

Hermit's Cave

Things I've learned and want to share

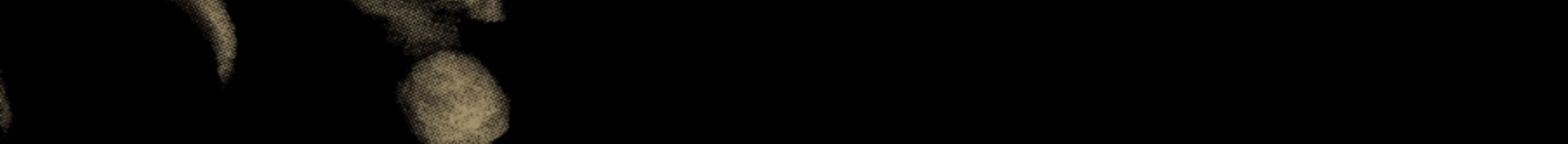


≡ MENU



OSINT: Google and LinkedIn





This is the quick-hit version of the Open Source Intelligence (OSINT) training I gave on using data from Google and LinkedIn to profile an individual or organization. As with all of the formal training, you can use the below for a quick reference, or view the full presentation here: [OSINT – Social Media \(Google and LinkedIn\) \(basic_0x08\)](#)

Google

Note: Do not use spaces between an operator (e.g. "-") and the thing it operates on. For example:

```
bob -dylan      # No Bob Dylan results
bob - dylan     # Bob Dylan shows up in results
```

Standard Google search:

```
https://www.google.com/search?q={KEYWORD}
```

Search with wildcards (e.g. "the rise of man" and "the fall of man"):

```
"the * of man"
```

Search for exact phrases:

```
"COMPLETE PHRASE OR WORDS"
```

Exclude results including a word:

```
- {TERM}
```

Search using Boolean "OR" (if text, "OR" must be capitalized)

```
{TERM_1} OR {TERM_2} OR {TERM_N}  
{TERM_1} | {TERM_2} | {TERM_N}
```

Search for file types:

```
filetype:{EXTENSION}  
ext:{EXTENSION}
```

Require that a word or phrase be present in search results:

```
{TERM} "{REQUIRED_TERM}"  
{TERM} +{REQUIRED_TERM}
```

Perform loose matches (synonyms and related terms will be used more aggressively):

```
~{TERM}
```

Filter results by country (use ISO-3166 2 character codes):

```
location:{COUNTRY_CODE}
```

Filter results by US state:

```
location:{POSTAL_STATE_CODE}
```

Filter results by reporting source:

```
source:{NAME}
```

Search for a currency:

```
${VALUE}  
€{VALUE} (etc)
```

Search for a numeric range:

```
{LOW}...{HIGH}
```

Search for a currency range:

```
${LOW}...${HIGH}  
€{LOW} . . . €{HIGH}
```

Search on social media:

```
@{TERM}
```

Search Google Groups:

```
group:{QUALIFIED_GROUP_NAME}
```

Search for hashtags:

```
#{TERM}
```

Search for results only on a particular site or TLD:

```
site:{qualified_domain}  
site:{TLD}
```

Search for results that are like a known site:

```
related:{URL}  
related:{qualified_domain}
```

Search for information about a site:

```
info:{URL}  
info:{qualified_domain}  
id:{URL}  
id:{qualified_domain}
```

Show cached versions:

```
cache:{URL}
```

Search results in the page title:

```
{TERM_A} {TERM_B} intitle:{TERM}
```

Search results in the page title, restricted to Google Groups:

```
{TERM_A} {TERM_B} insubject:{TERM}
```

Search for results that have multiple terms in the page title:

```
allintitle:{TERM_1} {TERM_2} {TERM_N}
```

Search results in the body text:

```
{TERM_A} {TERM_B} intext:{TERM}
```

Search for results that have multiple terms in the body text:

```
allintext:{TERM_1} {TERM_2} {TERM_N}
```

Search for results in page anchors:

```
{TERM_A} {TERM_B} inanchor:{TERM}
```


Search for results that have multiple terms in anchors:

```
allinanchor:{TERM_1} {TERM_2} {TERM_N}
```

Search results in the URL path:

```
{TERM_A} {TERM_B} inurl:{TERM}
```

Search for results that have multiple terms in the URL path:

```
allinurl:{TERM_1} {TERM_2} {TERM_N}
```

Get a quick definition of a term:

```
define:{TERM}
```

Get pages that link to a particular page:

```
link:{URL}  
link:{DOMAIN}
```

Find only external links to a particular page or domain:

```
link:{URL} -site:{URL_DOMAIN}  
link:{DOMAIN} -site:{DOMAIN}
```

Constrain searches to content posted in date range:

```
daterange:{START_JULIAN_DATE} - {END_JULIAN_DATE}
```

Search for phone numbers:

```
phonebook:{NAME}
```

Force results in map view:

```
map:{SEARCH TERMS}
```

LinkedIn

Generic keyword search:

```
https://www.linkedin.com/search/results/index/?keywords={KEYWORD}
```

Search for people results:

```
https://www.linkedin.com/search/results/people/?keywords={KEYWORD}
```

Search for job results:

```
https://www.linkedin.com/jobs/search/?keywords={KEYWORD}
```

Search for user content postings:

```
https://www.linkedin.com/search/results/content/?keywords={KEYWORD}
```

Search for companies:

```
https://www.linkedin.com/search/results/companies/?keywords={KEYWORD}
```

