

# Cellebrite Collection Acquisition and Triage

## Global Training



### Level

Intermediate

### Length

four (4) day

### Delivery Mode



Instructor  
Led



Live  
Online

### Course Description

The Cellebrite Collection Acquisition and Triage (C<sup>2</sup>AT) four (4) day course that combines the Cellebrite Certified Operator (CCO) and BlackBag Forensic Investigations (BFI) courses. Participants who attend and successfully complete the exam and knowledge assessments will earn two (2) certifications. The intermediate level program expands on forensic fundamental concepts by providing information essential to the collection of devices, the acquisition of data from devices, and the triaging of evidence using Cellebrite and BlackBag digital forensic solutions.

The C<sup>2</sup>AT program is ideal for professionals involved in extracting, authenticating, analyzing, and reporting on digital evidence found on computers or mobile devices. Instructor-led activities include device extractions/acquisitions, screen previews, evidence triage, and the operation of Cellebrite (Touch2/4PC), Reader, MacQuisition, and BlackLight solutions. Course participants will use multiple data intelligence tools to conduct basic searches, analyze data, mark (tag) digital artifacts, and create reports using Cellebrite and BlackBag solutions.

**Note:** No pre-requisites exist to attend the C<sup>2</sup>AT class, which can be taken to meet the second of three requirements, to qualify for the Cellebrite Certified Mobile Examiner (CCME) certification exam. The C<sup>2</sup>AT course is NOT available as a test-out option for those individuals seeking to achieve CCME pre-requisites.

Prior knowledge or use of BlackBag's BlackLight, MacQuisition, Cellebrite Touch2, or 4PC is not required to take this course but, it is recommended that students have completed the Cellebrite Mobile Forensics Fundamentals (CMFF), course or test out, prior to this class.

## Learning Tracks

Cellebrite aims to support learners in the pursuit of excellence in Digital Intelligence specialty areas without the need to commit to any degree program. Cellebrite's Academic & Learning Tracks provide guided training programs and continuous skillset development to achieve various levels of educational or professional goals. By choosing a "track" or "learning path" students can focus on personal, professional, and leadership skills in a Digital Intelligence career for either law enforcement, military, intelligence, and private sector practitioners.

Below is general information related to the audiences and focus areas for professionals taking this course. Cellebrite's curriculum reflects our commitment to digital forensics excellence; training forensics examiners, analysts, investigators and prosecutors around the world to achieve a higher standard of professional competence and success.

The C<sup>2</sup>AT training is designed for the following professionals:

- CSI Staff
- Digital Forensic Examiners
- Forensics Staff
- Investigators
- Corporate Investigators
- Technicians

## Course Objectives and Module Topics

The successful completion of Cellebrite Collection Acquisition and Triage C<sup>2</sup>AT will result in two certifications, aimed at augmenting your professional portfolio as outlined by the individual course objectives listed below.

### CCO Course Objectives

Upon successful completion of the course, the student will be able to:

- Describe pre-extraction considerations.
- Install and configure Touch, Touch 2, or 4PC and Physical Analyzer software.
- Explain the best practices for the on-scene identification, collection, packaging, transporting, examination, and storage of digital evidence data and devices.
- Display best practices when conducting cell phone extractions.
- Identify functions used within Touch, Touch 2, or 4PC to perform supported data extractions.
- Exhibit how to open extractions using Physical Analyzer.

- Summarize how to conduct basic searches using Cellebrite Physical Analyzer.
- Outline how to create a Triage report using Cellebrite Physical Analyzer.
- Demonstrate proficiency by completing a knowledge-based and practical skills assessment.

## BFI Course Objectives

Upon successful completion of the course, the student will be able to:

- Explain Live Triage and Imaging procedures.
- Describe the features and functions of MacQuisition.
- Perform multiple Case Study reviews
- Examine macOS and iOS artifacts
- Explore the processing of Microsoft Windows in BlackLight
- Identify, Tag and Annotate extracted data
- Generate investigative Reports
- Demonstrate proficiency by completing a knowledge-based skills assessment

