



# Open Source Intelligence (OSINT) Handout and References



**Tuesday, June 21, 2022**

**Valarie Findlay**

International Association of Law Enforcement Intelligence Analysts (IALEIA)  
American Society for Evidence-Based Policing (ASEBP)



# OSINT manual searches and queries

## Must have sources:

- <https://osintframework.com/>
- <https://github.com/jivoi/awesome-osint>
- US DOJ's Cyber Unit's Guidance on OSINT:  
<https://www.justice.gov/criminal-ccips/page/file/1252341/download>

## Common free OSINT / SOCMINT tools:

- Whois data <http://whoxy.com>
- Company data <http://opencorporates.com>
- Person data <http://truepeoplesearch.com>
- Twitter data <http://tweetbeaver.com>
- EXIF data <http://exif.regex.info/exif.cgi>
- Archive <http://archive.org>



# OSINT tool links

- Web 3.0 and its impact on SOCMINT and OSINT, Ginsberg5150's page on github: <https://github.com/Ginsberg5150/Web3> )
- Google is a good resource using Boolean searches and Reverse Image searches.
- Facebook Lookup ID (<https://lookup-id.com>)
- Whois data <http://whoxy.com>
- Company data <http://opencorporates.com>
- Person data <http://truepeoplesearch.com>
- Person data <https://pipl.com>
- EXIF data <http://exif.regex.info/exif.cgi>
- Archive <http://archive.org>

# Twitter tool links



- **Twitter data** <http://tweetbeaver.com>
- **Twitter Developer** utilizes the specialized operators. Find related Tweets with more precision: <https://developer.twitter.com/en/docs/tweets/rules-and-filtering/overview/standard-operators>.
- **All My Tweets** (<https://www.allmytweets.net>) shows all public tweets posted by any Twitter account on one page.
- **Trendsmap** (<https://www.trendsmap.com>) shows the most popular trends, hashtags, and keywords on Twitter from anywhere around the world.
- **First Tweet** (<http://ctrlq.org/first>) finds the first tweet of any search keyword or link.
- **Social Bearing** (<https://socialbearing.com/search/followers>) analyzes Twitter followers of any particular account (a maximum of 10,000 followers can be loaded).
- **Spoonbill** (<https://spoonbill.io>) monitors profile changes from profiles you follow on Twitter.

# OSINT tool suites



**SHODAN:** <https://www.shodan.io/>

Shodan is a search engine that lets users search for various types of servers connected to the internet using a variety of filters. Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client. [Wikipedia](#) ... Shodan Search, Shodan Trends, Shodan Maps, Shodan Images and Shodan Monitor

**x1 Social Discovery:** <https://www.x1.com/>

X1 Social Discovery provides for a case-centric workflow from search and collection through production in searchable native format, while preserving critical metadata, and enables reactive data collection capabilities for social media and website collections in a manner consistent with evidentiary best practices. An end-to-end workflow and case-driven tool, X1 can find, analyze, collect and load into an advanced review platform for all types of data.

**Maltego:** <https://www.maltego.com/>

Maltego provides a library of data transforms for discovery from open sources and visualizes information in a graph format, suitable for link analysis and data mining.

# OSINT tool suites



**Recon-ng:** <https://github.com/lanmaster53/recon-ng>

A little different, Recon-NG is a web Reconnaissance tool written in Python, similar to Metasploit 1 and Metasploit 2, that has many modules with database interactions, interactive help, and command completion. Recon-ng is free and available on GitHub.

**SpiderFoot:** <https://www.spiderfoot.net/>

SpiderFoot is a scanning tool for internet and dark web onion sites and allows automation of SOCMINT for scenario-based or subject area focus for threat intelligence, asset discovery, attack surface monitoring or security assessments.

# OSINT platforms and feeds



**ShadowDragon:** <https://shadowdragon.io/>

Uncover identities, correlations, networks of associates (social – not social media - network analysis), and available geographical information in just minutes.

**FiveCast:** <https://www.fivecast.com/>

Fivecast ONYX enables automated monitoring of large sets of data to identify a wide range of threats, such as group violence, protest activity or lone actor activity. Broadens the reach of law enforcement, intelligence and event management teams, ensuring cost efficient, automated risk detection requiring a smaller investment of human capital.

