Understanding the latest capabilities in the cyber threat landscape and approaches is the best way users and organizations can prepare for potential negative events. Adopting an experiential learning approach, this book describes how cyber forensics researchers, educators and practitioners can keep pace with technological advances, and acquire the essential knowledge and skills, ranging from IoT forensics, malware analysis, and GTV and cloud forensics to network forensics and investigations. Given the growing importance of incident response and cyber forensics in our digitalized society, this book will be of interest and relevance to enterprises and professionals in the field, as well as students wanting to learn about cyber forensics.

Enterprise security is an important area since all types of organizations require secure and robust environments, platforms and services to work with people, data and computing applications. The book provides selected papers of the Second International Workshop on Information Security Applications (ISA 2017) and International Conference on Cybersecurity and Cloud Computing (ICCC 2017) to provide an in-depth overview of the issues surrounding digital forensic investigations in cloud and mobile applications.

This book presents the proceedings of the International Conference on Information Technology - New Generations (ITNG 2018) and the International Conference on Cyber Security and Digital Forensics (ICCSDF 2018), which were held in Vancouver, Canada, November 30–December 3, 2016. The conference proceedings provide an opportunity for researchers, educators and practitioners to exchange their discoveries and practices, to share research experiences and to discuss current challenges and future trends in the field of information technology. The book covers topics on computer crime, cybercrime, digital forensics, information security, and privacy. The book is intended for researchers, educators, and practitioners in the field of information technology and for students and professionals who wish to stay informed about the latest developments in the field.

Strategic Leadership in Digital Evidence: What Executives Need to Know provides leaders with broad knowledge and understanding of practical concepts in digital evidence. The book's chapters cover the different areas of IT that are of interest and relevance to researchers, educators and practitioners in the field, as well as students wanting to learn about cyber forensics.

Digital forensics has been a discipline of Information Security for decades now. Its principles, methodologies, and techniques have remained consistent despite the evolution of technology, and, ultimately, it can be applied to any form of digital data. However, within a corporate environment, digital forensic professionals are particularly challenged. They must maintain the legal admissibility and forensic viability of digital evidence in support of a broad range of different business functions that include incident response, electronic discovery (ediscovery), and ensuring the controls and accountability of such information across networks. The book provides a comprehensive overview of the latest developments in digital forensics, including topics such as cloud forensics, mobile forensics, and big data forensics.

This book is intended for researchers, educators, and practitioners in the field of digital forensics, as well as students and professionals who wish to stay informed about the latest developments in the field. The book is also a valuable resource for digital forensic practitioners, researchers in big data, cyber threat hunting and intelligence, data mining and other related areas.
Digital forensics deals with the acquisition, preservation, examination, analysis, and presentation of electronic evidence. Practically every crime now involves some digital evidence; digital forensics provides the techniques and tools to articulate this evidence. This book describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the technical and legal issues related to digital evidence and electronic crime investigations.

Handbook of Digital Forensics and Investigative Technology builds on the success of the Handbook of Computer Crime Investigation, bringing together renowned experts in all areas of digital forensics and investigation to provide the consummate resource for practitioners in the field. It is also designed as an accompanying text to Digital Evidence and Computer Crime. This unique collection details how to conduct digital investigations in both criminal and civil contexts, and how to locate and utilize digital evidence on computers, networks, and embedded systems. Specifically, the Investigative Methodology section of the Handbook provides expert guidance in the three main areas of practice: Forensic Analysis, Electronic Discovery, and Intrusion Investigation. The Technology section is extended and updated to reflect the state of the art in each area of specialization. The main areas of focus in the Technology section are forensic analysis of Windows, Unix, Macintosh, and embedded systems (including cellular telephones and other mobile devices), and investigations involving networks (including enterprise environments and mobile telecommunications technologies). This handbook is an essential technical reference and on-the-job guide that IT professionals, forensic practitioners, law enforcement, and attorneys will rely on when confronted with computer related crime and digital evidence of any kind. *Provides methodologies proven in practice for conducting digital investigations of all kinds *Demonstrates how to locate and interpret a wide variety of digital evidence, and how it can be useful in investigations *Presents tools in the context of the investigative process, including EnCase, FTK, ProDiscover, forensic, XACT, Network Miner, Splunk, flow-tools, and many other specialized utilities and analysis platforms *Case examples in every chapter give readers a practical understanding of the technical, logistical, and legal challenges that arise in real investigations

