

FORENSIC TRACK

CE420, Continuing Education-EnCase Examinations (ENCASE)

Who Should Attend

DCIO and CI investigators and prospective lab examiners.

Prerequisites

TT110 (INCH), RT120 (CIRC) and FT215 (WFE-FTK) or Test Outs

Duration

2.5 Days

Course Description

Introduces students, who are already competent with the operation of other forensic applications, to the EnCase 6 analysis tool and how to use the application for common forensic procedures in the examination of digital media. Special emphasis is placed on the NTFS capabilities of EnCase in support of students who are familiar with Windows FAT file systems. {Mobile}

Objectives

- Obtain, install and configure the EnCase application
- Describe EnCase's interface and options
- Create, edit, and manage a case
- Perform a file signature analysis
- Perform a hash analysis
- Explain where to find Web-related evidence
- Recover e-mail messages and base64 attachments
- Recover evidentiary data from Windows system files
- Conduct searches
- Explain how to forensically wipe media using EnCase
- Explain the differences and similarities between FAT and NTFS file systems and apply the differences to forensic examinations
- Perform media verification
- Add evidence to a case
- Identify file permissions and how they can be used to associate the file to an user account
- Open and view Registry, Zip, e-mail, archive files, etc
- Bookmark files of evidentiary value
- Edit bookmarked files
- Add notes to bookmark folders
- Create an EnCase forensic report
- Export files, folders, applications, and the report
- Run EnScripts
- Run Filter for specific files

Topics Covered:

Using EnCase

- Use and Configuration of EnCase

EnCase Methodology – Case Management

- Beginning a case with EnCase
- EnCase Graphical User Interface
- Filters, Conditions, and Queries
- Bookmarking

FORENSIC TRACK

Analysis with EnCase

- Initial Evidence Processing
- Using Hash Sets
- Advanced Keyword Searching
- Web-Related Evidence
- Analyzing E-mail and Newsgroups
- EnScripts
- Exporting and Artifacts
- Date Searching
- EnCase Modules

Preparation

To assist in your preparation for the ADEF course, we recommend the following:

You should review:

- *Windows Forensic Examinations-Forensic Toolkit* (WFE-FTK) course book, paying special attention to:
 - FAT32 and NTFS file structures
 - Hash analysis
 - Signature analysis
 - Text searching
 - E-mail messages/attachments

These topics are covered in DCITA courses you may have attended previously and can also be found on the dcita.edu portal (<https://www.dcita.edu>), the internet, at Books 24/7, in your organization's technical library or at the public library. Instructions for D-Prep on the dcita.edu portal: log in. Under Online Courses, select DPrep Training; Course Name (WFE-E); Sort by Name Ascending.

ENCASE Grading Policy

Student progress is monitored through instructor observation during lecture, discussion and practical exercises as well as Knowledge and Performance Tests. Minimum passing score on all DCITA tests is 70%.