

Windows Forensics—Windows 7

Forensic Toolkit, FTK Imager and Registry Viewer

Advanced • Three-day Instructor-led Class



AccessData[®]

This advanced AccessData[®] training class provides the knowledge and skills necessary to analyze Microsoft[®] Windows 7[™] operating system artifacts and file system mechanics using Forensic Toolkit[®] (FTK[®]), FTK Imager, Password Recovery Toolkit[®] (PRTK[®]) and Registry Viewer[®].

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

- **Window 7 Overview:** Students will learn the new features of Microsoft Windows 7 and review the key areas where features remain unchanged from Vista and XP.
- **BitLocker Full Volume Encryption (FVE):** Students will use FTK Imager and Windows 7 technology to decrypt and acquire a sector-by-sector image of an FVE drive, including the new BitLocker To Go.
- **System Changes:** Students will discuss Windows 7 disk structures and drive partitioning as well as the Windows 7 ExFat and NTFS file systems.
- **Windows 7 Security:** Students will review the concepts behind the new User Access Control settings in Windows 7. Students will learn how these protective systems affect forensic analysis.
- **Windows 7 Registry:** Discuss the changes in the Windows 7 registry and recover forensic artifacts from the registry.
- **USB Devices:** Students will trace a USB device back to a system and recover forensic artifacts for mounted USB devices, including the volume serial number, the logged username that inserted the device, and the date and time the device was inserted.
- **VHD Drives:** This class will familiarize students with VHD drives. Students will create and manage a VHD drive, then navigate the drive in FTK Imager and add the drive as evidence in FTK.
- **Recovering Windows Vista artifacts:** Students will recover forensic artifacts from the following Windows 7 components:
 - Recent Folders
 - Jump Lists
 - Link files
 - Recycle Bin
 - NTUSER.DAT
 - SAM
 - SYSTEM
 - SOFTWARE
 - SECURITY
 - Libraries and Homegroups
 - Windows Event Logs
 - Thumbcache
 - Prefetch files and registry entries
 - Superfetch artifacts
 - Layout.ini

The class 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 class, attendees should be familiar with:

- BootCamp or equivalent experience with FTK 3.x, FTK Imager, and Registry Viewer
- Experience with Windows XP forensic analysis
- Familiarity with Windows NT file system (NTFS) mechanics

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

- Class outline
- Helpful Information

Lab

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

Module 2: Windows 7 Overview

Objectives

- Discuss new features of Windows 7 and its different version characteristics.
- Identify the artifacts that have not changed from previous versions:
 - System-related data
 - User-related artifacts
- Review Windows 7 folder structures:
 - Identify the location of user files and folders
 - Discuss supported partition schemes

Labs

The labs in this module are designed to familiarize participants with Windows 7 artifacts that have not changed their structure or folder location from Windows Vista.

Module 3: BitLocker and BitLocker To Go

Objectives

- Identify the fundamentals of BitLocker encryption and how it is implemented in the Windows 7 operating system.
- Successfully image and access data from a seized system that is protected by BitLocker.
- List the different modes of operation on a system drive where the operating system is protected.
- Provide an overview of the BitLocker To Go application and identify potential keys for recovery of data in unencrypted form.

Labs

The labs in this module guide participants through the following tasks:

- Use Windows 7 Ultimate to gain access to a Bitlocked drive.
- Create a Bitlocker To Go drive on a FAT and NTFS File system drive.
- Locate the BitLocker AutoUnlock key.

Module 4: GPT and File System Changes

Objectives

- Discuss Windows 7 disk structures and drive partitioning.
- Discuss the Windows 7 File System characteristics including ExFat and NTFS.

Lab

The labs in this module require you to navigate a GPT image, explore an exFAT disk, and use GUID partition tables to identify the addresses of various file system components.

Module 5: Recent Folder and Jump Lists

Objectives

- Identify the ways in which link files have changed in Windows 7.
- Describe what Jump Lists are and how they can be used in a forensic investigation.

Labs

The labs in this module introduce the new Jump Lists feature in Windows 7. During these labs, participants will create entries in the Windows Registry that link to Jump Lists in Explorer. Participants will then use FTK Imager and Registry Editor to view the data and recover forensic information.

Module 6: Security

Objectives

- Describe the three-tiered layer of the security model.
- Identify new locations for Windows artifacts.
- Review Registry artifacts and key information of interest.

Labs

The objective of the security lab is to review user account controls in Windows 7.

Module 7: Registry Introduction

Objectives

- Define the Windows registry structure and function.
- List the forensic benefits of the registry.
- Identify the hives that make up the registry and list the types of information associated with each hive.
- Discuss navigating the registry using traditional tools and Registry Viewer.
- Define different methods for obtaining both live registry files and registry files from an image.
- Categorize the three different methods of searching for data in Registry Viewer.

