

# AccessData Forensics Advanced BootCamp

## Forensic Toolkit, FTK Imager, Password Recovery Toolkit, Registry Viewer, and Portable Office Rainbow Table

*Five-day Instructor-led Class*



The AccessData® Technology class provides the knowledge and skills necessary to install, configure and effectively use Forensic Toolkit® (FTK™), FTK Imager™, Password Recovery Toolkit™ (PRTK™), and Registry Viewer™. Participants will also use AccessData products to conduct forensic investigations on Microsoft® Windows® systems, learning where and how to locate Windows system artifacts.

During this five-day, hands-on class, students will perform the following tasks:

- Install and configure FTK and its components, FTK Imager, PRTK and its components, and Registry Viewer.
- Use FTK Imager to preview evidence, export evidence files, create forensic images and convert existing images.
- Create and add evidence to 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.
- Conduct Live, Indexed, Internet Keyword and Regular Expression searches in FTK.
- Import search lists for Indexed searches in FTK.
- 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.
- Use the FTK Data Carving feature to recover BMP, GIF, JPEG, EMF, PDF, HTML and Microsoft Office documents.
- Utilize the index in FTK to create custom dictionaries for PRTK.
- Create regular expressions.
- Use Registry Viewer to locate evidentiary information in Windows 9x, 2K and XP registry files.
- Use PRTK to recover user logon passwords from the Windows SAM file and decrypt files with extended ASCII passwords.
- Integrate Registry Viewer with FTK.
- Use FTK and PRTK to recover EFS encrypted files on Windows 2000 and XP systems, including Windows XP SP1 and higher.
- Recover forensic information from Recycle Bin INFO2 files.
- Recover forensic information from Windows link files.
- Use PRTK to recover passwords from Microsoft Office documents, decrypt them, and display them in an FTK report in a decrypted format.

The class includes hands-on labs that allow participants to apply what they have learned to a mock case. These performance-based simulations are designed to help participants retain information learned during the training.

## Prerequisites

This hands-on class 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 class, 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.

## Class Materials and Software

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

### Module 1: Introduction

#### Objectives

- Identify the FTK components
- List the FTK and PRTK system requirements
- Describe how to receive upgrades and support for AccessData tools
- Install FTK Imager, FTK, PRTK, Registry Viewer, and the dongle drivers

#### 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
- Navigate evidence items
- Use the properties and interpreters windows
- Validate forensic images
- Create Custom Content Images
- Capture active RAM

#### Lab

This lab introduces the Forensic Toolkit Imager interface, and demonstrates how to acquire, preview, convert, export, and validate evidence.

During this lab, students will perform the following tasks:

- Image a USB device.
- Navigate the image file structure.
- Preview evidence.
- Export files, folders, and hash sets.
- Convert an acquired image to another format.
- Verify an image.
- Image an individual partition.
- Image custom content.
- Image a CD.

### Module 3: 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**

The objective of this lab is to teach students how to create users in FTK, start a case, and navigate the FTK Interface. During this lab, students will perform the following tasks:

- Create and add users.
- Review the FTK Interface.
- Create a new case.
- Review FTK interface.
- Customize the interface view.
- Add evidence to a case.

**Module 4: 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**

The objective of this lab is to expand on the FTK interface and demonstrates advanced features used to view and identify evidence.

During this lab, students will perform the following tasks:

- Manage evidence by highlighting and checking files.
- Manage bookmarks.
- Create custom column settings.
- Change the time zone display.
- View file properties.
- View metadata.
- View compound files.
- View files in the recycle bin.
- Use the Copy Special feature to copy column information.
- Export files and folders.
- Data carve evidence items.
- Decrypt EFS files.

**Module 5: 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**

The objective of this lab is to demonstrate the advanced features used to view and identify graphic and email evidence and export hash sets from FTK.

During this lab, students will perform the following tasks:

- 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 6: 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 7: Filtering the Case

### Objectives

- Explain the basic hierarchical structure of the File Filter Manager.
- Design and apply filters to narrow case evidence.
- Use filters in conjunction with containers and file lists in FTK to further narrow evidence.
- Explain the function of the Default Filter and Large Graphic Filter commonly used in case investigation.

### Lab

- Use File Filter Manager to create basic filters.
- Create a default filter.
- Create a bookmark filter.

## Module 8: Regular Expressions

### Objectives

- Create a basic regular expression that includes the following elements:
  - Operators and Literals
  - Character Classes
  - Sets
  - Function Groups
  - Repeat Values

### Lab

- Create a regular expression and add it to the list of expressions in the FTK Live Search tab.
- Perform a live search using the regular expression you created.

## 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.

### 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 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.

## Module 11: Windows Registry

### Windows 9x Registry

- Describe the function of the Windows registry.
- Identify the files that make up the Windows 9x registry.
- Describe how the registry is organized.
- Identify forensic issues associated with multiple profiles on Windows 9x systems.

