

EXPERMINT: 03

● **Aim:** Use OSINT DORKS (create and execute search queries) to verify the accuracy of the information by cross-referencing various sources and critically evaluating the reliability and credibility of the new article.

● **Theory:**

Google Dorks for OSINT Investigations

Dorking is a technique that uses advanced search operators within Google Search and other search engines to find information. Primarily used to locate security holes in the configuration and computer code within websites, Dorks can also provide investigators with opportunities to enhance intelligence gathering during OSINT investigations.

Advanced search operators are special commands within search engines that modify searches by adding parameters to narrow searches and drill deeper into results.

We've outlined 14 advanced search operators that can be useful to investigators to refine search results, which include:

- “search term” = exact phrase, i.e. "Skopenow streamlines your due diligence and claims process"

Quotation marks enable users to force an exact match for required words or phrases. The exact match operator can be used to refine results to ensure that a specific phrase is included in the results or to exclude synonyms when searching for single words. Searching for an exact phrase during an investigation can locate material written by a specific person or business.

- **OR** or **|** = *either* search term *or* search term, i.e. Ed OR Edward or Ed|Edward|Edwin

The OR operator enables searching for multiple words as alternatives to one another, locating either X or Y or both. The pipe (|) operator functions identically to “OR”. Investigators can utilize the OR operator when only a nickname is known for a subject, enabling different variations of the same name to be searched at once.

- **+** or **AND** = search term *and* search term, i.e. Steve Adams AND Skopenow

The AND operator enables searching for results that must include two different words phrases, searching for both X and Y. Results will only include results that include both search phrases. The plus (+) operator can also be used in place of “AND”. AND can be useful for investigators when searching for information on a person, ensuring results relate to them by including their employer's name.

- **-** = Not search term, i.e. Skopenow -www.skopenow.com

The minus operator enables users to exclude a word or phrase from search results. When results are extensive, removing irrelevant words that feature prominently in numerous results is particularly useful when looking to reduce results.

- **site:** = Only on this site, i.e. "Skopenow" **site:**twitter.com

The site operator enables users to restrict results to only those from a specific website. When investigating a business, the site operator can ensure results come specifically from their official website.

- **filetype:** = Only this type of file, i.e. OSINT **filetype:**pdf OR **filetype:**docx

The filetype operator enables search results to be restricted to those that are a specific file type, removing other file types and standard web pages. filetype: can provide benefit during an investigation when searching for contracts and whitepapers in PDF or Word documents.

- **intitle:** = Only show results where text is in title of site, i.e. **intitle:**final.attendee.list "Fraud"

The intitle operator enables users to find web pages with a certain word or phrase in the title. Investigators can use the intitle operator to find relevant web pages and articles containing a relevant keyword.

- **inurl:** = Only show results where text is in the web address of a website, i.e. **inurl:resume "john smith"**

The inurl operator enables users to find web pages with a certain word or phrase in the web address. Investigators can use the inurl operator to find relevant web pages containing a keyword in the web address.

- **intext:** = Only show results where text is in the main body of the text of a website, i.e. **Skopenow intext:OSINT**

The intext operator enables users to find web pages with a certain word or phrase in the main text of the web page. Investigators can use the intext operator to locate results where a keyword within the body of a web page will limit results, such as a year or location name.

- **allintext:** = locate all words in a web page, i.e. **allintext: skopenow insurance fraud**

The allintext operator enables users to find web pages that contain a list of keywords in the main text of the web page but not necessarily next to one another. Investigators can use the allintext operator when more than one keyword is necessary as an anchor within the body of a webpage to find results, such as multiple keywords or names related to a crime.

- **cache:** = Only show cached links, i.e. **cache:skopenow.com**

The cache operator enables users to return the most recently cached version of a webpage when the web page has been indexed. Investigators can use the cache operator to locate previous versions of edited or deleted web pages to locate removed intelligence.

