EnCase® Computer Forensics II Syllabus

Day 1

Day one starts with an overview of the EnCase® Forensic v7 (EnCase v7) environment. Attendees then move on to study the Master Boot Record partitioning model and deleted partition recovery. Instruction continues with an examination of compound files. Their structures are explored and issues surrounding their examination are discussed in detail. Students move on to exploring a very important type of compound file structure, the Windows® Registry hive file. They explore mounting and examining these files and are given instruction on the relationship of the hive files to the structure of the Registry in its on-line state. Students then progress to examining the time zone information contained within the Registry, its importance to their case, and how they apply it in EnCase v7. Day one finishes with intermediate-level instruction concerning NTFS and its most important metafile, the Master File Table (MFT).

The main areas covered on day one include:

- **Review of EnCase v7 case creation and adding evidence**
- **Understanding the Master Boot Record partitioning scheme**
- **Principles of attempting to recover data lost through the partitioning process**
  - Partition recovery
- **Compound files**
  - Mounting and searching compound files
  - Documenting data contained within these compound files
  - Pitfalls of not examining compound files properly
- **Windows Registry**
  - Elements of the Registry
    - » Registry keys (folders) and values
    - » Registry value types
  - Locating and mounting the Registry hive files
  - Examination of time zone settings with the Registry
    - » Applying time zones within EnCase v7
- **Introduction to NTFS**
  - Internal system files and their function
  - $MFT entries and contained attributes
  - Resident file data
  - Nonresident file data
  - Impact of file deletion

Day 2

Day two begins with a practical exercise and instruction continues with an overview of the EnCase® Evidence Processor. Students then move on to a discussion of the processes for recovering deleted folders on both FAT and NTFS volumes. Basic index query searches are discussed, configured, and executed with associated review of the responsive data findings. Instruction is then provided on the use of the EnCase® Virtual File System (VFS) Module and EnCase® Physical Disk Emulator (PDE) Module. The attendees are shown how to use these technologies to accomplish tasks outside of the EnCase v7 environment, such as virus scanning, as well as execution of a proprietary application present on the target media. Single file functionality as well as the value of logical evidence files is explored. Day two concludes with instruction regarding the use of the GREP operator functionality of EnCase v7 in order to perform advanced searches.

The main areas covered on day two include:

- **Evidence Processor overview**
- **Deleted folder recovery**
- **Basic Index searches**
- **Using the VFS**
  - External processing
    - » Virus scanning
    - » Dynamic mounting of compound files
- **Single files and logical evidence files**
- **Using the PDE**
- **Advanced search techniques**
  - Using the GREP operators within EnCase v7 to construct advanced search terms
  - Suitability of GREP, proper syntax, and potential results

Day 3

Day three focuses upon specific analysis of common artifacts that often provide vital information to investigations. These specific areas reveal data that can provide a clearer indication of user activities. We will examine specific artifacts that the operating system creates through the user's interaction with the computer. Students will explore the methods that EnCase v7 provides to examine common email files, Internet history and cache content, Internet bookmarks, as well methods to create conditions to filter data.

The main areas covered on day three include:

- **Windows artifacts**
  - User account information and associated data
  - System folders and files of interest
  - Thumbnail cache files
  - Windows 7 specific artifacts
    - » Folder structure and the effect of junctions (folder mount-points)
    - » User/administrator privileges and impact on storage of data
    - » Links and Library folder content
    - » System files
- **Shortcut or link files**
  - Deconstructing link files to reveal internal structures related to their target files
- **Condition creation**
  - Overview of properties, operators, and logic operators
- **Email and Internet history**
  - Examining both client-based and web-based email and methods available within EnCase v7 to locate and parse email data stores
  - Recovering and analyzing email attachments
  - Exploring the results of activity on the Internet, including cookies, history, web cache, and bookmark data

Day 4

Day four starts with a discussion of the printing process under the Windows operating system, the generated internal spool and shadow files, and the data contained within each. The function and content of the Windows Recycler is explored in detail. A review of the week's work will reveal a significant volume of data within the class case folders. Students will explore methods to document, organize, and prepare a professional, accurate and articulate final report. The course concludes with a practical exercise as a review of the week's activities.

The main areas covered on day four include:

- **Print spooler recovery**
  - Understanding the printing process and associated files
  - Recovery of SPL and SHD files as well as understanding and extracting the graphical and metadata they contain
- **The Windows Recycle Bin**
  - Examination of the Recycle Bin, its properties, and function
  - Exploring the way the Recycle Bin is implemented under Windows 7
  - Linking Recycle Bin data to the associated user
  - Registry entries controlling operation of the Recycle Bin
- **Reporting**
  - Using the data accumulated during the week's work, students will explore various methods to document, organize, and prepare professional reports for their agencies
  - Students will save their reports in various formats, including RTF, PDF, XML, and HTML and then compare the results in order to select the format that best meets the needs of their respective agency
  - Students will be shown how to export all of the metadata relating to the files and folders in their case and the best way to store, present and query this data