Standard Handbook Oil Spill Environmental ForensicsThe Official (ISC)2 SSCP CBK Reference Fundamentals of Network Forensics Forensic Engineering: Quality Management in Forensic Science Emerging Technologies for the Analysis of Forensic Traces CCWS 2020 15th International Conference on Cyber Warfare and Security Handbook of Digital Forensics of Multimedia Data and Devices, Enhanced E-Book Security, Privacy, and Digital Forensics in the Cloud The Forensic Laboratory Handbook Digital Forensics Cyber Forensics and Cyber Crime Publications of the National Institute of Standards and Technology Catalogue of Digital Forensics, Forensic Anthropology and Archaeology in Forensic Science Eining and Exchanging Electronic Evidence Across Europe Forensic Anthropology Digital Crime and Forensic Science in Cyberspace Information security: risk assessment, management systems, the ISO/IEC 27001 standardService-Oriented Mapping The Forensic Standard ISO/IEC 27037 to Cloud Computing Networking Forensic Engineering 11th International Conference on Cyber Warfare and Security CSA Guide to Cloud Computing A Guide to Forensic DNA Profiling The Global Practice of Forensic Science Advances in Digital Forensics XIII Forensic Laboratory Management Forensic Systems Engineering Forensic Investigation of Explosions Information Systems Design and Intelligent Applications Cybercrime Investigators Handbook Introduction to Environmental Forensics in Computing Trust, Privacy and Security in Digital Business Data-Centric Business and Applications Forensic Biology Information Systems: Development, Applications, Education Crime Scene Unit Management The increasingly arcane world of DNA profiling demands that those needing to understand at least some of it must find a source of reliable and understandable information. Combining material from the successful Wiley Encyclopedia of Forensic Science with newly commissioned and updated material, the Editors have used their own extensive experience in criminal casework across the world to compile an informative guide that will provide knowledge and thought-provoking articles of interest to anyone involved or interested in the use of DNA in the forensic context. Following extensive introductory chapters covering forensic DNA profiling and forensic genetics, this comprehensive volume presents a substantial breadth of material covering: Fundamental material – including sources of DNA, validation, and accreditation Analysis and interpretation – including, extraction, quantification, amplification and interpretation of electropherograms (epgs) Evaluation – including mixtures, low template, and transfer applications – databases, paternity and kinship, mitochondrial-DNA, wildlife DNA, single-nucleotide polymorphism, phenotyping and familial searching Court – report writing, discovery, cross examination, and current controversies With contributions from leading experts across the whole gamut of forensic science, this volume is intended to be authoritative but not authoritarian, informative but comprehensible, and comprehensive but concise. It will prove to be a valuable addition, and useful resource, for scientists, lawyers, teachers, criminologists, and judges. 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 XIII describes original research results and innovative applications in the 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; Mobile and Embedded Device Forensics; Network and Cloud Forensics; Threat Detection and Mitigation; Malware Forensics; Image Forensics; and Forensic Techniques. This book is the thirteenth volume in the annual 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 sixteen edited papers from the Thirteenth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in Orlando, Florida, USA in the winter of 2017. Advances in Digital Forensics XIII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA. Building on the authors’ previous work, this book addresses key
processes and procedures used in information/data processing and management. Modern methods of business information processing, which draw on artificial intelligence, big data, and cloud-based storage and processing, are opening exciting new opportunities for doing business on the basis of information technologies. Thus, in this third book, the authors continue to explore various aspects - technological as well as business and social - of the information industries. Further, they analyze the challenges and opportunities entailed by these kinds of business. New technologies, including DNA and digital databases that can compare known and questioned exemplars, have transformed forensic science and greatly impacted the investigative process. They have also made the work more complicated. Obtaining proper resources to provide quality and timely forensic services is frequently a challenge for forensic managers, who are often promoted from casework duties and must now learn a whole new set of leadership skills. The interdisciplinary and scientific nature of laboratories requires strong leadership ability to manage complex issues, often in adversarial settings. Forensic Laboratory Management: Applying Business Principles provides laboratory managers with business tools that apply the best science to the best evidence in a manner that increases the efficiency and effectiveness of their management decision making. The authors present a performance model with seven recommendations to implement, illustrating how forensic managers can serve as leaders and strategically improve the operation and management in scientific laboratories. Topics include: Key business metrics and cost-benefit analyses; Ethical lapses: why they occur, possible motives, and how problems can be