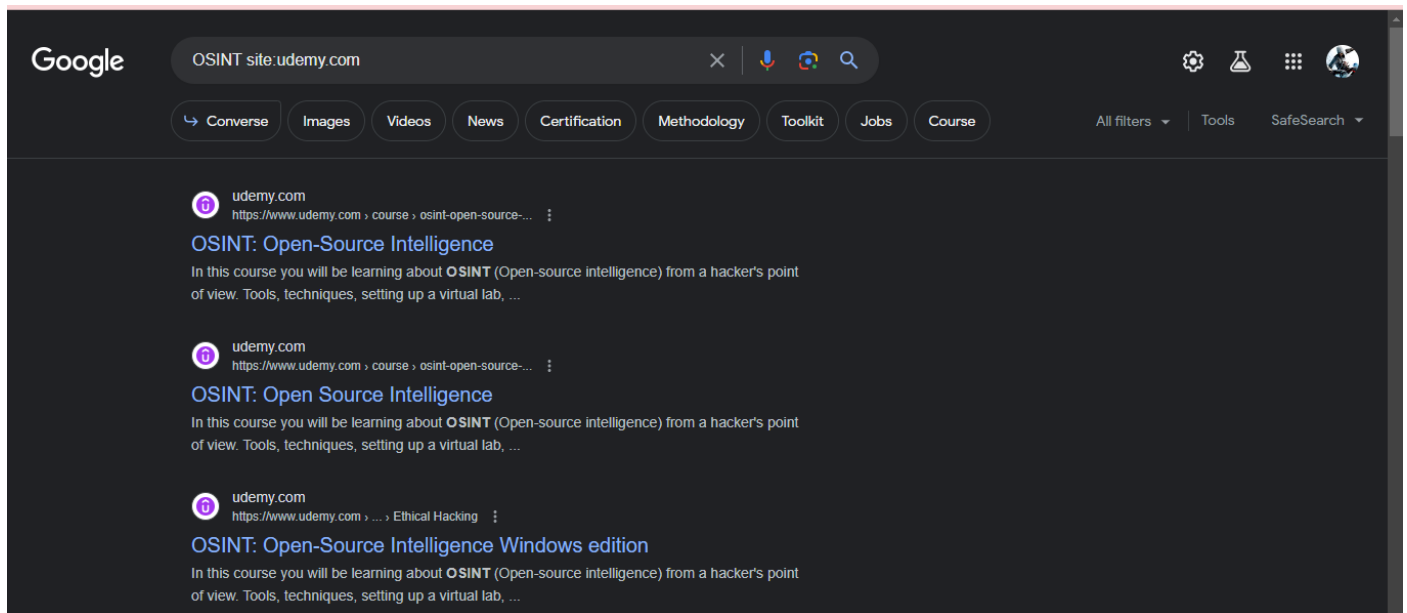
- ***** = wildcard, i.e. **"robdouglas*.com"**

The asterisk operator represents a wildcard within search strings, taking the place of words or phrases between two keywords. Investigators can use the asterisk operator to find email addresses by replacing the domain name with the wildcard character.

