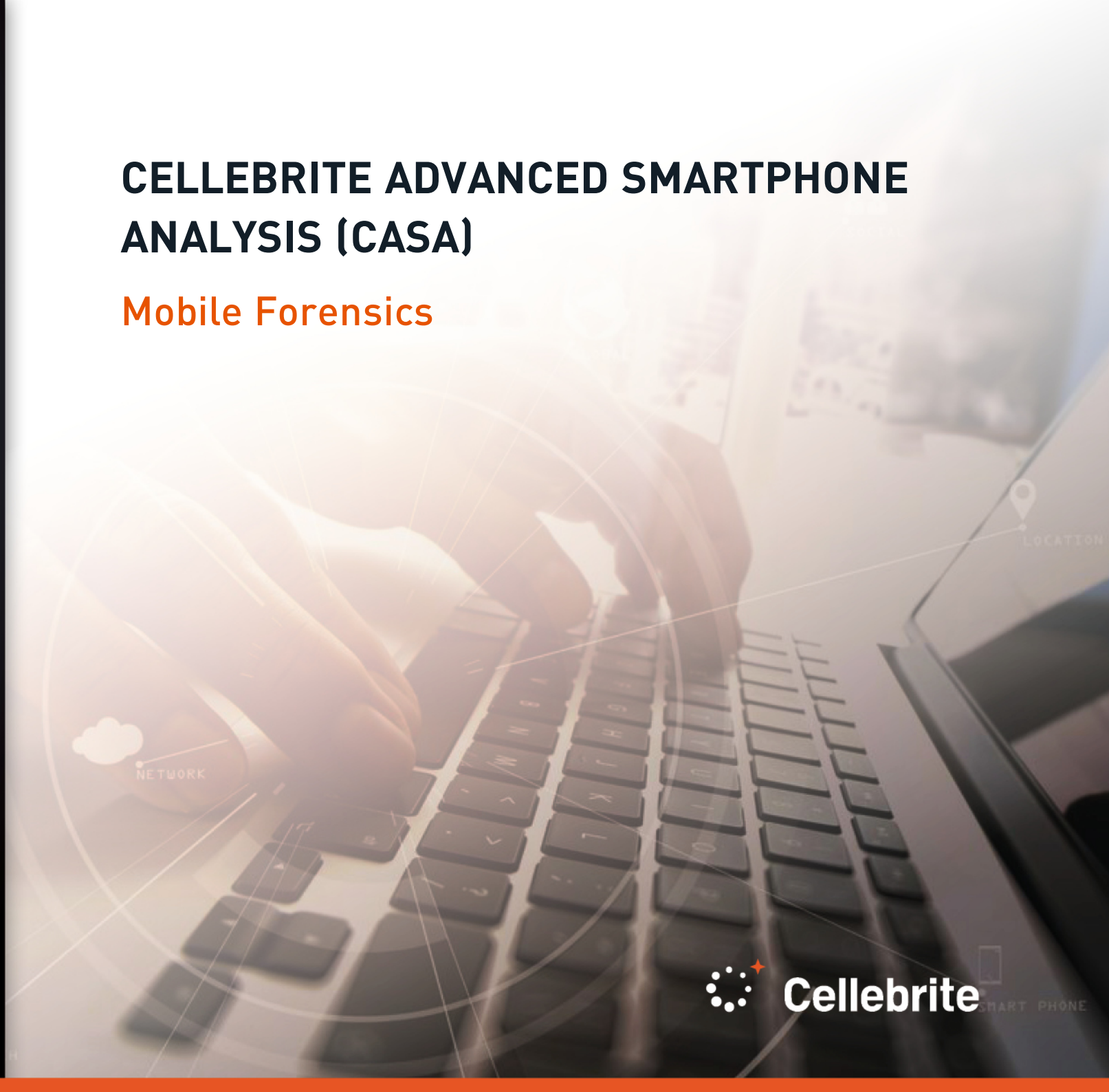
CELLEBRITE ADVANCED SMARTPHONE ANALYSIS (CASA)

Mobile Forensics



Cellebrite

Level

Expert

Length

Four-Day (28 hours)

Training Track

Mobile Forensics

Delivery Mode

Instructor-Led
Web-Based
Live Online

Course Description

Cellebrite Advanced Smartphone Analysis (CASA) class is four (4) day expert level course designed to provide training in forensic recovery of application data from smartphones. The CASA class is recommended for practitioners familiar with Physical Analyzer and graduates of the CCPA course. In the CASA course, participants will learn how to decode information not commonly decoded by forensic tools. Attendees will also use third-party software and Python scripts to decode, analyse, verify, and validate findings.

Mobile Forensics

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 skill set development to achieve various levels of educational or professional goals.

By following a "learning track" or "training 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 professionals around the world achieve a higher standard of competence and success. and training around the world by empowering heroes with smart solutions. Below are general audiences and focus areas relative to this course.

