Open Source Intelligence Osint Investigation Training

Thank you unconditionally much for downloading **Open Source Intelligence Osint Investigation Training** .Most likely you have knowledge that, people have look numerous period for their favorite books subsequently this Open Source Intelligence Osint Investigation Training , but end occurring in harmful downloads.

Rather than enjoying a fine PDF later a mug of coffee in the afternoon, then again they juggled when some harmful virus inside their computer. **Open Source Intelligence Osint Investigation Training** is simple in our digital library an online entry to it is set as public appropriately you can download it instantly. Our digital library saves in merged countries, allowing you to acquire the most less latency era to download any of our books as soon as this one. Merely said, the Open Source Intelligence Osint Investigation Training is universally compatible later than any devices to read.

Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise - Heather J. Williams 2018
"Prepared for the Office of the Secretary of Defense."
Congressional Record - United States. Congress 2009
The Congressional Record is the official record of the proceedings and debates of the United States Congress. It is published daily when Congress is in session. The Congressional Record began publication in 1873. Debates for sessions prior to 1873 are recorded in The Debates and Proceedings in the Congress of the United States (1789-1824), the Register of Debates in Congress (1824-1837), and the Congressional Globe (1833-1873)
Manuals Combined: U.S. Marine Corps Basic Reconnaissance Course (BRC) References -
Over 5,300 total pages .... MARINE RECON Reconnaissance units are the commander’s eyes and ears on the battlefield. They are task organized as a highly trained six man team capable of conducting specific missions behind enemy lines. Employed as part of the Marine Air-Ground Task Force, reconnaissance teams provide timely information to the supported commander to shape and influence the battlefield. The varying types of missions a Reconnaissance team conduct depends on how deep in the battle space they are operating. Division Reconnaissance units support the close and distant battlespace, while Force Reconnaissance units conduct deep reconnaissance in support of a landing force. Common missions include, but are not limited to: Plan, coordinate, and conduct amphibious-ground reconnaissance and surveillance to observe, identify, and report enemy activity, and collect other information of military significance. Conduct specialized surveying to include: underwater reconnaissance and/or demolitions, beach permeability and topography, routes, bridges, structures, urban/rural areas, helicopter landing zones (LZ), parachute drop zones (DZ), aircraft forward operating sites, and mechanized reconnaissance missions. When properly task organized with other forces, equipment or personnel, assist in specialized engineer, radio, and other special reconnaissance missions. Infiltrate mission areas by necessary means to include: surface, subsurface and airborne operations. Conduct Initial Terminal Guidance (ITG) for helicopters, landing craft, parachutists, air-delivery, and re-supply. Designate and engage selected targets with organic weapons and force fires to support battlespace shaping. This includes designation and terminal guidance of precision-guided munitions. Conduct post-strike reconnaissance to determine and report battle damage assessment on a specified target or

area. Conduct limited scale raids and ambushes. Just a SAMPLE of the included publications: BASIC RECONNAISSANCE COURSE PREPARATION GUIDE RECONNAISSANCE (RECON) TRAINING AND READINESS (T&R) MANUAL RECONNAISSANCE REPORTS GUIDE GROUND RECONNAISSANCE OPERATIONS GROUND COMBAT OPERATIONS Supporting Arms Observer, Spotter and Controller DEEP AIR SUPPORT SCOUTING AND PATROLLING Civil Affairs Tactics, Techniques, and Procedures MAGTF Intelligence Production and Analysis Counterintelligence Close Air Support Military Operations on Urbanized Terrain (MOUT) Convoy Operations Handbook TRAINING SUPPORT PACKAGE FOR: CONVOY SURVIVABILITY Convoy Operations Battle Book Tactics, Techniques, and Procedures for Training, Planning and Executing Convoy Operations Urban Attacks

