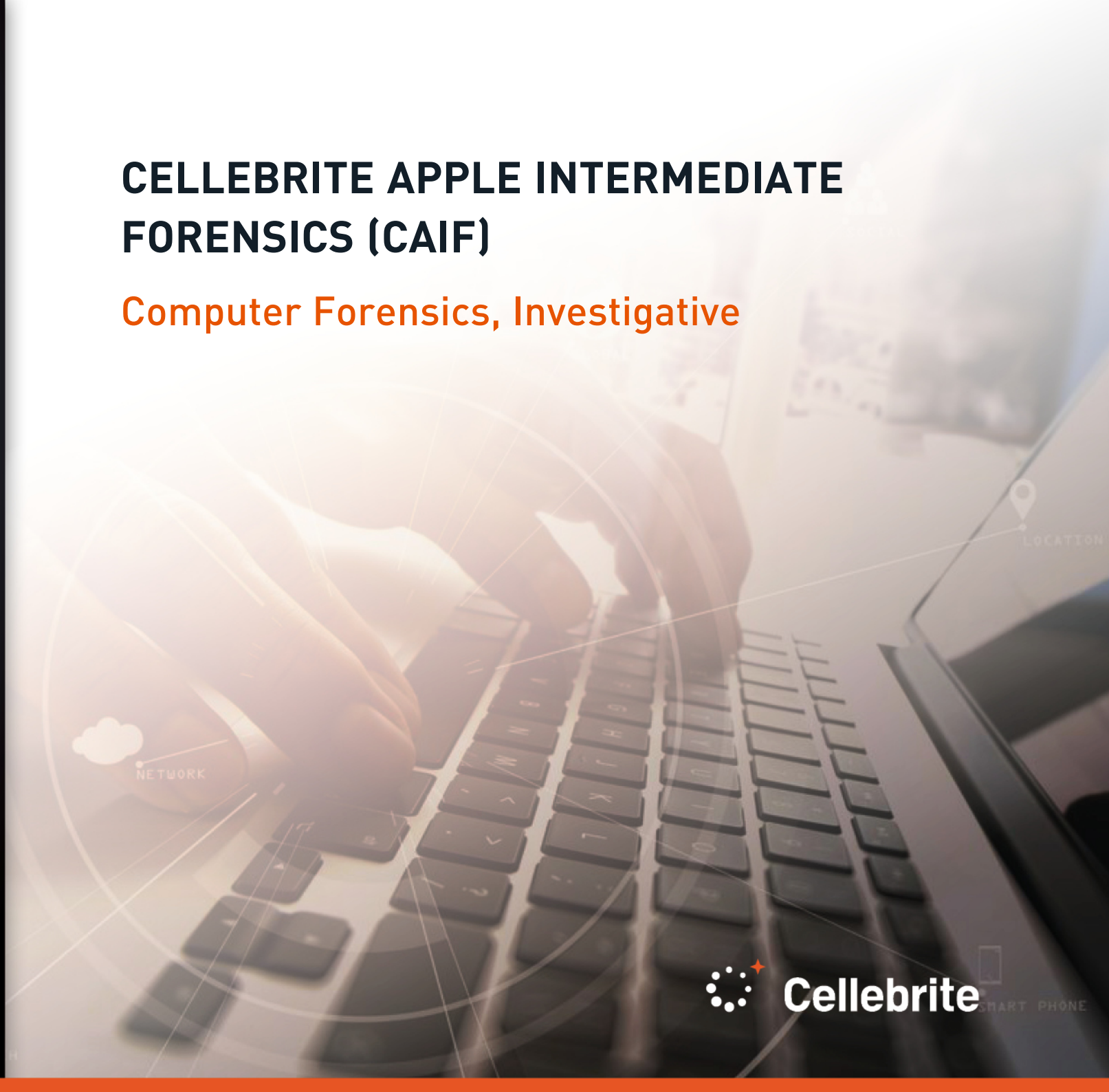
CELLEBRITE APPLE INTERMEDIATE FORENSICS (CAIF)

Computer Forensics, Investigative



Cellebrite

Level

Intermediate

Length

Three-Day (21 hours)

Training Track

Computer Forensics Investigative

Delivery Mode

Instructor-Led
Live Online

Course Description

Cellebrite Apple Intermediate Forensics (CAIF) is a three (3)-day course designed with hands-on learning and real case scenario data using Cellebrite Inspector software. Participants will analyze mounted volume evidence, device connection evidence, and network connections in macOS. A CAIF instructor will review log files found on macOS and iOS devices and how to analyze Apple Mail including its structure, mail messages, and related files. The advanced instruction includes a comprehensive exploration of the GUID Partition Table, Terminal, HFS+ and APFS file system, Time Machine Backups, Snapshots and understand the difference between link files, APFS clones, and APFS firmlinks.

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

Cellebrite

Course Learning Objectives

- Analyze mounted volume evidence, device connection evidence, and network connections in macOS.
- Interpret log files found on macOS and iOS devices to analyze Apple Mail including its structure, mail messages, and related files.
- Identify evidence related to the use of Terminal as well as utilize Terminal.
- Recognize the GUID Partition Table and understand its structure.
- Understand the Hierarchical File System (HFS+).
- Distinguish and interpret APFS disk structures from varying macOS versions.
- Create, examine, and analyze an APFS disk.
- Recognize and understand the difference between link files, APFS clones, and APFS firmlinks in macOS.
- Understand how Time Machine creates backups and APFS Snapshots and be able to analyze both.

DEVICE CONNECTION

- Examine unified logs to view device connections
- Determine Bluetooth connected devices in macOS
- Analyze network connections in macOS
- Examine AirDrop artifacts in macOS

EMAIL ANALYSIS

- 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.

COMMAND LINE BASICS

- Practice entering commands in a Terminal session
- Analyze a computer image to find evidence of command line use
- Create a shell script to run in macOS

GUID PARTITION TABLE

- Describe the GUID Partition Table (GPT) structure
- Recognize the GUID Partition Table (GPT) on disk

HFS+

- Inspect the unique aspects of the proprietary Hierarchical File System (HFS+).

APFS

- Describe APFS features
- Recognize the value of the additional APFS volumes
- Demonstrate methods of obtaining information from APFS disks
- Identify APFS disk structures from various versions of macOS
- Construct an APFS disk
    - Examine the disk for vital APFS artifacts
    - Create an APFS role for the contained volume
    - Create an APFS volume group with the existing volume
    - Analyze the APFS disk structure

LINK FILES

- Compare the types and differences of Link Files in MacOS.

TIME MACHINE MOBILE BACKUPS, AND APFS SNAPSHOTS

- Examine TimeMachine Mobilebackups and APFS Snapshots
- Explain how TimeMachine creates backups
- Identify the difference between a TimeMachine and Time Capsule backup
- Describe how APFS snapshots are created
- Use Cellebrite Inspector to analyze a TimeMachine Backup
- Analyze an APFS Snapshot using Cellebrite Insepctor
- Identify .MobileBackups in an HFS+ Mac computer

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 Intermediate Forensics