

AccessData BootCamp

Forensic Toolkit, FTK Imager, Password Recovery Toolkit and Registry Viewer

Course Number 240 • Three-day Instructor-led Class



AccessData®

The AccessData® BootCamp provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit® (FTK™), FTK Imager™ Password Recovery Toolkit™ (PRTK™) and Registry Viewer™.

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

- Install and configure FTK and its components, FTK Imager, PRTK and its components, Registry Viewer and LicenseManager.
- Use FTK Imager to preview evidence, export evidence files, create forensic images and convert existing images.
- Create a case in FTK.
- Use FTK to process and analyze documents, metadata, graphics and e-mail.
- 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® Office documents.
- Create reports that include exported files, custom logos and external information such as hash lists, search results, or PRTK password lists.
- Use custom dictionaries and dictionary profiles to recover passwords in PRTK.
- Identify the basic components of the Windows registry.
- Review Registry Viewer functions, including accessing the Protect Storage System Provider and hidden keys, indexing the registry, creating reports and integrating those reports with your FTK case report.
- Utilize the index in FTK to create custom dictionaries in PRTK.

Prerequisites

This hands-on course 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 course, you should meet the following requirements:

- Read and understand the English language.
- 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.

Course Materials and Software

You will receive the following AccessData course materials and software to use during and after the training:

- Student training manual and CD containing the training material, lab exercises and course-related information.
- Ultimate Toolkit™ Demo CD containing the following forensic tools:
 - FTK— 5,000 item Authorized Version
 - FTK Imager — 30-day Trial Version
 - Registry Viewer—Limited Demonstration Version
 - PRTK— WinZip SuperFast Attack
 - Distributed Network Attack® (DNA®) 2.0— 1 Server / 2 Clients Authorized Version
 - WipeDrive — Limited Demonstration Version

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: Installation

Objectives

- Describe the minimum system requirements for running FTK.
- Install FTK and FTK Imager.
- Install the dongle drivers.
- Install KFF.
- Describe the directory structure created during FTK installation.
- Describe how to receive upgrades and support for FTK and KFF.
- Describe the dongle subscription service and LicenseManager.

Lab

- Install FTK and FTK Imager.
- Install the KFF and dongle drivers.
- Install LicenseManager.
- Install PRTK and Registry Viewer.

Module 3: Working with FTK Imager

Objectives

- Describe standard data storage devices.
- Identify some common software and hardware acquisition tools.
- List some common forensic image formats.
- Use FTK Imager to perform the following functions:
 - Preview evidence.
 - Export data files.
 - Create a hash to benchmark your case evidence.
 - Acquire an image of evidence data.
 - Convert existing images to other formats.

Lab

- Preview evidence.
- Export files and folders.
- Create a hash to benchmark case evidence.
- Acquire an image of evidence data.
- Convert an acquired image to another format.

Module 4: Working with FTK

Objectives

- Identify the basic FTK interface components including the menu and tool bar options and the program tabs.
- Create a case.
- Add evidence to a case.
- Obtain basic analysis data including file and folder properties, file formats, metadata and specific file information such as dates and times.
- Export files.
- Use the Copy Special feature to export information about case files.

Lab

- Review the FTK Interface.
- Create a new case.
- View file and folder properties and metadata.
- Use the Copy Special feature to export date and time information about files in the case.
- Add evidence to an existing case.

Module 5: Processing the Case—Graphics

Objectives

- Identify the elements of a graphics case.
- Identify standard graphics formats.
- Navigate the FTK Graphics tab.
- Use the List All Descendants feature
- Export graphics files and hash sets.
- Tag graphics files using the Bookmarks feature.
- Use the Thumbnail feature.

Lab

- Bookmark and flag graphics files.
- View a PowerPoint slide show in the FTK viewer.
- View an AVI file in its associated program.
- Export graphics files.
- Use the Copy Special feature to export date and time information about selected graphics files to tab-delimited files and an Access database.

Module 6: Processing the Case—E-Mail

Objectives

- Identify the elements of an e-mail case.
- Identify supported e-mail types.
- Navigate the FTK E-mail tab.
- Find a word or phrase in an e-mail message or attachment.
- Bookmark e-mail items.
- Export e-mail items.
- Print e-mail items.

Lab

- Bookmark e-mail files and their attachments.
- Apply a comment to a bookmark.
- Create a column setting that displays information specific to e-mail.
- Locate e-mail messages and attachments in a case.
- View e-mail messages in the FTK viewer.
- Export selected e-mail files.

