

Introduction to OSINT

Nipun Negi

17th March , 2024

What is OSINT?

OSINT is a phrase you'll hear about in the cybersecurity community. It's an essential skill and methodology for researchers and defensive security professionals. So what is it?

Introduction to OSINT

- Open Source Intelligence (OSINT) is the practice of collecting and analyzing information from publicly available sources to gather insights and make informed decisions.
- Using various tools and techniques, OSINT plays a crucial role in cybersecurity, threat intelligence, and investigative work by uncovering valuable data from the open web.
- These sources may include social media, websites, public records, and more. OSINT is crucial for understanding and assessing security threats, as well as gathering valuable insights for various investigative purposes.

Why do people do OSINT?

Here are some of the reasons why people engage in OSINT:

- To learn about employers or job applicants before hiring
- To learn about people before dating or making friends with them
- To make consumer or corporate purchasing decisions
- To engage in many different areas of academic work
- To learn about cybercriminal activity
- To learn about specific cyber threats
- To conduct old-fashioned criminal investigation for law enforcement
- To find missing people or lost family members
- To plan holidays or business trips
- To facilitate pentesting, to gather information on your pentesting target

And the list goes on and on.

OSINT in action

- Tracking cyber threats
- Social media analysis
- Geospatial Analysis

Gathering information from open sources

Public Records

- Accessing public records to gather information on individuals, businesses, and properties.
- Examples: Property deeds, court filings, business licenses.

Social Media

- Utilizing social media platforms to monitor public posts, interactions, and user-generated content.
- Considerations: Geo-tagged posts, user profiles, connection networks.

Online Forums and Communities

- Engaging with online communities to gather insights, discussions, and opinions on specific topics or events.
- Considerations: Forums, Q&A websites, interest-based communities.

Importance of OSINT in security

Early Threat Detection

- OSINT allows for the early detection of potential security threats by monitoring public information.

Risk Assessment

- It plays a crucial role in conducting comprehensive risk assessments to identify vulnerabilities and potential attacks.

Reputation Management

- Helps in monitoring online reputation and identifying any potential reputational risks or security breaches.

Competitive Analysis

- Use in understanding the competitive landscape and potential risks posed by competitors in the cyber domain.

Best Practices for Using OSINT

Data Collection

- Ensure data gathered is legal and ethical

Source Verification

- Confirm the credibility and authenticity of information sources

Data Analysis

- Thoroughly

Why is OSINT important?

- **Investigations:** OSINT is crucial for investigations by law enforcement, intelligence agencies, and private organizations. It helps uncover hidden connections, track individuals, and identify potential threats.
- **Threat Assessment :** OSINT assists in assessing risks, monitoring online activities, and understanding the intentions of individuals or groups.
- **Business Intelligence:** Companies use OSINT to gather competitive intelligence, analyze market trends, and make informed decisions.

Examples of OSINT Sources:

- **Social Media:** Profiles, posts, and interactions on platforms like Twitter, Facebook, LinkedIn, and Instagram.
- **Websites and Forums:** Extracting data from websites, forums, and blogs.
- **Public Records:** Court records, property records, business registrations, and government databases.
- **News Articles:** Analyzing news reports for relevant information.
- **Geospatial Data:** Maps, satellite imagery, and location-based data.

What isn't OSINT?

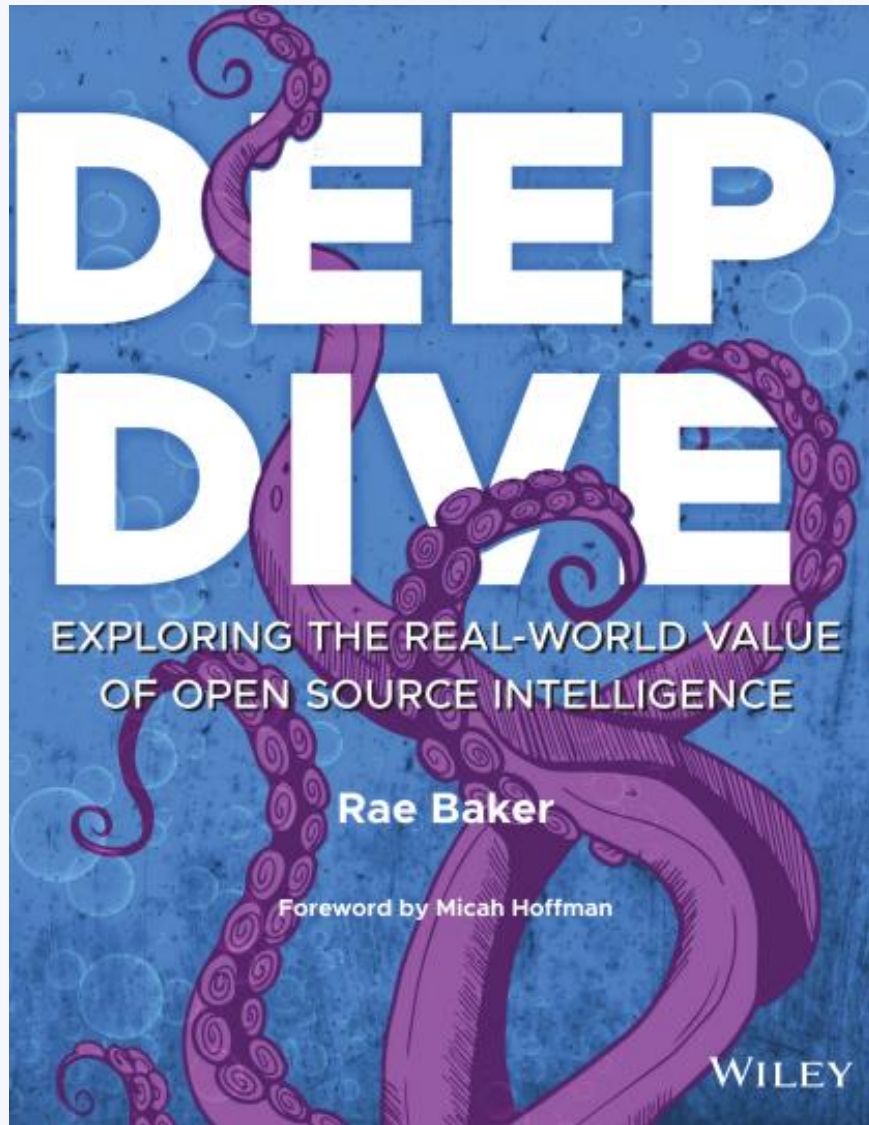
- OSINT is passive and lawful research. OSINT is based only on the passive gathering of information. So the moment you have to directly ask someone for information or initiate a scan that interacts with the target, that isn't OSINT. That's active research. And if your research requires breaking the law or otherwise accessing information you aren't permitted to access, that isn't OSINT either. Cyber attacks such as brute forcing and spyware usage, and any espionage conducted by civilians and without a police search warrant are both highly illegal pretty much everywhere in the world. That definitely isn't OSINT.

