

Mobile Device Forensics

3-Day Practitioner Course — iOS, Android & App Data

Duration	Price per Seat	Certification	Prerequisites
3 Days (24 hrs)	\$1,800 / seat	Certificate of Completion	Basic investigative or IT background

Course Overview

A hands-on, practitioner-focused course covering the full mobile forensics workflow from evidence receipt through court-ready reporting. Participants work with real iOS and Android devices using industry-standard tools. Emphasis is on defensible acquisition methods, artifact interpretation, and testimony-ready documentation — skills that hold up under cross-examination.

Learning Objectives

- Apply four acquisition tiers (logical, file system, physical, chip-off) and select appropriately
- Perform iOS full-file-system and advanced logical extractions
- Extract and decode Android physical images across major OEMs
- Analyze SMS, iMessage, WhatsApp, Signal, Snapchat, and 30+ app artifacts
- Recover deleted data, parse SQLite databases, and interpret plist files
- Geolocate activity using location history, Wi-Fi logs, and cell-site data
- Produce court-accepted mobile forensic reports

Daily Schedule

Day / Module	Topics Covered
Day 1 Acquisition	<ul style="list-style-type: none"> • Mobile evidence intake: documentation and chain of custody • Airplane mode, Faraday, and network isolation procedures • iOS acquisition: iTunes backup, logical, file system, and GrayKey overview • Android acquisition: ADB, EDL/Qualcomm, Samsung BL bypass concepts • Cellebrite UFED Touch 2 and 4PC hands-on lab • Magnet AXIOM Cyber acquisition workflow
Day 2 App & Data Analysis	<ul style="list-style-type: none"> • SQLite database parsing: contacts, calls, SMS, and app databases • iOS plist files: binary vs. XML, common artifacts • iMessage, FaceTime, and iCloud artifact correlation • WhatsApp, Telegram, Signal: msgstore.db and key extraction • Social media app artifacts: Facebook, Instagram, TikTok • Cloud account artifacts and remote data access

Day 3

Geolocation, Deleted Data & Reporting

- Location artifacts: Google Timeline, Apple Significant Locations, Wi-Fi logs
- Digital analysis fundamentals and CSLI evidence
- Deleted data recovery: SQLite WAL, unallocated carving
- Comprehensive report writing for mobile cases
- Courtroom preparation and cross-examination simulation
- Course assessment and certificate presentation

Tools Covered

- Cellebrite UFED 4PC and Physical Analyzer
- Magnet AXIOM and AXIOM Cyber
- Oxygen Forensic Detective
- DB Browser for SQLite
- iExplorer and 3uTools (iOS)
- ADB and Android Debug Bridge utilities

Who Should Attend

- Detectives and digital evidence technicians
- Federal agents and task force officers
- Corporate investigators and HR professionals
- Attorneys managing mobile device evidence
- Private investigators expanding mobile capabilities

Logistics

- Format: Virtual (Zoom + hosted lab) or In-Person
- Group rate: \$1,450/seat for 8+ participants
- Government PO and net-30 invoicing accepted
- CPE credits: 24 hours