

# OSINT (Open-Source Intelligence)

OSINT Training Course – Open-Source Intelligence Training

<https://www.youtube.com/watch?app=desktop&v=ZDtQ0bapigg>

## Search Engine OSINT –

- Use “text” to search for that exact text in the exact order.
- Use - to exclude a keyword from search results. Ex: - “nutrition -facts” will give results containing nutrition but not facts.
- `allintext:password filetype:log after:2018` is another interesting search to see unencrypted passwords.
- `filetype:xls inurl:“email.xls”` will give many email xls files.
- OR and AND are used to give results excluding or including the keywords respectively.
- Use `inurl:`, `intitle:`, `intext:`, `filetype:`, `site:` etc. Ex: - `site:obama.org filetype:pdf` will show all pdfs on the site.
- <https://coursera.org/robots.txt> will give what is allowed/disallowed on the website coursera.org.
- Shodan is used IoT search engine OSINT.
- Use archive.org as a Wayback machine.
- More on usage of symbols in Search Engine: <https://www.webnotes.com/how-to-use-shortcuts-and-symbols-in-google-search/>
- Name `-site:sitename.com` will give all results excluding searches from the selected site.

## Darknet OSINT –

- Darknet browsers – Tor, Ahmia, Haystack, Torch, Kilos (Blackmarket).
- Clustering search engines provide URLs related to the original keyword. Ex: - Biznar, Yippy (IBM Watson).
- Bielefeld Academic Search Engine (BASE) provides research papers and such.

## People, Company, and Phone Number Search –

- People search – `thatsthem.com` (name, address, phone, etc), `who.is` (domain name and IP),  
`melissa.com` (freemium)
- Company Search – google street view to verify  
`opencorporates.com`, `brownbook.net`  
govt business records service (if available)

## Document Search and Metadata –

The tool used to collect metadata – metagoofil

The Tool used to extract information from files – metaforge by chriswmorris

## Image OSINT –

- Reverse Image Search – Yandex, Google Images, TinEye(least).
- Exif data viewers – `exiftool(cli)`, Foresically, FotoForensics.

## Fixing Blurred Images –

Use gimp’s gmic for this purpose

To install gmic: `apt-get install gimp` and `apt-get install gimp gimp-gmic`

Website, social media OSINT etc are still left

## #SEARCH ENGINES

- |                     |                       |
|---------------------|-----------------------|
| 1. shodan.io        | (Server)              |
| 2. google.com       | (Dorks)               |
| 3. wigle.net        | (WiFi Networks)       |
| 4. grep.app         | (Codes Search)        |
| 5. app.binaryedge   | (Threat Intelligence) |
| 6. onyphe.io        | (Server)              |
| 7. viz.greynoise.io | (Threat Intelligence) |
| 8. censys.io        | (Server)              |
| 9. hunter.io        | (Email Addresses)     |
| 10. fofa.info       | (Threat Intelligence) |
| 11. zoomeye.org     | (Threat Intelligence) |
| 12. leakix.net      | (Threat Intelligence) |
| 13. intelx.io       | (OSINT)               |
| 14. app.netlas.io   | (Attack Surface)      |
| 15. searchcode.com  | (Codes Search)        |
| 16. urlscan.io      | (Threat Intelligence) |
| 17. publicwww.com   | (Codes Search)        |
| 18. fullhunt.io     | (Attack Surface)      |
| 19. socradar.io     | (Threat Intelligence) |
| 20. binaryedge.io   | (Attack Surface)      |
| 21. ivre.rocks      | (Server)              |
| 22. crt.sh          | (Certificate Search)  |
| 23. vulners.com     | (Vulnerabilities)     |
| 24. pulsedive.com   | (Threat Intelligence) |