prevented; Forensic training, education, and institutes; ISO/IEC 17025 accreditation implementation; The book includes case studies simulating a working laboratory in which readers can apply business tools with actual data reinforcing discussion concepts. Each chapter also includes a brief review of current literature of the best management theories and practice. The downloadable resources supply two mock trial transcripts and associated case files along with PowerPoint® slides from Dr. George Carmody’s workshop on Forensic DNA Statistics and Dr. Doug Lucas’s presentation on ethics. This book provides a line of communication between academia and end users/practitioners to advance forensic science and boost its contribution to criminal investigations and court cases. By covering the state of the art of promising technologies for the analysis of trace evidence using a controlled vocabulary, this book targets the forensics community as well as, crucially, informing the end users on novel and potential forensic opportunities for the fight against crime. By reporting end users' commentaries at the end of each chapter, the relevant academic community is provided with clear indications on where to direct further technological developments in order to meet the law requirements for operational deployment, as well as the specific needs of the end users. Promising chemistry-based technologies and analytical techniques as well as techniques that have already shown to various degrees an operational character are covered. The majority of the techniques covered have imaging capabilities, that is the ability to visualize the distribution of the target molecules within the trace evidence recovered. This feature enhances intelligibility of the information making it also accessible to a lay audience such as that typically found with a court jury. Trace evidence discussed in this book include fingerprints, bodily fluids, hair, gunshot residues, soil, ink and questioned documents thus covering a wide range of possible evidence recovered at crime scenes. This volume publishes new trends and findings in hot topics related to ubiquitous computing/networking. It is the outcome of UNet - an international scientific event that took place on September 08-10, 2015, in the fascinating city of Casablanca, Morocco. UNet'15 is technically sponsored by IEEE Morocco Section and IEEE COMSOC Morocco Chapter. The only official body of knowledge for SSCP—(ISC)2’s popular credential for hands-on security professionals—fully revised and updated. Systems Security Certified Practitioner (SSCP) is an elite, hands-on cybersecurity certification that validates the technical skills to implement, monitor, and administer IT infrastructure using information security policies and procedures. SSCP certification—fully compliant with U.S. Department of Defense Directive 8140 and 8570 requirements—is valued throughout the IT security industry. The Official (ISC)2 SSCP CBK Reference is the only official Common Body of Knowledge (CBK) available for SSCP-level practitioners, exclusively from (ISC)2, the global leader in cybersecurity certification and training. This authoritative volume contains essential knowledge practitioners require on a regular basis. A concise, up-to-date chapters provide in-depth coverage of the seven SSCP domains: Access Controls; Security Operations and Administration; Risk Identification, Monitoring and Analysis; Incident Response and Recovery; Cryptography; Network and Communications Security; and Systems and Application Security. Designed to serve as a reference for information security professionals throughout their careers, this indispensable (ISC)2 guide: Provides comprehensive coverage of the latest domains and objectives of the SSCP Helps better secure critical assets in their organizations Serves as a complement to the SSCP Study Guide for certification candidates The Official (ISC)2 SSCP CBK Reference is an essential resource for SSCP-level professionals, SSCP candidates and other practitioners involved in cybersecurity. Now in its second edition, Forensic Investigation of Explosions draws on the editor’s 30 years of explosives casework experience, including his work on task forces set up to investigate major explosives incidents. Dr. Alexander Beveridge provides a broad, multidisciplinary approach, assembling
the contributions of internationally recognized experts. This book constitutes the refereed proceedings of the 13th International Conference on Trust, Privacy and Security in Digital Business, TrustBus 2016, held in Porto, Portugal, in September 2016 in conjunction with DEXA 2016. The 8 revised full papers presented were carefully reviewed and selected from 18 submissions. The papers are organized in the following topical sections: security, privacy and trust in eServices; security and privacy in cloud computing; privacy requirements; and information audit and trust. The investigator’s practical guide for cybercrime evidence identification and collection. Cyber attacks perpetrated against businesses, governments, organizations, and individuals have been occurring for decades. Many attacks are discovered only after the data has been exploited or sold on the criminal markets. Cyber attacks damage both the finances and reputations of businesses and cause damage to the ultimate victims of the crime. From the perspective of the criminal, the current state of inconsistent security policies and lax investigative procedures is a profitable and low-risk opportunity for cyber attacks. They can cause immense harm to individuals or businesses online and make large sums of money—safe in the knowledge that the victim will rarely report the matter to the police. For those