This book examines two key themes in terrorism studies, the radicalization process and counter-terrorism policies, through the lens of social networks. The book aims to show that networks should be at the forefront not only when analysing terrorists, but also when assessing the responses to their actions. The volume makes a unique contribution by addressing two relatively new themes for terrorism studies. First it puts social relations and cooperation issues at the forefront – an approach often identified as crucial to future breakthroughs in the field. Second, many contributions tackle the role of the Internet in the process of radicalization and in recruitment more generally, a highly debated topic in the field today. In addition, the book provides a valuable mix of review essays, critical essays, and original empirical studies. This balanced approach is also found in the topics covered by the authors, as well as their academic disciplines, which include sociology, computer science, geography, history, engineering, and criminology as well as political science. Many of the true advances in terrorism studies depend on the successful collaboration of multi-disciplinary teams, each with a different set of methodological and conceptual tools. This volume reflects the newfound diversity in this field and is a true product of its time. This book will be of much interest to
students of terrorism studies, social networks, security studies, sociology, criminology and international relations in general. As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study. This book constitutes the proceedings of the 5th International Conference on Internet Science held in St. Petersburg, Russia, in October 2018. The 23 papers presented were carefully reviewed and selected for inclusion in this volume. They were organized in topical sections named: risks on the Internet: detecting harmful content and discussing regulation; methodologies for studies of online audiences; and online media and public issues. An exploration of the Dark Web—websites accessible only with special routing software—that examines the history of three anonymizing networks, Freenet, Tor, and I2P. The term “Dark Web” conjures up drug markets, unregulated gun sales, stolen credit cards. But, as Robert Gehl points out in Weaving the Dark Web, for each of these illegitimate uses, there are other, legitimate ones: the New York Times’s anonymous whistleblowing system, for example, and the use of encryption by political dissidents. Defining the Dark Web straightforwardly as websites that can be accessed only with special routing software, and noting the frequent use of “legitimate” and its variations by users,
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

journalists, and law enforcement to describe Dark Web practices (judging them “legit” or “shit”), Gehl uses the concept of legitimacy as a window into the Dark Web. He does so by examining the history of three Dark Web systems: Freenet, Tor, and I2P. Gehl presents three distinct meanings of legitimate: legitimate force, or the state’s claim to a monopoly on violence; organizational propriety; and authenticity. He explores how Freenet, Tor, and I2P grappled with these different meanings, and then discusses each form of legitimacy in detail by examining Dark Web markets, search engines, and social networking sites. Finally, taking a broader view of the Dark Web, Gehl argues for the value of anonymous political speech in a time of ubiquitous surveillance. If we shut down the Dark Web, he argues, we lose a valuable channel for dissent.Bill Gates quote, “Banking is necessary, but banks are not”, showcases the opportunity for financial services digital transformation. The next transition from industry 4.0 to 5.0 will impact all sectors, including banking. It will combine information technology and automation, based on artificial intelligence, person-robot collaboration, and sustainability. It is time to analyze this transformation in banking deeply, so that the sector can adequately change to the New Normal and a wholly modified banking model can be properly embedded in the business. This book presents a conceptual model of banking 5.0, detailing its implementation in processes, platforms, people, and partnerships of financial services organizations companies. The last part of the book is then dedicated to future developments. Of interest to academics, researchers, and professionals in banking, financial technology, and financial services, this book also includes business cases in financial services. Bernardo Nicoletti is a Professor of Operations Management at Temple University, Rome, Italy. He also provides consultancy advice and coaching in Europe, the Middle East, and Asia on ICT strategy, process improvement, and financial services. In his research, Bernardo has been particularly active in the application of the agile method and its tools to a variety of industries. He has authored 30 books on management and published 250 articles in domestic and international journals. He frequently speaks at international conferences. The University of Arizona Artificial Intelligence Lab (AI Lab) Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach. We aim to collect "ALL" web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc. We have developed various multilingual data mining, text mining, and web mining techniques to perform link analysis, content analysis, web metrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis in our research. The approaches and methods developed in this project contribute to advancing the field of Intelligence and Security Informatics (ISI). Such advances will help related stakeholders to perform terrorism research and facilitate international security and peace. This monograph aims to provide an overview of the Dark Web landscape, suggest a systematic, computational approach to understanding the problems, and illustrate with selected techniques, methods, and case studies developed by the University of Arizona AI Lab Dark
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

Web team members. This work aims to provide an interdisciplinary and understandable monograph about Dark Web research along three dimensions: methodological issues in Dark Web research; database and computational techniques to support information collection and data mining; and legal, social, privacy, and data confidentiality challenges and approaches. It will bring useful knowledge to scientists, security professionals, counterterrorism experts, and policy makers. The monograph can also serve as a reference material or textbook in graduate level courses related to information security, information policy, information assurance, information systems, terrorism, and public policy.


