FORENSIC TRACK

CE425, Continuing Education - Forensic Toolkit (FTK)

Who Should Attend

DCIO and CI investigators and prospective lab examiners.

Prerequisites	Duration
TT110 (INCH), RT120 (CIRC) and FT210 (WFE-E) or FT215 (WFE-FTK) or Test Outs	2.5 Days

Course Description

Introduces students, who are already competent with the operation of other forensic applications, to forensic methodology in the use of FTK software in the examination of digital media. {Mobile}

Objectives

- Obtain, install, and configure FTK and associated applications
- Understand FTKs 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
- Perform media verification
- Acquire evidence and add evidence to a case
- Recover ownership information of files and locate the owner
- Open and view Registry, Zip, e-mail archive files, and more
- Bookmark files of evidentiary value
- Edit bookmarked files
- Add notes to bookmark folders
- Create an FTK forensic report
- Export files, folders, applications, and the report
- Password Cracking with PRTK

Topics Covered

Introduction to Forensic Toolkit (FTK)

- Introduction to and Installation of FTK
- Introduction to FTK Imager (including imaging, previewing and exporting files)
- Creating Custom content Images

Case Management

- Starting a New Case
- Working with Existing Cases
- The FTK Interface
- Bookmarks
- Flagged Graphics

FORENSIC TRACK

Forensic Analysis with FTK

- The FTK Case Log
- Text Searching
- Examining Graphics Files
- E-mail Analysis
- File Filtering and Data Carving
- Registry Examination
- Exporting Files and File Information

Password Recovery Toolkit (PRTK)

- Introduction to Password Recovery Toolkit
- PRTK Recovery Modules, Dictionaries and Profiles
- Windows EFS
- Password Cracking

Case Reporting

- Creating and Customizing Your Report

<u>Preparation</u>

To prepare for this course, we recommend the following review, reading, or research:

- Review the *Windows Forensic Examinations-EnCase* (WFE-E) 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-FTK); Sort by Name Ascending.

FTK 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%.