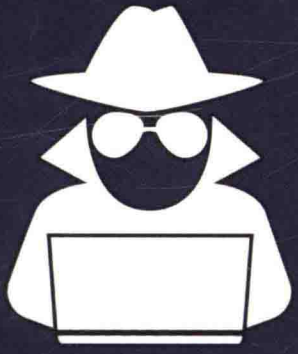
OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION

SIXTH EDITION



MICHAEL BAZZELL

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 *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, 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

Michael Bazzell spent 18 years as a government computer crime investigator. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on open source intelligence (OSINT) collection and analysis. He has trained thousands of individuals employed by state and federal agencies, as well as the private sector, in the use of his OSINT investigation techniques. He is also the author of *Hiding from the Internet*. His books are used by numerous government agencies as training manuals for intelligence gathering and proper securing of personal information.

$ 44.99 US
£ 29.99 UK
€ 37.99 EU

ISBN 9781984201577
90000 >
9 781984 201577

IntelTechniques.com

OPEN SOURCE INTELLIGENCE TECHNIC

ION

Open Source Intelligence Techniques

Resources for Searching and Analyzing Online Information

Sixth Edition

常州大学图书馆
藏书章

Michael Bazzell

Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information

Sixth Edition

Copyright © 2018 by Michael Bazzell

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the author.

Sixth Edition First Published: February, 2018

Project Editor: Y. Varallo

The information in this book is distributed on an "As Is" basis, without warranty. The author has taken great care in preparation of this book, but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Due to the use of quotation marks to identify specific text to be used as search queries and data entry, the author has chosen to display the British rule of punctuation outside of quotes. This ensures that the quoted content is accurate for replication. To maintain consistency, this format is continued throughout the entire book.

Library of Congress Cataloging-in-Publication Data:
Application submitted

ISBN-13: 978-1984201577

ISBN-10: 1984201573

试读结束：需要全本请在线购买： www.ertongbook.com

About the Author

Michael Bazzell

Michael Bazzell spent 18 years as a government computer crime investigator. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on open source intelligence, cyber-crime cases, and personal data removal methods. As an active investigator for multiple organizations, he has been involved in numerous high-tech criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and high-level computer intrusions. He has trained thousands of individuals in the use of his investigative techniques and privacy control strategies.

Michael currently works and resides in Washington, D.C. He also served as the technical advisor for the first season of the television hacker drama *Mr. Robot*. His books *Open Source Intelligence Techniques* and *Hiding from the Internet* have been best sellers in both the United States and Europe. They are used by several government agencies as training manuals for intelligence gathering and securing personal information.

INTRODUCTION

Sixth Edition

The previous (fifth) edition of this book was originally released in May of 2016. I assumed that it would be the final version, and stated in a few communication channels that it would be the last book I would write on the topic. In that book, I focused more on global techniques instead of specific resources in an attempt to get some extra mileage out of it. Since the first edition was released in 2012, I had been pushing out an updated version every year. The fifth edition seemed like the proper exit for the series. It was not because I was tired of online investigations. I may be more passionate now about collecting online evidence than I ever was before. I simply wanted to focus more energy toward other interests and opportunities, and I began spending a large amount of my time researching advanced privacy techniques.

In that down-time, I co-wrote *The Complete Privacy & Security Desk Reference,* and started a weekly podcast titled *The Complete Privacy & Security Podcast.* I also launched a new company dedicated to assisting other people in disappearing completely when bad situations arose. Whether conducting online data-mining removals for privacy; facilitating property purchases through the use of anonymous land trusts and LLCs for asset protection; or complete relocations to safe houses in the middle of the night for protection, it was a fascinating two years of research and execution.

In late 2017, I had the itch to begin writing about online research methods again. Earlier that year, I co-created a Linux virtual machine targeted toward research professionals that included numerous utilities never mentioned in my previous books. This pre-configured operating system gained a lot of public interest and we continue to update it twice yearly. Over the past two years, I updated my online research tools every month in order to continue to provide functional resources. I kept a running log of all of the changes that might need more explanation. In early 2018, I started documenting all of this, plus some of my favorite new Linux tools, in written form with anticipation of creating a supplement to the fifth edition of this book. Within a couple of weeks, I realized that the entire book should be re-written and released as a new edition. I have always self-imposed a "rule" in reference to my book revisions. The potential release must include at least 25% brand new material, 25% updated content, and 25% untouched stable and beneficial techniques. I believe that this sixth edition meets this criteria.

Keeping a book up to date about ways to access information on the internet is a difficult task. Websites are constantly changing or disappearing, and the techniques for collecting all possible public information from them are affected. While the fifth edition of this book is still highly applicable, a lot has changed over the past two years. Much of this book contains new techniques

that were previously not available. The Facebook Graph search options continue to grow considerably. I have also created several new online search tools to help with the investigative process. While Twitter and Instagram took away a few features, there is an abundance of new techniques available to all of us. Finally, a surge of Python tools has bombarded us with new capabilities never available before. It is a very exciting time for internet investigations.

