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

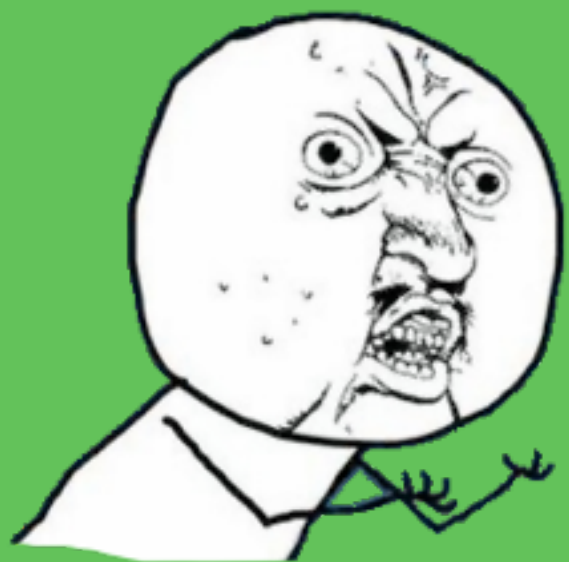
Day-in day-out

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

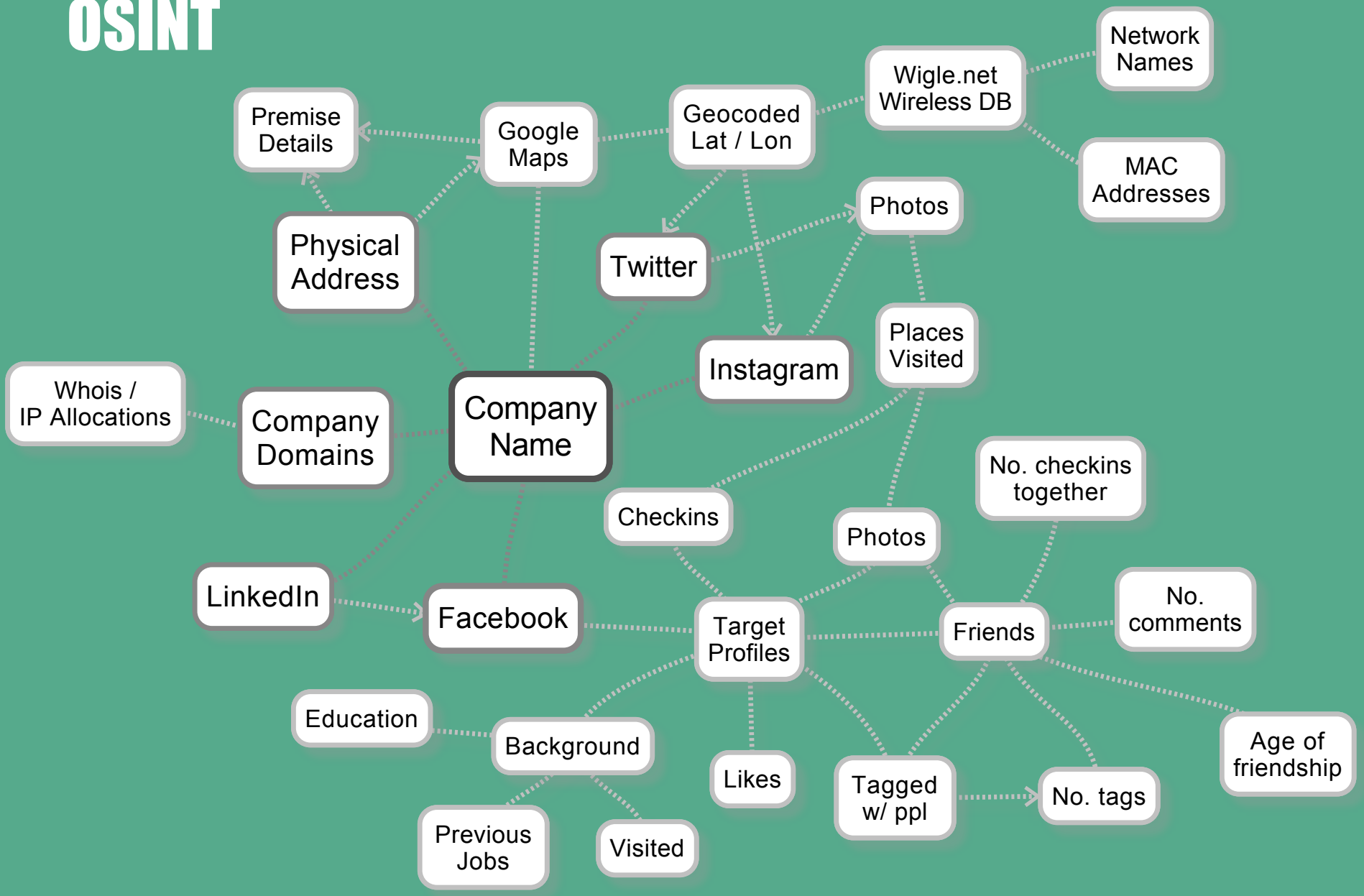
Set specific targets

Gain access any way you can

...

