

FORENSIC TRACK

FT220, Macintosh Forensic Examinations (McFE)

Who Should Attend

DCIO and CI investigators and prospective lab examiners.

Prerequisites

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

Duration

10 Days

Course Description

A combination of lecture, instructor-led demonstrations, and hands-on practical exercises that introduce investigators and analysts to the fundamental concepts necessary to perform a forensic examination of a Macintosh computer system. {Mobile}

Objectives

- Explain the basics of how Apple Computer hardware and software work
- Setup Macintosh and Windows Forensic Workstations
- Import digital evidence into EnCase 6 and conduct various investigative tasks
- Import digital evidence into Macintosh environment and conduct further analysis
- Apply knowledge of Apple file systems and applications to forensic examinations of Apple Computer systems
- Document in a report how the evidence supports the investigation

Topics Covered

Apple Computer Technologies

- Apply knowledge of Apple hardware, software, and file systems to forensic examinations
- Apple hardware such as the PowerBook G4, Power Mac G5, iMac, iBook, and iPod
- OS X and Apple software for Internet browsing, e-mail, digital photography, and office productivity
- HFS, Extended HFS+, and other file systems supported by OS X

Analysis

- Conduct forensic examinations of Macintosh systems using EnCase 6 and the Macintosh native environment
- Examining Web-related evidence including Web-enabled features of iDisk and .Mac
- Analyzing e-mail
- Analyzing artifacts created by Macintosh software Applications
- Analyzing OS X system data
- Performing file vault analysis
- Searching and identifying files using EnCase 6
- Handling encryption

FORENSIC TRACK

Preparation

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

- Review the *Introduction to Networks and Computer Hardware* (INCH) and the *Computer Incident Responders Course* (CIRC) course books, paying special attention to:
 - Imaging
 - Working from a command line prompt interface
- Have a fundamental knowledge of Macintosh hardware and operating systems, such as OS X
- Have an understanding of basic computer forensics

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 (INCH/CIRC); Sort by Name Ascending.

McFE Grading Policy

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