This book explores how potential bio-threats and risks may evolve post 9/11 given the rapid changes in biotechnology and synthetic biology. It also explores what role intelligence communities can play in understanding threats and risks. It argues that although bio-threats and risks are largely low probability and high impact in nature, intelligence in ‘Five Eyes’ countries remain insufficiently prepared to understand them. This book identifies key areas where intelligence reforms need to take place including a more strategic and systematic collaboration between national security/law enforcement intelligence and the scientific community. It is aimed at intelligence analysts, those in the scientific community working on health security threats, policy makers and researchers working on biosecurity and bioterrorism threats and risks.

This book presents the first
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

reference exposition of the Cyber-Deception Chain: a flexible planning and execution framework for creating tactical, operational, or strategic deceptions. This methodology bridges the gap between the current uncoordinated patchwork of tactical denial and deception (D&D) techniques and their orchestration in service of an organization’s mission. Concepts for cyber- D&D planning operations and management are detailed within the larger organizational, business, and cyber defense context. It examines the necessity of a comprehensive, active cyber denial scheme. The authors explain the organizational implications of integrating D&D with a legacy cyber strategy, and discuss trade-offs, maturity models, and lifecycle management. Chapters present the primary challenges in using deception as part of a security strategy, and guides users through the steps to overcome common obstacles. Both revealing and concealing fact and fiction have a critical role in securing private information. Detailed case studies are included. Cyber Denial, Deception and Counter Deception is designed as a reference for professionals, researchers and government employees working in cybersecurity. Advanced-level students in computer science focused on security will also find this book useful as a reference or secondary text book. This Volume presents the selected papers from the 5 Parallel Symposiums of the 2014 Fourth World Congress on Information and Communication Technologies (WICT 2014) held in Malacca, Malaysia. The theme of WICT 2014 ‘Innovating ICT for Social Revolutions’. WICT 2014 is Co-Organized by Machine Intelligence Research Labs (MIR Labs), USA and Universiti Teknikal Malaysia Melaka, Malaysia. WICT 2014 is technically co-sponsored by IEEE Systems, Man & Cybernetics Society Malaysia and Spain Chapters and Technically Supported by IEEE Systems Man and Cybernetics Society, Technical Committee on Soft Computing. Inside the Dark Web provides a broad overview of emerging digital threats and computer crimes, with an emphasis on cyberstalking, hacktivism, fraud and identity theft, and attacks on critical infrastructure. The book also analyzes the online underground economy and digital currencies and cybercrime on the dark web. The book further explores how dark web crimes are conducted on the surface web in new mediums, such as the Internet of Things (IoT) and peer-to-peer file sharing systems as well as dark web forensics and mitigating techniques. This book starts with the fundamentals of the dark web along with explaining its threat landscape. The book then introduces the Tor browser, which is used to access the dark web ecosystem. The book continues to take a deep dive into cybersecurity criminal activities in the dark net and analyzes the malpractices used to secure your system. Furthermore, the book digs deeper into the forensics of dark web, web content analysis, threat intelligence, IoT, crypto market, and cryptocurrencies. This book is a comprehensive guide for those who want to understand the dark web quickly. After reading Inside the Dark Web, you’ll understand The core concepts of the dark web. The different theoretical and cross-disciplinary approaches of the dark web and its evolution in the context of emerging crime threats. The forms of cybercriminal activity through the dark web and the technological and "social engineering" methods used to undertake such crimes. The behavior and role of offenders and victims in the dark web and analyze and assess the impact of
cybercrime and the effectiveness of their mitigating techniques on the various
domains. How to mitigate cyberattacks happening through the dark web. The dark
web ecosystem with cutting edge areas like IoT, forensics, and threat intelligence
and so on. The dark web-related research and applications and up-to-date on the
latest technologies and research findings in this area. For all present and aspiring
cybersecurity professionals who want to upgrade their skills by understanding the
concepts of the dark web, Inside the Dark Web is their one-stop guide to
understanding the dark web and building a cybersecurity plan. The global halal
