opentext™

Training overview

# DF125 Mobile Device Examinations with OpenText EnCase

## Syllabus

### Day 1

Day one starts with instruction on installing, configuring and navigating through OpenText™ EnCase™ Mobile Investigator. Next, students will learn the structures of mobile data followed by an explanation and discussion regarding acquisitions concepts.

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

### On day one, students will:

- Learn how mobile devices have become part of many digital investigations
- Install OpenText™ EnCase™ Forensic and EnCase Mobile Investigator and apply global configurations
- Use EnScript™ plugins to adapt the EnCase environment for an examination of mobile devices
- Create and add evidence to a case within EnCase Mobile Investigator
- Identify the structures within mobile devices, including Apple PList, SQLite and EXIF
- Identify the various types of mobile acquisition
- Acquire from a device and implement troubleshooting techniques if necessary
- Identify the available file types and import their content
- Acquire from cloud services
- Review acquired evidence
- Identify methods for iOS device acquisition, even when passcode protected
- Perform a logical acquisition of an iOS device
- Identify the difference between an iOS9 and iOS10/11 iTunes backup
- Discuss the encoding methods of Apple filenames in the backup
- Identify the key components of an iTunes iOS backup
- Acquire an iTunes backup using EnCase
- Learn the history behind the creation of Android devices
- Learn the options for acquiring data from Android devices and use EnCase to conduct an acquisition

opentext™

## Day 2

Day two begins with instruction on searching through a case of evidence added to a mobile case. Instruction will next involve examining the artifacts available from Android and Apple iOS devices. Students will close out the day and the course by learning how to prepare reports from mobile device cases.

## On day two, students will:

- Perform an index search across mobile evidence within EnCase Forensic
- Discuss the process of Optical Character Recognition relating to the use of EnCase Mobile Investigator
- Perform and review the results from a raw search with EnCase Mobile Investigator, discussing the associated options
- Process the evidence loaded into EnCase Mobile Investigator
- Perform an index search and review the results using EnCase Mobile Investigator
- Perform a Categorized Items search applying relevant filtering within EnCase Mobile Investigator
- Navigate the pathways to key artifacts within Android evidence from both a logical and physical acquisition using EnCase Forensic and EnCase Mobile Investigator
- Extract SQLite DB files for viewing and analysis with SQLite Viewer
- Use relevant EnScript programs for viewing and parsing
- Receive an explanation of the artifact paths with potential evidentiary value
- Discuss the core artifacts of Apple iOS, such as call history and contacts
- Receive an explanation of the function of SMS/imessage and link to attachments
- Locate and understand where digital photographs are stored
- View the EXIF data with EnScript and EnCase Mobile Investigator
- Receive an explanation of applications' aspects in terms of where the data can be identified, relating to the acquisition from an iOS device and iTunes backup
- Use application artifacts to parse those for Safari
- Verify relevant parsed content with the use of SQLite queries
- Examine unsupported applications via the construction of SQLite queries and SQLite viewers
- Bookmark various data types
- Generate various reporting types
- Understand reporting navigation options
- Create reports for both logical and physical acquisitions

**opentext.com/contact**