SANS

OSINT POSTER

sans.org/cyber-defense

CD_OSINT_11-25

<table>
<tr><th>OPERATOR</th><th>FUNCTION</th><th>EXAMPLE</th></tr>
<tr><td>“[term]”</td><td>Search exact phrase in quotes</td><td>“HGTV Shows”</td></tr>
<tr><td>[term] OR [term]</td><td>Search for either term</td><td>tv OR streaming</td></tr>
<tr><td>[term] AROUND(n) [term]</td><td>Search for a term within n words of another term</td><td>stream AROUND(5) “HGTV Shows”</td></tr>
<tr><td>@[term]</td><td>Search social media for a handle</td><td>@hgtv</td></tr>
<tr><td>-[term]</td><td>Exclude a term</td><td>“fixer upper” “stream” –HGTV</td></tr>
<tr><td>filetype:[type]</td><td>Only show results with a certain file type, such as xlsx or pdf</td><td>site:hgtv.com filetype:pdf</td></tr>
<tr><td>([operations])</td><td>Group operations together to control how a complex search executes</td><td>site:gov wifi (password OR key)</td></tr>
<tr><td>site:</td><td>Limit results to a specific site or class of site</td><td>site:gov
site:example.com</td></tr>
<tr><td>intitle:[term]</td><td>Search for one term in the title of a page</td><td>intitle:hgtv | site:hgtv.com</td></tr>
<tr><td>allintitle:[term]</td><td>Search for all of the terms that follow the : in the title of the HTML page</td><td>allintitle:bbc news | site:bbc.com</td></tr>
<tr><td>inurl:[term]</td><td>Find sites with one term in URL</td><td>inurl:magnolia | site:magnolia.com</td></tr>
<tr><td>allinurl:[term]</td><td>Find sites with multiple terms in URL</td><td>inurl:magnolia table
site:magnolia.com</td></tr>
<tr><td>intext:[term]</td><td>Search for occurrences of a term in website text</td><td>intext:waco | site:magnolia.com</td></tr>
<tr><td>allintext:[term]</td><td>Search for occurrences of multiple terms in website text</td><td>allintext:silo shops
site:magnolia.com</td></tr>
<tr><td>link:[url]</td><td>Find pages that link to a page, but doesn’t seem to work consistently</td><td>link:www.magnolia.com
site:www.magnolia.com</td></tr>
<tr><td>before:[Date]
after:[Date]</td><td>Find results before or after a specific date or year, or in between a specific date range</td><td>before:2020 after:2015-7</td></tr>
<tr><td>[n]..[n]</td><td>Put .. between two numbers to search a range (not super accurate)</td><td>nikon $300..$500</td></tr>
</table>

Useful Google Alerts

Example Alerts for Force Protection/Situational Awareness

- (hancock) AND (john OR sally OR kevin) AND ("123 main st" OR 530-555-1212 OR 520-555-1212)
- (email@test.org) AND ("123 main st" OR 530-555-1212 OR 520-555-1212)

Example Alerts for Brand/Reputation Monitoring

- ("Globex Industries") AND ("scandal" OR "fraud" OR "hate" OR “terrible” OR “scam”)
- ("Wonka Industries") AND ("food safety violation" OR "product contamination" OR "factory shutdown")
- ("Pied Piper") AND ("patent infringement" OR "intellectual property theft" OR "copyright violation")

