

FACEBOOK OSINT

ITS FASTER THAN SPEED DATING

17 October 2013 | HITB2013KUL

Keith Lee

Jonathan Werrett

 Trustwave®
SpiderLabs®

INTRODUCTION

Keith Lee

Security Analyst, SpiderLabs, Singapore

klee@trustwave.com

<http://github.com/milo2012/osintstalker>

@keith55



Jonathan Werrett

Managing Consultant, SpiderLabs, Hong Kong

jwerrett@trustwave.com

@werrett



AGENDA

- ▶ Background / Motivation
- ▶ Introduction to GeoStalker and FBStalker tools
- ▶ Problem they solves
- ▶ GeoStalker in-depth
- ▶ FBStalker in-depth
- ▶ What you can do to protect yourself



MOTIVATION

Spend our days on “Penetration tests”

Web apps and networks

Day-in day-out

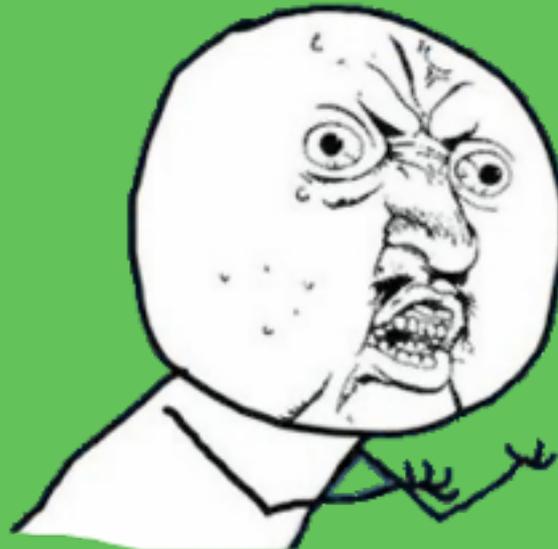


MOTIVATION

Spend our days on “Penetration tests”

Web apps and networks

Day-in day-out



BUT WAIT

Some times we get a real pentest

Set specific targets

Gain access any way you can

...



BUT WAIT

Some times we get a real pentest

Set specific targets

Gain access any way you can

...

Red team, Physical Security, Phishing
Open Source Intelligence



GEOSTALKER

Takes

- ▶ Location (address or coordinates)

Retrieves location data from

- ▶ Wigle.net (Wireless DB)
- ▶ Instagram
- ▶ Twitter
- ▶ Foursquare
- ▶ Flickr

Provides

- ▶ Wireless access points near-by
- ▶ Photos taken at that location
- ▶ Social media accounts of people who've visited

FBSTALKER

Takes

- ▶ Facebook profile user

Uses Graph Search to reverse

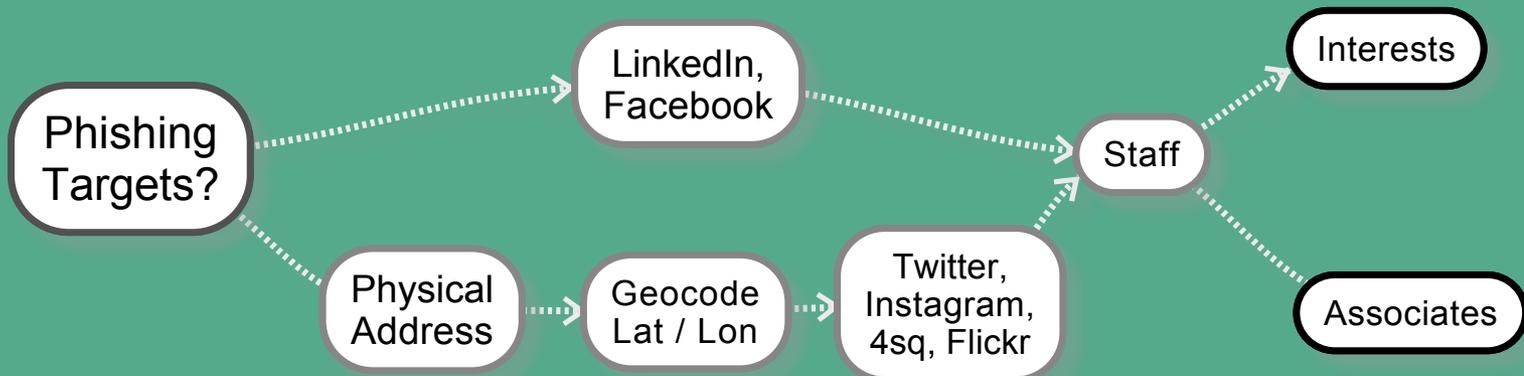
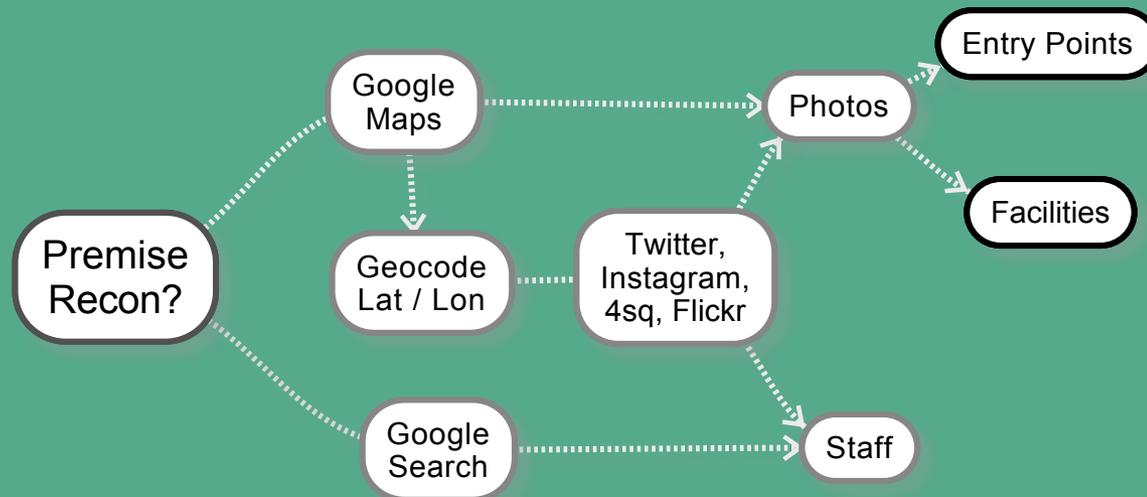
- ▶ Friends
- ▶ Likes
- ▶ Check-ins
- ▶ Comments