Red team, Physical Security, Phishing
Open Source Intelligence

OSINT


Network Names
Wigle.net Wireless DB
Premise Details
Google Maps
Geocoded Lat / Lon
MAC Addresses
Photos
Physical Address
Twitter
Places Visited
Instagram
Whois / IP Allocations
Company Domains
Company Name
No. checkins together
Checkins
Photos
LinkedIn
Facebook
Target Profiles
Friends
No. comments
Education
Background
Age of friendship
Likes
Tagged w/ ppl
No. tags
Previous Jobs
Visited

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

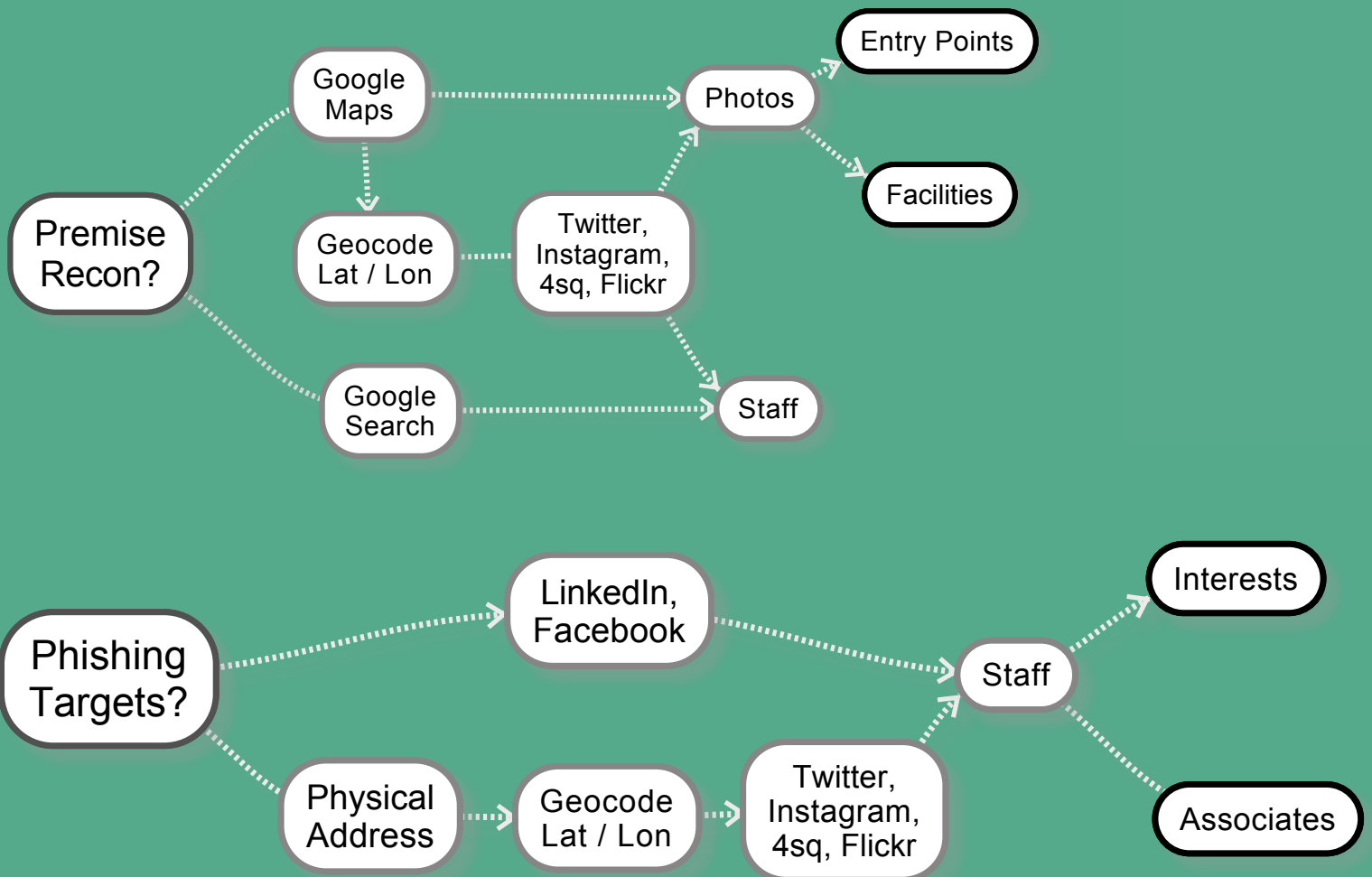
Uses Graph Search to reverse

- 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

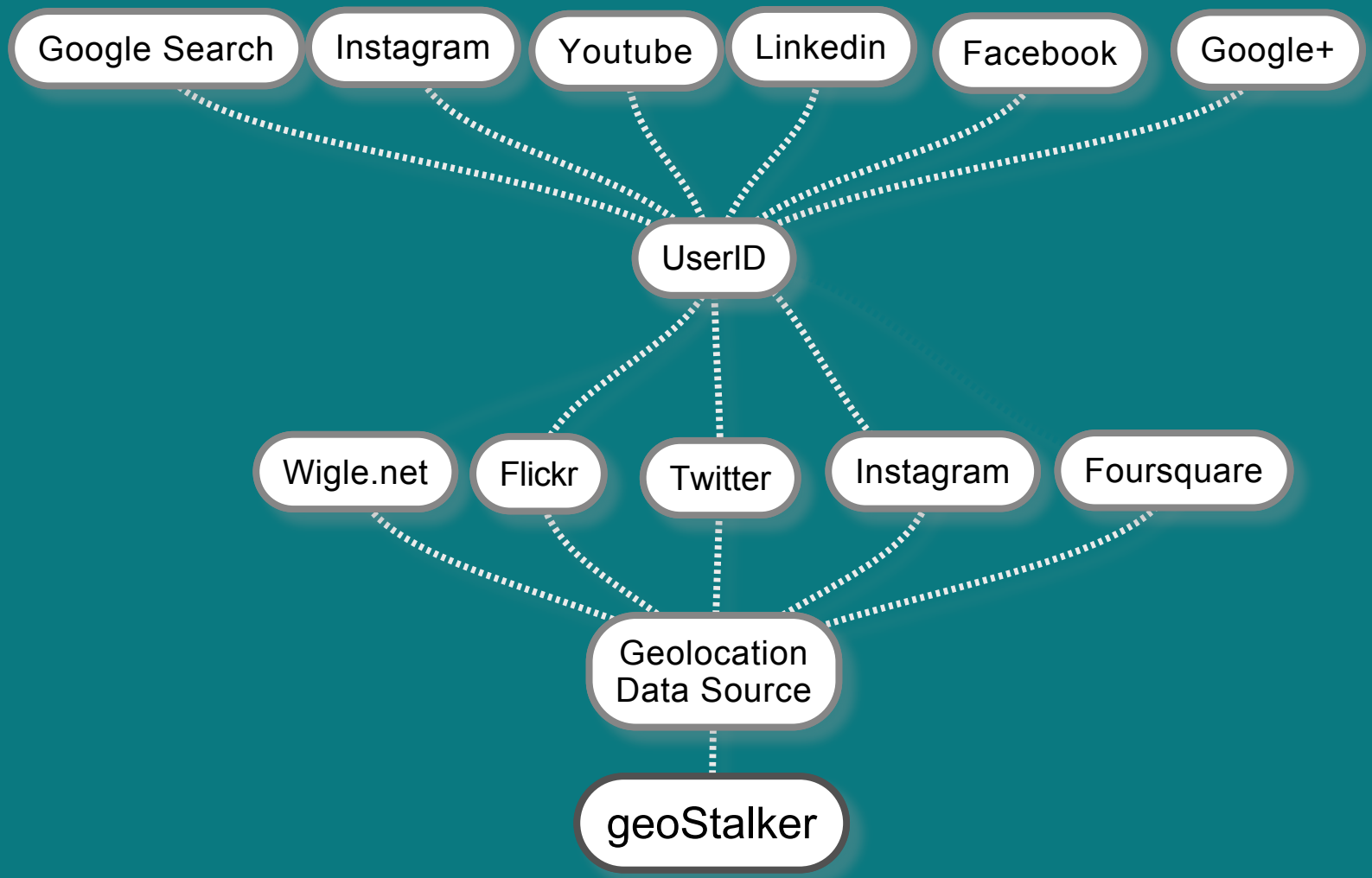
Queries sources

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

Provides

- Wireless devices
- Photos
- Social network accounts
- Searches social network accounts for ‘like’ names

