opentext™

Training overview

DF320 Advanced Analysis of Windows® Artifacts with EnCase™

Syllabus

Day 1

Day one begins with an overview of SQLite databases and how to query the data they contain followed by a practical exercise allowing the students to exercise these new skills and knowledge. Next, instruction continues with techniques on recovering deleted SQLite data.

The last lesson of the day focuses on to how to use block-based file hash analysis to recover deleted target files even if those files have been fragmented or partially overwritten followed by a practical exercise.

Day 1 will cover:

- Documenting the aspects of SQLite that will be most relevant to the forensic investigator
- Using Structured Query Language (SQL) to query SQLite data
- Understanding the structure of SQLite database files and how and why deleted data may be recoverable
- Using block-based hash analysis for file recovery

Day 2

Day two begins with instruction regarding the structure of the Windows® Registry and the examination techniques of associated artifacts. Students are shown how to extract registry values to facilitate the mounting of them into their own system in support of running applications extracted from the evidence file.

Next, the students are taught how to locate, recognize, and interpret Userassist and

Day 2 will cover:

- Understanding the purpose and structure of the Windows Registry
- Identifying, mounting, and extracting data from registry hive files both in OpenText™ EnCase™ software 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 Userassist registry data
- Parsing ShellBag data in conjunction with NTFS USN change-log data
- Understanding the purpose of the Windows Prefetcher and the structure and content of the prefetch files it maintains
- Understanding and accessing various application databases

Day 4

Day four begins with a lesson on decrypting a Windows BitLocker® protected volume. Students learn various techniques for examining RAM and for recovering information from ZIP archives and how this can be used to recover data from the latest type of Microsoft Word documents.

Next, the students will discuss the technology behind hardware and software RAID devices, how these devices should be forensically examined and how the RAID functionality within EnCase functions.

Students will complete relevant practical exercises throughout the day, reinforcing their new knowledge.

Day 4 will cover:

- Exploring the recovery options for decrypting Windows BitLocker protected volume
- Learning how to setup and configure the ability to conduct examinations of RAM
- Discussing the ZIP file format and how it affects 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
- Understanding RAID configurations and stripe sets
- Understanding how RAID affects forensic examinations
- Discussing options for forensic acquisition of RAID devices and their examination in EnCase software

opentext.com/contact