industry is likely to grow to between three and four trillion US dollars in the next
five years, from the current estimated two trillion, backed by a continued demand
from both Muslims and non-Muslims for halal products. Realising the importance
of the halal industry to the global community, the Academy of Contemporary
Islamic Studies (ACIS), the Universiti Teknologi MARA Malaysia (UiTM) and
Sultan Sharif Ali Islamic University (UNISSA) Brunei have organised the 4th
International Halal Conference (INHAC) 2019 under the theme ‘Enhancing Halal
Sustainability’. This book contains selected papers presented at INHAC 2019. It
addresses halal-related issues that are applicable to various industries and
explores a variety of contemporary and emerging issues. It covers aspects of halal
food safety, related services such as tourism and hospitality, the halal industry-
including aspects of business ethics, policies and practices, quality assurance,
compliance and Shariah governance Issues, as well as halal research and
educational development. Highlighting findings from both scientific and social
research studies, it enhances the discussion on the halal industry (both in
Malaysia and internationally), and serves as an invitation to engage in more
advanced research on the global halal industry. Terrorism and Counterterrorism in
Canada analyses the nature and scope of the terrorist threat, the challenge of
Canadian foreign fighters and far-right extremism, key counterterrorism policies
and practices, and their consequences for Canadian society. In terms of public
opinion, new religious movements are considered controversial for a variety of
reasons ranging from how they speak, dress, and eat, to the way they think and
their sense of community. Their social organization often runs counter to popular
expectations by experimenting with communal living (or strict individualism),
alternative leadership roles (or flat network structures), unusual economic
dispositions, and new political and ethical values. As a result the general public
views new religions with a mixture of curiosity, amusement, and anxiety, sustained
by lavish media emphasis on oddness and tragedy rather than familiarity and lived
experience. This updated and revised second edition of Controversial New
Religions offers a scholarly, dispassionate look at those groups that have
generated the most attention, including some very well-known classical groups like
The Family, Unification Church, Scientology, and Jim Jones’ People’s Temple;
somerelative newcomers such as the Kabbalah Centre, the Order of the Solar
Temple, Branch Davidians, Heaven’s Gate, and the Falun Gong; and some
interesting cases like contemporary Satanism, the Raelians, Black nationalism,
and various Pagan groups. Written by established scholars as well as
youngerexperts in the field, each essay combines an overview of the history and
beliefs of each organization or movement with original and insightful analysis. By presenting decades of scholarly work on new religious movements in an accessible form, this book will be an invaluable resource for all those who seek a view of new religions that is deeper than what can be found in sensationalistic media stories. This book examines the most recent and contentious issues in relation to cybercrime facing the world today, and how best to address them. The contributors show how Eastern and Western nations are responding to the challenges of cybercrime, and the latest trends and issues in cybercrime prevention and control. Sponsored by the Communication, Information Technologies, and Media Sociology section of the American Sociological Association (CITAMS), this volume celebrates the section's thirtieth anniversary. It looks at the history of the section, reviews some of its most important themes, and sets the agenda for future discussion. The University of Arizona Artificial Intelligence Lab (AI Lab) Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach. We aim to collect "ALL" web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc. We have developed various multilingual data mining, text mining, and web mining techniques to perform link analysis, content analysis, web metrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis in our research. The approaches and methods developed in this project contribute to advancing the field of Intelligence and Security Informatics (ISI). Such advances will help related stakeholders to perform terrorism research and facilitate international security and peace. This monograph aims to provide an overview of the Dark Web landscape, suggest a systematic, computational approach to understanding the problems, and illustrate with selected techniques, methods, and case studies developed by the University of Arizona AI Lab Dark Web team members. This work aims to provide an interdisciplinary and understandable monograph about Dark Web research along three dimensions: methodological issues in Dark Web research; database and computational techniques to support information collection and data mining; and legal, social, privacy, and data confidentiality challenges and