Automating Open Source Intelligence - Robert Layton 2015-11-15

Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data

Digital Pursuit IV. - Attila Kokenyesi-Bartos 2022-02-21

The exact operation of the internet and our digital devices is a mystery to many, even though we use it every day. We run into technical problems that we often cannot solve on our own. When we become a victim of crime, we feel even more vulnerable in this virtual space. Digital crooks can’t wait to take advantage of the unpreparedness of others. They take the opportunity to obtain our confidential information and assets as soon as they can. The security of our own data and assets, the data we handle in the course of our work and that of our workplace comes under risk every time we connect to the internet. Many of us will sooner or later meet the first digital fraudsters, blackmailers, and bullies. What can we do to prevent our beautiful new digital world becoming a nightmare? This publication seeks to provide an answer to this. As a legal practicioner, the author has encountered several similar crimes, describing from his experience what happens in a real criminal investigation when digital data needs to be found. We examine in detail the tools and methods that members of the investigating authorities also work with on a regular basis. We analyze one by one the solutions that can be used to do this to understand how is it possible, which we considered to be impossible: identifying the unknown, faceless digital crooks based on the digital traces they have left behind. Our publication starts from the basics and helps you learn in a simple, fun way everything that benefits anyone who cares about their own digital security. We also provide knowledge that is a good starting point for future experts who wish to familiarize themselves with the world of cybercriminals more seriously due of their occupation and studies.

Open Source Intelligence Methods and Tools - Nihad A. Hassan 2018-06-30

Apply Open Source Intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support your intelligence analysis. Use the harvested data in different scenarios such as financial, crime, and terrorism investigations as well as performing

business competition analysis and acquiring intelligence about individuals and other entities. This book will also improve your skills to acquire information online from both the regular Internet as well as the hidden web through its two sub-layers: the deep web and the dark web. The author includes many OSINT resources that can be used by intelligence agencies as well as by enterprises to monitor trends on a global level, identify risks, and gather competitor intelligence so more effective decisions can be made. You will discover techniques, methods, and tools that are equally used by hackers and penetration testers to gather intelligence about a specific target online. And you will be aware of how OSINT resources can be used in conducting social engineering attacks. Open Source Intelligence Methods and Tools takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your searching activities without revealing your identity. What You'll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the Internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises

Open Source Intelligence Techniques - Michael Bazzell 2016-03-12
Fifth Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details

Digital Witness - Sam Dubberley 2020
This book covers the developing field of open source research and discusses how to use social media, satellite imagery, big data analytics, and user-generated content to strengthen human rights research and investigations. The topics are presented in an accessible format through extensive use of images and data visualization (éditeur).

Insights on Peace and Conflict Reporting - Kristin Skare Orgeret

2021-07-26

As the second book in the Routledge Journalism Insights series, this edited collection explores the possibilities and challenges involved in contemporary reporting of peace and conflict. Featuring 16 expert contributing authors, the collection maps the field of peace and conflict reporting in a digital world, in a context where the financial prospects of the news industry are challenged and professional authority, credibility and autonomy are decaying. The contributors, ranging from prominent scholars to the Head of Newsgathering at the BBC, discuss a diverse range of key case studies, including the role of Bellingcat in conflict journalism; war and peace journalism in Bangladesh; visual storytelling in conflict zones; and rampant cyber-misogyny confronting women journalists in Finland, India, the Philippines and South Africa. Bringing together theory and practice, the collection offers an in-depth examination of the changes taking place in the working practices of journalists as ongoing, strategic assaults against them increase. Insights on Peace and Conflict Reporting is a powerful resource for students and academics in the fields of global journalism, foreign news reporting, conflict reporting, globalisation, media and international communication.