**Flashpoint:** <https://flashpoint.io/>

Flashpoint Intelligence Platform grants access to an archive of finished intelligence reports, data from illicit forums, marketplaces, chat services, blogs, paste sites, technical data, card shops, and vulnerabilities, in a single, finished intelligence experience. Also merges with Palantir.

# OSINT preservation tool links



**Pagefreezer:** <https://www.pagefreezer.com/>

Pagefreezer automatically archives websites, social media, mobile text messages and enterprise collaboration platforms through its suite of archiving software solutions.

**WebPreserver:** <https://www.pagefreezer.com/webpreserver/>

WebPreserver is a subscription-based Chrome Extension developed by PageFreezer that captures webpages, social media pages, videos and even complete websites in evidentiary quality. Collections can be exported to PDF, MHTML and WARC along with a collection report.

**PageVault:** <https://www.page-vault.com/>

PageVault is comparable alternative to WebPreserver that provides exemplary capabilities to expand, preserve and present lengthy posts.



# Twitter Developer - Advanced Operators



×

Advanced search

Search

Words

All of these words

Example: what's happening · contains both "what's" and "happening"

This exact phrase

Example: happy hour · contains the exact phrase "happy hour"

Any of these words

Example: cats dogs · contains either "cats" or "dogs" (or both)

None of these words

Example: cats dogs · does not contain "cats" and does not contain "dogs"

These hashtags

×

Advanced search

Search

From these accounts

Example: @Twitter · sent from @Twitter

To these accounts

Example: @Twitter · sent in reply to @Twitter

Mentioning these accounts

Example: @SFBART @Caltrain · mentions @SFBART or mention

Filters

Replies

Include replies and original Tweets

Only show replies

×

Advanced search

Search

Engagement

Minimum replies

Example: 280 · Tweets with at least 280 replies

| Operator                          | Finds Tweets...                                                            |
|-----------------------------------|----------------------------------------------------------------------------|
| watching now                      | containing both "watching" and "now". This is the default operator.        |
| "happy hour"                      | containing the exact phrase "happy hour".                                  |
| love OR hate                      | containing either "love" or "hate" (or both).                              |
| beer -root                        | containing "beer" but not "root".                                          |
| #haiku                            | containing the hashtag "haiku".                                            |
| from:interior                     | sent from Twitter account "interior".                                      |
| list:NASA/astronauts-in-space-now | sent from a Twitter account in the NASA list astronauts-in-space-now       |
| to:NASA                           | a Tweet authored in reply to Twitter account "NASA".                       |
| @NASA                             | mentioning Twitter account "NASA".                                         |
| politics filter:safe              | containing "politics" with Tweets marked as potentially sensitive removed. |
| puppy filter:media                | containing "puppy" and an image or video.                                  |
| puppy -filter:retweets            | containing "puppy", filtering out retweets                                 |

# Intelligence X and Facebook Graph Searcher

**Intelligence X** (<https://intelx.io>) develops and maintains search engine and data archives and uses unique selectors, i.e. specific search terms, such as email addresses, domains, URLs, IPs, CIDRs, Bitcoin addresses, IPFS hashes, etc.

It can search the darknet, document sharing platforms, whois data, public data leaks and other keeps a historical data archive of results, similar to the Wayback Machine from archive.org does.

Intelligence X's Facebook Graph Searcher: <https://intelx.io/tools?tab=facebook>

# Closer Look at Intelligence X



\_IntelligenceX

[About](#) [Product](#) [Blog](#) [Tools](#) [Integrations](#)  

[Login](#)

[Sign up](#)

Third Party Search:

 [General](#)

 [Email](#)

 [Domain](#)

 [IP](#)

 [Bitcoin](#)

 [Image](#)

 [Username](#)

 [Person](#)

 [Phone Number](#)

 [Location 2 Map](#)

 [File](#)

 [VIN](#)

 [Hash](#)

 [Google Analytics](#)

## Facebook Graph Searcher

Note: You need to be logged in at Facebook!