This book constitutes the refereed proceedings of the 10th International Conference on Global Security, Safety and Infrastructures, ICGSSI 2015, held in Magdeburg, Germany, in August 2017. The 30 papers presented in this volume were carefully reviewed and selected from 48 submissions. The contributions are covering the following areas: Systems Engineering, Cybersecurity and Information Security, Digital Forensics and Anti-Forensics, Computer Vision, Cyber-physical Systems, and Communications and Information Security. This book provides a comprehensive overview of the current state of research and practice in the field of digital forensics and provides an excellent resource for students, researchers, and professionals.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands for Information Security at the University of Tulsa, Tulsa, Oklahoma, USA. For more information about the 300 other books in the IFIP series, please visit www.springeronline.com. For more information about IFIP, please visit www.ifip.org.

This book features high-quality research papers presented at the International Conference on Application of Digital Security and Watermarking, IDW 2017, held in Magdeburg, Germany, in August 2017. The 30 papers presented in this volume were carefully reviewed and selected from 48 submissions. The contributions are covering the following areas: Systems Engineering, Cybersecurity and Information Security, Digital Forensics and Anti-Forensics, Computer Vision, Cyber-physical Systems, and Communications and Information Security. This book provides a comprehensive overview of the current state of research and practice in the field of digital forensics and provides an excellent resource for students, researchers, and professionals.

This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, IDF2C 2012, held in October 2012 in Lafayette, Indiana. USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybersecurity investigations.

Digital Forensics deals with the acquisition, preservation, examination, analysis, and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance – investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and issues in Digital Forensics Investigative Techniques Network Forensics Portable Electronic Device Forensics Linux and File System Forensics Applications and Techniques This book is the first volume of a new series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty-five edited papers from the First Annual IFIP WG 11.9 Conference on Digital Forensics, held at the National Center for Forensic Science, Orlando, Florida, USA in February 2005; Advances in Digital Forensics is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in development efforts for digital forensic communities. Mark Pollitt is President of Digital Evidence Professional Services, Inc., Ellicott City, Maryland, USA. Mr. Pollitt, who is retired from the Federal Bureau of Investigation (FBI), served as the Chief of the FBI's Computer Analysis Response Team, and Director of the Regional Computer Forensic Laboratory National Program. Subject Shetho is the F. P. W. Walter Professor of Computer Science and a principal with the Center for Information Security at the University of Tulsa, Tulsa, Oklahoma, USA. For more information about the 300 other books in the IFIP series, please visit www.springeronline.com. For more information about IFIP, please visit www.ifip.org.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

This book constitutes the refereed proceedings of the 10th International Conference on Global Security, Safety and Sustainability, ICGSSS 2015, held in London, UK, in September 2015. The 31 revised full papers presented were carefully reviewed and selected from 57 submissions. The papers focus on the challenges of complexity, rapid pace of change and risk/opportunity issues associated with the 21st century living systems, structures and infrastructures.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

This book constitutes the refereed proceedings of the 16th International Conference on Digital Forensics and Watermarking, IDW 2017, held in Magdeburg, Germany, in August 2017. The 30 papers presented in this volume were carefully reviewed and selected from 48 submissions. The contributions are covering the following areas: Systems Engineering, Cybersecurity and Information Security, Digital Forensics and Anti-Forensics, Computer Vision, Cyber-physical Systems, and Communications and Information Security. This book provides a comprehensive overview of the current state of research and practice in the field of digital forensics and provides an excellent resource for students, researchers, and professionals.
Implementing Digital Forensic Readiness: From Reactive to Proactive Process, Second Edition presents the optimal way for digital forensic and IT security professionals to implement a proactive approach to digital forensics. The book details how digital forensic processes can align strategically with business operations and an already existing information and data security program. Detailing proper collection, preservation, storage, and presentation of digital evidence, the procedures outlined illustrate how digital evidence can be an essential tool in mitigating risk and reducing the impact of both internal and external, digital incidents, disputes, and crimes. By utilizing a digital forensic readiness approach and stance, a company’s preparedness and ability to take action quickly and respond as needed. In addition, this approach enhances the ability to gather evidence, as well as the relevance, reliability, and credibility of any such evidence. New chapters to this edition include Chapter 4 on Code of Ethics and Standards, Chapter 5 on Digital Forensics as a Business, and Chapter 10 on Establishing Legal Admissibility. This book offers best practices to professionals on enhancing their digital forensic program, or how to start and develop one the right way for effective forensic readiness in any corporate or enterprise setting.

