1. Record Nr. UNINA9910792087503321

Autore	Bunting Steve V
Titolo	Encase computer forensics [[electronic resource]] : the official ENCE : Encase certified examiner study guide / / Steve Bunting
Pubbl/distr/stampa	Indianapolis, IN, : Wiley Pub., Inc., 2012
ISBN	1-283-59322-X 9786613905673 1-118-21940-6
Edizione	[3rd ed.]
Descrizione fisica	1 online resource (746 p.)
Disciplina	005.8
Soggetti	Electronic data processing personnel - Certification Computer security - Examinations Computer networks - Security measures - Examinations Computer crimes - Investigation - Examinations Forensic sciences - Examinations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	EnCase Computer Forensics The Official EnCE: EnCase Certified Examiner Study Guide, Third Edition; Acknowledgments; About the Author; Contents at a Glance; Contents; Table of Exercises; Introduction; Assessment Test; Answers to Assessment Test; Chapter 1: Computer Hardware; The Boot Process; Partitions; File Systems; Summary; Exam Essentials; Review Questions; Chapter 2: File Systems; FAT Basics; NTFS Basics; exFAT; Exam Essentials; Chapter 3: First Response; Planning and Preparation; The Physical Location; Personnel; Computer Systems; What to Take with You Before You Leave Recording and Photographing the Scene Seizing Computer Evidence; Bagging and Tagging; Summary; Exam Essentials; Review Questions; Chapter 4: Acquiring Digital Evidence; Booting a Computer Using the EnCase Boot Disk; Other Reasons for Using a DOS Boot; Steps for Using a DOS Boot; Drive-to-Drive DOS Acquisition; Steps for Drive-to-Drive DOS Acquisition; Supplemental Information About Drive-to-Drive DOS Acquisition; Network Acquisitions; Reasons to Use Network Acquisitions; Preparing an EnCase Network Boot Disk; FastBloc 2

Features; Steps for Tableau (FastBloc) Acquisition
FastBloc SE Acquisitions About FastBloc SE; Steps for FastBloc SE Acquisitions; LinEn Acquisitions; Mounting a File System as Read-Only; Updating a Linux Boot CD with the Latest Version of LinEn; Steps for LinEn Acquisition; Enterprise and FIM Acquisitions; Summary; Exam Essentials; Review Questions; Chapter 5: EnCase Concepts; CRC, MD5, and SHA-1; EnCase Backup Utility; Evidence Cache Folder; Summary; Exam Essentials; Review Questions; Chapter 6: EnCase Environment; Home Screen; EnCase Layout; Creating a Case; Tree Pane Navigation; Disk View; View Pane Navigation; Text View; Hex View
Picture View Report View; Doc View; Transcript View; File Extents View; Permissions View; Decode View; Field View; Lock Option; Dixon Box; Find Feature; Other Views and Tools; Conditions and Filters; EnScript; Text Styles; Adjusting Panes; Other Views; Global Views and Settings; EnCase Options; Summary; Exam Essentials; Review Questions; Chapter 7: Understanding, Searching For, and Bookmarking Data; Understanding Data; Binary Numbers; Characters; Unicode; Searching for Data; GREP Keywords; Starting a Search; Bookmarking; Summary; Exam Essentials; Review Questions
Chapter 8: File Signature Analysis and Hash AnalysisFile Signature Analysis; Creating a New File Signature; Conducting a File Signature Analysis; Hash Analysis; Summary; Exam Essentials; Review Questions; Chapter 9: Windows Operating System Artifacts; Dates and Times; Time Zones; Windows 64-Bit Time Stamp; Adjusting for Time Zone Offsets; Recycle Bin; Determining the Owner of Files in the Recycle Bin; Using an EnCase Evidence Processor to Determine the Status of Recycle Bin Files; Recycle Bin Bypass; Windows Vista/Windows 7 Recycle Bin; Link Files; Changing the Properties of a Shortcut
Forensic Importance of Link Files

Sommario/riassunto

The official, Guidance Software-approved book on the newest EnCE exam! The EnCE exam tests that computer forensic analysts and examiners have thoroughly mastered computer investigation methodologies, as well as the use of Guidance Software's EnCase Forensic 7. The only official Guidance-endorsed study guide on the topic, this book prepares you for the exam with extensive coverage of all exam topics, real-world scenarios, hands-on exercises, up-to-date legal information, and sample evidence files, flashcards, and more. Guides readers through preparation for the newest EnCase Ce