Open Source Intelligence Methods and Tools

A Practical Guide to Online Intelligence

Nihad A. Hassan
Rami Hijazi

Apress®

Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence

Nihad A. Hassan
New York, USA

Rami Hijazi
Mississauga, Ontario, Canada

ISBN-13 (pbk): 978-1-4842-3212-5
ISBN-13 (electronic): 978-1-4842-3213-2
https://doi.org/10.1007/978-1-4842-3213-2

Library of Congress Control Number: 2018948821

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484232125. For more detailed information, please visit www.apress.com/source-code.

Printed on acid-free paper

To my mom, Samiha, thank you for everything.
Without you, I'm nothing.

—Nihad A. Hassan

Table of Contents

About the Authors

Nihad A. Hassan is an independent information security consultant, digital forensics and cybersecurity expert, online blogger, and book author. He has been actively conducting research on different areas of information security for more than a decade and has developed numerous cybersecurity education courses and technical guides. He has completed several technical security consulting engagements involving security architectures, penetration testing, computer crime investigation, and cyber open source intelligence (OSINT). Nihad has authored four books and scores of information security articles for various global publications. He also enjoys being involved in security training, education, and motivation. His current work focuses on digital forensics, anti-forensics techniques, digital privacy, and cyber OSINT. He covers different information security topics and related matters on his security blog at www.DarknessGate.com and recently launched a dedicated site for open source intelligence resources at www.OSINT.link. Nihad has a bachelor's of science honors degree in computer science from the University of Greenwich in the United Kingdom.

Nihad can be followed on Twitter (@DarknessGate), and you can connect to him via LinkedIn at https://www.linkedin.com/in/darknessgate.

Rami Hijazi has a master's degree in information technology (information security) from the University of Liverpool. He currently works at MERICLER Inc., an education and corporate training firm in Toronto, Canada. Rami is an experienced IT professional who lectures on a wide array of topics, including object-oriented programming, Java, e-commerce, agile development, database design, and data handling analysis. Rami also works as information security consultant, where he is involved in designing encryption systems and wireless networks, detecting intrusions and tracking data breaches, and giving planning and development advice for IT departments concerning contingency planning.

About the Technical Reviewer

Reem Naddar has a bachelor's of science degree in mathematics from Dalhousie University and has been in the data analytics industry since 2006. She has substantial experience in designing and executing solutions that address complex business problems involving large-scale data warehousing, real-time analytics, software architecture, and reporting solutions. She employs leading-edge tools and techniques when implementing fast and efficient data acquisition including Big Data processing used by global practitioners.

Reem has worked for major corporations and chartered banks in Canada both as a contractor and as a permanent staff member. She is fond of open source intelligence (OSINT) projects where she adopts different frameworks and processes to capture, transform, analyze, and store terabytes of structured and unstructured data gathered from publicly available sources.

Acknowledgments

I start by thanking God for giving me the gift to write and convert my ideas into something useful. Without God's blessing, I would not be able to achieve anything.

I want to thank the ladies at Apress: Susan, Rita, and Laura. I was pleased to work with you again and very much appreciate your valuable feedback and encouragement.

Specifically, to book acquisitions editor Susan McDermott, thank you for believing in my book's idea and for your honest encouragement before and during the writing process. To book project editor Rita Fernando, you were very supportive during the writing process. You made authoring this book a joyful journey. To book development editor Laura Berendson, thank you very much for your diligent and professional work in producing this book.

I also want to thank all the Apress staff who worked behind the scenes to make this book possible and ready for launch. I hope you will continue your excellent work in creating highly valued computing books. Your work is greatly appreciated.

—Nihad A. Hassan

Introduction

Open Source Intelligence Methods and Tools focuses on building a deep understanding of how to exploit open source intelligence (OSINT) techniques, methods, and tools to acquire information from publicly available online sources to support intelligence analysis. The harvested data can be used in different scenarios such as financial, crime, and terrorism investigations as well as in more regular tasks such as analyzing business competitors, running background checks, and acquiring intelligence about individuals and other entities. This book will also improve your skills in acquiring information online from the surface web, the deep web, and the darknet.

Many estimates show that 90 percent of useful information acquired by intelligence services comes from public sources (in other words, OSINT sources). Social media sites open up numerous opportunities for investigations because of the vast amount of useful information located in one place. For example, you can get a great deal of personal information about any person worldwide by just checking their Facebook page. This book will show you how to conduct advanced social media investigations to access content believed to be private, use advanced search engines queries to return accurate results, search historical deleted versions of websites, track individuals online using public record databases and people-searching tools, locate information buried in the deep web, access and navigate the dark web, collect intelligence from the dark web, view multiple historic satellite images and street views of any location, search geolocation information within popular social media sites, and more. In short, you will learn how to use a plethora of techniques, tools, and free online services to gather intelligence about any target online.

