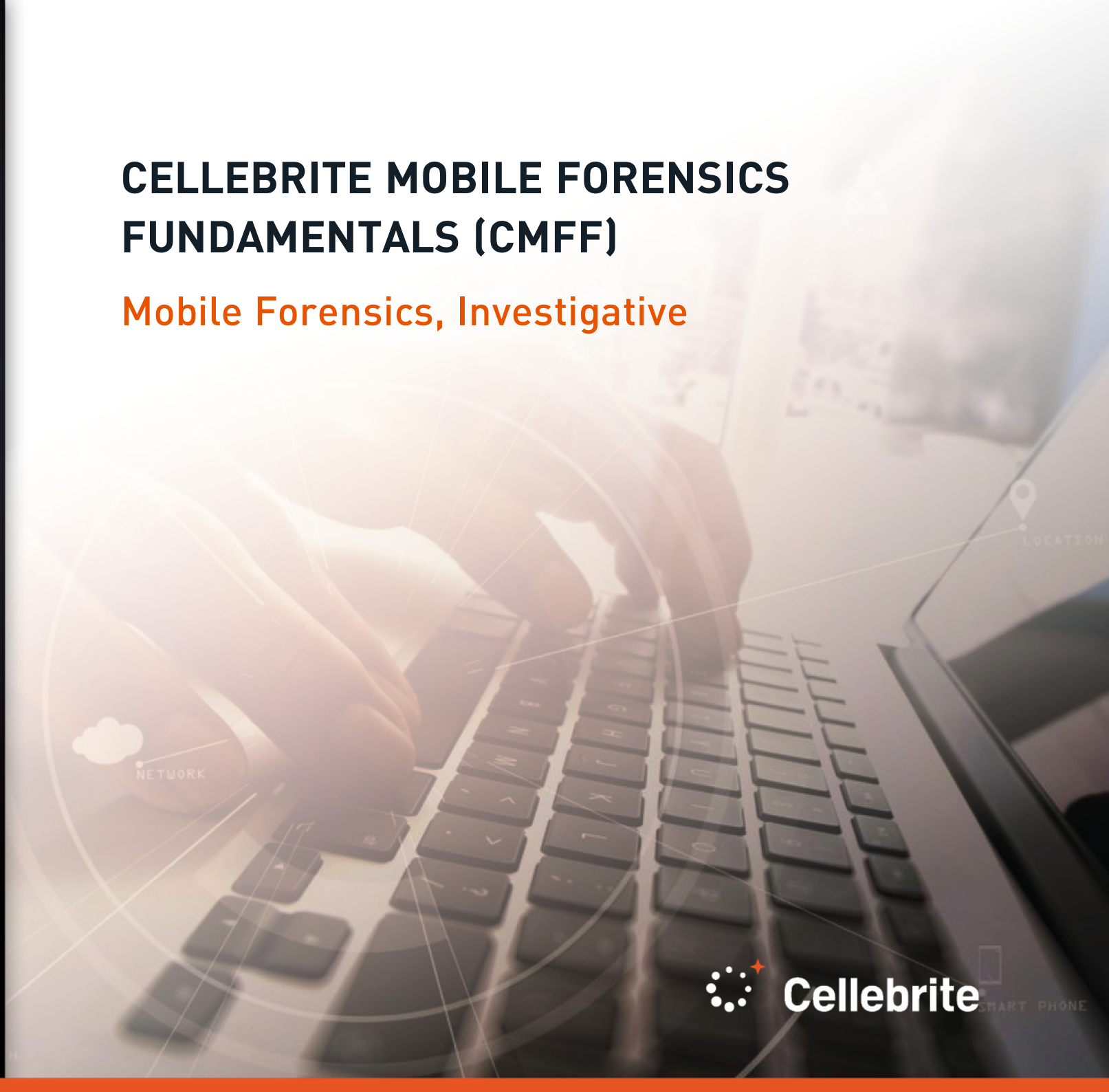
CELLEBRITE MOBILE FORENSICS FUNDAMENTALS (CMFF)

Mobile Forensics, Investigative



Cellebrite

Level

Entry/Beginner

Length

Two-Day (14 hours)

Training Track

Mobile Forensics Investigative

Delivery Mode

Instructor-Led
Web-Based
Live Online

Course Description

Cellebrite Mobile Forensics Fundamentals (CMFF) is a two (2) day entry level course designed to provide attendees with compulsory digital forensics fundamental knowledge including: mobile device communication networks, explorations of Android and iOS file systems, extraction methodologies. memory (NAND) functions, and the proper handling of digital evidence for use in administrative, civil, or criminal actions. Attendees will learn the reasoning and strategies used by creditable practitioners and organisations to form the future of digital forensic best practices.

