Static and Dynamic Acquisition Methods Show Distinct Performance in Drone Data Collection

Rio Fiorido Panggabean[1*], Niken Cahyani[1], Fazmah Arif Yulianto[1]

[1]School of Computing, Telkom University, Bandung, Indonesia

[*]Coressponding Author Email : riofiorido@student.telkomuniversity.ac.id

Abstract. General Background: Digital forensic acquisition on Unmanned Aerial Vehicles (UAVs) is essential to ensure the integrity and admissibility of digital evidence in forensic investigations. Specific Background: Two primary acquisition approaches, namely dynamic physical acquisition and static physical acquisition, are commonly applied to extract data from drone devices such as the DJI Mini 3. Knowledge Gap: However, limited comparative analysis exists regarding the performance and data consistency of these two acquisition methods under standardized forensic procedures. Aims: This study aims to compare dynamic and static physical acquisition methods for drone data collection based on forensic parameters and standards. Results: Using experimental scenarios guided by SNI ISO/IEC 27037:2014, data were analyzed with Autopsy 4.22.0, showing that both methods produced identical MD5 and SHA-1 hash values and extracted the same number of artifacts, including media files, deleted files, system logs, and unallocated sectors. Dynamic acquisition demonstrated shorter acquisition time, while both methods maintained consistent metadata such as EXIF data, video parameters, and system logs, confirming equivalent capabilities in preserving data structure and forensic value. Novelty: This study proposes an integrated acquisition process combining dynamic and static physical methods for UAV forensic investigations. Implications: The findings support the complementary use of both acquisition approaches to optimize digital forensic procedures on drones according to operational field conditions while maintaining evidence integrity.

Keywords: UAV digital forensics; Physical acquisition methods; Drone data collection; Forensic data integrity; DJI Mini 3

1 Introduction

The use of Unmanned Aerial Vehicles (UAVs), or drones, has grown rapidly across various sectors such as aerial photography, infrastructure monitoring, precision agriculture, and environmental observation[1], [2]. Conversely, the misuse of drones for illicit purposes—such as smuggling, unauthorized surveillance, and unauthorized entry into restricted zones—is on the rise [3], [4]. Consequently, drones have become an important source of

R. Lomotey et al. (eds.), *Proceedings of the 1st International Conference on Communication and Digital Multimedia 2025 (ICCDM 2025)*, Advances in Social Science, Education and Humanities Research 1020,
https://doi.org/10.2991/978-2-38476-589-8_39

digital evidence, highlighting the critical role of forensic drone investigations in supporting public safety and law enforcement efforts[5]. UAVs generate operational data such as flight records, sensor data, images, and system logs[6], all of which must be reliably acquired in accordance with forensic validity principles to ensure admissibility in court. Most recent drone models are notably difficult to analyze due to enhanced security mechanisms[7], [8].

In digital forensics, the acquisition process for potential evidence is regulated by ISO/IEC 27037:2014, which differentiates acquisition methods based on device status: dynamic acquisition when the device is powered on, and static acquisition when the device is powered off[9]. In the UAV context, these approaches correspond to dynamic physical acquisition (the device remains active during imaging) and static physical acquisition (the storage medium is removed and acquired offline). The selection of an acquisition method depends on several factors, including examiner expertise, device condition at the time of seizure, the types of Artifacts sought, and the objectives of the investigation[10]. Although both approaches are widely used, no technical guidelines currently exist that explain how device conditions at the moment of acquisition affect Artifact consistency and data integrity in modern UAV platforms. Several prior studies have examined aspects of data acquisition on drones. Nayak[11] proposed disk imaging techniques to assist forensic investigators in extracting metadata and historical data from UAV storage media. Meanwhile, Halim[12] applied both physical dynamic acquisition and physical static acquisition, showing that physical dynamic acquisition yields a greater number of digital Artifacts compared to physical static acquisition. This indicates inconsistencies in the quantity and types of Artifacts obtained through dynamic versus static physical acquisition. Such discrepancies not only reflect differences in acquisition techniques but also suggest that the characteristics of modern UAVs now equipped with encrypted file systems, more complex flight controllers, and firmware-based data protection mechanisms[13] may significantly influence the acquisition process. This difference in findings indicates a research gap for developing a physical acquisition process model that can explain the equivalence of artifacts on modern UAVs in maintaining data integrity and consistency throughout the acquisition process.