- **map:** = map a specific location, i.e. **map: Manhattan**

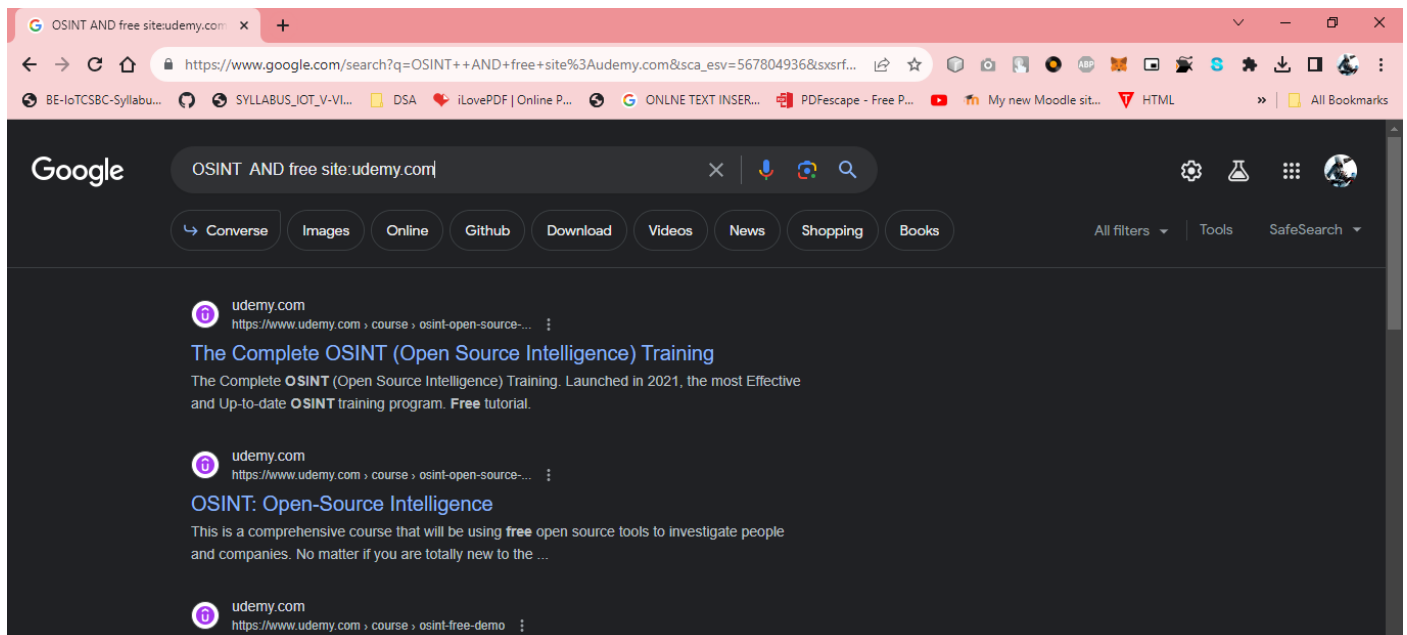
The map operator enables users to force Google to show map results for a locational search. The results show only location-specific data and do not include recent news stories. Investigators can use the map operator to focus on geospatial relevant intelligence.

Skopenow augments investigations by instantly building comprehensive, court-ready, digital reports on businesses and individuals. Skopenow collects, collates, and analyzes information from data sources, including social media, the dark web, associated vehicles, court records, and contact data.



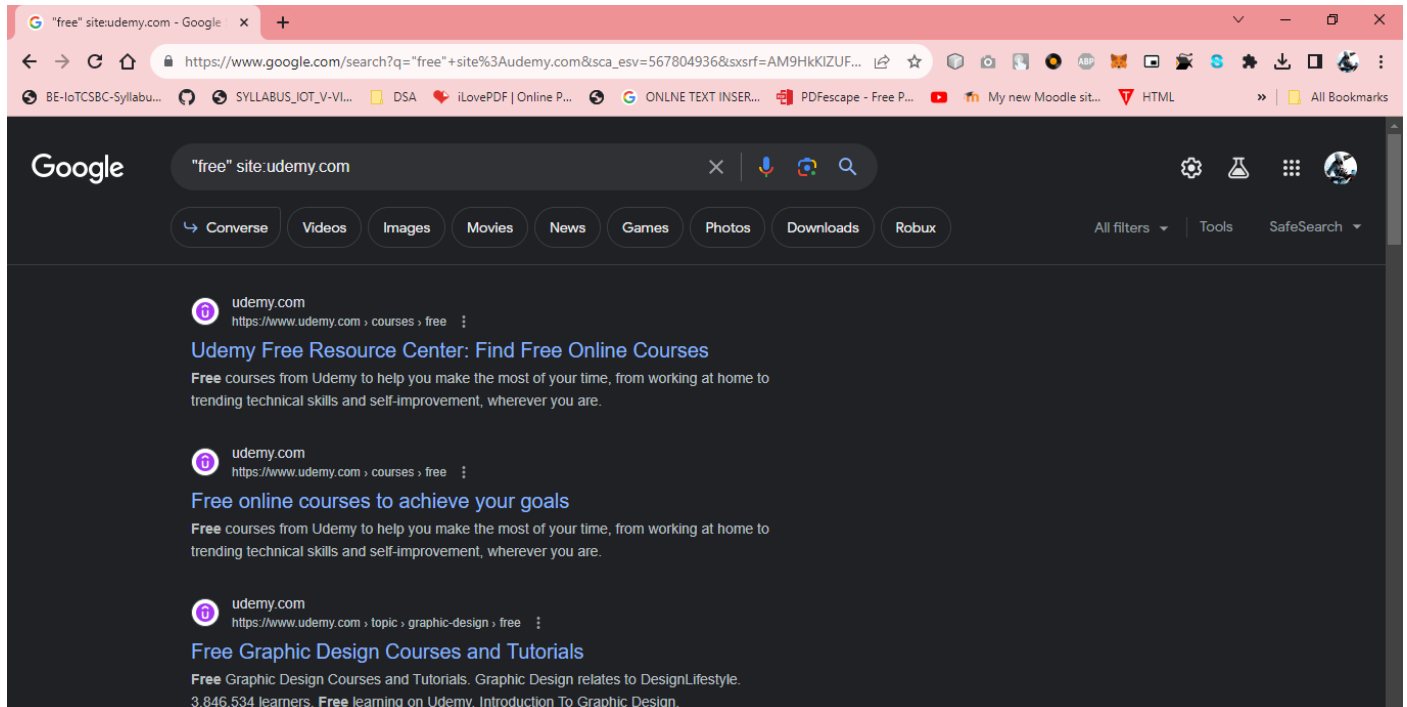
Google search results for "OSINT site:udemy.com". The search bar shows the query "OSINT site:udemy.com". The results list three courses from UDEMY.COM:

