Cellebrite Collection Acquisition and Triage

Global Training

Level

Intermediate

Length

Four-Day (28 hours)

Delivery Mode

Instructor Led

Live Online

Course Description

The Cellebrite Collection Acquisition and Triage (C2AT) course is a combination of Cellebrite's CCO (Cellebrite Certified Operator) and BlackBag's BFI (Basic Forensic Investigations) to bring you a Four-Day (28 hours) Intermediate level program. C2AT expands on concepts introduced in Cellebrite Mobile Forensic Fundamentals (CMFF) while introducing extractions and data sets using both Cellebrite and BlackBag products and software. The combined program of CCO and BFI is ideal for professionals working in or seeking to work in areas related to mobile and desktop investigation or data extraction teams.

The CCO portion of the program is designed for investigators to learn about mobile devices, understand general ideas of the forensic process, learn how to seize devices, and review extracted device data using Cellebrite's Touch2 or 4PC solutions. Participants are introduced to baseline concepts and prerequisite knowledge to understand issues surrounding the handling of mobile devices as evidence while not including data extractions.

The BFI portion of the program is designed for data extraction team members, tasked with extracting data using BlackBag's BlackLight or MacQuisition software. Participants will perform a triage analysis of a full case using digital forensic concepts and advanced functions of BlackBag software while taking a hands-on investigative approach to extract, authenticate, analyze, and report on digital evidence found on computers or smartphone devices running a variety of operating systems. BFI involves the seizure and imaging of Apple computer systems along with the analysis of Apple, Windows, and iOS data using BlackBag software.

Cellebrite Digital intelligence for a safer world

Release Date: 06 1AY 2020

The C2AT course introduces extractions and data sets for use case scenarios both on mobile and desk or laptop devices. The overall focus of is on-screen previews, evidence triage, and operating Cellebrite (Touch2/4PC), MacQuisition, and BlackLight solutions. Course participants will use multiple data intelligence tools to conduct basic searches, analyze data, create bookmarks or tags, and reports in both Cellebrite and BlackBag software. Throughout the course, participants have opportunities to gain the fundamental understanding needed to triage evidence and analyze data extractions in various case scenarios.

Note: No pre-requisites exist to attend the C2AT class, which can be taken to meet the second of three requirements, to qualify for the Cellebrite Certified Mobile Examiner (CCME) certification exam. The C2AT course is NOT available as a test-out out option for those individuals seeking to achieve CCME pre-requisites.

Prior knowledge or use of BlackBag's BlackLight, 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 C2AT 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 (C2AT) 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 the collection of Mac 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 and practical skills assessment

CCO Modules Topics

Module	Topics
Module 1: Introduction	• Discuss course administration. • Describe Cellebrite's core training and certification process. • Review of the capabilities engineered in the Cellebrite Platforms and digital forensic solutions. • Discuss a practitioner's legal responsibilities using Cellebrite products, software, and services.
Module 2: Forensic Handling of Mobile Devices	• Install 4PC and review licensing options • Install Physical Analyzer and review licensing options • Describe the phases of the digital forensics process • Populate data on an Android phone to complete extractions • Conduct Logical extractions of mobile devices • Review legal considerations for seizing and searching devices • Describe the importance of proper evidence handling and documentation
Module 3: Touch2 and 4PC Familiarization	• List the components, features, or functions for the Touch2 and 4PC. • Describe how to purchase and maintain the license(s) for UFED technology. • Discuss how to update software and firmware for Touch2 and 4PC. • Conduct an installation of 4PC on a computer workstation. • Modify Touch2 and 4 PC configurations for the extraction of different devices and investigative needs.
Module 4: Cellebrite Extraction Methodologies	• Identify best practices for the extraction of data from digital evidence devices. • Discuss the methods frequently employed by forensic examiners to acquire data from mobile devices. • Explain the SIM file system organization. • Conduct SIM card extractions and cloning comparisons. • Apply forensic techniques to produce media storage extractions. • Operate the Touch2 or 4PC, and Physical Analyzer to conduct device extractions. • Demonstrate the removal of a passcode from a locked device using Touch2 or 4PC. • Describe the uses for UFED Camera Services.