### Windows 2000 and XP Registries

- Identify the files that make up the Windows 2000 and XP registry; list their locations; and describe the information they contain.
- Identify reasons to resolve a user to a SID.
- Identify notable tracking differences in the registry on FAT and NTFS systems.

## Registry Access and Concerns

- Locate registry files on Windows 9x and 2000/XP systems.
- Describe how Windows systems manage information such as Instant Messenger accounts for multiple user profiles.
- Describe how Windows protects active registry files.
- Describe methods of seizure that maintain the integrity of information in the registry.
- Identify overt and covert methods to access Windows registry files.
- View and export active registry files using FTK Imager and Registry Viewer.

### Lab

- Export active registry files.

## Module 12: Registry Viewer

### Working with Registry Viewer

- Identify the menu and toolbar options in Registry Viewer.
- Describe how Registry Viewer displays MRU lists.
- Describe the function of the Registry Viewer's common areas.
- Describe different methods to search the registry.
- Create a report in Registry Viewer.
- Create a Summary report in Registry Viewer.
- Utilize Registry Viewer help.

### Gathering Evidence and Reporting

- Identify hidden key values in the registry.
- Decrypt user information from the PSSP key.
- Use the SAM file to determine a user's last logon time.
- Use the SYSTEM file to determine a computer's time bias.
- Use the SOFTWARE file to determine a computer's current settings.
- Describe the function of Windows restore points.
- Identify what versions of Windows maintain restore points.
- List the information stored in Windows restore points.

### Lab

- Install Registry Viewer.
- Review the Registry Viewer interface.
- Examine a Windows registry using Registry Viewer and Regedt32 and compare the differences.
- Decrypt Protect System Storage Provider (PSSP) key.
- Search registry files, including hidden keys.
- Generate reports in Registry Viewer.
- Recover information from the SAM, SYSTEM, and SOFTWARE file.
- Use Registry Viewer to access registry information from Restore Points.

- Use wildcard values in a report.
- Create Summary Reports in Registry Viewer.
- Integrate the Registry Viewer reports in your FTK case report.

## Module 13: ID Theft 1 Practical

This practical requires you to apply information from the preceding modules to investigate a mock case.

## Module 14: The Recycle Bin

### Objectives

- Describe the function of the Windows Recycle Bin.
- Identify the differences in the Recycle Bin on FAT and NTFS systems.
- List what information can be recovered from the INFO2 file.
- Describe how FTK parses and displays INFO2 files.
- Describe what happens when a file is deleted or removed from the Recycle Bin.
- Explain what happens when a user empties the Recycle Bin.
- Identify how forensic information can still be retrieved when items are removed from the Recycle Bin.
- Describe the forensic implications of files located in the Recycle Bin.
- Describe the function of the Orphan folder.
- Create a regular expression to recover unallocated INFO2 file records.

### Lab

- Retrieve deleted evidence from the Recycle Bin.
- Locate a specific user's files within the Recycle Bin.
- Retrieve the following information from INFO2 files:
  - Deleted File Path
  - Deleted File Index
  - Deleted File Drive
  - Deleted File Date and Time
  - Deleted File Physical Size
- Create a regular expression that locates INFO2 files.

## Module 15: Link and Spool Files

### Objectives

- Define the function of a link file.
- Identify what evidentiary information is contained in link files.
- Describe how FTK parses and displays link files.
- Define the function of a spool file and its related files.
- Identify what evidentiary information is contained in spool files.

**Lab**

- Use FTK to recover forensic information from link files, including the MAC address of the target machine.
- Use FTK to recover forensic information from spool files.
- View USB Mass Storage device registry values.
- Use link file data to associate a file with a USB drive.

**Module 16: Encrypting File System****Objectives**

- Describe how EFS works.
- List what information is required to recover EFS encrypted files on Windows 2000 systems.
- List what information is required to recover EFS encrypted files on Windows XP SP1 and higher systems.
- List potential problems associated with recovering EFS encrypted data.

**Lab**

- Recover EFS encrypted files on Windows 2000 and XP systems.
- Create EFS encrypted files.

**Module 17: Processing Information Lab—EFS**

This lab requires you to apply information from the Decryption Technology and Encrypting File System modules to complete the following:

- Decrypt EFS files in FTK.
- Bookmark decrypted EFS files and alternate data streams.
- Export the bookmarked items as part of your case report.

**Module 18: ID Theft 2 Practical**

The final practical is a cumulative exercise that requires you to apply information from the entire class to complete your investigation on the ID Theft case.

## Practical Skills Assessment

The AccessData Technology class includes a Practical Skills Assessment (PSA). This performance-based assessment requires participants to apply key concepts presented during the class 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 class 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.