- OSINT: Open-Source Intelligence**
In this course you will be learning about **OSINT** (Open-source intelligence) from a hacker's point of view. Tools, techniques, setting up a virtual lab, ...
- OSINT: Open Source Intelligence**
In this course you will be learning about **OSINT** (Open-source intelligence) from a hacker's point of view. Tools, techniques, setting up a virtual lab, ...
- OSINT: Open-Source Intelligence Windows edition**
In this course you will be learning about **OSINT** (Open-source intelligence) from a hacker's point of view. Tools, techniques, setting up a virtual lab, ...



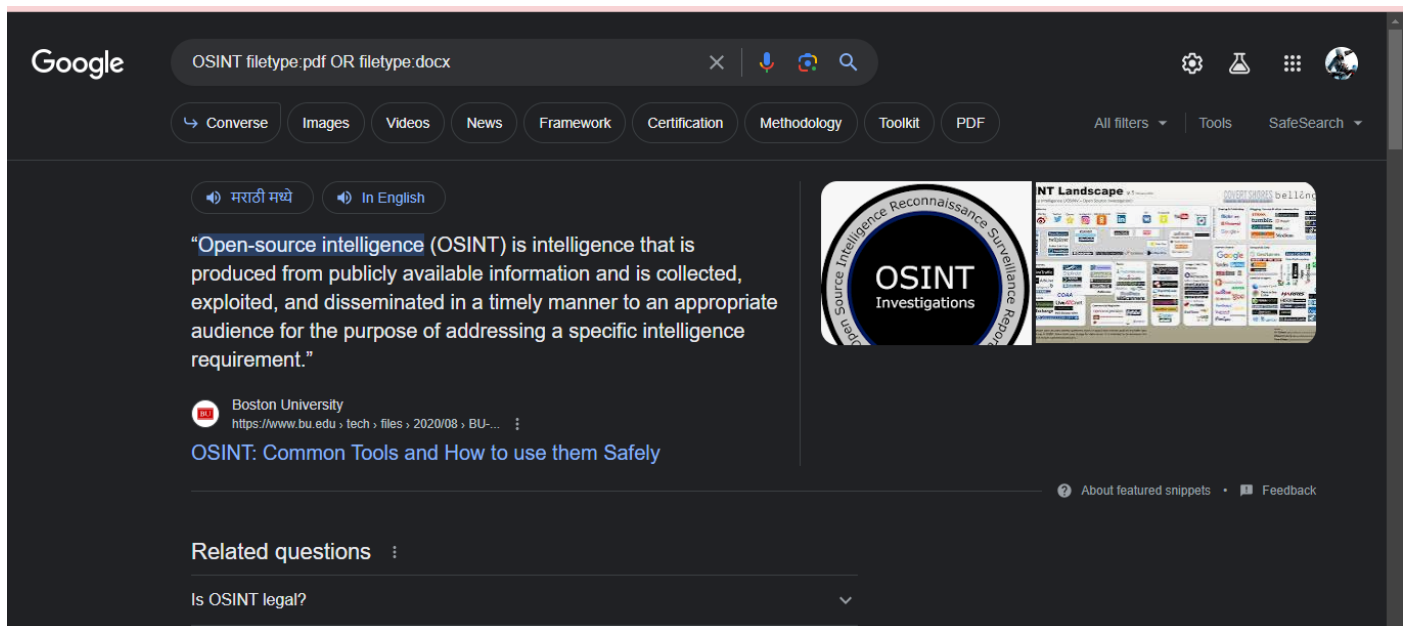
Google search results for "OSINT AND free site:udemy.com". The search bar shows the query "OSINT AND free site:udemy.com". The results list three courses from UDEMY.COM:

