# Breaking Down Drone Forensics: A Framework for Analyzing UAV Evidence

MALAVATH NITHIN KUMAR
*Parul University*

***Abstract*— The rapid proliferation of Unmanned Aerial Vehicles (UAVs), commonly known as drones, has revolutionized various sectors, including military, medical, and agricultural applications. However, their increasing accessibility and sophistication have raised significant security concerns, particularly regarding their potential misuse in criminal activities. This paper presents a comprehensive examination of drone forensics, addressing the urgent need for effective investigative frameworks to analyze drone-related crimes. We propose a robust digital forensic methodology that encompasses hardware and software analysis, focusing on the extraction and examination of critical data from various drone models, including DJI Phantom 4 and Yuneec Typhoon H. Our research identifies the challenges posed by enhanced security features in modern drones and emphasizes the necessity for novel forensic tools and processes. We introduce the Comprehensive Collection and Analysis Forensic Model (CCAFM), which outlines a systematic approach to drone evidence collection, preservation, and analysis. The model integrates machine learning techniques to facilitate the classification of drone data, enhancing the accuracy of forensic investigations. Furthermore, we explore the implications of digital twin technology in improving the efficiency of drone accident investigations. By leveraging simulation environments, our approach aims to advance the understanding of drone behavior in various scenarios, thereby aiding in the identification of potential criminal activities. Telemetry***

***Index Terms- Flight logs, Geolocation, Data extraction, Firmware analysis, Radio frequencies, Payload, Communication protocols, Digital forensics, Signal interception.***

## I. INTRODUCTION

1) Background:
Drones have become ubiquitous due to their affordability and versatility. While they serve beneficial purposes, their misuse poses significant security threats.

Need for Forensic Investigation: The necessity for a comprehensive forensic investigation framework is underscored by the growing incidence of drone-related crimes.

2. Challenges in Drone Forensics
Rapid Technological Advancements: The swift evolution of drone technology complicates forensic investigations.

Data Security: Enhanced security features in newer drone models make data extraction challenging.

Lack of Standardized Protocols: There is an absence of uniform guidelines for conducting drone forensic investigations.

3. Methodologies in Drone Forensics
Data Collection:
Examination of four hobbyist drone models (DJI Mavic 2 Pro, DJI Mavic Air, DJI Spark, DJI Phantom 4) to assess data extraction capabilities.
Emphasis on both hardware/physical and digital forensics.
Digital Forensic Applications:
Development of a GUI-based application using JavaFX for extracting and analyzing onboard flight information.
Implementation of file converters for 3D flight trajectory
visualization.
4. Proposed Frameworks
Comprehensive Collection and Analysis Forensic Model (CCAFM):
Processes:
Acquisition and Preservation: Collecting and safeguarding digital evidence.
Reconstruction and Analysis: Analyzing flight data and reconstructing events.
Post-Investigation Process: Documenting findings and sharing knowledge among practitioners.

Conceptual Drone Forensic Framework (CDFF):
A structured approach for identifying, capturing, preserving, analyzing, and documenting UAV incidents.
Stages include preparation, data collection, analysis, and documentation.

5. Machine Learning in Drone Forensics
Application of AI Techniques: Leveraging machine learning to classify drone data and detect anomalies.
Potential for Improved Investigations: Properly trained models can enhance the accuracy of drone data assessments in forensic contexts.

## II. LITERATURE REVIEW

The increasing prevalence of Unmanned Aerial Vehicles (UAVs), commonly known as drones, has led to significant advancements across various sectors, including military, agriculture, healthcare, and surveillance. However, the dual nature of drones—serving beneficial purposes while also being susceptible to misuse in criminal activities—necessitates the development of a robust framework for drone forensics. This literature review synthesizes current research, identifies challenges, and evaluates methodologies and frameworks in the field of drone forensics.

Group discussion:

The increasing prevalence of drones, or unmanned aerial vehicles (UAVs), has sparked significant interest and concern across various sectors, particularly in law enforcement and digital forensics. While drones offer numerous benefits, such as enhanced surveillance capabilities, environmental monitoring, and efficient delivery systems, their misuse in criminal activities poses serious threats to security and public safety. Recent conflicts have highlighted the potential for drones to be weaponized, underscoring the urgency for robust forensic methodologies to investigate drone-related crimes effectively.

## CONCLUSION

The rapid proliferation of Unmanned Aerial Vehicles (UAVs), or drones, has revolutionized numerous fields, providing valuable applications in areas such as surveillance, delivery, and environmental monitoring. However, this technological advancement has also introduced significant security challenges, particularly concerning their potential misuse in criminal activities. Consequently, there is an urgent need for comprehensive forensic frameworks tailored to address the unique complexities of drone-related incidents.

## REFERENCES

[1] Sharma, S., Arora, A., & Saraswat, D. (2018). "A survey on Unmanned Aerial Vehicle forensics." Journal of Information Security and Applications, 43, 88-101

[2] Grover, J., & Ashokkumar, S. (2020). "Forensic analysis of DJI drone data logs." Digital Investigation, 32, 200906.

[3] Quick, D., & Choo, K. K. R. (2018). "Digital forensic challenges and future trends for the UAV ecosystem." Computers & Security, 85, 165-183.

[4] Choudhary, R., Kundu, S., & Prasad, M. (2020). "UAV forensics: A detailed analysis of data acquisition and forensic tools." Journal of Information Security, 11, 61-71.

[5] Shakhatreh, H., Sawalmeh, A., Al-Fuqaha, A., et al. (2019). "Unmanned Aerial Vehicles (UAVs): A survey on civil applications and key research challenges." IEEE Access, 7, 48572-48634.

[6] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). "Deep learning for IoT big data and streaming analytics: A survey." IEEE Communications Surveys & Tutorials, 20(4), 2923-2960.

[7] Khan, L. Z., Salahuddin, M. A., & Khan, S. (2021). "Leveraging machine learning for digital forensics." Journal of Forensic Sciences, 66(3), 1129-1137.

[8] Zhang, Y., Zhang, W., & Kang, X. (2022). "Artificial Intelligence for UAV crime investigations: Challenges and opportunities." Applied Intelligence, 52(4), 3121-3138.

[9] Bojarski, M., et al. (2020). "Digital twins in UAV forensic investigations: A framework for drone

accident analysis." IEEE Access, 8, 196894-196907.

[10] Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2021). "Digital forensic investigations in UAVs: Challenges and approaches." Forensic Science International: Digital Investigation, 37, 301119.