Provides

- ▶ Social engineering targets
- ▶ Associates of those targets
- ▶ Times online
- ▶ Interests, commonly visited places



EXAMPLE OBJECTIVES



EXAMPLES FROM ENGAGEMENTS



EXAMPLES FROM ENGAGEMENTS

FB Apps

- ▶ Indicate phishing target uses mac
- ▶ Ditch our Windows based payloads for OSX



EXAMPLES FROM ENGAGEMENTS

FB Apps

- ▶ Indicate phishing target uses mac
- ▶ Ditch our Windows based payloads for OSX

FB Friends

- ▶ Identify targets wife
- ▶ Wife runs Pilates studio
- ▶ Spear phish wife based on Pilates



EXAMPLES FROM ENGAGEMENTS

FB Apps

- ▶ Indicate phishing target uses mac
- ▶ Ditch our Windows based payloads for OSX

FB Friends

- ▶ Identify targets wife
- ▶ Wife runs Pilates studio
- ▶ Spear phish wife based on Pilates

Instagram Photos

- ▶ Client was a power utility
- ▶ Staff target found via on photos from facilities



GEOSTALKER - INTRO

Requires

- ▶ Address
- ▶ Latitude / Longitude Coordinates

Queries sources

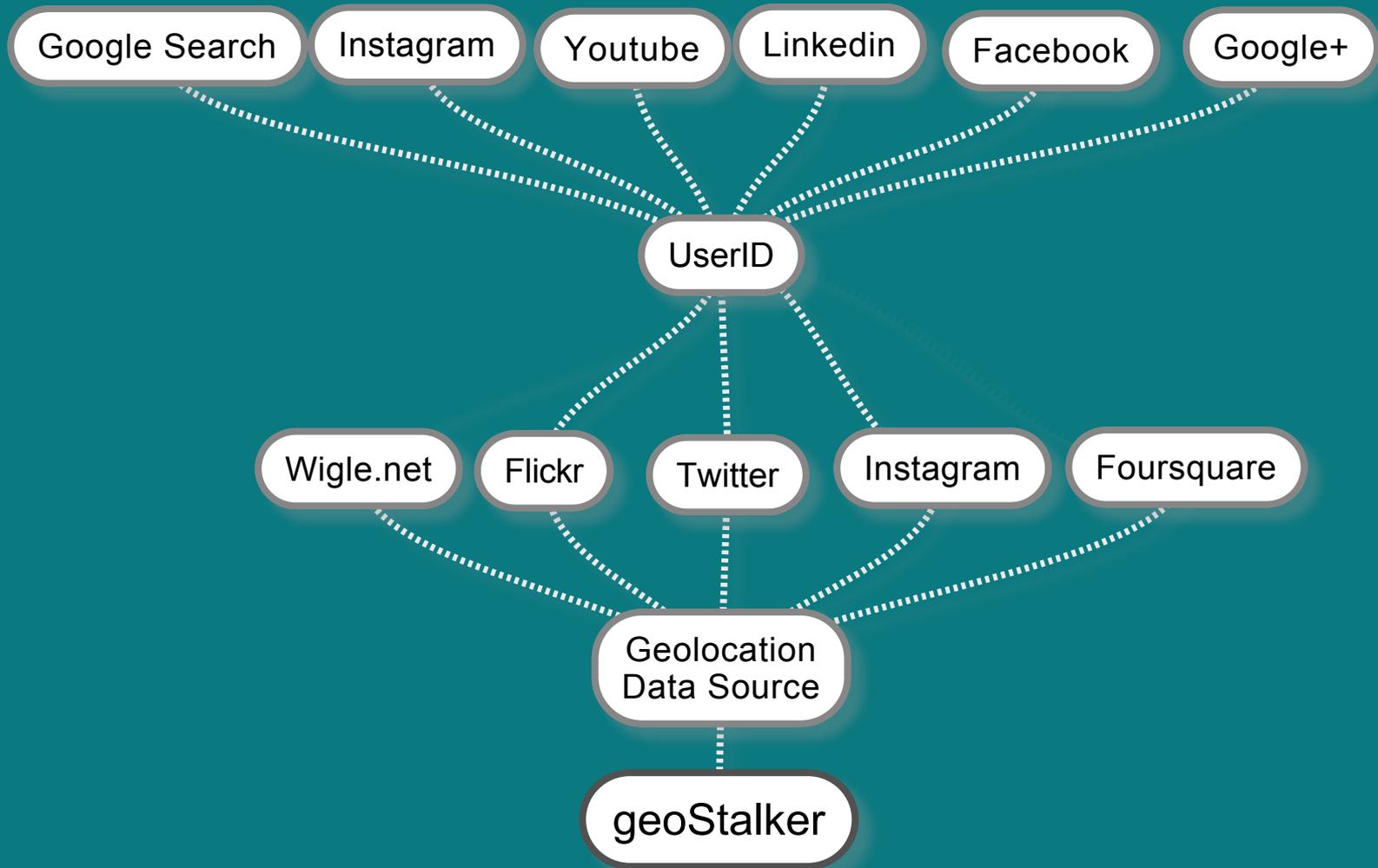
- ▶ Wigle.net (Wireless DB)
- ▶ Instagram
- ▶ Twitter
- ▶ Foursquare
- ▶ Flickr

Provides

- ▶ Wireless devices
- ▶ Photos
- ▶ Social network accounts
- ▶ Searches social network accounts for 'like' names