- The Complete OSINT (Open Source Intelligence) Training**
The Complete **OSINT** (Open Source Intelligence) Training. Launched in 2021, the most Effective and Up-to-date **OSINT** training program. **Free** tutorial.
- OSINT: Open-Source Intelligence**
This is a comprehensive course that will be using **free** open source tools to investigate people and companies. No matter if you are totally new to the ...
- OSINT: Open-Source Intelligence**
In this course you will be learning about **OSINT** (Open-source intelligence) from a hacker's point of view. Tools, techniques, setting up a virtual lab, ...



Google search results for "free" site:udemy.com. The search bar shows the query. Below the search bar, there are tabs for Converse, Videos, Images, Movies, News, Games, Photos, Downloads, and Robux. The results show three entries from udey.com:

- Udey Free Resource Center: Find Free Online Courses**
Free courses from Udey to help you make the most of your time, from working at home to trending technical skills and self-improvement, wherever you are.
- Free online courses to achieve your goals**
Free courses from Udey to help you make the most of your time, from working at home to trending technical skills and self-improvement, wherever you are.
- Free Graphic Design Courses and Tutorials**
Free Graphic Design Courses and Tutorials. Graphic Design relates to DesignLifestyle. 3,846,534 learners. Free learning on Udey. Introduction To Graphic Design.

