

## Encase V6 Advanced Internet Examinations

**Vendor Course Code:**

**Course Length:** 4 days

**Overview:** This hands-on course involves practical exercises and real-life simulations. The class focuses on the forensic evidence located on the computer belonging to the suspect and /or victim – not online or cyber investigations. Email files and the Internet are cornerstones of consumer and business computer use. Virtually all computer forensic examinations will involve analysis of email and Internet artifacts, underscoring the need to understand the relevance of Internet and email-based evidence recovered during examinations.

**Skills Gained:** The course will enable students to recover and examine from peer-to-peer file-sharing applications (BitTorrent, Gnutella, etc.), instant messaging applications (Windows® Live Messenger and Yahoo! Instant Messenger) and web browsers (Microsoft Internet Explorer and Mozilla-based browsers). Students will also be able to examine computer systems with regards to Trojan viruses and key loggers. Students will also learn important information with regard to the examination of Outlook PST, web and Lotus Notes email. Students will be able to properly explain the browser caching process and rebuild cached Internet Explorer web pages.

Students will learn the history, operation and artifacts associated with peer-to-peer file-sharing applications, such as BitTorrent™ and the Gnutella P2P Network

Students will learn the impact of Trojan viruses through examination of:

- Defense issues
- The Windows® Registry
- Hash analysis
- Anti-virus scanning and virus analysis using the EnCase® Virtual File System (VFS) Module and the EnCase® Physical Disk Emulator (PDE) Module

Students will learn about Autostart examinations.

Students will learn how to identify artifacts from instant message clients, such as Windows® Live Messenger and Yahoo!® Messenger.

Students will learn the operation of the Microsoft® Internet Explorer web browser with regards to typed URLs, password and form-data storage, cookies, Internet history and cache content.

Students will learn how web pages are constructed and will use this information, together with their new-found knowledge of cached Internet Explorer web content, to correctly rebuild web pages.

Students will learn about artifacts introduced with Microsoft® Internet Explorer 7.

Students will learn about the history, operation and artifacts associated with Mozilla Firefox®.

Students will learn about the operation of web search engines.

Students will learn about web-based email.

Students will learn about the Microsoft® Outlook PST structure and about viewing Lotus® Notes email data.

### Key Topics:

#### 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.

#### Day 2

Day two continues with instruction on the Gnutella network devoting special attention to the LimeWire™ and BearShare client applications. Trojan virus programs are covered next. The students will gain an understanding of how these programs operate and the artifacts associated with

them. Students will observe how the EnCase® Physical Disk Emulator (PDE) Module and EnCase®Virtual File System (VFS) Module can be used to identify Trojan programs and analyse their operation. Students will have the opportunity to apply their newly gained knowledge to identify the files belonging to a sophisticated key-logging program and ascertain how it launches automatically at system start up. The day's activities will conclude with instruction on two well-known instant messenger applications and an associated practical exercise.

#### Day 3

Day three starts with an in-depth analysis of the Microsoft® Internet Explorer web browser software and the way in which it maintains Internet cookies, history and cache-content. Following this 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.

#### Day 4

Day four starts with instruction on browser-helper objects and favourite links, placing emphasis on browser hi-jacks. Following this the students are provided with tuition on artifacts introduced with Microsoft® Internet Explorer 7 and Mozilla Firefox®; also information on web search engines and web-based email. They are then provided with information with regard to Microsoft® Outlook PST files, Lotus® Notes and the Mozilla Thunderbird email client.

### Target Audience:

This course is intended for corporate and government/law enforcement investigators, legal professionals and network security personnel. Incident response supervisors and team members are encouraged to attend as are individuals working in a penetration testing or network intrusion investigation role. An understanding of the concepts of computer forensics and familiarity with the EnCase® Forensic software is required. Class curriculum is designed to provide a good overview of Internet usage investigation issues, both from a forensic and intruder perspective.

### Prerequisites:

EnCase® Computer Forensics II

EnCE® Certification

EnCase® Computer Forensics II or EnCE® Certification.

Advance preparation for this course is not required.

Note: The content of this course is significantly different and we recommend that anyone who took the EnCase Internet & E-mail course prior to February 2004 now take EnCase Advanced Internet Examinations