Forensic Analysis of UAV DJI MINI 3 and Non-rooted RC-N1 Android Smartphone Using DRF Framework

Muhammad Yusuf Halim[1*], Ahmad Luthfi[2]

[1]*Graduate of Master Program in Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[2]*Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*

*corr-author: Muhammad.halim@alumni.uii.ac.id

Abstract - The increasing use of Unmanned Aerial Vehicles across various sectors also raises potential misuse, such as unauthorized surveillance and airspace violations. This research aims to analyze digital artefacts from UAV DJI Mini 3 and Android Smartphone Controller (DJI RC-N1) using the DRF Field forensic framework. Data acquisition was performed through static and dynamic methods on the UAV and both physical and logical methods on the smartphone, without rooting the device. The analysis reveals that dynamic acquisition on the UAV provides geotagged EXIF images, including latitude, longitude, and altitude information. Meanwhile, flight log data were not found on the UAV but were successfully retrieved from the smartphone via logical acquisition by identifying the DJI Fly application package (dji.go.v5). The extracted flight logs were then processed into .kmz format using Phantomhelp.com and visualized through Google Earth to confirm airspace violations. This study highlights that all forensic acquisition was conducted without rooting, ensuring device integrity and legal admissibility.

Keywords: UAV forensics, android forensics, DJI Mini 3, digital evidence analysis, non-root acquisition

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), or drones, are pilotless aircraft that can be operated remotely and are increasingly used across a wide range of applications, including photography, videography, reconnaissance, mapping, and surveillance [1-4]. While UAVs were initially limited to military purposes, their usage has significantly expanded into commercial and personal domains [5]. According to data from Statista, global UAV sales reached 5 million units in 2020 and are projected to increase to 9.6 million units by 2030 [6]. In Indonesia, UAVs are also widely adopted in various sectors, particularly in coal mining, where they are utilized for mapping and exploration. This implementation enhances operational efficiency, improves safety, and reduces overall costs [7-8]. However, the widespread availability and increasingly sophisticated features of UAVs also bring new challenges related to security and privacy. There have been several cases of UAV misuse, including unauthorized flights in restricted zones, smuggling, industrial espionage, and breaches of personal or institutional privacy [9-10]. These incidents underscore the importance of UAV forensics [11], which focuses on identifying, acquiring, and analyzing digital evidence from UAVs and their associated control systems [12-13].

This study presents a simulated case in which a UAV pilot conducted a road-mapping task but violated operational boundaries by flying the drone beyond the authorized mining area. Such incidents require digital forensic investigation to acquire and analyze data that can serve as admissible evidence in legal or disciplinary proceedings. Artifacts such as images, videos, GPS coordinates, and flight logs become key digital evidence in understanding the intent and scope of the violation [14]. Prior research has explored UAV forensic acquisition on devices such as the DJI Phantom 3 Advanced and DJI Mini 2 [15-16], typically using Android smartphones that had been rooted to gain access to data. However, rooting a device can compromise system integrity and jeopardize the validity of the digital evidence in legal contexts [17]. This study differs by successfully conducting forensic acquisition on a non-rooted Android smartphone connected to a DJI RC N1 controller, thereby preserving the reliability and admissibility of the extracted data [18-19].

Compared to previous UAV forensic studies, most existing research has relied on generic digital forensic models and rooted Android environments, which allow full system access but risk data manipulation and legal inadmissibility. Tools like MAGNET Axiom and MOBILedit are commonly used, but they face significant limitations when applied to non-rooted smartphones. Furthermore, earlier frameworks such as those proposed

by Clark and Renduchintala [20] offer foundational guidance but are not specifically designed for newer UAV models such as the DJI Mini 3 that lack internal memory. This research employs the DRF Field framework as a more structured and adaptable approach that fits the modern constraints of UAV forensic investigations [21].

To extract artifacts effectively, this study employs both static and dynamic forensic methods, guided by the Conceptual Digital Forensics Model (CDFM) for the Drone Forensic (DRF) field framework, which provides a structured process from data acquisition to reporting [22]. While many previous studies have focused on UAVs with internal memory such as the DJI Phantom[20, 23-24], DJI Mavic Air [25-26], DJI Matrice 210 [27-28], and DJI Mavic [29-30], the DJI Mini 3 presents a unique forensic challenge due to the absence of internal storage, unlike the DJI Mini 3 PRO, which has internal memory [31]. This distinct characteristic requires forensic investigators to explore alternative sources of digital evidence, primarily from external storage and controller-linked devices.

The novelty of this research lies in two key contributions. This study extends the author's previous work on the DJI Mini 3, published under the title "Digital Forensic Analysis of UAV Flight Data Using Static and Dynamic Methods in Coal Mining Area," [32] which focused solely on UAV-level forensic acquisition. First, it presents a forensic study focused specifically on the DJI Mini 3 (non-Pro), a model that has not been explored in previous UAV forensic literature such as the DJI Mini 2, Phantom 3, or Mavic series. The DJI Mini 3 differs from those models because it lacks internal storage, which presents unique challenges in data acquisition. Second, it advances the scope of analysis by including the DJI RC-N1 Android controller smartphone, demonstrating successful flight log extraction without rooting. This process is technically challenging because access to critical directories is normally restricted on non-rooted devices. By achieving flight log extraction without rooting, this study offers a practical and legally sound approach that improves upon previous forensic methodologies. These two innovations directly address a research gap in UAV digital forensics and offer new perspectives beyond existing studies.