tasked with probing such crimes in the field, information on investigative methodology is scarce. The Cybercrime Investigators Handbook is an innovative guide that approaches cybercrime investigation from the field-practitioner’s perspective. While there are high-quality manuals for conducting digital examinations on a device or network that has been hacked, the Cybercrime Investigators Handbook is the first guide on how to commence an investigation from the location the offence occurred—the scene of the cybercrime—and collect the evidence necessary to locate and prosecute the offender. This valuable contribution to the field teaches readers to locate, lawfully seize, preserve, examine, interpret, and manage the technical evidence that is vital for effective cybercrime investigation. Fills the need for a field manual for front-line cybercrime investigators. Provides practical guidance with clear, easy-to-understand language. Approaches cybercrime form the perspective of the field practitioner. Helps companies comply with new GDPR guidelines. Offers expert advice from a law enforcement professional who specializes in cybercrime investigation and IT security. The Cybercrime Investigators Handbook is much-needed resource for law enforcement and cybercrime investigators, CFOs, IT auditors, fraud investigators, and other practitioners in related areas. Forensic anthropology has seen a recent expansion in depth and scope as well as increased attention from the media and the legal system. This constantly evolving science requires a comprehensive introductory text that approaches forensic anthropology as a modern discipline, with attention to theory as well as recent advances in research, technology, and challenges in the field. Forensic Anthropology: Current Methods and Practice, 2nd edition approaches forensic anthropology using current practices and case studies drawn from the varied experiences, backgrounds, and practices of working forensic anthropologists. This text guides the reader through all aspects of human remains recovery and forensic anthropological analysis. It presents principles at a level that is appropriate for those new to the field, while at the same time incorporating evolutionary, biomechanical, and other theoretical foundations for the features and phenomena encountered in forensic anthropological casework. Attention is focused on the most recent and scientifically valid applications commonly employed by working forensic anthropologists. Readers will learn about innovative techniques in the discipline, and aspiring practitioners will be prepared by understanding the necessary background needed to work in the field today. Instructors and students will find Forensic Anthropology: Current Methods and Practice, 2nd edition comprehensive, practical, and relevant to the modern discipline of forensic anthropology. Focuses on current methods, advances in research and technology, and recent challenges in the science of forensic anthropology. Addresses issues of international relevance such as the role of forensic anthropology in mass disaster response and human rights investigations. Includes chapter summaries, topic-oriented case studies, keywords, and reflective questions to increase active student learning. With contributions from 70 experienced practitioners from around the world, this second edition of the authoritative Handbook of Forensic Archaeology and Anthropology provides a solid foundation in both the practical and ethical components of forensic work. The book weaves together the discipline’s historical development; current field methods for analyzing crime, natural disasters, and human atrocities; an array of laboratory techniques; key case studies involving legal, professional, and ethical issues; and ideas about the future of forensic work—all from a global perspective. This fully revised second edition expands the geographic representation of the first edition by including chapters from practitioners in South Africa and Colombia, and adds exciting new chapters on the International Commission on Missing Persons and on forensic work being done to identify victims of the Battle of Fromelles during World War I. The Handbook of Forensic Anthropology and Archaeology provides an updated perspective of the disciplines of forensic archaeology and anthropology. CSA Guide to Cloud Computing brings you the most current and comprehensive understanding of cloud security issues and deployment techniques from industry thought leaders at the Cloud Security Alliance (CSA). For many years the CSA has been at the forefront of research and analysis into the most pressing security and privacy related issues associated with cloud computing. CSA Guide to Cloud
Computing provides you with a one-stop source for industry-leading content, as well as a roadmap into the future considerations that the cloud presents. The authors of CSA Guide to Cloud Computing provide a wealth of industry expertise you won't find anywhere else. Author Raj Samani is the Chief Technical Officer for McAfee EMEA; author Jim Reavis is the Executive Director of CSA; and author Brian Honan is recognized as an industry leader in the ISO27001 standard. They will walk you through everything you need to understand to implement a secure cloud computing structure for your enterprise or organization. Your one-stop source for comprehensive understanding of cloud security from the foremost thought leaders in the industry. Insight into the most current research on cloud privacy and security, compiling information from CSA’s global membership. Analysis of future security and privacy issues that will impact any enterprise that uses cloud computing. Forensic Engineering, the latest edition