OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION

SIXTH EDITION

MICHAEL BAZZELL

OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION

SIXTH EDITION

MICHAEL BAZZELL

OPEN SOURCE INTELLIGENCE TECHNIQUES:
RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION

Sixth Edition

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

CONTENTS

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.

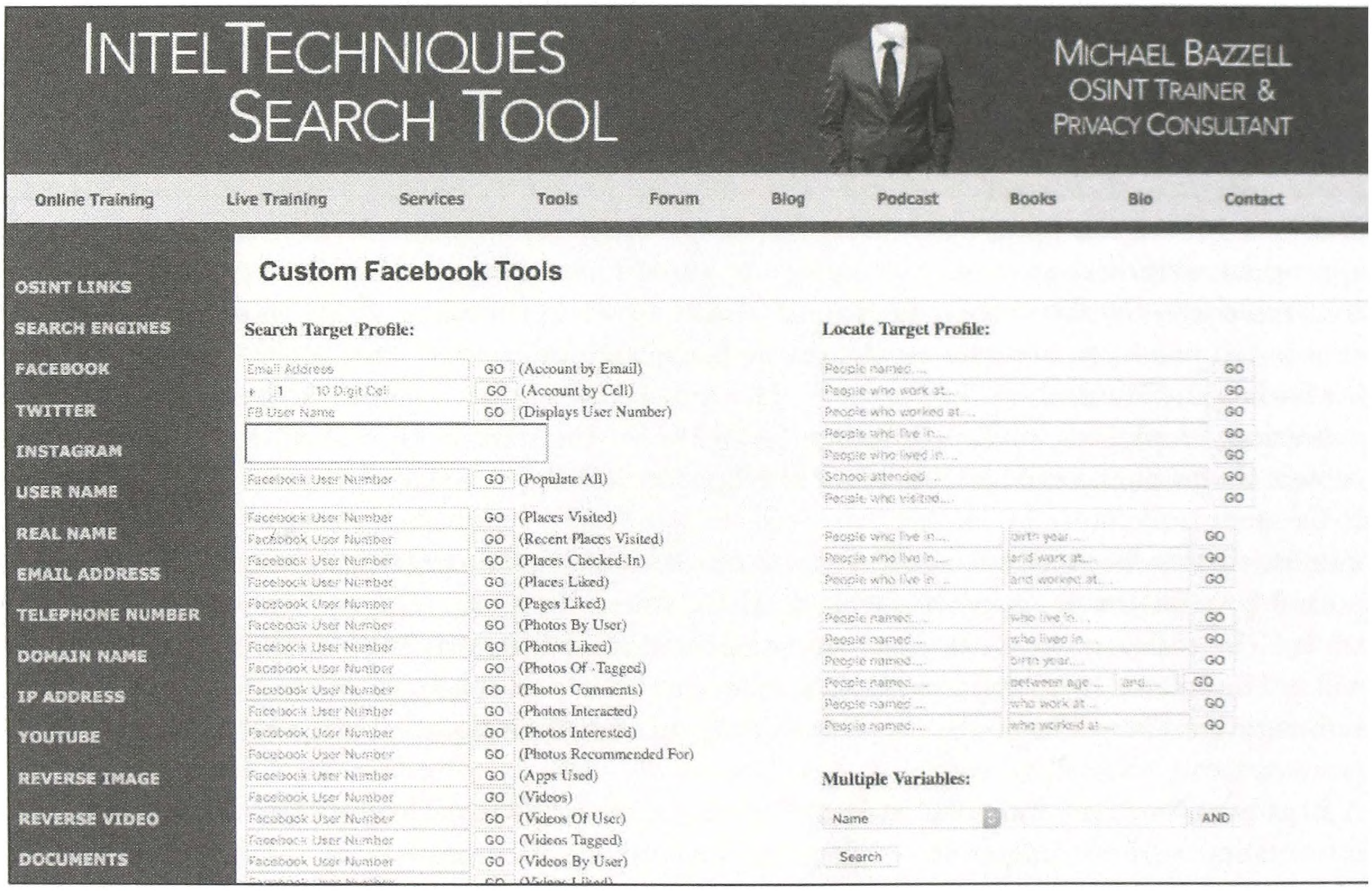
Parents and teachers are encouraged to use this book as a guide to locating social media content posted by children. In many households, the children know more about the internet than the adults. The children use this to their advantage and often hide content online. They know that it will not be located 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.


