

Internet Forensics

Forensic Toolkit, Password Recovery Toolkit and Registry Viewer

Advanced • Three-day Instructor-led Class



AccessData[®]

This advanced AccessData training course provides the knowledge and skills necessary to use AccessData[®] tools to recover forensic information from Internet artifacts. Participants will learn where and how to locate Internet artifacts using Forensic Toolkit[®] (FTK[™]), Registry Viewer[™] and Password Recovery Toolkit[™] (PRTK[™]).

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

- Use PRTK to break sign-on passwords for the following applications:
 - MSN Instant Messenger
 - Yahoo Instant Messenger
 - America Online and AOL Instant Messenger
 - Internet Explorer and Firefox Auto-Complete
- Use FTK to complete the following:
 - Locate and decrypt Yahoo Instant Messenger .DAT files.
 - Parse Internet Explorer .DAT files (History and Temporary Files) for hit rates, use counts and more.
 - Parse America Online client files for user history, search terms, address books, buddy lists, e-mail and more.
- Use Registry Viewer to analyze the following Instant Messenger data:
 - Shared file permission status and file transfer information
 - Block or allow information for user contacts (buddy lists)
 - Last-user access information and recent contacts through the messenger
- During the course, participants work a missing person case initiated from an instant message found on the computer screen of the missing person. The case takes participants to several different machines on multiple Internet chat, browsing and e-mail platforms.

Prerequisites

This hands-on course is intended for forensic investigators, law enforcement personnel, and security and network administrators with a basic working knowledge of FTK, PRTK, and Registry Viewer.

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

- Read and understand the English language.
- Attend the AccessData BootCamp or have equivalent experience with FTK and PRTK.
- Have previous experience in forensic case work.
- Have a working knowledge of the latest Internet applications such as MSN Messenger, Windows Messenger, AIM, Internet Explorer and AOL.

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
- FTK and PRTK environments

Lab

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

Module 2: AOL Instant Messenger

Objectives

- Identify where AOL Instant Messenger stores the following evidentiary items in the registry:
 - Last user to be logged into the machine
 - Registered screen names used on the machine
 - Screen names who have had contact with the local user
 - Indications of file transfer activity
 - Permissions for file sharing or file transfers
- Identify where AOL Instant Messenger stores the following evidentiary items in the file structure:
 - The Buddy List
 - Any shared or downloaded files

Lab

- Create a case.
- Examine evidence items in the file structure.
- Examine evidence items in the registry.

Module 3: Firefox

Objectives

- Identify what evidentiary items Firefox stores in the file structure and where they are located.
- Identify where Firefox stores cached Web content.
- Identify the files that store Firefox user preferences and download activity.
- Examine the naming convention of cached files and how they are tracked.

Lab

- Examine file locations.
- Examine the Firefox cache.
- Examine Firefox cache map files.
- Carve imbedded images from the Firefox cache

Module 4: Internet Explorer

Objectives

- Identify where Internet Explorer stores the following evidentiary items in the file structure:
 - Favorites
 - Cookies
 - History
 - Temporary Internet Files
- Identify where Internet Explorer stores the following evidentiary items in the registry:
 - Typed URLs
 - Passwords
 - Protected Storage Information

Lab

- Examine evidence items in the file structure.
- Examine evidence items in the registry.

Module 5: Yahoo Messenger

Objectives

- Distinguish between global registry items that apply to everyone and user-specific registry items.
- Identify what evidentiary items Yahoo stores in the file structure and where they are located.
- Identify what evidentiary items Yahoo stores in the registry and where they are located.

Lab

- Examine evidence items in the registry.
- Examine evidence items in the file structure.

Module 6: Windows Messenger

Objectives

- List the types of communication enabled by Microsoft .NET Passport technology.
- Recover information from Windows Messenger chat room activities and file exchanges.
- Identify what evidentiary items Windows Messenger stores in the file structure and where they are located.
- Identify what evidentiary items Windows Messenger stores in the registry and where they are located.
- Identify what evidentiary items Windows Messenger stores on Microsoft servers and how that information may be obtained.

Lab

- Examine evidence items in the registry.

Module 7: MSN Messenger

Objectives

- Recover information from MSN Messenger chat room activities and file exchanges.
- Identify what evidentiary items MSN Messenger stores in the file structure and where they are located.
- Identify what evidentiary items MSN Messenger stores in the registry and where they are located.

Lab

- Examine evidence items in the registry.
- Recover and view logged IM sessions.

Module 8: America Online

Objectives: Information from America Online

- List what information you can obtain with a subpoena.
- List what information you can obtain with a search warrant.
- List what information you can obtain from an AOL Terms of Service violation.
- Identify how to recover instant message data.

Objectives: Information from the Computer

- Locate the following evidentiary items in the file structure:
 - o Buddy lists
 - o Screen names
 - o Address books
 - o AOL companion information
 - o Client logs / error files
 - o Auto-complete / history
 - o Deleted file information
 - o Connectivity information
 - o Passwords (Sign-On / PFC)
 - o Uninstall information (Leftovers)

Objectives: Personal Filing Cabinet

- Obtain the following information from the Personal Filing Cabinet:
 - o E-mail messages
 - o E-mail headers
 - o Attachments
 - o Favorite Places
 - o Away messages
 - o Newsgroup information
- Identify how long e-mail is retained on the AOL server.
- List what types of information may be contained in an AOL message.
- Determine if a user downloaded an e-mail attachment.
- List the implications Auto-AOL may have on a case.

Lab

- Examine evidence items in AOL Client files.
- Examine evidence items in AOL user files.
- Examine evidence items in the Personal Filing Cabinet.
- Examine evidence items in miscellaneous files.

Module 9: Internet Password Decryption Methods

Objectives

- Identify the file structure and registry location of passwords and encrypted information.
- Identify the techniques used to recover encrypted information with Ultimate Toolkit (UTK).

Lab

- Examine password decryption methods for each of the Internet applications discussed in the course.

Practical Skills Assessment

The Internet 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.

© 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, Forensic Toolkit, FTK, FTK Imager, Known File Filter, KFF, Password Recovery Toolkit, PRTK, Registry Viewer, Ultimate Toolkit and WipeDrive are either registered trademarks or trademarks of AccessData Corporation in the United States and/or other countries. Other trademarks referenced are property of their respective owners.