### Posts in a particular date

[Search](#)

### Posts in a particular month

[Search](#)

### Posts in an interval

From

to

[Search](#)

### Posts from someone posting about something

ID of the user

Talking about

# Closer Look at Intelligence X



Intelligence X's Alternative Facebook Graph Searcher that cased in 2019:

<https://intelx.io/tools?tab=facebook>

\_IntelligenceX

[About](#) [Product](#) [Blog](#) [Tools](#) [Integrations](#)  

[Login](#)

[Sign up](#)

Search

IntelX Tools:

 [Magic File Tool](#)

 [Validate Emails](#)

 [GeoIP Lookup](#)

 [Encoding](#)

 [URLs](#)

Social Media Tools:

 [Facebook](#)

 [Twitter](#)

 [LinkedIn](#)

 [Telegram](#)

 [YouTube](#)

Other:

 [Link Collection](#)

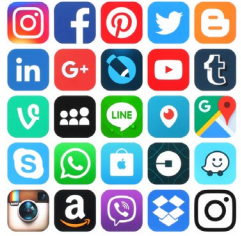
## Alternative Facebook Graph Searcher

This tool is based on the [sowdust code](#). Disclaimer: It is your responsibility to comply with the Facebook Terms of Service.

For some searches, using a keyword is necessary. If you don't want to filter via keyword, try to leave this field blank at first. If you get no results, you can also try to add more "neutral" filters (i.e.: sort by chronological order). If it still doesn't work, try to put the name of the entity you are filtering for as a keyword. For example, if you are looking for people living in London, just use "london" as a keyword.

### Search

What do you want to search:



# Closer Look at Intelligence X

Intelligence X's Dark Web Search Engine:

<https://intelx.io/>

Dark web search engines are a very specialized tool; since there is no central Tor .onion registry, no engine can cover all pages. Other challenges are finding the .onion links, the data size to be searched, data formats, and depth of crawling.

Some engines endeavour to cover these challenges, but Intelligence X is the most robust. This is a comparison of Intelligence X capabilities to other engines:

|                    | Intelligence X | Ahmia   | Torch   | Not Evil | Haystack       | DarkSearch |
|--------------------|----------------|---------|---------|----------|----------------|------------|
| Darknet Tor        | Yes            | Yes     | Yes     | Yes      | Yes            | Yes        |
| Darknet I2P        | Yes            | Yes     | No      | No       | No             | No         |
| Cache              | Yes            | No      | Yes     | No       | Yes (Premium)  | No         |
| Historical Archive | Yes            | No      | No      | No       | Yes (Premium)  | No         |
| Download           | Yes            | No      | No      | No       | ?              | No         |
| Safe Inline View   | Yes            | No      | No      | No       | No             | No         |
| API                | Yes            | No      | No      | Yes      | Yes (Premium)  | Yes        |
| Search via         | Selector       | Keyword | Keyword | Keyword  | Keyword, Regex | Keyword    |

