

1. Record Nr.	UNINA9910975182203321
Titolo	Big Data Analytics and Computing for Digital Forensic Investigations
Pubbl/distr/stampa	Milton, : CRC Press LLC, 2020
ISBN	1-00-302474-2 1-000-04503-X 1-000-04505-6 1-003-02474-2
Edizione	[1st ed.]
Descrizione fisica	1 online resource (235 pages) : illustrations
Altri autori (Persone)	SatpathySuneeta MohantySachi Nandan
Disciplina	363.25968 005.7
Soggetti	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 contenuto	Cover -- Half Title -- Title Page -- Copyright Page -- Table of Contents -- Preface -- Acknowledgments -- Editors -- Contributors -- Chapter 1 Introduction to Digital Forensics -- 1.1 Digital Forensics Overview -- 1.1.1 Definitions of Digital Forensics -- 1.1.2 The 3A's of Digital Forensics Methodology -- 1.1.3 The History of Digital Forensics -- 1.1.4 The Objectives of Digital Forensics -- 1.2 Digital Evidence -- 1.2.1 Active Data -- 1.2.2 Archival Data -- 1.2.3 Latent Data -- 1.2.4 Residual Data -- 1.3 Branches of Digital Forensics -- 1.3.1 Computer Forensics -- 1.3.2 Network Forensics -- 1.3.3 Software Forensics -- 1.3.4 Mobile Forensics -- 1.3.5 Memory Forensics -- 1.3.6 Malware Forensics -- 1.3.7 Database Forensics -- 1.3.8 Social Network Forensics -- 1.3.9 Anti-Forensics -- 1.3.10 Cloud Forensics -- 1.3.11 Bit Coin Forensics -- 1.3.12 Big Data Forensics -- 1.4 Phases of Forensic Investigation Process -- 1.4.1 Readiness -- 1.4.2 Identification -- 1.4.3 Collection -- 1.4.4 Analysis -- 1.4.5 Presentation -- 1.4.5.1 Chain of Custody -- 1.5 Conclusion -- References -- Chapter 2 Digital Forensics and Digital Investigation to Form a Suspension Bridge Flanked by Law Enforcement, Prosecution, and Examination of Computer Frauds and Cybercrime -- 2.1 Forensic

Science and Digital Forensics -- 2.2 Digital Forensics -- 2.2.1 Digital Evidence -- 2.3 Segments of Digital Forensics -- 2.3.1 Preparation -- 2.3.1.1 An Investigative Plan -- 2.3.1.2 Training and Testing -- 2.3.1.3 Equipment -- 2.4 Compilation -- 2.4.1 Evidence Search and Collection -- 2.4.2 Data Recovery -- 2.4.3 Assessment -- 2.4.4 Post-Assessment -- 2.5 Stepladder of Digital Forensic Investigation Model -- 2.5.1 Recognition of Sources of Digital Evidence -- 2.5.2 Conservation of Evidentiary Digital Data -- 2.5.3 Mining of Evidentiary Data from Digital Media Sources.

2.5.4 Recording of Digital Evidence in Form of Report -- 2.6 Disciplines of Digital Forensics -- 2.6.1 Computer Forensics -- 2.6.2 Network Forensics -- 2.6.3 Software Forensics -- 2.7 Digital Crime Investigative Tools and Its Overview -- 2.7.1 EnCase Toolkit -- 2.7.2 Forensic Toolkit -- 2.7.3 SafeBack Toolkit -- 2.7.4 Storage Media Archival Recovery Toolkit -- 2.8 Taxonomy of Digital Crime Investigative Tools -- 2.8.1 Functionalities of Digital Investigative Tool Can Be Grouped under -- 2.8.1.1 Replica of the Hard Drive -- 2.8.1.2 Investigational Analysis -- 2.8.1.3 Presentation -- 2.8.1.4 Documentary Reporting -- 2.9 Boundaries and Commendations of Digital Crime Investigative Tools -- 2.10 Conclusion -- References -- Chapter 3 Big Data Challenges and Hype Digital Forensic: A Review in Health Care Management -- 3.1 Introduction -- 3.2 Big Data for Health Care -- 3.3 Big Data for Health Care Strategy Making -- 3.3.1 Pattern Developments -- 3.3.2 Evaluation and Interpretation -- 3.3.3 Result and Usage -- 3.4 Opportunity Generation and Big Data in Health Care Sector -- 3.4.1 Value Creation -- 3.5 Big Data and Health Care Sector Is Meeting Number of Challenges -- 3.5.1 Volume -- 3.5.2 Variety -- 3.5.3 Velocity and Variety -- 3.5.4 Data Findings -- 3.5.5 Privacy -- 3.6 Digitalized Big Data and Health Care Issues -- 3.6.1 Effective Communication Safely Data Storage -- 3.6.2 Availability of Data for General People -- 3.6.3 Logical Data -- 3.6.4 Effective Communication of Health Care Data -- 3.6.5 Data Capturing -- 3.6.5.1 Alignment of Data Sources -- 3.6.5.2 Algorithm of Data for Suitable Analysis -- 3.6.6 Understanding the Output and Accessibility towards the End Users -- 3.6.6.1 Privacy and Secrecy -- 3.6.6.2 Governance and Ethical Standards -- 3.6.6.3 Proper Audit -- 3.7 Precautionary Attempt for Future Big Data Health Care -- 3.7.1 Data Secrecy.

