1.

Record Nr.	UNINA990009685500403321
Autore	Tombrägel, Martin
Titolo	Die republikanischen Otiumvillen von Tivoli / Martin Tombrägel
Pubbl/distr/stampa	Wiesbaden : Reichert, 2012
ISBN	978-3-89500-875-7
Descrizione fisica	256 p. : ill. ; 29 cm
Collana	Palilia ; 25
Disciplina	728.8209377 930.1
Locazione	FLFBC
Collocazione	930.1 PALILIA 25
Lingua di pubblicazione	Tedesco Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2.	Record Nr.	UNISA996214755903316
	Autore	Hatcher Robert D.
	Titolo	Southern Appalachian Windows: Comparison of Styles, Scales, Geometry, and Detachment Levels of Thrust Faults in the Foreland and Internides of a Thrust-Dominated Orogen
	Pubbl/distr/stampa	[Place of publication not identified], : American Geophysical Union, 1989
	ISBN	1-118-66691-7
	Descrizione fisica	1 online resource (ix, 93 pages) : illustrations
	Collana	Field trip guidebook (International Geological Congress (28th : 1989 : Washington, D.C.)) ; ; T167
	Disciplina	557.688
	Soggetti	Geology - Appalachian Region, Southern
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Sommario/riassunto	Published by the American Geophysical Union as part of the Field Trip Guidebooks Series, Volume 167. The southern Appalachian orogen contains most of the subdivisions that characterize a classic collisional orogen: A foreland fold-and-thrust belt (Cumberland Plateau and Valley and Ridge), high-grade metamorphic core (central to eastern Blue Ridge and western Piedmont), and a plutonic/volcanic belt (Charlotte belt and Carolina slate belt). In addition, a younger Alleghanian high-grade metamorphic core is present on the eastern edge of the Piedmont (Kiokee-Raleigh belt).

3.	Record Nr.	UNINA9910484631603321
	Titolo	Malware Analysis Using Artificial Intelligence and Deep Learning / / edited by Mark Stamp, Mamoun Alazab, Andrii Shalaginov
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
	ISBN	3-030-62582-6
	Edizione	[1st ed. 2021.]
	Descrizione fisica	1 online resource (XX, 651 p. 253 illus., 209 illus. in color.)
	Disciplina	005.84
	Soggetti	Computer crimes Machine learning Computational intelligence Data protection Computer Crime Machine Learning Computational Intelligence Security Services
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references.
	Nota di contenuto	1. Optimizing Multi-class Classification of Binaries Based on Static Features -- 2.Detecting Abusive Comments Using Ensemble Deep Learning Algorithms -- 3. Deep Learning Techniques for Behavioural Malware Analysis in Cloud IaaS -- 4. Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges -- 5. A Selective Survey of Deep Learning Techniques and Their Application to Malware Analysis -- 6. A Comparison of Word2Vec, HMM2Vec, and PCA2Vec for Malware Classification -- 7. Word Embedding Techniques for Malware Evolution Detection -- 8. Reanimating Historic Malware Samples -- 9. DURLD: Malicious URL detection using Deep learning based Character-level representations -- 10. Sentiment Analysis for Troll Detection on Weibo -- 11. Beyond Labeling: Using Clustering to Build Network Behavioral Profiles of Malware Families -- 12. Review of the Malware Categorization in the Era of Changing Cybethreats Landscape: Common Approaches,

Challenges and Future Needs -- 13. An Empirical Analysis of Image-Based Learning Techniques for Malware Classification -- 14. A Survey of Intelligent Techniques for Android Malware Detection -- 15. Malware Detection with Sequence-Based Machine Learning and Deep Learning -- 16. A Novel Study on Multinomial Classification of x86/x64 Linux ELF Malware Types and Families through Deep Neural Networks -- 17. Cluster Analysis of Malware Family Relationships -- 18. Log-Based Malicious Activity Detection using Machine and Deep Learning -- 19. Deep Learning in Malware Identification and Classification -- 20. Image Spam Classification with Deep Neural Networks -- 21. Fast and Straightforward Feature Selection Method -- 22. On Ensemble Learning -- 23. A Comparative Study of Adversarial Attacks to Malware Detectors Based on Deep Learning -- 24. Review of Artificial Intelligence Cyber Threat Assessment Techniques for Increased System Survivability -- 25. Universal Adversarial Perturbations and Image Spam Classifiers.

Sommario/riassunto

This book is focused on the use of deep learning (DL) and artificial intelligence (AI) as tools to advance the fields of malware detection and analysis. The individual chapters of the book deal with a wide variety of state-of-the-art AI and DL techniques, which are applied to a number of challenging malware-related problems. DL and AI based approaches to malware detection and analysis are largely data driven and hence minimal expert domain knowledge of malware is needed. This book fills a gap between the emerging fields of DL/AI and malware analysis. It covers a broad range of modern and practical DL and AI techniques, including frameworks and development tools enabling the audience to innovate with cutting-edge research advancements in a multitude of malware (and closely related) use cases.