

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&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 --

2.5 ICIP's Procedural Stages -- 2.5.1 Investigation Initiation -- 2.5.2 Modeling -- 2.5.3 Planning and Prioritization -- 2.5.4 Impact and Risk Assessment -- 2.5.5 Action and Collection -- 2.5.6 Analysis and Integration -- 2.5.7 Documentation and Presentation -- 2.5.8 Evaluation -- 2.6 Cognitive and Human Error in Cyber Investigations -- 2.6.1 Cognitive Factors -- 2.6.2 Cognitive Biases -- 2.6.3 Countermeasures -- 2.7 Summary -- 2.8 Exercises -- Chapter 3 Cyber Investigation Law -- 3.1 Cyber Investigation in Context. 3.2 The Missions and Some Implications to Privacy Rights -- 3.2.1 The Police, Law Enforcement Agencies, and National Security Service -- 3.2.2 Reasonable Ground to Open a Criminal (Cyber) Investigation -- 3.2.3 The Legal Framework(s) -- 3.2.4 General Conditions for Privacy-Invasive Cyber Investigation Methods -- 3.2.5 The Private Sector Cyber Investigator -- 3.3 The Different Mandates of the LEA, NIS, and the Police -- 3.3.1 Law Enforcing Agencies and the Police -- 3.3.2 The National Intelligence Service (NIS) -- 3.4 Jurisdiction and International Cooperation -- 3.4.1 The eNIS and the Principle of Sovereignty -- 3.4.2 The iNIS and the LEA - International Cooperation -- 3.5 Human Rights in the Context of Cyber Investigations -- 3.5.1 The Right to Fair Trial -- 3.5.2 Covert Cyber Investigation -- 3.5.3 Technical Investigation Methods (Technical Hacking) -- 3.5.4 Methods Based on Social Skills (Social Hacking) -- 3.5.5 Open-Source Intelligence/Investigation -- 3.6 The Private Cyber Investigator -- 3.6.1 Cyber Reconnaissance Targeting a Third Party -- 3.6.2 Data Protection and Privacy Rights -- 3.7 The Way Ahead -- 3.8 Summary -- 3.9 Exercises -- Chapter 4 Perspectives of Internet and Cryptocurrency Investigations -- 4.1 Introduction -- 4.2 Case Examples -- 4.2.1 The Proxy Seller -- 4.2.2 The Scammer -- 4.2.3 The Disgruntled Employee -- 4.3 Networking Essentials -- 4.4 Networks and Applications -- 4.4.1 Operational Security -- 4.4.2 Open Sources -- 4.4.3 Closed Sources -- 4.4.4 Networks -- 4.4.5 Peer-to-Peer -- 4.4.6 Applications -- 4.5 Open-Source Intelligence (OSINT) -- 4.5.1 Methodology -- 4.5.2 Types of Open-Source Data -- 4.5.3 Techniques for Gathering Open-Source Data -- 4.6 Internet Browsers -- 4.6.1 HTTP, HTML, JavaScript, and Cache -- 4.6.2 Uniform Resource Locators (URLs) -- 4.6.3 Cookies and Local Storage -- 4.6.4 Developer Tools. 4.6.5 Forensic Tools -- 4.7 Cryptocurrencies -- 4.7.1 Addresses and Transactions -- 4.7.2 Privacy -- 4.7.3 Heuristics -- 4.7.4 Exploring Transactions -- 4.8 Preparation for Analysis -- 4.8.1 Entity Extraction -- 4.8.2 Machine Translation and Transliteration -- 4.8.3 Metadata Extraction -- 4.8.4 Visualization and Analysis -- 4.9 Summary -- 4.10 Exercises -- Chapter 5 Anonymity and Forensics -- 5.1 Introduction -- 5.1.1 Anonymity -- 5.1.2 Degree of Anonymity -- 5.2 Anonymous Communication Technologies -- 5.2.1 High-Latency Anonymity -- 5.2.2 Low-Latency Anonymity -- 5.2.3 Anonymous Proxy -- 5.2.4 Cascading Proxies -- 5.2.5 Anonymity Networks -- 5.2.6 Recent Live Messaging and Voice Communication -- 5.3 Anonymity Investigations -- 5.3.1 Digital Forensics and Anonymous Communication -- 5.3.2 Local Logs -- 5.3.3 Network Logs -- 5.3.4 Live Forensics and Investigations -- 5.4 Summary -- 5.5 Exercises -- Chapter 6 Internet of Things Investigations -- 6.1 Introduction -- 6.2 What Is IoT? -- 6.2.1 A (Very) Short and Incomplete History -- 6.2.2 Application Areas -- 6.2.3 Models and Concepts -- 6.2.4 Protocols -- 6.3 IoT Investigations -- 6.3.1 Types of Events Leading to Investigations -- 6.3.2 Identifying an IoT Investigation -- 6.4 IoT Forensics -- 6.4.1 IoT and Existing Forensic Areas -- 6.4.2 Models -- 6.4.3 New Forensic Challenges -- 6.5 Summary -- 6.6 Exercises -- Chapter 7 Multimedia Forensics -- 7.1 Metadata -- 7.2 Image

Forensics -- 7.2.1 Image Trustworthiness -- 7.2.2 Types
of Examinations -- 7.2.3 Photography Process Flow -- 7.2.4
Acquisition Fingerprints -- 7.2.5 Image Coding Fingerprints -- 7.2.6
Editing Fingerprints -- 7.2.7 Deepfake Creation and Detection -- 7.3
Video Forensics -- 7.3.1 Video Process Flow -- 7.3.2 Reproduction
Detection -- 7.3.3 Source Device Identification -- 7.4 Audio Forensics
-- 7.4.1 Audio Fundamentals.
7.4.2 Digital Audio Recording Process -- 7.4.3 Authenticity Analysis --
7.4.4 Container Analysis -- 7.4.5 Content-Based Analysis -- 7.4.6
Electric Network Frequency -- 7.4.7 Audio Enhancements -- 7.4.8
Other Audio Forensic Methods -- 7.5 Summary -- 7.6 Exercises --
Chapter 8 Educational Guide -- 8.1 Academic Resources -- 8.2
Professional and Training Organizations -- 8.3 Nonacademic Online
Resources -- 8.4 Tools -- 8.4.1 Disk Analysis Tools -- 8.4.2 Memory
Analysis Tools -- 8.4.3 Network Analysis Tools -- 8.4.4 Open-Source
Intelligence Tools -- 8.4.5 Machine Learning -- 8.5 Corpora and Data
Sets -- 8.6 Summary -- References -- Index -- EULA.
