



CELLEBRITE APPLE FORENSICS (CAF)

Computer Forensics , Investigative



Level

Intermediate



Length

Five-Day (35 hours)



Training Track

Computer Forensics
Investigative



Delivery Mode

Instructor-Led
Web-Based
Live Online

Course Description

Cellebrite Apple Forensics (CAF) is a five (5)-day, course designed with hands-on learning and real case scenario data. Participants will learn how to perform both triage and analysis of specific data points that exist within operating system and file system artifacts. An CAF instructor will guide attendees through the most important macOS and iOS digital artifacts. The macOS and iOS operating systems, HFS+ and APFS file systems and significant application data are explored throughout the class.

Computer 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 professionals around the world achieve a higher standard of competence and success. Below are general audiences and focus areas relative to this course.

- Digital Forensic Examiners

Course Learning Objectives

FUNCTIONS OF THE EFI



- Recognize Apple computer start-up functions.
- Explain the purpose of disk sharing modes.
- Recognize a Mac computer in safe sleep mode

TRIAGE AND IMAGING



- Recognize the macOS live environment.
- Demonstrate using Cellebrite Digital Collector.
- Review and identify the various.
- Apple computer disk configurations.
- Explain how the various forms of encryption affects disk imaging and data acquisition.

SYSTEM OVERVIEW



- Recognize Apple computer structures.
- Describe how the structure of macOS affects analysis.
- Describe the value and purpose of FileIDs and Catalog Node IDs.
- Explain how macOS handles PLIST files.
- Analyze data contained with PLIST files on macOS.
- Use SQLite queries to enhance your forensic analysis.

TIME ZONE ANALYSIS



- Identify services using location services in macOS.
- Locate time zone settings in macOS .
- Analyze date and time preferences.

DISK IMAGES



- Define how Apple Disk Images are used .
- Demonstrate how to make Apple Disk Images .
- Differentiate between the types of Apple Disk Images.
- Discover methods to mount troublesome disk images.

INTERNET



- Identify web browser data in macOS.
- Describe the purpose of containers in macOS.
- Interpret data found within Safari web history.
- Discover extended attributes found in files downloaded on a macOS computer.
- Analyze internet artifacts from Safari, Firefox and Chrome.

MEDIA ANALYSIS



- Describe the default locations of media files in macOS.
- Recognize how Photos application stores files in macOS.
- Examine data from Photos application.
- Describe the affects of iCloud on Photos application.
- Analyze extended attributes of media files in macOS.

DEVICE CONNECTION ARTIFACTS



- Describe how volumes are mounted in macOS.
- Analyze macOS for evidence of mounted volumes.
- Determine Bluetooth connected devices in macOS.
- Analyze network connections in macOS.
- Examine AirDrop artifacts in macOS.

ICLOUD



- Describe iCloud as a service in macOS and iOS.
- Analyze iCloud account information and services in macOS.
- Recognize files shared through iCloud file sharing.
- Analyze iCloud data from Apple.

IOS ANALYSIS



- Describe how iOS locks can affect analysis.
- Identify an iOS backup on a local computer.
- Differentiate between the iOS acquisition methods.
- Analyze crucial iOS device data to show how the device has been used.

EMAIL FORENSICS



- Describe how Apple Mail stores mail data.
- Identify email messages with attachments.
- Describe the purpose of the Mail Downloads folder.
- Analyze data in the Envelope Index file.

BOOT CAMP



- Describe how Bootcamp is installed on Apple computers.
- Demonstrate how the start-up manager works on Apple computers.
- Recognize that Apple computers can contain numerous operating systems.

REPORTING



- Recognize the elements of a concise report.
- Demonstrate how to refine tagged artifacts to maximize their value.
- Demonstrate creating a report in Cellebrite Inspector.



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 Apple Forensics

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.