# Closer Look at Intelligence X

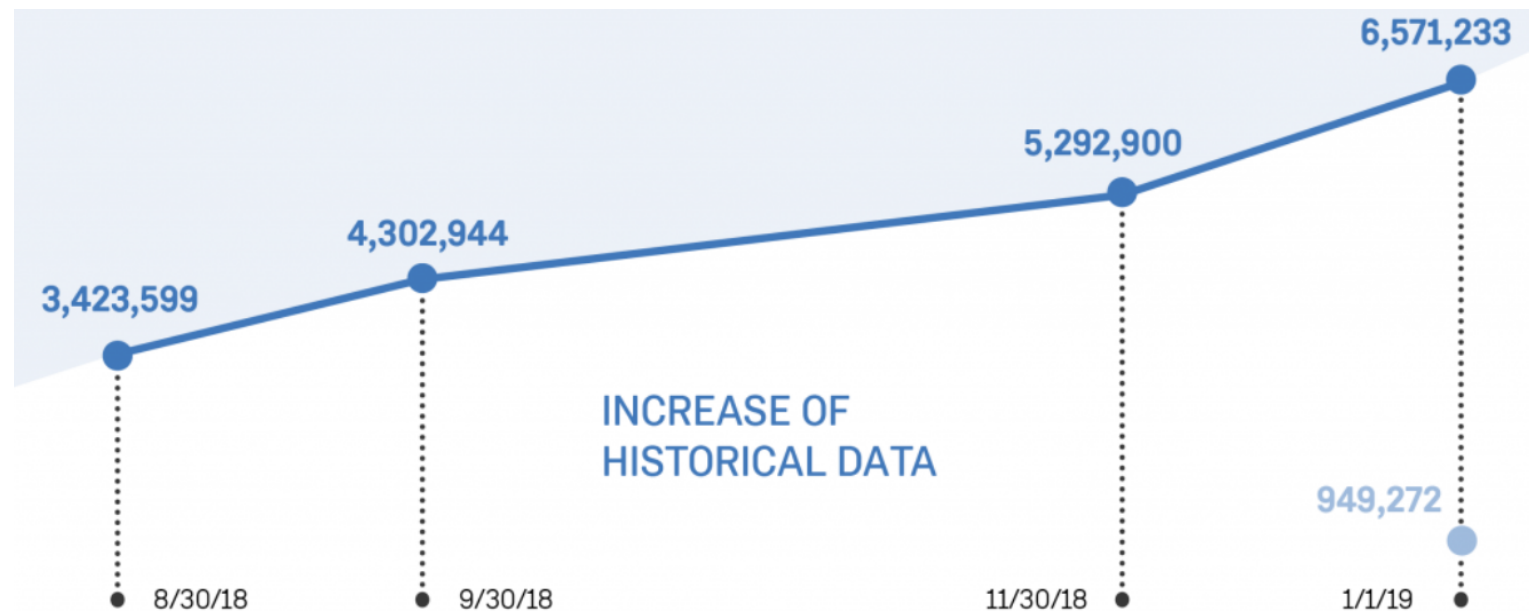


Intelligence X's Dark Web Search Engine:

<https://intelx.io/>

Intelligence X has access to over 79M records, through their search engines, including 10,197,379 items indexed for Tor and 1,557,915 items for I2P, and in any supported file format (HTML, text, PDF, eBooks, Word, Excel and PowerPoint files).

Intelligence X also has 2,250,020 .onion addresses indexed and 3,565 .i2p domains listed.



# SOWSearch.info

SOWSearch  
(<https://SOWSearch.info>)

SOWSearch, a former project on github, provides extensive search capabilities on numerous artifacts: allows investigators, and others, to uncover an array of social media evidence from airstrikes in another nation to non-technical identification of illicit imagery. It does this by providing extensive searches on numerous artifacts.



## About

This page tries to be a simple interface to show how the current Facebook search function works, after [Graph search was closed](#). Although still experimental and in development, it is published in the hope it can be useful to overcome the void left by the old graph search. Any suggestion, issue, bug, proposal, contribution etc. are very welcome; please open an issue on the [project's github page](#).

The tool is made by [sowdust](#) and it is completely **free** and **open**, as knowledge should be.

The initial work of understanding how the new search function works was done by [D Nemec](#) and [Henk Van Ess](#) and summarized [here](#).

## Notes

**For some searches, using a keyword is necessary.** If you don't want to filter via keyword, try to leave this field blank at first. If you get no results, you can also try to add more "neutral" filters (i.e.: sort by chronological order). If it still doesn't work, try to put the name of the entity you are filtering for as a keyword. For example, if you are looking for people living in London, just use "london" as a keyword.

**WARNING! Do not copy and paste** values inside the below forms from unknown sources unless you first inspect their content: pasting malicious information may result in a [Cross-Site scripting](#) attack.

## Search

What do you want to search:

-- select a search type -- ▾  
-- select a search type --  
Posts  
People  
Photos  
Pages  
Places  
Videos  
Events  
Top

## Updates

- 20/11/09: Small fix for new interface
- 20/01/03: Small updates
- 19/08/01: SearchBook stops working because of Facebook changes
- 19/06/17: SearchBook extension supports videos and photos search
- 19/06/17: [Searchbook extension](#)
- 10/06/12: Search for events

## Disclaimer

This is simply an html page that shows how the new Facebook search works providing a way to form search links. Make sure to read [Facebook Terms of Service](#). The authors of this page will not be held responsible for any misuse.



# Closer Look at SOWSearch.info



SOWSearch.info search capabilities mimic Facebook's Graph by searching posts, people, events, images, etc. with keyword, date range, etc. filters.

<https://SOWSearch.info>

## About

This page tries to be a simple interface to show how the current Facebook search function works, after [Graph search was closed](#). Although still experimental and in development, it is published in the hope it can be useful to overcome the void left by the old graph search. Any suggestion, issue, bug, proposal, contribution etc. are very welcome; please open an issue on the [project's github page](#).

The tool is made by [sowdust](#) and it is completely **free** and **open**, as knowledge should be.

The initial work of understanding how the new search function works was done by [D Nemec](#) and [Henk Van Ess](#) and summarized [here](#).

