EnCase® v7 Advanced Computer Forensics

Day 1

Day one begins with instruction on the more advanced use of conditions within EnCase® Forensic v7 (EnCase® v7) and moves onto instruction on how to use EnCase® v7 to examine smartphones. The final lesson on day one instructs the students on the use of block-based file hash analysis to recover files and the day winds up with a practical exercises on those skills.

The information covered on day one includes:

- **Conditions**
  - The function and purpose of conditions
  - Creating and using complex compound conditions, involving the use of different layers of logic and multiple criteria
- **Smartphone examinations**
  - Evidence handling
  - Acquisitions from various devices
  - iOS and Android artifacts
  - Report creation
- **File recovery using block-based hash analysis**

Day 2

Day two focuses on additional functionality of Microsoft® Windows operating systems and then moves onto the subject of encrypted data. An examination is conducted of the technology behind hardware and software RAID devices, the way in which these devices should be forensically examined, and how the RAID functionality is provided by the EnCase® v7 software. Students are shown how to understand and examine Windows® event log data, associate files and folders with Windows local and domain accounts, and obtain valuable information from the Windows Registry. They are also shown how to recreate the Registry information needed to extract and run applications preserved within a forensic disk image. Attendees then learn about the history and terminology associated with encrypted data. They will also learn the principles behind the recognition of encryption software and encrypted data and how they should approach the decryption of encrypted data. During the final lesson of the day the students will be introduced to the purpose and use of the Microsoft Windows prefetcher. Practical exercises will be administered throughout the day to allow the students to test their newly learned skills.

Day two's instruction includes:

- **Understanding RAID configurations and stripe sets**
  - RAID levels
  - Difference between hardware and software RAID
  - Effect of RAID on forensic examinations
  - Options for forensic acquisition of RAID devices
  - Rebuilding hardware and software RAIDs in EnCase® v7
  - Parity
- **Identifying Windows log files and examining their contents using both the EnCase® v7 software and an NT-based examination machine**
  - Fixing corrupted EVT event log files
- **Understanding the purpose and structure of the Windows Registry**
  - Identifying, mounting, and extracting data from Registry hive files both in EnCase® v7 and within Windows on a forensic examination machine
  - Recreating the Registry data necessary to run an extracted application on the examiner's forensic workstation
- **Understanding exactly what encrypted data is and the terminology associated with it**
- **The principles behind identification of encryption software and encrypted data and the methodology behind decrypting encrypted data**
- **Understanding the purpose of prefetch files, their structure, and content**

Day 3

Day three begins with a practical exercise regarding prefetch files. Instruction then continues with the various techniques for examining RAM. Next the students will learn about the Volume Shadow Copy Service (VSS), which allows volume backups to be created while file-system write operations continue to take place. The students will participate in practical exercises throughout the day.

The activities of day three include:

- **Learning how to enhance the ability to conduct examinations of RAM**
- **An introduction to the VSS operation and learning how to conduct examinations of VSS data created by the system as part of system restore operations**

Day 4

The activities on day four begin with a lesson on recovering information from ZIP files and how this can be used to recover data from the latest type of Microsoft® Word documents. Instruction is then given with regards to Windows Search and how the examiner can examine the data that it maintains. The final lesson of the course provides in-depth instruction on the use and analysis of removable USB devices. The students will again complete practical exercises throughout the day, underscoring the techniques learned during the day.

The information covered on day four includes:

- **The ZIP file format and how it impacts the ability to locate and recover ZIP data**
- **Using knowledge of the ZIP file format to recover data from the latest version of Microsoft Word documents**
- **The nature and use of Windows Search, which is now installed and active by default with Windows Visa and allows indexed searching within the Windows operating system**
- **A detailed discussion on the myriad of removable USB devices, how they are used today, and how to determine if a removable USB device has been used**

©2012 Guidance Software, Inc. All Rights Reserved. EnCase and Guidance Software are registered trademarks or trademarks owned by Guidance Software in the United States and other jurisdictions and may not be used without prior written permission. All other marks and brands may be claimed as the property of their respective owners.