Example Alerts for Cybersecurity Awareness

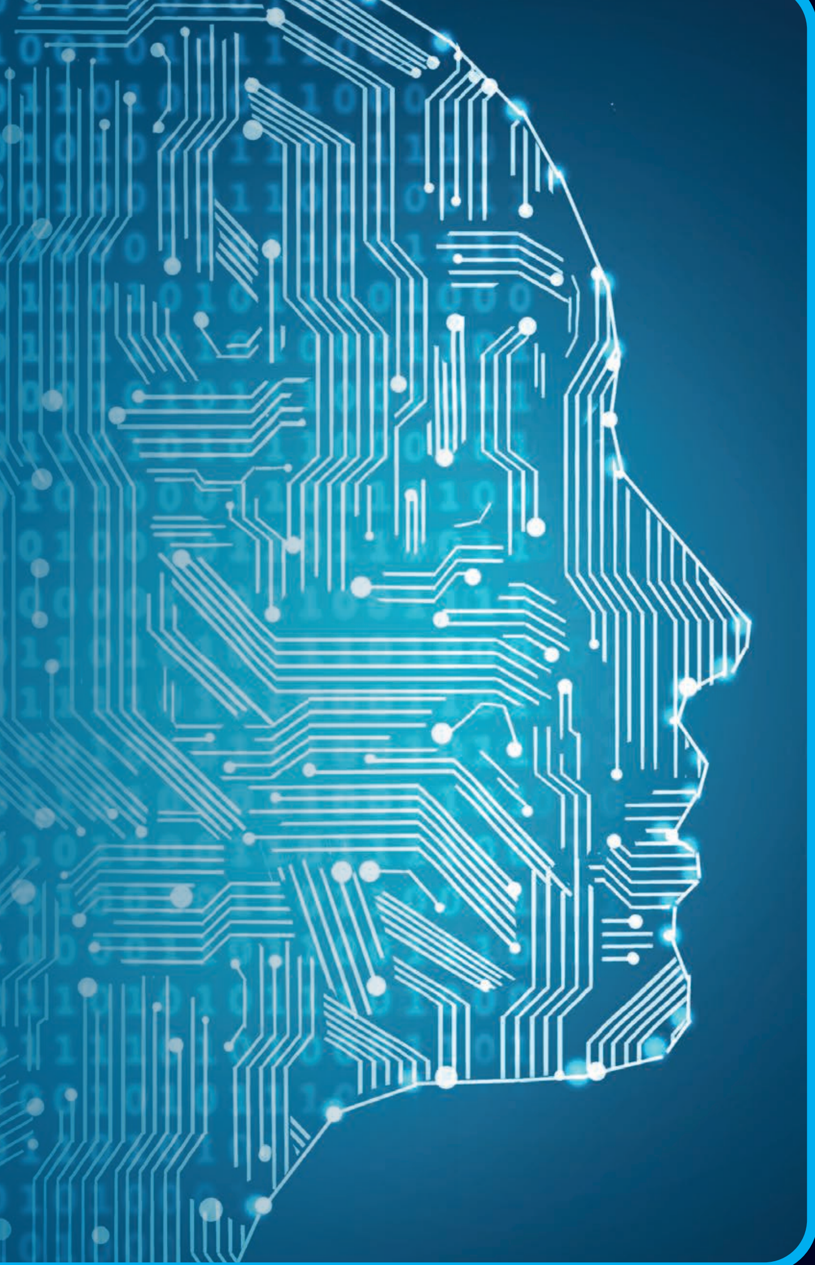
- ("Acme Corporation" OR acmecorp.com) AND ("vulnerability" OR "exploit" OR "zero-day")
- ("industry sector") AND ("cyber attack" OR "data breach" OR "security incident")
- ("supply chain" OR "third-party vendor") AND ("cyber risk" OR "data breach" OR "security vulnerability")

Useful OSINT APIs

- **Grayhatwarfare.com** – Grayhat Warfare monitors for exposed data in cloud buckets.
- **PeopleDataLabs.com** – People Data Labs allows you to search by email address, phone number, name, etc., and retrieve records.
- **IPQualityScore.com** – IPQS allows 5,000 lookups a month for IP addresses, email addresses, etc.
- **Shodan.io** – Shodan searches for devices connected to the internet, including servers, webcams, and IoT devices.