The first chapter helps you properly configure your online investigation computer. It briefly discusses proper security protocols and free software. Great emphasis is placed on proper use of secure web browsers. A major change since the previous edition was the launch of Firefox version 57. In this update, all legacy add-ons were eliminated. If the add-ons were not upgraded to Firefox's new requirements, the tools no longer work. We lost some great resources, but this chapter will outline some new benefits.

A brand-new chapter explains the importance of virtual machines and instructs you on making your own or using a pre-configured option called Buscador. This virtual machine, co-created by David Westcott and myself, takes away the technical difficulties of installing custom Python applications, and leaves the user with a point-and-click environment ready for any type of investigation. Users of any skill level can now take advantage of Linux-based applications once restricted to those that understood programming and terminal prompts. With proper use of this system, you will no longer need to worry about viruses or malware. Dozens of applications, all included in Buscador, are explained in great detail in Chapter Two.

The remaining chapters are structured a bit differently from previous editions. Instead of trying to combine related topics into a single chapter, such as "Telephone Numbers & Addresses" or "Domains & IP Addresses", each category now has its own chapter. This allowed me to really delve into each topic and isolate the various techniques.

Fortunately, knowing methods for accessing data on one website often carries over nicely to other websites. This entire sixth edition was accurate as of February 2018. If, or more likely when, you find techniques that no longer work, use the overall lessons from the entire book to push through the changes and locate your content. Once you develop an understanding of the data, you will be ready to adapt with it. As always, I will publish updates to my online blog and free newsletter.

I will also post new video tutorials for the members of my online training program. You can access all of this, including my current investigation tools and links, on my website located at **IntelTechniques.com**. More importantly, please consider joining my free online forum at that address. This is where you will hear about all of the amazing OSINT techniques and methods that are being discovered every day from some of the brightest minds in online research. There are currently over 4,000 registered users, some of whom are active daily.

Open Source Intelligence (OSINT)

Open Source Intelligence, often referred to as OSINT, can mean many things to many people. Officially, it is defined as any intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. For the CIA, it may mean information obtained from foreign news broadcasts. For an attorney, it may mean data obtained from official government documents that are available to the public. For most people, it is publicly available content obtained from the internet.

What is this book?

Overall, this book includes several hundred sources of free and open data which could identify personal information about anyone. All of the resources are 100% free and open to the public. Each resource is explained, and any creative search techniques involving the resource are detailed. When applicable, actual case examples are provided to demonstrate the possibilities within the methods. The book can be read in any order and referenced when a specific need arises. It is a guidebook of techniques that I have found successful in my investigations.

Locating this free online information is not the final step of OSINT analysis. Appropriate collection methods will be detailed and referenced. Whether the data you obtain is for an investigation, a background check, or identifying problem employees, you must document all of your findings. You cannot rely on the information being available online forever. A website may shut down or the data may be removed. You must preserve anything of interest when you find it. The free software solutions presented here will help you with that.

OSINT search techniques do not apply only to websites. There are many free programs that automate the search and collection of data. These programs, as well as application programming interfaces, will be explained to assist the advanced investigator of open source intelligence.

In summary, this book is to serve as a reference guide to assist you with conducting more accurate and efficient searches of open source intelligence.

What the book is not...

This is not a debate about the ethics or politics of online reconnaissance for personal information. It is not a historical look at OSINT or a discussion of administrative policy. There are better books that tackle these subjects. Furthermore, it is not a how-to guide for criminals to steal your identity. Nothing in this book discusses illegal methods of obtaining information.

Book Audience

When I first considered documenting my OSINT techniques, the plan was to post them on my website in a private area for my co-workers. This documentation quickly turned into over 250 pages of content including screen shots. It had grown too big to place on my site in a manner that was easy to digest. I changed course and began putting together this book as a manual to accompany my multiple-day training sessions. I now hope that a wider investigation community can gain something from these techniques.

Many readers are in some form of law enforcement. Police officers can use these techniques to help locate missing children or investigate human trafficking. Intelligence analysts can apply these methods to a large part of their daily work as they tackle social media posts. Detectives can use the search techniques to re-investigate cases that have gone unsolved.

I now offer my online and live OSINT training to the private sector, especially global security divisions of large corporations. This book can help these teams locate more concise and appropriate information relative to their companies. These methods have been proven successful for employees that monitor any type of threat to their company, from physical violence to counterfeit products. I encourage the use of these techniques to institutions that are responsible for finding and eliminating "bad apples". This may be the human resources department, applicant processing employees, or "head hunters" looking for the best people. The information about a subject found online can provide more intelligence than any interview or reference check.

