Scientific Working Group on Digital Evidence

Best Practices for Drone Forensics

21-F-002-1.2

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification

Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Drone Forensics

Table of Contents

1. Purpose

This document is to provide a foundational resource regarding best practices for conducting digital forensics on drones.

2. Scope

Drones come in different configurations with different applications for ground, swim or flight. This document will focus solely on consumer drones that fly and their connected systems.

For the purposes of this document, the term "examiner" refers to individuals who have specialized training, knowledge, skills, and abilities that allow them to handle a wide range of technical issues related to digital forensics, and who may be performing technical tasks to include collections, acquisitions, and/or analysis.

Following are general description for commonly discussed drones:

- UAS (Unmanned Aircraft System): A system that includes the drone itself, as well as its ground control station, any payloads it is carrying, and any other necessary components.
- UAV (Unmanned Aerial Vehicle): The aircraft itself, without any of the other components of a UAS.
- sUAS (Small Unmanned Aircraft System): A UAS that weighs less than 55 pounds.
- RPAS (Remotely Piloted Aircraft System): Another term for a UAS.
- RPV (Remotely Piloted Vehicle): Another term for a UAV.

For the purposes of this document, 'drone' will be used interchangeably with sUAS and will explicitly apply to the commercial and consumer level devices.

3. Limitations

This document is not all-inclusive, does not contain information relative to or in support of specific commercial products, is not intended to be a training manual or to specify operating procedures, and the ideas, concepts, and technical aspects referenced are strictly related to what was available at the time this document was created and what were currently the most prominent considerations. Considerations regarding UAS and UAV classes of devices are outside the scope of this document and will not be discussed herein. Some artifacts listed in this document may not apply to alternative vendors, custom built and/or non-commercially available drones.

4. Device Seizure

4.1 Safety Concerns

Drones discussed in this document generally use propellers for powered flight that spin at thousands of rotations per minute and fly at speeds of up to 60 miles per hour or more. Propellers or rotors on a powered device can start spinning without notice. These factors make them potentially dangerous to whomever is handling or seizing the device.

If the device cannot be powered off, or a method for powering off the device cannot be ascertained, a large heavy blanket or mesh net can be draped across the top of the device to prevent the propeller from spinning and potentially harming the individual seizing the device.

Turn the device upside down to prevent the rotors from spinning up and determine if the battery can be removed. Lithium-ion polymer (LiPo) batteries can be highly volatile if damaged. If undamaged, remove and store the battery in an approved LiPo transportation container or separately in any dry container.

If the cells are damaged, collecting personnel should consider the risk to both people and the evidence before deciding to remove the battery. Fire and chemical resistant gloves should be worn to mitigate risks involved with handling damaged batteries. Devices may be modified to cause harm such as being configured as an Improvised Explosive Device.

4.2 Collection

Prior to or contemporaneous with the collection, the collecting examiner should document the following, in addition to the examiner's standard collection policies:

- Power state (on or off)
- Physical condition including any noticeable damage to the aircraft
- Identifiers such as serial numbers, model numbers, FAA registration (may be found underneath battery or externally on the chassis)
- Person(s) in the vicinity with controllers or person(s) who convey control or ownership of the drone
- Payloads or modifications (determine if hazardous or weaponized, mechanical or biological)
- Electronic devices in close proximity (phones, tablets, laptops, controllers, ground station radio antenna etc.)
- GPS coordinates for collection location
- Previously observed flight paths or direction of travel and possible flight targets (building, car, person, etc.)
- Make and model of attached camera(s)
- Make a note of any exterior markings or registration numbers

When collecting digital evidence, it is important to remember that other devices may be synchronized with or otherwise connected to the aircraft and relevant to the investigation. Evidence may be stored on these devices as well; controllers, phones, tablets computers, external antennas (plugged into computer or controller). It is important to include them in your search authority.

Data may be stored in a flash chip on the motherboard or in an onboard SD card. When packing for transport, leave the device as intact as possible. Ensure that packaging is secure enough to prevent possible impact or shock damage.