II. METHOD

This study uses a case study approach focusing on the DJI Mini 3 UAV and DJI RC-N1 Android controller. Digital forensics methods include static and dynamic, as well as physical and logical acquisition to collect flight logs, metadata, and multimedia files without rooting the controller to preserve system integrity. The case was simulated in a coal mining area where the UAV flew outside permitted boundaries, violating safety rules. In total, four acquisition sessions were conducted using distinct techniques for each device. The first acquisition was performed on the UAV using a static method by imaging the microSD card while the device was powered off. The second acquisition involved a dynamic method on the UAV while it was powered on. The third and fourth acquisitions focused on the Android smartphone controller using physical and logical methods respectively, both conducted under static conditions with airplane mode enabled. This multi-method approach ensured comprehensive artifact collection and allowed cross-validation of findings between acquisition types. CDFM for the DRF field framework guided the investigation stages, highlighting novel non-root acquisition on the Android controller and acquisition from the UAV without internal memory. An overview of the entire research workflow is illustrated in Figure 1, integrating both UAV and controller processes from the simulated incident to the reporting phase.

A. Simulated Case Study

This study adopts a case study approach by simulating a scenario of UAV flight violations in a coal mining environment. In this simulation, a UAV operator is found to fly the UAV for road survey and mapping purposes. However, the operator deliberately flew the UAV beyond the operational area boundary without official approval from the company. This case illustrates a real-world situation in which UAVs may be used for activities that potentially violate legal regulations and standard operating procedures, such as exceeding certain territorial boundaries [33]. The research location is in a former coal mining area located in a village in Kutai Kartanegara Regency, East Kalimantan Province.

B. Framework

This study uses CDFM for the DRF Field framework as a reference for the forensic process implementation. This framework was specifically developed to address the characteristics of UAV devices. It has a structured and systematic workflow, encompassing the stages of identification, acquisition, analysis, and reporting of results, enabling a comprehensive forensic process that can be reproduced by other researchers. This framework starting with the Preparation Stage, which secures the incident site, documents initial conditions, and understands the event context to ensure structured investigation and accurate evidence identification. Next, the Collection Stage gathers digital and physical evidence from the DJI Mini 3 UAV and the DJI RC-N1

controller with an Android smartphone, following forensic procedures to obtain complete and legitimate data. The Analysis Stage reviews the collected data to reconstruct events, understand UAV usage, and detect potential violations. Finally, the Documentation Stage compiles and presents the investigation results systematically for use by authorities or relevant parties.

C. Tools and Acquisition Techniques

This study utilizes various hardware and software to support the acquisition and analysis of digital artifacts on the DJI Mini 3 UAV and the Android Smartphone Controller DJI RC-N1. A list of the hardware and software used is presented in Table I and Table II.

After all devices were prepared, the acquisition process was carried out separately for each device: the UAV and the controller. Each device required a tailored acquisition approach and method, adapted to its storage structure and operating system.

Fig. 1 illustrates the integrated research workflow for both the DJI Mini 3 UAV and the DJI RC-N1 Android controller smartphone. The process begins with physical acquisition using static and dynamic methods for the UAV, and static acquisition for the RC-N1 Android controller smartphone. If the acquisition results are incomplete, such as missing flight logs, logical acquisition is performed on the RC-N1 using Android Debug Bridge (ADB). Once the required data is obtained, both UAV and controller data undergo hash verification to ensure authenticity, followed by artifact analysis and correlation to identify digital evidence. The workflow concludes with reporting and presenting the combined findings from the UAV and the RC-N1 Android controller smartphone. This integrated approach ensures that evidence from both devices is validated and cross-referenced, strengthening the reliability and admissibility of the forensic results. The acquisition process on the DJI Mini 3 UAV used physical methods with static and dynamic approaches. In the static method, data was collected while the device was off by extracting the microSD card and imaging it with FTK Imager. The dynamic method accessed data with the UAV powered on. All data was analyzed using Autopsy to identify digital artifacts. For the DJI RC-N1 controller, acquisition was done under static conditions with airplane mode enabled. Physical acquisition using MOBILedit Forensic Express PRO failed to retrieve flight logs due to restricted access to the /data/ directory on non-rooted devices. To resolve this, logical acquisition via Android Debug Bridge (ADB) was performed, allowing secure data extraction without root access [34-36]. This method successfully retrieved relevant data from the DJI Fly application while maintaining system integrity and ensuring the legal admissibility of digital evidence.

III. RESULT AND DISCUSSION

This section presents the results and discussion of the digital forensic acquisition and analysis processes conducted on two primary devices: the DJI Mini 3 UAV and the DJI RC-N1 controller integrated with an Android Smartphone Controller. All findings are structured according to the stages in the CDFM for the DRF Field framework, starting from preparation, acquisition, and analysis to reporting. To maintain a systematic flow of discussion, the results are first focused on the UAV device, followed by the analysis of the Android controller as part of the UAV control system.

A. Preparation Stage

In the initial stage, as outlined by the adopted framework, a preparation process was carried out, which included location identification, preliminary documentation, and incident simulation to establish the forensic investigation context. This study was simulated in a mining area located in a village in East Kalimantan Province, Indonesia. The site was selected as reflecting a real-world work environment in the mining sector, where UAVs are commonly used for mapping activities. The simulation focused on a UAV operational violation, in which the operator deliberately flew the UAV beyond the designated mapping boundary set by the company.

