January 2026

Drone Data Collection and Analysis Tool Specification, Test Assertions, and Test Cases

Draft 2 of Version 1.0

Abstract

This specification defines the requirements, test assertions, and test cases for drone forensic tools designed to identify, extract, and report evidentially valuable data from drones. The requirements serve as a structured list of mandatory and optional functional objectives that a tool must satisfy. Each requirement is further specified into a test assertion to ensure verifiability. Test assertions are then implemented as test cases—each consisting of input data, procedures, and expected results—which are executed during the actual verification process.

The requirements systematize the essential capabilities that a tool must provide and comply with, forming the foundation from which corresponding test assertions are derived. Each test assertion is executed through one or more test cases, which define the test configuration, execution steps, and methods for measuring outcomes.

Through this hierarchical structure, the document establishes clear traceability across requirements, test assertions, and test cases, providing a rigorous basis for objectively evaluating the functional completeness and reliability of drone forensic tools.

1 Introduction

As drone technologies continue to advance, their applications have rapidly expanded beyond simple media capture or entertainment to include illicit activity tracking, crash-cause investigations, surveillance, and intelligence collection. Consequently, drone forensics—the process of acquiring and analyzing data from drones—has emerged as a significant subfield within digital forensics.

Although various drone forensic tools have been developed and deployed, efforts to ensure their reliability remain insufficient. A representative model for establishing forensic tool reliability is the Computer Forensics Tool Testing (CFTT) Program led by the U.S. National Institute of Standards and Technology (NIST). CFTT provides a widely recognized framework that systematically evaluates tool accuracy and reproducibility through specification development, test procedure definition, and result verification. However, because CFTT was designed primarily for computer and mobile forensic tools, it has limitations when applied directly to drone forensic tools.

Against this backdrop, this document presents a Drone Data Collection and Analysis Tool Specification as a foundational framework to ensure the legal reliability and objective verifiability of drone forensic tools.

2 Purpose

This document defines the requirements, test assertions, and test cases for drone forensic tools capable of performing the following operations:

1. Logical acquisition of all or selected folders/files from a drone's internal or external memory into an image file
2. Physical acquisition of all or selected partitions of a drone's internal or external memory into an image file
3. Extraction and presentation of data artifacts from drone image files generated by the tool

The requirements specify the mandatory and optional functional capabilities that the tool must support, and they serve as the basis for deriving the test assertions, which define the specific conditions to be verified after executing each test case. A test assertion describes the observable state—such as the tool's output—after test execution. Each test assertion is addressed by one or more test cases, which consist of a test protocol and expected results.

A test case outlines the test protocol (including environment setup and procedural rules) along with the expected test outcomes. The test protocol defines the detailed procedures for configuring, executing, and measuring the results of the test.

3 Scope

The scope of this document is limited to software and hardware tools that provide capabilities for collecting and analyzing data from (i) internal and external memory of drones manufactured by various vendors (e.g., DJI, Parrot, Yuneec), (ii) drone remote controllers (dedicated devices or smartphones), and (iii) vendor-specific cloud services.

4 Definitions

This glossary defines terms used within this document.

Artifact - A trace generated during the operation of an operating system or application.

Accelerometer - A device that measures acceleration along a specific axis; it enables a drone to maintain stable flight in windy conditions.

Ascent Speed - The speed at which a drone ascends into the air.

Cloud Service - A service that stores data on an external server rather than on local hardware, allowing access from anywhere without storage-capacity limitations.

Controller - A handheld device used by the operator to control the drone; also referred to as a remote controller or transmitter.

Descent Speed - The speed at which a drone descends.

Drone - A general term for an unmanned aerial vehicle (UAV), encompassing a wide range of aircraft from military platforms to hobbyist photography drones. UAVs are also referred to as remotely piloted aircraft (RPA).

Firmware - An operating system or program responsible for controlling and operating hardware components.

Gimbal - A specialized camera mount that uses servos to keep the camera stabilized and level regardless of drone movement.

GPS (Global Positioning System) - A satellite-based navigation system used by drones to determine their position.