in the Advanced Forensic Science series that grew out of recommendations from the 2009 NAS Report: Strengthening Forensic Science: A Path Forward, serves as a graduate level text for those studying and teaching digital forensic engineering, as well as an excellent reference for a forensic scientist’s library or for their use in casework. Coverage includes investigations, transportation investigations, fire investigations, other methods and professional issues. Edited by a world-renowned leading forensic expert, this series is a long overdue solution for the forensic science community. Provides basic principles of forensic science and an overview of forensic engineering. Contains sections on investigations, transportation investigations, fire investigations and other methods includes a section on professional issues, such as: from crime scene to court, forensic laboratory reports and health and safety. Incorporates effective pedagogy, key terms, review questions, discussion questions and additional reading suggestions. This book constitutes the refereed proceedings of the SIGSAND/EPLAIS EuroSymposium 2015 titled Information Systems: Development, Applications, Education, held in Gdansk, Poland, in September 25. The objective of this symposium is to promote and develop high-quality research on all issues related to systems analysis and design (SAND). It provides a forum for SAND researchers and practitioners in Europe and beyond to interact, collaborate, and develop their field. The 11 papers presented in this volume were carefully reviewed and selected from 28 submissions. They are organized in topical sections: on Information systems development; business process modeling; and information systems education. Forensic Engineering: The Art and Craft of a Failure Detective synthesizes the current academic knowledge, with advances in process and techniques developed in the last several years, to bring forensic materials and engineering analysis into the 21st century. The techniques covered in the book are applied to the myriad types of cases the forensic engineer and investigator may face, serving as a working manual for practitioners. Analytical techniques and practical, applied engineering principles are illustrated in such cases as patent and intellectual property disputes, building and product failures, faulty design, air and rail disasters, automobile recalls, and civil and criminal cases. Both private and criminal cases are covered as well as the legal obligation, requirements, and responsibilities under the law, particularly in cases of serious injury or even death. Forensic Engineering will appeal to professionals working in failure analysis, loss adjustment, occupational health and safety as well as professionals working in a legal capacity in cases of produce failure and liability—including criminal cases, fraud investigation, and private consultants in engineering and forensic engineering. A comprehensive and easy-to-read introduction to the work of the modern forensic laboratory. The authors explain in simple language the capabilities and limitations of modern forensic laboratory procedures, techniques, analyses, and interpretations. Here, the interested reader will find an understandable and fascinating introduction to the complex worlds of forensic serology DNA, chemistry, crime reconstruction, digital evidence, explosives, arson, fingerprints, firearms, tool marks, odontology, and pathology. Additional chapters address the problems of assuring quality and seeking trace evidence in the forensic laboratory. In a unique and systematic way, this book discusses the security and privacy aspects of the cloud, and the relevant cloud forensics. Cloud computing is an emerging yet revolutionary technology that has been changing the way people live and work. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue. Written by some of the top experts in the field, this book specifically discusses security and privacy of the cloud, as well as the digital forensics of cloud data, applications, and services. The first half of the book enables readers to have a comprehensive understanding and background of cloud security, which will help them through the digital investigation guidance and recommendations found in the second half of the book. Part One of Security, Privacy and Digital Forensics in the Cloud covers cloud infrastructure security; confidentiality of data; access control in cloud IaaS; cloud security and privacy management; hacking and countermeasures; risk management and disaster recovery; auditing and compliance; and security as a service (SaaS). Part Two addresses cloud forensics — model, challenges, and approaches; cyberterrorism in the cloud; digital forensic process and model in the cloud; data acquisition; digital evidence management, presentation, and court preparation; analysis of digital evidence; and forensics as a service (FaaS). Thoroughly covers both security and privacy of cloud and digital forensics. Contributions by top researchers from the U.S.,
the European and other countries, and professionals active in the field of information and network security, digital and computer forensics, and cloud and big data. Of interest to those focused upon security and implementation, and incident management. Logical, well-structured, and organized to facilitate comprehension. Security, Privacy, and Digital Forensics in the Cloud is an ideal book for advanced undergraduate and master's-level students in information systems, information technology, computer and network forensics, as well as computer science. It can also serve as a good reference book for security professionals, digital forensics practitioners and cloud service providers.

