Macintosh Forensics

Forensic Toolkit, FTK Imager and Password Recovery Toolkit

Advanced • Three-day Instructor-led Workshop

This advanced AccessData® training course provides the knowledge and skills necessary to recover and analyze forensic artifacts from the Macintosh operating system using Forensic Toolkit® (FTK®), FTK Imager, and Password Recovery Toolkit® (PRTK®). Participants will learn GPT drive structure and sound methodology for imaging Macintosh hard drives as well as how to obtain date and time information from Macintosh systems. In addition to working with the Macintosh operating system, participants will recover artifacts from Macintosh-associated programs such as Safari and Firefox browsers, iChat, and Apple Mail. Participants will also learn how to recover artifacts from iPod and iPhone devices.

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

- Use FTK and FTK Imager to examine HFS drive structure.
- Image, examine, and report on Macintosh evidence.
- Examine Property Lists and the SQLite databases on Macintosh systems to recover the same evidence found in Index.dat files, the registry, and link files on Windows systems.
- Obtain date and time information from Macintosh systems.
- Defeat the File Vault.
- Use FTK and PRTK to recover the user logon password.
- Recover artifacts from the Safari and Firefox browsers including cookies, download path entries, form data, browser history, cache files, bookmarks, chat files, and sign-on passwords.
- Recover iChat artifacts including AIM user names, user icons, user account information, saved transcripts, and download files.
- Navigate the Apple Mail directory structure to review user mailboxes, email messages, and attachments.
- Recover iPod artifacts including photos, contacts, and calendars.
- Recover iPhone artifacts including address book and calendar information, call history, text messages, photos, and voicemail.

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

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Course outline
- Helpful Information

Lab

- Check system information.
- Install software.

Module 2: Macintosh GPT Structure

Objectives

- Describe the Apple Extensible Firmware Interface.
- Describe the GUID Partition Table.

Lab

The objective of this lab is to use FTK Imager to navigate the Macintosh GUID Partition Table.

Module 3: Obtaining the Date and Time from a Mac

Objectives

- Describe the Mac Open Firmware and how it affects password protection and bootable partitions.
- Locate the date and time in Single User Mode.

Module 4: Imaging a Mac

Objectives

- Image a Mac for evidentiary use by removing the hard drive or using a bootable CD.
- Identify the advantages and disadvantages of each imaging method.

Lab

The objective of this lab is to image a Mac drive using FTK Imager and Raptor Live CD.

Module 5: Directory Structure—Finding Evidence

Objectives

- Identify the directory structure and location of important directories.
- Identify the user's Library directory and its content.
- Examine the Property Lists for forensic evidence.
- Examine the SQLite Databases for forensic evidence.

Lab

The objective of this lab is to use FTK to recover evidence from the Macintosh directory structure.

Module 6: Recovering the User Logon Password

Objectives

- Identify the Mac Password Hash files, where they are located and the encryption scheme.
- Recover the logon password using various methods.

Lab

The objective of this exercise is to use PRTK to recover the Mac user logon password.

Module 7: Application Data--Safari

Objectives

- Identify what evidentiary items Safari creates and where they are located.
- Identify what evidentiary items are created by the use of the Safari client and where they are located including:
  - Bookmarks
  - Downloads
  - Browsing Histories
  - Last Session
  - Cookies
- Identify what evidentiary items Safari caches and where they are located.

Lab

The objective of this lab is to recover artifacts from the Safari browser including bookmarks, download path entries, browser history, session information and cache files.

Module 8: Application Data—Firefox

Objectives

- Identify what evidentiary items Firefox creates and where they are located.
- Identify what evidentiary items are created by the use of the Firefox client and where they are located including:
  - Cookies
  - Downloads
  - Form Histories
  - Browsing Histories
  - Bookmarks
- Import Bookmarks for forensic analysis

Lab

The objective of this lab is to recover artifacts from the Firefox browser including cookies, download path entries, form data, browser history, cache files, bookmarks, chat files, and sign-on passwords.

Module 9: Application Data—iChat

Objectives

- Identify what evidentiary items are created by the use of iChat and where they are located including:
  - User account data
  - Contact information
  - User and contact pictures
  - Chat transcripts
  - Server information

Lab

The objective of this lab is to recover iChat artifacts including AIM user names, user icons, user account information, saved transcripts, and download files.

Module 10: Apple Mail

Objectives

- Identify what evidentiary items are created by the use of the Apple Mail and where they are located.
- Recover messages from Apple Mail.
- Recover attachments from Apple Mail.

Lab

The objective of this lab is to navigate the Apple Mail directory structure to review user mailboxes, email messages, and attachments.

Module 11: iPod Analysis

Objectives

- Handle and storing the iPod for evidentiary purposes.
- Image the iPod for evidentiary purposes.
- Identify what evidentiary items are created by the use of an iPod and where they are located including:
  - Photos
  - Contacts
  - Calendars

Lab

The objective of this lab is to recover iPod artifacts including photos, contacts, and calendars.

Module 12: iPhone Backup

Objectives

- Locate iPhone backup files
- Determine how backup files are named
- Identify what evidentiary items may be recovered from the iPhone backup files including:
  - Pictures
  - Call History
  - Address Book
  - Notes
  - SMS Messages
  - Voicemail
  - Administrative Information

Lab

The objective of this lab is to recover iPhone artifacts including the following:

- Calendar information
- Address book information and icons
- SMS messages
- Voicemail and call logs
- General account settings
- Property lists
- Pictures
- Notes

Practical Skills Assessment

The AccessData Macintosh 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.

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