approaches. It will bring useful knowledge to scientists, security professionals, counterterrorism experts, and policy makers. The monograph can also serve as a reference material or textbook in graduate level courses related to information security, information policy, information assurance, information systems, terrorism, and public policy. Health Security Intelligence introduces readers to the world of health security, to threats like COVID-19, and to the many other incarnations of global health security threats and their implications for intelligence and national security. Disease outbreaks like COVID-19 have not historically been considered a national security matter. While disease outbreaks among troops have always been a concern, it was the potential that arose in the first half of the twentieth century to systematically design biological weapons and to develop these at an industrial scale, that initially drew the attention of security, defence and intelligence communities to biology and
medical science. This book charts the evolution of public health and biosecurity threats from those early days, tracing how perceptions of these threats have expanded from deliberately introduced disease outbreaks to also incorporate natural disease outbreaks, the unintended consequences of research, laboratory accidents, and the convergence of emerging technologies. This spectrum of threats has led to an expansion of the stakeholders, tools and sources involved in intelligence gathering and threat assessments. This edited volume is a landmark in efforts to develop a multidisciplinary, empirically informed, and policy-relevant approach to intelligence-academia engagement in global health security that serves both the intelligence community and scholars from a broad range of disciplines. The chapters in this book were originally published as a special issue of the journal, Intelligence and National Security. An argument that as we engage with social media on our digital devices we receive, modify, intensify, and transmit moods. Political risk was first introduced as a component for assessing risk not directly linked to economic factors following the flow of capital from the US to Europe after the Second World War. However, the concept has rapidly gained relevance since, with both public and private institutions developing complex methodologies designed to evaluate political risk factors and keep pace with the internationalization of trade and investment. Continued global and regional economic and political instability means a plethora of different actors today conduct a diverse range of political risk analyses and assessments. Starting from the epistemological foundations of political risk, this book bridges the gap between theory and practice, exploring operationalization and measurement issues with the support of an empirical case study on the Arab uprisings, discussing the role of expert judgment in political forecasting, and highlighting the main challenges and opportunities political risk analysts face in the wake of the digital revolution. This book demonstrates the advantage of a corpus based approach to Arabic, and presents an overview of current research on the Arabic language within corpus linguistics. Dealing not only with modern standard Arabic, the book also considers classical and colloquial forms. The ubiquity of the internet and social media has influenced the lives of people across the globe, including young people involved in street gangs and troublesome youth groups. This development raises important questions about the causes, features, and consequences of online gang behavior, as well as the consequences of this new phenomenon for gang prevention and intervention. In this edited volume, members of an international network of gang researchers, the Eurogang Program of Research, present findings and insights from recent academic gang studies focused on the use of internet and social media. It focuses on online features of gangs and the consequences of social media for the study of these groups. The second section of the book focuses on the meaning of online media for the prevention, monitoring and intervention of gangs, and for gang disengagement processes. This is the first volume focused on the role of internet and social media in the study of gangs. Providing much needed insights into online gang processes, it will appeal to students and researchers interested in gangs and juvenile delinquency, and to professionals, practitioners, and policy-makers working on
