THE WALDREP COMPANY

UAS / Drone Forensics

5-Day Advanced Training for Investigators & Forensic Examiners

Duration	Price per Seat	Certification	Prerequisites
5 Days (40 hrs)	$3,500 / seat	Certificate of Completion	Basic digital forensics or investigative backgr

Course Overview

This intensive 5-day course delivers the skills required to conduct court-ready forensic examinations of unmanned aerial systems (UAS) and drone platforms. Developed from real casework and refined through delivery to U.S. State Department ATA partner nations, this is the most operationally focused drone forensics training available. Participants leave with hands-on tool proficiency and a defensible methodology for any jurisdiction.

Learning Objectives

- Identify drone hardware architectures and data storage locations across major platforms
- Extract flight logs, GPS tracks, telemetry, and media using commercial and open-source tools
- Parse DJI, Parrot, Autel, and custom-build controller and cloud data
- Reconstruct flight paths and correlate with geospatial evidence
- Identify registration data, operator profiles, and remote ID signals
- Apply proper chain-of-custody procedures for drone evidence
- Produce court-accepted forensic reports for drone-related investigations
- Present findings as a qualified expert witness

Daily Schedule

Day / Module	Topics Covered
Day 1 Foundations	• UAS taxonomy: fixed-wing, multirotor, hybrid platforms • Regulatory framework: FAA Part 107, LAANC, Remote ID • Evidence recognition and scene documentation • Safe handling, battery safety, and evidence packaging • Legal authorities: search warrants, consent, exigent circumstances
Day 2 Data Acquisition	• Internal NAND/eMMC acquisition — hardware and software methods • SD card, controller, and companion app acquisition • DJI Go / DJI Fly app data on Android and iOS • Cloud sync artifacts: DJI FlightHub, AirData, SkyPixel • Drone ID and registration database lookups
Day 3 Flight Log Analysis	• DJI .DAT and .TXT log structure and parsing • Airdata, CsvView, and Phantom Help tools • GPS track reconstruction and Google Earth integration • Altitude, speed, and battery telemetry interpretation • Identifying tampering, log deletion, and firmware rollback

Day 4 Media & Advanced Analysis	• Photo/video metadata: EXIF, GPS, encoding artifacts • Camera sensor fingerprinting and image authentication • Parrot and Autel platform analysis • Open-source DIY/FPV drone forensics • Operator identification: account data, serial number tracing
Day 5 Reporting & Moot Court	• Forensic report writing standards for drone cases • Exhibit preparation: maps, timelines, and annotated imagery • Daubert and FRE 702 qualification requirements • Live moot court exercise — direct and cross-examination • Course exam and certificate presentation

Tools Covered

- Berla iVe (vehicle/controller module)
- Oxygen Forensic Detective (drone module)
- Cellebrite UFED (companion device extraction)
- DJI Assistant 2, DatCon, CsvView, Airdata UAV
- QGIS and Google Earth Pro (geospatial analysis)
- ExifTool, PhotoME, and FTK Imager

Who Should Attend

- Law enforcement investigators and digital evidence technicians
- Military and intelligence community personnel
- FAA safety inspectors and aviation security officers
- Private investigators and corporate security professionals
- Attorneys managing drone-related litigation

Logistics

- Format: Virtual (Zoom + lab environment) or In-Person (travel rates apply)
- Group rate: $2,800/seat for 8+ participants
- Government PO and net-30 invoicing accepted
- Custom on-site delivery available — contact for pricing
- All materials, tools, and lab images included
- CPE credits: 40 hours