# CELLEBRITE APPLE ADVANCED FORENSICS (CAAF)

## Computer Forensics, Investigative

**Cellebrite**

## Level

Advanced

## Length

Three-Day (21 hours)

## Training Track

Computer Forensics
Investigative

## Delivery Mode

Instructor-Led
Live Online

## Course Description

Cellebrite Apple Advanced Forensics (CAAF) is a three (3)-day, course designed with hands-on learning and real case scenario data using Cellebrite Inspector software. Participants will learn how to recover artifacts from allocated and unallocated space. A CAAF instructor will review the most important macOS and iOS digital artifacts common to most investigations. The advanced instruction includes a comprehensive exploration of macOS and iOS systems, deleted files from HFS+ and APFS file systems, hardware and software RAIDS, log files, extended artifacts and password data.

## Computer Forensics, Mobile Forensics, Investigative

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 Paths provide guided training programs and continuous skill set development to achieve various levels of educational or professional goals.

By following a learning path, students can target personal, professional, and leadership skills in a Digital Intelligence career for law enforcement, military, intelligence, and private sector practitioners. Cellebrite's curriculum reflects its commitment to digital intelligence excellence by helping  training forensics examiners, analysts, investigators and prosecutors around the world to achieve a higher standard of professional competence and success. Below are general audiences and focus areas relative to this course.

- Digital Forensic Examiners

## Course Learning Objectives

- Distinguish how to handle deleted files from both APFS and HFS+.
- Demonstrate how to recover artifacts from allocated and unallocated space.
- Breakdown hardware and software RAID.
- Understand iOS analysis advanced practices.
- Utilize log files to recreate usage history and create a timeline.
- Understand and examine Extended Attributes, Spotlight evidence, and file sharing artifacts.
- Identify and utilize how passwords are saved and used in macOS.

### DELETED FILES AND RECOVERING ARTIFACTS

- Distinguish the differences and handling of deleted files by APFS and HFS+
- Explain the difference between the .Trash and .Trashes folder
- Recall how files get deleted in macOS
- Create queries to successfully locate specific artifacts from macOS carved files

### IOS ANALYSIS

- Explain the advanced practice for mobile device iOS analysis
- Explain iOS Security
- Interpret SIM Card information on iOS devices
- Analyze RECENTS database from an iOS device
- Interpret iOS usage information
- Examine Photos application artifacts showing iCloud photo sharing

**Cellebrite**

## LOG FILES

- Define and discuss the use of Log Files to recreate usage history
- Describe Apple unified logs
- Explain how to collect unified logs Analyze unified logs from Apple devices using Cellebrite Inspector
- Explain how to collect Sysdiagnose Logs from macOS and iOS devices
- Identify the difference between short-term and long-term ASL files
- Analyze other logs from macOS computer

## FILE SYSTEM EVENTS

- Explain the automatic logging of file system events
- Describe FSEVENTS
- Identify the value of FSEVENTS in forensic analysis
- Analyze FSEVENTS in a disk image

## EXTENDED ATTRIBUTES SPOTLIGHT AND FILE SHARING

- Discuss extended attributes, Spotlight, and file sharing

Cellebrite

# 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

EMEA | London, UK

EMEA | München, Germany

USA | Vienna, Virginia

USA | Las Vegas, Nevada

USA | San Jose, California

APAC | Singapore

Cellebrite

Cellebrite Apple Advanced Forensics