

Windows Forensics—Registry

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

Advanced • Three-day Instructor-led Class



AccessData[®]

This advanced AccessData training class provides the knowledge and skills necessary to use AccessData[®] products to conduct forensic investigations on the Microsoft[®] Windows[®] registry. Participants will learn where and how to locate registry 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:

- Use FTK Imager to obtain a clean copy of the Windows registry.
- Backup individual registry keys, registry files, and whole registry sets.
- Use a Regular Expression to carve registry key names from unallocated space.
- Identify and locate potential trace evidence in the regf and hbin blocks.
- Use the SAM file to identify system user accounts, user information and properties, user logon password information, user profiles, and group membership.
- Use the SYSTEM file to identify computer name, time zone, last shutdown time, network connections, and hardware information.
- Use the SECURITY file to identify current and archived system passwords, if present.
- Break the SECURITY file passwords in PRTK.
- Use the SOFTWARE file to identify USB volume serial numbers in Windows Vista, recycle bin settings, user profiles, wireless connections, printer information, evidence of uninstalled software, application restrictions, autologon settings, and cached password settings.
- Identify individual application settings such as Internet Explorer (IE) main settings; IE use count; Internet Account Manager; URL history; IE5 history settings; MSN accounts; mount points and mapped drives; and FTP site settings.

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, Registry Viewer, and PRTK. Prior familiarity with the Microsoft Regedit utility is also helpful.

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

- Read and understand the English language.
- Attend the AccessData Forensic BootCamp and Windows Forensics 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

- Use the Windows registry, rather than Windows Explorer, to configure Explorer settings.
- Install the following AccessData software:
 - FTK Imager
 - Registry Viewer
 - PRTK

Module 2: Registry Utilities

Topics

- Use Regedit—a non-forensic tool with editing capabilities—to perform the following functions:
 - View registry files.
 - Alter registry keys.
 - Backup individual Windows registry keys, files, and entire registry sets.
- Use FTK Imager to capture Registry files.
- Discuss forensic registry utility requirements.
- Use Registry Viewer to perform the following functions:
 - Navigate the registry.
 - View encrypted registry values.
 - Search the registry for specific values.

Lab

- Navigate the registry using Registry Viewer and Regedit.
- Use FTK Imager to obtain a clean copy of the workstation's registry files.
- Backup the registry using Windows utilities.

Module 3: Registry 201

Objectives

- Discuss the function of the Windows registry and its importance to forensic investigations.
- Describe the basic structure of the Windows registry.
- List the files that make up the Windows registry and identify the data associated with each file.
- Navigate the Windows registry structure and locate forensically relevant information.
- Discuss basic registry structure including hives; keys; subkeys and values; and regf and hbin blocks.
- Explain how to capture memory in first response situations.

- Identify potential registry evidence that may be found in memory.
- List practical search methods for retrieving registry information in memory.
- Carve key names from unallocated space and memory capture.

Lab

- Compare registry structure in Registry Viewer and Regedit.
- Locate and view registry files in FTK Imager.
- Navigate through the regf and hbin blocks in the SAM file to locate key values.
- Carve regf and hbin blocks.
- Carve key names for an uninstalled application.
- Use memory captures to obtain registry keys from memory.
- Identify key values from recent computer operations that may not be written to the registry keys

Module 4: Preliminary Case Info

Objectives

- Generate the following Registry Viewer reports:
 - SAM Info (Users)
 - SYSTEM Info (Time Zone/Computer Name)
 - SOFTWARE Info (Registered User/Current Operating System/Profiles)
 - NTUSER Info (E-Mail Accounts, Printers)

Lab

- View SAM, SYSTSEM, SOFTWARE, and NTUSER files in Registry Viewer.
- Generate standard and summary reports in Registry Viewer.

Module 5: Security Accounts Manager Registry Files (SAM)

Objectives

- Use the SAM file to identify the following information on a target system:
 - System user accounts
 - User information and properties
 - User logon password information
 - User profiles
 - Groups and group membership
- Describe how Security Identifiers (SIDs) are used in the SAM file.
- Explain how Relative Identifiers (RIDs) are used in the SAM file.
- Describe the application behavior of the SAM file.

Module 6: Practical

- Carve a set of associated regf and hbin blocks from unallocated space.
- Identify recent dates and times of regf and hbin blocks.
- Identify the registry file type that carved regf blocks come from.
- Locate a specific key name in the hbin block and identify its associated date and time.
- Create a preliminary report in FTK.
- Document user information, including group association, using the SAM file.

Module 7: SYSTEM Registry Files**Objectives**

- Use the SYSTEM file to identify the following information on a target system:
 - Computer Name
 - Time Zone Information
 - Last Shutdown Time
 - Hardware Information
 - o Floppy Present
 - o Drives Present
 - o Human Interface Devices
 - o LPT Ports
 - o Storage Devices, Fixed And Removable
 - o USBSTOR – USB Storage Devices
 - o Mounted Devices
 - o Clear Page File Memory On Shutdown
 - o Network Connections
 - Disabled 8.3 Filename Generation
 - Processor Information
 - CD Autorun settings

Lab

- Use the SYSTEM file to identify information on a target system.
- Use the SYSTEM file, link files and log files to identify information on specific USB drives.
- Discuss the ramifications of network connections.

Module 8: SECURITY Registry Files**Objectives**

- Use the SECURITY file to identify the following information on a target system:
 - Passwords and historical passwords in a domain environment.
 - The password from the user's last logon.
- Discuss traditional methods used to crack a user's logon password.

Lab

- Use the SECURITY file to identify information on a target system.
- Use PRTK to recover passwords stored in the SECURITY file.

Module 9: SOFTWARE Registry Files**Objectives**

- Use the SOFTWARE file to identify the following information on a target system:
 - USB Volume Serial Numbers In Vista (Readyboost)
 - Class Identifiers (CLSIDs)
 - Recycle Bin Settings
 - User Profiles
 - Wireless Connections
 - Printer Information
 - Evidence Of Uninstalled Software
 - Software Set To Run On Startup
 - Application Restrictions (Winlogon Restrictions)
 - Autologon Settings
 - Cached Passwords Enabled

Lab

- Use the SOFTWARE file to identify information on a target system.
- View USB ReadyBoost.

Module 10: Application Behavior Part I**Objectives**

- Discuss user behavior and how to identify culpability using Registry keys and values.
- Identify where user behavior is stored for each individual.
- Identify the following individual application settings:
 - Internet Explorer Browser Main Settings
 - Internet Explorer Use Count
 - Internet Account Manager
 - URL History
 - IE5 History Settings
 - MSN Accounts
 - Windows Explorer Settings
 - Mount Points And Mapped Drives
 - FTP Site Settings
 - UserAssist values that show how frequently an application is used
 - Screensaver Lockout Enabled
- Identify new application behavior.

Lab

- Identify application settings on a target system.

Module 11: Application Behavior Part II

Objectives

- Locate WinZip evidence in the registry.
- Locate Google Hello by Picasa evidence in the registry.
- Locate peer-to-peer client evidence (Kazaa) in the registry.

Lab

- Load WinZip, then view relevant registry settings.
- Load Google Hello, then view relevant registry settings.
- Load Kazaa, then view relevant registry settings.

Module 12: Trojan Horse Defense Issues

Objectives

- Discuss the Trojan Horse defense.
- Define Trojan Horse applications.
- Use the registry to determine if a Trojan Horse is present.

Lab

- Locate Trojan Horse settings in the registry.
- Determine underlying object of specific Trojan Horse applications.

Practical Skills Assessment

The Windows Forensics—Registry class includes an optional 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.

© 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, 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.