opentext™

Training overview

DF220 Navigating EnCase Version 8

Syllabus

Day 1

Day one begins with an overview of the new OpenText™ EnCase™ Version 8 software, including its new features and improvements. The students learn the details for installing, opening and navigating EnCase Version 8. The day will conclude with an overview of the new evidence file format and acquisition of both a local device and a remote running node.

Day 1 will cover:

- Getting started with EnCase Version 8
- Learning standard components of EnCase Version 8
- Supported encryption
- Major improvements
- Installing EnCase Version 8 and the cert file
- Running the program
- Creating a case in EnCase Version 8
- Managing your cases
- Case templates
- New investigation pathways
- Navigating within the new environment
- Configuring EnCase Version 8 for your environment
- Navigating the EnCase environment
- Previewing a local drive
- Acquiring and adding evidence to a case
- Initiating the acquisition process
- Using FastBloc™ SE to write protect devices
- Adding evidence to a case
- Using EnCase Portable
- WinEn and WinAcq
- Using Direct Network Preview and Acquisition to triage or image computers
- Preparing the computer to enable the connection
- Creating the essential small, command-line program called a “servlet”
- Connecting and configuring computers to perform and run a Direct Network Preview

opentext™

Day 2

Instruction on day two begins with an overview of the new function, EnCase Evidence Processor. Next, students get right to work using Evidence Processor to search a case, view the results and capture the results for later reporting. The day continues with lessons on how EnCase Version 8 works with external viewers and how to create conditions. The day closes with instruction on the methods of file signature analysis in the new program.

Day 2 will cover:

- Getting familiar with EnCase Evidence Processor
- Preparing evidence for Evidence Processor
- Managing the settings and using the Evidence Processor toolbar
- Learning about tasks and modules
- Bookmarking and tagging evidence
- Bookmarking single and multiple items
- Creating a note bookmark and bookmark highlighted data
- Bookmarking decoded data
- Bookmarking folders and creating tables
- Creating tags and tag items
- Searching the case
- Conducting index searches
- Metadata within index searches
- Conducting raw searches
- Viewing the search results
- Reviewing search results and creating Results sets
- Volume recovery
- Using the Full Investigation pathway
- Identifying deleted volumes
- Recovering deleted volumes
- Learning about conditions
- Learning to create conditions
- Creating and using custom conditions
- Installing and using external viewers in EnCase Version 8
- Using File types table and external file viewers
- Copying files and folders from EnCase
- Extracting data from EnCase
- Analyzing file signatures
- Understanding file signatures and file types
- Adding and editing a file signature
- Starting and running an analysis and viewing the results

Day 3

On day three, students will learn how to conduct a hash analysis in EnCase Version 8 and add hash libraries to the case, as well as how Entropy can be used in a case. Instruction continues with a lesson on how to use EnCase Version 8 to search for email and internet elements. Students will learn how to use the new reporting functionality to create and customize their final report. The final lesson of the day focuses on archiving cases.

Day 3 will cover:

- Learning about EnCase Version 8 and hash analysis
- Understanding how hash analysis differs in EnCase Version 8 from EnCase Version 6
- Creating a hash library and hash sets
- Performing a hash analysis
- Finding hash set matches
- Querying in the hash library
- Documenting the hash sets used during an examination
- Searching for email
- Email threading
- Bookmarking email elements
- Creating reports
- Using report templates and understanding their structure
- Adding and modifying elements to templates
- Exporting a report
- Preserving a customized report as a template
- Archiving a case in EnCase Version 8
- Duplicating examination data
- Verifying archived evidence files
- Restoring a case that has been archived

opentext.com/contact