Hash Value - A value computed using a hashing algorithm, used to verify the identity and integrity of copied digital evidence.

Hovering Time - The amount of time a drone can remain stationary in the air; this duration varies with payload weight.

Integrity - The principle that digital evidence must be protected from alteration or damage from the time it is collected until it is presented in court.

Log File - A recorded history of operations, events, or related data.

Logical Collection - An exact copy of the information contained within a logical volume (e.g., mounted volume, assigned logical drive).

Metadata - Data that describes a file or directory, which may include the storage location of the content, timestamps, application-specific information, permissions, and more.

No-Fly Zone (NFZ) - A designated area where drone flight is restricted or disabled by government regulation.

Originality - The principle that digital evidence must remain free from tampering or errors during processing, including analysis.

Payload - Any object that a drone can transport, lift, or deliver.

Physical Collection - A bit-for-bit duplicate of the data contained within a device.

Reliability - The requirement that digital evidence must be accurate, consistent, clearly attributable, and free from manipulation throughout legal procedures.

Receiver - A wireless device that receives control commands from the operator to the drone.

Return to Home (RTH) - A function that returns the drone to its takeoff point.

Serial Number (S/N) - A unique identification number assigned to a device or product.

Telemetry - A technology that converts various monitoring and control data between two remote entities into digital signals for transmission and reception.

Thumbnail - A small preview image used to visually represent media files such as videos or photographs.

Waypoint - A predefined point along a flight path. Stored via a GPS device and typically determined through user interaction.

Yaw - A flight-control term describing a drone's rotation around its vertical axis, determining the direction the drone is facing.

5 Background

5.1 Characteristics of Drone Devices[1]

Drones share certain similarities with mobile and embedded devices, yet they possess highly unique attributes and functionalities as aerial platforms. The following illustrate representative characteristics of drone functions and drone-generated data.

5.1.1 Representative Functions of Drones

- Flight and navigation (the most distinctive capability)
- Carriage and operation of various payloads such as cameras and sensors
- Remote control and communication via Wi-Fi or similar technologies
- Real-time video and data streaming

5.1.2 Characteristics of Drone Data

- Data formats differ significantly depending on the manufacturer and model
- Data may be distributed across multiple physical storage locations
- Data is often stored as continuous time-series logs corresponding to flight duration

5.2 Primary Evidence Sources of Drones

Unlike many other electronic devices, drones require a variety of supporting components to operate properly. Therefore, when extracting evidence from a drone, it is advisable to secure comprehensive evidence sources beyond the drone body itself. The methods of data storage and retention may vary significantly depending on the drone's manufacturer and specifications. The primary evidence sources for drones are listed below (**Figure 1** illustrates these sources):

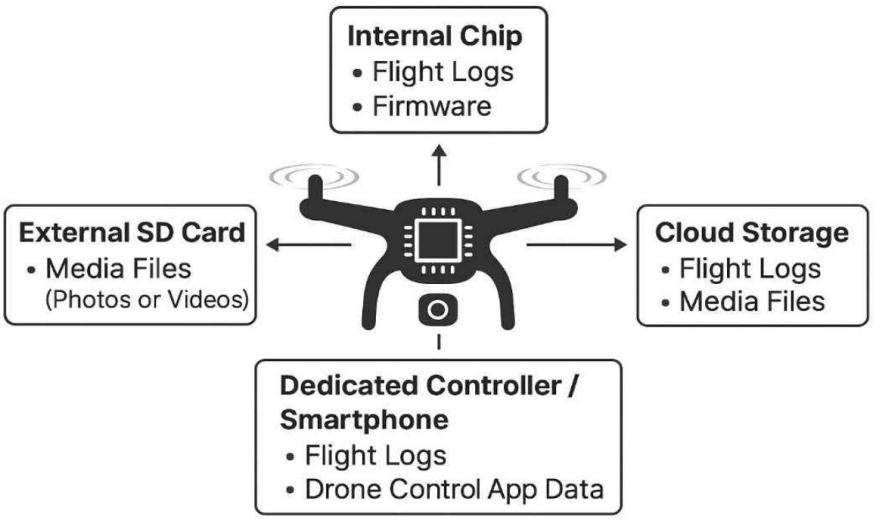

Figure 1. Primary evidence sources of drones

[1] INTERPOL, "FRAMEWORK FOR RESPONDING TO A DRONE INCIDENT", 2020, pp. 12-19

1) Internal Data Storage
Some drones store and maintain information within memory and processors embedded in the drone body or the flight controller. Depending on the drone model and port specifications, the methods for extracting these data may vary.