Standard Handbook Oil Spill Environmental Forensics: Fingerprinting and Source Identification, Second Edition, provides users with the latest information on the tools and methods that have become popular over the past ten years. The book presents practitioners with the latest environmental forensics techniques and best practices for quickly identifying the sources of spills, how to form an effective response, and how to determine liability. This second edition represents a complete overhaul of the existing chapters, and includes 13 new chapters on methods and applications, such as emerging application of PAH isomers in oil spill forensics, development and application of computerized oil spill identification (COSI), and fingerprinting of oil in biological and passive sampling devices. Contains 13 new chapters on methods and applications, including emerging application of PAH isomers in oil drill forensics, the development and application of computerized oil spill identification (COSI), and the fingerprinting of oil in biological and passive sampling devices. Presents the latest technology and methods in biodegradation of oil hydrocarbons and its implications for source identification, surface trajectory modeling of marine oil spills, and identification of hydrocarbons in biological samples for source determination. Contains new case studies to illustrate key applications, methods, and techniques.

Digital forensics is the science of collecting the evidence that can be used in a court of law to prosecute the individuals who engage in electronic crime. Provided by publisher. The third international conference on Information Systems Design and Intelligent Applications (INDIA – 2016) held in Visakhapatnam, India during January 8-9, 2016. The book covers all aspects of information system design, computer science and technology, general sciences, and educational research. Upon a double blind review process, a number of high quality papers are selected and collected in the book, which is composed of three different volumes, and covers a variety of topics, including natural language processing, artificial intelligence, security and privacy, communications, wireless and sensor networks, microelectronics, circuit and systems, machine learning, soft computing, mobile computing and applications, cloud computing, software engineering, graphics and image processing, rural engineering, e-commerce, e-governance, business computing, molecular computing, nano-computing, chemical computing, intelligent computing for GIS and remote sensing, bio-informatics and bio-computing. These fields are not only limited to computer researchers but also include mathematics, chemistry, biology, bio-chemistry, engineering, statistics, and all others in which computer techniques may assist.

In this book, the following subjects are included:

- Information security, the risk assessment and treatment processes (with practical examples), the information security controls.
- The text is based on the ISO/IEC 27001 standard and on the discussions held during the editing meetings, attended by the author. Appendices include short presentations and check lists. CESARE GALLOTTI has been working since 1999 in the information security and IT process management fields and has been leading many projects for companies of various sizes and market sectors. He has been leading projects as consultant or auditor for the compliance with standards and regulations and has been designing and delivering ISO/IEC 27001, privacy and ITIL training courses. Some of his certifications are: Lead Auditor ISO/IEC 27001, Lead Auditor 9001, CISA, ITIL Expert and CBI, CIPPE. Since 2010, he has been Italian delegate for the the editing group for the ISO/IEC 27000 standard family. Web: www.cesaregallotti.it. Introduction to Environmental Forensics helps readers unravel the complexities of environmental pollution cases. It outlines techniques for identifying the source of a contaminant release, when the release occurred, and the extent of human exposure. Written by leading experts in environmental investigations, the text provides detailed information on chemical "fingerprinting" techniques applicable to ground water, soils, sediments, and air, plus an in-depth look at petroleum hydrocarbons. It gives the environmental scientist, engineer, and legal specialist a complete toolbox for conducting forensic investigations. It demonstrates the range of scientific analyses that are available to answer questions of environmental liability and support a legal argument, and provides several examples and case studies to illustrate how these methods are applied. This is a textbook that would prove useful to a range of disciplines, including environmental scientists involved in water and air pollution, contaminated land and geographical information systems; and archaeologists, hydrochemists and geochemists interested in dating sources of pollution. Co-edited by one of the experts from the Civil Action case in Woburn, MA. Provides essential information about identifying environmental contaminants responsible for millions of deaths per year. Contains the latest information and coverage of issues crucial to both forensics investigators and environmental scientists. Over the last several years, new research and developments in analysis methods and practice have led to rapid advancements in forensic biology. Identifying critical points of knowledge
and new methodological approaches in the field. Forensic Biology, Second Edition focuses on forensic serology and forensic DNA analysis. It provides students and professionals with a comprehensive understanding of the latest developments in the field. The book covers the principles of forensic science, including crime scene investigation, evidence collection, and analysis. It also includes chapters on the use of forensic techniques in various types of cases, such as violent crimes, sexual assault, and arson. The text is written in an accessible style, with numerous examples and case studies to illustrate the application of forensic science in real-world situations. It is an essential resource for students and professionals in the field of forensic science.