AI Resources for OSINT

- **ChatGPT** – ChatGPT is a large language model (LLM) useful for helping with writing Python code, analyzing code, writing reports, generating biographical information for sock puppet accounts, and more.
- **Claude AI** – Claude AI is a LLM similar to ChatGPT but with an emphasis on writing quality content.
- **Whisper** – Whisper is a transcription engine which generates text output from audio/video files. It automatically detects what language is being used in the video and can be utilized offline. It is capable of translating the text and the generated text files can be used as subtitles when playing the source video.
- **Face Swap** – Face Swap is an artificial intelligence (AI) model capable of morphing multiple profile pictures to generate a “fake” profile picture that appears real.
- **Concierge** – Concierge is an open-source LLM which is able to run on low-powered hardware and ingest new information to incorporate into its analysis via retrieval-augmented generation (RAG).



IPV4 and IPv6 Address

IPv4 addresses were deployed in 1981 and have 4.3 billion possible addresses.

40.112.72.205

IPv6 addresses were deployed in 1998 and have 340 undecillion possible addresses.

2001:4998:0024:120d:0000:0000:0001:0001

2001:4998:24:120d::1:1

Note: IPv6 addresses are so long, there are rules for shortening them!
The two IPv6 addresses above are actually the same address, the bottom adddress just had any leading zeros removed.

Sites to Research IP Addresses

- Maxmind.com – Maxmind provides free information about IP addresses, including the ISP and city-level geolocation accuracy. The premium data includes user type (cellular, residential, business, etc.).
- IPQualityScore.com – IPQS provides 5,000 free lookups a month as well as information on ISP, city-level accuracy, proxy/VPN/Tor status, etc.
- IKnowWhatYouDownload.com – I KNOW allows you to see any peer-to-peer (P2P) file sharing activity from an IP address.
- Shodan.io – Shodan is a technology-focused search engine that allows you to see what services are running on a system and other detailed information.
- Search.Censys.io – Censys is a technology-focused search engine that allows you to see what services are running on a system and other detailed information on known vulnerabilities and SSL certificates.
- Greynoise.io – GreyNoise catalogs traffic flowing across the internet, allowing you to determine if activity from an IP address is targeted towards a specific group or indiscriminately scanning the internet.
- AbuseIPDB.com – AbuseIPDB is a central repository for reporting IP addresses that have been associated with malicious online activity.

Internal IP Addresses

These internal IP addresses are usually of little interest to OSINT investigators:

- 10.X.X.X
- 172.16.X.X–172.31.X.X
- 192.168.X.X–192.168.X.X
- 127.0.0.1 (localhost)

Shodan Search Syntax

- city:"[city name]" – Searches for devices in a specific city
- country:"[country code]" – Searches for devices in a specific country
- hostname:"[hostname]" – Searches for devices with a specific hostname
- net:"[IP range]" – Searches for devices within a specific IP range
- os:"[operating system]" – Searches for devices with a specific operating system
- port:"[port number]" – Searches for devices with a specific port
- org:"[organization name]" – Searches for devices associated with a specific organization
- isp:"[internet service provider]" – Searches for devices using a specific internet service provider
- product:"[product name]" – Searches for devices that are using a specific software or hardware product
- version:"[version number]" – Searches for devices running a specific version of software or firmware
- has_screenshot:"true" – Searches for devices with available screenshots
- ssl.cert.subject.cn:"[common name]" – Searches for SSL certificates with a specific common name
- http.title:"[title text]" – Searches for web pages with a specific title
- http.html:"[html content]" – Searches for web pages containing specific HTML content
- before:"[date]" | after:"[date]" – Searches for devices that were online before or after a specific date
- product:"[product name]" – Searches for devices running a specific product
- version:"[version]" – Searches for devices with a specific version number
- webcam – Searches for internet-connected webcams

Example Shodan Searches

- "default password" – Searches for devices using default passwords
- "MongoDB Server Information" port:27017 -authentication – Finds exposed MongoDB databases
- "in-tank inventory" port:10001 – Finds gas station pump controllers