Open Source Intelligence Techniques - Michael Bazzell 2016

This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content, Cell Phone Owner Information, Twitter GPS & Account Data, Hidden Photo GPS & Metadata, Deleted Websites & Posts, Website Owner Information, Alias Social Network Profiles, Additional User Accounts, Sensitive Documents & Photos, Live Streaming Social Content, IP Addresses of Users, Newspaper Archives & Scans, Social Content by Location, Private Email Addresses, Historical Satellite Imagery, Duplicate Copies of Photos, Local Personal Radio Frequencies, Compromised Email Information, Wireless Routers by Location, Hidden Mapping Applications, Complete Facebook Data, Free Investigative Software, Alternative Search Engines, Stolen Items for Sale, Unlisted Addresses, Unlisted Phone Numbers, Public Government Records, Document Metadata, Rental Vehicle Contracts, Online Criminal Activity.

Deep Dive - Rae L. Baker 2023-05-09

Learn to gather and analyze publicly available data for your intelligence needs In Deep Dive: Exploring the Real-world Value of Open Source Intelligence, veteran open-source intelligence analyst Rae Baker explains how to use publicly available data to advance your investigative OSINT skills and how your adversaries are most likely to use publicly accessible data against you. The author delivers an authoritative introduction to the tradecraft utilized by open-source intelligence gathering specialists while offering real-life cases that highlight and underline the data collection and analysis processes and strategies you can implement immediately while hunting for open-source info. In addition to a wide breadth of essential OSINT subjects, you'll also find detailed discussions on ethics, traditional OSINT topics like subject intelligence, organizational intelligence, image analysis, and more niche topics like maritime and IOT. The book includes: Practical tips for new and intermediate analysts looking for concrete intelligence-gathering strategies Methods for data analysis and collection relevant to today's dynamic intelligence environment Tools for protecting your own data and information against bad actors and potential adversaries An essential resource for new intelligence analysts, Deep Dive: Exploring the Real-world Value of Open Source Intelligence is also a must-read for early-career and intermediate analysts, as well as intelligence teams seeking to improve the skills of their newest team members.

Open Source Intelligence Tools and Resources Handbook - i-intelligence 2019-08-17

2018 version of the OSINT Tools and Resources Handbook. This version is almost three times the size of the last public release in 2016. It reflects

the changing intelligence needs of our clients in both the public and private sector, as well as the many areas we have been active in over the past two years.

International Conference on Cyber Security, Privacy and Networking (ICSPN 2022) - Nadia Nedjah 2023-02-20

This book covers selected high-quality research papers presented in the International Conference on Cyber Security, Privacy and Networking (ICSPN 2022), organized during September 09–11, 2022, in Thailand in online mode. The objective of ICSPN 2022 is to provide a premier international platform for deliberations on strategies, recent trends, innovative approaches, discussions and presentations on the most recent cyber security, privacy and networking challenges and developments from the perspective of providing security awareness and its best practices for the real world. Moreover, the motivation to organize this conference is to promote research by sharing innovative ideas among all levels of the scientific community and to provide opportunities to develop creative solutions to various security, privacy and networking problems.

Open Source Intelligence Methods and Tools - Nihad A. Hassan 2018-07-01

Apply Open Source Intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support your intelligence analysis. Use the harvested data in different scenarios such as financial, crime, and terrorism investigations as well as performing business competition analysis and acquiring intelligence about individuals and other entities. This book will also improve your skills to acquire information online from both the regular Internet as well as the hidden web through its two sub-layers: the deep web and the dark web. The author includes many OSINT resources that can be used by intelligence agencies as well as by enterprises to monitor trends on a global level, identify risks, and gather competitor intelligence so more effective decisions can be made. You will discover techniques, methods, and tools that are equally used by hackers and penetration testers to gather intelligence about a specific target online. And you will be aware of how OSINT resources can be used in conducting social engineering attacks. Open Source Intelligence Methods and Tools takes a practical approach and lists hundreds of OSINT resources that can be used to gather intelligence from online public sources. The book also covers how to anonymize your digital identity online so you can conduct your searching activities without revealing your identity. What You'll Learn Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making in your organization Use OSINT resources to protect individuals and enterprises by discovering data that is online, exposed, and sensitive and hide the data before it is revealed by outside attackers Gather corporate intelligence about business competitors and predict future market directions Conduct advanced searches to gather intelligence from social media sites such as Facebook and Twitter Understand the different layers that make up the Internet and how to search within the invisible web which contains both the deep and the dark webs Who This Book Is For Penetration testers, digital forensics investigators, intelligence services, military, law enforcement, UN agencies, and for-profit/non-profit enterprises

Open Source Intelligence Investigation - Babak Akhgar 2017-01-01

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 thorough, first-hand knowledge from serving experts in the field.

