opentext™

Training overview

DFIR350 Internet-based Investigations with OpenText EnCase

Syllabus

Day 1

The first day of this course focuses exclusively on the P2P file sharing protocol, BitTorrent™. Instruction includes a demonstration using one of the most popular BitTorrent clients, µTorrent, and will be followed by an examination of the BitTorrent protocol, BitTorrent encoded (bencoded) data, metadata (torrent) files and an examination of the file system artifacts associated with µTorrent.

The day concludes with an in-depth practical exercise, allowing the students to apply their newly gained knowledge and skills in a scenario that involves the use of BitTorrent together with other forensic topics, such as data recovery and encryption.

Day 1 will cover:

- BitTorrent P2P networks
- The history of P2P and BitTorrent
- A practical demonstration of BitTorrent
- BitTorrent protocol
- Bencoded data
- The content of metadata (torrent) files in µTorrent
  - Configuration files
  - Search activity

Day 2

Day two continues with instruction on the Ares Galaxy P2P network and the associated Ares and LimePro client applications. The next lesson of the day focuses on GigaTribe, another P2P network that allows file sharing between members who are on the user's contact list.

A practical exercise follows the lesson, which allows students to identify files shared with this specific network. Instruction continues with an in-depth analysis of the Microsoft® Internet Explorer and Edge web browser software applications, commencing with an examination of the way in which computer security has affected the development of both browsers. This will be followed by an examination of pertinent registry settings and application files.

opentext™

Day 2 will cover:

- The Ares Galaxy P2P network
  - Background
  - Installation
  - Initial Setup
  - Features and configuration shared by Ares and LimePro
  - Artifacts
- GigaTribe introduction and use
  - Origination
    - Mode of operation
    - Membership options
    - Application version and installation
    - Adding contacts
    - Downloading content
    - Examining the download process and data
    - Passwords
    - Chatting
    - User blogs
- Microsoft Internet Explorer and Edge
  - How computer security concerns have affected the operation of both web browser programs
  - Default browser settings and version identification
  - Registry data, including typed URLs, homepage settings and version identification
  - Cookie files
  - Download folder location, bookmarks and reading-list entries

Day 3

Day three continues with an examination of the WebCacheV01.dat Extensible Storage Engine (ESE) database file used by Internet Explorer and Edge to store index cookie, history and cache content.

Next, students undertake a practical exercise allowing them to apply their newly acquired knowledge to perform advanced recovery and analysis of internet history data. They are then given instruction on the structure of websites and component pages.

This information will be used together with their new-found knowledge of Internet Explorer and Edge cache content to extract and rebuild a cached copy of a website containing a picture of note. The day ends by beginning a lesson on the artifacts introduced with Mozilla Firefox®.

Day 3 will cover:

- The nature, content and structure of WebCacheV01.dat Extensible Storage Engine (ESE) database files
- Determining true visit count of internet history entries stored in WebCachceV01.dat files
- Recovery of deleted WebCacheV01.dat records
- Parsing internet data from IndexedDb.edb files, including those used by Cortana
- Understanding the structure of HTML web pages
  - Role of the web server
  - Web server port numbers
  - Characteristics of a darknet
  - Content storage
  - Static vs. dynamic web pages
  - HTML, CSS and JavaScript
  - Using web browser development functionality to de-obfuscate web pages and hide undesirable content
- Rebuilding web pages
  - Identifying and rebuilding the component files of a cached website that contains a picture of note
- Understanding Mozilla Firefox
  - History
  - Impact on forensic examination
  - Structure
  - Examination techniques

opentext™

Day 4

Day four starts with instruction on Google Chrome®. Next, students are provided information about web search engines followed by a detailed lesson on email fundamentals. Students will then learn about Microsoft® Outlook PST files.

Day 4 will cover:

- Google Chrome
  - History
  - Structure
  - Examination techniques
- Identifying and processing artifacts associated with web search engines
- Email fundamentals
  - Introduction to and history of the use of electronic mail, including the three main email protocols
    - Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP)
  - Basic modes of email operation
  - Identification of internet email servers using DNS MX records
  - Sending/receiving email manually and using OpenText™ EnScript™ programs in order to demonstrate email spoofing and the ability to send/receive email without email client software
  - Email encoding
  - Recovering deleted email attachments
- Outlook PST files
  - Structure
  - Extraction to view outside of the OpenText™ EnCase™ environment
  - Overcoming password protection
  - Understanding and viewing PST data stored using compressible encryption
  - Ancillary files
  - Registry settings

opentext.com/contact