TABLE I
HARDWARE USED

No	Hardware	Information
1	UAV DJI Mini 3	Main UAV device as a research object
2	DJI RC-N1	The UAV controller used to operate the DJI Mini 3, connected to an Android smartphone via USB
3	VIVO V19 Smartphone Android	Android device that functions as the main screen and system on the DJI RC-N1 controller via the DJI Fly app
4	MicroSD SanDisk Extreme PRO 32GB	External storage media on DJI Mini 3 UAV
5	SanDisk Adapter	Media connecting Micro SD memory to laptop *workstation*
6	Laptop Acer (Intel i5 Gen 8)	Used for acquisition, analysis, and reporting of digital artifacts

TABLE II
SOFTWARE USED

No	Software	Version	Information
1	Microsoft Windows	11	The main operating system on the forensic analysis device
2	DJI Fly	1.13.10	UAV controller app on smartphone
3	MOBILedit Forensic Express PRO	7.4.1.21502	Forensic software used for physical acquisition on smartphones
4	FTK Imager	4.7.1	Used for data acquisition (physical image)
5	Autopsy	4.21.0	Used for forensic analysis of digital artifacts
6	Android	12	Operating system on DJI RC-N1 android smartphone
7	Android Debug Bridger	35.0.2	Tools for communication and data extraction from Android devices
8	earth.google.com/web/	Website	Website to analyze GPS
9	airdata.com	Website	Website to analyze logs
10	phantomhelp.com	Website	Website to read flight logs

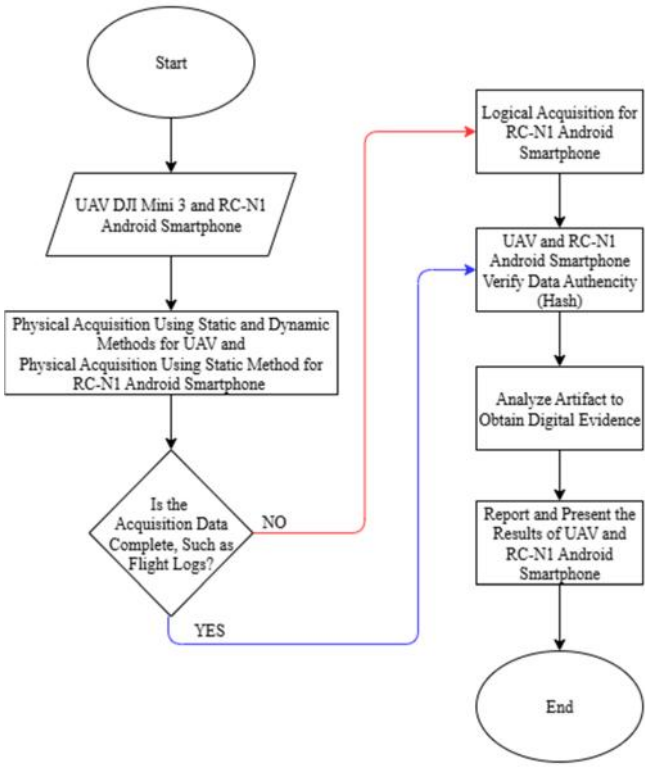

Fig. 1 Integrated workflow for forensic acquisition and analysis of DJI Mini 3 UAV and RC-N1 android smartphone

B. Collection Stage

The second stage is the collection stage. In this stage, acquisition steps were carried out on both the UAV and the controller. For the UAV, acquisition was performed using both static and dynamic methods as part of physical acquisition. In the static step, the microSD from the UAV was connected to an adapter. The adapter was then acquired using FTK Imager to obtain an image file with the .001 extension. Once the acquisition process was completed, FTK Imager automatically displayed a comparison of the MD5 and SHA1 hash values between the source data and the duplicated file. Based on the verification results, the hash values showed a match, indicating that the integrity of the data was preserved during the acquisition process. This can be seen in Fig. 2.

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 Fig. 3 and 4.

Subsequently, on the RC-N1 controller, acquisition was performed using the static method (airplane mode) as part of physical acquisition on the Android smartphone. The developer options on the smartphone device were activated, after which the smartphone was connected to the laptop using a USB Type-C cable for acquisition using MOBILedit Forensic Express PRO. At this stage, the MOBILedit tool displayed a pop-up message indicating that the artifact data would be incomplete if the smartphone was not rooted. The acquisition file from the physical acquisition process on the smartphone using MOBILedit tools generated three files ready for analysis, namely Report.pdf, Report_index.pdf, and Report_long.pdf. Subsequently, a

logical acquisition process was performed because no flight log files from the UAV were found in the acquisition results using MOBILedit tools. The tool used in this stage was ADB, which is known to be effective for data extraction in forensic purposes [37]. Acquisition using ADB must be performed manually through the Command Prompt (CMD). Before acquisition, the smartphone was set to airplane mode and developer options were enabled. The adb devices command was executed via CMD to detect the connected device. At this stage, a pop-up appeared on the smartphone requesting USB debugging authorization, which had to be granted to proceed with the process.

