Windows Forensics—FTK 3

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

Advanced • Three-day Instructor-led Class

This advanced AccessData training class 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 class, participants perform the following tasks:

- 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 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 EFS encrypted files on Windows 2000 and XP systems.

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 class 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 class, you should meet the following requirements:

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.

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

Topics

- Introductions
- Class materials and software
- Prerequisites
- Class outline
- Helpful information

Lab

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

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.

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 3: Windows Registry

Windows Registry 101

- 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

- 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

- 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 files.
- 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 5: ID Theft Practical

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

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.

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 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 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.
- 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.

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 8: ID Theft—Practical 2

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

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.

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.

Module 10: 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.

Lab

- Add SAM and Syskey values to PRTK.

Module 11: 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.

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 or to register for available courses, see www.accessdata.com .