opentext™

TRAINING OVERVIEW

DFIR350 Internet-based Investigations with OpenText EnCase

Syllabus

Training facilities

Los Angeles, CA (Pasadena, CA)
1055 East Colorado Boulevard
Suite 400
Pasadena, CA 91106-2375

Washington, DC (Dulles, VA)
21000 Atlantic Boulevard,
Suite 750
Dulles, VA 20166

London, UK (Reading)
420 Thames Valley, Park Drive
Earley
Reading
Berkshire RG6 1PT

Munich, Germany (Grasbrunn)
Werner-von-Siemens-Ring 20
85630 Grasbrunn/München
Germany

For a complete list of locations, including Authorized Training Partners around the world, please visit **opentext.com/learning-services/learning-paths**.

Day 1

The first day of this course starts with a study of the Google Chrome browser, which is also pertinent to Microsoft Edge, because both browsers are built on the Chromium open-source browser project. Instruction continues with examination of the Chrome cache followed by the first part of a lesson showing how the browser uses LevelDB and IndexedDB to store web-application data.

Day 1 will cover:

- Google Chrome
  - Browser history and relevance to Microsoft Edge
  - Program installation
  - Understanding/locating Chrome user profiles
  - Significance of SQLite database files
  - Session information and user preferences
  - Bookmarks and internet history, including downloads and search terms
  - Using Windows credentials to decrypt Chrome cookies, form history and stored login credentials
  - Snapshots
  - Private browsing considerations

- Google Chrome cache
  - Importance
  - Relevance to Microsoft Edge
  - Cache structure and indexing
  - Parsing sparse cached data
- Google Chrome LevelDB and IndexedDB
  - Understanding the nature and significance of JavaScript objects and the need to store them using IndexedDB
  - Running a JavaScript application and using Chrome to inspect its IndexedDB data
  - Examining IndexedDB data from a Chrome extension, one that captures clipboard data

Day 2

Instruction continues the second day with the examination of the Chrome use of LevelDB and IndexedDB, after which students will participate in an associated practical exercise.

Students will then turn their attention to the nature and structure of web pages, how they are served, and how the tools of a browser developer can be used to manipulate their view. Students will then progress to rebuilding a web page using cached content parsed by OpenText™ EnCase™ software (EnCase). Instruction will then be provided in respect of Mozilla Firefox® and the operation of web search engines.

Day 2 will cover:

- Conclusion of Google Chrome LevelDB and IndexedDB
  - On-disk location of Google Chrome IndexedDB data
  - Understanding the layered nature of IndexedDB and its relationship to LevelDB
  - Using OpenText™ EnScript™ programs to parse Microsoft Teams IndexedDB records from LevelDB block files
  - Using EnScript programs to parse IndexedDB records from LevelDB log files
  - Understanding IndexedDB BLOB data
- Understanding the structure of HTML web pages
  - Role of the web server
  - Web server port numbers
  - Notable 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
  - Using cached content parsed by EnCase to rebuild a page viewed at a WordPress website
- Mozilla Firefox
  - Browser history
  - Creation, location, and use of Firefox user profiles
  - User preferences
  - Typed URLs, bookmarks, browsing history, and downloads
  - Session storage
  - Cookies
  - Form history
  - Decryption of cached login credentials
  - Private browsing
  - Data synchronization
  - Cache structure
- Identifying and processing artifacts associated with web search engines
  - Understanding basic searches performed using HTTP GET
  - Examination of Google search parameters including EI, SEI, and VED values and timestamps that they may contain
  - Google image and video searches
  - Google Safe Search
  - The effects of searching using HTTP POST as opposed to GET
  - Google Suggest

Day 3

Instruction on day three concludes the study of web search engines and is followed by a detailed lesson on email fundamentals, including the way in which attachments are encoded using MIME. Students will then move on to examinations of the P2P file-sharing protocol, BitTorrent™. Instruction includes a demonstration using one of the most popular BitTorrent clients, uTorrent, 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 uTorrent.

Students then receive instruction on the eMule P2P file-sharing software during which students will see how anyone can run a private eMule server that encourages sharing but is only accessible to certain clients.

Day 3 will cover:

- Continuing examination of web search engine artifacts
  - Understanding the nature and effects of HTTP caching
  - Importance of decompressing cached content through the use of evidence processing
  - Extraction of URL parameters using EnScript programs

- Determining the use of HTTP POST when conducting searches using DuckDuckGo
- Viewing cached auto-complete data using EnCase

- 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 EnScript programs in order to demonstrate email spoofing and the ability to send/receive email without email client software
  - Email encoding and MIME
  - Recovering deleted email attachments
- BitTorrent P2P network
  - The history of P2P and BitTorrent
  - A practical demonstration of BitTorrent using uTorrent
  - BitTorrent protocol
  - Bencoded data
  - The content of the metadata (torrent) files used by uTorrent
  - Configuration files
  - Search activity
- eMule P2P file-sharing application
  - Background
  - eMule server availability and configuration
  - eMule client installation and configuration
  - Sharing, searching, and downloading files

Day 4

On the fourth day, students complete the lesson on eMule P2P file-sharing software followed by a practical exercise that meshes eMule artifacts together with other internet artifacts and forensic methodologies. Instruction continues with a lesson on GigaTribe, a P2P file-sharing application that supports end-to-end encryption, allowing users to share files and chat within secure groups. The course concludes with a practical exercise, allowing students to test their new-found knowledge on GigaTribe.

Day 4 will cover:

- Concluding the study of the eMule P2P file-sharing application
  - Examination of eMule artifacts in OpenText™ EnCase™ Forensic
  - eMule hash values, their nature, and purpose

- Purpose and examination of the known.met and clients.met files
- Using File Block Hash Map Analysis to locate deleted files originally downloaded/ shared via eMule

- GigaTribe P2P file-sharing application
  - History
  - Mode of operation
  - Membership options
  - Application version, installation, and configuration
  - Adding groups and contacts
  - Chat
  - Sharing files and folders
  - Downloading shared content
  - Accessing password-protected folders

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **X (formerly Twitter)** | **LinkedIn**

opentext.com/contact