Fig. 5 illustrates the process of acquiring data from the folder /storage/emulated/0/Android/data/dji.go.v5 on the smartphone, while simultaneously saving the acquisition process log and the process of applying hash values to the acquired files.

Fig. 7 illustrates the process of applying hash values to the original data stored on the smartphone and Fig. 8 illustrates the process of transferring hash data from the original files obtained from the smartphone to the laptop used for analysis. The hash values, using MD5 and SHA-256, are then compared with the hash values from the acquisition results. The verification shows that all hash values are identical, indicating that the integrity between the original data and the acquired data has been successfully maintained.

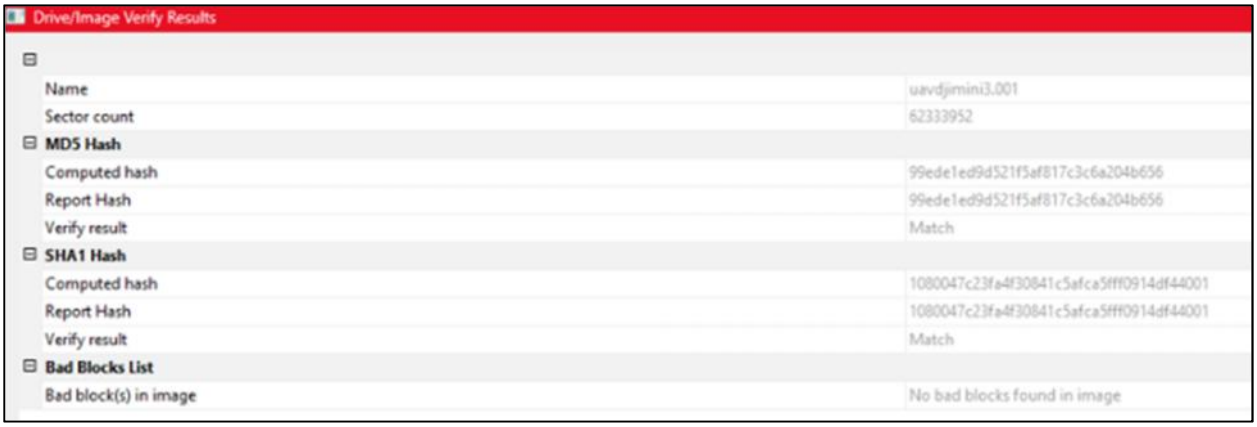

Fig. 2 Hash value of DJI Mini 3 acquisition using FTK imager (static method)

Fig. 3 Dynamic method acquisition process

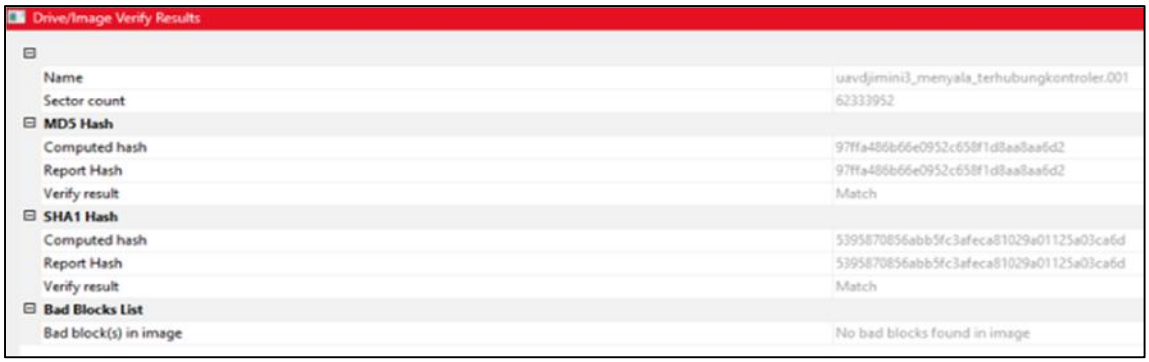

Fig. 4 Hash value of DJI Mini 3 acquisition using FTK imager (dynamic method)

```
C:\Windows\System32>adb pull "/storage/emulated/0/Android/data/dji.go.v5" "C:\AkuisisiLogicalAndroid
" > C:\AkuisisiLogicalAndroid\log_akuisisi.txt 2>&1

C:\Windows\System32>notepad C:\AkuisisiLogicalAndroid\log_akuisisi.txt
```

Fig. 5 Data acquisition process on RC-N1 android smartphone

```
Administrator: Command Prompt
" > C:\AkuisisiLogicalAndroid\log_akuisisi.txt 2>&1

C:\Windows\System32>notepad C:\AkuisisiLogicalAndroid\log_akuisisi.txt

C:\Windows\System32>for /R "C:\AkuisisiLogicalAndroid\dji.go.v5" %f in (*) do @certutil -hashfile "%
f" MD5 >> C:\AkuisisiLogicalAndroid\hash_md5.txt

C:\Windows\System32>for /R "C:\AkuisisiLogicalAndroid\dji.go.v5" %f in (*) do @certutil -hashfile "%
f" SHA256 >> C:\AkuisisiLogicalAndroid\hash_sha256.txt
```