TOP OSINT TOOLS

- Maltego
- SpiderFoot
- Intelligence X
- Shodan
- OSINT Framework
- Metagoofil
- Lampyre
- Spokeo
- Recon-ng
- Mitaka
- Babel Street
- Seon
- ***Resource : <https://builtin.com/big-data/osint-tools> *****

- SANS Blog on OSINT

<https://www.sans.org/blog/what-is-open-source-intelligence/>



Book Recommended by
SANS for OSINT

Open-source information is content that can be found from various sources such as:

- Public Records
- News media
- Libraries
- Social media platforms
- Images, Videos
- Websites
- The Dark web



Public Records



Images/Videos



Websites



Social Media
Platforms



News Media



Libraries

- Government
- Law Enforcement
- Military
- Investigative journalists
- Human rights investigators
- Private Investigators
- Law firms
- Information Security
- Cyber Threat Intelligence
- Pen Testers
- Social Engineers



Government



Investigative Journalist



Law Firms



Private Investigators



Social Engineers



Military

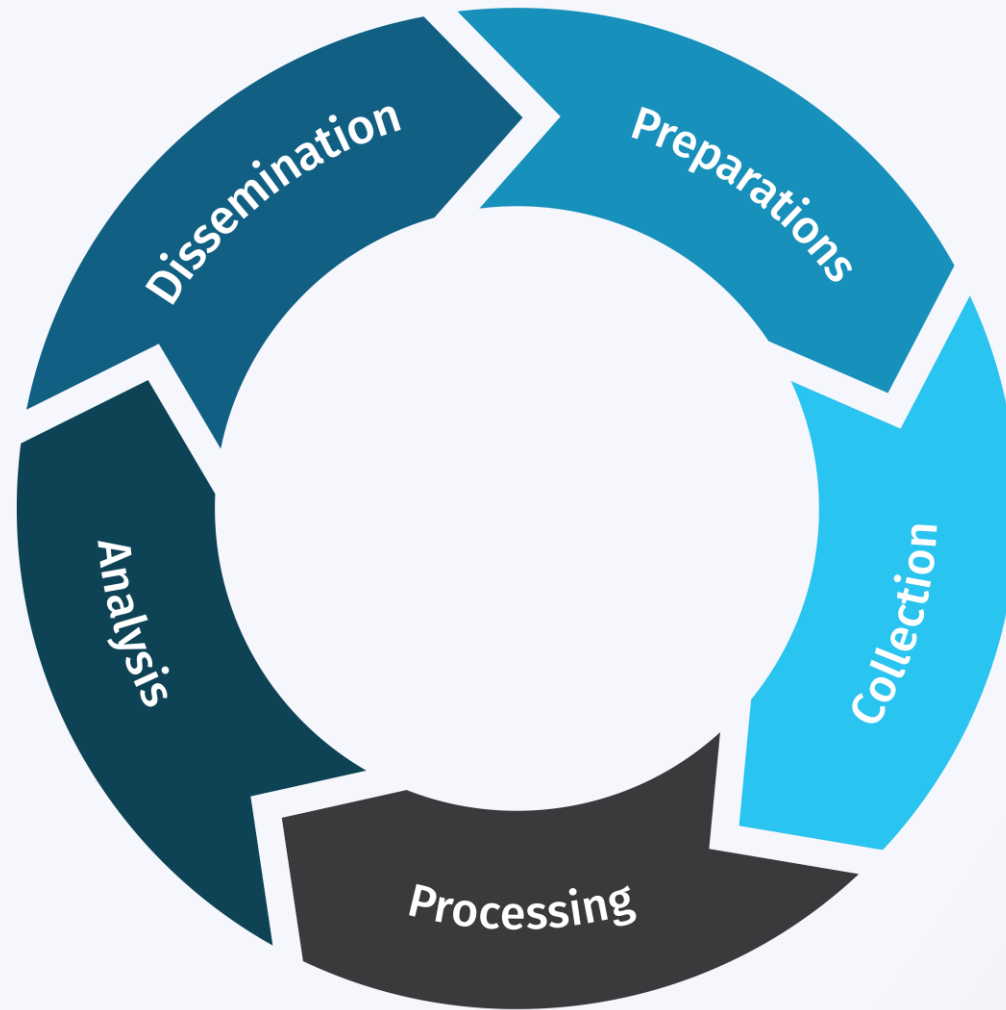
- **We all use open-source and probably** don't even realize it, but we also use it for different reasons. You might use open-source information to do a credibility check and to find out more about the person selling you something on Facebook marketplace. You may research someone you met on a dating app or before hiring someone for a job.
- A few years ago I found someone's driver's license on the street when I was on a lunch break. I picked it up, thinking I should drop it off at the local driver's license branch. Then I thought to myself, I wonder what I will find if I just Google the person's name (which I did). Turns out the second Google result was a LinkedIn page with the person's name, photo, and workplace which was in the area. I decided to call the company and ask to speak with this person and let them know I had found their license on the street.
- It seems like it was too easy to Google and find the result quickly but this is not uncommon nowadays. Most people, if not everyone, have some sort of **digital footprint**. This is a simple example to show you how quickly you can find information on a person by simply Googling their name.

Intelligence Cycle

- Let's talk about the Intelligence Cycle and what it means for those working in OSINT. There are some variations of the intelligence cycle but generally, it includes similar steps. Using the Intelligence Cycle can assist with understanding what each stage of the cycle means to the OSINT research that will follow.

Stages of the Intelligence Cycle

- **Preparation** is when the needs and requirements of the request are assessed, such as determining the objectives of the tasking and identifying the best sources to use to find the information for which you are looking.
- **Collection** is the primary and most important step in collecting data and information from as many relevant sources as possible.
- **Processing** is when the collected data and information are organized or collated.
- **Analysis and Production** is the interpretation of the collected information to make sense of what was collected, i.e. identifying patterns or a timeline of travel history. Produce a report to answer the intelligence question, draw conclusions, and recommend next steps.
- **Dissemination** is the presentation and delivery of open-source findings, i.e. written reports, timelines, recommendations, etc. Answer the intel question for stakeholders.



Passive versus Active OSINT

- **Passive means you do not engage with a target.** Passive open-source collection is defined as gathering information about a target using publicly available information. Passive means there will be no communicating or engaging with individuals online, which includes commenting, messaging, friending, and/or following.
- **Active means you are engaging with a target in some fashion**, i.e. adding the target as a friend on social profiles, liking, commenting on the target's social media posts, messaging the target, etc. Active open-source research is considered engagement and can be looked upon as an undercover operation for some organizations. Please be aware of the differences and request clarification from your agency prior to engaging.
- For active research, it's a must to blend in with the group. If you are engaging with a target you may want to create a couple of accounts on different platforms to make it look like you are a real person.
- Each organization may have different interpretations of what is considered passive versus active engagement. For example, joining private Facebook Groups may appear passive to some organizations, whereas others may consider this as engaging. Sometimes this difference can imply some sort of undercover operation capacity, therefore it's extremely important to have SOPs that outline where the organization stands with this type of engagement.
- Some researchers justify joining groups as passive, as they are only "passively" looking and not actually communicating with targets.
- A good example to consider is where a Facebook Group consists of 500 members or more, where blending in may be easy, whereas a smaller group of 20 people may be riskier. Talk to your managers before proceeding one way or the other.