GEOSTALKER - APPLICATION FLOW



DEMO

GHOSTALKER



GEOSTALKER - INPUT

```
MMMMMM$ZMMMMHDIMMMMMMMNIMMMMMMIDMMMMMM
MMMMMMNINMMMMHDINMMMMMMZIMMMMMZIMMMMMMM
MMMMMMMIIMMMMI$MMMMMMMIIMMM8I$MMMMMM
MMMMMMMIINMMMIIMMMMMMMNIMMMOIIMMMMMMM
MMMMMMMOIINH$I$MMMMNI8MNIINMMMMMM
MMMMMMMMZIIZMIIMMMIIM7IIDMMMMMM
MMMMMMMMMDIIIIIIIZMIIIIII$MMMMMM
MMMMMMMM8IIIIIIIZIIIIIMMMMMMM
MMMMMMMMNIIIIIIIIIIIMMMMMMM
MMMMMM$IIIIIIIIIIII8MMMMMM
MMMMMMMIIIIZIIIZMIIIDIIIMMMMMMM
MMMMMMOIIDMDIIIZMMMIIMMOIINMMMMMM
MMMMMNIIIMMMII8MMMM$IIIZMDIIMMMMMMM
MMMMMIIZZMM8IIZMMMMMMIIMMM7IIZMMMM
MM$IIMMMOIIMMMMMMMMIIMMM8IIDMMM
MMDIZMMMMMIIMMMMMMMNII7MMMMNIIMMM
MMIOMMMMMNI8MMMMMM7IIMMMMM77MM
MO$MMMM7IIMMMMMMMMI8MMMMIMM
MIMMMMMMIIDMMMMMMMM$II7MMMM7M
MMMMMMMIIMMMMMMMMIIMMMMMDM
MMMMMMMI$MMMMMMMIIMMMMMMM
MMMMMMNINMMMMMMMOIIMMMMMMM
MMMMMMNIOMMMMMM7IMMMMMMM
MMMMMMNINMMMMMMZIMMMMMMM
MMMMMMMIIMMMMMMM8IMMMMMMM
```

```
*****
***** GeoStalker Version 1.0 HackInTheBox Release *****
*****
```

Please enter an address or GPS coordinates (e.g. 4.237588,101.131332): 1.358143,103.944826



GEOSTALKER - RUNNING

```
*****
***** GeoStalker Version 1.0 HackInTheBox Release *****
*****

Please enter an address or GPS coordinates (e.g. 4.237588,101.131332): 1.358143,103.944826
[*] Converting address to GPS coordinates: 1.358143 103.944826
[*] Downloading Wigle database from Internet
[*] Wigle database already exists: 1.358143_103.944826.dat
[*] Checking Google Docs if File Exists
[*] Logging in... Login success!
[!] File: 1.358143_103.944826.kml exists!
[*] Change: 1.358143_103.944826.kml Access to Public
[*] Logging in... Login success!
owner user testosint1@gmail.com
reader default None
Permissions change success!
[*] Extracting MAC addresses from Wigle database: 1.358143_103.944826.dat
[*] Retrieving match for vendor name: TP-LINK TECHNOLOGIES CO., LTD.
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: 2wire
[*] Retrieving match for vendor name: Cisco-Linksys LLC
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Cisco-Linksys
[*] Retrieving match for vendor name: 2Wire
[*] Retrieving match for vendor name: Aztech Electronics Pte Ltd
[*] Retrieving match for vendor name: Cisco-Linksys, LLC
[*] Retrieving match for vendor name: TP-LINK TECHNOLOGIES CO., LTD.
```



GEOSTALKER - RUNNING

```
[*] Downloading Instagram Data based on Geolocation
[*] Found http://instagram.com/valarieong (1.353651352,103.947589982)
[*] Found http://instagram.com/the__vilson (1.35708421,103.946482756)
[*] Found http://instagram.com/qkserene (1.3530119,103.9475502)
[*] Found http://instagram.com/jolenengg (1.356181544,103.944273863)
[*] Found http://instagram.com/cakebayy (1.356601622,103.946155753)
[*] Found http://instagram.com/mdsuffi34 (1.3585548,103.9456923)
[*] Found http://instagram.com/staticattack7 (1.366655089,103.950112024)
[*] Found http://instagram.com/zesablaza (1.3530664,103.95006925)
[*] Found http://instagram.com/lionravrs (1.35444017,103.94413959)
[*] Found http://instagram.com/syhrh (1.35508942,103.948098505)
[*] Found http://instagram.com/_tinc (1.35965,103.949211667)
[*] Found http://instagram.com/staticattack7 (1.36678,103.95011)
[*] Found http://instagram.com/_juicebox (1.354171506,103.945083532)
[*] Found http://instagram.com/justjiro (1.363914306,103.953111302)
[*] Found http://instagram.com/susan_vong (1.358982817,103.936033609)
[*] Found http://instagram.com/leo1992430 (1.354916,103.9507291)
[*] Found http://instagram.com/victorhooi (1.35653,103.9441)
[*] Found http://instagram.com/slyj91 (1.354732627,103.939547539)
[*] Found http://instagram.com/careyblue21 (1.355752622,103.941212641)
[*] Found http://instagram.com/nashrfredhilton (1.3577772,103.947360)
[*] Found http://instagram.com/jacquikyl (1.3529967,103.9486539)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567486,103.9472094)
[*] Found http://instagram.com/snailvhi tesingapore (1.352943594,103.939024806)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567597,103.9471805)
[*] Found http://instagram.com/abelspears (1.352668869,103.944063542)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567204,103.9472365)
[*] Found http://instagram.com/sellingcheapsquishy_ (1.3567208,103.9473055)
[*] Found http://instagram.com/conxtaxxx (1.355943009,103.942008859)
[*] Found http://instagram.com/shannonsohh (1.3595,103.940166667)
[*] Found http://instagram.com/xxiaooxuann (1.360709293,103.95300796)
[*] Found http://instagram.com/salihahyourbabygurl (1.35426069,103.951074971)
[*] Found http://instagram.com/syhrh (1.353779637,103.943500409)
[*] Found http://instagram.com/staticattack7 (1.36678,103.95011)
[*] Found http://instagram.com/yonkeezyyy (1.366642948,103.946193808)
[*] Found http://instagram.com/frnhh_ (1.3566542,103.9460057)
[*] Found http://instagram.com/jannykarma (1.35605193,103.9441048)
[*] Found http://instagram.com/syhrh (1.354931434,103.947856092)
[*] Found http://instagram.com/friendlyweirdo (1.367088449,103.950825054)

[*] Downloading Flickr Data Based on Geolocation
[*] Continue Downloading Flickr Data
```



