



WhitePaper

FROM TAKEOFF TO TAKEDOWN: THE ART OF DRONE FORENSICS

by Sarah Frances
Director of Reverse Engineering



SkySafe

From Takeoff to Takedown: The Art of Drone Forensics



Introduction

I recently had the pleasure of presenting a talk with the same title at the 2023 [Digital Forensics for National Security Symposium](#) in College Park, MD. The thesis of the presentation seemed to strike a chord with the attendees, namely that our current mindset around digital forensics needs a bit of a reboot. To simplify things, I asked the audience to view the small Unmanned Aircraft Systems (sUAS) forensic analysis process through two separate phases. I am calling phase one the “Takeoff” phase, where the aircraft is powered on and possibly airborne, and phase two the “Takedown” phase, where the aircraft is no longer airborne and is in the possession of a forensic examiner.

Takeoff

Our concept of traditional digital forensics revolves around the procedures for extracting, processing, and analyzing digital artifacts from a recovered device, which means the tools and techniques are primarily focused on the Takedown phase. But sUAS begin emitting a trail of digital artifacts from the *moment* they are powered up and take flight.

We, as a community, need to begin shifting our mindset from one of incident *response* to incident *prevention*, and we need to start building tools that allow us to perform forensic analysis in **real-time**. Using a tool like SkySafe Cloud, we can begin to identify patterns of compliance and patterns of non-compliance in sUAS behavior.

Patterns of Compliance

When we speak of compliance in this context, we are referring to Federal Aviation Administration (FAA)-regulated behavior of sUAS. For example, is the aircraft broadcasting Remote ID? Is it flying in controlled airspace but has Low Altitude Authorization and Notification Capability (LAANC) authorization? Is it appropriately avoiding No-Fly Zones (NFZ)? Is the aircraft generally exhibiting behavior that would not be considered reckless under any circumstances? Patterns like this can help to inform our threat model of an aircraft in real-time.

Patterns of Non-Compliance

In addition to identifying patterns of compliance, we also need to be able to identify patterns of *non-compliance*. If an aircraft is trying to hide its location, it might spoof Remote ID data and/or Aeroscope data (in the case of a DJI drone, specifically). In order to identify a trend like this, we need tools like SkySafe Cloud that can identify the *real* location of the aircraft while also identifying and alerting on the divergent data stream being broadcast over the air. In some cases, we have seen threat actors completely disable these location-based broadcasts, which may also be indicative of malicious behavior when that aircraft is used to drop contraband over the walls of a correctional facility.

From Takeoff to Takedown: The Art of Drone Forensics

New Approach

The absence of specific forensic artifacts can also inform a threat model, and we need more technology like SkySafe Cloud that can identify these trends in real-time, while also tracking the historical data associated with aircraft flight patterns and behavior. Traditional legacy hardware systems can't keep pace with today's tech-savvy adversaries. We need to be providing users with key insights of sUAS flight behavior while the aircraft is in flight, allowing organizations to make data-driven decisions.

SkySafe's team of engineers is constantly iterating through the data and searching for patterns of anomalous activity. When such patterns are identified, we are investing in the reverse engineering effort to understand the behavior, and the software development to add new heuristics to SkySafe Cloud to ensure our customers are alerted to these patterns of non-compliance in real-time. This results in a live feedback loop of improvements to real-time data based on historical data which is something that standalone, hardware-based technology cannot provide.

Takedown

Traditional forensics are still at play in the world of sUAS and are essential to closing the complete lifecycle that begins in the Takeoff phase. Vendors like DJI are implementing forensic countermeasures, such as encryption of flight logs, which are the most valuable digital forensic artifact on sUAS. We still need tooling to extract and decrypt this data and that tooling needs to keep pace with sUAS vendor release schedules.

Aircraft Modifications

That said, our approach to traditional digital forensics around sUAS could also benefit from a thought shift. Logical and physical extractions are no longer enough on their own, because these tools do not typically identify hardware and/or software *modifications* made to the device. If a bad actor has modified his or her device to disable specific broadcasts, for example, there might not be evidence of this in the extracted contents. Or, in some cases, we just don't have forensic tools designed to be *looking* for these types of artifacts, nor the training for those in the field to teach examiners what they *should* be looking for in recovered data.



From Takeoff to Takedown: The Art of Drone Forensics

Scope

Our current methods of forensic examination can also unintentionally limit the scope of the resulting investigation. That is, the examiner knows there was a specific incident that led to confiscation of the device, and the extracted artifacts will hopefully support evidence of that event in pursuit of legal action. Using the example of an incident response scenario at a correctional facility, at the micro level, it may appear as though that aircraft was engaging in illegal behavior by breaching the airspace of that facility and attempting to drop a malicious payload. Extraction of digital artifacts can give the appearance that the scope of the incident is indeed limited to that correctional facility.

If the examiner can, instead, use the recovered data along with historical data provided by technology like SkySafe Cloud, the investigator might discover that the aircraft was seen at *other* correctional facilities located in *different* geographical regions, which broadens the scope of the investigation and completely changes the threat model.

When we are able to pair data recovered post-Takedown with the historical data captured in the Takeoff phase, we have a complete picture of an aircraft's pattern of behavior.

Takeaway

The takeaway here is that we need to be combining traditional forensics with cloud-based forensic data to build a complete and accurate threat model. Our concept of digital forensics in this new space needs to expand beyond the traditional close-access data collection methods because those are not sufficient on their own; they only give us a small piece of what could be a much larger picture. Our adversaries are constantly evolving to find new ways to evade detection; we must be evolving as well to stay ahead.

SkySafe is proud to be on the forefront of this new approach, and is working diligently to get this technology into the hands of key stakeholders and decision makers. If you'd like to know more about SkySafe's novel approach to sUAS airspace awareness and detection, or you are interested in a demonstration for your organization, please reach out to SkySafe at info@skysafe.io; we would love to hear from you!