Therefore, this study aims to conduct an empirical assessment by comparing the digital Artifacts produced through dynamic physical acquisition and static physical acquisition on UAVs, evaluating the consistency and integrity of the data obtained from each method, and formulating technical recommendations for selecting the most appropriate acquisition approach to support drone forensic investigations.

2 Methodology

This study adopts an empirical methodology with a comparative experimental to assess the outcomes of static physical acquisition and dynamic physical acquisition on drone devices. The procedures are developed with reference to the forensic acquisition principles specified in SNI ISO/IEC 27037:2014[9], namely preserving integrity, ensuring repeatability, and minimizing alterations to digital evidence.

2.1 Preparation

Preparation. The experiment was conducted in a controlled environment using devices with identical configurations and datasets, and both acquisition methods were applied to identical storage media to ensure comparative validity. Table 1 presents the hardware specifications and forensic software utilized in this study. The DJI Mini 3 drone was used as a research object, as DJI is one of the world's leading drone manufacturers with a market share of around 76% in the global drone industry[14]. Previous studies have shown that unformatted memory cards may retain Artifacts from prior flights, thereby posing a risk of contaminating experimental results[15]. The dataset was generated through a controlled flight scenario, as illustrated in Figure 1, involving the capture of fifteen images and five video recordings. Subsequently, five image files and three video files were deleted.

Table 1. The hardware specifications and forensic software utilized.

Name	Version	Description
Computer	Windows 11, 12th Core(TM) i7	Forensic workstation
Drone DJI Mini 3	firmware V01.00.0500	Drone evidence
MicroSd	30,437MB, SanDisk V30 A1	Drone data storage media
Card Reader	-	Memory card reader
NVMeSSD	245 GB	Image file storage
Usb-C Cable	-	Drone-workstation connector
FTK Imager [16]	4.7.1.2	Digital image acquisition
Autopsy[17]	4.22.0	Forensic data analysis tools
Write blocker	all_windows	Data writing to evidence media

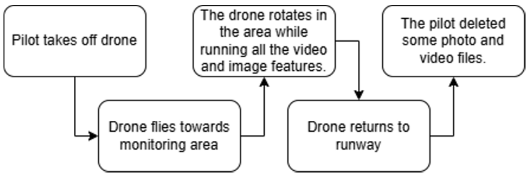

Fig. 1. Flight scenario.

2.2 Dynamic Physical Acquisition and Static Acquisition

Dynamic Physical Acquisition. In the power-on state, the drone is connected to a forensic workstation via a USB-C cable equipped with an active write blocker. The acquisition process was performed using FTK Imager, which generated a digital image in .dd format. Upon completion of the acquisition, hash documentation of the acquired image was recorded following the dynamic physical acquisition method. The step-by-step procedure of the dynamic physical acquisition is illustrated in Figure 2, and Figure 4 shows the dynamic physical acquisition process.

Static Physical Acquisition. When the device is powered off, the external storage is extracted and attached to the forensic workstation using a card reader. Prior to data access, the write blocker was activated to ensure the protection of the original evidence. The acquisition process was performed using FTK Imager, producing a .dd-format disk image. Subsequently, a hash documentation of the acquired image was recorded following the static physical acquisition procedure. The step-by-step procedure of dynamic static acquisition is illustrated in Figure 3, and Figure 4 shows the dynamic physical acquisition process.

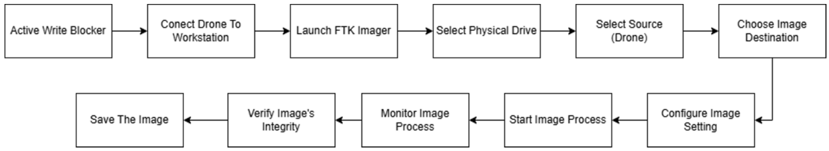

Fig 2. Proposed flowchart for dynamic physical acquisition.

