C21 A Forensic Investigation of Drones

Niels Ter Bork, BS, NFI, Laan Van Ypenburg 6, Den Haag 2288GD, NETHERLANDS; and Zeno J. Geradts, PhD, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, SH 2497 GB, NETHERLANDS*

After attending this presentation, attendees will learn what type of data can be extracted from drones after they have been used.

This presentation will impact the forensic science community by highlighting several methods for the digital investigation of drones. Since the number of drones is rising, they are also being used in criminal activities.

Drones come in all shapes and sizes and are becoming more accessible to individuals. Drones are increasingly popular among criminal organizations due to their ease of operation and the different functions they offer. Criminals use drones to explore unseen locations and to transport illegal cargo.

Because little is known about what data is stored on different types of drones, it is important to focus on an exploratory study. The Netherlands Forensic Institute (NFI) wanted to know what research questions regarding drones to take into consideration. For this purpose, six different types of drones popular in 2016 were purchased. These include drones from the DJI®, 3DR®, and Align, and Yuneec brands. These drones have assistance systems, making it easy to control the drones. The auxiliary systems themselves handle a large amount of data that can be useful for forensic examination.

Data extraction is divided into two categories: destructive testing and non-destructive testing. For destructive testing, chip-off may be used. Non-destructive testing consists of extracting data from forensic software using a Joint Test Action Group (JTAG) method. This study uses the least intrusive method, namely Forensic Toolkit® (FTK®). The study consists of an external examination, which looks at possible access ports on storage media (e.g., USB, SD card) and an internal examination, which looks at the printed circuit boards inside the drones. Raw data that is acquired is converted from the drones and ground stations to a readable file. There are many converter programs that are specifically designed for these specific drones. A disadvantage of many of these converter programs is that data must be uploaded to a site, which is not possible for case-related data.

The Align M690L is the only drone that stores any data unless a data logger has been purchased. The other drones include all data that have been extracted and analyzed using standard forensic software. It includes data about various assistance systems such as Global Positioning System (GPS), Gyro, Accelerator, and a barometer. The GPS coordinates can be plotted on a map to provide an escape route. The 3DR® IRIS+ contains waypoints that are pre-programmed and can be downloaded at any time. Imports logged on the remote controls are visible so that a statement can be made about a possible driver.

For several drones, the route flown can be extracted; however, the owner could not be found from the data extracted from the drone. Conventional forensic methods such as DNA and fingerprints of the drone might be used to find the owner of the drone. In further research, chip-off will be tested to determine if more information pertaining to the drone owner can be obtained.

Drone Forensics, UAV, Digital Investigation