This unique book discusses the latest research, innovative ideas, challenges and computational intelligence (CI) solutions in computing. It presents novel, in-depth fundamental research on achieving a sustainable lifestyle for society, either from a methodological or from an application perspective. Sustainable computing has expanded to become a significant research area covering the fields of computer science and engineering, electrical engineering and other engineering disciplines, and there has been an increase in the amount of literature on aspects sustainable computing such as energy efficiency and natural resources conservation that emphasizes the role of ICT (information and communications technology) in achieving system design and operation objectives. The energy impact/design of more efficient IT infrastructures is a key challenge in realizing new computing paradigms. The book explores the uses of computational intelligence (CI) techniques for intelligent decision support that can be exploited to create effective computational models. It assesses sustainability in computing and information processing environments and technologies at the different levels of CI paradigms. An excellent guide to surveying the state of the art in computational intelligence applied to challenging real-world problems in sustainable computing, it is intended for scientists, practitioners, researchers and academicians dealing with the new challenges and advances in area.

This book constitutes the refereed proceedings of the 12th Pacific Asia Workshop on Intelligence and Security Informatics, PAISI 2017, held in Jeju Island, South Korea, in May 2017 in conjunction with PAKDD 2017, the 21st Pacific Asia Conference on Knowledge Discovery and Data Mining. The 8 revised full papers and one short paper were carefully reviewed and selected from 13 submissions. The papers cover topics such as information access and security, cybersecurity and infrastructure protection, data and text mining, and network based data analytics.

In recent years, industries have transitioned into the digital realm, as companies and organizations are adopting certain forms of technology to assist in information storage and efficient methods of data processing. This dependence has significantly increased the risk of cyber crime and breaches in data security. Fortunately, research in the area of cyber security and information protection is flourishing; however, it is the responsibility of industry professionals to keep pace with the current trends within this field. The Handbook of Research on Cyber Crime and Information Privacy is a collection of innovative research on the modern methods of crime and misconduct within cyber space. It presents novel solutions to securing and preserving digital information through practical examples and case studies. While highlighting topics including virus detection, surveillance technology, and social networks, this book is ideally designed for cybersecurity professionals, researchers, developers, practitioners, programmers, computer scientists, academicians, security analysts, educators, and students seeking up-to-date research on advanced approaches and developments in cyber security and information protection.


Digital forensics and multimedia forensics are rapidly growing disciplines whereby electronic information is extracted and interpreted for use in a court of law. These two fields are finding increasing importance in law enforcement and the investigation of cybercrime as the ubiquity of personal computing and the internet becomes ever-more apparent. Digital forensics involves investigating computer systems and digital artefacts in general, while multimedia forensics is a sub-topic of digital forensics focusing on evidence extracted from both normal computer systems and special multimedia devices, such as digital cameras. This book focuses on the interface between digital forensics and multimedia forensics, bringing two closely related fields of forensic expertise together to identify and understand the current state-of-the-art in digital forensic investigation. Both fields are expertly attended by both researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic image, forensic photogrammetry, biometric forensics, multimedia device identification, and image forgery detection among many others. Key features: Brings digital and multimedia forensics together with contributions from academia, law enforcement, and the digital forensics industry for extensive coverage of all the major aspects of digital forensics of multimedia data and devices Provides comprehensive and authoritative coverage of digital forensics of multimedia data and devices Offers not only explanations of techniques but also real-world and simulated case studies to illustrate how digital and multimedia forensics techniques work Includes a companion website hosting continually updated supplementary materials ranging from extended and updated coverage of standards to best practice guides, test datasets and more case studies

The current IT environment deals with novel, complex approaches such as information privacy, trust, digital forensics, management, and human aspects. This volume includes papers offering research contributions that focus both on access control in complex environments as well as other aspects of computer security and privacy.