GEOSTALKER - RUNNING

3C:EA:4F:7E:13:71	1.35665429, 103.94680786	275.215640762 meters	2Wire
C0:C1:C0:22:70:EA	1.35664415, 103.94662476	259.805809074 meters	Cisco-Linksys, LLC
64:0F:28:4E:9B:42	1.35667121, 103.94638024	230.143533895 meters	2Wire
00:10:39:A3:2F:00	1.35635722, 103.94628143	255.394849989 meters	Cisco-Linksys LLC
64:0F:28:4A:7F:AE	1.35664880, 103.94675446	270.846315942 meters	2Wire
98:2C:8E:15:CF:02	1.35664880, 103.94675446	270.846315942 meters	2Wire
F4:EC:38:AD:3B:B4	1.35667121, 103.94638024	230.143533895 meters	TP-LINK TECHNOLOGIES CO., LTD.
82:96:A0:DA:D8:B0	1.35635722, 103.94628143	255.394849989 meters	None
00:13:10:2F:80:6B	1.35666323, 103.94677734	271.905214342 meters	Cisco-Linksys, LLC
7A:54:99:4A:94:84	1.35663831, 103.94632721	235.7840465 meters	None
00:1F:B3:63:81:69	1.35665846, 103.94647217	245.984346522 meters	2Wire
B0:E7:54:F6:F6:C9	1.35635722, 103.94628143	255.394849989 meters	2Wire
64:0F:28:47:1E:BA	1.35664880, 103.94675446	270.846315942 meters	2Wire
00:0F:66:2F:4B:58	1.35665429, 103.94680786	275.215640762 meters	Cisco-Linksys
34:EF:44:79:8C:39	1.35664713, 103.94671631	267.608745764 meters	2Wire
00:26:75:57:4E:7B	1.35649900, 103.94627300	242.906112603 meters	Aztech Electronics Pte Ltd
02:2A:CA:A4:27:A4	1.35667121, 103.94638024	230.143533895 meters	None
00:12:17:0F:69:05	1.35665429, 103.94680786	275.215640762 meters	Cisco-Linksys, LLC
34:EF:44:80:01:01	1.35665429, 103.94680786	275.215640762 meters	2Wire
C0:C1:C0:22:70:EC	1.35664415, 103.94662476	259.805809074 meters	Cisco-Linksys, LLC
B0:49:7A:E2:9B:F4	1.35664880, 103.94675446	270.846315942 meters	TP-LINK TECHNOLOGIES CO., LTD.
98:2C:8E:15:FB:2A	1.35665429, 103.94680786	275.215640762 meters	2Wire
00:22:75:E7:EC:1F	1.35667121, 103.94638024	230.143533895 meters	Belkin International Inc.
00:1A:2B:88:5C:34	1.35664880, 103.94675446	270.846315942 meters	Ayecom Technology Co., Ltd.
00:1A:2B:88:49:EB	1.35664880, 103.94675446	270.846315942 meters	Ayecom Technology Co., Ltd.
FA:00:7F:FF:00:07	1.35661042, 103.94630432	236.18882303 meters	None
00:24:56:D2:37:51	1.35665429, 103.94680786	275.215640762 meters	2Wire
38:60:77:5D:6D:DD	1.35665429, 103.94680786	275.215640762 meters	PEGATRON CORPORATION
84:C9:B2:8B:A8:AE	1.35656381, 103.94628906	238.752214988 meters	D-Link International
98:2C:8E:01:28:B9	1.35664880, 103.94675446	270.846315942 meters	2Wire
74:EA:3A:8C:0D:DC	1.35644329, 103.94628143	240.10992204 meters	TP-LINK Technologies Co.,Ltd.
58:6D:8F:66:7B:1D	1.35665429, 103.94680786	275.215640762 meters	Cisco-Linksys, LLC
64:0F:28:4F:AC:66	1.35664713, 103.94671631	267.608745764 meters	2Wire
00:1C:10:03:3D:3C	1.35665429, 103.94680786	275.215640762 meters	Cisco-Linksys, LLC
00:24:56:F3:8D:E9	1.35666323, 103.94677734	271.905214342 meters	2Wire
00:26:75:4E:0F:03	1.35664237, 103.94638024	240.33410330 meters	Aztech Electronics Pte Ltd
00:1C:10:40:EF:30	1.35664880, 103.94675446	270.846315942 meters	Cisco-Linksys, LLC
3C:EA:4F:82:CE:D1	1.35665429, 103.94680786	275.215640762 meters	2Wire
00:26:50:2C:C3:B9	1.35666323, 103.94677734	271.905214342 meters	2Wire
98:2C:8E:16:10:FE	1.35664713, 103.94671631	267.608745764 meters	2Wire
00:1A:2B:4F:99:38	1.35665429, 103.94680786	275.215640762 meters	Ayecom Technology Co., Ltd.
00:23:69:2C:A1:8D	1.35666323, 103.94677734	271.905214342 meters	Cisco-Linksys, LLC
00:26:50:FC:DF:41	1.35665429, 103.94680786	275.215640762 meters	2Wire



