

Windows Forensics—Vista

Forensic Toolkit, FTK Imager and Registry Viewer

Advanced • Three-day Instructor-led Workshop



AccessData[®]

This advanced AccessData[®] workshop provides the knowledge and skills necessary to analyze Microsoft[®] Windows Vista[™] operating system artifacts and file system mechanics using Forensic Toolkit[®] (FTK[®]), FTK Imager, Password Recovery Toolkit[®] (PRTK[®]) and Registry Viewer[®].

During this three-day workshop, participants will review the following:

- GUID Partition Tables (GPT): Students will use FTK Imager to navigate the new GPT formatted drive partitioning scheme.
- File Structure Changes: Students will learn the mechanics of reparse and mount points in the Windows Vista file structure.
- BitLocker Full Volume Encryption (FVE): Students will use FTK Imager and Windows Vista technology to decrypt and acquire a sector-by-sector image of an FVE drive.
- Vista Security: Students will review the concepts behind the new Protected Mode security system in Vista and how these protective systems affect forensic analysis.
- Windows Vista Artifacts such as:
 - Vista EFS
 - Recycle Bin
 - Thumbcache
 - Activity History
 - Link and Spool Files
 - Windows Event Logs
 - Volume Shadow Copy
 - Windows Vista Registry
 - NTUSER.DAT Changes
 - SAM Hive User Changes
 - System USBStor Information
 - Updated EFS Algorithms
 - Updated File Recovery Mechanics
 - Updated SuperFetch Structure
 - Enhanced Thumbs.db Functionality
 - Local Machine and Browser Indices
 - Structure and Content Changes
 - Enhanced XML Output and Viewing
 - Previous File Version Recovery (SVI)
 - PSSP, MRU and UserAssist Changes
 - Domain and User Value Additions
 - Device Identification and Protection

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

Prerequisites

To obtain the maximum benefit from this workshop, attendees should be familiar with:

- Windows XP forensic analysis
- Windows NT file system (NTFS) mechanics
- FTK, FTK Imager, Registry Viewer, and PRTK

Course Materials and Software

You will receive the student training manual and CD containing the training material, lab exercises and course-related information.

AccessData

384 South 400 West, Suite 200, Lindon, UT 84042 • www.accesdata.com

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Course outline
- Helpful Information
- Review changes between Windows Vista and Windows XP.

Lab

- Check system information.
- Install software.
- Set up Windows Explorer.

Module 2: Bitlocker

Objectives

- Describe Bitlocker technology and how it works in Windows Vista.
- List the Bitlocker requirements.
- Describe how Bitlocker uses TPM technology.
- Describe how Windows Vista manages the Bitlocker encryption keys.
- Describe Bitlocker encryption and decryption methods.
- Identify Bitlocker encrypted files.
- Recover Bitlocker encrypted media.
- Image a Bitlocker drive.

Lab

- Decrypt a Bitlocker image.

Module 3: GUID Partition Table (GPT)

Objectives

- Describe the GUID Partition Table (GPT).
- Describe the Extensible Firmware Interface (EFI) and how it relates to the GPT.
- List the GPT rules.
- Explain how Windows Vista generates the GUID.
- Identify the differences between GPT and MBR formatting.
- Describe the GPT structure and offsets.

Lab

- Navigate a GPT partitioned drive.
- Parse a GPT partitioned drive.

Module 4: File Structure and Security

Objectives

- Review the following Vista file structure changes:
 - User File Locations
 - System File Locations
 - Reparse Points
- Describe how Protected Mode affects artifacts.
- Describe how Protected Mode affects forensic applications.
- Describe how User Access Levels (ACLs) are managed in Windows Vista.

Lab

- Navigate the Windows Vista file structure.
- Demonstrate how Reparse Points work in Windows Vista.
- View the artifact changes created by the Protected Mode Vista security system.
- Load the local hard drive in FTK Imager.

Module 5: Windows Vista Transactional Logs for Files (TxF) and Registry (TxR)

Objectives

- Describe the Windows Vista Transactional File System.
- Describe how to enable and view Transactional Logs for the Windows Vista Transactional File System and Registry.

Lab

- Simulate recovery of transactional logs.
- View and recover artifacts from transactional logs including:
 - Date and Time changes to the system
 - USB device attachment
 - Logon and Logoff tracking by user

Module 6: Practical Lab

- Open a Bitlocker image.
- Image a Bitlocker drive.
- Identify and navigate a GPT formatted system.
- Use the Vista system to locate and document changes in user and system file locations.

Module 7: Registry 1

Objectives

- Describe the Windows registry.
- Review the Windows XP SYSTEM, SOFTWARE, and NTUSER.DAT registry files.
- Discuss the primary changes in the Windows Vista SYSTEM, SOFTWARE, and NTUSER.DAT registry files.

Lab

- Use the SAM file to identify the system users.
- Use the SYSTEM file to identify the computer name and time zone.
- Use the SOFTWARE file to identify the registered owner of the Windows Vista operating system.
- Use the NTUSER.DAT file to identify specific user behavior artifacts.

Module 8: Registry 2—DPAPI and IntelliForms

- Discuss the use of IntelliForms Registry keys to store user passwords, search terms and form data.
- Define Data Protection application programming interface (DPAPI).
- Recount the steps to encrypt IntelliForms.
- Decrypt IntelliForms in FTK and PRTK.
- Document the results of IntelliForms decryption using PRTK.

