1.	Record Nr.	UNINA9910677213903321
	Titolo	Digital forensics and internet of things : impact and challenges / / edited by Anita Gehlot [and three others]
	Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, , [2022] ©2022
	ISBN	1-119-76905-1 1-119-76903-5
	Descrizione fisica	1 online resource (252 pages)
	Disciplina	363.252
	Soggetti	Digital forensic science Internet of things
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Front Matter -- Face Recognition-Based Surveillance System: A New Paradigm for Criminal Profiling / Payal Singh, Sneha Gupta, Vipul Gupta, Piyush Kuchhal, Arpit Jain -- Smart Healthcare Monitoring System: An IoT-Based Approach / Paranjeet Kaur -- Design of Gesture-Based Hand Gloves Using Arduino UNO: A Grace to Abled Mankind / Harpreet Singh Bedi, Dekkapati Vinit Raju, Meghanath Reddy C Nandyala, Partha Sai Kumar, Mandla Ravi Varma -- Playing With Genes: A Pragmatic Approach in Genetic Engineering / Prerna Singh, Dolly Sharma -- Digital Investigative Model in IoT: Forensic View / Suryapratap Ray, Tejasvi Bhatia -- Internet of Things Mobility Forensics / Shipra Rohatgi, Aman Sharma, Bhavya Sharma -- A Generic Digital Scientific Examination System for Internet of Things / Shipra Rohatgi, Sakshi Shrivastava -- IoT Sensors: Security in Network Forensics / D Karthika -- Xilinx FPGA and Xilinx IP Cores: A Boon to Curb Digital Crime / B Khaleelu Rehman, G Vallathan, Vetriveeran Rajamani, Salauddin Mohammad -- Human-Robot Interaction: An Artificial Cognition-Based Study for Criminal Investigations / Deepansha Adlakha, Dolly Sharma -- VANET: An IoT Forensic-Based Model for Maintaining Chain of Custody / Manoj Sindhwani, Charanjeet Singh, Rajeshwar Singh -- Cognitive Radio Networks: A Merit for Teleforensics / Thareja Yogita, Kamal Kumar Sharma, Parulpreet Singh -- Fingerprint

Sommario/riassunto

DIGITAL FORENSICS AND INTERNET OF THINGS It pays to be ahead of the criminal, and this book helps organizations and people to create a path to achieve this goal. The book discusses applications and challenges professionals encounter in the burgeoning field of IoT forensics. IoT forensics attempts to align its workflow to that of any forensics practice--investigators identify, interpret, preserve, analyze and present any relevant data. As with any investigation, a timeline is constructed, and, with the aid of smart devices providing data, investigators might be able to capture much more specific data points than in a traditional crime. However, collecting this data can often be a challenge, as it frequently doesn't live on the device itself, but rather in the provider's cloud platform. If you can get the data off the device, you'll have to employ one of a variety of methods given the diverse nature of IoT devices hardware, software, and firmware. So, while robust and insightful data is available, acquiring it is no small undertaking. Digital Forensics and Internet of Things encompasses: State-of-the-art research and standards concerning IoT forensics and traditional digital forensics Compares and contrasts IoT forensic techniques with those of traditional digital forensics standards Identifies the driving factors of the slow maturation of IoT forensic standards and possible solutions Applies recommended standards gathered from IoT forensic literature in hands-on experiments to test their effectiveness across multiple IoT devices Provides educated recommendations on developing and establishing IoT forensic standards, research, and areas that merit further study. Audience Researchers and scientists in forensic sciences, computer sciences, electronics engineering, embedded systems, information technology.