PLAINATLAS PUBLISHING — BEGINNER SERIES

Open-Source Intelligence for Beginners

How to Find Anyone Online —
and How to Stop Them From Finding You

SAMPLE PREVIEW — PAGES 1–10

REAL TOOLS · REAL TECHNIQUES · LEGAL & ETHICAL FRAMEWORK · PROTECT YOURSELF

100%
Techniques use only publicly available data

50+
Real tools and websites listed and explained

Free
Most tools in this book cost nothing

A practical, ethical guide to open-source investigation — real tools, real techniques, and a clear framework for finding information online and protecting yourself from the same methods.

OPEN-SOURCE INTELLIGENCE FOR BEGINNERS

What's Inside

ABOUT THIS BOOK

This book is written for readers who want a practical, honest introduction to Open Source Intelligence — commonly called **OSINT**. It is for curious individuals, journalists, researchers, HR professionals, security enthusiasts, and anyone who wants to understand how investigators find people and information using only publicly available data.

Every tool, technique, and website mentioned in this book is legal to use in most jurisdictions when applied to publicly available information. This book does not encourage harassment, stalking, doxxing, or any illegal use of the techniques described.

> **Important**
>
> This book is educational, not operational. Always verify the legal requirements in your jurisdiction before conducting any investigation. What is lawful in one country may not be lawful in another. When in doubt, consult a legal professional.

What You Will Get From This Book

- Real tools and websites — not vague descriptions, but actual URLs you can visit today
- Practical techniques used by journalists, investigators, and security researchers
- How to protect yourself from the same techniques being used against you
- A clear ethical and legal framework so you stay on the right side of the line
- A master tool reference, cheat sheets, and a reusable investigation checklist

HOW TO USE THIS GUIDE

You do not need to read this book from start to finish. Each chapter is designed to stand on its own. If you want to jump straight to finding people, start with Chapter 17. If you want to protect yourself first, start with Chapter 23. If you are new to OSINT entirely, the recommended path is

Chapters 1 through 5, then whatever topic interests you most.

> **Try It on Yourself First**
>
> The safest and most educational way to learn OSINT is to use every technique on yourself before trying it on anyone else. You will quickly discover how much of your own information is publicly available — and that discovery alone is worth the price of this book.

CHAPTER 1

What Is OSINT?

Definition, history, and what counts as an open source

Open Source Intelligence — **OSINT** — is the collection and analysis of information from publicly available sources to produce actionable intelligence. The word "open" does not mean easy or obvious. It means the sources are not secret, classified, or obtained through hacking. They are public — websites, social media, public records, news archives, academic papers, and anything else anyone can legally access.

The term originated in military and intelligence communities, where analysts distinguished between classified intelligence gathered through covert means and intelligence gathered from public sources. Today, OSINT has moved far beyond government use. Journalists use it to verify stories. HR departments use it to vet candidates. Cybersecurity teams use it to assess threats. Private investigators use it as their primary research method. And ordinary people use it every time they Google someone before a first date.

A Brief History

OSINT is not new. Intelligence agencies have monitored foreign newspapers, radio broadcasts, and public communications for over a century. The CIA's Foreign Broadcast Information Service, established in 1941, monitored overseas media for strategic intelligence. What changed was the internet — specifically, the explosion of publicly available digital information after the mid-1990s and the rise of social media after 2004.

Today, a single person with a laptop and internet connection can conduct research that would have required a team of analysts and weeks of work twenty years ago. The tools have democratized the discipline — and this book puts those tools in your hands.

What Counts as an Open Source?

- **Surface web content** — anything indexed by search engines
- **Social media profiles** — public posts, photos, connections, check-ins
- **Public records** — court filings, property records, business registrations
- **News archives** — historical and current journalism

- **Academic and professional publications** — research papers, LinkedIn profiles
- **Domain and IP registration data** — WHOIS records, DNS information
- **Government databases** — voter rolls, company filings, patent records
- **Data breaches** — leaked databases that became publicly available

Pro Tip

The most important OSINT skill is not knowing which tools to use. It is knowing how to think systematically — asking the right questions, verifying what you find, and recognizing when you have enough information.

CHAPTER 2

Who Uses OSINT and Why

From intelligence agencies to ordinary people

OSINT is one of the most widely used investigative disciplines in the world, and most people who use it do not call it by that name. Here is who is doing it, and why.

Journalists and Investigative Reporters

Modern investigative journalism relies heavily on OSINT. Reporters use it to verify sources, find contact information for witnesses, track the assets of public figures, identify the origin of photos in conflict zones, and reconstruct timelines from social media. Organizations like **Bellingcat** have built their entire reputation on open-source investigation — their work identifying the perpetrators of the MH17 shootdown and the Salisbury poisoners used almost entirely public data.

Law Enforcement and Government Agencies

Police departments, federal agencies, and intelligence organizations use OSINT extensively — both for investigations and for monitoring public sentiment. Many law enforcement OSINT operations involve monitoring public social media, tracking criminal networks through open forums, and using public records to build profiles of suspects.

Cybersecurity Professionals

Security teams use OSINT to understand their own attack surface — what information about their organization is publicly available that an attacker could exploit. This is called **reconnaissance** or **red teaming**. They also monitor dark web forums and breach databases for leaked credentials belonging to their employees.

HR and Background Screening

Employers routinely search candidates online before interviews and after offers. While formal background checks are regulated, public social media searches are not. This is one of the most common everyday uses of OSINT and one most people do not think about when they post online.

Private Investigators

Licensed private investigators have largely shifted their primary research method to OSINT. Physical surveillance is expensive and time-consuming. A social media profile, location check-in, or public court record can answer the same question in minutes from a desk.

Ordinary People

People use informal OSINT constantly — searching a date's name before meeting them, looking up a landlord before signing a lease, verifying whether a charity is legitimate before donating, or checking whether a business has complaints. The techniques in this book are a more systematic version of what people already do intuitively.

> **The Core Point**
>
> OSINT is not a niche skill used only by spies and hackers. It is a systematic approach to public research that anyone can learn — and that most people already use informally without realizing it has a name.

SAMPLE ENDS HERE

The full guide continues with 15 more chapters.

The complete **Open-Source Intelligence for Beginners** covers every major OSINT technique with real tools, real URLs, and practical step-by-step guidance — including how to investigate people, domains, and companies, how to recover deleted content, and a full chapter on protecting yourself from the same techniques.

- ✓ 50+ real tools and websites — all listed with direct URLs
- ✓ Chapter 5: Google Dorking — advanced search operators with examples
- ✓ Chapter 6: Social media intelligence, platform by platform
- ✓ Chapter 7: Reverse image search engines including facial recognition tools
- ✓ Chapter 8: Username lookup tools + check if your email is in a breach
- ✓ Chapter 9: Phone number lookups + opt-out table for 10 major people-finder sites
- ✓ Chapter 10: WHOIS lookup sites, DNS records, certificate transparency
- ✓ Chapter 12: The Wayback Machine and recovering deleted content
- ✓ Chapter 17: Step-by-step guide to investigating a person
- ✓ Chapter 23: How to protect yourself — opt-out services and monitoring tools
- ✓ Appendix B: Google Dork cheat sheet — 12 ready-to-use search strings
- ✓ Appendix C: Full investigation checklist — printable and reusable
- ✓ Appendix D: Complete OSINT glossary

Get the Full Book

www.plainatlas.com

PlainAtlas Publishing · plainatlas.com