

# AccessData BootCamp

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

*Intermediate • Three-day Instructor-led Class*



**AccessData**<sup>®</sup>

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

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

## Module 1: Introduction

### Objectives

- Identify the UTK components.
- List the FTK and PRTK system requirements.
- Identify the FTK .INI files.
- Describe how to receive upgrades and support for AccessData tools.
- Install the UTK.

### Lab

- Prepare your system.
- Install AccessData Software.

## Module 2: 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.
- Use dockable windows in FTK Imager.

### 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 3: Registry Viewer Introduction

### Objectives

- Describe which files comprise the Windows 2000/XP Registry.
- Seamlessly launch Registry Viewer from an FTK case.
- Determine a user's time zone setting.
- Determine a user's SID.

### Lab

- Open a registry hive independently.
- Recover a user's SID number, user name, full name, logon count, and last logon time using a SAM registry file.
- Generate registry reports.
- Integrate the Registry Viewer report with FTK

## Module 4: 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.
- Manage Time Zone display settings.

### Lab

- Review the FTK Interface.
- Create a new case.
- View file and folder properties and metadata.
- Add evidence to an existing case.

## Module 5: Working with FTK—Part 2

### Objectives

- Change time zone display.
- 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 Info features.
- Create and manage bookmarks.
- Perform additional analysis, such as full text indexing, after evidence has been added to the case.
- Perform automatic and manual data carving functions.

### Lab

- Use the Copy Special feature to copy column information.
- Export files and folders.
- View evidence items using internal and external viewers.
- Manage evidence by highlighting and checking files.
- Create and add to bookmarks.
- Manage hash sets in the KFF.
- Data carve evidence items.

## Module 6: Processing the Case

### Objectives

- Identify the elements of a graphics case.
- Navigate the FTK Graphics tab.
- Export graphics files and hash sets.
- Tag graphics files using the Bookmarks feature.

- Use the Flag Thumbnail feature.
- Identify the elements of an email case.
- 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.

### Lab

- Bookmark and flag graphics files.
- Export a file hash list.
- Use the Copy Special feature to export date and time information about selected graphics files to tab-delimited files and an Access database.
- Create a column setting that displays information specific to e-mail.
- Bookmark e-mail files and their attachments.
- Locate e-mail messages and attachments in a case.
- 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.
- Use regular expressions to find all US phone numbers in the body of case evidence.
- Use the Ignore feature to ignore specific items in the case.

## Module 8: 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 default filter.
- Create a bookmark filter.

## Module 9: 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 in the report.
  - Export case files associated with specific file categories.
  - Append a registry report to the case report.
- Generate reports in PDF, HTML, RTF, WML, XML, DOCX, and ODF formats.
- 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.

## Module 10: Working with PRTK

### Objectives

- Navigate within the PRTK interface.
- 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.
- Create biographical dictionaries.
- Set up profiles.
- Explain what a PRTK profile is and how it is used.
- Recount the AccessData Methodology.

### Lab

- Create a biographical dictionary.
- Create a profile.
- Recover passwords from an encrypted Word document.
- Add recovered files to the case report.
- Recover passwords from NTUSER.DAT files.

## Practical Skills Assessment

The AccessData Technology course includes a 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.

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 course 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, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.