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems preventing or reducing gang involvement and delinquent behavior. This volume examines how generative mechanisms emerge in the social order and their consequences. It does so in the light of finding answers to the general question posed in this book series: Will Late Modernity be replaced by a social formation that could be called Morphogenic Society? This volume clarifies what a ‘generative mechanism’ is, to achieve a better understanding of their social origins, and to delineate in what way such mechanisms exert effects within a current social formation, either stabilizing it or leading to changes potentially replacing it. The book explores questions about conjuncture, convergence and countervailing effects of morphogenetic mechanisms in order to assess their impact. Simultaneously, it looks at how products of positive feedback intertwine with the results of (morphostatic) negative feedback. This process also requires clarification, especially about the conditions under which morphostasis prevails over morphogenesis and vice versa. It raises the issue as to whether their co-existence can be other than short-lived. The volume addresses whether or not there also is a process of ‘morpho-necrosis’, i.e. the ultimate demise of certain morphostatic mechanisms, such that they cannot ‘recover’. The book concludes that not only are generative mechanisms required to explain associations between variables involved in the replacement of Late Modernity by Morphogenic Society, but they are also robust enough to account for cases and times when such variables show no significant correlations. This two-volume set LNCS 11314 and 11315 constitutes the thoroughly refereed conference proceedings of the 19th International Conference on Intelligent Data Engineering and Automated Learning, IDEAL 2018, held in Madrid, Spain, in November 2018. The 125 full papers presented were carefully reviewed and selected from 204 submissions. These papers provided a timely sample of the latest advances in data engineering and automated learning, from methodologies, frameworks and techniques to applications. In addition to various topics such as evolutionary algorithms, deep learning neural networks, probabilistic modelling, particle swarm intelligence, big data analytics, and applications in image recognition, regression, classification, clustering, medical and biological modelling and prediction, text processing and social media analysis. This book examines the illegal behaviour of entrepreneurs and discusses how criminal entrepreneurs acquire information, learn from their entrepreneurial experiences, and utilize acquired knowledge to develop their organizations. Entrepreneurship in Policing and Criminal Contexts explores the contemporary and under researched themes of ‘entrepreneurial policing’ and ‘entrepreneurialism in criminal justice contexts’ which are emerging topics of both theoretical and practical interest in the current rapidly changing criminal justice environment. This book explores the challenges leaders in intelligence communities face in an increasingly complex security environment and how to develop future leaders to deal with these issues. As the security and policy-making environment becomes increasingly complicated for decision-makers, the focus on intelligence agencies ‘to deliver’ more value will increase. This book is the first extensive exploration of contemporary leadership in the context of intelligence agencies, principally in the ‘Five Eyes’ nations (i.e. Australia, United States,
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

United Kingdom, Canada, and New Zealand). It provides a grounded theoretical approach to building practitioner and researcher understanding of what individual and organisational factors result in better leadership. Using interviews from former senior intelligence leaders and a survey of 208 current and former intelligence leaders, the work explores the key challenges that leaders will likely face in the twenty-first century and how to address these. It also explores what principles are most likely to be important in developing future leaders of intelligence agencies in the future. This book will be of much interest to students of intelligence studies, strategic studies, leadership studies, security studies, and international relations.

This volume introduces the reader to the wide range of methods that digital humanities employ, and offers a practical guide to the study, interpretation, and presentation of cultural material and practices. In this instance, the editors consider digital humanities to include both the use of computing to understand cultural material in new ways, and the application of theories and methods from the humanities to interpret new technologies. Each chapter provides a step-by-step guide to cutting-edge methodologies so that students can make informed decisions about the methods they use, consider ethical practices, follow practical procedures, and present their work effectively. Readers will develop practical and reflexive understandings of the software and digital devices that they study and use for research, and the book will help new researchers collaborate and contribute to their scholarly communities, and to public discourse. As contemporary humanities work becomes increasingly interdisciplinary, and increasingly permeated by and with digital technologies, this volume helps new researchers navigate an evolving academic environment. Humanities and social sciences students will find this textbook an invaluable resource for assessing and creating digital projects.