2) Removable Storage Devices
Some drones store and maintain information within memory and processors embedded in the drone body or the flight controller. Depending on the drone model and port specifications, the methods for extracting these data may vary.

3) Mobile Devices and Applications
Many drones allow full or partial control of the aircraft or its payload through a smart device via a web-based interface or a native mobile application..

4) Remote Controller
In many cases, drones require a remote controller. The controller may store data that help identify the connected drone as well as the phone or tablet used to view the drone's video feed.

5) Cloud-Based Data Platforms
Cloud-based storage can also be a source of drone-related data. Users may intentionally utilize cloud services to reduce local storage demands, or cloud storage may be generated automatically as part of drone cloud-posting platforms that store data on behalf of the user.

6) Network Packet Data
Drones often communicate via wireless networks using remote controllers or similar means. The network packet data generated during such communication can serve as a valuable source of forensic evidence.

5.3 Digital Artifacts Extractable from Drones

A wide range of digital artifacts can be collected from the primary evidence sources described in Section 5.2. These artifacts provide comprehensive information about all activities associated with drone operation. Depending on how a drone stores its data, the methods for accessing and analyzing these artifacts may vary.

Below is an overview of the major digital artifacts that can be extracted from drones. **Table 1** presents example classifications of flight log files—one of the most critical artifacts—by manufacturer. The types of artifacts that can be collected may differ depending on the acquisition method and the specific drone model.

5.3.1 Drone Device Information

- Drone Model Name: Identifies the drone's capabilities, specifications, and supported payloads
- Unique Serial Number: Used to verify ownership and purchase records through the manufacturer's database
- Drone and Controller Firmware Versions: Reveal functional characteristics and potential vulnerabilities based on applied security patches

5.3.2 Application Information Used for Drone Operation

- Drone Control Application Details: Identifies the flight plan and control methods based on the mobile application name, version, and configuration used to operate the drone
- App Logs and Settings: Include stored flight plans, user settings, account details, and other operational records

5.3.3 Captured Media Files and Metadata

- Photo and Video Files: Provide visual records of scenes captured by the onboard camera, stored in internal or external memory
- Metadata: Includes information needed for media analysis (e.g., geolocation, timestamps)

5.3.4 Flight Log Information

- Flight Path: GPS-recorded flight routes used for tracking drone movement patterns
- Flight Time and Date: Enables timeline reconstruction
- Flight Mode: Identifies operational intent and usage mode (e.g., autonomous, manual control)
- Flight Status: Includes speed, altitude, and heading to support behavioral analysis of the drone

5.3.5 System Log Information

- Takeoff and Landing Events: Reveal start/end points of flight and total duration
- Incident and Anomaly Records: Include system errors, emergency landings, and other safety-related events
- Battery Status: Voltage, remaining capacity, and other indicators used to evaluate energy efficiency and available flight time

5.3.5 Communication and Network Information

- Controller Commands: Identify control inputs and operator behavior patterns
- Wi-Fi Information: SSID, MAC address, IP address, and related network details used to assess network environment and security settings
- Bluetooth Information: Identifies connected Bluetooth devices and their relevance to nearby equipment
- Proprietary Protocol Information: Communication data from proprietary protocols (e.g., OcuSync, ELRS) used to interpret transmitted and received operational signals

Table 1. Example of manufacturer-specific classification of drone flight logs

Manufacturer	Drone Model	File Extension(s)	Primary Storage Location (Evidence Source)
DJI	Phantom 4 Pro	*.DAT	Drone Internal Memory
		*.txt	Mobile Drone Control App (DJI GO 4)
Parrot	ANAFI	.bin	Drone Internal Memory
		.txt/.JSON	Mobile Drone Control App (FreeFlight)
Yuneec	Typhoon H	*.csv	Drone Internal Memory

6 Requirements & Test Assertions

This section enumerates the requirements for drone forensic collection and analysis tools. Each requirement is followed by one or more corresponding test assertions, which specify the conditions that must be verified after executing the associated test cases. The requirements include both core features, which all tools must support, and optional features, which apply only to tools offering extended capabilities.