Gray Hat Python - Justin Seitz 2009-04-15

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Open Source Intelligence in the Twenty-First Century - C. Hobbs 2014-05-09

This edited book provides an insight into the new approaches, challenges and opportunities that characterise open source intelligence (OSINT) at the beginning of the twenty-first century. It does so by considering the impacts of OSINT on three important contemporary security issues: nuclear proliferation, humanitarian crises and terrorism.

Cybersecurity Threats with New Perspectives - Muhammad Sarfraz 2021-12-08

Cybersecurity is an active and important area of study, practice, and research today. It spans various fields including cyber terrorism, cyber warfare, electronic civil disobedience, governance and security, hacking and hacktivism, information management and security, internet and controls, law enforcement, national security, privacy, protection of society and the rights of the individual, social engineering, terrorism, and more. This book compiles original and innovative findings on issues relating to cybersecurity and threats. This comprehensive reference explores the developments, methods, approaches, and surveys of cyber threats and security in a wide variety of fields and endeavors. It specifically focuses on cyber threats, cyberattacks, cyber techniques, artificial intelligence, cyber threat actors, and other related cyber issues. The book provides researchers, practitioners, academicians, military professionals, government officials, and other industry professionals with an in-depth discussion of the state-of-the-art advances in the field of cybersecurity.

Introduction to Intelligence Studies - Carl J. Jensen, III 2022-09-15

Introduction to Intelligence Studies (third edition) provides an overview of the US intelligence community, to include its history, organization, and function. Since the attacks of 9/11, the United States Intelligence Community (IC) has undergone an extensive overhaul. This textbook provides a comprehensive overview of intelligence and security issues, defining critical terms and reviewing the history of intelligence as practiced in the United States. Designed in a practical sequence, the book begins with the basics of intelligence, progresses through its history, describes best practices, and explores the way the intelligence community looks and operates today. The authors examine the "pillars" of the American intelligence system—collection, analysis, counterintelligence, and covert operations—and demonstrate how these work together to provide "decision advantage." The book offers equal treatment to the functions of the intelligence world—balancing coverage on intelligence collection, counterintelligence, information management, critical thinking, and decision-making. It also covers such vital issues as laws and ethics, writing and briefing for the intelligence community, and the emerging threats and challenges that intelligence professionals will face in the future. This revised and updated third edition addresses issues such as the growing influence of Russia and China, the recent history of

the Trump and Biden administrations and the IC, and the growing importance of the cyber world in the intelligence enterprise. This book will be essential reading for students of intelligence studies, US national security, foreign policy and International Relations in general.

Extreme Privacy - Michael Bazzell 2019

"This textbook is PROACTIVE. It is about starting over. It is the complete guide that I would give to any new client in an extreme situation. It leaves nothing out and provides explicit details of every step I take to make someone completely disappear, including document templates and a chronological order of events. The information shared in this book is based on real experiences with my actual clients, and is unlike any content ever released in my other books. " -- publisher.

