EnCase® v7 Advanced Computer Forensics

Day 1

Day one begins with instruction regarding additional Registry examination techniques and artifacts. Students are shown how to extract Registry hive files and mount them into their own system for the purpose of application extraction and installation. They are also shown how to examine user-assist data and shell-bag data. The penultimate lesson on day one instructs the students on the use of block-based file hash analysis to recover deleted target files even if those files have been fragmented and/or partially overwritten. The final lesson on day one documents the examination of Windows event logs.

The information covered on day one includes:

- **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
  - Mapping local and domain-level user accounts
  - Examining user-assist Registry data
  - Parsing shell-bag data in conjunction with NTFS USN change-log data
- **File Recovery using block-based hash analysis**
- **Windows event-log analysis**

Day 2

Day two begins with instruction on the Volume Shadow Copy Service (VSS), which allows volume backups to be created while file-system write operations continue to take place. 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 in the EnCase v7 software functions. The third lesson on day two provides in-depth instruction on examination of removable USB device-artifacts. The last lesson of the day introduces students to the Microsoft Windows prefetcher, and shows them how to examine the files that it creates with a view to determining application usage. Practical exercises will be administered throughout the day so as to allow the students to test their newly learned skills.

The information covered on day two includes:

- **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**
- **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
- **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 and when**
- **Understanding the purpose of prefetch files, their structure, and content**

Guidance® SOFTWARE

Day 3

Day three begins with a practical exercise regarding prefetch files. 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 such data. Instruction continues with the various techniques used for examining RAM and concludes with instruction on Windows Search and how the examiner can examine the data that it maintains. The students will participate in practical exercises throughout the day.

The information covered on day three includes:

- **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**
- **Learning how to enhance the ability to conduct examinations of RAM**
- **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**

Day 4

The activities on day four begin with a practical exercise on the techniques learned during the Windows Search lesson. Instruction resumes 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. The course concludes with instruction on how to use EnCase v7 to examine smartphones. Students will undertake relevant practical exercises throughout the day so as to reinforce their new-found knowledge.

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**
- **Smartphone examinations**
  - Evidence handling
  - Acquisitions from various devices
  - iOS and Android artifacts
  - Report creation