COURSE DESCRIPTION

UAV (Drone) Forensics

Course Overview

This 32 hour Advanced level course will equip you with the practical skills and competencies required to identify and extract various sources of data recoverable from Unmanned Aircraft Systems (UAS), also known as Drones, including their associated control devices in line with approved best practices.

Using leading research and development from Spyder Forensics, this course will introduce you to the world of UAV's and instruct you how a Drone fly's followed by best practices in conducting forensically sound extractions and analysis of UAS data for use as evidence or intelligence gathering. Attendees will learn how to collect data from within the aircraft using non-destructive processes utilizing industry-standard tools to create forensic collections of storage media that include flight logs, aircraft data, photo, and video files without the need to disassemble the aircraft or controller. Students will then learn procedures in the acquisition of application data found on the mobile device.

Once data has been acquired, attendees will master how to analyze the flight logs and user data using software originally designed to work with these types of structures, gaining knowledge on workflows to connect data between the drone application and the flight data recovered from the aircraft.

This course uses non-destructive processes to extract and analyze the data from all hardware in the UAS including the handheld device, mobile application, and drone. Much of the software used in class can be utilized your DFIR lab free of charge and without the need to purchase additional applications to conduct a simple Drone examination.

Course Type
Specialized

Course Length
4 days

Course Code
UAV Analysis

Primary Learning Objectives

- Become proficient in the extraction of UAV controller data from mobile devices and UAV's using industry recognized forensic software.
- Recognize types of data available from drones, their linked devices and third-party sources.
- Conduct forensic extractions of data from the leading drone devices,
- analyze extracted data effectively to produce reports fit for use in criminal justice proceedings.
- Use CFID, Disero and Forensic software to extract and analyze UAV data

COURSE DESCRIPTION

Learning Module Outlines

- Introduction to UAV Forensics
    - Introduction to sUAS
    - Criminal use of UAV's
    - Manufacturers variables
    - Attack vectors – risks to public safety
    - Drone adaptation
    - Capacity and Capability of drones
    - Health and Safety – Handling and seizure
    - Health and Safety – LiPo Batteries
    - Linked devices – controller considerations
    - Digital vs. Physical Evidence
    - Packaging/Storage and continuity
    - Understanding of how flight logs are created and updated
        - Aircraft power on flowchart.

- Components of sUAS
    - Components and features of small unmanned aircraft systems (sUAS)
    - Controller options
        - Mobile and Tablet Devices
        - Bespoke flight controllers
        - Integrated displays
        - FPV controllers
    - Autonomous flights
        - Return-to-home feature
        - WiFi controls
        - Signal interception.

- Extraction techniques
    - First Responder Responsibilities
        - Securing the Evidence for Transport
    - Disassembling Techniques
    - Data sources and considerations
        - Extraction of data from the aircraft
        - Extraction of data from mobile \ tablet device
        - Extraction of controller data
    - Advanced extractions using a CFID and Disaro applications
    - Concepts in using FTP protocols to extract data
    - Exploitation of ADB connectivity

- Interpretation of data
    - Techniques in using opensource and commercial forensic tools to review the evidence
        - Interpretation of data contained on the UAV
            - File System considerations
            - Registered user information
            - Aircraft details
            - Flight log analysis techniques
        - Interpretation of data from portable devices
            - Default folder structures of the controlling app from an Android and iOS device
            - Synchronized logs vs. local logs
            - Error log analysis
            - Media file examination (geolocations and dates & times)
            - Workflows in combining offline files for further analysis
    - Techniques in the interpretation additional data on other devices.

- Advanced Analysis Techniques
    - Flight recorder “Black box”
    - Examination of Custom build aircraft flight controllers (PixHawk)
    - Examination of Smart controllers and 5G communications hardware
    - Advanced examination workflows using forensic tools designed for UAV Analysis
    - Linking hardware devices within the sUAS
    - Mapping of flight paths using Google Earth

- Presentation of Evidence capable of acceptance in court
    - Discussion on courtroom preparation and presentation
    - Overview of UAV report considerations
    - Glossary of terms
    - Report writing practical

- Final Assessment
    - Student knowledge assessment.

PREREQUISITES

To get the most out of this class, you should:

- Have minimal experience of forensic examinations.

CLASS MATERIALS AND SOFTWARE

You will receive a student manual, lab exercises, software for UAV analysis.

Students will have the ability to learn how to fly a UAV and collect data from the handset and aircraft.