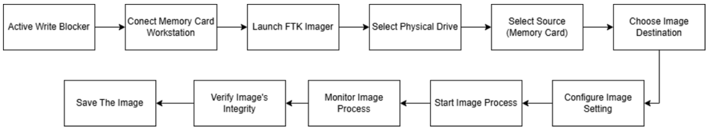

Fig 3. Proposed flowchart for static physical acquisition.

2.3 Analysis

Analysis. The analysis stage was carried out on the acquired digital images from both methods using Autopsy 4.22.0 as the primary forensic analysis platform. Autopsy was selected due to its comprehensive features for file system examination, Artifact reconstruction, and structured metadata analysis, making it widely adopted in modern digital forensic practice[17]. At this stage, the images obtained through dynamic physical acquisition and static physical acquisition were analyzed in parallel. The analysis encompassed several key parameters: Verification of data integrity through the comparison of hash values (MD5 and SHA-1) to ensure that the acquisition process did not alter the contents of the images; Measurement of acquisition time as an indicator of each method's efficiency; Calculation and comparison of the number of digital Artifacts successfully extracted, including image files, video files, deleted files, and log files; Examination of file metadata; and Analysis of the proportion of allocated and unallocated sectors contained within the images to assess the coverage of the storage media obtained by each method. This approach provides a comprehensive evaluation of both acquisition methods in terms of their ability to preserve the integrity, completeness, and forensic value of drone data.

3 Result

This section reports the results of the data analysis for both acquisition methods, accompanied by a systematic comparison across all evaluation parameters. The results are organized to underscore both differences and commonalities in terms of data integrity, acquisition performance, artifact extraction, metadata completeness, and storage coverage.

3.1 Time Acquisition and Data Integrity

Time Acquisition. The acquisition time revealed a clear difference between the two methods. The dynamic physical acquisition method completed the process in 19 minutes and 42 seconds, whereas the static physical acquisition method required 35 minutes and 07 seconds. Thus, the dynamic method was recorded to be nearly twice as fast as the static method. This difference in duration indicates that dynamic physical acquisition is more time-efficient.

Data Integrity. Integrity verification of the acquisition results was performed by comparing the MD5 and SHA-1 hash values of the disk images generated through dynamic physical acquisition and static physical acquisition. The analysis showed that both images produced identical hash values, indicating that no alterations occurred during the acquisition process. The hash results are presented in Table 2.

Table 2. A comparison of hash values.

Metode	MD5	SHA 1
Dynamic	147c5cf5bc0b5b9812bd542e2a05b355	746404534bca4f3b587e09be1e0a974bf884b727
Static	147c5cf5bc0b5b9812bd542e2a05b355	746404534bca4f3b587e09be1e0a974bf884b727

3.2 Digital Artifact

Digital Artifact. The extraction and analysis of the disk images using Autopsy 4.22 showed that both acquisition methods produced equivalent results in terms of data completeness and the types of data recovered. Each method successfully extracted a total of twenty media files (comprising three MP4 video files, ten JPEG images, and seven deleted files), together with three system log files (linux_log, camera_log, and fc_log) and twenty-nine unallocated files. This equivalence indicates that static and dynamic physical acquisition offer comparable capabilities for data acquisition. A comparative summary of the extraction results for both methods is provided in Table 3.

Table 3. Digital image extraction results from both methods.

	Dynamic	Static
Photo	10 files	10 files
Video	3 files	3 files
Deleted Photo	5 files	5 files
Deleted Video	2 files	2 files
File log	3 files	3 files

A comparative analysis of the artifacts process is shown in Figure 4, and Figure 5 shows that both the static physical acquisition and dynamic physical acquisition methods produce consistent metadata and file structures. For the video files (.mp4), both methods preserve the same metadata; the metadata contained in the video files is present in Table 4.

Table 4. Metadata contained in the video files.

