

# AccessData FTK 3 Transition Workshop

## Forensic Toolkit

*Intermediate • One-day Instructor-led Workshop*



**AccessData**<sup>®</sup>

The AccessData<sup>®</sup> Forensic Toolkit<sup>®</sup> 3 (FTK<sup>™</sup> 3), One-Day Transition Workshop is designed to provide the knowledge and skills to enable participants to transition from FTK 1.x or FTK 2.x to FTK 3.. Participants will learn how to utilize FTK 3 to process a case and locate evidence.

During this one-day, hands-on workshop, participants will perform the following tasks:

- Install and configure FTK.
- Create a case in FTK.
- Use FTK to process and analyze documents, metadata, graphics and email.
- Use bookmarks and check marks to efficiently manage and process case data.
- Update and customize the KFF database.
- Create and apply file filters to manage evidence in FTK.
- Conduct Live, Indexed, Internet Keyword and Regular Expression searches in FTK.
- Import search lists for Indexed searches in FTK.
- Use the FTK Data Carving feature to recover BMP, GIF, JPEG, EMF, PDF, HTML and Microsoft<sup>®</sup> Office documents.
- Create reports that include exported files, custom logos and external information such as hash lists, search results, or PRTK password lists.

### Prerequisites

This workshop is intended for users who have attended the AccessData BootCamp and/or Windows Forensic training classes and has a basic understanding of the following AccessData tools:

- Forensic Toolkit 1.x or 2.x
- FTK Imager
- Registry Viewer
- Password Recovery Toolkit (PRTK)

### Workshop Materials and Software

You will receive the student training manual and CD containing the training material, lab exercises and course-related information.

## Module 1: Introduction

### Objectives

- List the FTK system requirements.
- Describe how to receive upgrades and support for AccessData tools.
- Install FTK, Oracle, KFF, and the CodeMeter license driver.

### Lab

- Prepare your system.
- Install AccessData Software.

## Module 2: Working with FTK—Part 1

### Objectives

- Effectively use the Database Manager.
- Create and administer users.
- Back up, delete, and restore cases.
- Identify the evidence processing options.
- Identify the basic FTK interface components, including the menu and toolbar options as well as the program tabs.
- Create a case.
- Add evidence to a case.
- Obtain basic analysis data.

### Lab

- Create and add users.
- Manage case reviewer rights.
- Create a new case.
- Review the FTK interface.
- Customize the FTK interface.
- Create custom tab settings.
- Add evidence to an existing case.

## Module 3: Working with FTK—Part 2

### Objectives

- Change the time zone display.
- Identify and view compound files.
- Export files and folders.
- Create custom column settings to manage the information that appears in the FTK file list.
- Use the Copy Special and Export File List features.
- Create and manage bookmarks.
- Perform analysis functions, such as full text indexing, after evidence has been added to the case.
- Perform automatic and manual data carving functions.
- Acquire Remote Live Evidence.

### Lab

- Manage evidence by highlighting and checking files.
- Bookmark files.
- Define custom column settings.
- Change the time zone display.
- View file properties, metadata, and compound files.
- Recover evidence from the Recycle Bin.
- Use the Copy Special feature to copy column information.
- Export file list information.
- Export files and folders.
- Data carve evidence items using automated and manual data carving.

## Module 4: Processing the Case

### Objectives

- Navigate the FTK Graphics tab.
- Export graphics files and hash sets.
- Tag graphics files using the Bookmarks feature.
- Use the Flag Thumbnail feature.
- Identify supported email types.
- Navigate the FTK Email tab.
- Sort email.
- Find a word or phrase in an email message or attachment.
- Export email items.
- Process Macintosh systems.

### Lab

- Launch native content viewers from within FTK.
- Bookmark graphics.
- View EXIF data in graphics.
- Nest bookmarks.
- Export file hash lists.
- View Internet chat files.
- Locate e-mail messages and attachments in a case.
- Create a column setting that displays information specific to e-mail.
- Bookmark e-mail files and their attachments.
- Export selected e-mail files.
- Decrypt files.
- Process Macintosh evidence.

## Module 5: Narrowing Your Focus

### Objectives

- Narrow evidence items using the Known File Filter (KFF), checked items, and filtered/ignored items.
- Perform an indexed search.
- Perform a live search.
- Import search terms from text files.
- Perform a regular expression search.

### Lab

- Add Alert hash sets to the KFF database.
- Perform a full text index search.
- Import search terms from a user-defined list.
- Search checked items only.
- Use regular expressions to perform live searches.
- Use the Ignore feature to ignore specific items in the case.
- Mark files Privileged to manage reviewer access to the files.

## Module 6: Filtering the Case

### Objectives

- Explain basic concepts of rule-based filtering in FTK.
- Define a basic filter and use it to filter data.
- Create filter rules.
- Nest filters.
- Explain the difference between global and tab filters.
- Import and export filters.
- Apply a filter to a report to customize output.
- Apply a filter to an index search.

### Lab

- Use File Filter Manager to create basic filters.
- Create a filter that filters evidence by item category.
- Create a filter that filters graphics by logical size.
- Create a filter that filters email items within a specific date range.
- Create a filter that filters files by user SID.
- Import a filter.
- Create a nested filter.
- Apply global filters.

## Module 7: Case Reporting

### Objectives

- Define a report:
  - Modify the case information.
  - Include a list of bookmarked files.
  - Export bookmarked files with the report.
  - Include thumbnails of bookmarked graphics.
  - Manage the appearance of the Bookmark section.
  - Include thumbnails of case graphics.
  - Link thumbnails to full-size graphics in the report directory.
  - Include a list of directories, subdirectories, files, and file types.
  - Include a list of case files and file properties.
  - Export case files associated with specific file categories.
  - Append a registry report to the case report.
- Generate reports in the following formats:
  - PDF
  - HTML
  - RTF
  - WML
  - XML
  - DOCX
  - ODF
- Generate reports in other languages.

### Lab

- Create and modify reports.
- Include all bookmarks or graphics in a report.
- Include only flagged bookmarks and graphics in a report.
- Export bookmarked files to a report.
- Create a PDF report.

For a complete listing of scheduled courses or to register for available courses, see [www.accessdata.com](http://www.accessdata.com).

© 2009 AccessData Corporation – All rights reserved.

Some topics and items in this workshop syllabus are subject to change. This document is for information purposes only. AccessData makes no warranties, express or implied, in this document. AccessData, Forensic Toolkit, FTK, FTK Imager, Known File Filter, KFF, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are either registered trademarks or trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.