AccessData Forensics BootCamp

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

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, Registry Viewer and LicenseManager.
- Use FTK Imager to preview evidence, export evidence files, create forensic images and convert existing images.
- 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.
- 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.
- Use regular expressions to perform live searches.
- Import search lists for Indexed searches in FTK.
- Use the FTK Data Carving feature to recover files from unallocated disk space.
- Create and customize reports.
- Use custom dictionaries and dictionary profiles to recover passwords in PRTK.
- Utilize the index in FTK to create custom dictionaries in PRTK.
- Create regular expressions.
- Use the Registry Viewer to locate evidentiary information in Windows 2K and XP registry files.
- Integrate Registry Viewer with FTK.
- Recover forensic information from Recycle Bin INFO2 files.
- Recover forensic information from the following Windows XP artifacts:
    - Thumbs.db files
    - Metadata
    - Link and Spool Files
    - Alternate Data Streams
    - Windows XP Prefetch
- Use a FTK word list to create a custom dictionary, profile, and biographical dictionary in PRTK.
- Add SAM and Syskey values to PRTK to recover passwords and decrypt encrypted files.
- Recover EFS encrypted files on Windows 2000 and XP systems.

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 required applications and 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.

Interactive Demonstrations and Student Practicals

- Navigate FTK Imager interface.
- Create an image.
- Preview evidence.
- Convert an acquired image to another format.
- Verify an image.
- Create a custom content image.
- Export files, folders, and hash lists from an image.
- Detect EFS encryption.
- Acquire an image of evidence data.
- Mount and unmount images.
- Use FTK Imager to locate file system information.

Module 3: Registry Viewer Introduction

Objectives

- Describe which files comprise the Windows Registry.
- Discuss the elements of the Registry Viewer interface.
- Identify the key features of the Registry Viewer.
- Outline the use of FTK with other tools.
- Create a basic report from FTK.
- Seamlessly launch Registry Viewer from an FTK case.
- Determine a user's time zone setting.
- Determine a user's SID.

Interactive Demonstrations and Student Practicals

- Navigate Registry Viewer interface.
- Create a SYSTEM registry report.
- Create a SAM registry report.
- Recover a user's SID number, user name, full name, logon count, and last logon time using a SAM registry file.
- Recover current time zone settings and control set information using a SYSTEM registry file.
- Generate registry reports.

Module 4: Working with FTK—Part 1

Objectives

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

Interactive Demonstrations and Student Practicals

- Manage user accounts in FTK.
- Create a case and assign users to the case.
- Walk through the process of backing up, deleting, and restoring a case.
- Differentiate between the processes of archiving a case, archiving and detaching a case, and attaching a case.
- Restore an image.
- Manage the following shared objects:
  - Custom Carvers
  - Custom Identifiers
  - Columns
  - File Extension Maps
  - Filters
  - Labels
- Manage case processing options.
- Navigate the FTK interface.
  - Menu bar and toolbars
  - Explore tab and QuickPicks
  - Overview tab and file content view options
  - Email, Graphics, Bookmarks, Live Search, and Index Search tabs
- Customize the FTK interface.
- Add evidence to an existing case.
- Add a memory dump file to a case.

Module 5: Working with FTK—Part 2

Objectives

- Change time zone display.
- Create and manage bookmarks.
- 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.

Interactive Demonstrations and Student Practicals

- Modify the time zone display in FTK.
- Manage bookmarks in FTK:
  - Create bookmarks.
  - Add to existing bookmarks.
  - Nest and delete bookmarks.
  - Create an empty bookmark to hold supplemental files.
  - Bookmark selections in files.
- View metadata and compound files.
- View and open registry files.
- View Index.dat entries.
- Examine Windows XP, Vista/Windows 7 Recycle Bins.
- Export files and folders.
- Create custom column settings.
- Use the Copy Special and Export File List Info features to export file information.
- Decrypt EFS files.
- Utilize automated and manual data carving to recover files from unallocated disk space.
- Create custom carvers.
- Use FTK to verify image integrity.

