GUIDANCE SOFTWARE

ENCASE ADVANCED INTERNET EXAMINATIONS

Syllabus

Day 1

The first day of this course focuses exclusively on the P2P file sharing protocol, BitTorrent™. The instruction will include 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.

On day one the students will:

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

Day 2

Day two continues with instruction on the Ares Galaxy P2P network and the associated Ares and Lime Pro 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 the students to identify files shared with this specific network. Instruction continues with an in-depth analysis of the Microsoft® Internet Explorer Web browser software, commencing with Registry artifacts and an examination of how index.dat files are used to store and/or index cookie, history, and cache content under older versions of the browser, which are still in widespread use today, particularly in corporate environments.

On day two the students will:

- 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
- Windows Internet Explorer
  - Registry artifacts
  - Understanding the purpose and content of Internet cookies
  - Structure and content of index.dat files
  - Identification of cached files and their originating website

Day 3

Day three continues the analysis of Microsoft Internet Explorer focusing on the structure and use of Extensible Storage Engine (ESE) database files used by later versions of the browser (including the Edge web browser that is part of Windows 10) to store and/or index cookie, history, and cache content. The students undertake a practical exercise allowing them to apply their newly acquired knowledge to perform advanced recovery and analysis of deleted Internet history data. They are then given instruction on the structure of HTML Web pages and use this, together with their new-found knowledge of Internet Explorer cache content, to identify a cached Web page and its component files and rebuild it. The day ends by beginning a lesson regarding the artifacts introduced with and Mozilla Firefox®.

On day three students will:

- Understanding how Internet Explorer history is maintained and indexed
- Understanding the operation of the Internet Explorer Web cache, including the storage and indexing of cache content
- Understanding the structure of HTML Web pages
- Rebuilding Web pages
  - Identifying and recovering the component files linked to and embedded in a cached Web page
  - Rebuilding and displaying a cached Web page by modifying its source code
- Understanding Mozilla Firefox
  - History
  - Impact on forensic examination
  - Structure
  - Examination techniques

Day 4

Day four starts with tuition on Google Chrome®. Next the students are provided information about Web search engines followed by a detailed lesson on email fundamentals. The students will then learn about Microsoft® Outlook PST files.

On day four students will:

- 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 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 EnCase® environment
  - Overcoming password protection
  - Understanding and viewing PST data stored using compressible encryption
  - Ancillary files
  - Registry settings

GUIDANCE SOFTWARE™

About Guidance Software

At Guidance, we exist to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems, and LogRhythm. Our field-tested and court-proven solutions are used with confidence by more than 70 of the Fortune 100 and hundreds of agencies worldwide. Get to know us at guidancesoftware.com.