AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

This advanced five-day course 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, participants will perform the following tasks:

- Install and configure FTK, FTK Imager, PRTK, and Registry Viewer.
- Use FTK Imager to preview evidence, export evidence files, create forensic images and convert existing images.
- Use the Registry Viewer to locate evidentiary information in Windows 2K and XP registry files.
- 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.
- Create regular expressions.
- Import search lists for indexed searches in FTK.
- Use the FTK Data Carving feature to recover files from unallocated disk space.
- Use custom dictionaries and dictionary profiles to recover passwords in PRTK.
- Use a FTK word list to create a custom dictionary in PRTK.
- Create a user profile and biographical dictionary in PRTK.
- Add SAM and Syskey values to PRTK to recover passwords and decrypt encrypted files.
- 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
- Recover EFS encrypted files on Windows 2000 and XP systems.
- Create and customize reports.

The class includes multiple hands-on labs that allow students to apply what they have learned in the workshop.

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.

AccessData®

For a complete listing of scheduled courses, visit http://www.accessdata.com/training/calendar-and-syllabi

AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

(Continued)

Module 1: Introduction

Topics

- 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

Participants will install the UTK components—FTK, KFF Library, FTK Imager, Registry Viewer, and PRTK.

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.
- Mount images.
- Capture active RAM.

Labs

During the practical, participants acquire an image of a thumb drive, then explore the FTK Imager features and functions discussed in the module, including converting an image to a different image format, creating a Custom Content Image, and mounting an image.

Module 3: Windows Registry

Windows Registry 101

Objectives

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

Windows 2000 and XP Registries

Objectives

- 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 including a look a tracking mounted devices.

Module 4: Registry Viewer

Working with Registry Viewer

Objectives

- 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.

Lab

- Review the Registry Viewer interface.
- Harvest and view registry files.

For a complete listing of scheduled courses, visit http://www.accessdata.com/training/calendar-and-syllabi

AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

(Continued)

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.

Lab

During the practical, participants go through the introductory steps of processing a case, including creating a case, adding evidence to the case, and processing case evidence. Students will also perform basic system functions such as creating user accounts and defining different levels of permissions to a case, managing shared objects, and customizing the FTK interface.

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.

Lab

The labs in this module guide participants through more advanced functions in processing case evidence. During the practical, participants will bookmark evidence, view metadata and compound files, examine registry files, recover deleted files from the Recycle Bin, export case files and folders, create custom column settings, decrypt files, and use the data carving feature to recover evidence items from file slack and unallocated space.

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.
- 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

During the practical, participants explore FTK features to view, sort, and export email and graphic artifacts from the case. Students will also create custom columns for graphics and email, export email and graphics files, and create a hash list.

For a complete listing of scheduled courses, visit http://www.accessdata.com/training/calendar-and-syllabi

AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

(Continued)

Module 7: Narrowing Your Focus

Objectives

- Narrow evidence items using the Known File Filter, 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

During the practical, participants learn how to effectively sort through case evidence to locate items of interest. Students will use the KFF database to ignore or flag known files, perform keyword searches, use dtSearch options to customize a search, and use regular expressions to search case evidence for pattern data such as credit card numbers or IP addresses.

Module 2: 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.
- Integrate a new TR1 Expression 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 the regular expression you created.

Module 8: 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.

Lab

During the labs, participants create filters to locate specific items of interest. Students will further refine filter results using compound filters. Finally, students will have a change to import and export filters so they can share filters with co-workers and colleagues.

Module 6: 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 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.

For a complete listing of scheduled courses, visit http://www.accessdata.com/training/calendar-and-syllabi

AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

(Continued)

Lab

- Retrieve deleted evidence from the Recycle Bin.
- Use a regular expression to locate INFO2 files.
- Retrieve the following information from INFO2 files:
  - Deleted File Path
  - Deleted File Index
  - Deleted File Drive Number
  - Deleted File Date and Time

Module 7: 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.

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 link file data to associate a file with a USB drive.
- Use FTK to recover forensic information from spool files.

Alternate Data Streams

Objectives

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

Lab

- Identify alternate data stream files in your case.

Windows 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 Prefetch settings in the Registry.
- View Prefetch entries in FTK to find the last date and time an application was launched.
- View Prefetch entries in FTK to determine the number of times an application was launched.

Module 9: 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.
- Recover Windows logon passwords.

For a complete listing of scheduled courses, visit http://www.accessdata.com/training/calendar-and-syllabi

AccessData Advanced Forensics

Forensic Toolkit / FTK Imager / Registry Viewer / Password Recovery Toolkit

Intermediate • Five-Day Instructor-Led Course

(Continued)

Lab

- Export encrypted files from a case.
- Export a word list and create a custom dictionary.
- Create a Biographical dictionary.
- Create a profile.
- Recover a password.
- Locate SAM and SysKey Files
- Attack and decrypt encrypted files, then list the recovered passwords.

Module 10: Encrypting File System

Objectives

- Describe how EFS works.
- List the information required to recover EFS encrypted files on Windows 2000 systems.
- List the information 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

- Create EFS encrypted files.
- Recover EFS encrypted files in FTK.

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-sized graphics in the report directory
  - Export and link video files
  - Export rendered videos and thumbnails
  - 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 the following formats:
  - PDF
  - HTML
  - RTF
  - WML
  - XML
  - DOCX
  - ODT
- Generate reports in other languages.

Lab

During the practical, participants create multiple reports from a single case to explore all options available from the report wizard. They build from a very basic report to a detailed report that contains customized report items.

Practical Skills Assessment

The Windows Forensics 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, visit http://www.accessdata.com/training/calendar-and-syllabi