C3 An Investigation Into the Encoding and Encryption of Black Box Data on a DJI Spark

Elijah A. Vela, Laredo, TX 78043; Josh Brunty, MS, Marshall University, Huntington, WV 25701; Dale Mosley, West Virginia State Police Digital Forensics Unit, Huntington, WV 25701; Rob Attoe, BS, Spyderforensics LLC, Masontown, WV 26542*

Learning Overview: After this presentation, attendees will have a better understanding of the black box files obtained from a drone and the formatting of their encoding or encryption.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by attempting to identify patterns of obfuscation and encryption within black box files of a DJI Spark. In addition, several open source tools will be used to acquire, parse, and compare data to ascertain which tool or combination of tools provides the most amount of usable data.

With the increased use of Unmanned Aerial Vehicles (UAV), new methods of forensic data collection and analysis of UAVs and their associated devices have been developed. In an attempt to combat the unwanted access to sensitive device data by outside third parties, such as law enforcement, companies who make these UAVs have increased their security. This increased security requires new methods and techniques to be employed in order for information to be gleaned.

DJI, a Chinese technology company, is one of the most prominent suppliers of drones to the world. The drones sold by DJI range from professional drones aimed at experienced flyers to smaller user-friendly amateur drones. The specific type of drone used during this study was the DJI Spark, a small drone primarily made for taking short flights while capturing pictures and videos. This drone has the capability of being controlled by a remote control, cellular device, or motion control. For the purposes of this study, the Spark was connected to a Samsung™ SM-G900I® mobile device.

The cellular device was imaged using Magnet® ACQUIRE™ version 2.13.0.15121. Files from this device and the drone's on-board microSD card were imaged using AccessData® FTK Imager® version 4.2.0.13. The DJI Spark flight logs were obtained using DJI Assistant 2® version 1.2.5. This free DJI app provided files from the internal memory of the drone. Flight logs were exported in a single .DAT file while black box data was exported in series of .log files. The DJI .DAT file was then extracted using DatCon's ExtractDJI® version 1.4.2, which provided a series of FLYxxx.DAT files. These individualized files provided a three-digit number, in place of "xxx," that corresponded to a recorded flight on the drone.

The .DAT files were parsed through using various open source tools, including DatCon®, Airdata™, and DROP.[1] Using these programs, readable .txt, .log, and .csv files were created where information about a drone's systems and flight parameters were displayed. The amount of information displayed across the applications varied. Common information among the tools used included the time of flight, battery percentage in relation to the time, and the mode of flight the drone was using.

Files pertaining to the black box consisted of mostly text documents that displayed information in WidChar when opened in Notepad® version 6.1. The hex values of these files were observed using FTK Imager® and HxD Hex Editor® version 2.3.0.0.

Log files obtained from the companion cellular device contained information about the flights extracted from the drone. In addition to the flights pulled from the drone directly, the companion cellular device included information about previous flights that were inaccessible from the drone. Located in a folder for the DJI Go 4® application, a flight error propagation log was found containing error notifications and time stamps.

The results of this research will provide a better understanding of the obfuscation and encryption techniques employed by DJI. In addition, this study aims to obtain a greater insight of which open source tools may retrieve usable forensic data from a DJI Spark and its associated products.

Reference(s):

1. Devon R. Clark, Christopher Meffert, Ibrahim Baggili, Frank Breitinger. DROP (Drone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. *Digital Investigation 22*, (August 2017), S3-S14, https://doi.org/10.1016/j.diin.2017.06.013.

Black Box, Drone, Encoded

*Presenting Author