## CCO Modules Topics

Module	Topics
Module 1: Introduction	<ul style="list-style-type: none"><li>• Discuss course administration.</li><li>• Describe Cellebrite's core training and certification process.</li><li>• Review of the capabilities engineered in the Cellebrite Platforms and digital forensic solutions.</li><li>• Discuss a practitioner's legal responsibilities using Cellebrite products, software, and services.</li></ul>
Module 2: Forensic Handling of Mobile Devices	<ul style="list-style-type: none"><li>• Install 4PC and review licensing options</li><li>• Install Physical Analyzer and review licensing options</li><li>• Describe the phases of the digital forensics process</li><li>• Populate data on an Android phone to complete extractions</li><li>• Conduct Logical extractions of mobile devices</li><li>• Review legal considerations for seizing and searching devices</li><li>• Describe the importance of proper evidence handling and documentation</li></ul>

Module	Topics
Module 3: Touch2 and 4PC Familiarization	<ul style="list-style-type: none"> <li>• List the components, features, or functions for the Touch2 and 4PC.</li> <li>• Describe how to purchase and maintain the license(s) for UFED technology.</li> <li>• Discuss how to update software and firmware for Touch2 and 4PC.</li> <li>• Conduct an installation of 4PC on a computer workstation.</li> <li>• Modify Touch2 and 4 PC configurations for the extraction of different devices and investigative needs.</li> </ul>
Module 4: Cellebrite Extraction Methodologies	<ul style="list-style-type: none"> <li>• Identify best practices for the extraction of data from digital evidence devices.</li> <li>• Discuss the methods frequently employed by forensic examiners to acquire data from mobile devices.</li> <li>• Explain the SIM file system organization.</li> <li>• Conduct SIM card extractions and cloning comparisons.</li> <li>• Apply forensic techniques to produce media storage extractions.</li> <li>• Operate the Touch2 or 4PC, and Physical Analyzer to conduct device extractions.</li> <li>• Demonstrate the removal of a passcode from a locked device using Touch2 or 4PC.</li> <li>• Describe the uses for UFED Camera Services.</li> </ul>
Module 5: Triage Reporting	<ul style="list-style-type: none"> <li>• Explain the fundamental elements of a Reader (UFDR) report produced by Physical Analyzer.</li> <li>• Describe the reporting options within the Physical Analyzer interface.</li> <li>• Compose PDF and UFDR reports using digital evidence artifacts recovered during mock investigations.</li> </ul>
Module 6: Final Exam	<ul style="list-style-type: none"> <li>• Complete a knowledge-based and practical skills assessment</li> <li>• Evaluate the course components using the Feedback Survey</li> <li>• Download a Certificate of Attendance</li> <li>• Download a Certificate of Completion (if awarded)*</li> </ul>

## BFI Modules Topics

Module	Topics
Module 1: Introduction	<ul style="list-style-type: none"> <li>• Discuss course administration</li> <li>• Describe BlackBag's training and certification process</li> <li>• Review of the capabilities of BlackBag's Platforms and digital forensic solutions</li> <li>• Recognize the legal responsibility in using BlackBag's products and services</li> </ul>
Module 2: Acquiring Data	<ul style="list-style-type: none"> <li>• Discuss MacQuisition Features and Functions</li> <li>• Explain Logical File Collection Procedures</li> <li>• Describe Apple Encryption</li> <li>• Review Imaging Processes for Different Media</li> <li>• Explore the Investigations Workflow Overview</li> <li>• Discuss the Proper Handling of Digital Case Evidence</li> </ul>
Module 3: BlackLight Introduction	<ul style="list-style-type: none"> <li>• Provide an Introduction to the BlackLight Interface</li> <li>• Describe the System Requirements</li> <li>• Discuss Program Dependencies</li> <li>• Explain how to Create a Case and Add Evidence</li> <li>• Review how to Open an existing Case</li> </ul>
Module 4: BlackLight Features and Functions	<ul style="list-style-type: none"> <li>• Explore the BlackLight Interface</li> <li>• Review the procedure for marking evidence</li> <li>• Describe the purpose of the Component List</li> </ul>
Module 5: Processing Options	<ul style="list-style-type: none"> <li>• Review Mac Artifacts and Processing</li> <li>• Discuss Windows Artifacts and Processing</li> <li>• Practice Viewing Artifacts</li> <li>• Create Artifact Filters</li> <li>• Explain the Importance of Metadata</li> </ul>
Module 6: Tagging Items of Interest	<ul style="list-style-type: none"> <li>• Explain How to Tag Items of Interest</li> <li>• Practice Tagging Item of Interest</li> <li>• Discuss Tagging Multiple Items Simultaneously</li> <li>• Explain the Value of Tagging in Hex View</li> </ul>