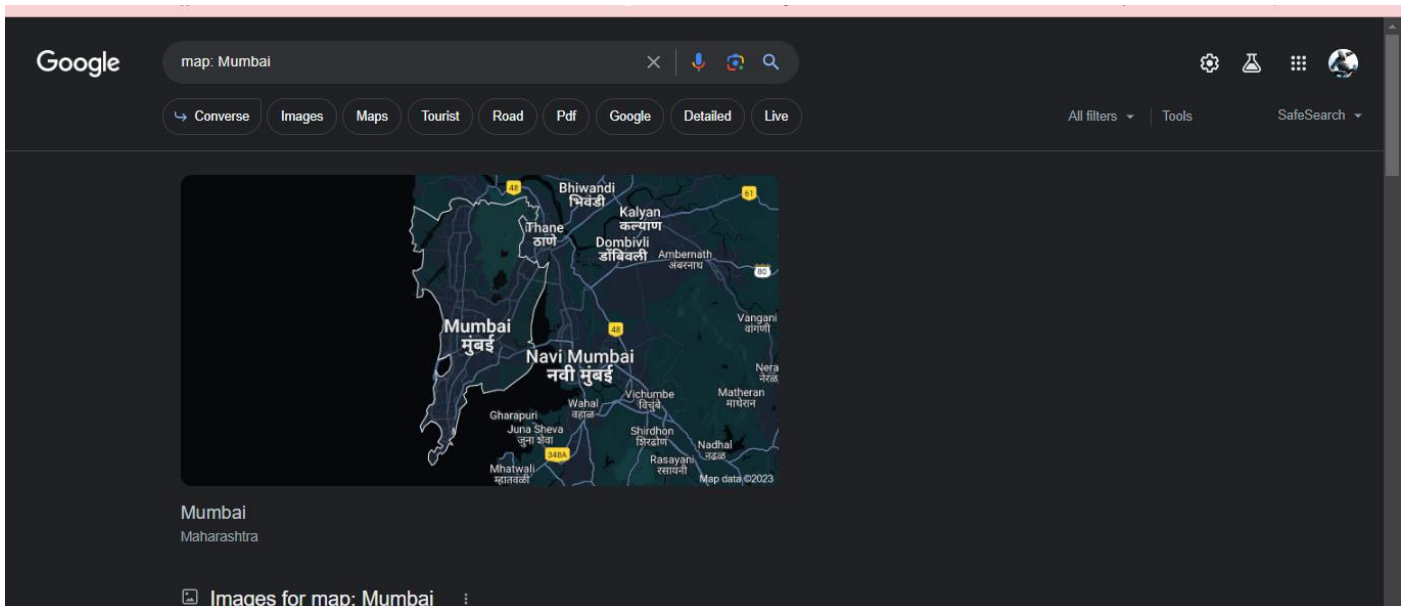
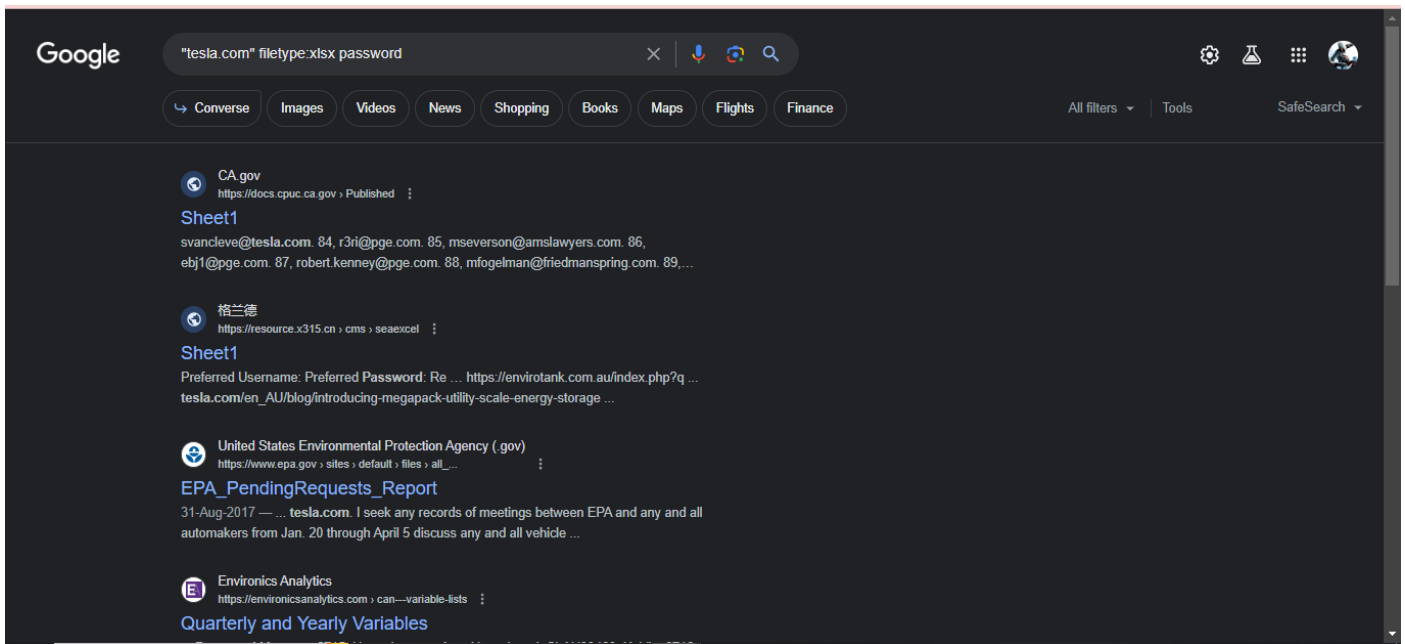


