

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Other forensic training organizations
- Course outline
- Helpful information
- FTK and PRTK environments

Lab

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

Module 3: AOL Instant Messenger

Objectives

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

Lab

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

Module 5: 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 6: Internet Explorer

Objectives

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

Lab

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

Module 7: 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 8: 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 10: 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 11: 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 12: 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.