OSINT-gathering activities should be conducted secretly to avoid revealing the searcher's identity. Therefore, this book will teach you how to conceal your digital identity and become anonymous online. You will learn how to exchange data secretly across hostile environments like the Internet and how to communicate with your peers privately and anonymously. You will also learn how to check your digital footprint and discover what kind of digital traces you are leaving behind and how to delete them.

Open Source Intelligence Methods and Tools is an indispensable guide for anyone responsible for collecting online content from public data, and it is a must-have reference for any casual Internet user who wants to dig deeper into the Internet to see what information it contains.

Target Audience

The following types of people will benefit from this book:

- Penetration testers
- Digital forensics investigators
- Intelligence services
- Military personnel
- Law enforcement
- UN agencies and nonprofit organizations
- For-profit enterprises
- Risk management professionals
- Journalists
- Academic researchers
- University students
- End users who want to learn how to exploit Internet resources effectively

What the Book Is Not

This book is not about the history of open source intelligence, and it does not discuss at length the legal issues of personal reconnaissance online. We will not talk about policies and regulations that govern different countries or business organizations. Although some of these issues are discussed briefly in Chapter 1, the main aim of this book is to create a guidebook to support all types of investigations. You can read the chapters in any order because each chapter is considered an isolated unit that discusses the chapter subject's comprehensively.

Summary of Contents

Here is a brief description of each chapter's contents:

- Chapter 1, "The Evolution of Open Source Intelligence": In this chapter, we introduce you to the term OSINT and explain how it has evolved over time. We introduce the different parties interested in exploiting publicly available data and the benefits gained from doing so. We include some technical information about online gathering techniques and the challenges involved, as well as the legal aspects when harvesting data from publicly available sources.
- Chapter 2, "Introduction To Online Threats and Countermeasures": In this chapter, we teach you everything you need to know to stay safe when going online. This knowledge is essential when conducting advanced searches online to avoid being tracked since using advanced search operators and other OSINT search techniques will attract attention online and make your connection a target for interception by different outside parties.
- Chapter 3, "The Underground Internet": This chapter is devoted to uncovering the secrets of the invisible web, which contains both the darknet and the deep web. This knowledge is essential as the underground net contains a wealth of valuable information that any cybersecurity professional should know how to access.
- Chapter 4, "Search Engine Techniques": In this chapter, we show you how to use advanced search techniques using typical search engines such as Google and Bing to find anything online. We also cover other specialized search engines for images, video, news, web directories, files, and FTP.
- Chapter 5, "Social Media Intelligence": In this chapter, we show you how to use a wide array of tools and techniques to gather intelligence about a specific person or entity from social media sites. For instance, using Facebook you can gather intelligence about people worldwide. Other major tech companies like Google and Microsoft own huge databases of information about their users. A great amount of information is published publicly on these sites, and this chapter

teaches you how to search for people, including their relationships, names, addresses, and communications (and interactions) with others on social sites, to formulate a complete profile about your target.

- Chapter 6, “People Search Engines and Public Records”: Here we list specific search engines and other public resources to search for people’s names and get details around them. You will learn to use different reverse search criteria to find people online such as birth records, mail addresses, résumés, dating websites, e-mails, phone numbers, previous breached usernames, and more. We also cover government resources such as vital records, tax records, criminal information, and other public sources you can use to gain intelligence about people and entities.
- Chapter 7, “Online Maps”: This chapter covers how to use Google Maps and other free geolocation services to investigate the geolocation information acquired about target people.
- Chapter 8, “Technical Footprinting”: This chapter covers how to gather technical information about a target website and network system in passive mode to support your OSINT intelligence.
- Chapter 9, “What’s Next?”: This chapter covers the OSINT process and its future trends.

Book Companion Website

In this book, we list hundreds of online services that help OSINT gatherers to collect and analyze information. We all know about the ever-changing nature of the Web, though; new sites launch and others close down daily, so some links might not work by the time you read this. To prevent this hassle and to avoid making part of this book useless after publishing it, we have created a dedicated website where we offer a digital list of all the links mentioned in this book in addition to many more resources that just wouldn’t fit in the printed version. We will do our best to keep this site updated and continually work to add new useful OSINT content that reflects improvements in the field. Dead links will get deleted or updated, so the content of this book will remain current for many years to come.

See `www.OSINT.link`.

Comments and Questions

To comment or ask technical questions about this book, send an e-mail to `nihad@protonmail.com`. For additional references about the subject, computer security tools, tutorials, and other related matters, check out the author's blog at `www.DarknessGate.com`.