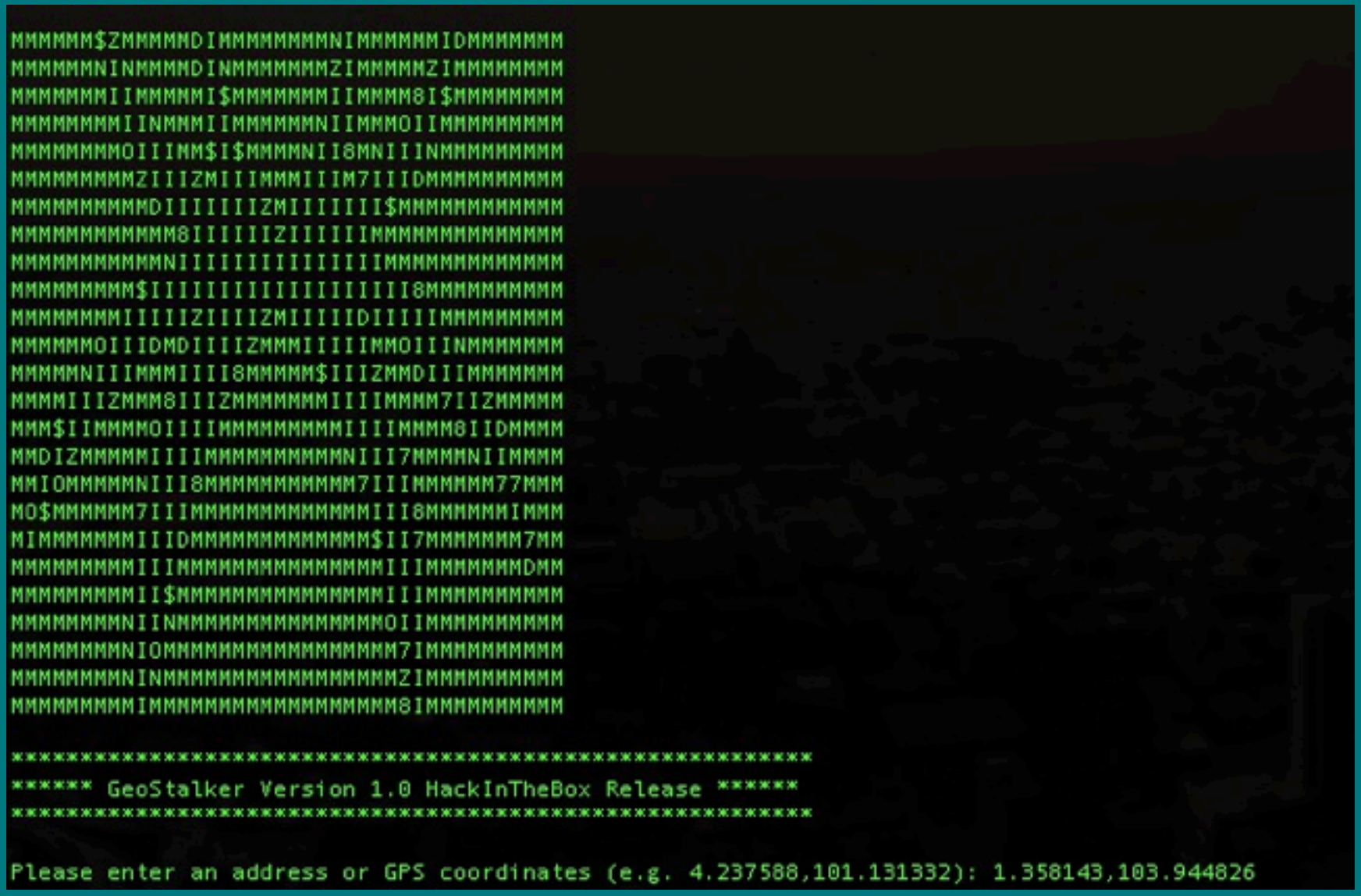
GEOSTALKER - APPLICATION FLOW



DEMO

GEOSTALKER

GEOSTALKER - INPUT



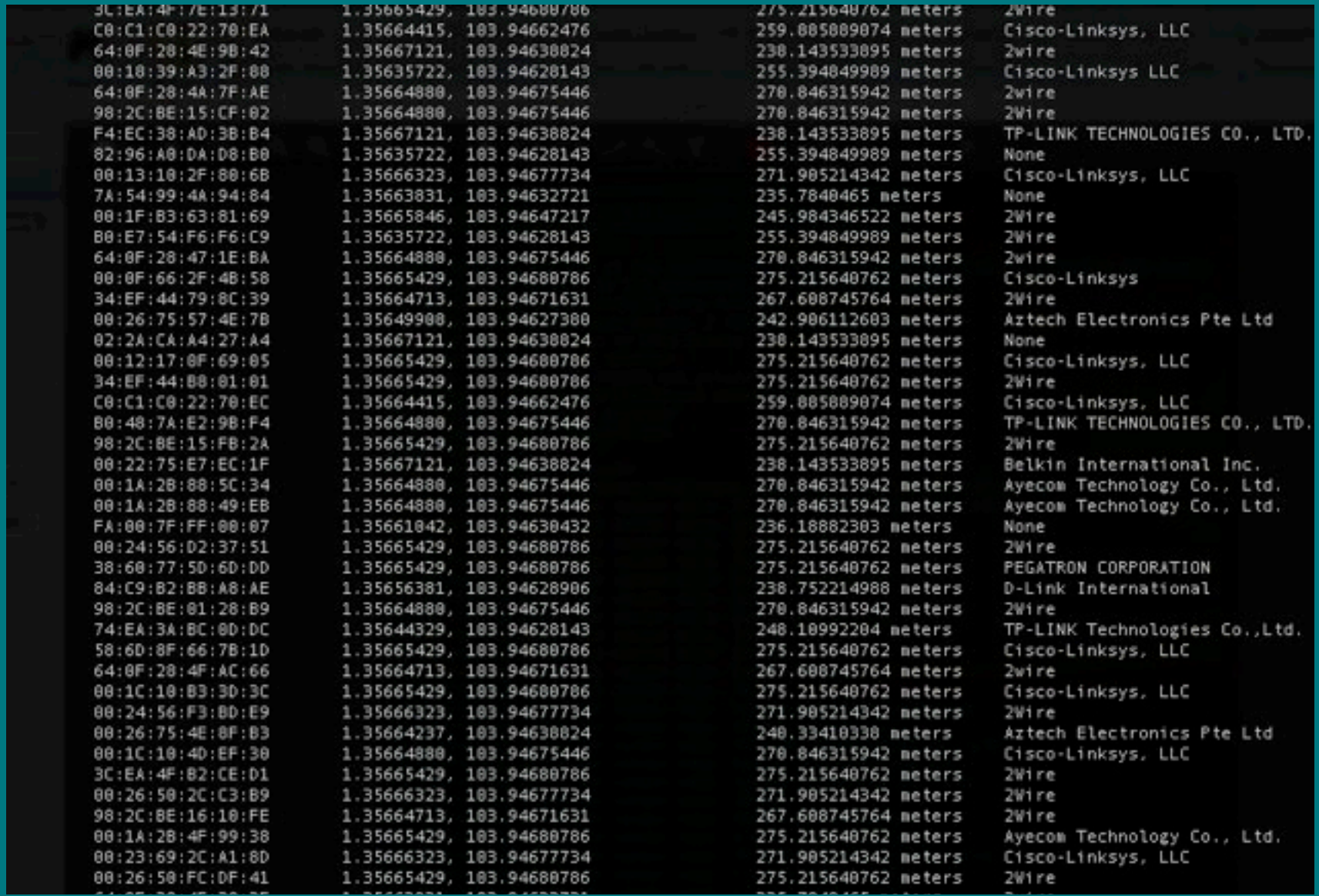
GEOSTALKER - RUNNING

```
************************************************************
****** 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/mdsufi34 (1.3585548,103.9456923)
[*] Found http://instagram.com/staticattack7     (1.366655009,103.950112024)
[*] Found http://instagram.com/zesablaza         (1.3530664,103.95086925)
[*] 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_wong        (1.358982817,103.936033689)