Passive OSINT

- No engagement with the target
- Passively collecting from publicly available information
- Low risk of attribution

Active OSINT

- Engagement with the target
- May require special permission
- High risk of attribution

Many job descriptions and fields incorporate OSINT skills including the following:

- Journalism
- Intelligence (CIA, NSA, FBI, etc.)
- Government
- Armed forces
- Business
- Genealogy
- Education (training)
- Private investigation
- Security assessments

Qualities and Skills of a Great OSINT Analyst

Curious	Analytical	Active listening	Communication
Detail-oriented	Creative	Technical interest	Methodical
Structured	Self-motivated	Written/oral skills	Critical thinker
Organized	Tenacious		

emailrepo.io--→ it will check an email is active or not

The Five INT's:

- HUMINT
- SIGINT
- IMINT
- MASINT
- OSINT

These are terms used in intelligence and military contexts:

- **HUMINT: Human Intelligence.** This involves collecting information from human sources, such as spies, informants, and other individuals with access to valuable information.
- **SIGINT: Signals Intelligence.** This refers to the interception and analysis of electronic signals, including communications, radar emissions, and other electronic transmissions.
- **IMINT: Imagery Intelligence.** This involves collecting and analyzing images, such as photographs, satellite imagery, and reconnaissance footage, to gather information about enemy activities and terrain.
- **MASINT: Measurement and Signature Intelligence.** This involves the analysis of various physical attributes, such as radar signatures, chemical compositions, and nuclear emissions, to gather intelligence.
- **OSINT: Open Source Intelligence.** This involves gathering information from publicly available sources, such as newspapers, websites, social media, and other publicly accessible data, to gather intelligence.

How Is Open Source Intelligence Used?

- Open Source Intelligence (OSINT) is the collection, analysis, and dissemination of information that is publicly available and legally accessible. Right now, OSINT is used by a organizations, including governments, businesses, and non-governmental organizations. It is useful in information gathering for a wide range of topics such as security threats, market research, and competitive intelligence.
- Here are some common ways in which OSINT is used:
- Security and Intelligence: OSINT can be used to gather information on potential security threats, such as terrorist activity or cyberattacks. It can also be used for intelligence gathering on foreign governments, organizations, or individuals.
- Business and Market Research: OSINT can be used to gather information on competitors, industry trends, and consumer behavior. This information can be used to inform business strategy and decision-making.
- Investigative Journalism: OSINT can be used by journalists to gather information on a range of topics, including politics, business, and crime. This can help to uncover stories and provide evidence for reporting.
- Academic Research: OSINT can be used by researchers to gather data on a range of topics, including social trends, public opinion, and economic indicators.
- Legal Proceedings: OSINT can be used in legal proceedings to gather evidence or to conduct due diligence on potential witnesses or defendants.
- OSINT is an exceptional tool for gathering information on a wide range of topics and can be used by a variety of organizations and individuals to inform decision-making and strategy.

How does open-source intelligence (OSINT) work?

- Open-source intelligence (OSINT) is the practice of collecting and analyzing publicly available information to generate actionable intelligence. Here's a general overview of how OSINT works:
- **Collection:** OSINT collection involves gathering publicly available information from a variety of sources such as social media, news articles, government reports, academic papers, and commercial databases. This process can be done manually by searching for and reviewing sources, or through automated tools that can search and aggregate information.
- **Processing:** Once the information is collected, it is processed to remove duplicate, irrelevant or inaccurate data. This step involves filtering and categorizing the information based on relevance and importance.
- **Analysis:** The processed information is then analyzed to identify trends, patterns, and relationships. This can involve using data visualization tools, data mining, and natural language processing to extract meaningful insights from the data.
- **Dissemination:** The final step in the OSINT process is disseminating the intelligence to decision-makers. This can be done in the form of reports, briefings, or alerts, depending on the needs of the organization.

OSINT is an iterative process that involves constantly refining the collection, processing, and analysis of information based on new data and feedback. Additionally, OSINT is subject to the same biases and limitations as other forms of intelligence collection, and therefore requires careful evaluation and interpretation by trained analysts.

Common OSINT techniques

Common OSINT techniques

Open-source intelligence (OSINT) encompasses a wide range of techniques for collecting and analyzing publicly available information. Here are some common OSINT techniques:

