

\$whoami preetham

- Creator,
FastRAPI, Vesper
- NCIIPC Pentathon
AIR 11th
- Freelance CGI/3D
Artist (45M+
views && Netflix)



@ppmpreetham

www.preetham.top/



TOPICS:

- OSINT
- Cryptography
- Malware Analysis
- Reverse Engineering
- Binary Exploitation

NOTES:



OSINT

OPEN SOURCE INTELLIGENCE

Because Stalking your crush Is Creepy, But OSINTing her
Sounds Professional AF



DISCLAIMER

INFORMATION IN THESE SLIDES ARE ONLY FOR
EDUCATIONAL PURPOSES. THE AUTHOR DISCLAIMS ALL
LIABILITY FOR THE MISUSE OF THE PROVIDED MATERIALS

TYPES OF OSINT

- SOCMINT
- SIGINT
- GEOINT
- HUMINT
- CTI
- ...etc

SOCMINT

Social Media Intelligence

GOOGLE DORKING

Hacking with Google?
BUT HOW?

GOOGLE DORKING

Operator	Description	Example
site:	Restricts search to a specific website or domain	site:example.com
filetype: or ext:	Limits results to specific file extensions (pdf, doc, xls, log, sql, env, etc.)	filetype:sql "password" ext:env
inurl:	Searches for specific text within the URL	inurl:admin inurl:login
allinurl:	Searches for multiple keywords within the URL (all must be present)	allinurl:admin login
intitle:	Searches for keywords within the web page title	intitle:"index of /"
allintitle:	Searches for multiple keywords within the title (all must be present)	allintitle:admin login
intext:	Searches for keywords within the body text of a page	intext:"confidential"
allintext:	Searches for all specified keywords in the body text	allintext:username password
cache:	Displays Google's cached version of a website	cache:example.com
link:	Finds pages that contain links to a specific URL	link:example.com
related:	Finds websites similar to a specified URL	related:example.com
info:	Provides detailed information about a website (if available)	info:example.com
inanchor:	Searches for keywords within the anchor text of links pointing to pages	inanchor:"click here"

GOOGLE HACK DB

<https://www.exploit-db.com/google-hacking-database>



USERNAME ENUMERATION

- Vesper
- Sherlock
- Maigret

VESPER

- Find anyone's social medias in just 20 seconds using their username



VESPER

- `./vesper parrothacker1`

TOUTATIS

- Instagram Enumeration tool
- Alternative: [SolG](#)