GEOSTALKER - RUNNING

```
[*] Searching for valid accounts: https://www.facebook.com/victorhooi
[*] Searching for valid accounts: https://www.youtube.com/user/victorhooi/feed
[*] Found: https://www.youtube.com/user/victorhooi/feed

[*] Searching for valid accounts: http://instagram.com/victorhooi

[*] Searching for valid accounts on Google+
[*] Searching Google+ for Possible Matches: victorhooi

[*] Searching for valid accounts on LinkedIn
[*] Searching on LinkedIn for: victorhooi

[*] Searching for valid accounts on Google Search

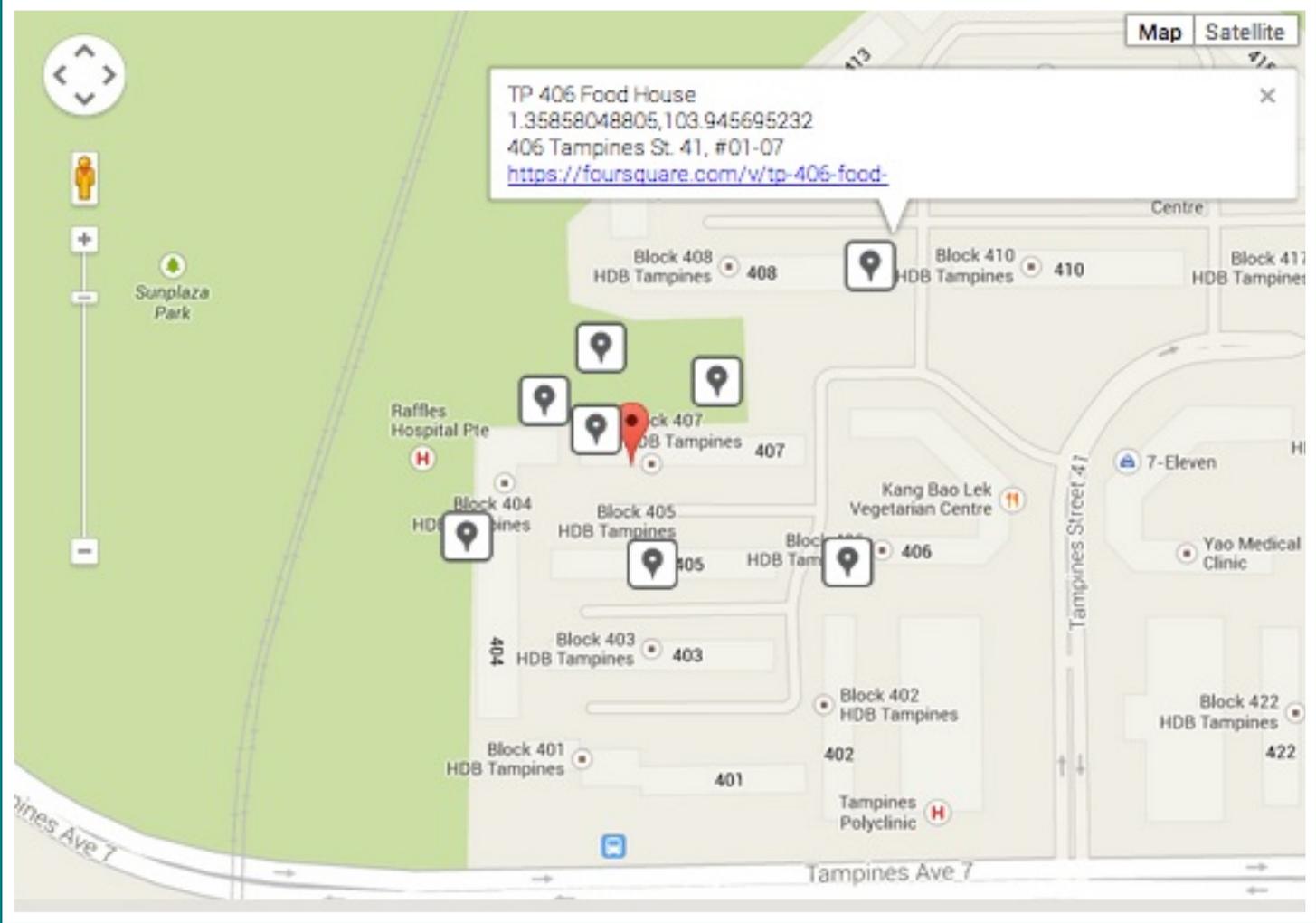
[*] Searching for valid accounts: https://www.facebook.com/slyj91
[*] Searching for valid accounts: https://www.youtube.com/user/slyj91/feed
[*] Searching for valid accounts: http://instagram.com/slyj91

[*] Searching for valid accounts on Google+
[*] Searching Google+ for Possible Matches: slyj91

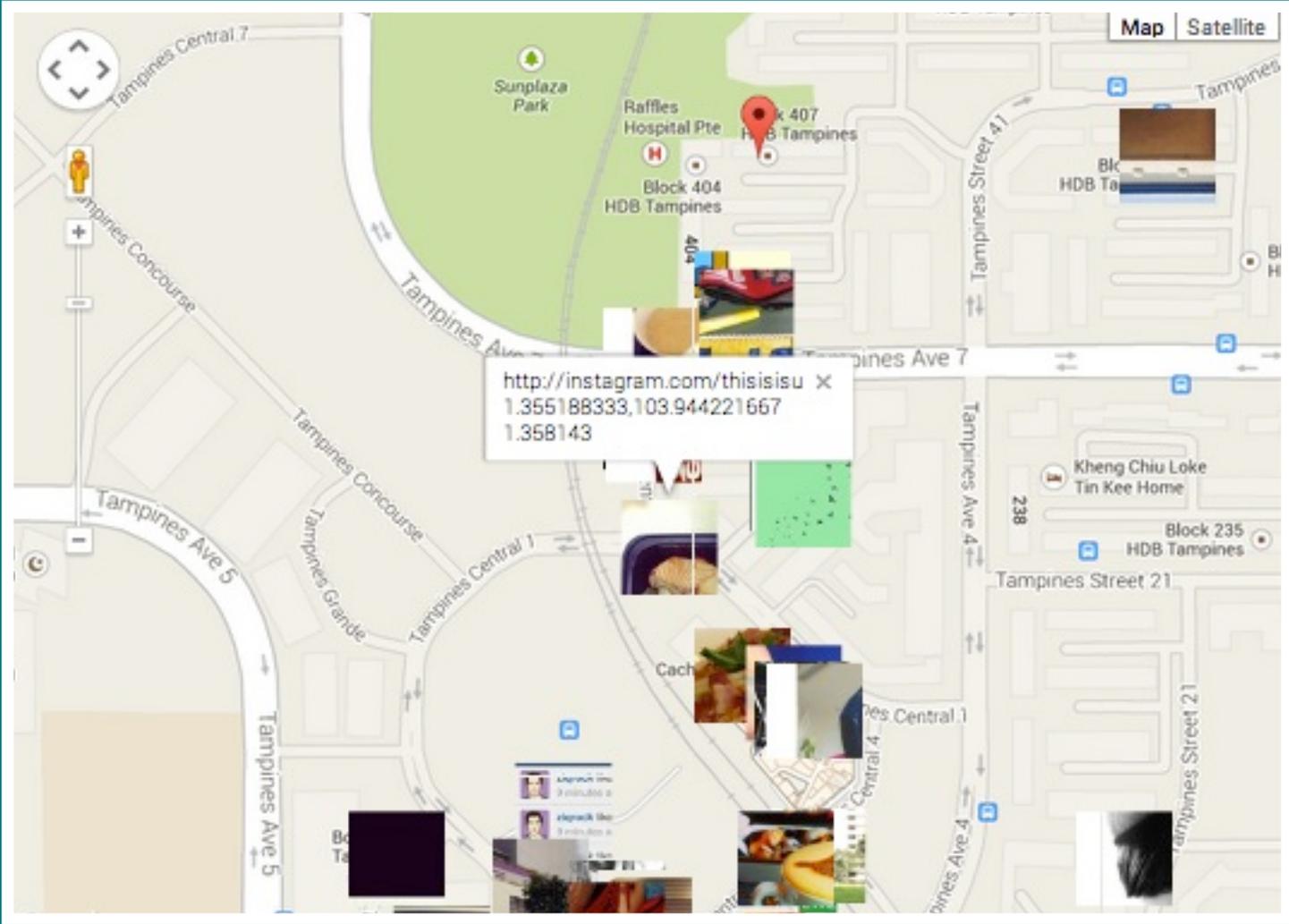
[*] Searching for valid accounts on LinkedIn
[*] Searching on LinkedIn for: slyj91
```



