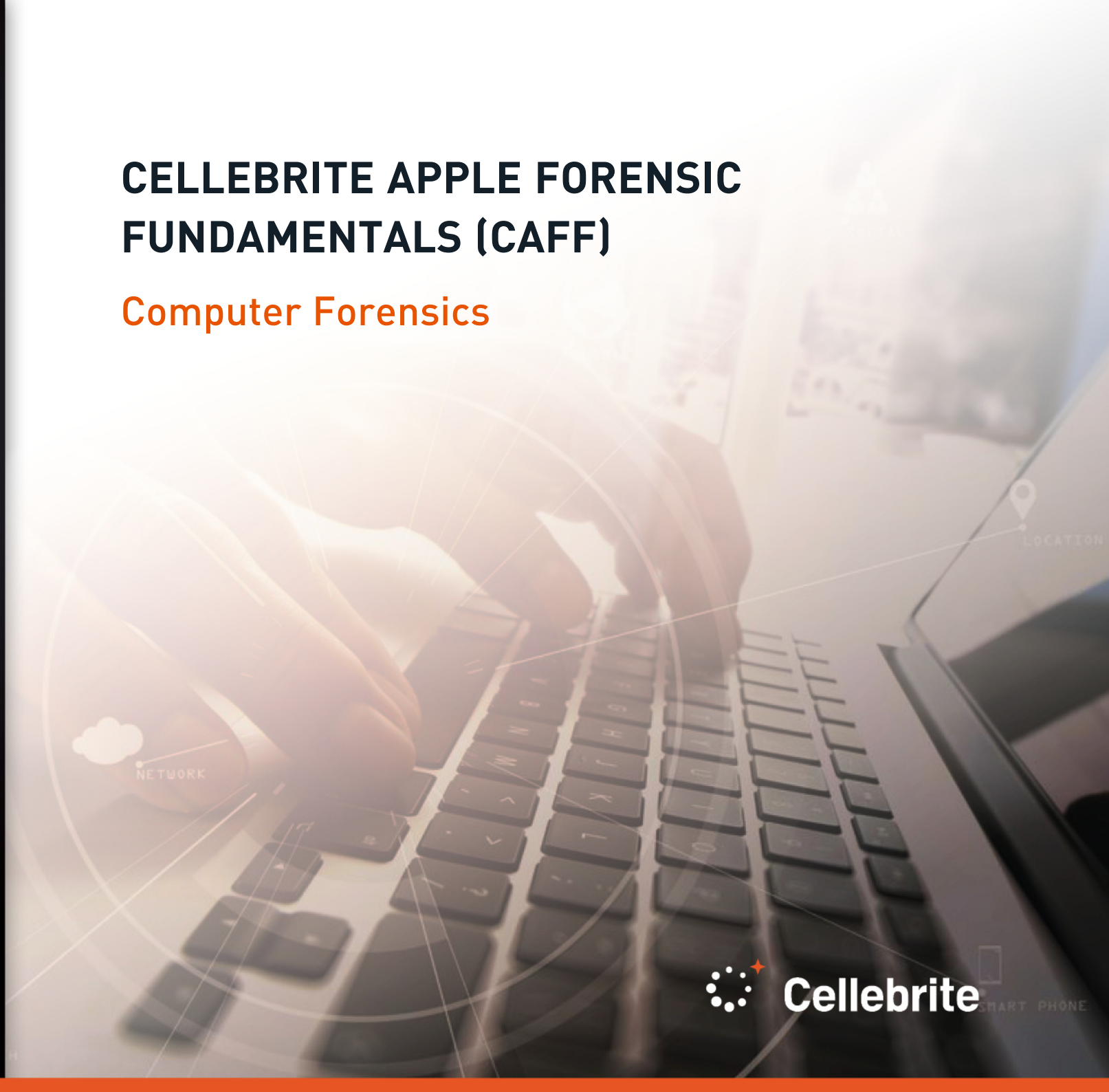
CELLEBRITE APPLE FORENSIC FUNDAMENTALS (CAFF)

Computer Forensics



Cellebrite

Level

Entry/Beginner

Length

Four-Day (28 hours)

Training Track

Computer Forensics Investigative

Delivery Mode

Instructor-Led
Live Online

Course Description

Cellebrite Apple Forensic Fundamentals (CAFF) is a four (4)-day, course designed with hands-on learning and real case scenario data using Cellebrite Digital Collector and Inspector software. Participants will learn how to perform both triage and analysis of specific data points that exist within operating system and file system artifacts. A CAFF instructor will guide attendees through the most important macOS and iOS digital artifacts. Participants will analyze mounted volume evidence, device connection evidence, and network connections in macOS. 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 Below are general audiences and focus areas relative to this course.

Course Learning Objectives

- Distinguish between the startup procedures for the various types of Apple computers.
- Develop a plan of attack to successfully triage and image Apple computers.
- Describe macOS structures and the limitations that each present.
- Explain the importance of HFS+ and APFS file system artifacts.
- Explain how changes to APFS and the macOS structure can impact forensic analysis.
- Describe how macOS handles property-list (PLIST) data.
- Identify user preferences and system preferences Analyze how date/time and time zone data affects analysis.
- Recognize the different disk images found in macOS examinations.
- Examine how media files found are stored, viewed and shared on macOS and iOS.
- Analyze various Apple metadata attributes and how they can assist in forensic analysis.
- Analyze mounted volume evidence, device connection evidence, and network connections in macOS.
- Examine artifacts from web browsers such as Safari and articulate your findings.
- Interpret numerous log files found on macOS and iOS devices and articulate your findings.

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
- Convert date values of mounted devices
- Examine unified logs to view device connections
- 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.

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 Apple Forensic Fundamentals