Digital Transformation in Policing: The Promise, Perils and Solutions - Reza Montasari 2023-01-02

This book shares essential insights into how the social sciences and technology could foster new advances in managing the complexity inherent to the criminal and digital policing landscape. Said landscape is both dynamic and intricate, emanating as it does from crimes that are both persistent and transnational. Globalization, human and drug trafficking, cybercrime, terrorism, and other forms of transnational crime can have significant impacts on societies around the world. This necessitates a reassessment of what crime, national security and policing mean. Recent global events such as human and drug trafficking, the COVID-19 pandemic, violent protests, cyber threats and terrorist activities underscore the vulnerabilities of our current security and digital policing posture. This book presents concepts, theories and digital policing applications, offering a comprehensive analysis of current and emerging trends in digital policing. Pursuing an evidence-based approach, it offers an extraordinarily perceptive and detailed view of issues and solutions regarding the crime and digital policing landscape. To this end, it highlights current technological and methodological solutions as well as advances concerning integrated computational and analytical solutions deployed in digital policing. It also provides a comprehensive analysis of the technical, ethical, legal, privacy and civil liberty challenges stemming from the aforementioned advances in the field of digital policing; and accordingly, offers detailed recommendations supporting the design and implementation of best practices including technical, ethical and legal approaches when conducting digital policing. The research gathered here fits well into the larger body of work on various aspects of AI, cybersecurity, national security, digital forensics, cyberterrorism, ethics, human rights, cybercrime and law. It provides a valuable reference for law enforcement, policymakers, cybersecurity experts, digital forensic practitioners, researchers, graduates and advanced undergraduates, and other stakeholders with an interest in counter-terrorism. In addition to this target audience, it offers a valuable tool for lawyers, criminologist and technology enthusiasts.

Cyber Crime Investigator's Field Guide - Bruce Middleton 2022-06-24

Transhumanism, Artificial Intelligence, the Cloud, Robotics, Electromagnetic Fields, Intelligence Communities, Rail Transportation, Open-Source Intelligence (OSINT)—all this and more is discussed in Cyber Crime Investigator’s Field Guide, Third Edition. Many excellent hardware and software products exist to protect our data communications systems, but security threats dictate that they must be all the more enhanced to protect our electronic environment. Many laws, rules, and regulations have been implemented over the past few decades that have provided our law enforcement community and legal system with the teeth needed to take a bite out of cybercrime. But there is still a major need for individuals and professionals who know how to investigate computer network security incidents and can bring them to a proper resolution. Organizations demand experts with both investigative talents and a technical knowledge of how cyberspace really works. The third edition provides the investigative framework that needs to be followed, along with information about how cyberspace works and the tools that reveal the who, where, what, when, why, and how in the investigation of cybercrime. Features New focus area on rail transportation, OSINT, medical devices, and transhumanism / robotics Evidence collection and analysis tools Covers what to do from the time you receive "the call," arrival on site, chain of custody, and more This book offers a valuable

Q&A by subject area, an extensive overview of recommended reference materials, and a detailed case study. Appendices highlight attack signatures, Linux commands, Cisco firewall commands, port numbers, and more.

ICCWS 2020 15th International Conference on Cyber Warfare and Security - Prof. Brian K. Payne 2020-03-12

Automating Open Source Intelligence - Robert Layton 2015-12-03 Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data

Open Source Intelligence Techniques - Michael Bazzell 2018-01-26 Completely Rewritten Sixth Edition Sheds New Light on Open Source Intelligence Collection and Analysis Author Michael Bazzell has been well known in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout twenty-five chapters of specialized websites, software solutions, and creative search techniques. Over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will greatly improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network Content Cell Phone Subscriber Information Deleted Websites & Posts Missing Facebook Profile Data Full Twitter Account Data Alias Social Network Profiles Free Investigative Software Useful Browser Extensions Alternative Search Engine Results Website Owner Information Photo GPS & Metadata Live Streaming Social Content Social Content by Location IP Addresses of Users Additional User Accounts Sensitive Documents & Photos Private Email Addresses Duplicate Video Posts Mobile App Network Data Unlisted Addresses &#s Public Government Records Document Metadata Rental Vehicle Contracts Online Criminal Activity Personal Radio Communications Compromised Email Information Automated Collection Solutions Linux Investigative Programs Dark Web Content (Tor) Restricted YouTube Content Hidden Website Details Vehicle Registration Details

