DF125 Mobile Device Examinations with OpenText Mobile Investigator

Syllabus

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado
Boulevard Suite 400
Pasadena, CA 91106-2375

Washington, DC
(Gaithersburg, MD)
9711 Washingtonian Blvd
6th floor, Room 601 (Paris Room)
Gaithersburg, MD 20878

London, UK (Reading)
420 Thames Valley Park Drive
Earley, Reading
Berkshire
RG6 1PT

Munich, Germany (Grasburnn)
Werner-von-Siemens-Ring 20
85630 Grasburnn/München
Germany

For a complete listing of locations, including Authorized Training Partners around the world, please visit opentext.com/learning-services/learning-paths.

EnCaseTraining@opentext.com

Day 1

Day one starts with instruction on installing, configuring, and navigating through OpenText™ Mobile Investigator.

Next, students will learn the structures of mobile data followed by an explanation and discussion regarding acquisitions concepts.

The day ends with students learning about and participating in the process of acquiring data from both the Apple iOS and Android.

Day 1 will cover:

- How mobile devices have become part of many digital investigations.
- Installing OpenText™ Forensic (EnCase) and OpenText Mobile Investigator and applying global configurations.
- Using EnScript plugins to adapt the OpenText Forensic environment for an examination of mobile devices.
- Creating and adding evidence to a case within OpenText Mobile Investigator.
- Identifying the structures within mobile devices, including Apple PList, SQLite, and EXIF.
- Identifying the various types of mobile acquisition.
- Acquiring from a device and implementing troubleshooting techniques if necessary.
- Identifying the available file types and importing their content.
- Performing acquisitions from cloud services.
- Reviewing acquired evidence.
- Identifying methods for iOS device acquisition, even when passcode protected.
- Performing a logical acquisition of an iOS device.
- Identifying the difference between an iOS9 and iOS10/11 iTunes backup.
- Discussing the encoding methods of Apple filenames in the backup.
- Identifying the key components of an iTunes iOS backup.
- Acquiring an iTunes backup using OpenText Forensic.
- The history behind the creation of Android devices.
- The options for acquiring data from Android devices and using OpenText Forensic to conduct an acquisition.

Day 2

Day two begins with a lesson on searching through a case of evidence added to a mobile case.

Next, instruction involves examining the artifacts available from Android and Apple iOS devices. Students close out the day and the course by learning how to prepare reports from mobile device cases.

Day 2 will cover:

- Performing an index search across mobile evidence within OpenText Forensic.
- Discussing the process of optical character recognition relating to the use of OpenText Mobile Investigator.
- Performing and reviewing the results from a raw search with OpenText Mobile Investigator and discussing the associated options.
- Processing the evidence loaded into OpenText Mobile Investigator.
- Performing an index search and reviewing the results using OpenText Mobile Investigator.
- Performing a Categorized Items search applying relevant filtering within OpenText Mobile Investigator.
- Navigating the pathways to key artifacts within Android evidence from both a logical and physical acquisition using OpenText Forensic and OpenText Mobile Investigator.
- Extracting SQLite DB files for viewing and analysis with SQLite Viewer.
- Using relevant EnScript programs for viewing and parsing.
- An explanation of the artifact paths with potential evidentiary value.
- Discussing the core artifacts of Apple iOS, such as call history and contacts.
- An explanation of the function of SMS/iMessage and link to attachments.
- Locating and understanding where digital photographs are stored.
- View the EXIF data with EnScript applications and OpenText Mobile Investigator.
- An explanation of applications' aspects in terms of where the data can be identified as they relate to the acquisition from an iOS device and iTunes backup.
- Using application artifacts to parse those for Safari.
- Verifying relevant parsed content with the use of SQLite queries.
- Examining unsupported applications via the construction of SQLite queries and SQLite viewers.
- Bookmarking various data types.
- Generating various reporting types.
- Understanding the options of reporting navigation.
- Creating reports for both logical and physical acquisitions.