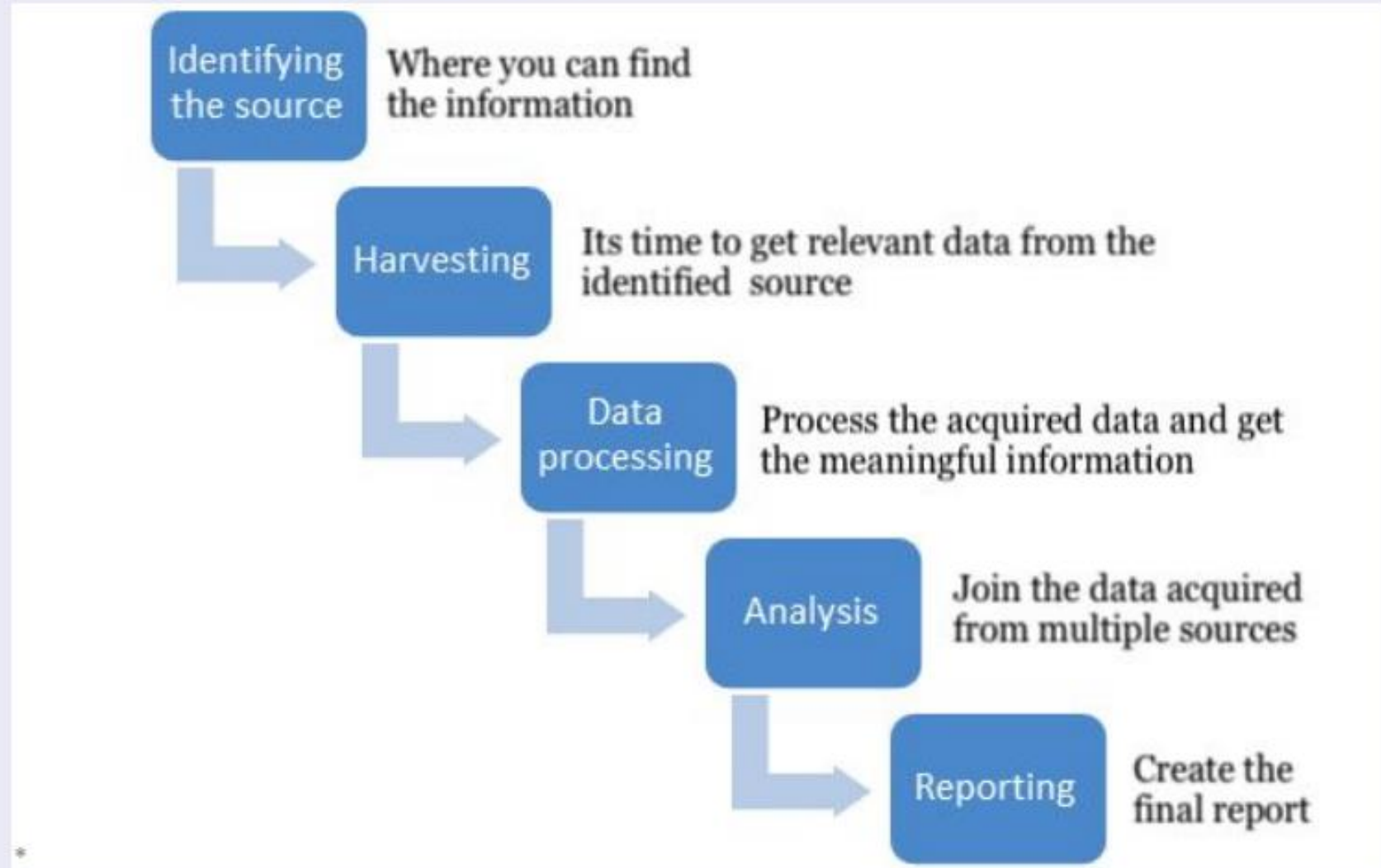
- **Search Engines:** Search engines such as Google, Bing, and Yahoo are valuable tools for gathering OSINT. By using advanced search operators, analysts can quickly filter and refine search results to find relevant information.
- **Social Media:** Social media platforms such as Twitter, Facebook, and LinkedIn are valuable sources of OSINT. By monitoring and analyzing social media activity, analysts can gain insight into trends, sentiment, and potential threats.
- **Public Records:** Public records such as court documents, property records, and business filings are valuable sources of OSINT. By accessing these records, analysts can gather information on individuals, organizations, and other entities.
- **News Sources:** News sources such as newspapers, magazines, and online news outlets are valuable sources of OSINT. By monitoring and analyzing news articles, analysts can gain insight into current events, trends, and potential threats.
- **Web Scraping:** Web scraping involves using software tools to extract data from websites. By scraping data from multiple websites, analysts can gather large amounts of data quickly and efficiently.
- **Data Analysis Tools:** Data analysis tools such as Excel, Tableau, and R are valuable for analyzing large datasets. By using these tools, analysts can identify patterns, trends, and relationships in the data.

OSINT techniques are constantly evolving as new technologies and sources of information become available. It's important for analysts to stay up-to-date on new techniques and tools in order to effectively gather and analyze OSINT.

How OSINT can benefit your organization

- Support criminal investigations by providing background profiles on people and businesses
- Support human source assessments
- Support security/risk assessments
- Support decision making
- Assist with making associations between entities
- Provide situational awareness such as getting insight into current events

The OSINT Process



Offensive OSINT – End goals:

The information above can lead to the following cyber attacks :

- Social Engineering
- Denial of Service
- Password Brute Force Attacks
- User accounts takeover
- Identity Theft
- Data theft
- And the list continues.....

OSINT Search Engines :

1. Google
2. Bing
3. Yahoo
4. Duckduckgo
5. Dogpile
6. Httrack

Conclusion :

- Open Source Intelligence is a powerful tool with far-reaching applications. Its ethical use can empower individuals, businesses, and governments with valuable insights. Understanding the types, methods, and significance of OSINT is key to harnessing its potential responsibly. As we navigate the information age, OSINT stands as a beacon of knowledge, accessible to those willing to explore its depths.
- In conclusion, **OSINT is not just a tool; it's a mindset that values transparency, accuracy, and the responsible use of information.** Whether you are a cybersecurity professional, a business strategist, or a curious individual, OSINT opens doors to a wealth of knowledge waiting to be discovered in the vast landscape of publicly available information.

DNS / Subdomain Enumeration

- Sub domain findings...

Digital Footprints and OSINT ??
Is there any relationship.....

Digital Footprints :

- **Definition:** The trail of data left behind by online interactions
- **Components:**
 - Social media activity (posts, likes, comments)
 - Browsing history
 - Publicly accessible records
- **Importance:**
 - Privacy
 - Security
 - Reputation

Open Source Intelligence (OSINT)

- **Definition:** Collecting and analysing publicly available information.
- **Sources:**
 - Public records
 - Social media
 - Websites
- **Applications:**
 - Criminal investigations
 - Journalism
 - Corporate due diligence

The Relationship

- **Data Collection:** OSINT uses digital footprints for information gathering.
- **Insights:** Social media analysis reveals behavior and connections.
- **Ethical Boundaries:** OSINT respects privacy and legal constraints.

Watching you drink Beer ...

- <https://github.com/WebBreach/untappdScraper>
- <https://brandone.github.io/untappd-scraper-web/>
- <https://webbreacher.com/2016/10/29/watching-you-drink-beer/>