Although some drone forensic tools provide both collection and analysis functionalities, others may support only one of these functions. **Table 2** summarizes each requirement, its associated test assertions, and the types of tools to which those assertions apply. Depending on the tool's functional scope, the applicable requirements and test assertions in an actual evaluation may vary.

Table 2. Relationship between requirements and their corresponding test assertions

Requirements		Test Assertions	Applicable Tool
Core	DR-CR-01	DR-CA-01, DR-CA-02, DR-CA-03, DR-CA-04, DR-CA-05	Analysis tool only
	DR-CR-02	DR-CA-06	Common
	DR-CR-03	DR-CA-07	Collection tool only
	DR-CR-04	DR-CA-08	Common
	DR-CR-05	DR-CA-09	Analysis tool only
Optional	DR-RO-01	DR-AO-01	Collection tool only
	DR-RO-02	DR-AO-02	
	DR-RO-03	DR-AO-03	
	DR-RO-04	DR-AO-04, DR-AO-05	Analysis tool only
	DR-RO-05	DR-AO-06, DR-AO-07, DR-AO-08	
	DR-RO-06	DR-AO-09	Collection tool only
	DR-RO-07	DR-AO-10	Analysis tool only
	DR-RO-08	DR-AO-11	Common

6.1 Core Requirements and Assertions (CR/CA)

** CR stands for Core Requirement, and CA stands for Core Assertion.*

6.1.1 Drone Artifact Analysis

DR-CR-01. The drone forensic tool shall extract all supported data artifacts from the image file, classify them, and present them to the user.

DR-CA-01. The tool presents all available drone device information (e.g., model name, drone serial number) from the image file.

DR-CA-02. The tool presents all available drone control application data (e.g., drone control app version and usage information) from the image file.

DR-CA-03. The tool presents all available flight log–related data (e.g., flight path, takeoff and landing times, anomaly events) from the image file.

DR-CA-04. The tool presents all available media file data and metadata (e.g., photos and videos captured by the drone) from the image file.

DR-CA-05. The tool presents all available communication and network records (e.g., drone Wi-Fi SSID and IP address, Bluetooth MAC address) from the image file.

6.1.2 Text Rendering

DR-CR-02. The drone forensic tool shall correctly render text provided in multiple languages.

DR-CA-06. The tool correctly renders the given text as proper character glyphs and supports the processing and display of multilingual text.

6.1.3 Error Event Handling

DR-CR-03. The drone forensic tool shall notify the user when it fails to access a connected drone device.

DR-CA-07. When access to the connected drone device fails, or when a non-supported model is connected such that drone data acquisition is not possible, the tool immediately notifies the user.

DR-CR-04. The drone forensic tool shall notify the user when its operation is interrupted.

DR-CA-08. When a collection or analysis process is interrupted, the tool immediately notifies the user.

6.1.4 Data Integrity

DR-CR-05. The drone forensic tool shall not modify the drone image file under examination.

DR-CA-09. The tool does not compromise the integrity of the drone image file during analysis, and the hash values (e.g., MD5, SHA-256) of the image file remain identical before and after tool execution.

6.2 Optional Requirements and Assertions (RO/AO)

** RO stands for Requirement Optional, and AO stands for Assertion Optional.*

6.2.1 Image File Generation

DR-RO-01. The drone forensic tool generates a drone image file during a physical acquisition of all or selected partitions of the drone's internal or external memory.

DR-AO-01. A physical image file of the drone is generated.

