AccessData FTK Intermediate

Intermediate • Three-Day Instructor-Led Course

For more information contact: training@accessdata.com

The AccessData FTK Intermediate, three-day course provides the knowledge and skills necessary to install, configure, and effectively use Forensic Toolkit (FTK), FTK Imager and Registry Viewer at an Intermediate level.

Prerequisites

This hands-on class is intended for new users, particularly forensic professionals and law enforcement personnel, who use AccessData forensic software to examine, analyze, and classify digital evidence.

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

- Able to understand course curriculum presented in English
- 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

Class Materials and Software

You will receive the associated materials prior to the course.

During this three-day, hands-on course, participants will perform the following tasks:

- Install and configure FTK, FTK Imager, and Registry Viewer
  - Learn to configure FTK to be more efficient on your forensic machine
  - Learn about and use Global Objects
- Use FTK Imager in a simulated "Incident Response" setting
- Review Registry Viewer functions: also conduct advanced searching and produce registry summary reports
- Conduct more detailed email analysis
  - Persons of Interest
  - Exporting of Email
- Use advanced processing options of FTK such as: EID, OCR, Event Log analysis, and Volume Shadow Copy
- Increase abilities to conduct more advanced Index and Live searches
- Create and use more complex filters
- Learn to use the Visualization tool
  - Heat Map
  - File Visualization
  - Email Visualization
  - Geo Location

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

AD ACCESSDATA

AccessData FTK Intermediate

Intermediate • Three-Day Instructor-Led Course

For more information contact: training@accessdata.com

(Continued on other side)

Module 1: Introduction

Topics:

- Identify the FTK components
- List the FTK and PRTK system requirements
- Describe how to receive upgrades and support for AccessData tools
- Install required applications and drivers

Lab:

Participants will install the UTK components—FTK, FTK Imager, and Registry Viewer

Module 2: FTK Imager 201

Objectives:

- Learn how to make FTK Imager portable
- Use features of FTK Imager in an incident response capacity
- Learn how to extract volatile data from live machines

Lab:

During the practical participants acquire volatile data from virtual machine, simulating a suspect machine.

Module 3: Registry Viewer 201

Objectives:

- Use basic and advanced searching through the Windows Registry
- Create Registry Summary Reports
- Select keys to put report in a specific order
- Discuss running summary reports during case processing

Lab:

During the practical, participants use Registry Viewer to search for specific registry keys and recover registry artifacts in a specific order, for a custom report. Students will also create registry summary reports and select summary reports to be run during case processing.

Module 4: Case Setup

Objectives:

- Optimum Setup
- Configuring Preferences
- Archive and Backup Operations
- Configure Global Objects
- Copying a case from an older version of FTK to a newer version.

Lab:

Students will learn how to copy a case from one version of FTK to another and perform backup and archive functions for cases.

Module 5: Advanced Filtering

Topics:

- Defining of global filters to manage case items
- Filters with multiple rules
- Filter Nesting
- Compound Filtering
- Tab Filters

Lab:

Participants will build and use complex filters to take large amounts of data and find specific items within that dataset.

Module 6: Email Analysis

Topics:

- Review Email tab
- Learn about the function of Persons of Interest
- Describe the different abilities of FTK to export email
- Use the features of email threading

Lab:

Students will walk through a case containing processed email and see the full abilities of FTK to deal with email.

ACCESSDATA

AccessData FTK Intermediate

Intermediate • Three-Day Instructor-Led Course

For more information contact: training@accessdata.com

Module 7: Disk Analysis Features

Topics:

- Learn about the FTK Disk Viewer
- Use the Deleted Partition Finder
- Conduct Image Verification

Lab:

Participants will go over the features listed in the topics above, using various evidence files.

Module 8: Advanced Processing Options

Objectives:

Students will use each of the below listed advanced processing options of FTK

- Analyze Windows Event Logs
- Explicit Image Detection
- Optical Character Recognition
- Language Identification
- Entity Extraction
- Volume Shadow Copy

Lab:

During the practical, participants will explore the advanced capabilities of FTK to analyze case data. The steps performed here will walk through the usage of each of the advanced processing options listed above, using various evidence files and cases.

Module 9: Advanced Searching

Objectives:

Students will conduct live and index searches using the follow features of the search tabs

- Live Search Options
  - Text
  - Pattern
  - Hex
- Index Search
  - Indexing Options
  - Conducting an Index Search
  - Importing/Exporting Search Terms
  - Search Operators
  - Searching for a phrase
  - Boolean Searches
  - Searching Options
  - TR1 Regular Expressions

Lab:

Students will see how to make searches more effective by making subtle to advanced changes to index options and search parameters.

Module 10: Visualization

Objectives:

- Launch the Visualization tool.
- Describe the Visualization page.
- Use Timeline views to review case data.
- Select a Theme.
- Use the Visualization function to review file data.
- Use the Visualization function to process email data:
- Perform an Email Social Analysis.
- Examine Email Traffic details.
- Use the Geolocation function to map evidence items that have geolocation information associated with them.

Lab:

Students learn how to use the functionality of the Visualization interface.

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, LLC. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.