GLOBAL FORENSIC TRAINING

Cellebrite Advanced Smartphone Analysis (CASA)

COURSE DESCRIPTION

Houston Forensic Science Center
April 24th – 27th, 2017
1301 Fannin ST, Floor 21, Houston TX 77002
Cellebrite Advanced Smartphone Analysis (CASA)
POC: Allison Sudik
allison.sudik@gmail.com

$2,995.00

>>> Level
Advanced

Length
4 days

Delivery Mode
Instructor Led Training

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

Cellebrite Advanced Smartphone Analysis (CASA)

Time and Estimated Time	Description and Objectives
SQLite Database Structures 240 Minutes (4 Hours)	This module focuses on SQLite database structures and functionality. You will 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 € 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 € List functions that may destroy data
iOS Overview and Analysis 300 Minutes (5 Hours)	In this module you will learn about the evolution and 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 and ! will also learn about date and time encoding schemes and using a number of " " # € $ % &' € Provide a brief overview of iOS demographics € Learn how to identify iOS devices € * &' € Discuss Cellebrite UFED support for iOS analysis € Analyze iOS extractions with UFED Physical Analyzer
iOS Device Passcodes 120 Minutes (2 Hours)	In this module, you will learn about the challenges caused by the Data + #+/ # &' ! € Identifying iOS device hardware € Simple and Complex passcodes € Touch ID … time limits and investigative implications € Recovery of simple and complex passcodes € How to bypass security and extract evidence without the passcode
iOS and iCloud Backups 60 Minutes (1 Hour)	In this module we will learn about iOS backups found on computer systems and what kind of information can be contained within them. We will also 7 8 7 # € Identify where iOS backups can be found € Identify iOS backup folder structures € Understand how to handle encrypted iOS Backups and Extractions

Cellebrite Advanced Smartphone Analysis (CASA)

Time and Estimated Time	Description and Objectives
	€ & 8 7 + # 9 € * : 7
Android Overview 120 Minutes (2 Hours)	In this module we will discuss the evolution of the Android operating system ;<<= ! > commonly used and how data is stored on Android devices and SD cards. We will discuss encryption, extractions and limitations. At the completion of € $ % # availability in 200? € / > # € # Cellebrite UFED Series € Be familiar with the various extraction methods with Android devices
Android System Artifacts 1@0 Minutes (3 Hours)	In this module you will learn about important Android system artifacts. You will learn about obtaining data that documents wireless networks, time zone '* 8 7 $ information, and operating system versionsG this information may prove critical to the investigation. At the completion of this module, you will be able € * Android device. € Determine which wireless networks the device has connected to and any network passwords. € Discuss partitioning schemas used on Android devices. € Look at other artifacts that may prove valuable to an investigation.
Android User Artifacts 1@0 Minutes (3 Hours)	In this module you will learn about artifacts created by the user•s interaction > # J " " 8 8 8 K ' ' ' many other types of data. At the completion of this module you will be able € Decode call logs and timestamps € : 7 # € Identify media locations € Decode information related to applications which are not automatically decoded by any forensic tools € Use Python scripts to assist in decoding data

Cellebrite Advanced Smartphone Analysis (CASA)

Time and Estimated Time	Description and Objectives
Windows Mobile Operating System 60 Minutes (1 Hour)	In this module you will learn about the evolution of the Windows Mobile operating system since its availability in 1NN6 up to Windows Phone 10. You > including a discussion of current encryption issues. At the completion of this € Discuss the evolution of the Windows Mobile operating system € Discuss extraction and decoding methods for Windows devices using UFED technology
Windows Phone System Artifacts 60 Minutes (1 Hour)	In this module we will discuss some of the system artifacts found on the Windows Phone operating system which may be useful to an investigation. We will also discuss VTAX extraction decoding in Physical Analyzer. By the € * Z € Open and decode a VTAX extraction in Physical Analyzer € Determine which wireless networks the device has connected to € Identify partitioning schemas used on Windows Phones € Identify other system artifacts important to an investigation
Windows Phone User Artifacts 120 Minutes (2 Hours)	/ to being stored in the proprietary Extensible Storage Engine (ESE) format. ESE databases are not well understood by most forensics tools. As a result, we K'K " € Recover evidence related to the user•s web site browsing with Internet Explorer € How to recover SMS and MMS messages sent and received by the user € How to recover user contacts stored on the phone € 9 ' ' ' email that may prove valuable to an investigation