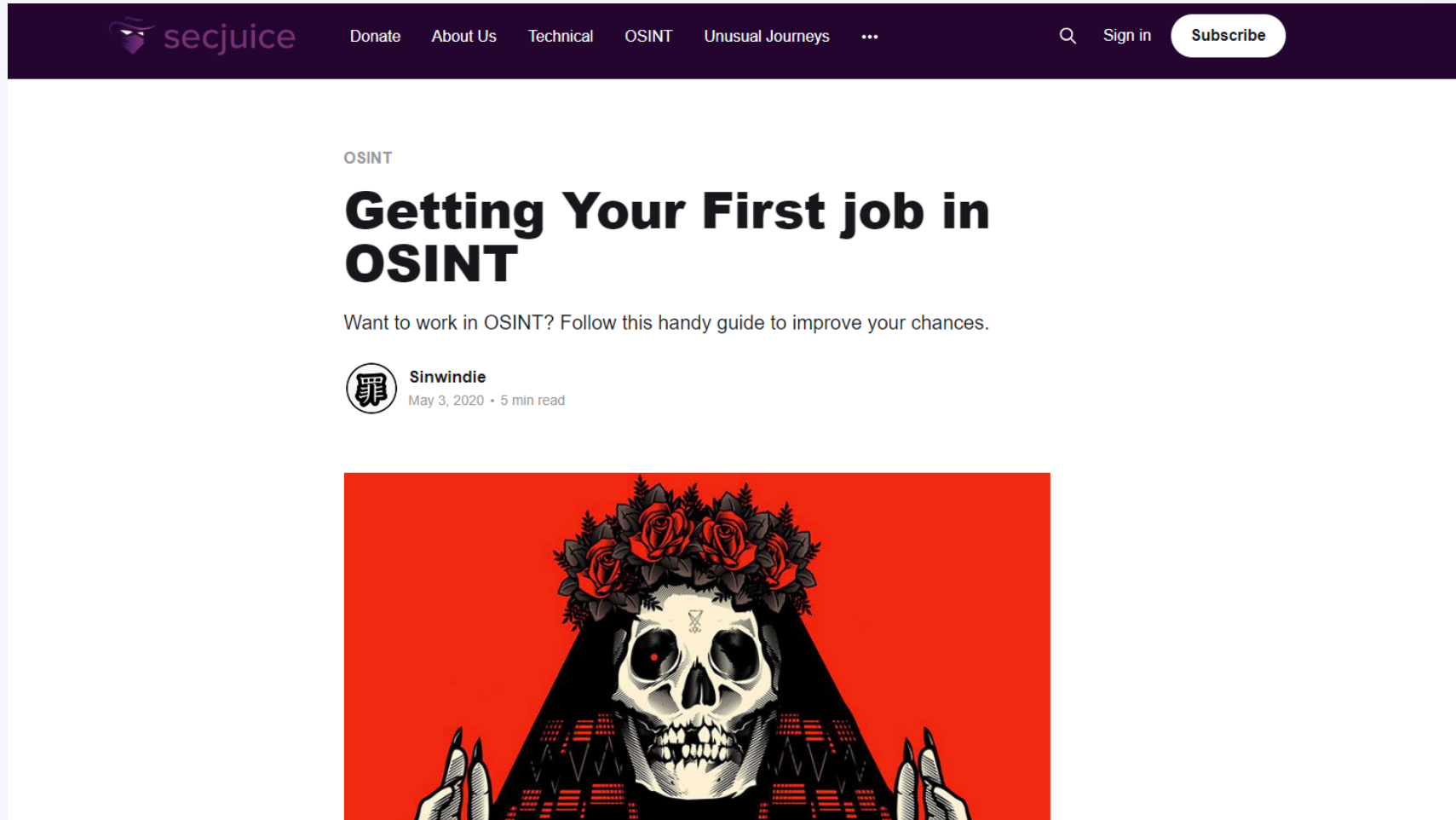
I noticed that many people on Twitter [publish when they use the Untappd.com](#) application. This app allows a user to “check-in” when they drink beer. They get badges, the dates and times of their drinking is noted, and many times the geographic location of where they drank is also available.....all with no authentication! Woohoo!

So I wondered if I could patch together some [Python](#) to scrape the [Untappd.com](#) web site for a given user and then do some analytics on their drinking habits. Stuff like:

- What time of day do they drink most often?
- What day of the week do they drink most often?
- What day of the month do they drink most often?
- Who do they drink with?
- Where do they drink?
- Are they “binge” drinking?

OWASP FOUNDATION owasp.org


<https://www.secjuice.com/landing-your-first-job-in-osint/>



https://www.osintdojo.com/resources/?source=post_page-----9993129c10c7-----#ctfs



[HOME](#)
[FAQS](#)
[RANKS](#)
[RESOURCES](#)



OSINT Resources

Submit Resource or Broken Link

General OSINT Dojo Resources

General OSINT and Methodology [↗](#)

First Steps to Getting Started in Open Source Research
OSINT Attack Surface Diagrams
OSINT & The Intelligence Cycle Part I
OSINT & The Intelligence Cycle Part II
OSINT & The Intelligence Cycle Part III
OSINT & The Intelligence Cycle Part IV
OSINT & The Intelligence Cycle Part V
UN OHCHR OSINT Guide
Verification Handbook I
Verification Handbook II
Verification Handbook III
What is OSINT?

Article Publishing Platforms [↗](#)

Secjuice
Blogger
Medium
OSINTCurious Contribute
Trace Labs Call for Content

OSINT CTFs and Quizzes [↗](#)

Kase Scenarios (CTF)
Quiztime Crew (QUIZ)
Sector035's OSINT Quiz (QUIZ)
OSINT and OSINT Quizzes (QUIZ)

<https://www.sans.org/brochure/course/practical-open-source-intelligence/4040>



The most trusted source for cybersecurity training, certifications, degrees, and research



GIAC
CERTIFICATIONS

SEC497: Practical Open-Source Intelligence (OSINT)

6
Day Program

36
CPEs

Laptop
Required

You Will Be Able To

- Perform a variety of OSINT investigations while practicing good OPSEC
- Create sock puppet accounts
- Locate information on the internet, including some hard-to-find and deleted information
- Locate individuals online and examine their online presence
- Understand and effectively search the dark web
- Create an accurate report of the online infrastructure for cyber defense, merger and acquisition analysis, pen testing, and other critical areas for an organization.
- Use methods that can often reveal who owns a website as well as the other websites that they own or operate
- Understand the different types of breach data available and how they can be used for offensive and defensive purposes
- Effectively gather and utilize social media data
- Understand and use facial recognition and facial comparison engines
- Quickly and easily triage large datasets to learn what they contain
- Identify malicious documents and documents designed to give away your location

Business Takeaways

- Improve the effectiveness, efficiency, and success of OSINT investigations
- Build an OSINT team that can perform a variety of OSINT investigations while practicing good OPSEC



GOSI
Open Source Intelligence
giac.org/gosi

SEC497 is a comprehensive training course on Open-Source Intelligence (OSINT) written by an industry professional with over two decades of experience. The course is designed to teach you the most important skills, tools, and methods needed to launch or further refine your investigation skills. SEC497 will provide actionable information to students throughout the OSINT world, including intelligence analysts, law enforcement officials, cyber threat intelligence and cyber defenders, pen testers, investigators, and anyone else who wants to improve their OSINT skills. There is something for everyone, from newcomers to experienced practitioners.

SEC497 focuses on practical techniques that are useful day in and day out. This course is constructed to be accessible for those new to OSINT while providing experienced practitioners with tried-and-true tools that they can add to their arsenal to solve real-world problems. The course has a strong focus on understanding how systems work to facilitate informed decisions, and includes hands-on exercises based on actual scenarios from the government and private sectors. We will discuss cutting-edge research and outlier techniques and not only talk about what is possible, we will practice doing it! Dive into the course syllabus below for a detailed breakdown of the topics covered.

Course Author Statement

"When I started the first open-source intelligence (OSINT) unit for my organization over a decade ago, I was told we had no budget for tools, equipment, or training. I used to joke that one nice thing about not having a budget was that it made many of my decisions very easy. If there was something I needed, I either built it myself or did without.

