Korean Nuclear Society Spring Meeting, 2025

Enhancing Nuclear Power Plant Security: Logical and Physical Imaging Techniques for Selective Digital Evidence Acquisition in Custom Drone Forensics

Juhyung Song, Sehoon Lee, Seongyeol Oh, Yonggu Lee, Seongoh Seo, Inhye Hahm, Taewoo Tak, Youngjun Lee
Korea Atomic Energy Research Institute
Corresponding author : jhsong@kaeri.re.kr

Introduction

Recently, unauthorized drone incursions around critical national facilities such as nuclear power plants (NPPs) have been on the rise, exacerbating security and safety concerns. To effectively analyze and respond to these drone threats, employing drone forensics to collect and analyze digital evidence is essential. Existing research has predominantly focused on commercial drones, leaving digital evidence collection methods for custom drones insufficiently standardized. Therefore, this study proposes a systematic methodology for selectively collecting digital evidence from custom drones. Additionally, it presents key considerations and implementation strategies in source code development to facilitate effective data acquisition. Specifically, the main contributions of this study are summarized as follows:

- Establishes a forensic methodology for custom-built drones, addressing the lack of standardized digital evidence collection techniques.
- Identifies the limitations of both logical imaging (e.g., PX4, ArduPilot) and physical imaging (e.g., Betaflight), and proposes optimized forensic approaches.
- Implements Burst Mode for efficient data acquisition and resolves challenges related to Sequence ID management.
- Proposes a systematic method for retrieving drone identification data (e.g., UUID) for forensic analysis.
- Provides key implementation strategies for forensic software development across various drone firmware platforms.

By integrating these approaches, this study aims to enhance the overall effectiveness and reliability of drone forensics, particularly in the context of custom-built drones of high-security environments.

Related works

In the field of digital forensics, methodologies for collecting evidence have traditionally centered on networks, servers, and mobile devices. International standards such as ISO/IEC 27037 prescribe procedures for identifying and collecting digital evidence in ways that guarantee its reliability and integrity. However, drone forensics presents unique characteristics distinct from conventional digital devices, and with the increasing threats posed by drones near critical national facilities—such as NPPs—new forensic approaches have become necessary.

- Existing studies include forensic analyses of PX4 and ArduPilot drones, with a primary focus on flight logs, communication signal analysis, and video data recovery. For instance, a study on PX4-based drones introduced methods for extracting mission logs and parameter data using the MAVSDK API. However, research on optimizing data downloads for rapid collection remains limited, and there has been limited analysis of the challenges associated with Burst Mode utilization and Sequence ID management.

Experimental Platforms and Environments

- In this study, we selected three representative drone firmware—ArduPilot, BetaFlight, and PX4—that are highly likely to be used for drone threats against NPPs. The ArduPilot and PX4 used in the experiments are based on the Pixhawk-project FMUv5 platform and are powered by the STM32F765 main processor (32-bit Arm Cortex-M7, 216MHz, 2MB memory, 512KB RAM). The operating systems for these two firmware are ChibiOS and NuttxOS, respectively, with the latest firmware (v4.5.7) installed. Similarly, BetaFlight utilizes the BETAFPVF405 platform, which employs the STM32F405 main processor (Arm Cortex-M4 32-bit MCU+FPU, 210 DMIPS, up to 1MB Flash/192+4KB RAM) and runs the latest firmware (v4.5.1).
- Although all three firmware use a MAVLink-based communication protocol, the process of developing source code for selectively collecting digital evidence from actual custom drones varies depending on the developer. For example, some developers use high-level libraries (e.g., MAVSDK), while others need to directly process raw MAVLink messages. These differences introduce challenges in parsing communication message and accessing data, further complicating the reliability of digital evidence. Moreover, each firmware exhibits distinct file system structures and data access methods. Therefore, this study conducted experiments based on the latest versions of drone firmware after thoroughly analyzing the hardware and software environments. This approach systematically presents methods for the selective collection of digital evidence tailored to custom drones, along with corresponding source code development strategies.

Development of Logical and Physical Imaging Tech.

- This study develops logical imaging and physical imaging techniques for drone forensics and compares their implementation across different firmware platforms. In drone forensic investigations, acquiring the unique identification information of a drone, such as MCU ID, UID, and Serial Number, is crucial as it serves as vital evidence. The experiments confirmed that identification can be performed using various methods, such as retrieving information via MAVLink, utilizing MAVSDK API for PX4-based drones, using MSP commands for BetaFlight drones, and analyzing logs for embedded identification details.
- To implement logical and physical imaging techniques, differences in file system access methods across various drone firmware platforms were considered. For ArduPilot and PX4 (Logical Imaging), the MAVFTP protocol was used to browse file directories and selectively download files. Recursive retrieval of files within designated directories was applied, optimizing transfer speeds using Burst Mode. BetaFlight (Physical Imaging) was configured to operate in USB Mass Storage Mode [11], enabling full system imaging. Bulk copying of data from the physical storage device to a local system was performed; however, some newer BetaFlight drones may not support Mass Storage Mode.