Censys Host Search Syntax

- **Single IP (supports IPv4 and IPv6)** – 8.8.8.8
- **Subnet by CIDR** – ip: "8.0.0.0/8"
- **Subnet by IP range** – ip: [1.12.0.0 to 1.15.255.255]
- **By TLD—**dns.names – "*.su"
- **Autonomous System Number (ASN)** – autonomous_system.asn:6167
- **Single port** – services.port:80
- **Any of these ports** – services.port:{22,80,443}
- **Service** – services.service_name:SSH
- **Labels** – labels: c2
- **Other label options include** – ics, login-page and open-dir

Censys Certificate Search Syntax

- **Self-signed certificates for a domain** – (cellebrite.com) and labels='self-signed'
- **Certificates issued by a specific organization** – parsed.issuer.organization='Internet Widgits Pty Ltd'

Example Censys Searches

- **Roombas** – services.tls.certificates.leaf_data.issuer.common_name: "Roomba CA"
- **Brute Ratel servers** – services.http.response.body_hash="sha1:1a279f5df4103743b823ec2a6a08436fdf63fe30"
- **ICS Protocols** – services.service_name: {BACNET, CODESYS, EIP, FINS, FOX, IEC60870_5_104, S7, MODBUS}

SANS OSINT Training Courses

SEC497: Practical Open-Source Intelligence (OSINT)™

SEC497™ is based on two decades of experience with OSINT research and investigations supporting law enforcement, intelligence operations, and a variety of private sector businesses ranging from small start-ups to Fortune 100 companies. The goal is to provide practical, real-world tools and techniques to help individuals perform OSINT research safely and effectively. One of the most dynamic aspects of working with professionals from different industries worldwide is getting to see their problems and working with them to help solve those problems. SEC497™ draws on lessons learned over the years in OSINT to help others. The course not only covers critical OSINT tools and techniques, it also provides real-world examples of how they have been used to solve a problem or further an investigation. Hands-on labs based on actual scenarios provide students with the opportunity to practice the skills they learn and understand how those skills can help in their research. SEC497™ includes 29 hands-on labs and a Capstone Capture-the-Flag event.

GIAC Certification: GIAC Open Source Intelligence (GOSI)

SEC587: Advanced Open-Source Intelligence (OSINT) Gathering and Analysis™

With OSINT being the engine of most major investigations in this digital age, the need for a more advanced course was inevitable. The data in almost every OSINT investigation becomes more complex to collect, exploit, and analyze. To address this reality, OSINT practitioners must be able to perform OSINT at scale and possess the means and methods to check and report on the reliability of their analysis. In SEC587™ you will learn how to perform advanced OSINT gathering and analysis as well as understand and use common programming languages such as JSON and Python. SEC587™ also will go into dark web and financial (cryptocurrency) topics as well as disinformation, advanced image, and video OSINT analysis. This is an advanced, fast-paced course that will give seasoned OSINT investigators new techniques and methodologies and entry-level OSINT analysts that extra depth in finding, collecting, and analyzing data sources from all around the world.

GIAC Certification: GIAC Strategic OSINT Analyst (GSOA)

Blueprint Podcast
sans.org/blueprint

Blog
sans.org/blog

Blue Team GitHub
github.com/sans-blue-team

Webcasts
sans.org/webcasts

OSINT Community
sansurl.com/osint

Videos
youtube.com/@SANSCyberDefense

SANS CYBER DEFENSE

Command Line Kung Fu

View the contents of a file

- **Linux** – `cat file.txt`
- **Windows** – `type file.txt`

Limit results to a line that contains a specific term

- **Linux** – `cat file.txt | grep -I sans`
- **Windows** – `type file.txt | findstr -I sans`

Find out how many lines contain that term

- **Linux** – `cat file.txt | grep -I sans | wc -l`
- **Windows** – `type file.txt | findstr -I sans | find /c /v ""`

Send the selected output to a new file

- **Linux** – `cat file.txt | grep -I sans > new_file.txt`
- **Windows** – `type file.txt | findstr -I sans > new_file.txt`

Dark Web Resources on the Internet

- `ahmia.fi` – Fantastic (and free) dark web search engine
- `Tor.taxi` – Trusted directory of sites on the dark web
- `Tor.link` – Directory of sites on the dark web
- `Daunt.link` – Trusted directory of sites on the dark web
- `Torry.io` – Dark web search engine
- `https://github.com/fastfire/deepdarkCTI` – Incredible list of URLS for dark websites including:
  - Forums such as Dread, XSS, Exploit, etc.
  - Ransomware blogs
  - Marketplaces

Tor Browser as a Proxy

When you start the Tor Browser, it automatically opens a proxy listener on port 9050 and/or 9150. Any application that can be configured to use this proxy will have its traffic routed through Tor and will be able to access the dark web.