3.7.2 Web-Based Health Care -- 3.7.3 Genetically and Chronic Disease -- 3.8 Forensic Science and Big Data -- 3.9 Types of Digital Forensics -- 3.9.1 Digital Image Forensics -- 3.9.2 Drawn Data for the Starting of a Process -- 3.9.3 Big Data Analysis -- 3.9.3.1 Definition -- 3.9.3.2 Interpretation -- 3.9.3.3 Big Data Framework -- 3.9.3.4 Forensic Tool Requirement for the Huge Data in Health Care -- 3.10 Digital Forensics Analysis Tools -- 3.10.1 AIR (Automated Image and Rest Store) -- 3.10.2 Autopsy -- 3.10.3 Window Forensic Tool Chart -- 3.10.4 Digital Evidence and Forensic Tool Kit -- 3.10.5 EnCase -- 3.10.6 Mail Examiner -- 3.10.7 FTK -- 3.10.8 Bulk Extractors -- 3.10.9 Pre-Discover Forensic -- 3.10.10 CAINE -- 3.10.11 Xplico -- 3.10.12 X-Ways Forensic -- 3.10.13 Bulk Extractor -- 3.10.14 Digital Forensics Framework -- 3.10.15 Oxygen Forensics -- 3.10.16 Internet Evidence Finder -- 3.11 Some Other Instruments for Big Data Challenge -- 3.11.1 MapReduce Technique -- 3.11.2 Decision Tree -- 3.11.3 Neural Networks -- 3.12 Conclusion -- References -- Chapter 4 Hadoop Internals and Big Data Evidence -- 4.1 Hadoop Internals -- 4.2 The Hadoop Architectures -- 4.2.1 The Components of Hadoop -- 4.3 The Hadoop Distributed File System -- 4.4 Data Analysis Tools -- 4.4.1 Hive -- 4.4.2 HBase -- 4.4.3 Pig -- 4.4.4 Scoop -- 4.4.5 Flume -- 4.5 Locating Sources of Evidence -- 4.5.1 The Data Collection -- 4.5.2