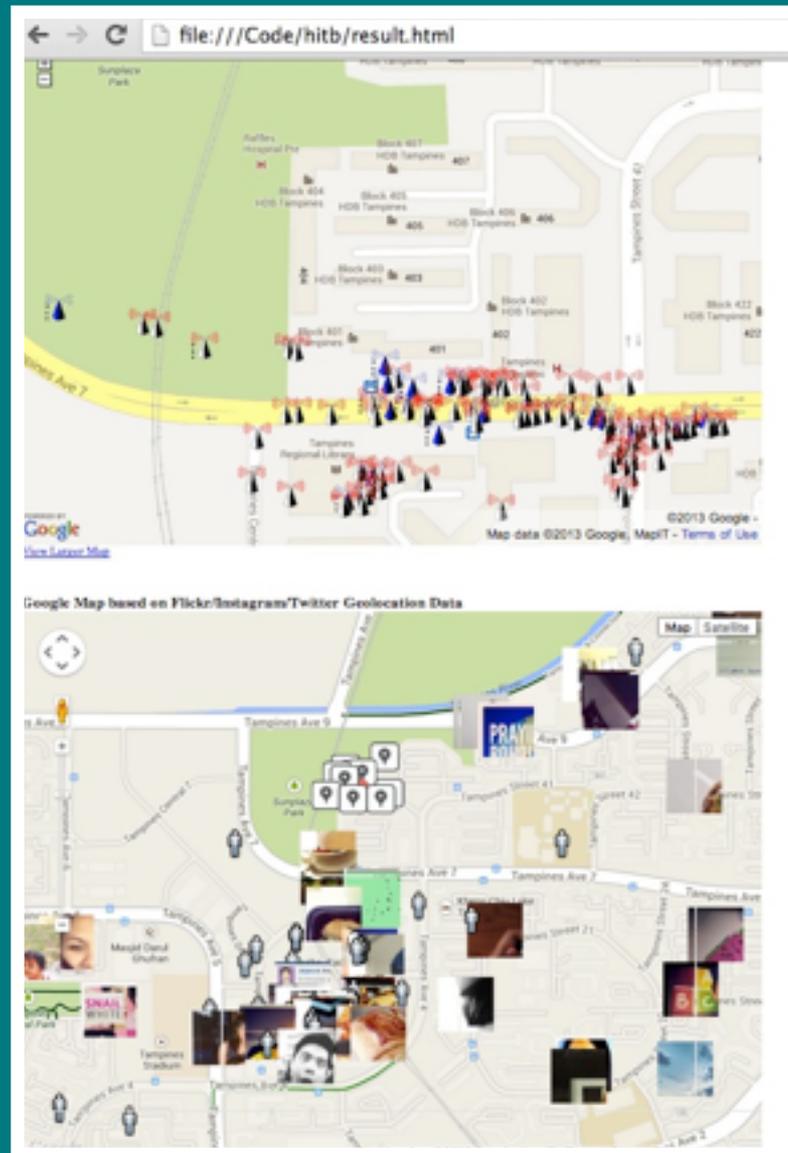
GEOSTALKER - FOURSQUARE



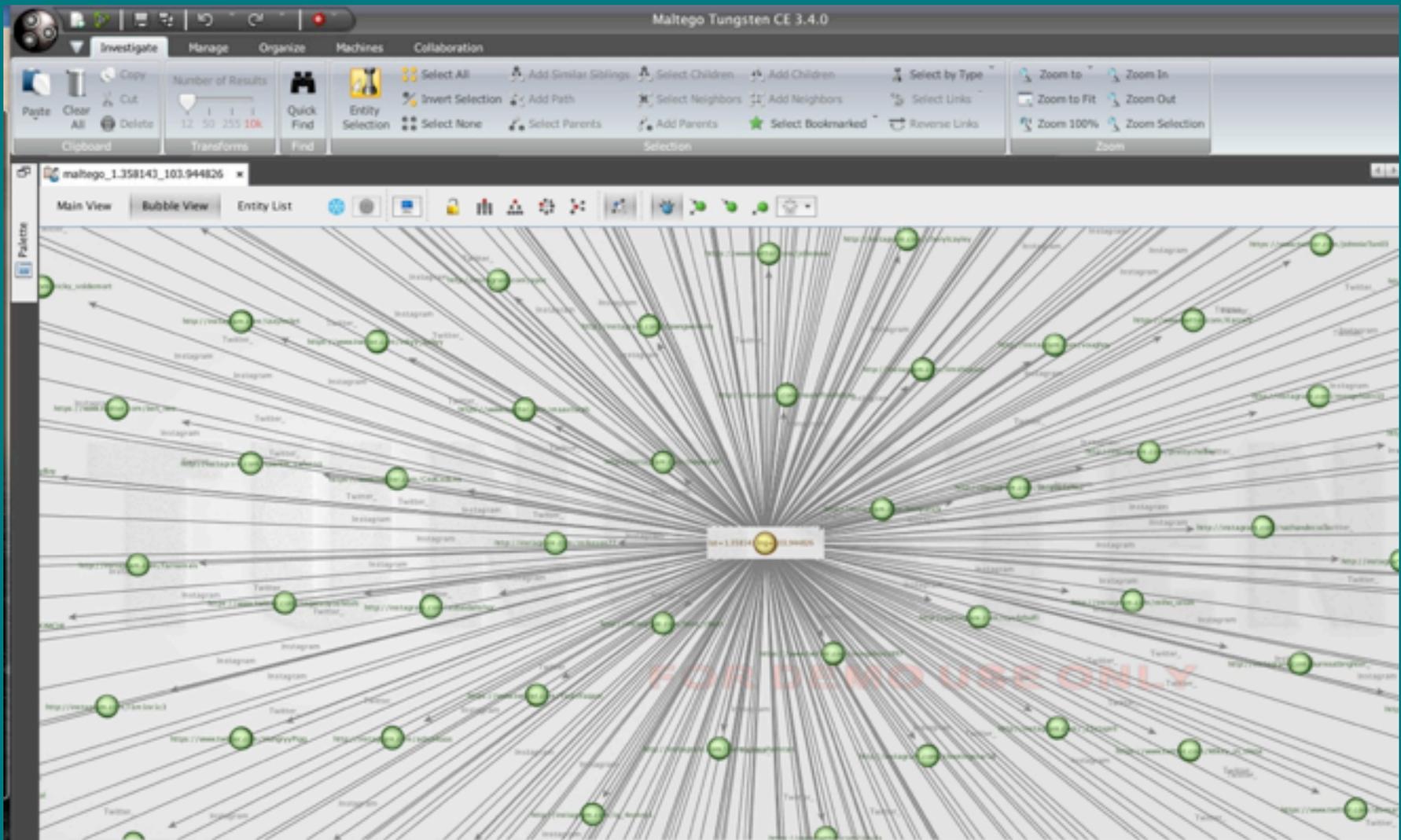
GHOSTALKER - INSTAGRAM



GHOSTALKER - HTML OUTPUT



GHOSTALKER - MALTEGO EXPORT



GEOSTALKER - LIMITATIONS

Single threaded

Query by GPS location or address only



GEOSTALKER - FUTURE VERSIONS

Multithreaded - Run faster!

Extend Maltego Mgtx export

Allow to disable specific datasource



FBSTAKLER - INTRO