Lab

- Decrypt IntelliForms with instructor.
- Decrypt IntelliForms individually.

Module 9: Registry 3—Readyboost

- Describe how Windows Vista handles system memory.
- Define ReadyBoost.
- List the ReadyBoost requirements.
- Identify ReadyBoost registry entries and describe how they can aid a forensic investigation.
- Explain how users can alter ReadyBoost registry entries.

Lab

- View ReadyBoost registry entries in an image.
- View ReadyBoost registry entries on a live machine using Regedit.
- Plug a USB device into the system and register it to ReadyBoost so you can view the changes to the registry entry.

Module 10: Event Logs

- Describe the function of Windows Vista event logs.
- Describe how event logs can be useful in a case investigation.
- Use the Windows Vista Event Log Viewer to review event logs.
- Use Windows Vista event logs to correlate the following system information:
 - Logon
 - Logoff
 - USB initialization
 - User initiated date and time changes

Lab

- View local machine event logs on a Windows Vista system.
- Locate the following system changes in the event log:
 - Date and time changes.
 - Connection to an unregistered USB device.
 - Logoff

Module 11: Shadow Copies and Restore Points

- Define restore points and shadow copies.
- Compare and contrast how restore points and shadow copies work in Windows 2K/XP and Windows Vista.
- Locate shadow copies.
- Use the VSSADMIN command to manage shadow copies.
- Use data carving and regular expressions to locate file headers, the actual file copy, and the \$MFT record archive in shadow copies.

Lab

- Navigate to the shadow copy location.
- Search and manual carve the following file components from a shadow copy:
 - \$MFT hit
 - Dates/times
 - File data
- Autocarve from a shadow copy.

Module 12: Live Mail

- Define Live Mail.
- Compare and contrast how MS Mail works in Windows 2K/XP with Live Mail in Windows Vista.
- Describe the Live Mail structure.
- Locate the Live Mail mailbox.

Lab

- Locate and view Live Mail.

Module 13: Student Practical

- Create a preliminary case report.
- Use the Windows registry to determine if last accessed date and UAC were enabled.
- Find the last USB device connected to the system.
 - List the document ID number.
 - Identify which drive it occupied.
 - Document the date and time in the setup api.log file.
 - Identify the ReadyBoost volume name.
- Decrypt IntelliForms.
- Use Event Logs to identify the following information:
 - Last logon time
 - Last logoff time
 - Last USB employed
 - User-initiated time changes
- Navigate LiveMail mailboxes and locate specific messages.
- Locate a valid shadow copy.
- Manually carve a document from a shadow copy.
- Manually carve a graphic from a shadow copy.
- Autocarve from a shadow copy.

Module 14: \$Recycle Bin

- Provide a brief overview of file recycling in the FAT, NTFS, and Vista file systems.
- Identify recycle bin locations.
- Describe recycle bin behavior.
- Describe the mechanics of file deletion for Windows 2K, XP, and Vista systems.
- Provide a brief description of the Master File Table tracking (\$MFT).
- Describe the \$MFT changes in deleted files.
- Explain how orphans are created.
- Find unallocated \$Recycle.Bin hits.

Lab

- View the XP Recycler.
- View Vista \$Recycle.bin.
- Identify the user associated with each recycle bin.
- Recover files from the Vista recycle bin.
 - Identify the original file name and location.
 - Identify the date and time the file was placed in the recycle bin.
- Bookmark recycle bin entries for report
- Create orphans and view the changes made to the \$MFT in FTK Imager.

Module 15: Thumbcache

- Provide a brief overview of thumbnail rendition in Windows ME, 2K, XP, and Server 2003.
- Identify the path and filenames of the thumbcache.
- Explain how Windows Vista renders thumbcache images.
- Parse a thumbcache entry.
- View thumbcache files in FTK.
- Identify file path information from thumbcaches files.

Lab

- Navigate to the thumbcache.
- View the cached files.
- View the archived graphics.
- Parse a thumbcache entry.
- Manually carve a thumbcache entry.

Module 16: Internet Artifacts

- Define Internet archiving and history tracking in Internet Explorer.
- Define index.dat files.
- List User Access Control (UAC) limitations in Internet Explorer 7 and Vista.
- Describe how Internet Explorer 7 stores and manages browser history.
- Discuss the forensic implications of the Microsoft Cover My Tracks utility.

Lab

- View locations of index.dat files.
- View a History index.dat.
- Run the Cover My Tracks MS utility to wipe deleted files and note the wiped results.

Module 17: Index Search

- Define the Microsoft index search capabilities and the associated forensic implications.
- Identify where local search terms are stored.
- Locate user search terms.

Lab

- Search for a document by filename.
- Search for text within a document.

Module 18: Office 2007

- Describe Office 2007 document architecture.
- Recover metadata in Office 2007 documents.
- Decrypt Office 2007 documents.

Lab

- View Office 2007 documents in hex, text, and native formats.
- Decrypt Office 2007 documents.

Module 19: Student Practical Lab

- Recover files from the Windows Vista recycle bin.
- View cached files and archived graphics using thumbcache files.
- Manually carve a thumbcache entry.
- Search for a document by filename.
- Search text within a document.
- Decrypt Office 2007 documents and recover file metadata.

Practical Skills Assessment

The AccessData Windows Vista 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.

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

© 2008 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, 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.