This functionality has many uses including being able to use Chrome/Firefox etc. and their plugins to gather information from dark websites as well as add the ability to access the dark web with your Python code.

Detecting AI Content

As AI models become more sophisticated, detecting AI-generated content has become more challenging.

METHOD	DETAILS
Look for repetitive phrases and ideas.	AI-generated content often includes repetitive phrases, sentences, or ideas. This happens because the model might generate similar outputs based on its training data. Identifying repetitive patterns, especially unusual repetition, can be a strong indicator of machine-generated text.
Check for inconsistent writing styles.	AI might produce content with sudden changes in tone or style. For example, a paragraph might switch from formal to informal language abruptly. These inconsistencies occur because AI models might pull from varied data sources, leading to a lack of uniformity in writing style.
Identify odd word choices or phrasing.	AI models sometimes use words or phrases in ways that seem slightly off or uncommon. This can include the use of synonyms that don't fit the context perfectly or awkward sentence constructions that a native speaker wouldn't typically use.
Assess the depth of content.	AI-generated text might lack the depth and nuance of human writing. While it can produce coherent and informative content, it often misses the detailed insights, unique perspectives, or expert knowledge that a human writer would provide.
Verify factual accuracy.	AI-generated content can include inaccurate information. It's essential to cross-check facts with reliable sources. AI may generate plausible-sounding but incorrect facts, especially when discussing niche or complex topics, making thorough verification critical.
Analyze sentence structure and linguistic patterns.	AI models may use more complex or unnatural sentence structures compared to human writers. Look for overly complex sentences, unusual grammar patterns, or repetitive sentence structures. These linguistic anomalies can signal that the text is machine-generated.
Monitor posting behavior.	Frequent, high-volume content posting without a corresponding number of human interactions can be a sign of AI-generated content. Analyze the posting frequency and engagement metrics. AI-generated posts might flood a platform with content at a rate that is impractical for human users.
Examine user engagement patterns.	AI-generated content might attract different engagement patterns compared to human content. For instance, such content might receive fewer meaningful comments or generate engagement that seems automated. Human users tend to engage in more nuanced and varied ways.

Specific Prompt Error Messages to Search For

- "As an AI language model"
- "I'm sorry, I cannot generate"
- "Not a recognized word"
- "Cannot provide a phrase"
- "Violates OpenAI's content policy"

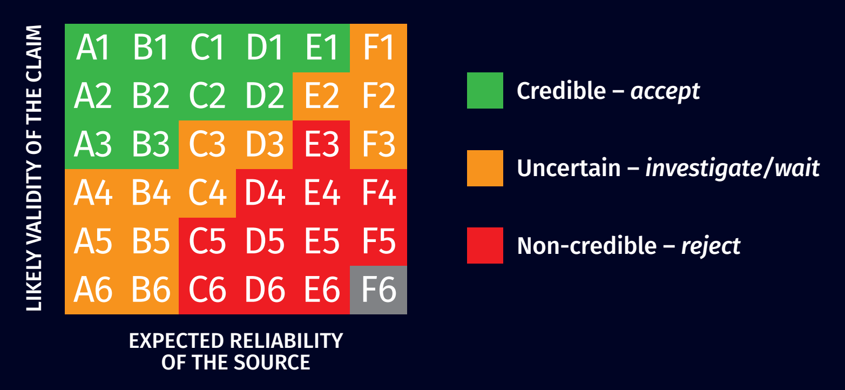
Resources for Researching Cryptocurrency Transactions