DR-RO-02. The drone forensic tool generates a drone image file during a logical acquisition of all internal or external memory data.

DR-AO-02. A logical image file of the drone is generated.

DR-RO-03. The drone forensic tool generates a drone image file during a logical acquisition of selected folders or files.

DR-AO-03. An image file of the selected folders/files is generated.

6.2.2 Flight Path Visualization Analysis

DR-RO-04. The drone forensic tool supports timeline analysis by visualizing the drone's flight path data on a map interface.

DR-AO-04. The tool visualizes the drone's flight log data (e.g., latitude–longitude coordinates) on a map over time.

DR-AO-05. The tool provides filtering capabilities that allow visualization of drone flight log data for specific time periods.

6.2.3 Cloud Data Acquisition and Analysis

DR-RO-05. The drone forensic tool supports acquisition and analysis of cloud-based drone data.

DR-AO-06. The tool uses available credential information (e.g., login credentials, access tokens) to acquire cloud-based drone data.

DR-AO-07. The tool presents the collected cloud data to the user in either a visual or structured format.

DR-AO-08. The tool provides an option to export collected cloud data in standardized formats (e.g., KML, CSV, JSON) for external analysis.

6.2.4 Deleted Data Recovery

DR-RO-06. The drone forensic tool supports acquisition of deleted data (e.g., flight logs, media files).

DR-AO-09. During drone data acquisition, the tool detects and collects deleted data and includes it in the resulting image file or extracted dataset.

DR-RO-07. The drone forensic tool identifies and analyzes recovered deleted data within the drone image file and presents it to the user.

DR-AO-10. The tool identifies the presence of recovered deleted data within the drone image file and analyzes and interprets it, providing the results to the user in a structured format.

6.2.5 Report Generation

DR-RO-08. The drone forensic tool generates a final report after all collection and analysis processes are completed.

DR-AO-11. The tool compiles all collection and analysis results and provides a report to the user that includes data content, integrity verification information, and analysis findings.

7 Test Cases for Drone Forensic Tools

This section presents test cases for evaluating tool functionalities derived from the test assertions. The specific test cases selected and applied in practice will vary depending on which functions the tool supports for a given drone model.

DR-01. Drone Image File Generation.

This test case verifies that the tool collects data from a drone device and successfully generates an image file. Additionally, it checks whether the tool generates appropriate notifications when it fails to create an image file due to drone access failure or interruption during the collection process. This test case applies only to the types of acquisition supported by the tool, and may have variants for each acquisition type:

- DR-01-LOG-ALL: Logical acquisition
- DR-01-LOG-SELECTED: Logical acquisition (selected folders/files)
- DR-01-PHY: Physical acquisition

Test Assertions:

DR-AO-01 A physical image file of the drone is generated.
DR-AO-02 A logical image file of the drone is generated.
DR-AO-03 An image file of the selected folders/files is generated.
DR-CA-06 The tool correctly renders the given text as proper character glyphs and supports the processing and display of multilingual text.
DR-CA-07 When access to the connected drone device fails, or when a non-supported model is connected such that drone data acquisition is not possible, the tool immediately notifies the user.
DR-CA-08 When a collection or analysis process is interrupted, the tool immediately notifies the user.

DR-02. Viewing Artifacts from Drone Image Files.

This test case verifies that data collected from a drone device can be reviewed as an image file and that the expected data elements are present when the image file is opened. Additionally, it checks whether the tool generates a notification if the analysis process is interrupted. Variants of this test case may exist depending on the acquisition method used to generate the image file:

- DR-02-IMG-LOG: Opening an image file generated through logical acquisition
- DR-02-IMG-PHY: Opening an image file generated through physical acquisition

Test Assertions:

DR-CA-01 The tool presents all available drone device information (e.g., model name, drone serial number) from the image file.
DR-CA-02 The tool presents all available drone control application data (e.g., drone control app version and usage information) from the image file.
DR-CA-03 The tool presents all available flight log–related data (e.g., flight path, takeoff and landing times, anomaly events) from the image file.
DR-CA-04 The tool presents all available media file data and metadata (e.g., photos and videos captured by the drone) from the image file.
DR-CA-05 The tool presents all available communication and network records (e.g., drone Wi-Fi SSID and IP address, Bluetooth MAC address) from the image file.
DR-CA-06 The tool correctly renders the given text as proper character glyphs and

supports the processing and display of multilingual text.
DR-CA-08 When a collection or analysis process is interrupted, the tool immediately notifies the user.