Name	Description
F/xx	Aperture or lens opening, indicating how much light enters the sensor.
SS xx	Shutter speed, expressed in units of 1/x seconds.
ISO xx	Sensor sensitivity to light; the higher the value, the brighter the image, but also the more noise.
EV xx	Exposure Value, indicating exposure compensation. Negative values mean the image is slightly darker than the automatic exposure standard.
DZOOM xx	Digital Zoom; in this case digital zoom is not used (1.000 means no magnification).
GPS (lat, long)	GPS coordinates of the drone's position.
D xx m	Horizontal distance between the drone and the take-off point (distance).
H xx m	Height of the drone above the take-off point.
H.S xx m/s	Horizontal Speed, i.e., the drone's horizontal velocity.
V.S xx /s	Vertical Speed, the drone's vertical velocity (negative means descending, positive means ascending, 0.00 means stationary along the vertical axis).

A similar outcome is observed in the extracted image files. The EXIF metadata, including latitude, longitude, altitude, serial number, camera model, software version, and date created, remains intact and consistent across both acquisition methods. This consistency is likewise found in the previously deleted image files, where all remaining metadata attributes exhibit alignment between the two acquired images. These findings confirm that both dynamic physical acquisition and static physical acquisition are capable of fully preserving forensic metadata and data structures, yielding results with equivalent characteristics.

Examination of the system artifacts revealed that three log files, linux_log, camera_log, and fc_log, were successfully captured. These files exhibited consistent names, structural formats, and metadata properties, such as timestamps, file sizes, and log sequence patterns. This uniformity indicates that both methods consistently captured system artifacts, without altering their content or metadata characteristics, thus supporting the validity and reproducibility of the findings.

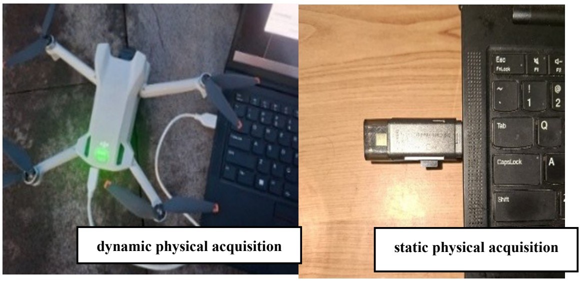

Fig 4. Process dynamic physical acquisition and static physical acquisition

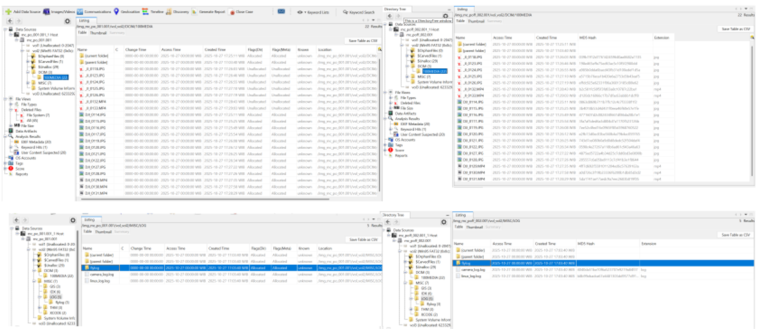

Fig 5. A comparative analysis of the digital Artifacts.

4 Conclusion and Future Work

Conclusion. In this paper, we propose a process for conducting both dynamic and static physical acquisition on drones and perform an empirical evaluation of two forensic acquisition approaches for UAVs: dynamic physical acquisition and static physical acquisition using the DJI Mini 3 platform. The experimental results show that both methods produce digital images with identical MD5 and SHA-1 hash values, confirming that the acquisition processes do not alter the data. Both methods also successfully extract the same categories of artifacts, including media files, deleted files, system logs (linux_log, camera_log, and fc_log), and unallocated sectors, indicating that they possess equivalent capabilities in data acquisition from drone storage. The consistency observed in EXIF metadata, GPS information, timestamps, and video parameters further reinforces the conclusion that both methods can preserve the data structure and overall forensic value. Nevertheless, the study identifies a significant difference in acquisition time: the dynamic method requires only 19 minutes and 42 seconds, whereas the static method takes 35 minutes and 07 seconds. Conversely, the static method remains particularly suitable for controlled laboratory environments, where device stability is prioritized and the risk of data alteration must be minimized, since no operating system processes or services are active. Overall, the two approaches are complementary and can be incorporated into a UAV forensic acquisition framework that supports digital investigation practices in line with the operational conditions encountered in the field..