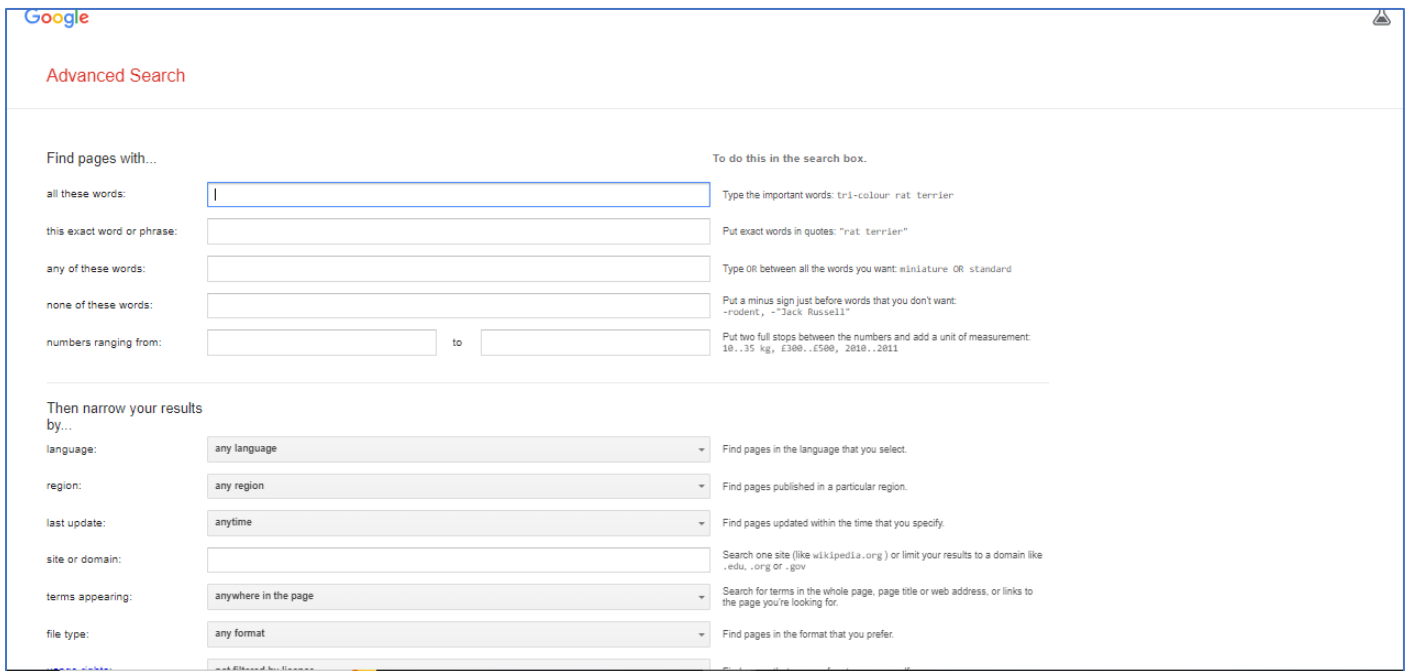
Google search results for "OSINT filetype:pdf OR filetype:docx". The search bar shows the query. Below the search bar, there are tabs for Converse, Images, Videos, News, Framework, Certification, Methodology, Toolkit, and PDF. The results show a snippet from Boston University:

"Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."

OSINT: Common Tools and How to use them Safely

Related questions: Is OSINT legal?





The image shows a screenshot of the Google Advanced Search page. At the top left is the Google logo, and at the top right is a small triangle icon. Below the logo is the text "Advanced Search". The main content area is divided into two columns. The left column is titled "Find pages with..." and contains five search criteria: "all these words:", "this exact word or phrase:", "any of these words:", "none of these words:", and "numbers ranging from:". Each criterion has a corresponding input field. The right column is titled "To do this in the search box." and provides instructions for each criterion: "Type the important words: tri-colour rat terrier", "Put exact words in quotes: 'rat terrier'", "Type OR between all the words you want: miniature OR standard", "Put a minus sign just before words that you don't want: -rodent, -'Jack Russell'", and "Put two full stops between the numbers and add a unit of measurement: 10..35 kg, £300..£500, 2010..2011". Below these columns is a section titled "Then narrow your results by..." with seven filters: "language:", "region:", "last update:", "site or domain:", "terms appearing:", and "file type:". Each filter has a dropdown menu and a description of the filter's function. At the bottom of the page, there is a search bar and a "Google" button.

● **Conclusion:**

By using OSINT dorks and cross-referencing information from multiple sources, you can critically evaluate the accuracy and reliability of news articles. This approach can help you make more informed judgments about the information you come across online.