IR250-Incident Investigation

Syllabus

Training facilities

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

Washington, DC (Gaithersburg, MD)
9711 Washingtonian Blvd
6th floor, Room 601 (Paris Room)
Gaithersburg, MD 20878

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 listing of locations, including Authorized Training Partners around the world, please visit opentext.com/learning-services/ learning-paths.

EnCaseTraining@opentext.com

Day 1

Day one starts with a discussion focused on incident response considerations, including examination options. Having introduced the course scenario, instruction moves on to the use of OpenText™ Endpoint Investigator to acquire critical disk and volatile operating system data.

This is followed by an in-depth look at capturing physical memory (RAM) and network data. Students will participate in a practical assignment, allowing them to exercise and apply their newfound knowledge and skill.

Day 1 will cover:

- Understanding incident response considerations, including education, planning, policy implementation, training, and equipment.
- Learning the benefits of capturing disk, network, and RAM data.
- Learning the importance of capturing non-digital evidence.
- Understanding the consequences of pursuing different examination methodologies when weighed against the need to acquire evidential data.
- Learning how to use OpenText Endpoint Investigator to preview and acquire data pertinent to your investigation and take a snapshot of volatile data.
- Learning how to acquire an image from RAM.
- Examining the concept of network sniffing, capturing network packet data and factors that can affect the process.
- Understanding the Microsoft® Windows® operating system registry.
- Learning to locate and decode registry data manually, using native OpenText Endpoint Investigator functionality or programs written in the EnScript programming language.

Day 2

Day two begins with a discussion on the types of files included in the NT File System (NTFS) and the header and structure of the NTFS Master File Table ($MFT). Students will then learn how NTFS time-stamp information is stored and how to examine redundant time-stamp data with a view to identifying files of evidential significance.

Further instruction details how file data is stored and how NTFS alternate data streams can provide additional information regarding the provenance of files and the presence of encrypted data.

Day two concludes with the examination of two important log files associated with the NT File System.

Day 2 will cover:

- Understanding the nature of NTFS metadata and how it is stored, as well as the basic layout of a $MFT record.
- Examining the contents of the $Standard Information attribute ($SIA) and the $Filename attribute ($FNA), paying particular regard to the time stamps they contain.
- Examining how the NTFS $MFT $Data attribute is used to either store or reference a file's data on an NTFS volume, along with the nature and potential importance of alternate data streams.
- Tackling data encrypted using the Microsoft Windows Encrypting File System (EFS) and BitLocker™.
- Extracting NTFS USN change-log journal records and subsequent analysis.
- Examining the NTFS $Logfile and its significance.

Day 3

Day three begins with a practical exercise that allows the students to test their knowledge of NTFS volumes and to identify recovered/deleted files and the provenance and source of certain files.

Instruction continues in several areas, including Windows event-log files, prefetch files, shortcut-link files and jump lists, the operation of the Windows Recycle Bin, ShellBag analysis and volume shadow copy examination. Day three concludes with a practical exercise that reinforces the day's lessons.

Day 3 will cover:

- Learning how event-log data can be processed, searched and bookmarked using OpenText Endpoint Investigator.
- Understanding how to examine event-log data using Windows, as well as the importance of prefetch file analysis.
- Operating shortcut link files and jump lists, their significance and how to examine them.
- Analyzing the Windows Recycle Bin folder and its contents.
- Studying the significance of Windows ShellBag data and its importance when determining the provenance of folders accessed by the user.
- Operating the Volume Shadow Service (VSS) and learning the importance and analysis of volume shadow copies.

Day 4

Day four focuses on the analysis of random access memory (RAM). This is followed by an examination of some of the most widely used web-browser applications and their individual peculiarities.

The course concludes with a final practical exercise that reinforces the benefits of RAM and browser-artifact analysis.

Day 4 will cover:

- Understanding the operation of RAM, its analysis using the Volatility memory framework, and the importance of timely analysis of volatile data, particularly where encryption and cloud-based file storage is concerned.
- An overview and explanation of the artifacts associated with many web browsers.