[*] 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   (1.3577772,103.947368)
[*] Found http://instagram.com/jacquikyl         (1.3529967,103.9486539)
[*] Found http://instagram.com/sellingcheapsquishy_      (1.3567486,103.9472094)
[*] Found http://instagram.com/snailvhitesingapore       (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       (1.3595,103.948166667)
[*] Found http://instagram.com/xxiaooxuann       (1.360709293,103.95308796)
[*] Found http://instagram.com/salihahyourbabygurl       (1.35426069,103.951874971)
[*] Found http://instagram.com/syhrh     (1.353779637,103.943580409)
[*] Found http://instagram.com/staticattack7     (1.36678,103.95011)
[*] Found http://instagram.com/yonkeezyyy        (1.366642948,103.946193808)
[*] Found http://instagram.com/frhnh_    (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    (1.367088449,103.958825054)

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

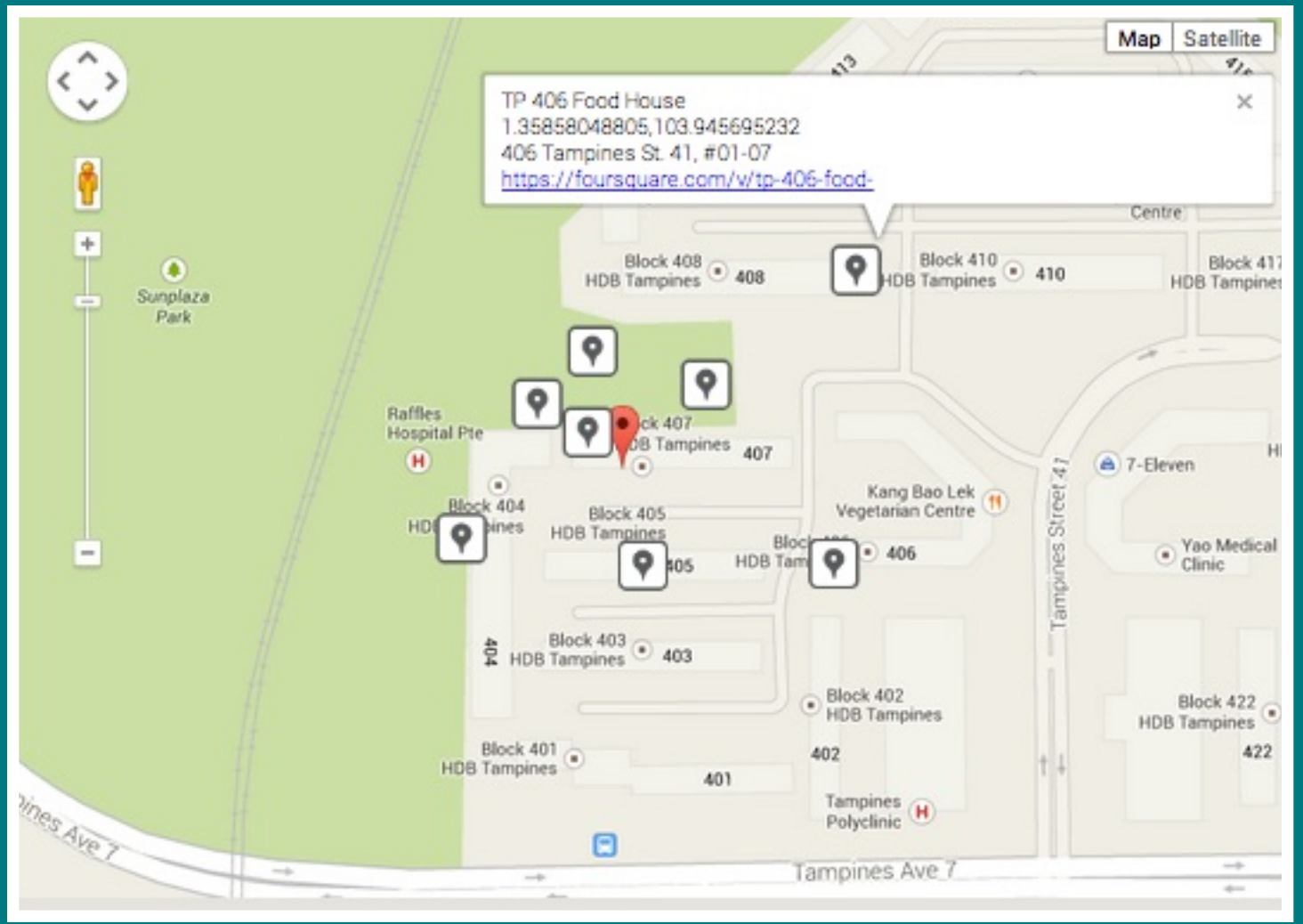
GEOSTALKER - RUNNING



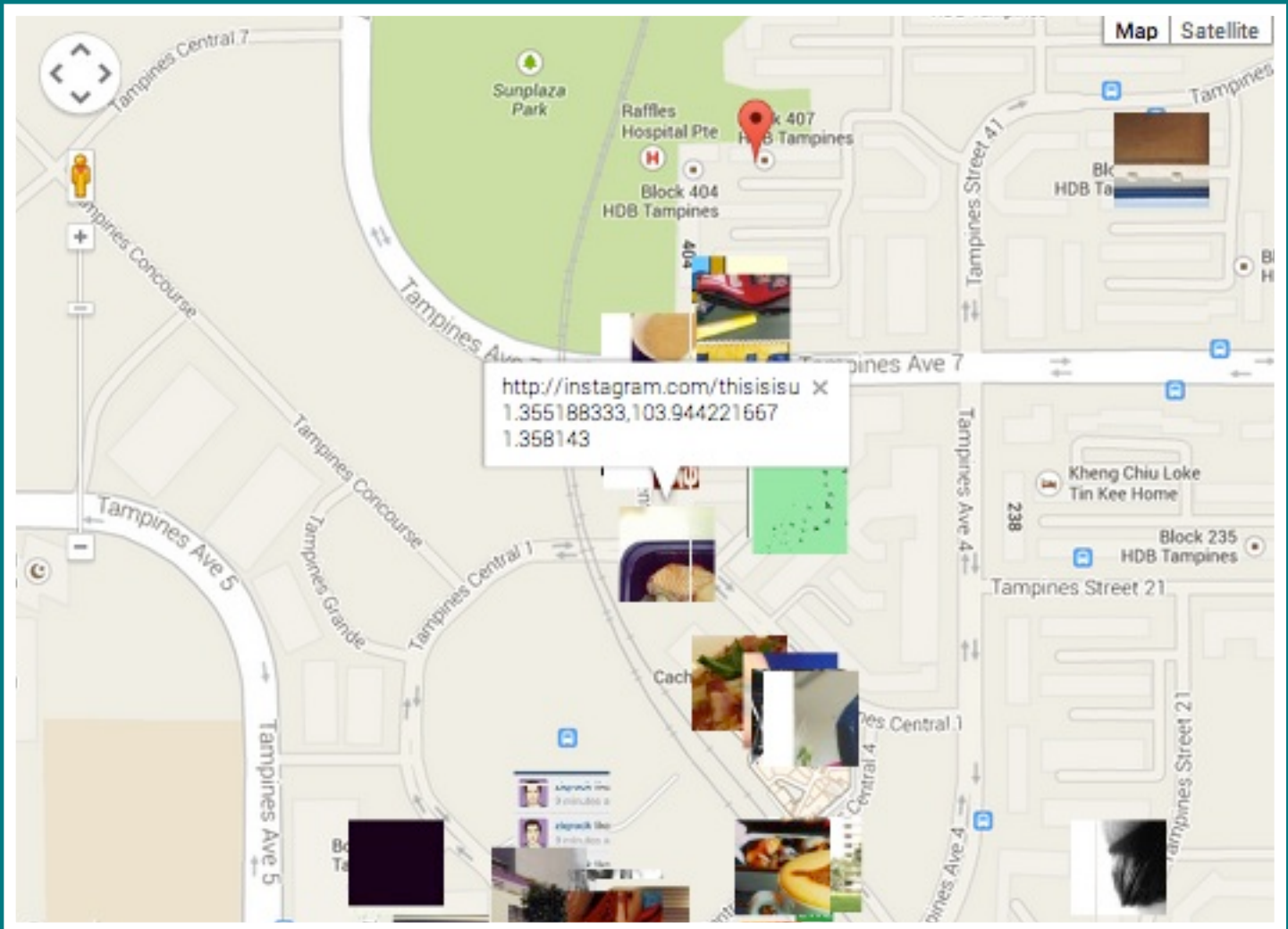
GEOSTALKER - RUNNING