A seized device should be isolated from network connections by transporting and storing it in a faraday container or similar type of chamber that will isolate it from wireless signals (if feasible due to size). If the device cannot fit inside such a container, removing the battery is the next best option.

As with other evidence, take care to preserve any DNA, fingerprints, or other physical evidence that may exist. Also, thoroughly document all damage to the device and actions taken during seizure, noting date and time.

If drone countermeasures (e.g., Radio Frequency jamming, or any other systems capable of interfering with drone systems) are used during the collection of the device, it is important to document the date and time the countermeasure was activated and deactivated, and the type of countermeasure that was used in order to understand the existence of any countermeasure-related artifacts within the seized evidence (e.g., erratic drone behavior, additional RF interference, or change in home location).

5. Data Acquisition

Acquiring data from a drone and its connected systems is not limited to any specific process or method. Drone data acquisition may be conducted using different methods including non-invasive processes such as logical file transfer via a cable or Wi-Fi, and more invasive techniques like chip-off. The choice of method for acquisition will depend on a variety of factors, such as the expertise of the examiner, condition of the device(s) upon seizure, types of artifacts being sought, and the goals of the investigation. An examiner will most likely not be able to obtain a full physical acquisition of the device's internal memory by simply attaching a USB cable and mounting the device's storage to the examiner's workstation. If a full physical acquisition is required, it will be necessary to use an alternative method such as ISP or removal of the memory chip (eMMC, MTD, etc.).

5.1 Evidence Sources

5.1.1 Secure Digital Cards (SD Cards)

Many drones have external and/or internal SD or micro-SD card slots for nonvolatile media and or flight log storage. In these cases, the card should be removed and a physical acquisition should be acquired directly from the card. It may be necessary to disassemble the drone to access the SD or microSD card. It is important to check for additional external media cards that may be attached to the gimbal or cameras that are attached to the drone. Refer to the SWGDE Best

Practices for Computer Forensic Acquisitions document for guidance on acquisition of these storage devices.

5.1.2 Printed Circuit Boards (PCBs)

Drones contain printed circuit boards (PCBs) akin to modern mobile devices, motherboards, and IoT devices. Therefore, PCBs on drones contain data storage components that can be removed using the same chip-off methods featured in mobile device forensics. Yet, it is important to note that just like many mobile devices, drone PCBs often also contain conformal coating and underfill so proper best practices should be pursued. Refer to the SWGDE Best Practices for Chip-Off document for guidance on the application of this process.

5.1.3 Synchronization

Data related to a drone device can often be found on a cellphone, computer, smartwatch, tablet, controller or other associated device due to synchronization or sharing of information through a backup process or cloud service accounts. Likewise, data from a computer or other devices that have been synchronized may also be found on the drone. Due to this information exchange, it may be possible to link a particular drone to a particular system or device with which it was connected. All devices that could potentially have been paired to the drone being seized should also be properly seized and examined for data of evidentiary value. Oftentimes, mobile devices that were used to control the drone may contain flight log data and media related to the drone's activity.

5.1.4 Cloud Data for Particular manufacturers

Most commercial and consumer drone companies require users to register information on their respective online portals, ultimately establishing a recurring login process for access into their software applications. Thus, in order for a user to pilot a drone with its native software client, a handshake must first take place between the user and the drone company. Of course, whether or not these drone companies store logs of these handshakes, or at minimum record user logins, will probably vary and be unique to the company.

Additionally, there are companies in the consumer drone industry that offer cloud storage and cloud management features. This includes everything from storing media to backing up flight logs to uploading content on social media platforms. Again, acquiring this type of data will be specific to the targeted drone and its associated systems as well as any limitations to the scope of the examiner's search.