Search for groups:

```
https://www.linkedin.com/search/results/groups/?keywords={KEYWORD}
```

Search for schools:

```
https://www.linkedin.com/search/results/schools/?keywords={KEYWORD}
```

List group members:

```
https://www.linkedin.com/groups/{GROUP_ID}/members
```

List other users followed by a user:

```
https://www.linkedin.com/in/{USER_ID}/interests/influencers/
```

List companies followed by a user:

```
https://www.linkedin.com/in/{USER_ID}/interests/companies/
```

List groups a user is part of:

```
https://www.linkedin.com/in/{USER_ID}/interests/groups/
```

List schools followed by a user:

```
https://www.linkedin.com/in/{USER_ID}/interests/schools/
```

Sort by date:

```
&sortBy=DD
```

Sort by relevance:

```
&sortBy=R
```

Search within generic location (by text name of location):

```
&location={LOCATION_NAME}
```

Search within country (use ISO-3166 2 character codes):

```
&locationID={COUNTRY_CODE}%3A0
```

Additional “worldwide” search modifiers:

```
locationID=OTHERS.worldwide  
location=worldwide
```

Additional relationship searches (for people searches):

```
&facetNetwork=%5B"F"%5D    # First degree contacts  
&facetNetwork=%5B"S"%5D    # Second degree contacts
```

```
&facetNetwork=%5B"0"%5D  
&facetNetwork=%5B"F"%2C"S"%5D
```

```
# All relationships  
# Both first/second degree contacts (etc)
```

Advanced People Searching

Look for previous employers:

```
&facetPastCompany=%5B"{COMPANY_ID}"%5D
```

Look for particular industries:

```
&facetIndustry=%5B"{INDUSTRY_ID}"%5D
```

Look for profile languages (use ISO 639-1 codes):

```
&facetProfileLanguage=%5B"{LANGUAGE_CODE}"%5D
```

Look for non-profit interests:

```
&facetNonprofitInterest=%5B"{INTEREST_NAME}"%5D
```

Look for schools attended:

```
&facetSchool=%5B"{SCHOOL_ID}"%5D
```

Advanced Location Searching

First identify the location codes for each location by looking at the URL after searching for a location:

```
https://www.linkedin.com/jobs/search/?  
keywords=A&location=Dallas%2C%20Texas&locationId=PLACES.us.10-4-0-57-5    # Code is us.10-4-0-57-5
```

Do the same for a second location (or more). Join the locations by using the “f_GC” parameter and separating locationIDs with URL encoded commas (%2C), then place the last location in the locationID parameter:

```
https://www.linkedin.com/jobs/search/?f_GC=us.10-4-0-57-11%2Cus.10-4-0-57-5%2Cus.10-4-0-43-  
13&keywords=A&locationId=PLACES.us.10-4-0-57-8
```

Advanced Job Searching

You can use the same trick as the location combinations for companies. For instance:

```
https://www.linkedin.com/search/results/companies/?keywords=IBM
```

Now look at the URL for the target and read the number at the end of the URL, in this case:

```
https://www.linkedin.com/company-beta/1009/    # Code is 1009
```

Then get more companies, and use the “f_C” parameter to join them:

```
https://www.linkedin.com/jobs/search/?f_C=6504%2C10887310%2C2620735%2C1009&keywords={KEYWORD}
```

List employees of a company:

```
https://www.linkedin.com/search/results/people/?facetCurrentCompany=%5B%22{COMPANY_ID}%22%5D
```

SHARE THIS:



Be the first to like this.

RELATED

[OSINT: Twitter and Facebook](#)
In "Hacking"

[OSINT: DNS](#)
In "Hacking"

[Intro to Cryptography \(Part 1 of 3\)](#)
In "Cryptography"



Published by Hermit

 May 23, 2017



[View all posts by Hermit](#)



Hacking, OSINT, QuickHits



dorking, google, Hacking, linkedin, OSINT, QuickHits



Bruteforcing ESSID Values



Search Engines

COMMENTS ARE CLOSED.

Search ...



ARCHIVES

» [May 2020](#)

» [April 2020](#)

- » September 2019
- » June 2019
- » March 2019
- » February 2019
- » January 2019
- » December 2018
- » November 2018
- » October 2018
- » September 2018
- » July 2018
- » June 2018
- » May 2018
- » January 2018
- » September 2017
- » August 2017
- » July 2017
- » June 2017
- » May 2017
- » April 2017
- » March 2017
- » February 2017
- » January 2017

» [December 2016](#)

» [October 2016](#)

CATEGORIES

BadgeLife

Coding

Cryptography

CTF Lab

CTFs

Defense

ESXi

Hacking

Hardware

Internet

Metasploit

Networking

OSINT

PowerShell

Protocols

QuickHits

Theory

TILFH

Tools

Tutorials

Uncategorized

VMWare

Wireless



FOLLOW BLOG VIA EMAIL

Enter your email address to follow this blog and receive notifications of new posts by email.

Follow

RECENT POSTS

» [QuickHit: Things to Attack](#) May 22, 2020

- » [Intro to BurpSuite](#) May 19, 2020
- » [Fire Talks Online: Intro to Woodworking](#) April 1, 2020
- » [DerbyCon 9 – DomainTools CTF – Reversing](#) September 23, 2019
- » [DerbyCon 9 – DomainTools CTF – Forensics](#) September 17, 2019

POWERED BY WORDPRESS.COM.

UP ↑