CELLEBRITE IRON PYTHON (CIP)

Mobile Forensics

Cellebrite

Level

Advanced

Length

Five-Day (35 hours)

Training Track

Mobile Forensics

Delivery Mode

Instructor-Led Live Online

Course Description

This 5-day advanced course takes a hands-on, in-depth look using Python to process and aid in the investigation of the forensic recovery of data found in today's smartphones. This class is recommended for those familiar with UFED Physical Analyzer or who have completed the CCPA course. Suited for those with little to no knowledge of Python or scripting, the course teaches you the fundamentals of scripting languages and incorporating them into your forensic investigations. You will explore data types and variables, look at strings, input, testing, and formatting. From there, learn about arguments and parameters, along with conditionals and nested conditionals. By the end of the course, you'll be able to create programs that prompt users for input, use conditional (True/False) logic and Python methods to interpret data from files and provide feedback for your reports. Plus, learn basic troubleshooting for your code.

Course Learning Objectives

INTRODUCTION

In this module, you will learn about Cellebrite's products, services, training, and certification processes available under Cellebrite's Training programs. Learners will be introduced to the course objectives, requirements, and administrative options to establish the foundation to succeed in your educational or professional goals. You will use the Cellebrite Learning Center and CelleConnect Portal to connect with various resources.

- Identify Cellebrite's global presence and service industry
- Describe Cellebrite's core training and certification process
- Recount Cellebrite's accolades and accomplishments
- Review the capabilities engineered in Cellebrite platforms and digital forensic solutions
- Identify other people in the community that can serve as a training or help resource
- Identify the learning objectives related to the course or training product
- Discuss a practitioner's legal responsibilities using Cellebrite products, software, and services

INTRODUCTORY PYTHON SCRIPTING

This module introduces you to scripting using the Python language. Python supports all models of forensics, from mobile, to computers, to networks. You can use Python to automate tasks, comb through data, and locate and process the vast amounts of digital evidence we get from devices today. You will use practical, hands-on exercises using open source software and integrate some scripts into Physical Analyzer. You will learn:

- Getting Started
- Displaying Text
- String Variables
- Storing Numbers
- Working with Dates and Times
- Making Decisions with Code
- Complex Decisions with Code
- Repeating Events
- Repeating Events Until Done
- Remembering Lists
- How to Save Information in Files
- Reading from Files
- Functions
- Handling Errors

PYTHON FORENSIC APPLICATION

In this module you will apply the skills you just learned into incorporating several scripts into a practical case. You may write your own scripts, change some of the ones provided or both to get the results from your evidence. This enjoyable team exercise lets you expand upon both your forensic and newly honed scripting experience.

PHYSICAL ANALYZER AND PYTHON

This module focuses on learning the basic Python interpreter used by Physical Analyzer. You will incorporate your newly learned Python skill into reading data from a device extraction and using a basic script to include it in analyzed data.

- Identify the Python functionality within PA
- Utilize the Python guide for Physical Analyzer
- Use a script to extract basic information
- Understand how to incorporate your findings into the Analyzed Data section

ADVANCED SQLITE

This module focuses on SQLite database structures and using the Python's SQLite library to interpret and generate a report on your findings.

- Identify SQLite databases
- Identify SQLite database structures
- Explain how data is stored within records
- Use Python to extract and analyze binary large object (BLOB) data from databases and process the results
- Use Python to search and extract data from SQLite files found in today's mobile devices
- Utilize both Physical Analyzer and open source tools to report on your findings

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 Iron Python