5.1.5 FAA Remote ID

On March 16, 2024, the Federal Aviation Administration will require most drones to comply with the remote identification rule (https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89). This law mandates the majority of drones operating in the United States have the capability to broadcast the following information:

- The identity of the unmanned aircraft, consisting of a serial number assigned to the unmanned aircraft by the person responsible for the production of the standard remote identification unmanned aircraft or a session ID.
- An indication of the latitude and longitude of the control station.
- An indication of the geometric altitude of the control station.
- An indication of the latitude and longitude of the unmanned aircraft.
- An indication of the geometric altitude of the unmanned aircraft.
- An indication of the velocity of the unmanned aircraft.
- A time mark identifying the Coordinated Universal Time (UTC) time of applicability of a position source output.
- An indication of the emergency status of the unmanned aircraft.

The physical remote ID component is built into most drones manufactured after December of 2022. However, drones without the built in broadcast hardware can be equipped with a broadcast module. Requirements of the remote ID rule apply to most drones operating in the United States but there are exceptions. If the drone weighs less than 0.55 pounds or is being operated in a FRIA (FAA-Recognized Identification Area) it will not be required to broadcast remote ID data.

The remote ID functions as a digital license plate and the broadcasted data can be made available to public and private entities via personal wireless devices within the range of broadcast. Associating the drone serial number or session ID with a registered owner will be limited to the FAA database but can be obtained by law enforcement or authorized personnel upon request.

5.2 Potential Forensic Artifacts

Drones and their associated systems contain a variety of forensic artifacts. As with any relatively new technology, drone technology is constantly changing, adding new capabilities, and subsequently new forensic artifacts are likely to become available. The below listing of possible artifacts is not intended to be exhaustive, but instead meant to acquaint the reader with the most commonly seen artifacts and provide a basic understanding of the types of data an examiner may encounter. The number and types of artifacts are contingent on the device model, operating system, application, etc. The examiner should be aware that data may exist in several locations, and data may be created intentionally by the user, by user activity, or purely by the operations of the device.

We divide artifacts into three categories, based on what the data describes. Artifacts an examiner may encounter include:

5.2.1 User-Created Data

- Digital imagery, video footage, or audio files
- Waypoints or flight plan defined by the user

5.2.2 User-Activity Data

- Flight logs
  - Dates and times of operation
  - Navigational waypoints utilized
  - GPS positions
  - Motor speeds
  - Altitude data
  - Directional information
  - Flight route or path
- Launch location, landing location
- Mission-specific payload information (such as audit logs)
- Configuration files

5.2.3 Device Operating Data:

- FAA Registration
  - Drones weighing over .55 lbs (250 grams) according to the FAA must be registered. Potential registration information may be obtained through proper legal process.
  - Search private (non-FAA regulated) drone registration database(s) such as https://reclaimdrone.com/faa-lookup/
- Associated devices (mobile phones, online accounts, connected controller, previous computer connections, battery serial numbers)
- Software versions/firmware versions

6. Data Analysis

Data acquired from drones and their connected systems may be analyzed utilizing traditional digital forensic practices and tools known to the community. At this point in time, a wide disparity exists in the ability of tools to comprehensively parse the data from these systems. Digital forensic practitioners should utilize best practices as well as the following principles against these new technology devices including:

- Identify what open source and vendor tools support this model.
  - Oftentimes, if a vendor supports a specific model, it will only be able to acquire a logical acquisition of the media or flight log partition.
- Utilize primary and secondary tools to review the data for cross-tool validation.
  - Tool testing and validation (this applies to ANY tool used), should be tested against a known dataset. NIST offers a set of drone datasets for testing on the NIST Computer Forensic Reference Data Sets (CFReDS) webpage.

- Recognize that drones and their connected systems use a variety of operating systems and file systems.
  - Examiners will need access to tools that can analyze Linux, UNIX, and Android operating systems.
  - Tools will also need the ability to parse various UNIX type file systems.