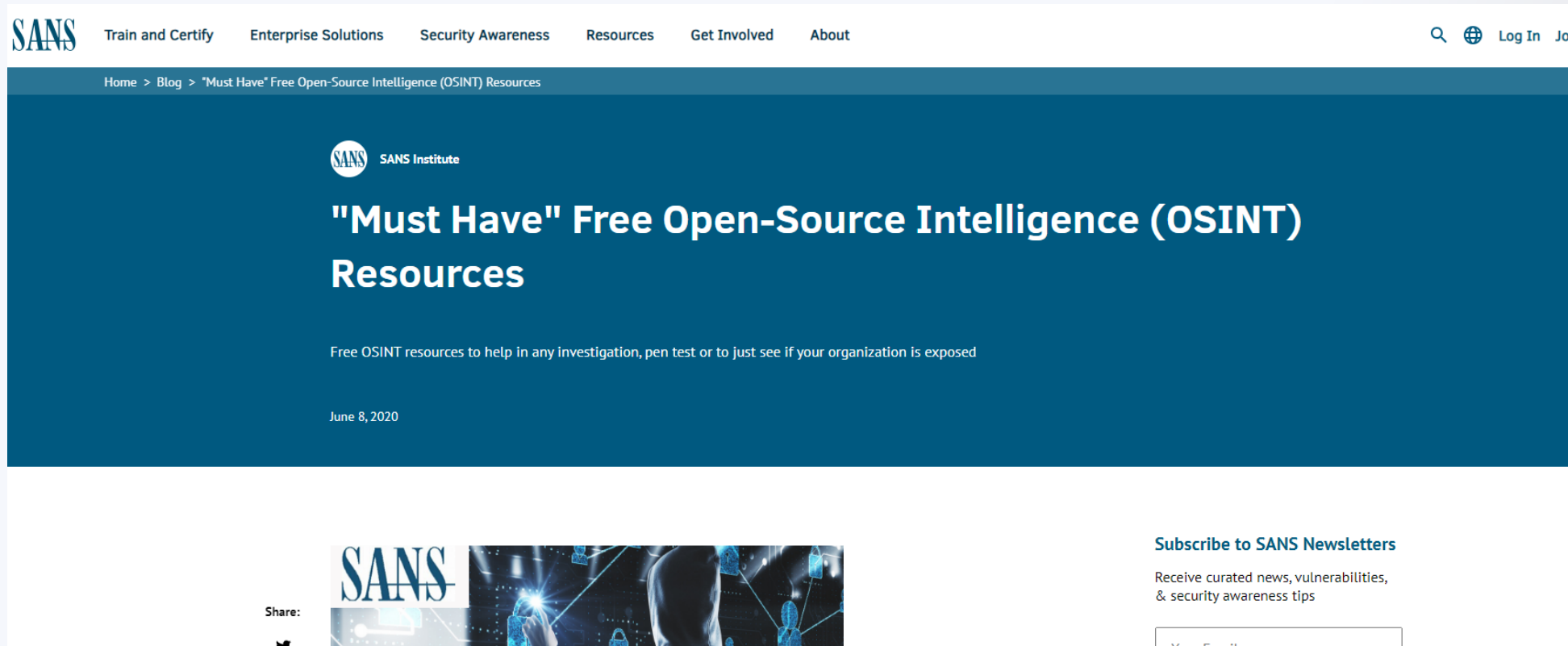
"Coming from that background forces you to understand how things work and what truly matters. In addition to performing countless OSINT investigations, I've traveled across the world for over a decade teaching operational security (OPSEC) and OSINT to various government agencies and consulted with numerous private companies, ranging from small start-ups to Fortune 100 enterprises. I have helped hunt down international fugitives, identified online infrastructure for a merger and acquisitions due diligence report, and handled numerous tasks in between. This course allows me to share my experience with what works, what does not work, and how we can achieve our goals with minimal effort and cost."

—Matt Edmondson



GOSI
Open Source Intelligence

<https://www.sans.org/blog/-must-have-free-resources-for-open-source-intelligence-osint-/>



The screenshot shows the SANS Institute website. The top navigation bar includes links for 'Train and Certify', 'Enterprise Solutions', 'Security Awareness', 'Resources', 'Get Involved', and 'About'. A search icon, globe icon, and 'Log In' link are on the right. Below the navigation bar, a breadcrumb trail reads 'Home > Blog > "Must Have" Free Open-Source Intelligence (OSINT) Resources'. The main content area has a dark blue background. It features the SANS Institute logo and the title '"Must Have" Free Open-Source Intelligence (OSINT) Resources' in large white text. Below the title, a subtitle reads 'Free OSINT resources to help in any investigation, pen test or to just see if your organization is exposed'. The date 'June 8, 2020' is displayed. At the bottom of the main content area, there is a 'Share:' section with a Twitter icon and a 'Subscribe to SANS Newsletters' section with a text input field labeled 'Your Email'.

SANS Institute

"Must Have" Free Open-Source Intelligence (OSINT) Resources

Free OSINT resources to help in any investigation, pen test or to just see if your organization is exposed

June 8, 2020

Share:

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email

☒ Company ☐ Director ☐ Trademark ☐ Address

Enter company name or cin



[Browse Companies by Activity, Age and Location](#)

HOW WELL DO YOU KNOW YOUR
CUSTOMERS, SUPPLIERS OR
COMPETITORS?

Finanvo



COMPANY ▾ WATCHLIST SUBSCRIPTIONS QUICK LINKS ▾

LOGIN

GET FREE ACCOUNT



COMPANY ▾

Search for a company

Search

🔍 Advance Search

Or analyse:

VISIONTAKES STUDIOS LLP

PSRS CONSTRUCTION PRIVATE LIMITED

PURPLE VOICE COMMUNICATIONS LLP

GROWTH CREST VENTURES LLP

CORBIN TECHNOLOGY SOLUTIONS PRIVATE LIMITED

AFFINITY REALTECH PRIVATE LIMITED

KYSALIX INNOVATE PRIVATE LIMITED

HORIZONLEAP VENTURES LLP

VIANSHI PROFESSIONALS (OPC) PRIVATE LIMITED

HATS ON ADVERTISING LLP



336,063+ Companies



2,227,519+ Directors



500,000+ Legal Cases



Check Company



Check Director Profiles



Check GST



Check Financials



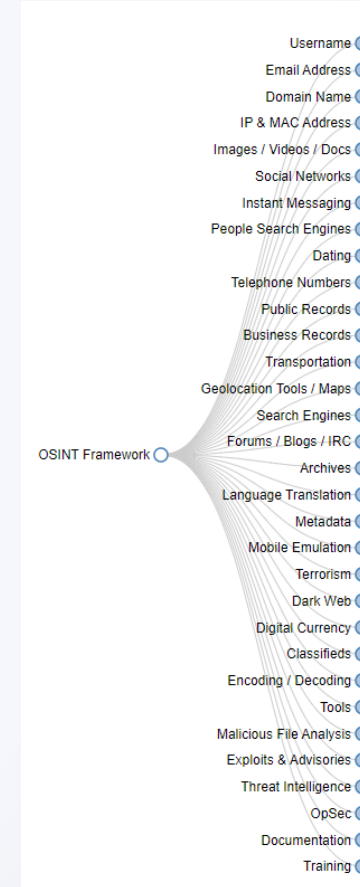
Check Legal Cases

What is the OSINT Framework?

- Gathering information from a vast range of sources is time-consuming, but there are many tools to simplify intelligence gathering. While you may have heard of tools like [Shodan](#) and port scanners like Nmap and Zenmap, the full range of tools is vast. Fortunately, security researchers themselves have begun to document the tools available.
- A great place to start is the [OSINT Framework](#) put together by [Justin Nordine](#). The framework provides links to a large collection of resources for a huge variety of tasks from harvesting email addresses to searching social media or the dark web.