As scholarly work on crime, deviance, criminal justice, and social control advances and sophisticated methods of investigation develop, chapter authors demonstrate the methodological maturity and diversity of current empirical research in criminology and criminal justice. With our ever-increasing reliance on computer technology in every field of modern life, the need for continuously evolving and improving cyber security remains a constant imperative. This book presents the 3 keynote speeches and 10 papers delivered at the 2nd Singapore Cyber Security R&D Conference (SG-CRC 2017), held in Singapore, on 21-22 February 2017. SG-CRC 2017 focuses on the latest research into the techniques and methodologies of cyber security. The goal is to construct systems which are resistant to cyber-attack, enabling the construction of safe execution environments and improving the security of both hardware and software by means of mathematical tools and engineering approaches for the design, verification and monitoring of cyber-physical systems. Covering subjects which range from messaging in the public cloud and the use of scholarly digital libraries as a platform for malware distribution, to low-dimensional bigram analysis for mobile data fragment classification, this book will be of interest to all those whose business it is to improve cyber security. The important and rapidly emerging new field known as ‘cyber threat intelligence’ explores the paradigm that defenders of computer networks gain a better understanding of their adversaries by
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

understanding what assets they have available for an attack. In this book, a team of experts examines a new type of cyber threat intelligence from the heart of the malicious hacking underworld - the dark web. These highly secure sites have allowed anonymous communities of malicious hackers to exchange ideas and techniques, and to buy/sell malware and exploits. Aimed at both cybersecurity practitioners and researchers, this book represents a first step toward a better understanding of malicious hacking communities on the dark web and what to do about them. The authors examine real-world darkweb data through a combination of human and automated techniques to gain insight into these communities, describing both methodology and results. This new Handbook provides a comprehensive, state-of-the-art overview of current knowledge and debates on terrorism and counterterrorism, as well as providing a benchmark for future research. The attacks of 9/11 and the ‘global war on terror’ and its various legacies have dominated international politics in the opening decades of the 21st century. In response to the dramatic rise of terrorism, within the public eye and the academic world, the need for an accessible and comprehensive overview of these controversial issues remains profound. The Routledge Handbook of Terrorism and Counterterrorism seeks to fulfil this need. The volume is divided into two key parts: Part I: Terrorism: This section provides an overview of terrorism, covering the history of terrorism, its causes and characteristics, major tactics and strategies, major trends and critical contemporary issues such as radicalisation and cyber-terrorism. It concludes with a series of detailed case studies, including the IRA, Hamas and Islamic State. Part II: Counterterrorism: This part draws on the main themes and critical issues surrounding counterterrorism. It covers the major strategies and policies, key events and trends and the impact and effectiveness of different approaches. This section also concludes with a series of case studies focused on major counterterrorism campaigns. This book will be of great interest to all students of terrorism and counterterrorism, political violence, counter-insurgency, criminology, war and conflict studies, security studies and IR more generally. A rigorous and comprehensive textbook covering the major approaches to knowledge graphs, an active and interdisciplinary area within artificial intelligence. The field of knowledge graphs, which allows us to model, process, and derive insights from complex real-world data, has emerged as an active and interdisciplinary area of artificial intelligence over the last decade, drawing on such fields as natural language processing, data mining, and the semantic web. Current projects involve predicting cyberattacks, recommending products, and even gleaning insights from thousands of papers on COVID-19. This textbook offers rigorous and comprehensive coverage of the field. It focuses systematically on the major approaches, both those that have stood the test of time and the latest deep learning methods. Despite illustrious origins dating to the 1920s, qualitative crime research has long been overshadowed by quantitative inquiry. After decades of limited use, there has been a notable resurgence in crime ethnography, naturalistic inquiry, and related forms of fieldwork addressing crime and related social control efforts. The Routledge Handbook of Qualitative Criminology signals this momentum as the first major reference work dedicated to crime ethnography.