```
[*] 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
```

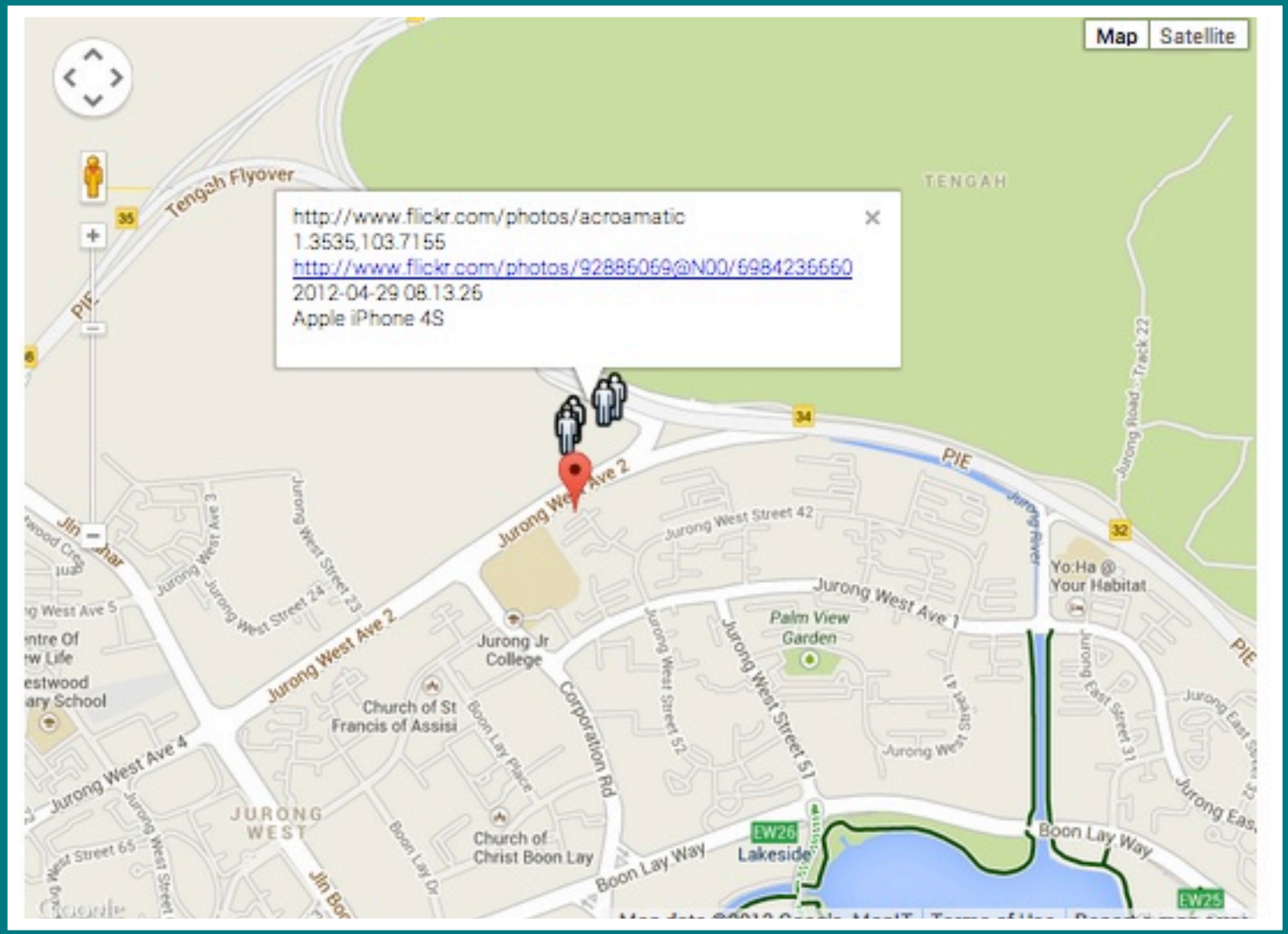
GEOSTALKER - FOURSQUARE



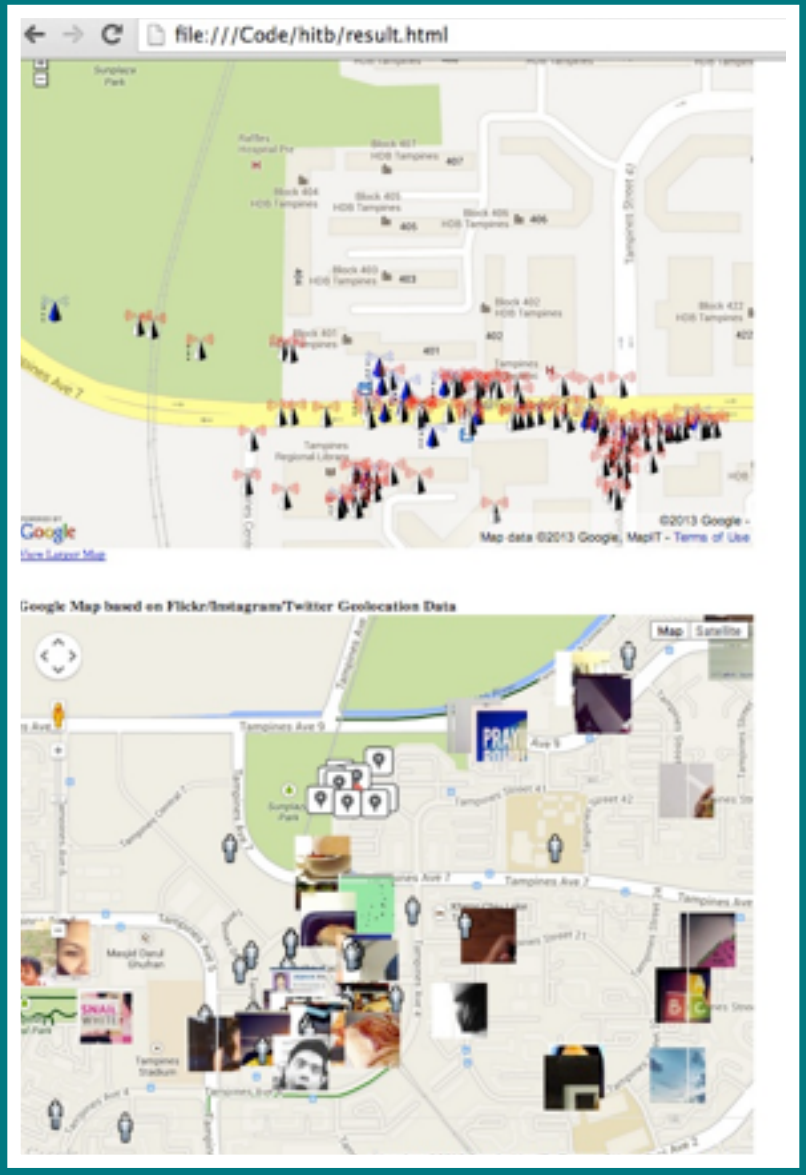