- `Breadcrumbs.app` – Breadcrumbs provides attribution (Coinbase, Binance, etc.) on over 50 million Ethereum and Bitcoin addresses. Breadcrumbs offers free plans and paid plans much cheaper than other solutions in the space.
- `Blockchain.com` – The blockchain.com explorer offers visibility into blockchains for Bitcoin, Bitcoin Cash, and Ethereum.
- `Walletexplorer.com` – Wallet Explorer groups cryptocurrency addresses together by wallet ID. It can help determine what site (dark web marketplace, cryptocurrency exchange, etc.) an address is tied to.
- `Chainabuse.com` – Chainabuse is a site where scam-related cryptocurrency addresses are reported and researched.
- `OpenSanctions.com` – OpenSanctions is an international database of persons and companies of political, criminal, or economic interest. The site contains datasets from over 120 sources, some of which have cryptocurrency wallet addresses for sanctioned individuals and/or groups.
- `ArkhamIntelligence.com` – Arkham Intelligence is a site with a large amount of information on which site/service a wallet address is tied to. It has its own cryptocurrency (ARKM) which it uses for an Intel Exchange where users can post bounties for information and/or sets of information for sale. Common listings include bounties to help identify the individuals behind cryptocurrency scams and users selling lists of wallets tied to known investment firms to see where and when they move funds.

The Admiralty Code

The Admiralty Code (AKA NATO System) is a relatively simple scheme for categorizing evidence according to its credibility. It was initially used by the British Admiralty for the assessment of evidence used in naval intelligence, but it is now used in many police departments, intelligence agencies, and defense-related organizations, including the U.S. Army. (U.S. Army Field Manual 2-22.3, 2006)

The Admiralty Code for Evaluating the Credibility of Evidence



🟩 A1	🟩 B1	🟩 C1	🟩 D1	🟩 E1	🟧 F1
🟩 A2	🟩 B2	🟩 C2	🟩 D2	🟧 E2	🟧 F2
🟩 A3	🟩 B3	🟧 C3	🟧 D3	🟥 E3	🟧 F3
🟧 A4	🟧 B4	🟧 C4	🟥 D4	🟥 E4	🟥 F4
🟧 A5	🟧 B5	🟥 C5	🟥 D5	🟥 E5	🟥 F5
🟧 A6	🟧 B6	🟥 C6	🟥 D6	🟥 E6	⬜ F6

- 🟩 Credible – *accept*
- 🟧 Uncertain – *investigate/wait*
- 🟥 Non-credible – *reject*

THE SOURCE		
A	Reliable	**No doubt** of authenticity, trustworthiness, or competency, has a history of complete reliability
B	Usually reliable	**Minor doubt** about authenticity, trustworthiness, or competency, has a history of valid information most of the time
C	Fairly reliable	**Doubt** of authenticity, trustworthiness, or competency, but had provided valid information in the past
D	Not usually reliable	**Significant doubt** about authenticity, trustworthiness, or competency, but had provided valid information in the past
E	Unreliable	**Lacking** authenticity, trustworthiness, or competency, has a history of invalid information
F	Cannot be judged	**No basis** for evaluating the reliability of the source

THE CONTENT		
1	Confirmed	**Confirmed** by other independent sources, logical in itself, consistent with other information on the subject
2	Probably true	**Not confirmed**, logical in itself, consistent with other information on the subject
3	Possibly true	**Not confirmed**, reasonably logical, ages with some other information on the subject
4	Doubtfully true	**Not confirmed**, possible but not logical, no other information on the subject
5	Improbable	**Not confirmed**, not logical in itself, contradicted by other information on the subject
6	Misinformation	**Unintentionally false**, not logical in itself, contradicted by other information on the subject, confirmed by other independent sources
7	Deception	**Deliberately false**, contradicted by other information on the subject, confirmed by other independent sources
8	Cannot be judged	**No basis** for evaluating the reliability of the source

Discord

A Discord server is a community space where users can chat, share media, and participate in various activities. Servers are divided into text channels (for chat) and voice channels (for voice communication). There are both public and private servers. Public servers are open to anyone and often focused on specific topics or interests. Private servers require an invitation to join and are usually for more exclusive or private groups. To find servers, use the "Explore Public Servers" option to search by category or interest. Here are some sample Google dorks to find discord content.

