1. Record Nr. UNINA9910827008003321

Autore	Marcella Albert J
Titolo	Cyber forensics : from data to digital evidence / / Albert J. Marcella, Jr., Frederic Guillossou
Pubbl/distr/stampa	Hoboken, NJ, : Wiley, 2012
ISBN	1-119-20345-7 1-280-59139-0 9786613621221 1-118-28268-X 1-118-28731-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (366 p.)
Collana	Wiley Corporate F&A series
Classificazione	BUS001000
Altri autori (Persone)	GuillossouFrederic <1970->
Disciplina	363.250285
Soggetti	Forensic sciences - Technological innovations Electronic evidence Evidence, Criminal Criminal investigation Computer crimes - Investigation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cyber Forensics: From Data to Digital Evidence; Contents; Preface; Acknowledgments; Chapter 1: The Fundamentals of Data; Base 2 Numbering System: Binary and Character Encoding; Communication in a Two-State Universe; Electricity and Magnetism; Building Blocks: The Origins of Data; Growing the Building Blocks of Data; Moving Beyond Base 2; American Standard Code for Information Interchange; Character Codes: The Basis for Processing Textual Data; Extended ASCII and Unicode; Summary; Notes; Chapter 2: Binary to Decimal; American Standard Code for Information Interchange; Computer as a Calculator Why Is This Important in Forensics?Data Representation; Converting Binary to Decimal; Conversion Analysis; A Forensic Case Example: An Application of the Math; Decimal to Binary: Recap for Review; Summary; Chapter 3: The Power of HEX: Finding Slivers of Data; What the HEX?; Bits and Bytes and Nibbles; Nibbles and Bits; Binary to HEX Conversion; Binary (HEX) Editor; The Needle within the Haystack; Summary; Notes;

Chapter 4: Files; Opening; Files, File Structures, and File Formats; File Extensions; Changing a File's Extension to Evade Detection; Files and the HEX Editor; File Signature
ASCII Is Not Text or HEXValue of File Signatures; Complex Files: Compound, Compressed, and Encrypted Files; Why Do Compound Files Exist?; Compressed Files; Forensics and Encrypted Files; The Structure of Ciphers; Summary; Notes; Appendix 4A: Common File Extensions; Appendix 4B: File Signature Database; Appendix 4C: Magic Number Definition; Appendix 4D: Compound Document Header; Chapter 5: The Boot Process and the Master Boot Record (MBR); Booting Up; Primary Functions of the Boot Process; Forensic Imaging and Evidence Collection; Summarizing the BIOS; BIOS Setup Utility: Step by Step
The Master Boot Record (MBR)Partition Table; Hard Disk Partition; Summary; Notes; Chapter 6: Endianness and the Partition Table; The Flavor of Endianness; Endianness; The Origins of Endian; Partition Table within the Master Boot Record; Summary; Notes; Chapter 7: Volume versus Partition; Tech Review; Cylinder, Head, Sector, and Logical Block Addressing; Volumes and Partitions; Summary; Notes; Chapter 8: File Systems-FAT 12/16; Tech Review; File Systems; Metadata; File Allocation Table (FAT) File System; Slack; HEX Review Note; Directory Entries; File Allocation Table (FAT)
How Is Cluster Size Determined?Expanded Cluster Size; Directory Entries and the FAT; FAT Filing System Limitations; Directory Entry Limitations; Summary; Appendix 8A: Partition Table Fields; Appendix 8B: File Allocation Table Values; Appendix 8C: Directory Entry Byte Offset Description; Appendix 8D: FAT 12/16 Byte Offset Values; Appendix 8E: FAT 32 Byte Offset Values; Appendix 8F: The Power of 2; Chapter 9: File Systems-NTFS and Beyond; New Technology File System; Partition Boot Record; Master File Table; NTFS Summary; exFAT; Alternative Filing System Concepts; Summary; Notes
Appendix 9A: Common NTFS System Defined Attributes

Sommario/riassunto

An explanation of the basic principles of data This book explains the basic principles of data as building blocks of electronic evidential matter, which are used in a cyber forensics investigations. The entire text is written with no reference to a particular operation system or environment, thus it is applicable to all work environments, cyber investigation scenarios, and technologies. The text is written in a step-by-step manner, beginning with the elementary building blocks of data progressing upwards to the representation and storage of information. It inlcudes practical exa