INTELTECHNIQUES SEARCH TOOL
MICHAEL BAZZELL OSINT TRAINER & PRIVACY CONSULTANT
Online Training
Live Training
Services
Tools
Forum
Blog
Podcast
Books
Bio
Contact
OSINT LINKS
SEARCH ENGINES
FACEBOOK
TWITTER
INSTAGRAM
USER NAME
REAL NAME
EMAIL ADDRESS
TELEPHONE NUMBER
DOMAIN NAME
IP ADDRESS
YOUTUBE
REVERSE IMAGE
REVERSE VIDEO
DOCUMENTS
Custom Facebook Tools
Search Target Profile:
Email Address GO (Account by Email)
+ 1 10 Digit Cell GO (Account by Cell)
FB User Name GO (Displays User Number)
Facebook User Number GO (Populate All)
Facebook User Number GO (Places Visited)
Facebook User Number GO (Recent Places Visited)
Facebook User Number GO (Places Checked-In)
Facebook User Number GO (Places Liked)
Facebook User Number GO (Pages Liked)
Facebook User Number GO (Photos By User)
Facebook User Number GO (Photos Liked)
Facebook User Number GO (Photos Of - Tagged)
Facebook User Number GO (Photos Comments)
Facebook User Number GO (Photos Interacted)
Facebook User Number GO (Photos Interested)
Facebook User Number GO (Photos Recommended For)
Facebook User Number GO (Apps Used)
Facebook User Number GO (Videos)
Facebook User Number GO (Videos Of User)
Facebook User Number GO (Videos Tagged)
Facebook User Number GO (Videos By User)
Locate Target Profile:
People named... GO
People who work at... GO
People who worked at... GO
People who live in... GO
People who lived in... GO
School attended... GO
People who visited... GO
People who live in... birth year... GO
People who live in... and work at... GO
People who live in... and worked at... GO
People named... who live in... GO
People named... who lived in... GO
People named... birth year... GO
People named... between age... and... GO
People named... who work at... GO
People named... who worked at... GO
Multiple Variables:
Name AND
Search

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.

CHAPTER ONE
PREPARE YOUR COMPUTER

The first four editions of this book began with search engine techniques. Right away, I offered my methods for collecting online information from various popular and lesser known search websites. This may have been due to my own impatience and desire to "jump in" and start finding information. This edition will begin much differently. Before you attempt any of the search methods within this book, I believe you should prepare your computing environment.

I was motivated to begin with this topic after teaching a multiple-day OSINT class. On day two, several attendees brought laptop computers in order to attempt the techniques I was teaching during the course. During a break, I observed police officers searching Facebook on patrol vehicle laptops; private investigators using Windows XP while browsing suspects' blogs; and global security professionals looking at hacker websites without possessing any antivirus software or script blockers.

I have also been guilty of all of this. Early in my career of researching OSINT, I did not pay any attention to computer security or proper browsing habits. While I was aware of malicious software, I knew I could re-install Windows if something really bad happened. This was reactive thinking. I believe that we must all proactively attack vulnerabilities in our privacy and security while conducting online research. This chapter is not meant to be a complete guide to computer security or a manual for total privacy. Instead, I hope to quickly and efficiently propose the most beneficial strategies that will protect you from the majority of attacks. Applying the changes mentioned in this chapter will provide a valuable layer of security to your online investigations and overall computing habits. In the next chapter, I present my solutions for guaranteed protection during online investigations.

The most basic place to start is your antivirus. It is likely that most readers already have an antivirus solution and are insulted at the mention of it in a book like this. I will keep my thoughts very brief. If you are using Microsoft Windows, you absolutely need antivirus software. If you are using an Apple computer, you might not. Antivirus applications only protect against known variants of viruses. They do not stop everything. A new virus can often bypass the best software detection solutions. A better defense is applying better browsing habits instead of relying on an application.

There are a dozen popular antivirus companies that will provide a free solution. For most Windows users, I simply recommend to use Microsoft's products. Users of Windows 7 should use Microsoft Security Essentials while Windows 8 and 10 users should use the default Windows Defender included with their installation. Privacy enthusiasts will disagree with this advice, and I understand their stance. Microsoft products tend to collect your computer usage history and analyze the data. Unfortunately, their core operating systems also do this, and it is difficult to disable long term. Therefore, I believe that Windows users are already disclosing sensitive information to Microsoft. Using their antivirus solutions will not likely enhance the data being collected.

Mac users do not have any built-in antivirus protection, and most do not need any. The software architecture of Mac computers is much more secure, and viruses are rare (but they do still occur). I no longer recommend the free commercial products such as Avast, Kaspersky, and others. They tend to be more of an annoyance than helpful, and their business practices can be questionable. However, I do believe that it is irresponsible to have absolutely no protection whatsoever. When I conduct investigations from a Mac computer, I possess an open-source antivirus solution called ClamAV.

ClamAV (not to be confused with the unnecessary paid option of ClamXAV), is a community-driven antivirus database, which is freely available to anyone. It usually does not score very high on "Top 10 Antivirus" websites, which are usually paid advertisements. However, it is completely free, does not run on your system non-stop, only executes when you desire, and can be completely removed easily. Unfortunately, there is no easy software installation process, and no point-and-click application. You will need to manually update the database through a Terminal command, then scan your system from the same prompt. ClamAV does not remove any viruses, it only discloses the presence and location of suspicious files. In my use, ClamAV has never found a virus that impacted a Mac computer. Instead, it has identified numerous malicious files that target Windows machines, but were present on my system (mostly as email attachments). This notification allowed me to manually remove those files, which could prevent future infection of my Windows virtual machines. If you have concerns about having a "naked" Mac with no antivirus, the following instructions will configure your Mac to be better protected.