QUERY	EXPLANATION
`site:discord.gg`	Searches for pages that contain Discord invite links from the primary domain used for Discord invites
`site:discord.gg "gaming community"`	Adds specific keywords related to the topic or interest (e.g., "gaming community") to find relevant servers
`filetype:pdf "discord invite"`	Looks for PDF documents containing Discord invite links—can also use filetype:txt, filetype:doc, etc.
`site:reddit.com "discord.gg" "cybersecurity"`	Combines keywords with site-specific searches to find Discord invites posted on Reddit, which often shares server invites
`inurl:discord.gg "music community"`	Uses the *inurl* operator to search for URLs that contain specific text such as "discord.gg" combined with keywords
`site:forum.example.com "discord invite"`	Targets specific forums (replace forum.example.com with the URL of the forum) to find Discord invites
`intitle:"discord invite" "technology"`	Uses the *intitle* operator to search for pages with specific words in the title, useful for finding blog posts or articles mentioning Discord invites
`site:discord.com inurl:invite "art community"`	Combines *site* and *inurl* operators with a specific keyword to narrow the search to Discord's own domain for invites related to art communities
`site:twitter.com "discord.gg" "book club"`	Targets social media platforms where users share Discord invites by combining the site operator with keywords
`site:pastebin.com "discord.gg"`	Pastebin and similar sites are often used to share collections of links and can be a source for Discord invites
`site:facebook.com "discord.gg" "fitness"`	Targets specific community-driven platforms like Facebook to find groups that share Discord server links
`site:discord.gg "FPS gaming"`	Searches for pages containing Discord invites specifically mentioning "FPS gaming"
`site:reddit.com/r/cybersecurity "discord.gg"`	Targets the Reddit cybersecurity community for shared Discord invites
`filetype:txt "discord.gg" "study group"`	Searches for text files containing Discord invites related to study groups
`intitle:"discord invite" "tech news"`	Finds blog posts or articles with titles indicating they contain Discord invites related to tech news

Telegram

Telegram is a cloud-based instant messaging app that allows users to send messages, share media, and create groups and channels for broadcasting messages to large audiences. It is known for its focus on privacy, encryption, and speed. These Telegram channels are often used by members of the criminal underground to exchange ideas and information such as breach data and information stealer logs. Additionally, they serve as marketplaces where illicit goods and services, including stolen credentials, hacking tools, and illegal substances, are bought and sold. Telegram has a built-in search functionality which can help you find users and channels. You can also use Google dorks to help find Telegram content.

QUERY	EXPLANATION
`site:t.me`	Searches for pages that contain Telegram links from the t.me domain
`site:t.me "cybersecurity"`	Adds specific keywords related to the topic (e.g., "cybersecurity") to find relevant Telegram links
`filetype:pdf "telegram invite"`	Looks for PDF documents containing Telegram invite links—can also use filetype:txt, filetype:doc, etc.
`site:reddit.com "telegram invite" "cybersecurity"`	Combines keywords with site-specific searches to find Telegram invites posted on Reddit, often shared in discussions
`inurl:t.me "trading group"`	Uses the *inurl* operator to search for URLs that contain specific text, such as "t.me", combined with keywords
`site:forum.example.com "telegram invite"`	Targets specific forums (replace forum.example.com with the URL of the forum) to find Telegram invites
`intitle:"telegram invite" "cryptocurrency"`	Uses the *intitle* operator to search for pages with specific words in the title, useful for finding blog posts or articles mentioning Telegram invites
`site:twitter.com "t.me" "book club"`	Targets social media platforms where users share Telegram invites by combining the site operator with keywords
`site:pastebin.com "t.me"`	Pastebin and similar sites are often used to share collections of links and can be a source for Telegram invites
`site:facebook.com "telegram invite" "fitness"`	Targets specific community-driven platforms like Facebook to find groups that share Telegram server links
`site:t.me "hacking group"`	Searches for pages containing Telegram invites specifically mentioning "hacking group"
`site:reddit.com/r/OSINT "telegram invite"`	Targets the Reddit OSINT community for shared Telegram invites
`filetype:txt "t.me" "study group"`	Searches for text files containing Telegram invites related to study groups
`intitle:"telegram channel" "tech news"`	Finds blog posts or articles with titles indicating they contain Telegram invites related to tech news