Module	Topics
Module 5: Triage Reporting	• Explain the fundamental elements of a Reader (UFDR) report produced by Physical Analyzer. • Describe the reporting options within the Physical Analyzer interface. • Compose PDF and UFDR reports using digital evidence artifacts recovered during mock investigations.
Module 6: Final Exam	• Complete a knowledge-based and practical skills assessment • Evaluate the course components using the Feedback Survey • Download a Certificate of Attendance • Download a Certificate of Completion (if awarded)*

BFI Modules Topics

Module	Topics
Module 1: Introduction	• About BlackBag • Introducing BlackBagTech.com • Participants self-Introduction • Training and Certifications • Description of BlackBag Products • Course objectives, schedule, and logistics
Module 2: Acquiring Data	• Discuss MacQuisition Features and Functions • Explain Logical File Collection Procedures • Describe Apple Encryption • Review Imaging Processes for Different Media • Explore the Investigations Workflow Overview • Discuss the Proper Handling of Digital Case Evidence
Module 3: BlackLight Introduction	• Provide an Introduction to the BlackLight Interface • Describe the System Requirements • Discuss Program Dependencies • Explain how to Create a Case and Add Evidence • Review how to Open an existing Case

Module	Topics
Module 4: Exploring BlackLight	• Explore the BlackLight Interface • Review the procedure for marking evidence • Describe the purpose of the Component List
Module 5: Actionable Intelligence	• Review Mac Artifacts and Processing • Discuss Windows Artifacts and Processing • Practice Viewing Artifacts • Create Artifact Filters • Explain the Importance of Metadata
Module 6: Advanced Options	• Explain How to Tag Items of Interest • Practice Tagging Item of Interest • Discuss Tagging Multiple Items Simultaneously • Explain the Value of Tagging in Hex View
Module 7: Media Analysis	• Discuss the Data Filtering • Explore the Use of Content Searches • Review the Use of Custom Hash Sets • Explained How to Complete Indexed Searches • Practice Searches by Content Types
Module 8: Mobile Device	• Discuss the Actionable Intelligence Tab • Explain the Parsing of Mac and Windows Artifacts • Practice Navigating to Actionable Intelligence Tab and Completing Searches • Explore Mac Actionable Intelligence Artifacts • Review Windows Actionable Intelligence Artifacts • Compare the Differences Between Preview Data and Actionable Intelligence Data
Module 9: Communications	• Review Media View Filtering and Organization • Explain GeoData Markers and Mapping • Practice Video file GeoData Mapping • Discuss Exporting Images for Review • Describe the Uses for Image Analyzer to Establish Categories and Assess Threat Levels

Module	Topics
Module 10: Narrowing Down the Data	• Explain the Android Acquisition Process • Discuss the iOS Acquisition Process • Describe the iOS Backups Data Acquisition Method • Review the Methods for Ingesting 3rd Party Acquisitions
Module 11: Tagging	• Describe Automated and Manual Productivity Features • Review the parsing of communications that include Mac call records • Practice Filtering Application Communication Records • Parse Locations Data from Media, Calendar, and Other Sources • Explain the Internet Connections and Browsing Data
Module 12: Reporting	• Explain the Case Data Analysis and Reporting Features • Practice Choosing Report Items • Review the Function that Permits Rearranging Tags for Reporting
Module 13: Other Topics	• Review Updated Features and Functions • Explain the Integration and Ability to Parse 3rd Party Data Acquisitions • Describe the BitLocker Integration Procedure
Module 14: Final Exam	• Complete a knowledge-based and practical skills assessment • Evaluate the course components using the Feedback Survey • Download a Certificate of Attendance • Download a Certificate of Completion (if awarded)*

Additional Information

Cellebrite Collection Acquisition and Triage (C2AT) 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

C²AT
Rev 22 May 2020 (En)