

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[®] 2 (FTK[®] 2), Registry Viewer[®] and Password Recovery Toolkit[®] (PRTK[®]).

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

- Recover sign-on passwords and autofill data for the following applications:
 - o AOL Instant Messenger
 - o Yahoo! Instant Messenger
 - o Windows Live Messenger
 - o Skype
 - o Safari
 - o Firefox
 - o Internet Explorer 7
- Use FTK to complete the following:
 - o Locate saved or archived instant messages, connection log artifacts, and contact information
 - o Locate outgoing file transfers
 - o Locate and decrypt instant messenger .DAT files
 - o Recover user history, search terms, address books, buddy lists, e-mail and more
- Use Registry Viewer and file structure to analyze the following instant messenger data:
 - o Instant messenger passwords and contact data
 - o Shared file permission status and file transfer information
 - o Chat room data
 - o Last-user access information and recent contacts through the messenger
 - o File transfer/sharing permissions and activity

Prerequisites

This course is intended for forensic investigators with a basic working knowledge of the following AccessData forensics tools:

- Forensic Toolkit (FTK)
- Password Recovery Toolkit (PRTK)
- Registry Viewer

Participants should also meet the following requirements:

- AccessData Bootcamp FTK 2 or equivalent experience with FTK and PRTK
- Previous investigative experience in computer forensics case work
- 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

- Identify the FTK 2 components
- List the FTK 2 and PRTK system requirements
- Describe how to receive upgrades and support for AccessData tools
- Install FTK Imager, FTK 2, PRTK, Registry Viewer, and the dongle drivers

Lab

- Install AccessData software.
- Prepare your system.

Module 2: AOL Instant Messenger

Objectives

- Provide a basic overview of AOL Instant Messenger (AIM) features.
- Identify where AOL Instant Messenger stores the following evidentiary items in the file structure:
 - The Buddy List location and meaning of the entries
 - Any saved instant messages
 - Direct IM
 - Linked screen names
- Identify where AOL Instant Messenger stores the following evidentiary items in the registry:
 - Last user to be logged in to 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

Lab

- Recover registry artifacts such as current user, AIM passwords, user accounts, and user preferences.
- Recover installation artifacts.
- Recover user artifacts such as away messages, buddy list and icons, emoticons, archived IM conversations, and the AIM profile.

Module 3: Yahoo! Instant Messenger

Objectives

- Distinguish between global registry items that apply to everyone and user-specific information stored in the registry.
- 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

- Recover registry artifacts such as last logged in user, login and logout times, message archiving settings, and chat room and file transfer activity.
- Recover file structure artifacts such as the send locations for file transfers, Index.dat file, archived messages, and Yahoo! Web Messenger artifacts.

Module 4: Windows Live Messenger

Objectives

- List the user-generated artifacts created when the Windows Live suite is installed and the account is authenticated to the Windows Live servers.
- Provide an overview of Windows Live Messenger features.
- List user-generated artifacts that can be recovered from Windows Live Messenger and identify where they are located in the file structure.
- List application-generated artifacts that can be recovered from Windows Live Messenger and identify where they are located in the file structure.
- Identify what evidentiary items are created by Windows Live Messenger in the registry and where they are located.

Lab

- Recover installation artifacts.
- Recover artifacts from the NTUSER.DAT file such as received file transfers, a manually-saved contact list, and manually-saved IM conversations.
- Recover file structure artifacts such as manually saved contact lists, instant messenger conversations, message history, MSN photo swaps, and file transfers.

Module 5: MySpace Instant Messenger

Objectives

- Identify the MSIM client's default installation paths on a Windows Vista system.
- Recover client-based, trace evidence from the Windows Vista registry.
- Recover the following user-generated artifacts:
 - Preferences/settings for the application
 - Contact (friend/buddy) lists
 - Profile information
 - File transfers
 - Message archiving and application logging

Lab

- Recover user artifacts such as last logged in user, user preferences, the MSIM contact list, user profile, display pictures, images, icons, automatic conversation logs, connection logs, and file transfers (sent and received).
- Create a custom KFF Alert set to identify download files.
- Recover the local user profile and remote contact information from the SkypeCache folder.

Module 6: Skype

Objectives

- Describe the basic features and availability of Skype.
- Identify what evidentiary items Skype creates during installation and where they are located.
- Identify what evidentiary items Skype are created by the use of the client and where they are located.

Lab

- Recover installation artifacts.
- Recover user artifacts such as last logged on user, user preferences, and user profile information.
- Identify outbound calls and their recipients.
- Recover chat conversations, file transfers, the user contact list, and message history.
- Use the Skype Log Parser (v1.3) to scan the Skype log files and create basic reports.
- Integrate a Skype Logs report into the FTK case report.

Module 8: Safari

Objectives

- Identify the artifacts left behind by the client's installation
- Discuss the artifacts left behind by the user's interaction with the application including:
 - Internet history
 - Cookies
 - Favorites/bookmarks
 - Typed URLs
 - Downloads
 - Temporary files/cache
 - Password storage

Lab

- Recover installation artifacts.
- Recover browser history and bookmark data.
- Recover user downloads, cookies, and user preferences.
- Recover user artifacts such as downloads, bookmarks, cookies, passwords, user preferences, passwords, and cached content.

Module 9: Firefox

Objectives

- Locate files of evidentiary interest and discuss how they are created or added to.
- Process Firefox evidentiary files.
- Describe how the browser stores its cached Web content and how FTK handles the information.
- Discuss how Firefox uses encryption and obfuscation to protect sensitive information.

Lab

- Recover installation artifacts.
- Recover user artifacts such as user preferences, browser history, bookmarks, and cookies.
- Recover standard form data and passwords.
- Recover the form data and passwords protected with a Master Password.
- Recover the browser cache files.

Module 10: Internet Explorer

Objectives

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

Lab

- Recover temporary Internet file, chat history, chat files, cookies, and favorites.
- Recover Web-based email accounts and cached files.
- Recover registry artifacts such as Windows Live Mail account information, typed URLs, and downloaded files.
- Decrypt PSSP data for IE 7.

Module 11: LimeWire

Objectives

- Discuss the Gnutella Network Overview including:
 - Architecture
 - Basic Operation
 - LimeWire Interaction
- Discuss LimeWire Features and Options
- Locate Installation Artifacts
- Locate User Artifacts including:
 - Preferences
 - Downloads
 - Sharing

Lab

- Recover installation artifacts.
- Recover user preferences, partial download files, as well as completed download files.
- Determine the Limewire sharing status for local directories.
- Search for specific files based on the file's converted Limewire SHA1 hash.

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 .

© 2009 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.