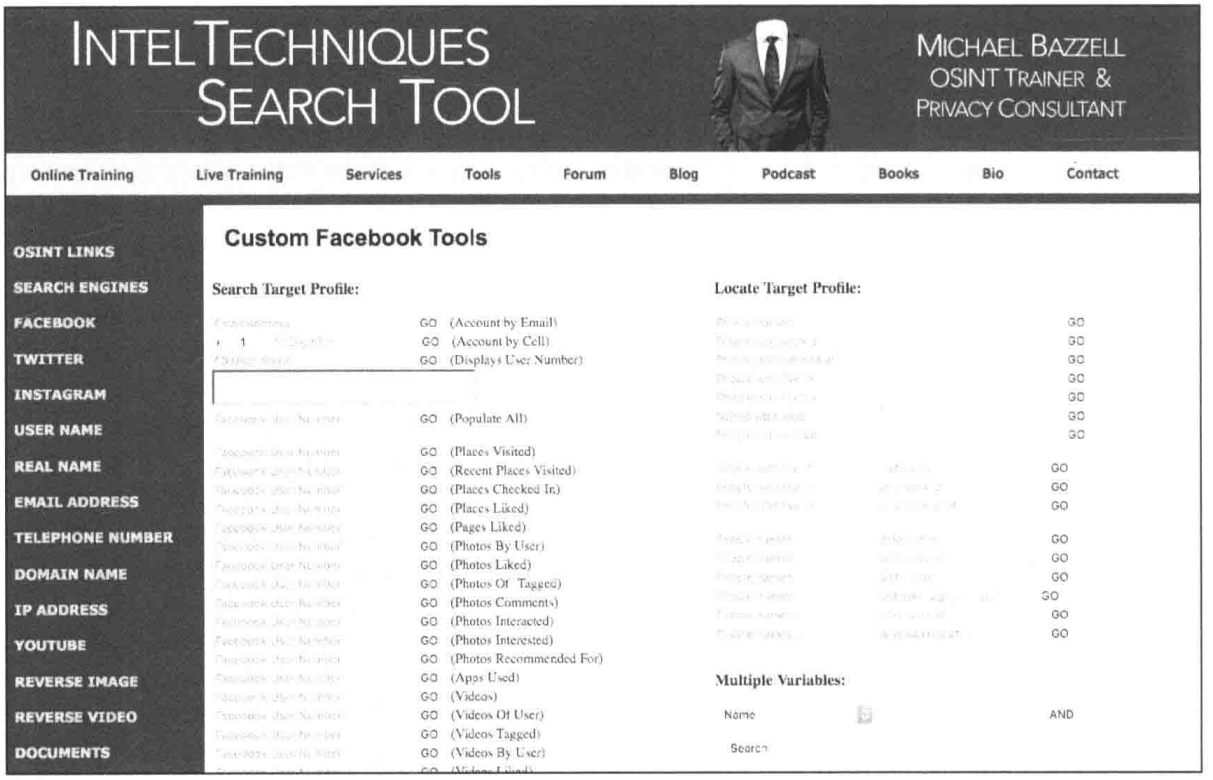
Parents and teachers are encouraged to use this book as a guide to locating social media content posted by children. In many households, the children know more about the internet than the adults. The children use this to their advantage and often hide content online. They know that it will not be located by their parents and teachers, and often post inappropriate content. This book can empower the adults and assist with identifying important personal information.

A large portion of my intended audience is private investigators. They can use this book to find information without possessing a deep understanding of computers or the internet. Explicit descriptions and occasional screen captures will ensure that the techniques can be recreated on any computer. Several universities have adopted this book as required reading, and I am honored to play a small role in some amazing courses related to network security.

I realize that people who use these techniques for devious purposes will read this book as well. Colleagues have expressed their concern about this possibility. My decision to document these techniques came down to two thoughts. First, anyone that really wants to use this information in malicious ways will do so without this book. There is nothing in here that could not be duplicated with some serious searching and time. The second thought is that getting this information out to those that will use it appropriately is worth the risk of a few people using it for the wrong reasons. Please act responsibly with this information.

Custom Search Tool

Throughout this book, I reference several custom search tools that I created to assist with automated queries. I have made available a single repository of every resource discussed in this guide, including the multiple custom search tools. This is presented in an easy to use format with search topics on the left and dedicated query tools within the main area. It can be found at the "Tools" tab of my website **IntelTechniques.com**. This complete archive may be useful as you complete the tutorials within this book. The image below displays the current state of the tool using the custom Facebook search options.



The IntelTechniques Custom Search Tools page.

Finally, a parting thought before you begin your journey through OSINT analysis and collection. This book was written as a reference guide. It does not need to be read straight-through. I encourage you to skip around when needed or if you feel overwhelmed. The second chapter about Linux may make you want to abandon the teachings before ever utilizing an online resource or website. When you encounter material that seems too technical or not applicable, please move on to the next topic. The book is suitable for all skill levels, and there is something here for everyone. You can always return to advanced topics later.

试读结束：需要全本请在线购买： www.ertongbook.com

CONTENTS

试读结束：需要全本请在线购买： www.ertongbook.com