Digital Evidence for Legal Professionals (CDFL)

Global forensic training

County of San Luis Obispo District Attorney's office
September 19 – 20, 2019
Central Coast Cyber Forensic Lab (3CFL) 10 Sonoma Ave., BLDG #633
San Luis Obispo, CA 93405
CDFL
$1990.00

Level
Intermediate

Length
Two days (14 hours)

Training Track
Investigative

Delivery mode
Instructor-Led

Course description

The two-day Cellebrite Digital Forensics for Legal Professionals course is designed to educate personnel charged with the review, submission, and pursuit of justice using digital forensics evidence. The comprehensive course materials are used to engage class participants in hands-on exercises for familiarization with the devices and software used by digital forensic experts. Participants are provided with tools and solutions for use to verify the experts claims, seek additional information from service providers to assist with timeline and location data, and conduct data analytics. Additionally, legal professionals are offered information on how to question the expert and prepare digital evidence witnesses for court to present effective testimony.

Module	Description and objectives
Introduction	€ The identification of digital forensic fundamentals. € Descriptions of best practices for seizing digital evidence items. € An overview of mobile device form factors and operating systems. € An explanation of cellular technologies and network architecture basics. € Discussion on the use of flash memory mass storage. € Instruction on the potential uses for cellular device and network location data records. € Relate the need to question experts and prepare digital evidence witnesses.
Digital Forensics Fundamentals for Legal Professionals	€ Define the meaning of the term forensic science. € Describe what the term scientific method means. € Practice digital forensic science, not exploitation. € Digital Forensic Science, not Exploitation
Best Practices for Seizing Mobile Devices	€ Explain what the term best practice means. € Digital and Physical Evidence Identification and Processing Terms € Forensically Wiping a Media € Documentation to Maintain the MF Scientific Standards € Pre-and-Post Evidence Collection € Securing the Scene € Evidence Identification and Seizure € Collecting the Evidence € Device Radio Isolation, Packaging and Transport. € Radio Isolation € Airplane Mode: a. iOS Airplane Mode b. Android Device Airplane Mode € Power Off or Leave Power On? € Packaging € Transport
Identifying Device and OSs	€ Useful Mobile Device Websites and Identification Tools € Identifying Mobile Devices € Feature Phones € Smart Phone € Enhanced Processor € Graphics Processing Unit (GPU) € MicroSD (a.k.a Transflash) Cards € Tablets € Smart Watches € Drones € IoT Devices
Android Overview	€ Recount a historical overview of the Android operating system platform. € Explain the reasons influencing popularity of Android devices and platforms. € Describe Android hardware designs and technologies. € Discuss the Android open-source Operating System and file system structure. € Relate the different varieties of Android security features and complications the protection mechanisms present to examiners and investigators. € Discuss the value of Android devices to investigators. € Explore Android mobile device data extractions with the Cellebrite Physical Analyzer analysis software. € Analyze an Android device data extraction to answer practical exercise questions.

Module	Description and objectives
iOS Overview	€ Recount a historical overview of the Apples iOS operating system platform. € Explain the reasons influencing popularity of iOS devices and platform. € Describe Apple hardware designs and technologies. € Discuss the Apple iOS Operating System and file system structure. € Relate the different varieties of iOS security features and complications the protection mechanisms present to examiners and investigators. € Discuss the value of Apple iOS devices to investigators. € Explore Apple mobile device data extractions with theCellebrite Physical Analyzer analysis software. € Analyze an iOS device data extraction to answer practical exercise questions.
Cellular Technology and Terminology Overview	€ Provide a brief history of mobile network technology € Identify the parts of a cellular network € Explain how mobile phones communicate on cellular networks € Describe different handset transmission techniques € Basic Cellular Network Diagram € Network Location Checks € TDMA - Time Division Multiple Access € iDen - Integrated Digital Enhanced Network € CDMA - Code Division Multiple Access € TDMA vs. CDMA\ € GSM - Global System for Mobile Communications € CDMA vs. GSM € 5G - The Future € Summary
SIM Cards	€ Accurately describe what a SIM card is € Identify the difference in SIM Card Versions € Outline the SIM card hierarchy € Explain how the SIM card may be used by the investigator € SIM Card Versions € SIM Card and Stored Data € Universal Subscriber Identity Module (USIM) € SIM Security - PIN/PUK € SIM Contacts
Flash Memory	€ Understand how Flash Memory works € Understand NOR memory € Understand NAND memory € Understand the difference between NOR vs NAND € Understand Embedded MultiMedia Card … eMMC € Understand Universal Flash Storage 2.0 … UFS € Understand Mobile Phone Flash Memory File Systems € Understand Encoding € Understand Binary € Understand the 7 Bit SMS format € Understand Garbage Collection € Understand Wear Leveling

Module	Description and objectives
Mobile Device Unique Identifiers and New Technologies	€ Explain why unique mobile device identifiers are used. € Identify the parts of a cellular network € Explain how mobile phones communicate on cellular networks € Overview € International Mobile Equipment Identity (IMEI) € Mobile Equipment Identifier (MEID) € Integrated Circuit Card Identifier (ICCID € International Mobile Subscriber Identity (IMSI € Mobile Station International Subscriber Directory Number (MSISDN) € Unique Device Identifier (UDID) … Practical € IMEI / MEID - Practical € Summary
Understanding Extraction Methods	€ Brief Review of File System Organization € SIM Extraction/ SIM Cloning - Practical € Camera Services € UFED Extractions € Extraction Methods Options € Logical Extraction Overview € File System Extractions € Physical Extraction Overview € Boot Loaders € Cellebrite Extraction Client € Overview of Advanced Techniques: a. Joint Test Action Group (JTAG) b. Chip-Off c. JTAG vs Chip-Off d. Micro Read e.In-System Programming (ISP) f. Flasher Boxes g. Flasher Box and Software Website
Locations Data for Mobile Devices	€ Call Details Records € NELOS € Per Call Measurement € Activity Log € Real Time Tool € Triangulation vs Trilateration € Analyze location data identified in a mobile device data extraction.
Introduction to UFED Reader and Physical Analyzer	€ Perform an installation of Cellebrite UFED products on a computer workstation. € All projects searches € Table searches € Advanced filtering € Tagging € Timeline € Report generation € Explore data extractions from mobile devices using the Cellebrite Physical Analyzer software. € Demonstrate viewing data in the Cellebrite UFED Physical Analyzer interface.
Examination and Reporting for Digital Evidence	€ Describe the critical elements of digital forensic reporting. € Discuss reporting options afforded to the practitioners using the Cellebrite UFED Physical Analyzer features. € Relate vital forensic best practice related to the storage electronic evidence devices and data. € Compile data from a mobile device extract using the Cellebrite Physical Analyzer filtering and tagging features, culminating in the generation of a digital forensic report. € Conduct authentication and validation testing of collected data, generate reports using the Cellebrite Physical Analyzer forensic solution.

Module	Description and objectives
Questioning the Expert	€ Written Policies and Procedures € Did changes to data occur? € Voir dire hearing. € Exhibits or demonstrative evidence. € Consider the defense counsels use of the digital evidence. € Best approach in testimony.
Data Encoding	€ Binary € Hex € ASCII € Unicode € 7 Bit PDU

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. CDFL 12-18 (EN)