Where To Download Dark Web Exploring And Data Mining The Dark Side Of The Web Integrated Series In Information Systems

and related fieldwork orientations. Synthesizing the foremost topics and issues in qualitative criminology into a single definitive work, the Handbook provides a "first-look" reference source for scholars and students alike. The collection features twenty original chapters on leading qualitative crime research strategies, the complexities of collecting and analyzing qualitative data, and the ethical propriety of researching active criminals and incarcerated offenders. Contributions from both established luminaries and talented emerging scholars highlight the traditions and emerging trends in qualitative criminology through authoritative overviews and "lived experience" examples. Comprehensive and current, The Routledge Handbook of Qualitative Criminology promises to be a sound reference source for academics, students and practitioners as ethnography and fieldwork realize continued growth throughout the 21st Century. "This introductory chapter sets forth three foundations for threat assessment and management: the first foundation is the defining of basic concepts, such as threat assessment and threat management; the second foundation outlines the similarities and differences between threat assessment and violence risk assessment; the third foundation is a detailed overview of the research findings, theoretical avenues, measurement instruments, and developments in practice over the past quarter century. The goal of our chapter is to introduce the professional reader to the young scientific field of threat assessment and management, and to clarify and guide the seasoned professional toward greater excellence in his or her work"--Die Bedeutung der Digitalisierung für Politik und Gesellschaft ist ein hoch aktuelles Themenfeld, das immer stärker auch politikwissenschaftlich beforscht und gelehrt wird. Die Beiträge des Bandes versammeln dazu programmatische Positionen, welche zentrale Aspekte und Perspektiven der sozialwissenschaftlichen Digitalisierungsforschung darstellen und diskutieren. Hierzu zählen u.a. Forschungsfelder aus den Bereichen Partizipations- und Parteienforschung, Governance der Digitalisierung, methodische Reflexionen über Computational Social Science und die Analyse von Demokратie und Öffentlichkeit unter den Bedingungen der Digitalisierung. One of the most important aspects for a successful police operation is the ability for the police to obtain timely, reliable and actionable intelligence related to the investigation or incident at hand. Open Source Intelligence (OSINT) provides an invaluable avenue to access and collect such information in addition to traditional investigative techniques and information sources. This book offers an authoritative and accessible guide on how to conduct Open Source Intelligence investigations from data collection to analysis to the design and vetting of OSINT tools. In its pages the reader will find a comprehensive view into the newest methods for OSINT analytics and visualizations in combination with real-life case studies to showcase the application as well as the challenges of OSINT investigations across domains. Examples of OSINT range from information posted on social media as one of the most openly available means of accessing and gathering Open Source Intelligence to location data, OSINT obtained from the darkweb to combinations of OSINT with real-time analytical capabilities and closed sources. In addition it provides guidance on legal and ethical considerations making it relevant reading for practitioners as well as academics and students with a view to obtain
trough, first-hand knowledge from serving experts in the field. Travelling through theories of emotion and affect, this book addresses the key ways in which media studies can be brought to bear upon everyday encounters with online cultures and practices. The book takes stock of where we are emotionally with regard to the Internet in the context of other screen media. Computational and mathematical models provide us with the opportunities to investigate the complexities of real world problems. They allow us to apply our best analytical methods to define problems in a clearly mathematical manner and exhaustively test our solutions before committing expensive resources. This is made possible by assuming parameter(s) in a bounded environment, allowing for controllable experimentation, not always possible in live scenarios. For example, simulation of computational models allows the testing of theories in a manner that is both fundamentally deductive and experimental in nature. The main ingredients for such research ideas come from multiple disciplines and the importance of interdisciplinary research is well recognized by the scientific community. This book provides a window to the novel endeavours of the research communities to present their works by highlighting the value of computational modelling as a research tool when investigating complex systems. We hope that the readers will have stimulating experiences to pursue research in these directions. The two-volume set LNCS 10587 + 10588 constitutes the refereed proceedings of the 16th International Semantic Web Conference, ISWC 2017, held in Vienna, Austria, in October 2017. ISWC 2017 is the premier international forum, for the Semantic Web / Linked Data Community. The total of 55 full and 21 short papers presented in this volume were carefully reviewed and selected from 300 submissions. They are organized according to the tracks that were held: Research Track; Resource Track; and In-Use Track.

Copyright code: f89eab2adf5b425f5af351c43c6c35a