Open Source Intelligence Techniques - Michael Bazzell 2016-04-07 Fifth Edition Sheds New Light on Open Source Intelligence Collection and Analysis.Author Michael Bazzell has been well known and respected in government circles for his ability to locate personal information about any target through Open Source Intelligence (OSINT). In this book, he shares his methods in great detail. Each step of his process is explained throughout sixteen chapters of specialized websites, application

programming interfaces, and software solutions. Based on his live and online video training at IntelTechniques.com, over 250 resources are identified with narrative tutorials and screen captures. This book will serve as a reference guide for anyone that is responsible for the collection of online content. It is written in a hands-on style that encourages the reader to execute the tutorials as they go. The search techniques offered will inspire analysts to "think outside the box" when scouring the internet for personal information. Much of the content of this book has never been discussed in any publication. Always thinking like a hacker, the author has identified new ways to use various technologies for an unintended purpose. This book will improve anyone's online investigative skills. Among other techniques, you will learn how to locate: Hidden Social Network ContentCell Phone Subscriber InformationDeleted Websites & PostsMissing Facebook Profile DataFull Twitter Account DataAlias Social Network ProfilesFree Investigative SoftwareUseful Browser ExtensionsAlternative Search Engine ResultsWebsite Owner InformationPhoto GPS & MetadataLive Streaming Social ContentSocial Content by LocationIP Addresses of UsersAdditional User AccountsSensitive Documents & PhotosPrivate Email AddressesDuplicate Video PostsMobile App Network DataUnlisted Addresses & #sPublic Government RecordsDocument MetadataRental Vehicle ContractsOnline Criminal ActivityPersonal Radio CommunicationsCompromised Email InformationWireless Routers by LocationHidden Mapping ApplicationsDark Web Content (Tor)Restricted YouTube ContentHidden Website DetailsVehicle Registration Details

A Research Agenda for Terrorism Studies - Lara A. Frumkin 2023-02-14

Asking vital questions concerning the future directions of terrorism research, this topical Research Agenda dives into the current state, emerging methodologies and key trends of this emotive and controversial field.

The Tao of Open Source Intelligence - Stewart Bertram 2015-04-23

OSINT is a rapidly evolving approach to intelligence collection, and its wide application makes it a useful methodology for numerous practices, including within the criminal investigation community.The Tao of Open Source Intelligence is your guide to the cutting edge of this information collection capability.

Dark Web Investigation - Babak Akhgar 2021-01-19

This edited volume explores the fundamental aspects of the dark web, ranging from the technologies that power it, the cryptocurrencies that drive its markets, the criminalities it facilitates to the methods that investigators can employ to master it as a strand of open source intelligence. The book provides readers with detailed theoretical, technical and practical knowledge including the application of legal frameworks. With this it offers crucial insights for practitioners as well as academics into the multidisciplinary nature of dark web investigations for the identification and interception of illegal content and activities addressing both theoretical and practical issues.

The Private Investigator's Licensing Handbook - Michael Kissiah 2017-06-05

Think you might be interested in pursuing a career as a private investigator? Browse through the pages of this book to: - Learn about the services provided by private investigators- Learn about the typical work environment, career outlook and salary range.- Get the details on the basic licensing requirements for each states and where to find more information- Understand where to get the necessary training and education- Get ideas and suggestions for getting your business up and running- Find out how to join industry associations to help grow your networkIf you're already a private investigator, this book can help you to expand your services into other states. You can use it as a quick reference for getting licensed, expanding your credentials and establishing a referral network. Likewise, agencies can provide a copy to new employees to help guide them through the licensing and application process. In short, if you're ready to embark on your path to becoming a private investigator, then you've found the right place to start.

