1. Record Nr. UNISA996418193003316

Autore	Iqbal Farkhund
Titolo	Machine Learning for Authorship Attribution and Cyber Forensics [[electronic resource] /] / by Farkhund Iqbal, Mourad Debbabi, Benjamin C. M. Fung
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-61675-4
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (IX, 158 p. 38 illus., 28 illus. in color.)
Collana	International Series on Computer, Entertainment and Media Technology, , 2364-9488
Disciplina	363.25028563
Soggetti	Data mining Machine learning Computer crimes Data Mining and Knowledge Discovery Machine Learning Cybercrime
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	1. Cybersecurity And Cybercrime Investigation -- 2. Machine Learning Framework For Messaging Forensics -- 3. Header-Level Investigation And Analyzing Network Information -- 4. Authorship Analysis Approaches -- 5. Authorship Analysis - Writeprint Mining For Authorship Attribution -- 6. Authorship Attribution With Few Training Samples -- 7. Authorship Characterization -- 8. Authorship Verification -- 9. Authorship Attribution Using Customized Associative Classification -- 10. Criminal Information Mining -- 11. Artificial Intelligence And Digital Forensics.
Sommario/riassunto	The book first explores the cybersecurity’s landscape and the inherent susceptibility of online communication system such as e-mail, chat conversation and social media in cybercrimes. Common sources and resources of digital crimes, their causes and effects together with the emerging threats for society are illustrated in this book. This book not only explores the growing needs of cybersecurity and digital forensics

but also investigates relevant technologies and methods to meet the said needs. Knowledge discovery, machine learning and data analytics are explored for collecting cyber-intelligence and forensics evidence on cybercrimes. Online communication documents, which are the main source of cybercrimes are investigated from two perspectives: the crime and the criminal. AI and machine learning methods are applied to detect illegal and criminal activities such as bot distribution, drug trafficking and child pornography. Authorship analysis is applied to identify the potential suspects and their social linguistics characteristics. Deep learning together with frequent pattern mining and link mining techniques are applied to trace the potential collaborators of the identified criminals. Finally, the aim of the book is not only to investigate the crimes and identify the potential suspects but, as well, to collect solid and precise forensics evidence to prosecute the suspects in the court of law. .