat Udara Kecil Tanpa Awak'. 2021.