Structured and Unstructured Data -- 4.5.3 Data Collection Types -- 4.6
The Chain of Custody Documentation -- 4.7 Conclusion --
Bibliography -- Chapter 5 Security and Privacy in Big Data Access
Controls -- 5.1 Introduction -- 5.1.1 Big Data Is Not Big? -- 5.2 Big
Data Challenges to Information Security and Privacy -- 5.3 Addressing
Big Data Security and Privacy Challenges: A Proposal -- 5.4 Data
Integrity Is Not Data Security! -- 5.4.1 What Vs Why?.
5.4.2 Data Integrity: Process Vs State -- 5.4.3 Integrity Types --
5.4.3.1 Physical Integrity -- 5.4.3.2 Logical Integrity -- 5.4.3.3 Entity
Integrity -- 5.4.3.4 Referential Integrity -- 5.4.3.5 Domain Integrity --
5.4.3.6 User-Defined Integrity -- 5.5 Infiltration Activities: Fraud
Detection with Predictive Analytics -- 5.6 Case Study I: In a Secure
Social Application -- 5.6.1 Overall System Architecture -- 5.6.2
Registration on the Platform -- 5.6.3 Sharing Content on the Platform
-- 5.6.4 Accessing Content on the Platform -- 5.7 Case Study II --
5.7.1 An Intelligent Intrusion Detection/Prevention System on a
Software-Defined Network -- 5.7.2 The Code Reveals -- 5.7.3
Evaluation -- 5.8 Big Data Security: Future Directions -- 5.9 Final
Recommendations -- References -- Chapter 6 Data Science and Big
Data Analytics -- 6.1 Objective -- 6.2 Introduction -- 6.2.1 What Is Big
Data? -- 6.2.2 What Is Data Science? -- 6.2.3 What Is Data Analytics? --
6.2.3.1 Descriptive Analytics -- 6.2.3.2 Diagnostic Analytics -- 6.2.3.3
Predictive Analytics -- 6.2.3.4 Prescriptive Analytics -- 6.2.4 Data
Analytics Process -- 6.2.4.1 Business Understanding -- 6.2.4.2 Data
Exploration -- 6.2.4.3 Preprocessing -- 6.2.4.4 Modeling -- 6.2.4.5
Data Visualization -- 6.3 Techniques for Data Analytics -- 6.3.1
Techniques in Preprocessing Stage -- 6.3.1.1 Data Cleaning -- 6.3.1.2
Data Transformation -- 6.3.1.3 Dimensionality Reduction -- 6.3.2
Techniques in Modeling Stage -- 6.3.2.1 Regression -- 6.3.2.2
Classification -- 6.3.2.3 Clustering -- 6.3.2.4 Association Rules --
6.3.2.5 Ensemble Learning -- 6.3.2.6 Deep Learning -- 6.3.2.7
Reinforcement Learning -- 6.3.2.8 Text Analysis -- 6.3.2.9 Cross-
Validation -- 6.4 Big Data Processing Models and Frameworks -- 6.4.1
Map Reduce -- 6.4.2 Apache Frameworks -- 6.5 Summary --
References.
Chapter 7 Awareness of Problems and Defies with Big Data Involved in
Network Security Management with Revised Data Fusion-Based Digital
Investigation Model -- 7.1 Introduction -- 7.2 Big Data -- 7.2.1 Variety
-- 7.2.2 Volume -- 7.2.3 Velocity -- 7.2.4 Veracity -- 7.2.5 Value --
7.3 Big Data and Digital Forensics -- 7.4 Digital Forensic Investigation
and Its Associated Problem Statements -- 7.5 Relevance of Data Fusion
Application in Big Data Digital Forensics and Its Investigation -- 7.6
Data Fusion -- 7.6.1 The JDL Practical Data Fusion Procedural Model --
7.7 Revised Data Fusion-Based Digital Investigation Model for Digital
Forensic and Network Threat Management -- 7.7.1 Data Collection and
Preprocessing -- 7.7.2 Look-Up Table -- 7.7.3 Low-Level Fusion --
7.7.4 Data Estimation Phase -- 7.7.5 High-Level Fusion -- 7.7.6
Decision-Level Fusion -- 7.7.7 Forensic Logbook -- 7.7.8 User
Interface -- 7.8 Practicability and Likelihood of Digital Investigation
Model -- 7.9 Conclusion and Future Work -- References -- Chapter 8
Phishing Prevention Guidelines -- 8.1 Phishing -- 8.1.1 Why Phishing
Works -- 8.1.2 Phishing in Enterprise -- 8.2 Phishing Prevention
Guidelines -- 8.2.1 Cyber Awareness and Hygiene -- 8.2.2 Phishing
Prevention on Ground Level -- 8.2.3 Phishing Precautionary Measures
at Enterprise Environs -- 8.2.4 Sturdy and Meticulous Web
Development Is Recommended -- 8.2.5 Suggestive Measures for other
Cybercrime -- 8.3 Implementation of Phishing Prevention Guidelines --
8.4 Validation of Phishing Prevention Guidelines -- 8.5 Summary --

References -- Chapter 9 Big Data Digital Forensic and Cybersecurity --
9.1 Introduction -- 9.2 Computer Frauds and Cybercrime -- 9.2.1
Tools Used in Cybercrime -- 9.2.2 Cybercrime Statistics for 2018-2019
-- 9.3 Taxonomy -- 9.4 Information Warfare -- 9.4.1 The Basic
Strategies in Information Warfare.
9.4.2 Various Forms of Information Warfare.

Sommario/riassunto

Digital forensics has recently gained a notable development and become the most demanding area in today's information security requirement. This book investigates the areas of digital forensics, digital investigation and data analysis procedures as they apply to computer fraud and cybercrime, with the main objective of describing a variety of digital crimes and retrieving potential digital evidence. Big Data Analytics and Computing for Digital Forensic Investigations gives a contemporary view on the problems of information security. It presents the idea that protective mechanisms and software must be integrated along with forensic capabilities into existing forensic software using big data computing tools and techniques. Features Describes trends of digital forensics served for big data and the challenges of evidence acquisition Enables digital forensic investigators and law enforcement agencies to enhance their digital investigation capabilities with the application of data science analytics, algorithms and fusion technique This book is focused on helping professionals as well as researchers to get ready with next-generation security systems to mount the rising challenges of computer fraud and cybercrimes as well as with digital forensic investigations. Dr Suneeta Satpathy has more than ten years of teaching experience in different subjects of the Computer Science and Engineering discipline. She is currently working as an associate professor in the Department of Computer Science and Engineering, College of Bhubaneswar, affiliated with Biju Patnaik University and Technology, Odisha. Her research interests include computer forensics, cybersecurity, data fusion, data mining, big data analysis and decision mining. Dr Sachi Nandan Mohanty is an associate professor in the Department of Computer Science and Engineering at ICFAI Tech, ICFAI Foundation for Higher Education, Hyderabad, India. His research interests include data mining, big data analysis, cognitive science, fuzzy decision-making, brain-computer interface, cognition and computational intelligence.
