opentext™

Training overview

DF320 Advanced Analysis of Windows Artifacts with EnCase

Syllabus

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 extraction and installation of applications.

They are also shown how to examine user-assisted and shell-bag data. Following that, students learn how to use block-based file hash analysis to recover deleted target files even if those files have been fragmented or partially overwritten. The final lesson on day one documents the examination of Microsoft® Windows® event logs.

Day 1 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 user-assist Registry data
- Parsing shell-bag data in conjunction with NTFS USN change-log data
- Using block-based hash analysis for file recovery
- Analyzing Windows event logs

Day 2

Day two begins with a practical exercise focused on material covered during the Windows Event Logs lesson and continues with instruction on the Volume Shadow Copy Service (VSS). This function allows volume backups to be created while file system write operations are temporarily frozen.

Students will discuss the technology behind hardware and software RAID devices, how these devices should be forensically examined and how the RAID functionality in the EnCase Version 8 software functions. The third lesson on day two, introduces students to the Microsoft Windows Prefetcher and shows them how to examine the files it creates with a view to determining application usage.

The final lesson of the day provides an overview of SQLite databases and how to query the data they contain. Practical exercises will be administered throughout the day, allowing the students to test their newly learned skills.

opentext™

Day 2 will cover:

- Learning VSS operation and how to examine VSS data created by the system as part of system restore operations
- 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
- Understanding the purpose of the Windows Prefetcher and the structure and content of the prefetch files it maintains
- Documenting the aspects of SQLite that will be most relevant to the forensic investigator.
- Using Structured Query Language (SQL) to query SQLite data

Day 3

Day three begins with a practical exercise regarding the previous day's lesson on SQLite and continues with instruction on recovering deleted SQLite data. Students then learn 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. Students participate in practical exercises throughout the day.

Day 3 will cover:

- Understanding the structure of SQLite database files and how and why deleted data may be recoverable
- Understanding exactly what encrypted data is and the terminology associated with it
- Learning the principles behind identification of encryption software, encrypted data and the methodology behind decrypting encrypted data

Day 4

Day four begins with a lesson on Windows BitLocker, which is a full-volume encryption feature. 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.

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

Day 4 will cover:

- Understanding methods, configurations, recovery options and locating recovery keys included in Windows BitLocker
- Learning how to enhance 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

opentext.com/contact

Copyright © 2018 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information • (08/2018)10054EN