Business Research Resources

- **The Organized Crime and Corruption Reporting Project (OCCRP)**
  The OCCRP provides an index of country specific resources for researching businesses across the world.
  `https://id.occrp.org/databases`
- **The UK's Companies House**
  In addition to UK coverage, the UK Companies House has a page listing several company registries from other countries.
  `www.gov.uk/government/publications/overseas-registries/overseas-registries`
- **Chinese Business Registries**
  Chinese Business Registries can provide details about Chinese companies including telephone numbers, email addresses, historical names, date of formation, legal representative, shareholders, executives, officers, directors, Chinese Unified Social Credit Score, and document filing history.
  `Qcc.com` & `Qixin.com`
- **OpenCorporates**
  OpenCorporates crawls the web, aggregates corporate ownership information, and structures it for free public use.
  `OpenCorporates.com`
- **Open Sanctions**
  Open Sanctions is a free international database of persons and companies of political, criminal, or economic interest that provides raw data from over 60 sources in downloadable formats. `OpenSanctions.org`
- **SEC EDGAR Database**
  `www.sec.gov/edgar/search-and-access`
  EDGAR is a database of corporate filings maintained by the Securities Exchange Commission (SEC) that can be difficult to search, but provides a wealth of information. Investigative journalist organization Bellingcat recently released a Python tool that can make aquiring information from EDGAR much easier. The tool is available here: `https://github.com/bellingcat/EDGAR`

Executive Summary (AKA Key Findings, Bottom Line Up Front (BLUF), etc.)

Unfortunately, no matter how great a report is, some people will only spend a few minutes reviewing it. To make sure that we convey the most importing findings to those individuals, we need an executive summary section at the beginning of our report.

Methodology

One of the key components of digital forensics is that if two forensics practitioners receive the same evidence, analyze it, and reports their findings, they should both come to very similar conclusions. OSINT is similar, and the methodology section is where you describe at a high level the methods used in your research and analysis.

Methodology helps others understand how something was accomplished so another practitioner can verify the results.

When results are scarce, the methodology section is more important than ever to let others know what you tried. This not only conveys how much effort you put into your research, but can help others avoid wasting time trying the same techniques you did.

Findings

The findings section likely represents the bulk of your report, and in addition to your writeup, it can include images, screenshots, tables, etc.

One of the most important things for an analyst to provide is an explanation of why things are important. Analysts who focus on a particular area often believe that what they know, others know as well, but that's often not the case. You likely have knowledge or context that others viewing the report may not, so you need to convey that information where possible to help answer the "so what?" question.

Appendices

One of the most difficult parts of report writing is meeting the needs of a majority of people who read your report. As a general rule, shorter reports are preferred over large ones. The executive summary meets the needs of those only spending a few minutes with your report, while the main body of the report meets the needs of someone spending a little more time. But what about another OSINT practitioner who receives a task based off your report? The report you generate may be the end of the journey on that particular topic, but someone else may receive that report and use it as the starting point for their own research.

In the case of your report being a starting point, that individual would likely appreciate more details, including some of the "raw" information, that anyone else reading the report would likely just gloss over. To help meet this goal, appendices are a fantastic tool. Raw output from tools or other sources that are summarized in your report can be placed in an appendix and included as an attachment with your report. Having an executive summary, a concise report, and additional raw information included as appendices can help ensure that your report meets the diverse needs of all readers.