CROSSLINKED

- Linkedin Enumeration tool



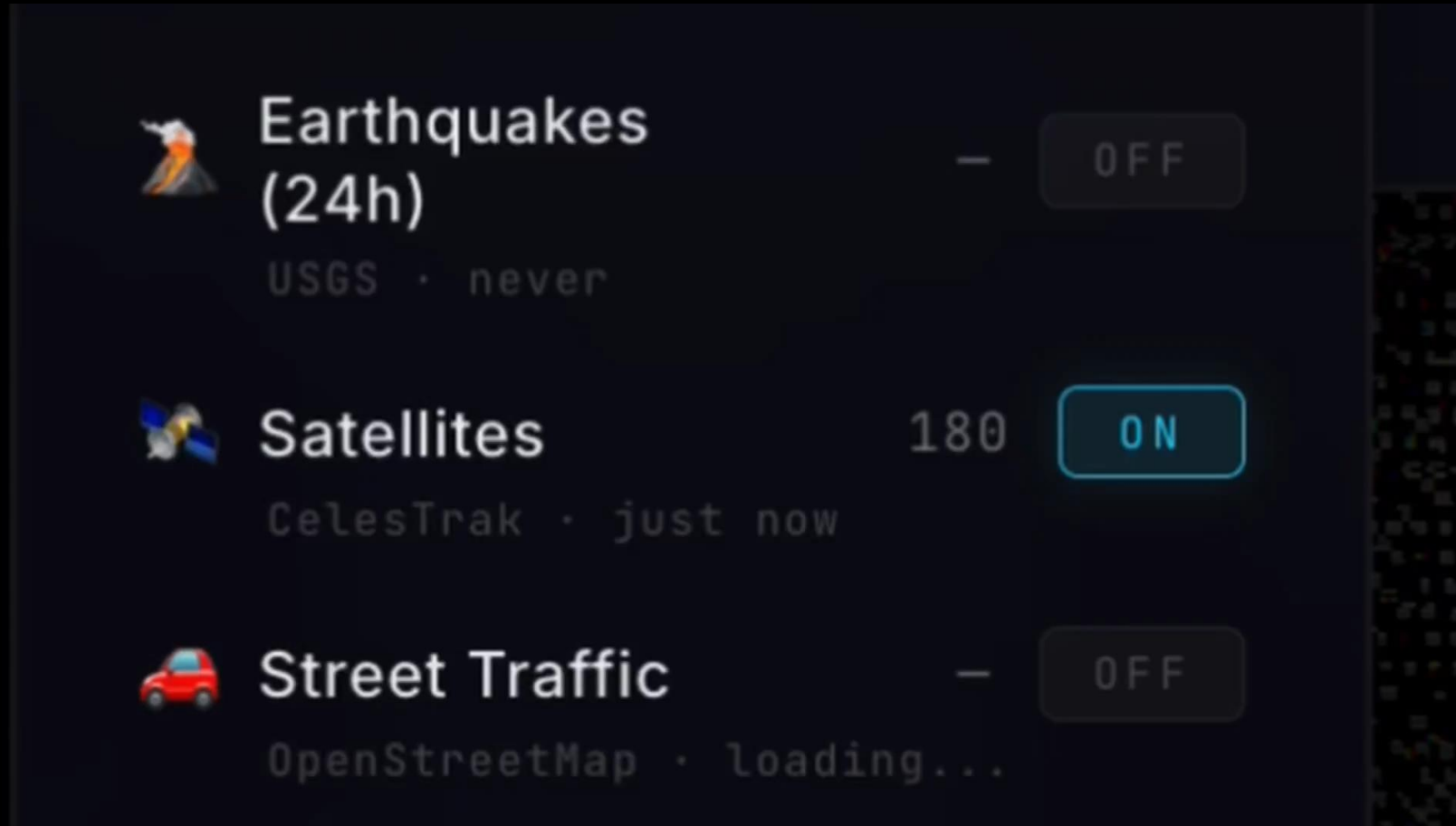
SIGINT

Signal based Intelligence

GEOINT

Geospatial Intelligence

SPATIALINTELLIGENCE.AI



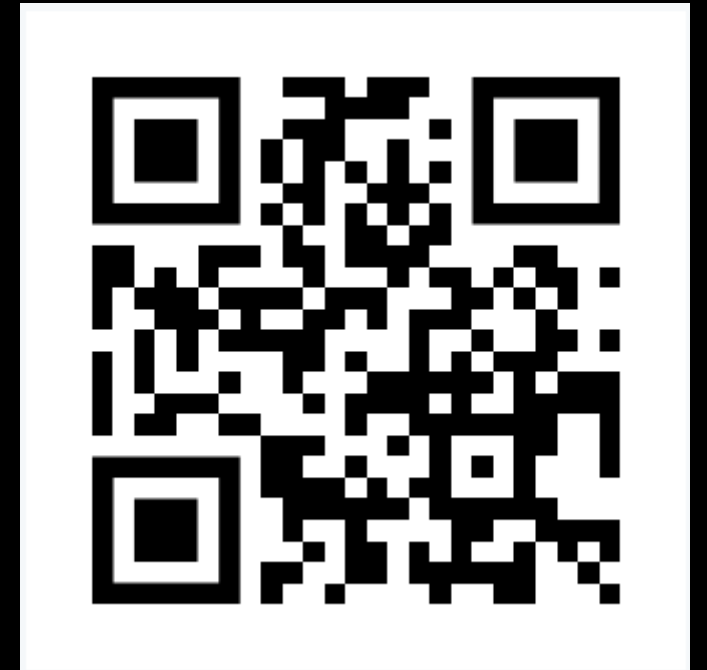
OVERPASS TURBO

- Let's you query specific things
- How many CC TV Cameras are there in Berlin?



SHODAN

- Crazy IOT devices accessing



WHAT 3 WORDS?

- Shows any location in 3 words
- `/// xxxxxx.xxxxxx.xxxxxx`



HUMINT
Human based Intelligence

IMAGE OSINT

Can you find people's name just with their face?



YES YOU CAN!

- <https://facecheck.id/>
- <https://tineye.com/>
- <https://pimeyes.com/>



SEARCH BY IMAGE

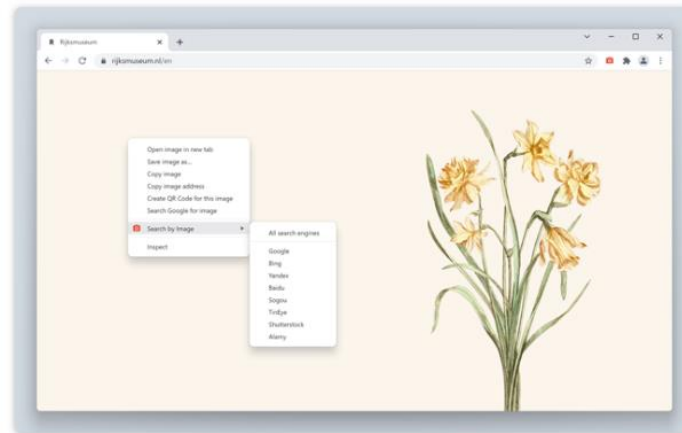
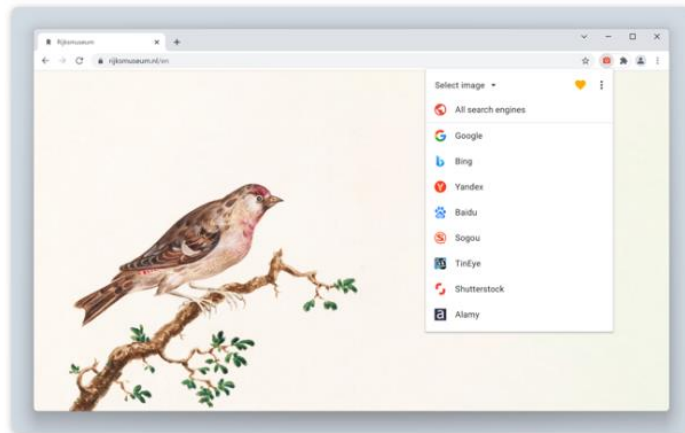


Search by Image

Remove from Vivaldi

armin.dev Featured 4.1★ (531 ratings) Share

Extension Tools 400,000 users



DOCUMENT METADATA

```
strings <filename>
```



ACTUAL OSINT

<https://gralhix.com/list-of-osint-exercises/>

CRYPTOCURRENCY

- <https://3xpl.com/bitcoin>



Cyber Threat Intelligence

INFOSECNINJA

- Real-time resources
- Shows latest attacks
- Newest Cybersec breakthroughs



HONEYDB

- <https://honeydb.io/>
- Shows recent honey pot activity

