

## FORENSIC TRACK

### FT215, Windows Forensic Examinations – FTK (WFE-FTK)

#### **Who Should Attend**

DoD and federal law enforcement agents and prospective intrusion analysts.

#### **Prerequisites**

TT110 (INCH) and RT120 (CIRC) or Test Outs

#### **Duration**

10 Days

#### **Course Description**

In a hands on environment, course introduces the basic concepts and practices of processing digital evidence using the Access Data Forensic Toolkit (FTK) 3.0 analysis tool. Students set up a forensic workstation, review a Case Jacket, import digital evidence into FTK, formulate and execute a method for forensic examination based on case type, properly document the case (through written forensic reports) and identify key legal concepts.

#### **Objectives**

- Demonstrate a basic knowledge of Windows operating systems and respective file systems
- Import digital evidence into FTK and conduct various investigative tasks
- Formulate and execute a methodology for a forensic examination based upon case type
- Document, in a report, how the evidence supports the investigation
- Identify key legal concepts for a forensic examination

#### **Topics Covered**

##### *Technical Background*

- Discuss the Windows file systems and how they relate to an investigation
- Basics of the NT and FAT file systems and how data is stored in each
- Structure of partition tables

##### *Case Setup and Management*

- Focus on the procedures to start and manage a case
- New case setup and management
- Open a new case, perform analysis, and record findings in the forensic report
- Set up your forensic workstation
- Install and configure FTK
- Understand the Case Jacket
- Perform a hash analysis
- Use the Windows registry to identify case data

##### *Automated Tools*

- Conduct analysis with automated tools
- Perform text searches, signature searches, and data carving
- Conduct a positive hash analysis

##### *File Level Analysis*

- Analyze evidence found on the Web, e-mail, and system files
- Recover and review e-mail, Web cache, and newsgroup mailboxes
- Recover passwords

## FORENSIC TRACK

### **Preparation**

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

- Review:
  - Introduction to Networks and Computer Hardware (INCH) course book
  - Computer Incident Responders Course (CIRC) course book
  - Working from a command prompt
- Have a fundamental knowledge of the Microsoft Windows Operating Systems and associated logical file structure
- Have a basic understanding of the FAT32 and NTFS file structures

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; Sort by Name Ascending.

### **WFE-FTK 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%.