AccessData Forensic Toolkit 101

Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

The AccessData Forensic Toolkit 101 five-day course provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit® (FTK™). This course is focused on understanding the features of FTK and the methods necessary to use those features effectively. Forensic Toolkit 101 sets the foundation for the more artifact focused Forensic Toolkit 201 and Forensic Toolkit 301.

Prerequisites

This hands-on class is intended for new and 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
- 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 Forensic Toolkit 101: FTK Imager 100, Registry Viewer 100, and Password Recovery Toolkit 100. While not required these courses will teach core concepts that will benefit students in 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 Forensic Toolkit 101

Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

Module 1: Installation of FTK

Topics:

- Installation of FTK Suite and associated tools
- FTK Basic Install
- FTK Advanced Install
- Using the AccessData License Manager
- Database configuration and user admin

Lab:

Participants will install FTK and associated software, and configure the database in preparation for case creation.

Module 2: Creating Cases in FTK

Objectives:

- Creation and modification of pre-case Processing Profiles
- Configuring Evidence Processing Options
- Configuring Evidence and Index Refinement
- Overview of FTK Lab and eDiscovery processing options
- Creating Custom File Identification settings

Lab:

Students will create a case and learn about the various evidence processing options available in FTK and how to use them effectively. Participants will create processing profiles in preparation for adding evidence.

Module 3: Managing Evidence for FTK Cases

Objectives:

- Supported Evidence Sources and the process of adding evidence to a case
- Creating Evidence Groups
- Configuring pre-case Time zone settings
- Create case and database backups and archives.
- Restore previously detached cases to FTK.

Lab:

Students will configure and add evidence to a case.

Module 4: Introduction to the FTK Interface

Objectives:

- Learn each tab and the specific features available in each.
  - System Information
  - Explore
  - Overview
  - Bookmarks
  - Email
  - Graphics
  - Video
  - Internet
  - Mobile Data
- Customize the FTK Interface to meet the examiners needs and style
- Configuring Time Zone settings within the case
- Modifying column settings
- Selecting evidence using Check marks, keyboard shortcuts, and Quick Picks
- Use the various view options and panes available to analyze evidence

Lab:

Participants will navigate through each tab using the features in each to view various evidence types.

Module 5: Filtering in FTK

Topics:

- One Rule Filtering and using Live Preview
- Multi-Rule Filtering
- Nested Filters
- Compound Filters
- Persons of Interest
- Managing, Saving, and Sharing Filters

Lab:

This in-depth module will introduce users to the powerful features associated with FTK filtering.

ACCESSDATA

AccessData Forensic Toolkit 101

Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

Module 6: Searching with FTK

Objectives:

- In depth coverage on using FTK's robust searching options.
- Index Searching
  - Configuring Index Search Options
  - Field and Date Recognition
  - Operators
  - TR1 Expressions
  - Result Comparisons
  - OCR and Abby OCR
- Live Search
  - ASCII and Unicode Searches
  - Searching with Filters
  - Pattern Searching using Regular Expressions

Lab:

Students will conduct in-depth searches of all types.

Module 7: FTK Manage Menu

Objectives:

- Use the Manage menu to control
  - Labels
  - Columns
  - Filters
  - Carvers

Lab:

Students will manage the various items available in FTK.

Module 8: Exporting Items from FTK

Objectives:

- Understand and apply the various options found in the Export option Window
- Learn the features associated with exporting the information in the file list.
- Export files and directories directly to a forensic image.

Lab:

Participants will export various files, in various formats to gain an understanding of the options.

Module 9: Known File Filter (KFF)

Objectives:

- Install and configure the Known File Filter database.
- Understand how to create hash lists
- Learn the process of importing hash lists into the KFF database and hash set groups.
- Understand some of the situations in which KFF can be used and how FTK can facilitate those uses.
- Know the various ways to view KFF marked files, and know the difference between the two types: ignore and alert.
- Discuss the NSRL hash list, and how to use the KFF Import Tool to load and configure the NSRL list.
- While specific to Law Enforcement, discuss the Project Vic implementation within KFF.

Lab:

Participants will install, configure, and run various Known File Filter processes.

Module 10: Disk Level Analysis in FTK

Topics: This module will cover the following topics related to disk level analysis:

- Data Carving
  - Automated
  - Manual
  - Custom Carvers
- Disk Viewer
- Find on Disk
- View File Sectors
- Verify Image
- Hex view
- Restore Image to Disk
- Mounting Images
- Virtual Shadow Copies

Lab:

Students will go hands on with the various features discussed in the module.

ACCESSDATA

AccessData Advanced Forensics

Intermediate • Five-Day Instructor-Led Course

For more information contact: training@AccessData.com

Module 11: FTK Python Scripter

Topics:

- Python code requirements for scripts with FTK
- Introduction to the Python Script wizard
  - Export Options
  - Script Options
  - Adding New Scripts
- Bookmarking
  - Automatic Bookmarking
  - Automatic Supplementary files added back to case

Lab:

Participants will use the FTK Python Scripter against various file types to create custom output for more in-depth analysis and dynamic reporting.

Module 12: Data Visualization

Objectives:

- Analyze and track email behavior using the email visualization feature.
- Quantify and map file size, and distribution within evidence using file heat maps.
- Map images embedded with Exif data

Lab:

Students will get hands on experience using the various visualization features and will understand the applications of each.

Module 13: Reporting

Objectives:

- Utilize the Reporting tool to deliver the findings of a case in the most effective format
- Use Portable Case to create a robust review tool for end users to search, label, bookmark, and export files from.

Lab:

Participants will create reports of various formats. Participants will also create a Portable case and view the options and features associated with it.

Module 14: FTK Management and Troubleshooting

Objectives:

- Explore the options and features associated with the Database Management's Tool menu.
- Learn how to manage and recover processing jobs.
- Cover basic troubleshooting steps for when things don't go quite as expected.

ACCESSDATA