DR-03. Interruption Notification.

In this test case, data collection or analysis is initiated for a given drone device, after which the connection to the drone is intentionally interrupted or the network is blocked at controlled time intervals to force a process interruption. This verifies whether the tool provides appropriate interruption notifications to the user. Variants may exist depending on whether the interruption occurs during collection or analysis:

- DR-03-COL: Interruption during the collection process
- DR-03-ANY: Interruption during the analysis process

Test Assertions:

DR-CA-08 When a collection or analysis process is interrupted, the tool immediately notifies the user.

DR-04. Image file integrity.

In this test case, the hash value of the drone image file (e.g., MD5, SHA-256) is calculated prior to tool execution. After the tool execution is completed, the hash value of the same drone image file is recalculated, and the pre- and post-execution hash values are compared to verify whether the image file has been modified as a result of the tool operation. In cases where the tool explicitly provides the hash value of the input image file through logs or result reports, the reported hash value is additionally compared with the precomputed hash value to verify the accuracy of the tool's hash calculation.

- DR-04-INT: Comparison of pre- and post-analysis hash values to verify the integrity of the drone image file

Test Assertions:

DR-CA-09 The tool does not compromise the integrity of the drone image file during analysis, and the hash values (e.g., MD5, SHA-256) of the image file remain identical before and after tool execution.

DR-05. Deleted file recovery.

In this test case, files on the drone device (such as flight logs or media files captured by the drone) are intentionally deleted. During image file generation, the test verifies whether the tool successfully extracts the deleted data. Subsequently, the test confirms whether the tool identifies deleted data present within the generated image file and accurately analyzes and presents it to the user. Variants may exist depending on the recovery phase:

- DR-05-COL: Extraction of deleted data during image file generation
- DR-05-ANY: Identification and analysis of deleted data within the extracted image file

Test Assertions:

DR-AO-09 During drone data acquisition, the tool detects and collects deleted data and includes it in the resulting image file or extracted dataset.
DR-AO-10 The tool identifies the presence of recovered deleted data within the drone image file and analyzes and interprets it, providing the results to the user in a structured

format.

DR-06. Flight path visualization.

This test case verifies that the drone's collected flight path data can be visualized on a map interface. Variants may exist depending on the visualization method:

- DR-06-TIMELINE: Visualizing drone flight log data on a map over time
- DR-06-FILTERED: Visualizing drone flight log data for a specific time period using filtering functions

Test Assertions:

DR-AO-04 The tool visualizes the drone's flight log data (e.g., latitude–longitude coordinates) on a map over time.

DR-AO-05 The tool provides filtering capabilities that allow visualization of drone flight log data for specific time periods.

DR-07. Cloud data collection and analysis.

In this test case, the tool uses credential information provided by the user (e.g., ID/password or access tokens) to perform authentication. Upon successful authentication, the tool collects and analyzes drone-related data stored on the cloud server, then presents the results to the user in either a visual or structured format.

- DR-07-COL: Collection of cloud-based drone data using credential information (e.g., login credentials, access tokens)
- DR-07-ANY: Analysis and visualization of the collected cloud data
- DR-07-EXP: Exporting the collected cloud data in standardized formats for external analysis

Test Assertions:

DR-AO-06 The tool uses available credential information (e.g., login credentials, access tokens) to acquire cloud-based drone data.

DR-AO-07 The tool presents the collected cloud data to the user in either a visual or structured format.

DR-AO-08 The tool provides an option to export collected cloud data in standardized formats (e.g., KML, CSV, JSON) for external analysis.

DR-08. Report generation.