The definitive test for students of digital forensics, as well as professionals looking to deepen their understanding of an increasingly critical field written by faculty members and associates of the world-renowned Norwegian Information Security Laboratory (NiLaB) at the Norwegian University of Science and Technology (NTNU), this textbook takes a scientific approach to digital forensics ideally suited for university courses in digital forensics and information security. Each chapter was written by an accomplished expert in his or her field, many of them with extensive experience in law enforcement and industry. The author team comprises experts in digital forensics, cybercrime law, information security and related areas. Digital forensics is a key competency in meeting the growing risks of cybercrime, as well as for criminal investigation generally. Considering the astonishing pace at which new information technology – and new ways of exploiting information technology – is brought on line, researchers and practitioners regularly face new technical challenges, forcing them to continuously upgrade their investigatory skills. Designed to prepare the next generation to rise to those challenges, the material contained in Digital Forensics has been tested and refined by use in both graduate and undergraduate programs and subjected to formal evaluations for more than ten years. Encompasses all aspects of the field, including methodological, scientific, technical and legal matters. Based on the latest research, it provides novel insights for students, including an informed look at the future of digital forensics Includes test questions from actual exam sets, multiple choice questions suitable for online use and numerous visuals. Illustrations and case example images Features real-world examples and scenarios, including court cases and technical problems, as well as a rich library of academic references and references to online media Digital Forensics is an excellent introductory text for programs in computer science and computer engineering and for master degree programs in military and police education. It is also a valuable reference for legal practitioners, police officers, investigators, and forensic practitioners seeking to gain a deeper understanding of digital forensics and cybercrime.

This book constitutes the thoroughly refereed proceedings of the 15th International Workshop on Information Security Applications, WISA 2014, held on Jeju Island, Korea, in August 2014. The 30 revised full papers presented in this volume were carefully reviewed and selected from 69 submissions. The papers are organized in topical sections such as malware detection; mobile security; vulnerability analysis; applied cryptography; network security; cryptography; hardware security; and critical infrastructure security and policy.

The book is a collection of high-quality peer-reviewed research papers presented at the Fifth International Conference on Innovations in Computer Science and Engineering (ICICSE 2017) held at Guru Nanak Institutions, Hyderabad, India during 18-19 August 2017. The book discusses a wide variety of industrial, engineering and scientific applications of the engineering technologies. Researchers from academic and industry present their original work and exchange ideas, information, techniques and applications in the field of Communication, Computing and Data Science and Analytics.

The purpose of law is to prevent the society from harm by declaring what conduct is criminal, and prescribing the punishment to be imposed for such conduct. The pervasiveness of the internet and its anonymous nature make cyberspace a lawless frontier where
anarchy prevails. Historically, economic value has been assigned to visible and tangible assets. With the increasing appreciation that intangible data disseminated through an intangible medium can possess economic value, cybercrime is also being recognized as an economic asset. The Cybercrime, Digital Forensics and Jurisdiction disseminate knowledge for everyone involved with understanding and preventing cybercrime - business entities, private citizens, and government agencies. The book is firmly rooted in the law demonstrating that a viable strategy to confront cybercrime must be international in scope.

Forensic science includes all aspects of investigating a crime, including chemistry, biology and physics, and also incorporates countless other specialties. Today, the service offered under the guise of forensic science includes specialties from virtually all aspects of modern science, medicine, engineering, mathematics and technology. The Encyclopedia of Forensic Sciences, Second Edition is a reference source that will inform both criminals and forensic investigators about criminal events and the laboratory equipment of each other’s protocols, methodologies and limitations. Written by leading scientists in each area, every article is peer reviewed to establish clarity, accuracy, and comprehensiveness. As reflected in the specialties of its Editorial Board, the contents cover the core theories, methods and techniques employed by forensic scientists – and applications of those that are used in forensic analysis. This 4-volume set represents a 35% growth in articles from the first edition, with a particular increase in coverage of DNA and digital forensics. Includes an international collection of contributors. The second edition features over 8,000 pages, nearly 350 articles, approximately 100 papers on average. Each article features a suggested readings which point readers to additional sources for more information, b) a list of related Web sites, c) a 5-10 word glossary and definition paragraph, and d) cross-references to related articles in the encyclopedia. Available online via ScienceDirect. Please visit www.info.sciencedirect.com for more information. This new edition continues the reputation of the first edition, which was awarded an Honorable Mention in the prestigious Dartmouth Medal competition for 2001. This award honors the creation of reference works of outstanding quality and significance, and is sponsored by the RUSA Committee of the American Library Association.

This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Workshop on Digital-Forensics and Watermarking, IWDW 2014, held in Taipei, Taiwan, during October 2014. The 32 full and 14 poster papers, presented together with 1 keynote speech, were carefully reviewed and selected from 79 submissions. The papers are organized in topical sections on forensic watermarking; reversible data hiding; visual cryptography; and steganography and steganalysis.