Module	Topics
Module 7: Data Filtering and Cultivation	<ul style="list-style-type: none"> <li>• Discuss the Data Filtering</li> <li>• Explore the Use of Content Searches</li> <li>• Review the Use of Custom Hash Sets</li> <li>• Explained How to Complete Indexed Searches</li> <li>• Practice Searches by Content Types</li> </ul>
Module 8: Developing Actionable Intelligence	<ul style="list-style-type: none"> <li>• Discuss the Actionable Intelligence Tab</li> <li>• Explain the Parsing of Mac and Windows Artifacts</li> <li>• Practice Navigating to Actionable Intelligence Tab and Completing Searches</li> <li>• Explore Mac Actionable Intelligence Artifacts</li> <li>• Review Windows Actionable Intelligence Artifacts</li> <li>• Compare the Differences Between Preview Data and Actionable Intelligence Data</li> </ul>
Module 9: Media	<ul style="list-style-type: none"> <li>• Review Media View Filtering and Organization</li> <li>• Explain GeoData Markers and Mapping</li> <li>• Practice Video file GeoData Mapping</li> <li>• Discuss Exporting Images for Review</li> <li>• Describe the Uses for Image Analyzer to Establish Categories and Assess Threat Levels</li> </ul>
Module 10: Mobile	<ul style="list-style-type: none"> <li>• Explain the Android Acquisition Process</li> <li>• Discuss the iOS Acquisition Process</li> <li>• Describe the iOS Backups Data Acquisition Method</li> <li>• Review the Methods for Ingesting 3rd Party Acquisitions</li> </ul>
Module 11: Data Analysis	<ul style="list-style-type: none"> <li>• Describe Automated and Manual Productivity Features</li> <li>• Review the parsing of communications that include Mac call records</li> <li>• Practice Filtering Application Communication Records</li> <li>• Parse Locations Data from Media, Calendar, and Other Sources</li> <li>• Explain the Internet Connections and Browsing Data</li> <li>• Explain the Case Data Analysis and Reporting Features</li> </ul>
Module 12: Reporting (supplemental resources)	<ul style="list-style-type: none"> <li>• Practice Choosing Report Items</li> <li>• Review the Function that Permits Rearranging Tags for Reporting</li> </ul>
Module 13: Other Topics	<ul style="list-style-type: none"> <li>• Review Updated Features and Functions</li> <li>• Explain the Integration and Ability to Parse 3rd Party Data Acquisitions</li> <li>• Describe the BitLocker Integration Procedure</li> </ul>

Module	Topics
Module 14: Final Exam	<ul style="list-style-type: none"><li>• Complete a knowledge-based assessment</li><li>• Evaluate the course components using the Feedback Survey</li><li>• Download a Certificate of Attendance</li><li>• Download a Certificate of Completion (if awarded)*</li></ul>

## Additional Information

Cellebrite Collection Acquisition and Triage (C<sup>2</sup>AT) is:

- an opportunity to achieve Cellebrite's Certified Operator (CCO) Certification below CCPA
- an opportunity to achieve BlackBag's Certified BlackLight Examiner (CBE) designation
- essential "toolkit" solution for professionals that handle or acquire data from various devices
- ideal for individuals with basic knowledge in digital forensics or successfully completed Cellebrite's CMFF

**Important:** Successful completion of this course is defined as the student being able to demonstrate proficiency in the Course Learning Objectives by passing a Final Exam assessment with a minimum score of 80.00% or higher to be awarded a Certificate of Completion.

Get skilled. Get certified.

Every day around the world, digital data is impacting investigations. Making it intelligent and actionable is what Cellebrite does best. The Cellebrite Academy reflects our commitment to digital forensics excellence; training forensics examiners, analysts, investigators and prosecutors around the world to achieve a higher standard of professional competency and success.

Learn more at [cellebritelearningcenter.com](https://cellebritelearningcenter.com)

The materials and topics provided herein are provided on an "as is" and "as available" basis without any warranties of any kind including, but not limited to warranties of merchantability, fitness for a particular purpose or guaranties as to its accuracy or completeness. Please note that some materials, topics and items provided herein are subject to changes. Cellebrite makes no warranties, expressed or implied, for registered trademarks of Cellebrite in the United States and/or other countries. Other trademarks referenced are property of their respective owners. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.