The Guide to Online Due Diligence Investigations - Cynthia Hetherington 2015

Just when you thought there was nothing new to learn, the author has created the most concise investigative guide to business intelligence and

the social media. This powerful resource contains useful insights and proven successful techniques the reader can apply immediately. Step-by-step examples coupled with proven strategies and a detailed practical approach all lead to achieving better results. Hetherington's methods appeal to and educate readers at all levels of expertise.

Web Intelligence: Research and Development - Ning Zhong 2003-06-30

This book constitutes the refereed proceedings of the First Asia-Pacific Conference on Web Intelligence, WI 2001, held in Maebashi City, Japan, in October 2001.The 28 revised full papers and 45 revised short papers presented were carefully reviewed and selected from 153 full-length paper submissions. Also included are an introductory survey and six invited presentations. The book offers topical sections on Web information systems environments and foundations, Web human-media engineering, Web information management, Web information retrieval, Web agents, Web mining and farming, and Web-based applications.

Illicit Enrichment - Andrew Dornbierer 2021-05-27

Illicit Enrichment by Andrew Dornbierer provides a comprehensive guide to illicit enrichment laws and their application to target unexplained wealth and recover proceeds of corruption and other crimes. The book covers both criminal and civil-based laws from around the world. Investigators, prosecutors, legislators and academics alike will benefit from the clear descriptions and practical guidance on different approaches to targeting unexplainable increases in wealth, how to establish cases in court, and common legal challenges to illicit enrichment laws. Features: Extensive analysis of jurisprudence and cases around the world Tables, flow charts and graphics explaining key concepts Discussion of common questions and challenges A collection of laws from 103 jurisdictions, also as an online database A step-by-step guide to financial investigation and source and application analysis to support illicit enrichment cases Illicit Enrichment was developed and published by the Basel Institute on Governance through its International Centre for Asset Recovery, with research support from the NYU School of Law

Hacking Web Intelligence - Sudhanshu Chauhan 2015-04-13

Open source intelligence (OSINT) and web reconnaissance are rich topics for infosec professionals looking for the best ways to sift through the abundance of information widely available online. In many cases, the first stage of any security assessment—that is, reconnaissance—is not given enough attention by security professionals, hackers, and penetration testers. Often, the information openly present is as critical as the confidential data. Hacking Web Intelligence shows you how to dig into the Web and uncover the information many don't even know exists. The book takes a holistic approach that is not only about using tools to find information online but also how to link all the information and transform it into presentable and actionable intelligence. You will also learn how to secure your information online to prevent it being discovered by these reconnaissance methods. Hacking Web Intelligence is an in-depth technical reference covering the methods and techniques you need to unearth open source information from the Internet and utilize it for the purpose of targeted attack during a security assessment. This book will introduce you to many new and leading-edge reconnaissance, information gathering, and open source intelligence methods and techniques, including metadata extraction tools, advanced search engines, advanced browsers, power searching methods, online anonymity tools such as TOR and i2p, OSINT tools such as Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, Social Network Analysis (SNA), Darkweb/Deepweb, data visualization, and much more. Provides a holistic approach to OSINT and Web recon, showing you how to fit all the data together into actionable intelligence Focuses on hands-on tools such as TOR, i2p, Maltego, Shodan, Creepy, SearchDiggity, Recon-ng, FOCA, EXIF, Metagoofil, MAT, and many more Covers key technical topics such as metadata searching, advanced browsers and power searching, online anonymity, Darkweb / Deepweb, Social Network Analysis (SNA), and how to manage, analyze, and visualize the data you gather Includes hands-on technical examples and case studies, as well as a Python chapter that shows you how to create your own information-gathering tools and modify existing APIs

Publications Combined: Studies In Open Source Intelligence (OSINT) And Information - 2019-03-23

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO

SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine's Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT): Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media: Valuable Tools in Today's Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS

Deep Dive - Rae L. Baker 2023-08-03

Practical Handbook for Professional Investigators, Third Edition - Rory J. McMahon, CLI, CFE 2013-06-18