OSINT Framework :

<https://osintframework.com/>





<https://centralops.net/co/domaindossier.aspx>

Domain Dossier

Investigate domains and IP addresses

domain or IP address



domain whois record



DNS records



traceroute



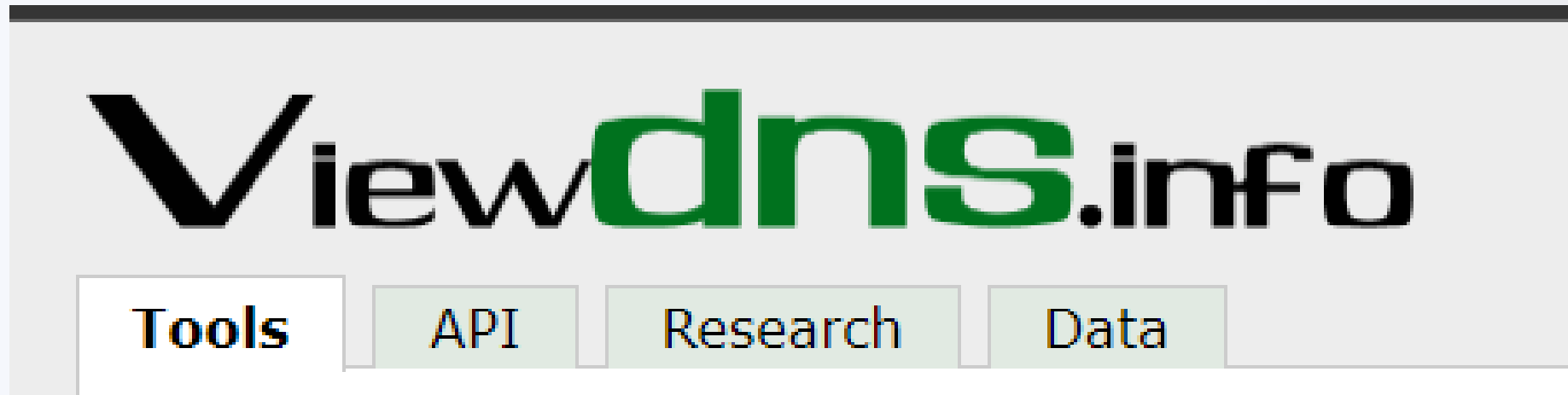
network whois record



service scan

go

<https://viewdns.info/>



DomainIQ <https://www.domainiq.com/>
<http://whois.domaintools.com/>
<https://dnsdumpster.com/>
<https://website.informer.com/> --->>> useful
<https://www.ip-tracker.org/>
<https://whoismind.com/>

Email OSINT


<https://epieos.com/>



The ultimate **OSINT tool for email
and phone reverse lookup**

<https://castrickclues.com/>

****Map****

 CASTRICK Sign In

**Find clues about anyone
Without leaving a **trace** |**

<https://www.signalhire.com/>

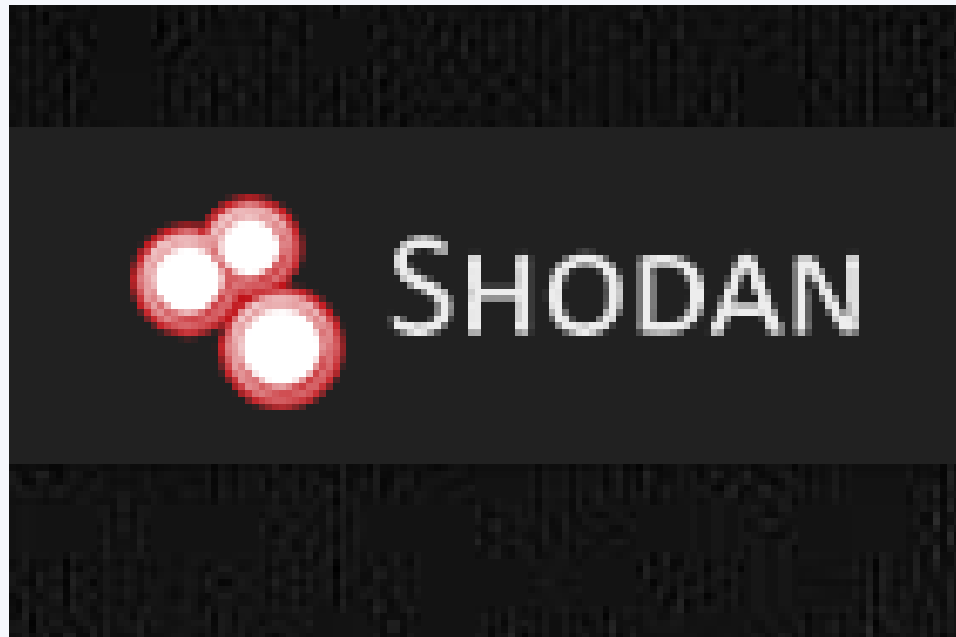
Very useful for LinkedIn based research.

<https://rocketreach.co/person>

';--have i been pwned?

Check if your email address is in a data breach

pwned?



Some more :

- Amass
- Maltego
- Recon-ng
- Phoneinfoga
- Truecaller
- Freecarrierlookup (Carrier Information / Wireless info)
- Numlookup (not supported in India)
- IRBIS , WHITEPAGES , SPYDIALER
- Twillo lookup api
- Phone Validator
- Numverify

1. <https://t.co/imoZqP0Tew>: OSINT TIP #278! OSINTBuddy - The Open-Source Alternative to Maltego! Node graphs, OSINT data mining, and plugins. Connect unstructured and public data for transformative insights.: <https://x.com/0xtechrock/status/1746216488133148709?s=20>
2. <https://github.com/The-Art-of-Hacking/h4cker/tree/master/osint>
3. asns cidr and subdomains: <https://twitter.com/Bugcrowd/status/1745460098540163498>
5. Brand new [#osint](https://twitter.com/hashtag/osint?src=hashtag_click) geolocation tool [<https://geospy.web.app>](<https://t.co/C6e13Mrc9T>) from Boston "startup" [@GrayLark_io](https://twitter.com/GrayLark_io).
6. [viewdns.info](<https://t.co/qsiAOPnHGG>) also allows you to find if email is associated with domain names. Simply enter the email address or name of the person or company to find other domains registered with the same data.
7. GitHub - iudicium/pryingdeep: Prying Deep - An OSINT tool to collect intelligence on the dark web.
8. <https://github.com/SocialLinks-IO/telegram-similar-channels>: visualization the connections between different channels (thanks to Telegram's new similar channels feature)
9. <https://play.google.com/store/apps/details?id=com.cuvora.carinfo> - car vehicle info for india
10. unmasking ip: <https://blog.sociallinks.io/center-of-excellence-column-ip-address-analysis-in-osint-investigations/>
11. <https://github.com/SocialLinks-IO/telegram-similar-channels> - similar telegram channels
12. GitHub - wishihab/userrecon: Find usernames across over 75 social networks
13. Fotoforensics, a multi-faceted photo analysis [#tool](https://twitter.com/hashtag/tool?src=hashtag_click), extracts metadata and detects any tampered images. [<http://fotoforensics.com>](<https://t.co/8XCYM0HwGM>) (from <https://x.com/DailyCTI/status/1724796291086217334?s=20>)
14. <https://x.com/lautyb/status/1729162359757766922?s=20> - real time location of any telegram user
15. [<https://github.com/Alfredredbird/alfred>](<https://t.co/Zi8GkWpdQ4>) - Alfred is a advanced OSINT information gathering tool that finds social media accounts based on inputs. (from <https://x.com/DailyDarkWeb/status/1722245636891066393?s=20>)
16. help you look up spam databases? SpamDB is the perfect solution for you. [<https://spamdb.org>](<https://t.co/yNZVRNilln>)
17. ipinfo.io: map every associated ip address associated with asn in a map

