AccessData Enterprise 105

Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

The AccessData Enterprise 105 is an Advanced three-day course providing the knowledge and skills necessary to use FTK Enterprise and conduct specialized investigations with an enterprise or corporate environment. This course assumes that the student is experienced in the basic features of AccessData's Forensic Toolkit, or has taken previous training from AccessData related to the features of FTK.

Prerequisites

This hands-on class is intended experienced forensic professionals who use AccessData forensic software to examine, analyze, and classify digital evidence.

To obtain the maximum benefit from this course, you should meet the following requirements:

- Able to understand course curriculum presented in English
- **MUST** have experience with FTK or have taken one of the following courses:
    - FTK Bootcamp
    - Forensic Toolkit 101
- Perform basic operations on a personal computer
- Have a basic knowledge of computer forensic investigations and acquisition procedures
- Be familiar with the Microsoft Windows environment

It is recommended that the student have taken the following AccessData courses prior to Enterprise 105: Forensic Toolkit 101 or FTK Bootcamp. The course assumes that the user has taken some training, or is experienced with FTK prior to taking this course.

Class Materials and Software

The course manual, hands-on instructions, and review questions are available for download from the class page on the AccessData training website.

All software, demonstration forensic images, and hardware required for the class will be provided.

The class includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

ACCESSDATA

AccessData Enterprise 105

Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

Module 1: Using FTK Enterprise

Topics:

- Creating Cases
- Creating User Roles
- Using Agents
- Adding remote data using agents:
  - Memory and Volatile Data
  - Creating Physical and Logical Images
  - Filter File Search
- Batch Remediation

Lab:

Students will get extensive hands on coverage of the features specific to FTK Enterprise.

Module 2: The Enterprise API

Objectives:

- Understand the program and code dependencies when working with the API
- Automate and standardize case creation and processing.
- Create custom workflows and interfaces specific to organizational needs.

Lab:

Students will learn the concepts related to the AccessData Enterprise API. Students will perform tasks using the API such as creating a case, and setting processing options.

Module 3: Using the Mac Agent

Objectives and Topics:

- Understand how the Mac Agent is different, and the installation process
- Deployment and collection of data using the Mac Agent
- Analysis of MacOS related data.

Lab:

Participants will configure a Mac Agent and analyze MacOS related data related to Mac Agent extractions.

Module 4: Cerberus

Topics:

- What is Cerberus?
- Describe the Cerberus Processing Stages
- Perform Cerberus analysis and review the results
- Create, Bookmark and Report Cerberus files.

Lab:

Students will learn to use Cerberus to scan an dataset, analyze the results, and create a meaningful report.

Module 5: Distributed Processing with FTK Enterprise

Topics:

- Setting up distributed processing.
  - Understand the requirements for distributed processing
  - Understand how Distributed processing works
- Using Distributed processing

Lab:

Participants will set up and configure Distributed Processing for FTK Enterprise.

Module 6: Class Practicals

Objectives:

- Apply the concepts learned to extract data from a Windows machine using a remote agent.
- Apply the concepts learned to extract data from a MacOS machine using the Mac Agent.
- Perform a basic analysis of the data and create a simple report.

ACCESSDATA