

Windows Forensics

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

Advanced • Three-day Instructor-led Class



AccessData[®]

This advanced AccessData training course provides the knowledge and skills necessary to use AccessData[®] products to conduct forensic investigations on Microsoft[®] Windows[®] systems. Participants will learn where and how to locate Windows system artifacts using Forensic Toolkit[®] (FTK[™]), FTK Imager[™], Registry Viewer[™] and Password Recovery Toolkit[™] (PRTK[™]).

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

- Create and apply custom file filters.
- Use advanced search options such as stemming, phonic, AND/OR operators and fuzzy logic.
- Create regular expressions.
- Create a Known File Filter[™] (KFF[™]) from an empty HDB file.
- Use the Registry Viewer to locate evidentiary information in Windows 9x, 2K and XP registry files.
- Integrate Registry Viewer with FTK.
- Recover forensic information from Recycle Bin INFO2 files.
- Recover forensic information from Thumbs.db files.
- Identify and recover forensic information from OLE metadata.
- Recover forensic information from Windows link and print spool files.
- Use PRTK to recover user login passwords from the Windows SAM file and decrypt files with extended ASCII passwords.
- 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 alternate data streams.

Each day of training concludes with a hands-on lab that allows students 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 course is intended for forensic investigators with experience in forensic case work and a basic working knowledge of FTK, FTK Imager and PRTK.

To obtain the maximum benefit from this course, you should meet the following requirements:

- Read and understand the English language.
- Attend the AccessData Forensic BootCamp (Course 240) or have equivalent experience with FTK and PRTK.
- Have previous investigative experience in forensic case work.
- 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:
 - Forensic Toolkit—5,000 Item Authorized Version
 - FTK Imager
 - Registry Viewer
 - PRTK—WinZip SuperFast Attack
 - Distributed Network Attack[®] (DNA[®])—1 Server / 2 Clients Authorized Version

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Other forensic training organizations
- Course outline
- Helpful information

Lab

- Check system information.
- Select Windows Explorer display preferences.
- Prepare your system.

Module 2: FTK Overview

Objectives

- Navigate the FTK interface.
- List six formats the FTK Data Carving tool can recover.
- Describe the function of the File Filter Manager.
- Define the function of each dtSearch option.

Lab

- Review FTK options and features.

Module 3: 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 4: KFF Management

Objectives

- Describe the function of the KFF.
- List the content sources for the KFF.
- Create hash sets in FTK Imager and FTK.
- Import custom Alert or Ignorable hash sets to the KFF.
- Display hash set properties.

- Set the location of the KFF database in FTK Preferences.
- Create a KFF from an empty HDB file.
- Use the KFF Editor to change an Ignore hash set to an Alert set in the KFF.

Lab

- Create and export custom hash values.
- Import custom Ignore and Alert hash sets to the KFF.
- Display hash set properties.
- Set the location of the KFF database.
- Use KFF Editor to change the status of hash sets in the KFF.

Module 5: Windows Registry

Windows 9x Registry Objectives

- 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 Registry Objectives

- Identify the files that make up the Windows 2000 and XP registry 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 2K/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

- Create a new Windows user account.
- Track how Windows manages the account settings for the new user account.
- Export active registry files.

Module 6: Registry Viewer

Working with Registry Viewer

- Identify the menu and tool bar options in Registry Viewer.
- Describe how Registry Viewer displays MRU lists.
- Describe the function of the Registry Viewer's common areas.
- Create a report in Registry Viewer and integrate the report with the FTK case report.
- Create a summary report in Registry Viewer.
- Utilize Registry Viewer Help.
- Within FTK, view registry files and launch Registry Viewer.
- Use Registry Viewer to export registry word lists to assist password recovery.

Gathering Evidence and Reporting

- Identify hidden key values in the registry.
- Decrypt user information from the Protected Storage System Provider (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

- Examine a Windows registry using Registry Viewer and Regedt32 and compare the differences.
- Access the system volume information for a specific user profile in FTK.
- Use Registry Viewer to access registry information from Restore Points.
- Recover information from the SAM file.
- Recover information from the SYSTEM file.
- Recover information from the SOFTWARE file.
- Create reports in Registry Viewer.
- Use wildcard values in a report.
- Create Summary Reports in Registry Viewer.
- Integrate the Registry Viewer reports in your FTK case report.

Module 7: ID Theft Practical

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

Module 8: 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 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.

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.
- Locate an Orphan folder on an NTFS drive.

Module 9: Thumbs.db Files

Objectives

- Describe how files are created in the Thumbs.db database file.
- Describe what happens to the Thumbs.db file when a graphic is deleted.
- Describe how different operating systems handle Thumbs.db files.
- Describe how Thumbs.db files handle EFS encrypted files.
- Identify how FTK classifies and displays Thumbs.db files.

Lab

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

Module 10: 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.

Module 11: Link and Spool Files

Objectives

- Define the function of a link file.
- Identify what evidentiary information is contained in 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 view print spool files.

Module 12: ID Theft—Practical 2

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

Module 13: PRTK Alternate Features

Objectives

- Describe the following feature enhancements in PRTK:
 - EFS Decryption Modules
 - SAM and Syskey Decryption
 - Dragging and Dropping Registry Files
 - Extended ASCII Passwords
- Describe the process of acquiring Windows login passwords contained in the SAM file.
- Describe how to enter extended ASCII passwords.

Lab

- Install PRTK.
- Add a Syskey value to PRTK.
- Recover Windows user login passwords.
- Decrypt files with extended ASCII character passwords.

Module 14: 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

- Create EFS encrypted files.

Module 15: 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.

Module 16: Processing Information Lab—EFS and ADS

This lab requires you to apply information from modules 12, 13 and 14 to complete the following:

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

Module 17: ID Theft—Practical 3

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

Practical Skills Assessment

The Windows Forensics course 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 Pricing

- \$2,095 (US) base price
- \$2,645 (US) with FTK and Registry Viewer
- \$2,995 (US) with Ultimate Toolkit (Up to three additional packages of the Ultimate Toolkit may be purchased within 10 business days of attending the class for \$1,249 per unit.)

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

For a complete listing of scheduled courses or to register for available courses, see www.accessdata.com.



Ultimate
The Complete
AccessData
Software Kit
Toolkit™



Forensic
Find Computer Evidence
Quickly & Easily
Toolkit™



Password
Recover
Passwords
Quickly & Easily
Recovery Toolkit™



Registry
Find Registry Data
Quickly & Easily
Viewer™



Distributed
Putting
Idle Time
To Work
Network 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, Distributed Network Attack, DNA, 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.