Recommended OSINT Tools for Security Research (**Sentinal one)

- Many different OSINT (Open-Source Intelligence) tools are available for security research. Some of the most popular and effective tools include:
- [Maltego](#): This tool is used for conducting open-source intelligence and forensic analysis. It allows users to collect, visualize, and analyze data from various sources, including social media, the deep web, and other online sources.
- [FOCA](#): This tool is used for metadata analysis, allowing users to extract hidden information from documents and other files. It can uncover hidden data, such as IP addresses, email addresses, and other sensitive information.
- [Shodan](#): This tool is used for internet scanning and search, allowing users to discover connected devices and networks. It can be used to identify vulnerabilities and potential security threats.
- [TheHarvester](#): This tool is used for collecting email addresses, subdomains, and other information from a variety of online sources, including search engines, social media, and the deep web.
- [Recon-ng](#): This tool is used for web reconnaissance, allowing users to gather information from various online sources, including social media, DNS records, and the deep web.
- These are just a few examples of OSINT tools that can be used for security research. There are many other tools available, and the best one for a given situation will depend on the specific needs and goals of the researcher.

Information Gathering

- ace-voip
- Amap
- APT2
- arp-scan
- Automater
- bing-ip2hosts
- braa
- CaseFile
- CDPSnarf

Vulnerability Analysis

- BBQSQL
- BED
- cisco-auditing-tool
- cisco-global-exploiter
- cisco-ocs
- cisco-torch
- copy-router-config
- Doona
- DotDotPwn

Wireless Attacks

- Airbase-ng
- Aircrack-ng
- Airdecap-ng and Airdecloak-ng
- Aireplay-ng
- airgraph-ng
- Airmon-ng
- Airodump-ng
- airodump-ng-oui-update

Web Applications

- apache-users
- Arachni
- BBQSQL
- BlindElephant
- Burp Suite
- CutyCapt
- DAVTest
- deblaze
- DIRB
- DirBuster

OSINT Tools recommended on blackberry :

- [OSINT Framework](#)
- [Nmap](#)
- [Recon-Ng](#)
- [Twint](#)
- [Metagoofil](#)

https://github.com/cipher387/osint_stuff_tool_collection

The screenshot shows the GitHub interface for the repository 'osint_stuff_tool_collection' by user 'cipher387'. The repository is public and has 122 watchers, 530 forks, and 4.5k stars. The main branch is 'main'. The repository description is 'A collection of several hundred online tools for OSINT'. The file list includes 'weekly_updates' (updated 2 years ago), 'README.md' (updated 3 months ago), and '_config.yml' (updated 2 years ago). The repository is tagged with several keywords: awesome, osint, tools, hacking, cybersecurity, awesome-list, toolset, geoint, socmint, and humint.

Repository: **osint_stuff_tool_collection** (Public)

Stats: Watch 122, Fork 530, Star 4.5k

Branch: **main**

Actions: **Code**, Issues 9, Pull requests 5, Actions, Projects, Security, Insights

About: A collection of several hundred online tools for OSINT

Keywords: awesome, osint, tools, hacking, cybersecurity, awesome-list, toolset, geoint, socmint, humint

Recent Commits:

File	Commit Message	Time Ago
weekly_updates	Update 2_February_2022.html	2 years ago
README.md	Update Digital Footprint Check C...	3 months ago
_config.yml	Update _config.yml	2 years ago



Art of Hacking

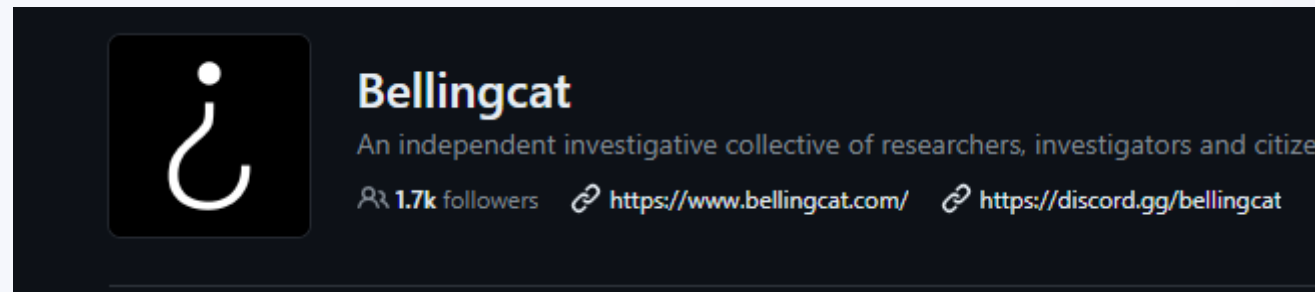
Primarily maintained by Omar Santos - resource

 998 followers

 <http://theartofhacking.org>

- Bellingcat is a well-known open-source investigative journalism organization. They are known for their work in using open-source intelligence (OSINT) and digital forensics to investigate a wide range of topics, including **conflict zones, human rights abuses, and geopolitical events**. Bellingcat gained significant recognition for their investigations into incidents like the downing of Malaysia Airlines Flight MH17 and the poisoning of Sergei Skripal. Their approach often involves analyzing publicly available information such as satellite imagery, social media posts, and other digital data to uncover facts and evidence that may not be readily apparent.

Belling Cat :



Challenges and Limitations of OSINT

- **Data Overload**
 - One of the main challenges in OSINT is sifting through vast amounts of data.
- **Data Quality**
 - Ensuring the accuracy and reliability of information obtained from open sources.
- **Data Privacy**
 - Respecting privacy boundaries while collecting and using open-source data.
- **Misinformation**
 - Dealing with the prevalence of fake news and misinformation in open sources.

OSINT is important and still gets overlooked by attackers and defenders

Feedback Form :

<https://forms.gle/9iDVVbDyVj9sTyqq7>



Lets connect :

LinkedIn : <https://www.linkedin.com/in/nipun-negi-020391227/>

Email: nipun.negi@owasp.org
nipunnegi2002@gmail.com