Analyzing drone data is virtually no different than the analysis performed on a hard disk drive (HDD) image or mobile device (See 2020-09-17 SWGDE Best Practices for Mobile Device Forensic Analysis v1.0 and 2018-07-11 SWGDE Best Practices for Computer Forensic Examination). The same forensic principles apply to analyzing drone data like any other data set being reviewed. What makes analyzing drone data seem different, however, is the scarcity of available parsing tools for the data. This is mainly due to the fact that many consumer drones have multiple partitions and utilize various types of UNIX compatible file systems. This partitioning scheme is different from what is typically featured in a mobile device or HDD; thus, most commercial and open-source tools are unable to support reading and parsing raw physical disk images from many drones on the market.

On the other hand, there are both commercial and open-source forensic applications available which support a limited number of drones or its corresponding data (i.e., flight log parsers).

7. Caveats and Cautions

According to the 2019 FAA registry, over one million non-recreational sUAS devices have been registered and the number is increasing. Due to the quantity of devices and variety of manufacturers, one major challenge in data acquisition and analysis from drones is the lack of available training, tools, research documents, and forensic procedures. Manufacturers may be reluctant to provide assistance or access to information regarding proprietary intellectual property and may not be forthright regarding the device specifications or user data available.

7.1 Volatile Data

Data on sUAS devices can be highly volatile. Specifically, it is important to note that with some of the popular models of drones, when the device is powered on, new flight logs will be created. These logs will fill with data as long as the drone is powered on. If the device's dedicated storage for flight logs is already full or near full, it will delete older flight logs to make room for newer ones. In this case, the examiner may be inadvertently deleting data of evidentiary value.

7.2 Remote device wiping

Many of the popular drones on the market run some version of Android OS. Although there are not many drones available yet that come with 4G/5G connectivity, it is important to treat the device as though it has the capability to connect to the internet, therefore leaving the ability to remotely wipe the device, similar to mobile phones/devices. A seized device should be isolated from a network connection by transporting and storing it in a faraday container or similar type of chamber that will isolate any incoming or outgoing connections (if feasible due to size). If the

device cannot fit inside a network isolation chamber, removing the power source (battery) is the next best option.

7.3 Encryption

Data of evidentiary interest may be located within proprietary, encrypted, and encoded DAT files. It is important to note that depending on the model of drone being examined, the acquisition method of choice may affect whether the data is acquired in an encoded/encrypted state or not.

7.4 Accuracy of Logged GPS Waypoints

If the GPS on the drone is not properly calibrated at the time of system startup, the drone may log inaccurate GPS locations on the device. The forensic examiner needs to be ready to validate the data represented with other sources such as the recovery location, third party observations, examination and comparison of the photographic or video records, number of GPS satellites device was connected to at the time, and GPS record from other synchronized devices.

8. Drone Specific Resources:

- Interpol. Framework for Responding to a Drone Incident: For First Responders and Digital Forensics Practitioners. Released 2020, Singapore. https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf
- Responder Slick Sheets. Drone Forensics Program 2017-2018, U.S. Department of Homeland Security, Science & Technology Contract Number HHSP233201700021C. Forensics Program
- Unmanned Aircraft Systems (UAS). U.S. Federal Aviation Administration (FAA). https://www.faa.gov/uas/

9. SWGDE Documents relevant to the topic of Drone Forensics:

- SWGDE Best Practices for Chip-Off
- SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition
- SWGDE Best Practices for Mobile Device Forensic Analysis
- SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices
- SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics
- SWGDE Best Practices for Digital Forensic Video Analysis
- SWGDE Technical Overview of Digital Video Files

10. History

Revision	Issue Date	History
1.0 DRAFT	9/17/2020	Initial draft created
1.0 DRAFT	1/14/2021	Initial draft formatted and voted by SWGDE for release as a Draft for Public Comment
1.0	1/13/2022	Released for public comment
1.1 DRAFT	10/23/2023	Updated content, released for public comment
1.2 DRAFT	1/11/2024	Addressed public comments and made substantive changes
1.2 DRAFT	2/29/2024	SWGDE voted to release as Draft for Public Comment; formatted for release for public comment.