Cellebrite Advanced Smartphone Analysis (CASA)

Global forensic training

Level
Expert

Length
Four days (28 hours)

Training Track
Forensics

Delivery mode
Instructor Led Training

Course description

This 4-day advanced analysis course takes a hands-on, in-depth look into the forensic recovery of application data found in today's smartphones. This class is recommended for those familiar with UFED Physical Analyzer or who have completed the CCPA course. In this course, participants will learn how to decode information which is not decoded by forensic tools. They will also utilize third party software and Python scripts to analyze, verify and validate findings.

Module	Description and objectives
SQLite Database Structures	This module focuses on SQLite database structures and functionality. 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 UFED Physical Analyzer and verify their findings using other software tools and be able to: • Identify mobile device hardware • Identify SQLite databases • Identify SQLite database structures • Explain how data is stored within SQLite databases • Explain how SQLite tables are joined • Discuss what happens when data is deleted from a SQLite database and recovery of data • List functions which may destroy data • Use scripts to extract and analyze binary large object (BLOB) data from databases • Assemble unsupported and new applications using UFED SQL Builder
iOS Overview and Analysis	In this module you will learn about the demographics of iOS. You will learn what happens during the extraction process of an iOS device using UFED technology. We will show you how applications are stored, accessed and various ways to decode information found in XML and binary plist files. You will also learn about date and time encoding schemes and using a number of hands-on practical exercises you will examine numerous files of interest. At the completion of this module, you will be able to: • Provide a brief overview of iOS demographics • Learn how to identify iOS devices • Describe the structure of the iOS file system • Discuss Cellebrite UFED support for iOS analysis • Analyze iOS extractions with UFED Physical Analyzer • Identify and decode data stored as base64 data from binary plist files • Analyze various artifacts such as health data, data usage, and preference files to support and use in your investigations • Review a processed application for additional relevant data • Parse an unsupported application using the SQL Builder and incorporate the data into Physical Analyzer • Use Python to obtain additional data from Safari and Webkit to aid in web investigations • Learn new artifacts from full file system extractions, such as those from Cellebrite Services and Gray Key
iOS Device Access	In this module, you will learn about the challenges caused by the Data Protection API found in Apple iOS devices. You will learn about: • Identifying iOS device hardware • iOS passcodes • Touch ID – time limits and investigative implications • Recovery of simple and complex passcodes • Various methods for potentially gaining access to locked iOS devices
iOS and iCloud Backups	In this module we will learn about iOS backups found on computer systems, encrypted iOS extractions, and what kind of information can be contained within them. We will also discuss backup file encryption and decryption using open source tools, iCloud backups, and decoding. At the completion of this module, you will be able to: • Identify where iOS backups can be found • Identify iOS backup folder structures • Understand how to handle encrypted iOS Backups and Extractions • Obtain iCloud backup files and how Physical Analyzer handles them • Use open source software to crack the password of an encrypted backup • Learn to use iOS settings to potentially remove the backup password

Module	Description and objectives
Android Overview	In this module we will discuss the evolution of the Android operating system since its availability in 2007. You will also learn about the different file systems commonly used and how data is stored on Android devices and SD cards. We will discuss encryption, extractions and limitations. At the completion of this module, you will be able to: • Briefly recount the evolution of the Android operating system since its availability in 2007 • Identify the different file systems commonly used by Android devices • List the Android devices, file systems, and applications supported by Cellebrite UFED Series • Be familiar with the various extraction methods with Android devices • Understand the various types of Android encryption and possible bypasses
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, pattern lock codes, Bluetooth information, and operating system versions; this information may prove critical to the investigation. At the completion of this module, you will be able to: • Discuss how to determine which file systems have been mounted on an Android device. • Locate and analyse relevant system logs, Android artifacts, and device files • Discuss partitioning schemas used on Android devices. • Look at other applications which may prove valuable to an investigation. • Locate and decode application usage logs • Identify and parse data from Android User account files
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 which store data about user activity which aren't parsed as part of any tool extraction. At the completion of this module you will be able to: • Decode call logs and timestamps • Track a downloaded files movement within an Android device • Identify media locations • Be able to interpret cloud-based storage accounts used on a mobile device • Decode information related to applications which are not automatically decoded by any forensic tools • Use Python scripts to assist in decoding data • Locate relevant user data items data from both supported and unsupported applications used on a device • Decode and parse Google Maps data • Recover additional Chrome and browser based data to include in your investigations

Note: Successful completion of the Cellebrite Advanced Smartphone Analysis (CASA) examination and practical skills test results in a Cellebrite Advanced Smartphone Analysis Certification credential.

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 Digital intelligence for a safer world

Rev. CASA 07-18 (EN)