First, you must install a package manager called Brew. This program is very beneficial when there is a need to install programs that would usually already be present on a Linux computer. It also happens to have a pre-configured version of ClamAV ready to go. The easiest way to install Brew is to visit the website brew.sh and copy and paste the following command into the Terminal application (Applications > Utilities > Terminal).

```
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

After Brew is installed, type the following commands, hitting "Return" after each line, into the same Terminal application used previously.

```
brew install clamav
cd /usr/local/etc/clamav/
cp freshclam.conf.sample freshclam.conf
sed -ie 's/^Example/#Example/g' freshclam.conf
```

These steps will install ClamAV, switch to the installation directory, make a copy of the configuration file, and then modify the configuration file to allow ClamAV to function. You are now ready to update your antivirus database and conduct a scan. Type the following commands into Terminal.

```
freshclam -v
clamscan -r -i /
```

The first option will download all virus definition updates, and should be executed before each scan. The second option conducts a scan of the entire computer, and will only prompt you with details of found viruses. While it may appear to be dormant, it is working, and will notify you upon completion. All of these commands must be exact. In order to assist with this, I have created a web page with all of these commands at IntelTechniques.com/clamav. On a final note about ClamAV, you may occasionally receive a false-positive report of a virus. Do not panic. Research the file on the internet and identify the issues. If you receive reports of malicious files within email, simply delete those messages. The use of ClamAV on Mac computers is more about preventing the spread of bad files to Windows users instead of protecting your own machine.

Whether on Windows or Mac computers, protection from malicious software, otherwise known as malware, is vital. Again, there are numerous free options from which to choose. I recommend Malware Bytes for both Windows and Apple users. It is completely free and thorough. I suggest executing, updating, and scanning at least once a week on every device that you use.

- Navigate to http://www.malwarebytes.org/ and select the "Free Download" option.
- Conduct a default installation.
- On a weekly basis, launch the program, update the database, and conduct a full scan.
- Malware Bytes will remove any issues it finds.

Your computer should also be cleaned weekly. As you browse the internet and use applications, unnecessary files accumulate and slow the operating system. I recommend CCleaner for all Windows and Apple users. It is free and easy to use. It provides a simple interface and is used to clean potentially unwanted files and invalid Windows Registry entries from your computer. The following steps will download and install the free version of the application.

- Navigate to http://www.piriform.com/ccleaner/download.
- In the "Free" column, click on "download".
- Execute the program and accept the default installation settings.

After the installation completes, launch the program. You have several options under the Cleaner tab that will allow you to choose the data to eliminate. The default options are safe, but I like to enable additional selections. Clicking on the "Analyze" button will allow the program to identify files to delete without committing to the removal. This will allow you to view the files before clicking "Run Cleaner" to remove them. If you are running this program on a computer with heavy internet usage, you may be surprised at the amount of unnecessary files present. The first time you use this program, the removal process can take several minutes and possibly an hour. If you run the program weekly, it will finish the process much quicker.

The Registry tab of CCleaner will eliminate unnecessary and missing registry entries. This can help your computer operate more efficiently. The default options on this menu are most appropriate. Click on "Scan for Issues" and allow it to identify any problems. This process should go quickly. When complete, click on "Fix Selected Issues" to complete the process.

The Tools tab provides an easy way to disable specific programs from launching when your computer starts. These programs can slow your computer down when they are running unnecessarily. These can be found by clicking the "Startup" button in the left column. I once selected the Adobe and Java programs and applied the "Disable" button. They were then marked as "No" and would not launch the next time my computer started. If I wanted to reverse this, I could select the entries again and choose "Enable".

Proper antivirus, malware protection, and cleaning solutions will greatly enhance your overall computing experience. It will help your computer to run smoothly and may prevent malicious files from infecting your operating system. It will help protect the integrity of any online investigations. I refer to these steps as the "staples". They are the minimum requirements before proceeding and apply to any computer user.

Those that want to conduct advanced searches on the internet must progress to another level. You must upgrade your web browser and stop relying on Microsoft's Internet Explorer or Edge browsers. I believe that you should only use one of two web browsers: Firefox or Chrome. Many of the techniques in this book, especially in the Application Programming Interfaces (APIs) chapter, will fail when used in conjunction with Microsoft's browsers. They require a more sophisticated solution with proper add-ons. I will focus on Firefox first, as it is my preferred browser for every investigation.

Many readers find that security restrictions on their computers prohibit them from installing any software, including web browsers. While I have found that downloading portable versions of Firefox and Chrome eliminate this restriction, my experience is that this action will upset the computer support personnel that originally enabled the rules. Please research your organization's computer use policies before placing any software on company owned machines.

Those in law enforcement should be more cautious than others. Not only could installing unauthorized software on a government computer violate internal policies, but it could also jeopardize your case in court. If a defense attorney can prove that you violated your own rules and regulations, regardless of how minor or inconsequential, it leaves an opening to request a judge to dismiss your entire findings. Please make sure that you always have the proper authorization to conduct any techniques mentioned in this book.