An increase in fraud cases has escalated government accountability and corporate oversight, and media attention on cases ranging from missing persons to white-collar crime has increased the visibility of professional investigators. This has resulted in a great source of increased work for the profession. The third edition of Practical Handbook for Professional Investigators continues to supply an up-to-date, nuts-and-bolts learning tool for students and an everyday reference for investigative professionals at all levels. More relevant than ever, this edition adds two new chapters on death and terrorism investigations and several new sections, including: Insurance fraud, fire and arson investigation, and liability claims investigation Indicators of online marital infidelity Obtaining governmental records to locate people and sample reports for skip tracing Practical considerations for surveillance and procedures for interception of wire or oral communications Service of subpoenas for witnesses in federal courts Testifying in court—including witness and evidence preparation, trial tactics used by attorneys, and an investigator's rights as a witness The Rules of Professional Conduct Niche markets in the investigative industry Managing and marketing an investigative practice, running a paperless office, and customer retention An unparalleled guide to the ins and outs of private investigation, Practical Handbook for Professional Investigators, Third Edition belongs on the shelf of every professional and trainee. Rory McMahon appeared on Al Jazeera America to discuss his new investigation company, The Grafton Group.

Corporate Investigations, Corporate Justice and Public-Private Relations - Clarissa A. Meerts 2019-08-26

This book seeks to understand the investigation and settlement of employer/employee disputes within companies. It argues that there is effectively no democratic knowledge about, or control over, corporate security, due to companies' preference for private, out-of-court settlements when faced with norm violations raised by employees. This book fills the knowledge gap by providing an overview of the corporate security sector including legal frameworks and an analysis of the role and powers of private investigative services, inhouse security, forensic accountants and forensic legal investigators. It draws on close observation, case studies and interviews with practitioners in and around the industry. Corporate Investigations, Corporate Justice and Public-Private Relations also looks at public-private relationships in this sector to propose policy remedies applicable to all corporate security providers, regardless of the disparate professional backgrounds and skill-sets of their staff.

Black Hat Python - Justin Seitz 2014-12-21

When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen? In Black Hat Python, the latest from Justin Seitz (author of the best-selling Gray Hat Python), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You'll

learn how to: –Create a trojan command-and-control using GitHub –Detect sandboxing and automate common malware tasks, like keylogging and screenshotting –Escalate Windows privileges with creative process control –Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine –Extend the popular Burp Suite web-hacking tool –Abuse Windows COM automation to perform a man-in-the-browser attack –Exfiltrate data from a network most sneakily Insider techniques and creative challenges throughout show you how to extend the hacks and how to write your own exploits. When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in Black Hat Python. Uses Python 2

Practical Social Engineering - Joe Gray 2022-06-14

A guide to hacking the human element. Even the most advanced security teams can do little to defend against an employee clicking a malicious link, opening an email attachment, or revealing sensitive information in a phone call. Practical Social Engineering will help you better understand the techniques behind these social engineering attacks and how to thwart cyber criminals and malicious actors who use them to take advantage of human nature. Joe Gray, an award-winning expert on social engineering, shares case studies, best practices, open source intelligence (OSINT) tools, and templates for orchestrating and reporting attacks so companies can better protect themselves. He outlines creative techniques to trick users out of their credentials, such as leveraging Python scripts and editing HTML files to clone a legitimate website. Once you've succeeded in harvesting information about your targets with advanced OSINT methods, you'll discover how to defend your own organization from similar threats. You'll learn how to: Apply phishing techniques like spoofing, squatting, and standing up your own web server to avoid detection Use OSINT tools like Recon-ng, theHarvester, and Hunter Capture a target's information from social media Collect and report metrics about the success of your attack Implement technical controls and awareness programs to help defend against social engineering Fast-paced, hands-on, and ethically focused, Practical Social Engineering is a book every pentester can put to use immediately.