

AccessData Case Reviewer

Forensic Toolkit (Case Review Mode)

Beginning • One-day Instructor-led Workshop



AccessData[®]

The AccessData[®] Case Reviewer Training provides an introduction to using AccessData Case Reviewer.

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

- Obtain basic analysis data in Case Reviewer.
- Bookmark evidence.
- Create and apply custom column and font settings.
- Locate and view graphics files.
- Locate, view, and search e-mail files and attachments.
- Perform indexed searches.
- Discuss regular expressions.

Prerequisites

This hands-on workshop 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 workshop, participants should meet the following requirements:

- Read and understand the English language.
- Perform basic operations on a personal computer.
- Be familiar with the Microsoft Windows environment.

Course 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

Topics

- Introductions
- Course materials and software
- Prerequisites
- Course outline
- Helpful Information

Lab

- Check system information.
- Select Windows Explorer display preferences.
- Prepare your system.

Module 2: Database Management

Objectives

- Identify the components of the FTK 2 Database Management Interface.
- Create User Accounts.
- Assign rights to a case.

Lab

- Create and add users.
- Assign users to a case.
- Log on to the database.
- Restore a case.

Module 3: Working with FTK—Part 1

Objectives

Identify the basic interface components, including the menu and toolbar options, tabs and panes, viewer options, and QuickPicks.

Lab

- Review Case Reviewer Interface.
- View files with bad extensions.
- View graphics, email, and deleted files.
- View indexed search options.
- Customize the interface view.

Module 4: Working with FTK—Part 2

Objectives

- Define column settings.
- Change case time zone settings.
- Set the temporary file folder.
- View compound files and their children.
- View metadata.
- View evidence item file properties.
- Identify and process Internet/chat files in a case.
- Identify and process registry files in a case.
- Use the Copy Special feature to copy file information.
- Use the Export File List feature to export file information to a tab-delimited text file.
- Create and manage bookmarks.

Lab

- Create and apply column settings.
- Change the time zone display.
- Highlight and check files.
- View file properties, metadata, and compound files.
- Bookmark files in the Recycle Bin.
- Use the Copy Special feature.
- Export File List information.
- Create and add to bookmarks.
- View chat program files.
- View Windows Index.dat and Link files.
- View Windows Registry files.

Module 5: Case Processing

Objectives

- Filter case data using global and tab filters.
- Perform a live search.
- Perform a regular expression search.
- Perform an indexed search.
- Search checked files.
- Process case graphics.
- View graphics in the four FTK view modes.
- View graphics in an external viewer.
- Export hash lists.
- Process case email.

Lab

- Bookmark graphics.
- Create and apply a custom column setting.
- View EXIF data in graphics.
- Create a custom email column setting.
- Bookmark email.
- Export a file has list.
- Nest and remove bookmarks.
- Conduct a full text index search.
- Import a user-defined word list for full text searching.
- Conduct a search using dtSearch options.
- Perform a regular expression search.

Module 6: Student Practical

During this student practical, students will perform the following:

- Identify files with bad extensions.
- Locate and bookmark EFS encrypted files.
- Locate files in the Recycle Bin and determine who recycled the files.
- Perform a search using dtSearch options.
- Locate and analyze email files and attachments.
- Bookmark graphics files.
- Recover case evidence.
- Perform a regular expression search to locate US telephone numbers.

For a complete listing of scheduled courses or to register for available courses, see 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.