Fig. 6 Hashing process on acquired data

```
Administrator: Command Prompt

C:\Windows\System32>
C:\Windows\System32>adb shell
1919:/ $ cd /storage/emulated/0/android/data/dji.go.v5
ind . -type f -exec md5sum "{}" \; > /sdcard/hash_dji_md5.txt                    <
1919:/storage/emulated/0/android/data/dji.go.v5 $ find . -type f -exec md5sum "{}" \; > /sdcard/hash
_dji_md5.txt
1919:/storage/emulated/0/android/data/dji.go.v5 $ find . -type f -exec md5sum "{}" \; > /storage/emu
lated/0/hash_dji_md5.txt
1919:/storage/emulated/0/android/data/dji.go.v5 $ find . -type f -exec sha256sum "{}" \; >/storage/e
mulated/0/hash_dji_sha256.txt
1919:/storage/emulated/0/android/data/dji.go.v5 $ exit
```

Fig. 7 Hashing process on android smartphone using MD5 and SHA256

```
Administrator: Command Prompt

C:\Windows\System32>adb pull /storage/emulated/0/hash_dji_md5.txt C:\AkuisisiLogicalAndroid\hash_dji
_md5.txt
/storage/emulated/0/hash_dji_md5.txt: 1 file pulled, 0 skipped. 9.2 MB/s (123815 bytes in 0.013s)

C:\Windows\System32>adb pull /storage/emulated/0/hash_dji_sha256.txt C:\AkuisisiLogicalAndroid\hash_
dji_sha256.txt
/storage/emulated/0/hash_dji_sha256.txt: 1 file pulled, 0 skipped. 12.6 MB/s (167847 bytes in 0.013s
)
```

Fig. 8 Retrieving hashing data for original files from android smartphone

All digital evidence in this study was verified using hashing algorithms to ensure data integrity. For UAV acquisitions, both static and dynamic, FTK Imager generated MD5 and SHA1 hashes automatically. For the Android RC-N1 controller, MD5 and SHA256 hashes were calculated manually using a hashing tool to validate extracted files. Using two different hash algorithms per device increases confidence in data integrity. MD5 is fast and sufficient for quick verification, while SHA1 and SHA256 provide higher resistance against collision. Although MD5 has known vulnerabilities, its use here is supported by a secondary hash and tool logging. All forensic tools used in this study are recognized in the digital forensic community and produce reproducible results. The summary of hash methods and admissibility status for each acquisition is shown in Table III.

C. Analysis Stage

The analysis phase was conducted in four stages: first, analyzing the UAV DJI Mini 3 using the static method, followed by the dynamic method. Next, the physical acquisition results from the smartphone were analyzed, and finally, the logical acquisition results from the smartphone were examined. 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.

Next, in the dynamic acquisition method applied to the UAV DJI Mini 3, analysis was conducted using Autopsy software. Based on the analysis results, a total of 64 media files were found, with some files in an active state and others in a deleted state. Additionally, 31 deleted files were identified, consisting of 4 video files with .MP4 extensions, 10 photo files with .JPG extensions, 2 video files with .MOV extensions, 10 files with .jpg extensions, 4 files with .txt extensions, and 1 file with a .swf extension. Furthermore, 63 photo files containing EXIF metadata were found, consisting of 53 files with .JPG extensions and 10 files with .jpg extensions. This EXIF metadata contained geographic information such as latitude, longitude, and altitude of the image captured location. All files had the same creation timestamp, which was August 28, 2024.

This analysis also revealed visual evidence that supports the occurrence of a violation as per the case scenario. One of the most significant pieces of evidence is the presence of a photo taken in a local farmer's plantation, where a farmer is seen at the location. This photo was obtained through EXIF data, enabling the verification of the image's capture location based on the recorded latitude, longitude, and altitude. This finding strengthens the conclusion that the UAV flew beyond the boundary of the designated coal mining area. The visual evidence can be seen in Fig. 9.

After analyzing the EXIF metadata artifacts, which contain coordinate points for each photo, the researcher conducted an analysis by plotting several photo evidence artifacts on the Google Earth website. This was done to mark the locations where the UAV had flown, committing violations, based on the visual evidence obtained from the coordinate points in the EXIF metadata. The physical acquisition using MOBILedit revealed that the UAV was operated using the DJI Fly application (package name dji.go.v5, version 1.13.10, size 534.5 MB), first installed on August 22, 2024, and last used on November 28, 2024, matching the case timeline. In the Photos directory, 1,388 images were discovered, including 51 from August 28. However, GPS coordinates extracted by MOBILedit showed inconsistencies compared to EXIF data obtained from dynamic analysis. In the Videos directory, 1,632 videos were found, 11 of which were related to the incident, with visual evidence of UAV boundary violations. Since no flight logs were initially found, a logical acquisition was performed on the directory /storage/emulated/0/Android/data/dji.go.v5/. This led to the discovery of the subfolder /dji.go.v5/files/FlightRecord/, which contained 19 flight log files in .txt format. Six of these logs corresponded to August 28. After processing through phantomhelp.com, the logs were converted to .kmz files and visualized using Google Earth, showing flight paths consistent with EXIF data and video coordinates. Two flight logs confirmed boundary violations, as shown in Fig. 10.

Fig. 10 shows the Google Earth website used for analysis. Based on the image, the blue points represent the coal mining area, while the red points indicate the area of the residents' plantations, and the yellow points mark the residential area, including the mosque. It was found that the UAV was proven to have flown over the

coal mining border area. Unfortunately, the satellite image on Google has not been updated, so the area still appears as green forest, not yet converted into a coal mining area. This finding strengthens the argument that flight log data is a crucial element in UAV forensics for precisely identifying the route and areas traveled by the UAV, complementing information obtained from media acquisition results.

