

# **FIRE**

## **Forensics of Internet Related Evidence**

### **Intermediate Level**



### **Course Objectives**

This 3 day class is designed to familiarize the student with the many artifacts left behind on Windows based media from the most popular Internet Browsers and Instant Messengers. Additionally, email basics and Windows Live Mail and Microsoft Outlook will be analyzed.

Internet Browsers analyzed:

- Internet Explorer 8 & 9
- Mozilla Firefox 3 & 4
- Google Chrome

Instant Messengers analyzed:

- AOL Instant Messenger
- Yahoo Messenger
- Windows Live Messenger
- SkyPE Messenger

Email Applications analyzed:

- Windows Live Mail
- Microsoft Outlook

### **Prerequisites**

This advanced course is designed for an experienced Digital Forensic or eDiscovery practitioner with a solid understanding of Microsoft Windows operating system functionality.

To gain the maximum benefit from this course you should meet or exceed the following requirements:

- Read and understand the English language
- Have attended intermediate to advanced digital forensic training
- Have conducted digital forensic examinations for at least 6 months
- Be familiar with the Microsoft Windows environment and data recovery concepts

### **Course Outline**

The course will follow adult learning principles through training aids such as presentations, diagrams and practical instructor lead examples. Each topic covered will be presented in either one or two 50 minute sessions followed by review questions. Students will be given the opportunity throughout the course to ask questions and discuss objectives covered in more detail. Ample time will be allotted for hands on exercises to reinforce the topics covered.

The course will be structured as follows:

### **Introduction and Forensic Tool Overview**

- Introductions by the course instructor and students
- An overview of both commercial products, such as Netanalysis, Internet Evidence Finder, Belkasof, EnCase and Forensic Toolkit, and tools that are free and in the public domain

### **Internet Explorer**

- Explanation of Internet Cookies
- Explanation of Internet History and Downloads
- Explanation of Temporary Internet Files
- Explanation of Tabbed Browsing
- Explanation of Favorites or Bookmarks
- Intelliforms vs. Protected Storage System Provider
- Identify the location of the artifacts left behind while browsing with Internet Explorer
  - Internet Explorer 8 and 9
- Describe the recoverable artifacts with InPrivate Browsing

### **Mozilla Firefox**

- Identify the location of the artifacts left behind while browsing with Firefox
  - Firefox 3 and 4
  - Cookies
  - History
  - Cache or Temporary Internet Files
- Form data and password recovery and the Master password implications
- Describe the Private Browsing feature of Firefox

### **Google Chrome**

- Identify the location of the artifacts left behind while browsing with Google Chrome
  - Cookies
  - History
  - Cache or Temporary Internet Files
  - Downloads
- Functions of the Chrome Omnibox
- Aero Peek option within Chrome

### **AOL Instant Messenger**

- Identify the chat logs for AOL Instant Messenger
- Identify local files of forensic value
  - Buddy Icons
  - Install logs
- Identify Registry specific artifacts

### **Yahoo Messenger**

- Describe the difference between a Yahoo user and an alias
- Identify the DAT files for archiving Yahoo Messenger chats
- Identify local files of forensic value
  - Buddy Icons
  - Local user Icon and Avatars
  - Install logs
  - File sharing data
- Identify Registry specific artifacts
  - File transfer information
  - Chat room history
  - Search history

### **Windows Live Messenger**

- Identify the XML files for archiving Live Messenger chats
- Identify local files of forensic value
  - Buddy Icons
  - File sharing data
- Identify Registry specific artifacts
  - Recent logged in user
  - File transfer information
  - Buddy icon location

### **SkyPE Messenger**

- Identify the files for archiving SkyPE chats
- Identify local files of forensic value
  - Contact list
  - File sharing data

## **Windows Live Mail**

- Identify the locations of the locally saved mail
- Recovery of deleted mail
- Explain the recovery of Windows Live Mail from the Temporary Internet Files

## **Microsoft Outlook**

- Explanation of the PST file
- Explanation of the OST file
- Describe deleted mail recovery with an email archive