Requires

- ▶ Profile Name

Graph Search to find

- ▶ Friends
- ▶ Likes
- ▶ Check-ins
- ▶ Comments

Provides

- ▶ Reverse engineered friend list
- ▶ Strength of associations
- ▶ Regular posting time
(wake time?)



FBSTALKER - LOCKDOWN VS NON-LOCKDOWN

Lockdown Profile

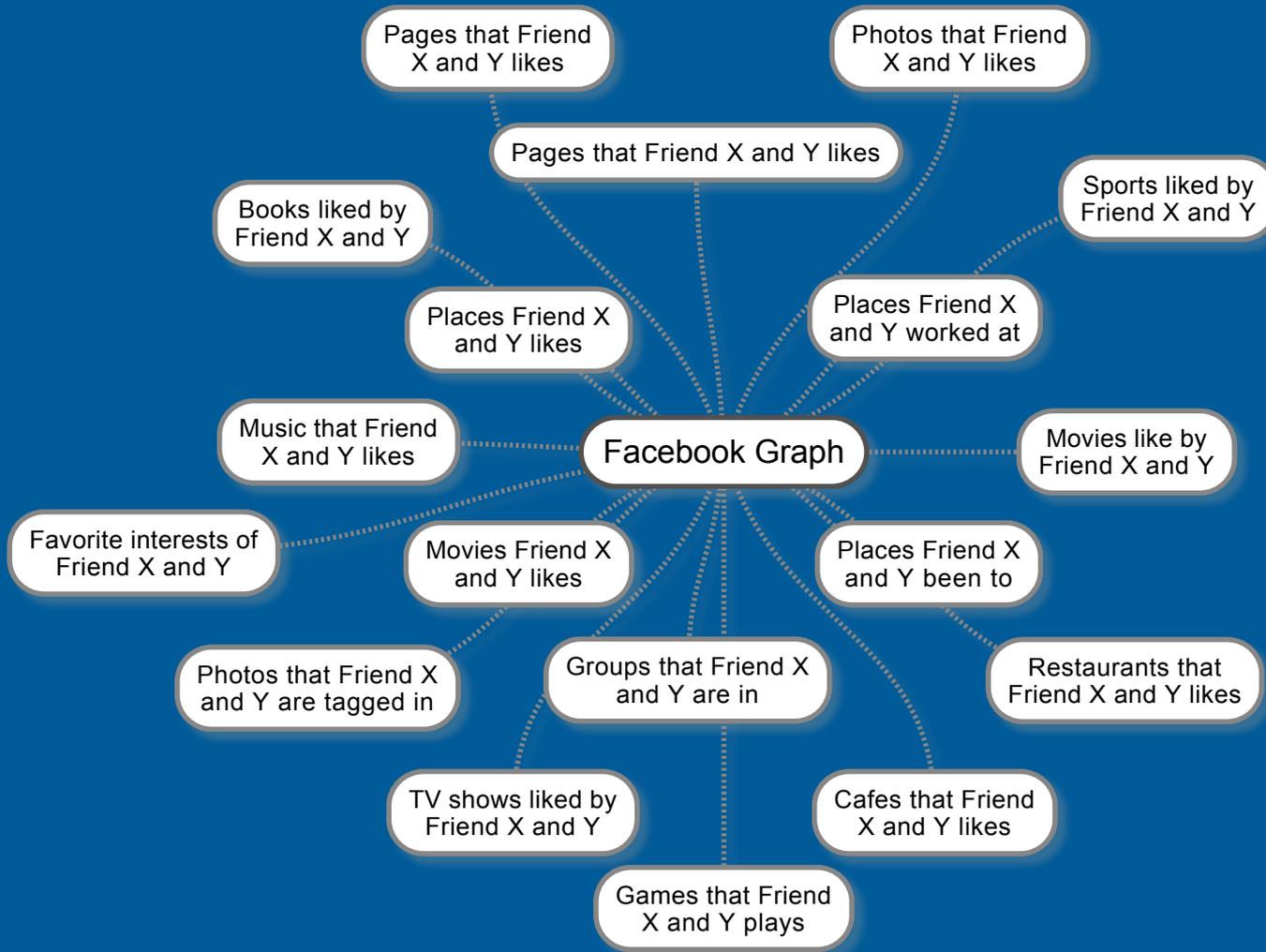
- ▶ Unable to see the list of friends
- ▶ Reverse engineer the list of friends from likes and tags