smartphone, and cloud forensics; reviews a number of freely available tools for performing forensic activities. Forensic science has been under scrutiny for some time, since the release of the NAS report in 2009. The report cited the need for standardized practices and the accreditation of crime labs. No longer can the forensic community take the position that cross-examination in a courtroom will expose weaknesses in methodology and execution. Quality Management in Forensic Science covers a wide spectrum of forensic disciplines, relevant ISO and non-ISO standards, accreditation and quality management systems necessary in any forensic science laboratory. Written by a globally well-respected forensic scientist with decades of experience in the forensic science laboratory and on the stand, as an expert witness who is also a Fellow of both the Royal Society of Chemistry and the Chartered Society of Forensic Sciences. This book will be a must-have resource for all forensic science stakeholders, particularly law enforcement agents and lawyers less familiar with the impact of quality management on the reliability of scientific evidence. A comprehensive, multidisciplinary reference of scientific practices for use in the forensic laboratory Coverage from DNA to toxicology, from trace evidence to crime scene and beyond Extensive review of ISO and non-ISO standards, accreditation, QMS and much more Written by a foremost forensic scientist with decades of experience in the laboratory and as an expert witness This volume offers a general overview on the handling and regulating electronic evidence in Europe, presenting a standard for the exchange process. Chapters explore the nature of electronic evidence and readers will learn of the challenges involved in upholding the necessary standards and maintaining the integrity of information. Challenges particularly occur when European Union member states collaborate and evidence is exchanged, as may be the case when solving a cybercrime. One such challenge is that the variety of possible evidence is so vast that potentially anything may become the evidence of a crime. Moreover, the introduction and the extensive use of information and communications technology (ICT) has generated new forms of crimes or new ways of perpetrating them, as well as a new type of evidence. Contributing authors examine the legal framework in place in various EU member states when dealing with electronic evidence, with prominence given to data protection and privacy issues. Readers may learn about the state of the art tools and standards utilized for treating and exchanging evidence, and existing platforms and environments run by different Law Enforcement Agencies (LEAs) at local and central level. Readers will also discover the operational point of view of LEAs when dealing with electronic evidence, and their requirements and expectations for the future. Finally, readers may consider a proposal for realizing a unique legal framework for governing in a uniform and aligned way the treatment and cross border exchange of electronic evidence in Europe. The use, collection and exchange of electronic evidence in the European Union context and the rules, practices, operational guidelines, standards and tools utilized by LEAs, judges, Public prosecutors and other relevant stakeholders are all covered in this comprehensive work. It will appeal to researchers in both law and computer science, as well as those with an interest in privacy, digital forensics, electronic evidence, legal frameworks and law enforcement. Crime Scene Unit Management: A Path Forward is a must-have resource for anyone involved with forensic investigations and the search for evidence at the crime scene. The book provides standards for how to manage a crime scene so that evidence is collected and preserved without errors and includes guidelines for how to implement the standards and set up regional training programs for smaller jurisdictions with tighter budgets. Key features include examples, checklists, and flow charts for evidence handling and routing. CSIs, fire investigators, homicide investigators, accident investigators, police executives, and students of forensic science will benefit from this thorough approach to how the crime scene—and the personnel charged with tending to the evidence—should be managed. The 11th International Conference on Cyber Warfare and Security (ICCWS 2016) is being held at Boston University, Boston, USA on the 17-18th March 2016. The Conference Chair is Dr Tanya Zlateva and the Programme Chair is Professor Virginia Greiman, both from Boston University. ICCWS is a recognised Cyber Security event on the International research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyber Warfare and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and expanding range of Cyberwar and Cyber Security research available to them. The keynote speakers for the conference are Daryl Haegley from the Department of Defense (DoD), who will address the topic Control Systems NetworksWhat’s