## Notes

**For some searches, using a keyword is necessary.** If you don't want to filter via keyword, try to leave this field blank at first. If you get no results, you can also try to add more "neutral" filters (i.e.: sort by chronological order). If it still doesn't work, try to put the name of the entity you are filtering for as a keyword. For example, if you are looking for people living in London, just use "london" as a keyword.

**WARNING! Do not copy and paste** values inside the below forms from unknown sources unless you first inspect their content: pasting malicious information may result in a [Cross-Site scripting](#) attack.

## Search

What do you want to search:

## Search Photos

Posted by

Tagged with location

Photos you have seen

## Filter by date

Start date:

End date:

## Filter by keywords

## Updates

- 20/11/09: Small fix for new interface
- 20/01/03: Small updates
- 19/08/01: SearchBook stops working because of Facebook changes
- 19/06/17: SearchBook extension supports videos and photos search
- 19/06/17: [Searchbook extension](#)
- 10/06/12: Search for events

## Disclaimer

This is simply an html page that shows how the new Facebook search works providing a way to form search links. Make sure to read [Facebook Terms of Service](#). The authors of this page will not be held responsible for any misuse.



# TwitWork

#Confinementjour17

▶ START

📄 SAVE SCREEN

🗑️ CLEAR

<> STABILIZE

OPTIONS

OUTPUT

☒ Is retweeted 551

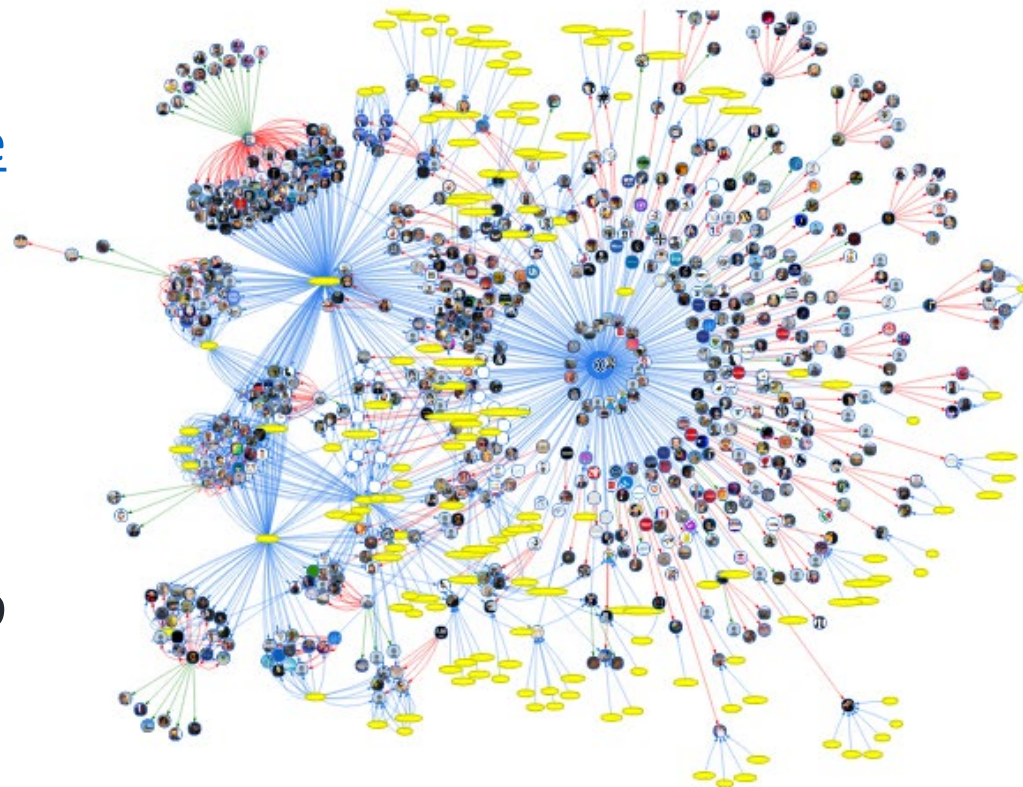
☒ Is quoted 58

☒ Is tweet 145

## TwitWork:

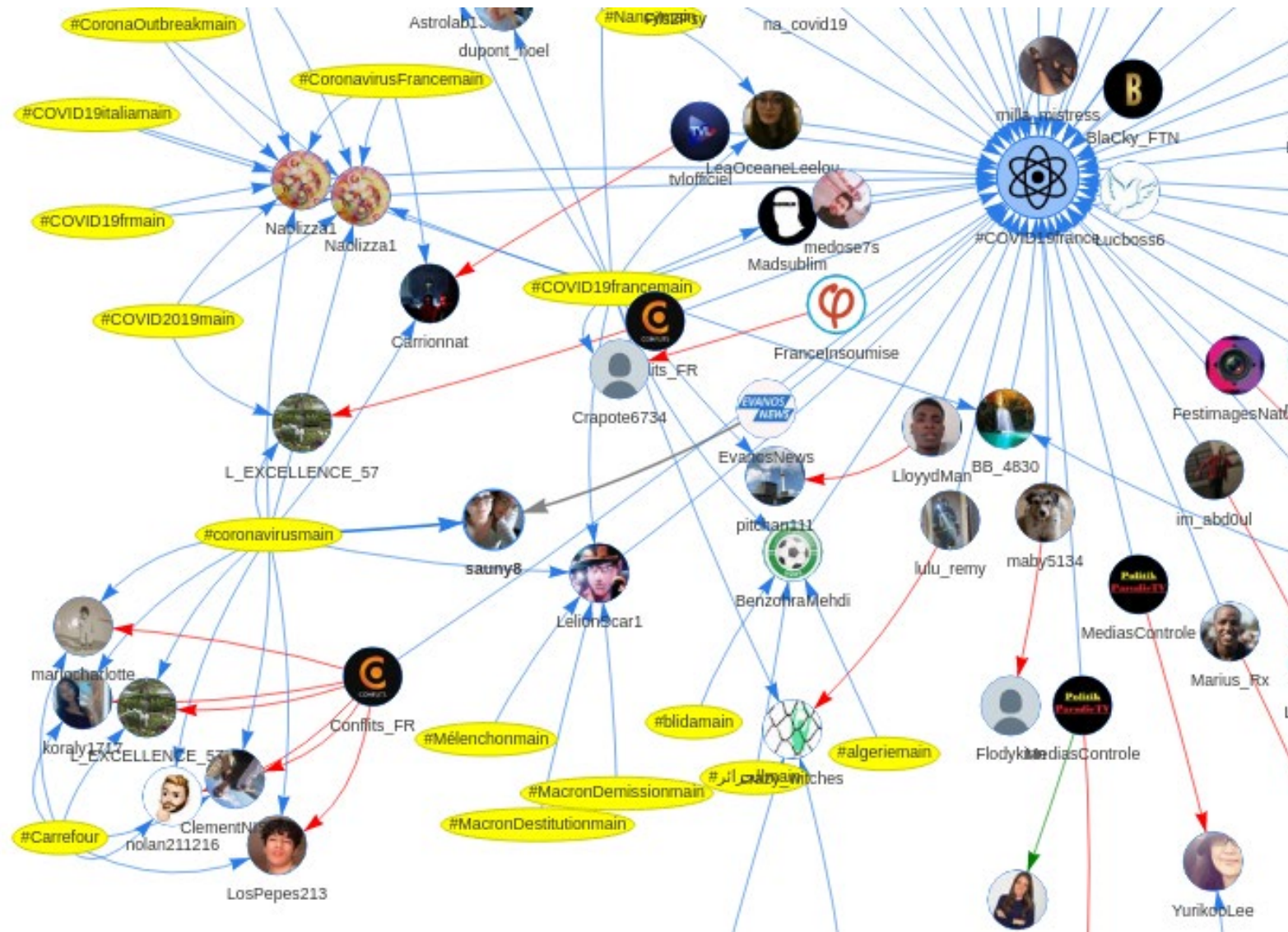
<https://github.com/atmone/r/TwitWork>

Uses the twitter stream which allows you to have a look at tweets in real-time. An input allows users to filter the flow on one (or more) keywords or on an @ based on twitter tracking



| Stats        |       |
|--------------|-------|
| KEY          | VALUE |
| Node         | 862   |
| Edge         | 1482  |
| VIEW HASHTAG |       |

# Closer Look at TwitWork



# OSINT



**Thank you for attending!**

**Should you have any questions, feel to email me directly:**

**[vfindlay@humanled.com](mailto:vfindlay@humanled.com)**