Open Profile

- ▶ Analyze all friends of target and determine how two individuals are connected or know each other.
 - ▶ Work place
 - ▶ School
 - ▶ Common interests
 - ▶ Common friends
 - ▶ Places that two individuals like

FACEBOOK GRAPH KEYWORDS

UNDERSTAND HOW 2 INDIVIDUALS ARE CONNECTED / RELATED



FBSTALKER - GRAPH SEARCH EXAMPLE

Photos that **Joe Sullivan** and **Mark Zuckerberg** like

SOL MEXICO

Introducción

Desayuno

Desayuno

Chorizo con Papas

Comeritos

Chalupas

Conchas

Nopales y Empanadas

Caldos De Pollo

Sopa Antrea

Empanada Sol

Empanada Verde

Like

Like

Refine This Search

Like



FBSTALKER - GRAPH SEARCH EXAMPLE



The screenshot shows a web browser window with the URL `https://www.facebook.com/search/733651102/places-visited/4/places-visited/intersect`. The page title is "Places visited by Mark Zuckerberg and Joe Sullivan". The search results are as follows:

- Greer Park**
Park
Mark Zuckerberg and Joe Sullivan were here
1098 Amarillo Avenue, Palo Alto, CA
71 like this
- Facebook Palo Alto**
Internet/Software
Mark Zuckerberg and Joe Sullivan were here
We're building a web where the default is social.
Permanently Closed
James Barre likes this
- Palo Alto, California**
City
Mark Zuckerberg and Joe Sullivan were here
Palo Alto is a California charter city located in the northwest corner of Sa...
People also like San Francisco, California and other cities
James Barre likes this
- Cambridge, Massachusetts**
City
Mark Zuckerberg and Joe Sullivan were here
Cambridge is a city in Middlesex County, Massachusetts, United States, s...
People also like Boston, Massachusetts and other cities
30,231 like this



DEMO

FBSTALKER



FBSTALKER - INPUT

```
FLD-SP-C02HJ1:test klee$ python2.6 fb_test2.py -user joesullivan
[*] Username:   joesullivan
[*] Uid:        733651102

[*] Writing 1 record(s) to database table: videosBy
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: DallasCAC
[*] Extracting Data from Photo Page: michael.doherty.967
[*] Extracting Data from Photo Page: adamconner
[*] Extracting Data from Photo Page: boz
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: DallasCAC
[*] Extracting Data from Photo Page: flexengineer
[*] Extracting Data from Photo Page: tomw
```

FBSTALKER - RUNNING

```
U
***** Places Visited By joesullivan *****
Public Places &amp;: Attractions:Gym      UCSF Mission Bay Conference Center      https://www.facebook.com/UCSFMissionBayConferenceCenter
Burger Restaurant:Arts &amp;: Entertainment      St. John's Bar &amp;: Grill      https://www.facebook.com/pages/St-Johns-Bar-Grill/244157021091
Hotel      Sheraton Dallas https://www.facebook.com/SheratonDallas
Event      Catawaran Resort Luau https://www.facebook.com/CatawaranResortLuau
Corporate Office:Campus Building      Facebook HQ      https://www.facebook.com/pages/Facebook-HQ/166793020034304
Corporate Office      Google CL5      https://www.facebook.com/pages/Google-CL5/121693804547006
Park      Greer Park      https://www.facebook.com/pages/Greer-Park/112570685464837

***** Places Liked By joesullivan *****

***** Places checked in *****
2013-03-02 14:18:10      Rsa Conference 2013      https://www.facebook.com/pages/Rsa-Conference-2013/462498270469891
2013-02-13 00:20:11      The Facebook Suite at the Center, University of Alabama Biraingham      https://www.facebook.com/pages/The-Facebook-Suit

***** Apps used By joesullivan *****

***** Videos Posted By joesullivan *****
https://www.facebook.com/photo.php?v=10100609712053311      Vhat most schools don&#039;t teach

***** Pages Liked By joesullivan *****

***** Friendship History of joesullivan *****

***** Friends of joesullivan *****
*** Backtracing from Facebook Likes/Comments/Tags ***

boz
maryp
charlotte
larrywagid
marisa.fagan
tvt
christian.p.sullivan
jack.christin
davidrecordon
sacredheartcs
LiveNationBayArea
traci.holdt
zuck
pondhockeymovie
tim.gould.1029
dustin
PaloAltoPolice
adamconner
97890471439
```


FBSTALKER - PROBLEMS

Facebook Graph API is limited

PhantomJS had some issues with Facebook site

Had to use Chromedriver

Single threaded

FBSTALKER - FUTURE WORK

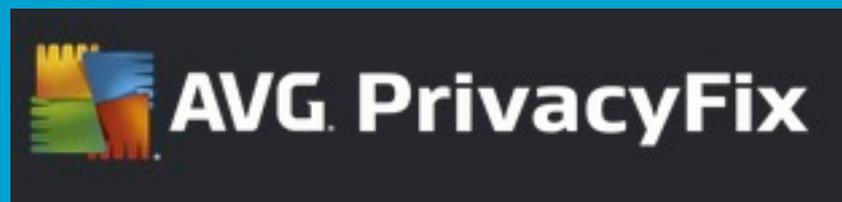
- ▶ Runs 100% headless
- ▶ Monitor changes / activities of user's FB profile.
- ▶ Allow name as input instead of userid
- ▶ Point system for Association strength
 - ▶ Photo Tags
 - ▶ Check-ins
 - ▶ Comments
 - ▶ Post / Photo Likes



HOW TO PROTECT YOURSELF

Turn off 'location' setting in social networking apps

Tighten Facebook privacy settings





<http://github.com/milo2012/osintstalker>

klee@trustwave.com
@keith55

jwerrett@trustwave.com
@werrett

 Trustwave®
SpiderLabs®