The geospatial analysis was supported by six flight logs obtained from the DJI Fly application, all conducted on August 28, 2024. These logs were extracted and processed through Airdata.com to identify the UAV's exact trajectory and duration. Specifically, the red markers were derived from Log 4 (recorded at 11:41 AM with a duration of 09m 18s), which indicated a flight over plantation areas, while the yellow markers were derived from Log 6 (recorded at 12:04 PM with a duration of 13m 40s), showing a flight path that extended into residential zones. These two sessions formed the basis of the simulated violation scenario. The chronological data across all six sessions helped validate flight consistency and contributed to the integrity of the forensic analysis.

TABLE III
SUMMARY OF EVIDENCE ADMISSIBILITY BY ACQUISITION METHODS

Acquisition Methods	Source Device	Hash Algorithms Used	Admissibility Status
Static Acquisition	UAV (SD Card)	MD5 and SHA1 (via FTK Imager)	Admissible
Dynamic Acquisition	UAV (Powered On)	MD5 and SHA1 (via FTK Imager)	Admissible
Physical Acquisition	Android Smartphone (RC-N1)	MD5 and SHA256 (via ADB)	Admissible
Logical Acquisition	Android Smartphone (RC-N1)	MD5 and SHA256 (via ADB)	Admissible

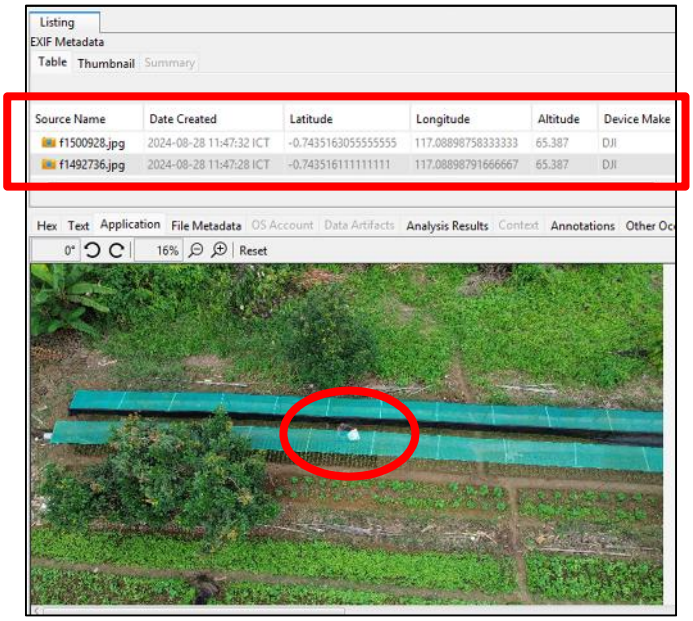

Fig. 9 EXIF metadata UAV DJI Mini 3 dynamic method: a farmer in the garden

Fig. 10 UAV flight path tracks

D. Documenting Stage

The documentation phase is the final stage in the DRF Field Framework, where all investigation findings are systematically organized. This stage presents tables summarizing artifact types, metadata, and digital evidence from both UAV and smartphone controller, using static, dynamic, physical, and logical acquisition methods. Tables IV, V, and VI provide a comprehensive overview of airspace violations found in the simulated case study.

Table IV presents a side-by-side comparison of artifacts extracted from the DJI Mini 3 UAV using static and dynamic acquisition methods. The table highlights differences in artifact types, quantities, and metadata availability, enabling an evaluation of which method yields more comprehensive and relevant evidence for UAV forensic investigations.

Table V presents the results of data acquisition from the Android Smartphone Controller using MOBILedit Forensic Express PRO. The table lists the types of artifacts recovered, the number of files for each category, and key information identified, such as UAV application details, photographs, videos, and GPS metadata. It also highlights evidence relevant to the simulated case study, including mapping activities and indications of boundary violations.

Table VI presents the results of artifact extraction from the Android Smartphone Controller using the Android Debug Bridge (ADB) method. The table outlines the recovered folders, flight logs, and .kmz files, along with their processing and analysis steps. It also notes the correlation between flight log data and GPS coordinates from both UAV EXIF metadata and MOBILedit video analysis, as well as evidence indicating UAV boundary violations.

From a legal perspective, the non-rooted acquisition method offers a significant advantage in maintaining chain-of-custody integrity [38] because the RC-N1 Android controller remains in its original state, reducing the risk of altering system files that could undermine evidentiary value. This approach aligns with Indonesian digital evidence regulations, where altering the original device state can lead to admissibility challenges. In international contexts such as jurisdictions following ISO 27037 [39] or the Daubert criteria, preserving device integrity through non-invasive methods strengthens the credibility of the forensic process and increases the likelihood that evidence will be accepted in court.