in Your Building? and Neal Ziring from the National Security Agency who will be providing some insight to the issue of Is Security Achievable? A Practical Perspective. ICCWS received 125 abstract submissions this year. After the double blind, peer review process there are 43 Academic Research Papers 8 PhD papers Research papers, 7 Masters and 1 work-in-progress papers published in these Conference Proceedings. These papers represent work from around the world, including: Australia, Canada, China, Czech Republic, District of Columbia, Finland, France, Israel, Japan, Lebanon, Netherlands, Pakistan, Russian Federation, Saudi Arabia, South Africa, Turkey, United Arab Emirates, UK, USA. This book gathers various perspectives on modern map production. Its primary focus is on the new paradigm of “sharing and reuse,” which
is based on decentralized, service-oriented access to spatial data sources. Service-Oriented Mapping is one of the main paradigms used to embed big data and distributed sources in modern map production, without the need to own the sources. To be stable and reliable, this architecture requires specific frameworks, tools and procedures. In addition to the technological structures, organizational aspects and geographic information system (GIS) capabilities provide powerful tools to make modern geoinformation management successful. Addressing a range of aspects, including the implementation of the semantic web in geoinformatics, using big data for geospatial visualization, standardization initiatives, and the European spatial data infrastructure, the book offers a comprehensive introduction to decentralized map production. This text provides an examination of the aetiological development of forensic criminology in the UK. It links the subjects of scientific criminology, criminal investigations, crime scene investigation, forensic science and the legal system and it provides an introduction to the important processes that take place between the crime scene and the courtroom. These processes help identify, define and label the ‘criminal’ and are crucial for understanding any form of crime within society. The book includes sections on: • the epistemological and ontological philosophies of the natural sciences; • the birth of scientific criminology and its search for the criminal ‘body’; • the development of early forms of forensic science and crime scene investigation; • investigating crime; • information, material and evidence; • crime analysis and crime mapping; • scientific support and crime scene examination; and • forensic science and detection methods and forensics in the courtroom. The text combines coverage of historical research and contemporary criminal justice processes and provides an introduction to the most common forensic practices, procedures and uses that enable the identification and successful prosecution of criminals. Forensic Criminology is essential for students of criminology, criminal justice, criminal investigations and crime science. It is also useful to those criminal justice practitioners wishing to gain a more in-depth understanding of the links between criminology, criminal investigations and forensics techniques.

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 to by contributions from researchers and forensic practitioners specializing in diverse topics such as forensic authentication, forensic triage, 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 This book constitutes the refereed proceedings of the 10th International Conference on Digital Forensics and Cyber Crime, ICDF2C 2018, held in New Orleans, LA, USA, in September 2018. The 11 reviewed full papers and 1 short paper were selected from 33 submissions and are grouped in topical sections on carving and data hiding, android, forensic readiness, hard drives and digital forensics, artefact correlation."Describes the purpose of forensic systems engineering: to identify dysfunctional processes and to determine root causes of process failure, and further, to assist the court in determining whether harm or a breach of contract has occurred”---The Global Practice of Forensic Science presents histories, issues, patterns, and diversity in the applications of international forensic science. Written by 64 experienced and internationally recognized forensic scientists, the volume documents the practice of forensic science in 28 countries from Africa, the Americas, Asia, Australia and Europe. Each country’s chapter explores factors of political history, academic linkages, the influence of individual cases, facility development, types of cases examined, integration within forensic science, recruitment, training, funding, certification, accreditation, quality control, technology, disaster preparedness, legal issues, research and future directions. Aimed at all scholars interested in international forensic science, the volume provides detail on the diverse fields within forensic science and their applications around the world.

Copyright code : 4a15c705cf87387135d2e14ec7032b7a