GEOSTALKER - INSTAGRAM



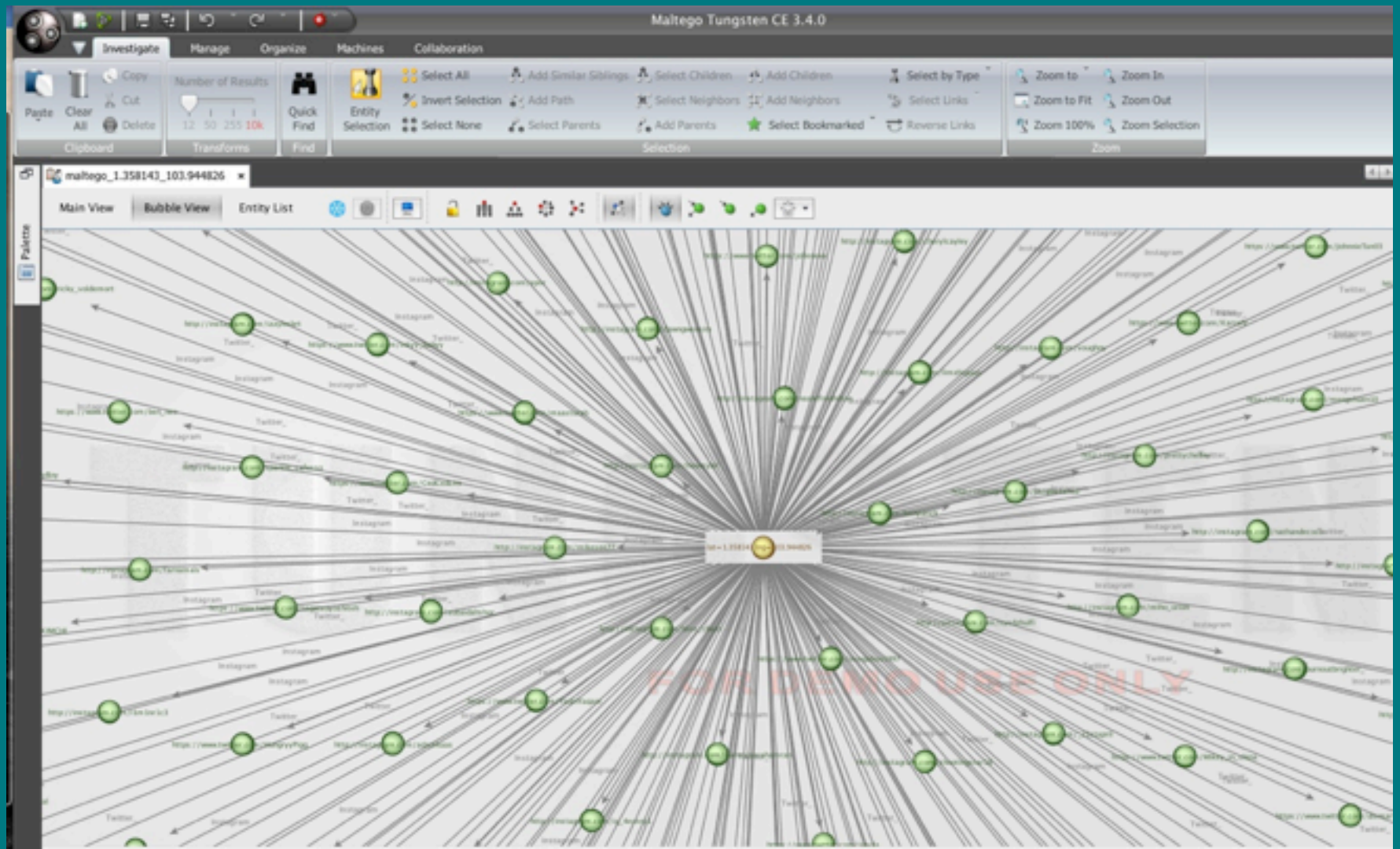
GEOSTALKER - FLICKR



GEOSTALKER - HTML OUTPUT



GEOSTALKER - 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