TABLE IV
COMPARATIVE ANALYSIS RESULTS OF DJI MINI 3 UAV ARTIFACTS USING STATIC AND DYNAMIC ACQUISITION METHODS

Artifact Types	Static Method	Dynamic Method
Photograph	53 photos (August 28, 2024)	63 photos: .JPG (53), .jpg (10); deleted: 10
Video	11 videos (August 28, 2024)	14 videos: .MP4 (11, including 4 deleted), .mov (2), .swf (1)
Audio	11 (cannot be played)	11 audios (part of videos)
Deleted files	11 photos, 4 videos	31 files: .MP4 (4), .mov (2), .JPG (10), .txt (4), .swf (1)
Plain text	-	4 .txt files
EXIF metadata	-	Present in 63 photos (contains GPS info)
File. log	3 files (unidentifiable)	3 files (same names, also unidentifiable)
Evidence of Violation	Yes. Found in photos/videos showing non-mining areas	Yes – photo of farmer gardening with GPS data confirms flight outside boundary

TABLE V
MOBILEDIT SMARTPHONE ANDROID ANALYSIS RESULTS

Artifact Types	Number of Files	Information
Application	1	DJI Fly (dji.go.v5), version 1.13.10
Photograph	1388	51 photos as of August 28, 2024, relevant to the case study
Video	1632	11 videos from August 28, 2024, containing information on mapping activities and area violations
GPS Coordinates Photos	51	Doesn't match the coordinates of the EXIF UAV Dynamic method
GPS Video Coordinates	11	Only at the starting point, it matches the EXIF UAV dynamic method
Evidence of Violation	Yes	The video and photos show UAV activity outside the boundaries of the mine area, including the compatibility of the video coordinate points with the EXIF data on the UAV

TABLE VI
ADB SMARTPHONE ANDROID ANALYSIS RESULTS

Artifact Types	Number of Files	Information
Folder Target	1	/storage/emulated/0/Android/data/dji.go.v5/files/FlightRecord/
Flight Logs (.txt)	19	There are 6 logs as of 28/08/24
.kmz extraction	6	Processed using Phantomhelp, then analyzed in Google Earth
Location Match	Yes	Flight logs correspond to the coordinate points on the EXIF metadata on the UAV and the coordinate points on the MOBILedit videos
Evidence of Violation	Yes	Flight traces show UAVs crossing clearance limits

IV. CONCLUSION

This study successfully applied the CDFM for DRF Field framework to investigate the DJI Mini 3 UAV and DJI RC-N1 Android Smartphone using static, dynamic, physical, and logical acquisition methods. Dynamic acquisition on the UAV yielded richer artifacts, notably EXIF metadata with spatial data revealing territorial violations. Although flight logs were absent on the UAV, they were retrieved from the Android Smartphone via logical acquisition without rooting, emphasizing the value of understanding application structures. The use of hash verification ensured data integrity. These findings demonstrate effective forensic strategies for UAV-related violations. However, the study is limited by its simulated case design, which may restrict generalization to real-world scenarios, and it has not been tested in an actual legal investigation. Future research is encouraged to automate non-root log retrieval processes, compare forensic outcomes across different UAV brands and models, and validate the methodology in real legal case contexts to further strengthen the applicability and reliability of the findings.

ACKNOWLEDGEMENT

This research was funded by the Ministry of Education, Culture, Research, and Technology, Republic of Indonesia, under the Master Thesis Research Grant number: 052/DirDPPM/70/DPPM/PFRKEMDIKBUDRISTEK/VI/2024.

REFERENCES

[1] D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim, and A. MacDermott, 'Drone Forensics: A Case Study on DJI Phantom 4', in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates: IEEE, Nov. 2019, pp. 1–6. doi: 10.1109/AICCSA47632.2019.9035302.

[2] 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.

[3] N. Y. Pinatik and F. S. Papilaya, 'Pengolahan Foto Udara UAV (Unmanned Aerial Vehicle) Menggunakan Software Agisoft Metashape', *jupel*, vol. 6, no. 1, pp. 1–11, Feb. 2024, doi: 10.32520/jupel.v6i1.2838.

[4] Y. Yu, D. Barthaud, B. A. Price, A. K. Bandara, A. Zisman, and B. Nuseibeh, 'LiveBox: A Self-Adaptive Forensic-Ready Service for Drones', *IEEE Access*, vol. 7, pp. 148401–148412, 2019, doi: 10.1109/ACCESS.2019.2942033.

[5] 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.

[6] 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.

[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] 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.

[9] H. Studiawan, G. Grispos, and K.-K. R. Choo, 'Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed', *Computers & Security*, vol. 132, p. 103340, Sep. 2023, doi: 10.1016/j.cose.2023.103340.

[10] V. Chamola, P. Kotesh, 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.

[11] 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.

[12] T. K. Shashidar, J. Shankara, and R. Shettigar, 'Aerial Insights: The Role of Drone Forensics in Modern Investigations', *Centre for Cybercrime Investigation Training & Research (CCITR)*, 2024, url: https://www.dsci.in/files/content/knowledge-centre/2024/Drone_Forensics_Investigation.pdf.

[13] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," *Computer Networks*, vol. 224, pp. 1–28, Apr. 2023, doi: 10.1016/j.comnet.2023.109626.

[14] 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.

[15] S. E. Prastya, S. P. Cipta, and B. Nugraha, 'Analisis Log Penerbangan Pada Unmaned Aerial Vechile (UAV) Sebagai Barang Bukti Digital', *JTekInfULM*, vol. 5, no. 1, pp. 11–18, Apr. 2020, doi: 10.20527/jtiulm.v5i1.42.

