1. Record Nr. UNINA9910831025003321

Autore	Arnes Andre <1976->
Titolo	Cyber investigations : a research based textbook for advanced studies / / Andre Arnes
Pubbl/distr/stampa	Hoboken, NJ : , : John Wiley & Sons, Inc., , [2022] ©2022
ISBN	1-119-58202-4 1-119-58213-X
Descrizione fisica	1 online resource (272 pages)
Disciplina	363.25/968
Soggetti	Computer crimes - Investigation Digital forensic science Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Preface -- List of Contributors -- List of Figures -- List of Tables -- List of Examples -- List of Definitions -- List of Legal Provisions -- List of Equations -- List of Abbreviations -- Chapter 1 Introduction -- 1.1 Introduction -- 1.2 Cybercrime and Cybersecurity -- 1.2.1 Cybercrime -- 1.2.2 Cybercriminals and Threat Actors -- 1.2.3 Cybersecurity -- 1.2.4 Threat Modeling - Cyber Kill Chain and MITRE ATT&amp -- CK -- 1.3 Cyber Investigations -- 1.3.1 Digital Forensics -- 1.3.2 Digital Evidence -- 1.3.3 Attribution -- 1.3.4 Cyber Threat Intelligence -- 1.3.5 Open-Source Intelligence (OSINT) -- 1.3.6 Operational Avalanche - A Real-World Example -- 1.4 Challenges in Cyber Investigations -- 1.5 Further Reading -- 1.6 Chapter Overview -- 1.7 Comments on Citation and Notation -- 1.8 Exercises -- Chapter 2 Cyber Investigation Process -- 2.1 Introduction -- 2.2 Investigation as Information Work -- 2.3 Developing an Integrated Framework for Cyber Investigations -- 2.4 Principles for the Integrated Cyber Investigation Process (ICIP) -- 2.4.1 Procedure and Policy -- 2.4.2 Planning and Documentation -- 2.4.3 Forming and Testing of Hypotheses -- 2.4.4 The Dynamics of ICIP -- 2.4.5 Principles for Handling Digital Evidence -- 2.4.6 Limitations --