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.

Interactive Demonstrations and Student Practicals

- Manage the different viewing options in FTK.
- View EXIF data in graphics.
- Bookmark and flag graphics files.
- Create and export a graphics file hash list.
- 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.

Module 7: Regular Expressions

Objectives

- Understand basic Operators and Literals in RegEx.
- Learn 10 very useful characters and concepts of RegEx++, enabling you to write hundreds of expressions.
- Create and interpret a basic regular expression that includes Function Groups and Repeat Values.
- Integrate a new RegEx into FTK for use.

Lab

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

Module 8: Narrowing Your Focus

Objectives

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

Interactive Demonstrations and Student Practicals

- Manage the KFF database:
  - Edit the KFF database.
  - Import a new hash set.
  - Create a new group.
  - Run a KFF lookup.
- Flag files as Ignorable and Privileged.
- Perform a full text index search.
- Import search terms from a user-defined list.
- Search only checked items.
- Use dtSearch options.
- Use regular expressions to credit card numbers in the case evidence.
- Use the Ignore feature to ignore specific items in the case.
- Use the email tab and search features to recover evidence in a sample case.

Module 9: Filtering the Case

Objectives

- Explain basic concepts of rule-based filtering in FTK.
- Design a basic filter and use it to filter data.
- Manage shared filters.
- Discuss the use of compound filters.
- Explain the difference between global and tab filters.
- Import and export filters.

Interactive Demonstrations and Student Practicals

- Use File Filter Manager to create basic filters.
- Create a default filter.
- Create shared filters.
- Create a nested filter.
- Create a compound filter.
- Create tab filters.
- Import and export filters.

Module 10: Skill Builder Exercise—Practical 1

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

Module 11: Common Windows XP Artifacts

Thumbs.db Files

Objectives

- Define the Thumbs.db file.
- Define Thumbs.db behavior.
- Identify thumbnail graphics.
- Define EFS file changes and Thumbs.db behavior.

Lab

- Use FTK to recover graphics information from Thumbs.db files from Windows ME, 2000, XP and 2003 systems.

Metadata

Objectives

- Define metadata.
- Identify information commonly captured as metadata.
- Identify how FTK classifies and displays metadata.

Lab

- Use FTK to identify and recover metadata such as Fast Save, document summary information, embedded URLs and internal date and time information.

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.
- 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.

Alternate Data Streams

Objectives

- Identify the differences between named and alternate data streams.
- Identify forensic issues associated with alternate data streams.
- Identify how FTK displays alternate data streams.
- Describe how alternate data streams impact file size, disk space and file creation date.

Lab

- Create alternate data streams using Notepad.
- Create an alternate data stream in a graphics file.

Windows XP Prefetch

Objectives

- Accurately define Prefetch, Superfetch, and their related functions.
- Define the forensic importance of Prefetch Registry entries, Prefetch files, and the Layout.ini file.
- View and analyze pertinent Prefetch artifacts as they relate to case analysis and user behavior.

Lab

- View and recover Prefetch files in FTK Imager.

Module 12: 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.

Interactive Demonstrations and Student Practicals

- Export a word list from FTK and create a custom dictionary in PRTK.
- Create a biographical dictionary and user profile.
- Recover passwords from an encrypted Word document.

Module 13: 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 Professional Service Pack 1 (SP1) and later 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 14: Skill Builder Exercise—Practical 2

This practical requires you to apply information from the preceding modules to the ID Theft case.

Module 15: 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-sized 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 ODT formats.
- Generate reports in other languages.

Interactive Demonstrations and Student Practicals

- Create and modify reports.
- Manage report options:
  - Bookmarks
  - Graphics
  - File Paths, Properties, and Categories
  - Column Settings
  - Registry Selections
- Create a PDF report.

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 .