[16] 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.

[17] T. Almehmadi and O. Batarfi, 'Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics', in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia: IEEE, 2019. doi: 10.1109/CAIS.2019.8769520.

[18] S. Lee, H. Seo, and D. Kim, 'Digital Forensic Research for Analyzing Drone Pilot: Focusing on DJI Remote Controller', *Sensors*, vol. 23, no. 21, p. 8934, Nov. 2023, doi: 10.3390/s23218934.

[19] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, 'Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations', *Internet of Things*, vol. 11, p. 100218, Sep. 2020, doi: 10.1016/j.iot.2020.100218.

[20] R. Kurniandi, D. Marlena, and D. Clarissa, 'Analisis Forensik Drone Menggunakan Metode Clark et al. dan Renduchintala et al. (Studi Kasus: DJI Phantom 3 Standard)', *Info Kripto*, vol. 17, no. 2, pp. 75–83, Sep. 2023, doi: 10.56706/ik.v17i2.75.

[21] 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.

[22] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, 'A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field', *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–13, Feb. 2022, doi: 10.1155/2022/8002963.

[23] H. Studiawan, T. Ahmad, B. J. Santoso, A. M. Shiddiqi, and B. A. Pratomo, 'DroneTimeline: Forensic timeline analysis for drones', *SoftwareX*, vol. 20, p. 101255, Dec. 2022, doi: 10.1016/j.softx.2022.101255.

[24] K. Al-Room, F. Iqbal, T. Baker, B. Shah, B. Yankson, A. MacDermott, and P. C. K. Hung, "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. 1–21, 2021, doi: 10.4018/IJDCF.2021010101.

[25] C.-C. Yang, H. Chuang, and D.-Y. Kao, 'Drone Forensic Analysis Using Relational Flight Data: A Case Study of DJI Spark and Mavic Air', *Procedia Computer Science*, vol. 192, pp. 1359–1368, 2021, doi: 10.1016/j.procs.2021.08.139.

[26] J. K. W. Lan and F. K. W. Lee, 'Drone Forensics: A Case Study on DJI Mavic Air 2', in *International Conference on Advanced Communications Technology*, South Korea: IEEE, 2021. doi: 10.23919/ICACT51234.2021.9370578.

[27] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, 'A Comparative UAV Forensic Analysis: Static and Live Digital Evidence Traceability Challenges', *Drones*, vol. 5, no. 2, p. 42, May 2021, doi: 10.3390/drones5020042.

[28] F. E. Salamh, M. M. Mirza, and U. Karabiyik, 'UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies', *Electronics*, vol. 10, no. 6, p. 733, Mar. 2021, doi: 10.3390/electronics10060733.

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

[30] Z. Zhao, Y. Wang, and G. Liao, 'Digital Forensic Research for Analyzing Drone and Mobile Device: Focusing on DJI Mavic 2 Pro', *Drones*, vol. 8, no. 7, p. 281, Jun. 2024, doi: 10.3390/drones8070281.

[31] A. Taylor, 'A Digital Forensics Case Study of the DJI Mini 3 Pro and DJI RC' *arXiv*, pp. 1–20, Sep. 2023, doi: 10.48550/arXiv.2309.10487.

[32] M. Y. Halim and A. Luthfi, 'Digital Forensic Analysis of UAV Flight Data Using Static and Dynamic Methods in Coal Mining Area', *Journal of Information Systems and Informatics*, vol. 7, no. 2, pp. 1042–1060, Jun. 2025, doi: 10.51519/journalisi.v7i2.1061.

[33] 'Permenhub No. 63 Tahun 2021', Database Peraturan | JDIH BPK. Accessed: Apr. 30, 2025. [Online]. Available:

http://peraturan.bpk.go.id/Details/284709/permenhub-no-63-tahun-2021

[34] K. Dabade, P. Dhalkar, S. Bandgar, and A. Shende, 'Forensic Tool for Android Mobile Device', vol. 09, no. 07, 2022, [Online]. Available: https://www.irjet.net/archives/V9/i7/IRJET-V9I7384.pdf

[35] A. Sameh, A. Chiziba, and V. D. Pronichev, 'Examining the File System of Android Devices: Implications for Digital Forensics', *IJNHS*, vol. 10–1, no. 97, pp. 228–232, 2024, doi: 10.24412/2500-1000-2024-10-1-228-232.

[36] R. Prathiba and D. S. Ganesh, 'ADB Debugging – Security Risks and Investigations', *IJIRSET*, vol. 14, no. 4, pp. 9343–9347, 2025, doi: 10.15680/IJIRSET.2025.1404477.

[37] G. B. Akintola, 'Evaluating the Security Vulnerabilities of the Selected Mobile Forensic Applications', *ISROSET*, vol. 11, no. 2, pp. 16–35, 2025, url: https://isroset.org/pub_paper/IJSRMS/3-ISROSET-IJSRMS-10261.pdf.

[38] N. Yalçın and T. Yıldırım, 'Logical Image Acquisition and Analysis of Android Smartphones', *Journal of Computer and Communications*, vol. 12, no. 4, pp. 139–152, Apr. 2024, doi: 10.4236/jcc.2024.124011.

[39] A. Faizal and A. Luthfi, 'Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis', *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 701–718, Jun. 2024, doi: 10.51519/journalisi.v6i2.717.