Labs

The labs in this module guide participants through the following tasks:

- Locate Windows registry artifacts in the file system.
- Navigate the Windows registry in Regedit.
- Navigate the Windows registry in Registry Viewer.
- Acquire Windows 7 registry files.
- Determine how applications write data to the Windows registry.
- Search the Windows registry with Registry Viewer.
- Create reports with Registry Viewer.

Module 8: Registry Artifacts

Objectives

- Define the forensic values found in the Windows 7 NTUSER.DAT file.
- Define the forensic values found in the Windows 7 SAM file.
- Define the forensic values found in the Windows 7 SYSTEM file.
- Define the forensic values found in the Windows 7 SOFTWARE file.
- Define the forensic values found in the Windows 7 SECURITY file.

Labs

The labs in this module guide participants through the following tasks:

- Recover forensic data from NTUSER.DAT MRU lists.
- Locate Microsoft Office artifacts in the registry.
- Recover NTUSER.DAT artifacts such as searches initiated from the Start button, typed paths, and UserAssist data.
- Recover artifacts from the PSSP.
- Recover file system registry artifacts such as MUI Cache and date and time information.
- Recover artifacts from the SAM file such as user RIDs and password hints from both active and deleted users.
- Recover artifacts from the SYSTEM file such as the computer name, time zone information, last accessed date and time stamp, and mounted devices.
- Recover artifacts from the SOFTWARE file such as the last logged on user, user information, wireless connections, and Recycle Bin information.
- Recover passwords from the SECURITY file.

Module 9: Tracking USB Devices

Objectives

- Define the function of the Mounted Devices Manager.
- List the forensic benefits of tracking drive identification.
- Determine when removable media was last inserted in the system.
- Determine when removable media was first inserted in the system.
- Resolve who was logged on when a device was inserted.
- Categorize other methods of identification of removable media.
- Discuss device behavior.

Labs

The labs in this module guide participants through the following tasks:

- Recover the drive identifier for a mounted device and the date and time the drive was mounted.
- Recover a mounted device's container identification number.
- Trace a USB device back to a system.
- Identify the date and time the USB was initially inserted as well as the time it was last inserted.
- Identify the logged username that inserted the device.
- Identify external USB HDDs.
- Associate system link files with files on a USB.
- Obtain a USB drive's volume serial number and name from link files.
- Use the SOFTWARE file to track a USB drive.

Module 10: Event Logs

Objectives

- Describe the location where Windows 7 event logs are stored within the file system.
- Use the Windows 7 event log viewer to import and examine log files.
- Use the Windows 7 event viewer to identify the following types of events:
 - System shutdown
 - USB installation
 - System clock changes
 - Wireless connections
 - ReadyBoost attachments
 - System Restore Point creation

Labs

During this lab, participants recover forensic artifacts from Windows 7 event logs.

Module 11: Libraries and Homegroups

Objectives

- Recover forensic artifacts related to Windows libraries.
- Recover artifacts related to Windows Homegroups.

Labs

The labs in this module introduce Windows 7 libraries and Homegroups with their associated artifacts.

Module 12: Recycle Bin

Objectives

- Compare and contrast the Windows XP Recycler with the Windows 7 \$Recycle.Bin.
- Identify the location and structure of the Windows 7 \$Recycle.Bin.
- List the values used to designate file status in the \$Recycle.Bin.
- Recover Recycle Bin artifacts from the Windows registry.
- Recover deleted file information.
- Describe the differences between deleted files and orphaned files.

Labs

The labs in this module familiarize participants with the Windows 7 \$Recycle.bin. Participants are also guided through the process of creating a regular expression that locates deleted entry records.

Module 13: Thumbcache

Objectives

- Review Thumbs.db in Windows XP.
- Compare Thumbcache in Windows 7 with Windows XP.
- Analyze Thumbcache files in FTK.
- Examine the Thumbcache architecture.

Labs

The labs in this module familiarize participants with the Thumbcache file location and structure. Participants are also guided through the process of recovering artifacts from Thumbcache files.

Module 14: Virtual Hard Drives and SSD Drives

Objectives

- Discuss the new solid state disk technology (SSD)
 - Data storage
 - Garbage collectors
 - Trim command
- Describe the new virtual hard disk (VHD) support feature in Windows 7 and how it can be used to control data storage.
- Create a virtual hard disk container.
- Describe how to encrypt the data.
- Describe how the virtual hard disk support feature in Windows 7 can be used to conceal potential evidence.
- List the best methods of detecting a VHD.
- Describe best practices in processing a VHD file with forensic tools.

Labs

The labs in this module guide participants through the following tasks:

- Create an encrypted VHD.
- Familiarize participants with VHD drives.
- Browse a VHD in FTK Imager.
- Add a VHD image as evidence in FTK.
- Search for a VHD on a suspect's machine.

Module 15: Superfetch and Prefetch

- 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.

Labs

During this lab, participants recover forensic artifacts from Windows 7 event logs.

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

© 2011 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.