Module 7: 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

- Perform a full text index search.
- Import search terms from a user-defined list.
- Perform an index search using the stemming option.
- Use regular expressions to find all US phone numbers in the body of case evidence.
- Create filters in the File Filter Manager.
- Use the Ignore feature to ignore specific items in the case.

Module 8: Case Reporting**Objectives**

- Generate a report.
- View reports.
- Modify reports.
- Update reports.
- Distribute reports.

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.
- Include thumbnails with links to full-size graphics.
- Specify file properties for bookmarked files.
- Include a List by File Path section in the report.
- Include a File List Properties section in the report.
- Include case audit files in the report.
- Add a custom logo to the report.

Module 9: Cryptography 101**Objectives**

- Define cryptography.
- Discuss the history of cryptography.
- Describe password protection versus password encryption.
- Explain how hash algorithms are used to generate ciphers.
- Discuss encryption standards and key space values.
- Perform dictionary and key space attacks.
- Know what to look for at an investigation site.

Module 10: Working with PRTK**Objectives**

- Identify the basic PRTK interface components, including the menu and toolbar.
- Identify the available Password Recovery modules and their associated attack types.
- Import user-defined dictionaries and FTK word lists to use in a password recovery attack.
- Define a biographical dictionary.
- Setup up profiles.

Lab

- Review the menu and tool bar options.
- Recover passwords from an encrypted Word document.
- Recover passwords from a Windows registry file.

Module 11: Registry Viewer Introduction**Objectives**

- Describe how the registry is organized.
- Describe how Registry Viewer displays MRU lists.
- Describe the function of Registry Viewer's common areas.
- Describe the registry's protected storage area.
- Describe the function of Registry Viewer's summary reports.
- Use the Registry Viewer to index the registry
- Explain how to include Registry Viewer reports in FTK Case reports.

Lab

- Compare the capabilities of the Windows Registry Editor with Registry Viewer.
- Open a registry hive independently.
- Decrypt Protect System Storage Provider (PSSP) key.
- Chronologically list MRU values.
- Search registry files, including hidden keys.
- Create a report.
- Use Registry Viewer help.
- Export the registry word list.

Module 13: Advanced UTK Functionality

Objectives

- Set program preferences in FTK.
- Use FTK analysis tools, such as MD5 Hash and Full Text Indexing.
- Import hash sets to the KFF.
- Perform data carving searches.
- Perform Internet keyword searches.
- View the file sectors associated with a selected file.
- Use the FTK index to assist PRTK in recovering passwords.
- Describe the components of the Ultimate Toolkit (UTK).

Comprehensive Lab

- Set FTK preferences.
- Import custom hashes into the KFF database.
- Perform a data carving search for JPEG files and add the recovered files to the case.
- Perform an Internet keyword search.
- View the file sectors associated with a selected file.
- Integrate FTK and PRTK to analyze encrypted files and recover their passwords.

Module 14: FTK Case Agent

Objectives

- Describe the function of the Forensic ToolKit's Case Agent Mode.
- Identify how to launch FTK in Case Agent Mode.
- List FTK features that are disabled in Case Agent Mode.
- Describe how to switch between Case Agent Mode and full FTK functionality.

Lab

- Run FTK in Case Agent mode.
- Create a batch file that automatically launches FTK in Case Agent mode.

Practical Skills Assessment

The AccessData BootCamp includes an optional Practical Skills Assessment (PSA). This performance-based assessment requires participants to apply key concepts presented during the course to complete a practical exercise. Participants who successfully complete the exercise receive a PSA certificate of completion.

Course content, prices and availability are subject to change without notice.



Ultimate
*The Complete
AccessData
Software Kit* **Toolkit™**



Forensic
*Find Computer Evidence
Quickly & Easily* **Toolkit™**



**Password
Recovery**
*Recover
Passwords
Quickly & Easily* **Toolkit™**



**Registry
Viewer**
*Find Registry Data
Quickly & Easily* **Viewer™**



**Distributed
Network
Attack**
*Putting
Idle Time
To Work* **Attack™**



WipeDrive™
3.0
Completely Eliminate Hard Drive Data

© 2005 AccessData Corporation – All rights reserved.
Some topics and items in this course 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, Ultimate Toolkit and WipeDrive 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.