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 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. Below are general audiences and focus areas relative to this course.

- Digital Forensic Examiners
- Corporate Investigators
- Administrators
- Intelligence Analysts
- Legal Professionals
- Criminal Investigators
- Crime Scene Investigators

Cellebrite

Course Learning Objectives

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

- Review of different mobile devices
- Description of digital forensic processes
- Discussion about best practice when seizing devices
- Exploration of extracted device data
- Explanation about generating basic reports using Reader,
- Demonstrate proficiency by completing an exam with a minimum passing score of 80%

Note: No pre-requisites exist to attend the CMFF class but is the first requirement to qualify for the Cellebrite Certified Mobile Examiner (CCME) certification exam. The CMFF course, is also available as a test-out for those individuals who feel they know the material and focused on achieving the CCME 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

- Discuss course administration.
- Review of the capabilities engineered in the Cellebrite Platforms and digital forensic solutions.
- Discuss a practitioner's legal responsibilities using Cellebrite products, software, and services.

INTRODUCTION TO MOBILE DEVICES

- Correctly identify mobile device hardware
- Identify mobile device operating systems
- Discuss mobile device communication technology
- Describe the effects of evolving technology on the mobile digital forensics industry
- Recount a historical overview of the Apples iOS operating system platform
- Discuss the value of Apple iOS devices to investigators
- Examine mobile device and internet of things (IoT) technologies of value in an investigation
- Explain the reasons influencing popularity of iOS devices and platform
- Recount a historical overview of the Android operating system platform
- Explain the reasons influencing popularity of Android devices and platforms
- Discuss the Android open-source Operating System and file system structure
- Discuss the value of Android devices to investigators
- Review the mobile communication network architecture and functions
- Explain the SIM file system organization

FORENSIC OVERVIEW PROCESS

- Describe and explore digital forensic media sterilization.
- Explain the four phases of the digital forensics process
- Recognize legal considerations for seizing and searching devices.
- Describe the first responder's role
- Describe the digital forensics practitioner's role
- Describe the importance for proper evidence handling and documentation.
- Relate the correct procedures for identifying and handling digital evidence devices as first responders.
- Identify investigative challenges that apply to the digital forensic processing of mobile devices.
- Identify tools and equipment needed to seize mobile devices as evidence.
- Recognize legal considerations for seizing and searching devices.
- Identify various locking mechanisms found on mobile devices.
- Demonstrate of the procedures used to seize mobile devices in a manner that preserves evidence integrity.
- Relate the different varieties of Android security features and complications the protection mechanisms present to examiners and investigators.
- Relate the different varieties of iOS security features and complications the protection mechanisms present to examiners and investigators.
- Describe the uses for UFED Camera Services.
- Relate the correct procedures for post-process handling of digital evidence devices.

EXTRACTION METHODOLOGIES

- Compare UFED 4PC Logical and Ultimate forensic solutions.
- Discuss the methods frequently employed by forensic examiners to acquire data from mobile devices.
- Identify best practices for the extraction of data from digital evidence devices.
- Describe the uses for UFED Camera Services.
- Review the value and use of hash values for evidence authentication.
- Modify UFED Touch2 and UFED 4 PC configurations for the extraction of different devices and investigative needs.
- Identify functions used within UFED Touch, UFED Touch 2 or UFED 4PC to perform supported data extractions.

DATA ENCODING AND STORAGE

- Describe data encoding schemes used by mobile devices to store information; including Binary, Hexadecimal, ASCII, and Unicode formats.
- Differentiate Wear Leveling and Garbage Collection as the functions influencing flash memory data.
- Identify basic flash storage characteristics and NAND organization

CELLEBRITE READER

- Discuss Reader capabilities
- Understand how an UFDR file is created
- Import a UFDR file into Reader for analysis and reporting
- Learn to Tag and filter a UFDR Report
- Create reports from Reader files

FINAL EXAM

- Complete a knowledge-based exam
- 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 Mobile Forensics Fundamentals