Auditing is constantly and quickly changing due to the continuous evolution of information and communication technologies. As the auditing process is forced to adapt to these changes, issues have arisen that lead to a decrease in the auditing effectiveness and efficiency, leading to a greater dissatisfaction among users. More research is needed to provide effective management and mitigation of the risk associated to organizational transactions and to assign a more reliable and accurate character to the execution of business transactions and processes. Organizational Auditing and Assurance in the Digital Age is an essential reference source that discusses challenges, identifies opportunities, and presents solutions in relation to issues in auditing, information systems auditing, and assurance services and provides best practices for ensuring accountability, accuracy, and transparency. Featuring research on topics such as forensic auditing, financial services, and corporate governance, this book is ideally designed for internal and external auditors, assurance providers, managers, risk managers, academicians, professionals, and students.

Computer software and its structures, devices and processes are woven into our everyday life. Their significance is not just technical: the algorithms, programming languages, abstractions and metadata that millions of people rely on every day have far-reaching implications for the way we understand the underlying dynamics of contemporary societies. In this innovative new book, software studies theorist Matthew Fuller examines how the introduction and expansion of computational systems into areas ranging from urban planning and state surveillance to games and voting systems are transforming our understanding of politics, culture and aesthetics in the twenty-first century. Combining historical insight and a deep understanding of the technology powering modern software systems with a powerful critical perspective, this book opens up new ways of understanding the fundamental infrastructures of contemporary life, economies, entertainment and warfare. In so doing Fuller shows that everyone must learn ‘how to be a geek’, as the seemingly opaque processes and structures of modern computer and software technology have a significance that no-one can afford to ignore. This powerful and engaging book will be of interest to everyone interested in a critical understanding of the political and cultural ramifications of digital media and computing in the modern world.

Digital Forensics with Open Source Tools is the definitive book on investigating and analyzing computer systems and media using open source tools. This book is a technical procedural guide, and explains the use of open source tools on Mac, Linux and Windows systems as a platform for performing computer forensics. Both well-known and novel forensic methods are demonstrated using command-line and graphical open source computer forensic tools for examining a wide range of target systems and artifacts. Written by world-renowned forensic practitioners, this book uses the most current examination and analysis techniques in the field. It consists of 9 chapters that cover a range of topics such as the open source examination platform; disk and file system analysis; Windows systems and artifacts; Linux systems and artifacts; Mac OS X systems and artifacts; Internet artifacts; and automating analysis and extending capabilities. The book lends itself to use by students and those entering the field who do not have means to purchase new tools for different investigations. This book will appeal to forensic practitioners from areas including incident response teams and computer forensic investigators; forensic technicians from legal, audit, and consulting firms; and law enforcement agencies. Written by world-renowned forensic practitioners Details core concepts and techniques of forensic file system analysis; Covers analysis of artifacts from the Mac, Mac, and Linux operating systems.

Issues in Applied Computing / 2013 Edition is a ScholarlyEditions™ book that delivers timely, authoritative, and comprehensive information about Computer-Assisted Tomography. The editors have built Issues in Applied Computing: 2013 Edition on the vast information databases of ScholarlyNews.™ You can expect the information about Computer-Assisted Tomography in this book to be deeper than what you can access anywhere else, as well as consistently reliable, authoritative, informed, and relevant. The content of Issues in Applied Computing: 2013 Edition has been produced by the world’s leading scientists, engineers, analysts, research institutions, and companies. All of the content is from peer-reviewed sources, and all of it is written, assembled, and edited by the editors at ScholarlyEditions™ and available exclusively from us. You now have a source you can cite with authority, confidence, and credibility. More information is available at http://www.ScholarlyEditions.com/.

This book constitutes the proceedings of the International Conference on Information Security and Assurance, held in Brno, Czech Republic in August 2011. As computer and internet technologies continue to advance at a fast pace, the rate of cybercrimes is increasing. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security, while cyberbullying, child stalking, cyber pornography, and trafficking crimes are made easier through the anonymity of the internet. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice addresses current challenges and issues emerging in cyber forensics and new investigative tools and methods that can be adopted and implemented to address these issues and counter security breaches within various organizations. It also examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. Highlighting a range of topics such as cybercrime, threat detection, and forensic science, this publication is an ideal reference source for security analysts, law enforcement, lawmakers, government officials, IT professionals, researchers, practitioners, academicians, and students currently investigating the up-and-coming aspects surrounding network security, computer science, and security engineering.