- Digital Forensic Examiners

Cellebrite

Course Learning Objectives

Upon successful completion of this course, students will be able to:

- Recognize smart devices
- Recover and bypass password locks
- Understand smart device file systems
- Understand database structures as used by smart devices
- Understand Property List and Registry structures
- Locate common artifacts on smart devices.

Note: The Cellebrite Certified Physical Analyst (CCPA) certification is a pre-requisite to attend the CASA class. The CCPA course is NOT available as a test-out option for those individuals seeking to achieve CASA pre-requisites.

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.

INTRODUCTION

In this module, you will learn about Cellebrite's products, services, training, and certification processes available under Cellebrite's Training programs. Learners will be introduced to the course objectives, requirements, and administrative options to establish the foundation to succeed in your educational or professional goals. You will use the Cellebrite Learning Center and CelleConnect Portal to connect with various resources.

SQLITE DATABASE STRUCTURES

In this module, you will learn about write-ahead log and shared memory files, binary large objects handling, free page lists and free page handling, the vacuum function, and how table data is joined. You will use practical, hands-on exercises using Cellebrite Physical Analyzer and verify their findings using other software tools.

- Identify SQLite databases.
- Recognize SQLite database structures and possible applications.
- Identify the data storage method for SQLite databases.
- Examine SQLite databases and how tables are joined together.
- Describe the events related to the deletion of data from an SQLite database.
- Recall databases performance behaviors capable of destroying data.
- Illustrate the use of practical skills and knowledge necessary to perform logic based Fuzzy Modeling procedures.

IOS OVERVIEW AND ANALYSIS

In this module, you will learn what occurs during the extraction process of an iOS device and best practices for seizing and storing devices. We will show you how applications are stored, accessed, and various ways to decode information found in binary plist files. You will also learn about date and time encoding schemes and using several hands-on practical exercises you will examine numerous files of interest.

- Briefly recount the evolution of iOS.
- Learn how to properly seize iOS devices
- Describe the structure of the iOS file system.
- Analyze applications and relevant data
- Identify Property List structures
- Gain additional artifacts from Safari

IOS ADVANCED ANALYSIS

In this module, you will analyze the newest artifacts recovered as part of your iOS extractions and how to utilize them fully in your investigations. This module applies context to analyzed data, moving beyond just "reporting" and teaching you to draw reliable conclusions from presented evidence.

- Examine KnowledgeC, Screentime, Data Usage artifacts, and diagnostic logs
- Use Cellebrite to generate and annotate a single timeline of events from multiple devices, painting a snapshot of what occurred.
- Learn the various sources of geolocation data, their meaning, and incorporating them into your case.
- Complete a challenging scenario, a culmination of what you learned about iOS forensics.

IOS AND ICLOUD BACKUPS

In this module, you will learn about iOS backups found on computer systems, encrypted iOS extractions, and what kind of information can be contained within them. We will discuss backup file encryption and decryption using open source tools, iCloud backups, and decoding.

- Location of iOS backup files
- Naming convention an iOS backup
- Handling Encrypted iOS Backup and Extractions
- iCloud Evidence
- Processing an iOS Backup

ANDROID OVERVIEW

In this module, you will learn about important Android system artifacts. You will learn about obtaining data that documents wireless networks, time zone settings, mounted file systems, SD Card usage, Bluetooth information, and operating system versions; this information may prove critical to the investigation.

ANDROID OVERVIEW

- The evolution of Android OS.
- Android file systems and encryption.
- Cellebrite UFED support for Android Extraction and analysis.
- Extractions methods from Android devices.

ANDROID SYSTEM ARTIFACTS

In this module, you will learn about important Android system artifacts. You will learn about obtaining data that documents wireless networks, time zone settings, mounted file systems, SD Card usage, Bluetooth information, and operating system versions; this information may prove critical to the investigation.

- Learn the various folders and their relevance on Android devices
- Understand Android multiple users
- Interpret SIM Card data
- Interpret various types of device and user tracking artifacts
- Install and use aLEAPP to triage and view various data sets
- Use Fuzzy Modeling to gain additional insights into location data

ANDROID USER ARTIFACTS

In this module, you will learn about artifacts created by the user's interaction with different applications on the Android device. Using hands-on practical exercises, you will examine Google Maps data, unsupported applications, and artifacts that store data about user activity which provides a challenge for tools to interpret.

ANDROID USER ARTIFACTS

- Learned the structure and to decode Android applications
- Processed installed applications
- Analyzed the Android Messaging app and SMS/MMS
- Used Android Well Being
- Processed Internet history
- Decoded Google Maps
- Used the location carver and validate results

FINAL EXAM

In this module, you will be offered an optional, and examination. Successful completion of the exam with a passing score of at least 80.00% will result in a certification credential and attendance credit. Completion of the course without a passing score awards the student a Certificate of Attendance, only.

- Complete a knowledge-based exam and practical skills assessment
- Evaluate the course components using the Feedback Survey
- Download a Certificate of Attendance
- Download a Certificate of Completion (if awarded)*

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

Cellebrite

Cellebrite Advanced Smartphone Analysis