In this test case, the tool generates a report file after completing the collection and analysis of data from a drone device. Once each process is finished, the tool produces a corresponding result report:

- DR-08-COLLECTION: Generation of a result report after completion of the collection process
- DR-08-ANALYSIS: Generation of a result report after completion of the analysis process

Test Assertions:

DR-AO-11 The tool compiles all collection and analysis results and provides a report to the user that includes data content, integrity verification information, and analysis findings.

8 Appendix

8.1 Components of a Drone

All drones are composed of the following two types of components:

8.1.1 Physical Components

The physical components that make up the drone's body and flight mechanism can be categorized as follows. Not all drones include every component listed below, but each element of a drone can be identified as one of the following:

1) Drone Body
The core structure of the drone that houses all other components.

2) Flight Controller
Used to control the drone's flight. This component stabilizes the drone and typically receives navigation inputs from a remote control device. In more advanced systems, the flight controller can be remotely operated in real time or pre-programmed for autonomous flight.

3) Motors, Rotors/Propellers/Wings, Speed Controllers
Provide lift and propulsion for the drone. Various design types exist, including designs specialized for higher speeds or extended flight duration.

4) GPS Receiver
Although not mandatory for all drones, it is commonly used. The GPS receiver helps manage the drone's position, supports return-to-home functionality, and enables autonomous flight path configuration.

5) Radio Receiver (RX)
Used to receive control input signals transmitted from a ground-based transmitter.

6) Transmitter (TX)
Used by the operator on the ground to send manual input commands to the drone.

8.1.2 Software Components

All drones incorporate applications or software used to control system operations. These software components fall into two main categories:

1) Flight Management Software
This software is uploaded to the drone's flight controller and the user's remote-control device (e.g., controller, transmitter). When the drone is in operation, flight management software controls common functions such as takeoff, landing, flight maneuvers, and device stabilization.

2) Ground Control Software
This software is used to control predefined navigation plans and effectively schedule flight operations. It is suitable for pilots preparing and planning missions while the drone is on the

ground. Ground control software also allows remote users other than the pilot to enhance real-time monitoring of the drone during flight via computers, tablets, or smartphones.

8.2 Drone Data Storage Locations

The following describes common storage locations for flight logs and multimedia files (e.g., photos, videos) used in many currently available commercial drones. Understanding these storage paths is essential for forensic data acquisition and analysis. Below (**Table 3** and **Table 4**) are example data paths for selected drone models:

8.2.1 Flight Log

Table 3. Flight log locations of selected commercial drones

Drone Model	Flight Log Data Location	File Path	File Format
DJI Phantom 3 Standard	External Memory (microSD)	/	FLY.DAT
DJI Phantom 4 Pro	Internal Memory	/	FLY.DAT
DJI MAVIC Air	Internal Memory	/blackbox/flyctrl/	FLY.DAT
		/blackbox/dji_flight/	DFLY.DAT
DJI Spark	Internal Memory	/flyctrl	FLY.DAT
Parrot ANAFI	External Memory (microSD)	/Internal/FlightData/	.bin(.json)

8.2.2 Media File

Table 4. Media file locations of selected commercial drones

Drone Model	Type	Data Location	File Path	File Format
DJI Phantom 3 Standard	Photo	External SD	/DCIM/100MEDIA/	.jpg/.dng
	Video	External SD	/DCIM/100MEDIA/	mp4/.mov
DJI Phantom 4 Pro	Photo	External SD	/DCIM/100MEDIA/	.jpg/.dng
	Video	External SD	/DCIM/100MEDIA/	mp4/.mov
DJI MAVIC Air	Photo	External SD	/DCIM/100MEDIA/	.jpg/.dng
	Video	External SD	/DCIM/100MEDIA/	mp4/.mov
YNEEX Q500 4K	Photo	Internal Memory	/DCIM/	.jpg/.dng
	Video	Internal Memory	/DCIM/	mp4
Parrot ANAFI	Photo	External SD	/DCIM/100MEDIA/	.jpg/.dng
	Video	External SD	/DCIM/100MEDIA/	mp4