Results and Limitations

- Experimental results confirmed that physical imaging was feasible for BetaFlight drones, whereas ArduPilot and PX4 were limited to logical imaging. Additionally, certain dynamically generated directories, such as /bin, could not be accessed during imaging. These findings highlight that file system access methods differ among drone firmware platforms, and logical imaging may have limitations in accessing specific directories. Therefore, it is necessary to reassess data acquisition methods for each firmware type and refine selective evidence collection techniques.
- This study determined that the most effective approach is to first acquire drone identification information and then proceed with either logical imaging (PX4/ArduPilot) or physical imaging (BetaFlight). Additionally, Burst Mode was implemented to enhance download speeds; however, Sequence ID management posed a significant challenge. To address this issue, a data management mechanism ensuring response packet integrity was applied, thereby minimizing packet loss and enhancing the reliability of data acquisition.

Conclusions and Future Work

This study presents a forensic methodology for extracting digital evidence from custom-built drones, comparing data retrieval approaches between logical and physical imaging techniques. The experiments provide insights into firmware-specific data acquisition constraints and help refine the forensic collection process to enhance efficiency.

Future research will focus on the following areas:

- Automated Drone Identification System: Developing an automated system that detects drone models in real time and dynamically selects the most efficient forensic imaging approach.
- Expansion of Firmware Compatibility: Extending forensic capabilities beyond ArduPilot, PX4, and BetaFlight to support a broader range of drone platforms.
- Optimization of Burst Mode and Sequence ID Management: Improving the efficiency of Burst Mode data transfers and addressing synchronization challenges in Sequence ID management to enhance download stability.
- Advanced Data Integrity Verification and Forensic Reliability: Implementing checksum validation, cryptographic integrity checks, and redundant storage mechanisms to ensure the forensic reliability and admissibility of collected data.
- Integration with Threat Intelligence Frameworks: Linking drone forensic data with cybersecurity threat intelligence platforms to analyze attack patterns and improve security response strategies.
- AI-Driven Forensic Automation: Developing AI models for automated log analysis, flight data interpretation, and anomaly detection to expedite forensic investigations and enhance analytical precision
- Standardization and Regulatory Compliance: Contributing to the establishment of standardized forensic procedures and ensuring compliance with international and national digital evidence regulations.

By pursuing these research directions, advancements in drone forensics will enhance the security of critical infrastructure and improve forensic capabilities against emerging drone-based threats.

REFERENCES

[1] Sentrycs, "Act Now to Protect Critical Infrastructure Against Drones," 2023, [online] Available: https://sentrycs.com/wp-content/uploads/2023/09/White-paper-Act-Now-to-Protect-Critical-Infrastructure-Against-Drones_FINAL.pdf /
[2] PX4 Autopilot: Open-Source Autopilot for Drones, 2025, [online] Available: https://px4.io/software/software-overview/.
[3]Ardupilot: Versatile, Trusted, Open, 2025, [online] Available: https://ardupilot.org/ardupilot/.
[4] Betaflight: Pushing the Limits of UAV Performance, 2025, [online] Available: https://betaflight.com
[5] Mavlink: File Transfer Protocol(FTP), 2025, [online] Available: https://mavlink.io/en/services/ftp.html.
[6] SO, ISO/IEC 27037:2012 - Information technology, 2012, [online] Available: https://www.iso.org/standard/44381.html.
[7] Y. Yoo and J. Cho, "Data extraction and analysis tool for drones based on PX4 Autopilot," Korean Institute of Information Scientists and Engineers, 2022.
[8] Y. Baek et al., "Study on Drone Forensic Methodology Using Open-Source-Based Live Forensic Tools for Drones," Korea Institute of Information Security & Cryptography, 2023.
[9] C. Lee et al., "Study on Custom Drone Data Extraction Method Using MAVLink," Korea Institute of Information Security & Cryptography, 2024.
[10] MAVSDK: a collection of libraries to interface with MAVLink, 2025, [online] Available: https://mavsdk.mavlink-.io/main/en/index.html.
[11] Betaflight: Mass Storage Device Support, 2025. [online] Available: https://betaflight.com/docs/wiki/guides/current-/mass-storage-device-support.

Acknowlegment
This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(Korean National Police Agency) (No. 2021M3C1C4039580)