**Assignment Proposal – Drone Forensics**

1. Goals
   * + 1. Learn how to perform forensic analysis on drone data
       2. Acquire, validate, and parse flight data including logs (.txt, .dat), cached videos (.mp4), and cached images.
       3. Extract and correlate forensic evidence such as GPS locations, flight paths, timestamps, and battery information.
       4. Compare different forensic tools (CsvView, PhantomHelp, AirData) for analyzing flight records

1. Steps

1. Data Preparation and Setup

Before beginning the analysis, students should select a single flight record file (either .txt or .dat) to serve as the common source for all methods. To ensure consistency and integrity, the file’s name and hash value (e.g., MD5 or SHA256) should be recorded. A dedicated working directory should be created, with subfolders for each method so that results and screenshots can be stored in an organized way. The necessary tools must also be prepared: a text editor for manual parsing, the PhantomHelp and AirData websites for online analysis, and the CsvView software as the desktop-based forensic tool. Once the environment is properly set up, students will proceed to analyze the same file through four different approaches.

2. Method 1 – Manual Parsing

Manual parsing requires students to open the flight record file directly and interpret its raw contents. They will need to identify critical fields such as UTC timestamps for take-off and landing, then calculate the total flight duration, keeping in mind that time zone discrepancies may cause errors. Students should also examine GPS status indicators, flight modes (such as P-GPS), and any recorded error messages. While this approach is labor-intensive and prone to human error, it allows students to understand the underlying structure of the log data and to appreciate the challenges forensic investigators face when no automated tools are available.

3. Method 2 – PhantomHelp

www.phantomhelp.com

The PhantomHelp website offers students a fast and user-friendly way to transform raw flight log files into structured and visualized evidence. After uploading the selected flight record, the platform generates an automated report that typically includes a map of the drone’s path, complete with markers for take-off and landing points, maximum altitude, flight distance, and the duration of the mission. This visualization allows students to immediately grasp the overall movement of the drone, something that would require extensive effort if working only with raw text. PhantomHelp also summarizes key metrics such as maximum speed, average altitude, and total distance traveled, providing forensic investigators with a quick “snapshot” of the flight.

In addition to the automated summaries, PhantomHelp highlights warnings, error codes, or unusual behaviors that were logged during the flight. Students should take note of these alerts, as they often point to potential technical problems or operational anomalies that may be relevant in a forensic context. One important task is to compare the values from PhantomHelp’s report with those obtained through manual parsing. This comparison not only tests the accuracy of the online tool but also helps students recognize the limitations of automated platforms. Finally, students should capture screenshots of the generated maps and summary tables, and save them alongside their manual parsing notes for cross-referencing later.

4. Method 3 – AirData

airdata.com

AirData provides a more comprehensive forensic view of drone activity, offering significantly richer analytics than PhantomHelp. Once students have registered for an account and uploaded the same flight record, they gain access to a dashboard that presents multiple layers of information. Beyond simply showing the flight path, AirData breaks down the flight into detailed charts showing altitude changes over time, velocity and acceleration patterns, GPS accuracy indicators, and communication strength between the drone and controller. Such information is valuable for reconstructing not only where the drone flew, but also how it was flown and whether there were any signal or control issues.

One of the strongest features of AirData is its in-depth treatment of battery information. Students can view graphs that display the percentage of battery charge throughout the flight, fluctuations in temperature, and even the discharge rate under different load conditions. These details are essential in forensic investigations where malfunction, operator negligence, or deliberate tampering with power sources may be in question. Another valuable aspect of AirData is the ability to visualize pilot stick movements, which reveals how the operator controlled the drone. This can provide context for sudden maneuvers, altitude drops, or unexpected flight path deviations.

Compared to PhantomHelp, AirData is not only more data-rich but also more customizable. Students should explore the interactive interface, compare metrics across different categories, and take note of discrepancies between AirData’s interpretation and the results from manual parsing or PhantomHelp. This will allow them to critically assess whether the additional data granularity adds forensic value or introduces complexity that may not always be necessary in practice.

5. Method 4 – CsvView

CsvView represents a standalone software solution that runs locally on the student’s workstation, and it is particularly well-suited for analyzing .dat files. After opening the flight record, students can access a wide range of functions designed to visualize and interpret raw drone logs. The GeoPlayer feature allows the user to view the exact flight path superimposed on a map, which is helpful for verifying location claims or reconstructing surveillance activity. The EventLogPlayer provides a chronological display of important events, such as take-off, landing, warnings, and critical errors, enabling investigators to clearly segment different stages of the flight.

One of CsvView’s most powerful forensic features is its ability to generate battery analysis plots. Students can create graphs showing battery percentage, voltage, and temperature over time, which can then be correlated with specific moments in the flight. This makes it possible to detect anomalies such as sudden voltage drops, overheating, or unexpectedly fast consumption rates. Such anomalies may indicate technical failures or deliberate attempts to over-stress the drone. CsvView also enables flexible exploration of other sensor readings, giving students a broader context than they may find on web-based platforms.

Unlike PhantomHelp and AirData, CsvView does not rely on server-side processing, meaning all data stays local to the analyst’s machine. This aspect should be emphasized, as it reflects real-world forensic principles of data integrity and chain of custody. However, students may also find CsvView more complex to operate, with a steeper learning curve. They should carefully document their workflow, capture screenshots of the graphs and logs, and evaluate whether CsvView’s additional level of control and independence outweighs the convenience of online platforms.

1. Assignment Questions
   * + 1. From the raw log, what are the take-off and landing times, and how long was the flight?
       2. What flight path and summary did PhantomHelp show, and how do they compare to manual parsing?
       3. What extra details does AirData give, especially about battery and pilot control inputs?
       4. In CsvView, what did GeoPlayer and EventLogPlayer reveal, and what did the battery graphs show?
       5. Which method gave the most useful evidence, and which was easiest to use?
       6. Were there any differences in results between the methods? Why might they appear?
       7. Which method would you trust most in a real forensic case, and why?
       8. What are the drawbacks of using online tools (PhantomHelp, AirData) compared to a local tool like CsvView?