Future Work. Future research should evaluate a broader range of UAV models and firmware versions to determine whether the findings observed in the DJI Mini 3 are consistent across devices with different architectures and system designs. Cross-device results of this kind could then serve as a foundation for developing a standardized UAV forensic framework.

References

[1] "statica." Accessed: Aug. 31, 2025. [Online]. Available: https://www.statista.com/outlook/cmo/consumer-electronics/drones/worldwide
[2] A. Renduchintala, F. Jahan, R. Khanna, and A. Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," *Digit. Investig.*, vol. 30, pp. 52–72, Sep. 2019, doi: 10.1016/j.diin.2019.07.002.
[3] "Detik.com." Accessed: Aug. 31, 2025. [Online]. Available: https://news.detik.com/berita/d-7959301/drone-mencurigakan-jatuhkan-bungkusan-ke-lapas-jelekong-ternyata-berisi-sabu
[4] "Detik semarang." Accessed: Aug. 31, 2025. [Online]. Available: https://news.detik.com/berita-jawa-tengah/d-5547252/bahaya-banget-ada-drone-terlihat-di-area-udara-bandara-semarang
[5] I. Husnjak, S., Forenbacher, I., Peraković, D., & Cvitić, "UAV forensics: DJI Mavic air noninvasive data extraction and analysis.," in *UAV forensics: DJI Mavic air noninvasive data extraction and analysis.*, 2021. doi: https://doi.org/10.1007/978-3-030-67241-6_10.
[6] R. R. Nair, H. Gayakwad, D. K. Mahida, and B. Podiya, "Drone Forensics part6," no. Singh 2015, pp. 99–123, 2021, doi: 10.1201/9781003386926-6.
[7] 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 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 66–71. doi: 10.1109/ICICS49469.2020.239530.
[8] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone open source parser) your drone: Forensic analysis of the DJI phantom III," in *DFRWS 2017 USA - Proceedings of the 17th Annual DFRWS USA*, Digital Forensic Research Workshop, 2017, pp. S3–S14. doi: 10.1016/j.diin.2017.06.013.
[9] Badan Standarisasi Nasional, "SNI ISO-IEC 27037-2014 tentang Teknologi Informasi - Teknik Keamanan - Pedoman Identifikasi, pengumpulan, Akuisisi, dan Preservasi Bukti Digital," vol.

2014, no. Konfirmasi, 2014, [Online]. Available: https://pesta.bsn.go.id/produk/detail/9830-sniisoiec270372014
[10]"Scientific Working Group on Digital Evidence SWGDE Best Practices for Drone Forensics." [Online]. Available: www.swgde.org
[11]S. C. Nayak, B. K. Samanthula, and V. Tiwari, "Investigating Drone Data Recovery beyond the Obvious Using Digital Forensics," in *2023 IEEE 14th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 254–260. doi: 10.1109/UEMCON59035.2023.10315995.
[12]M. Y. Halim, "Analisis Forensik Digital Non-Rooted Pada Data Penerbangan Unmanned Aerial Vechile (UAV) dan Controller Berbasis Android Untuk Pengungkapan Bukti Digital," 2025, [Online]. Available: https://doi.org/10.30595/juita.v13i3.26598
[13]Interpol, Framework for Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners. Singapore: INTERPOL Innovation Centre, 2020.
[14]Statista, "Global market share of drone manufacturers, 2021," 2021. [Online]. Available: https://www.statista.com/
[15]G. Thornton and P. Bagheri Zadeh, "An investigation into Unmanned Aerial System (UAS) forensics: Data extraction & analysis," *Forensic Sci. Int. Digit. Investig.*, vol. 41, Jun. 2022, doi: 10.1016/j.fsidi.2022.301379.
[16]Exterro, "FTK Imager: Forensic Data Imaging and Preview Tool," 2023. [Online]. Available: https://www.exterro.com/ftk-imager
[17]T. S. K. Labs, "Autopsy Digital Forensics Platform: User Documentation," 2025. [Online]. Available: https://www.autopsy.com