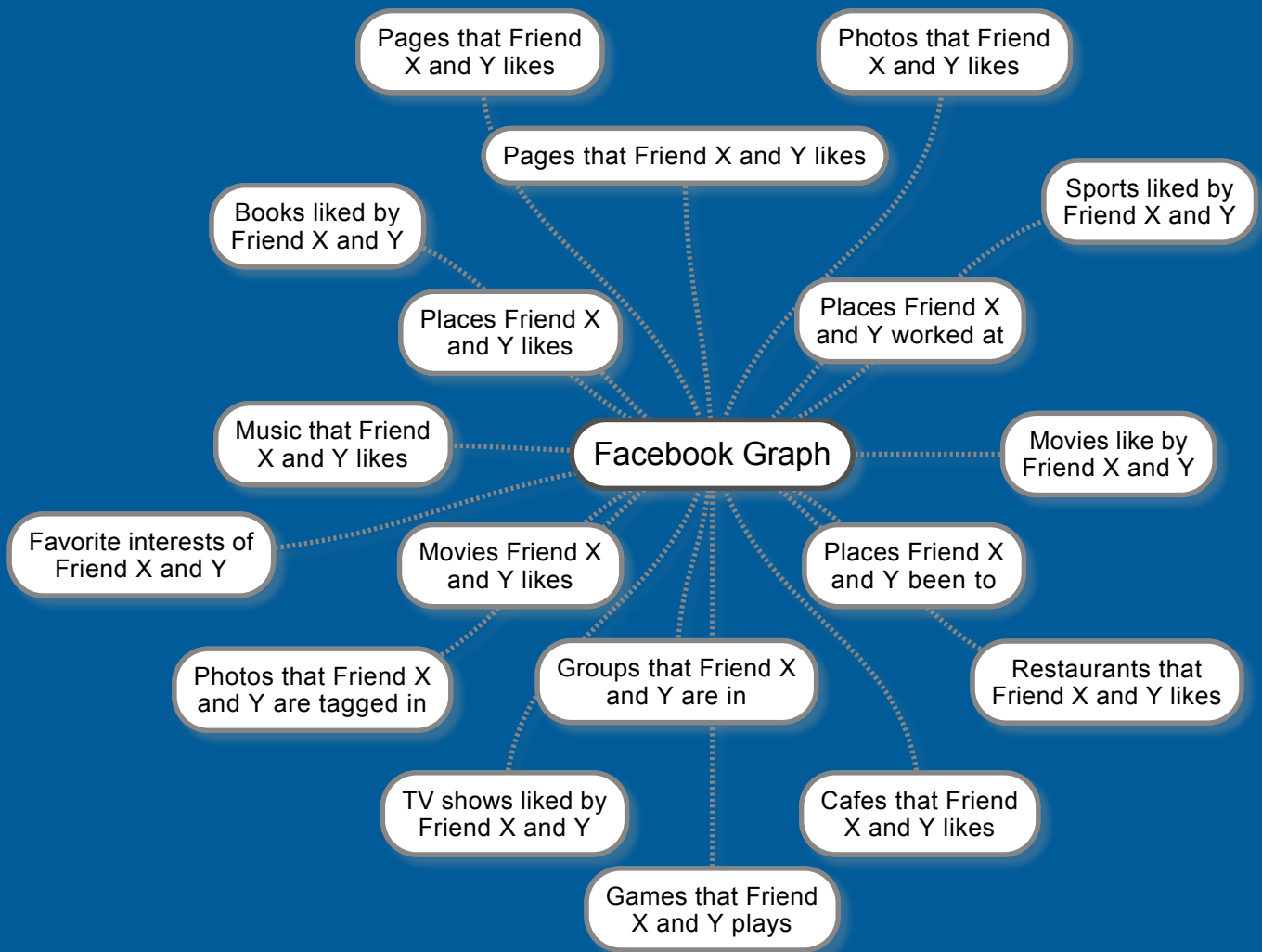
- Unable to see the list of friends
- Reverse engineer the list of friends from likes and tags

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

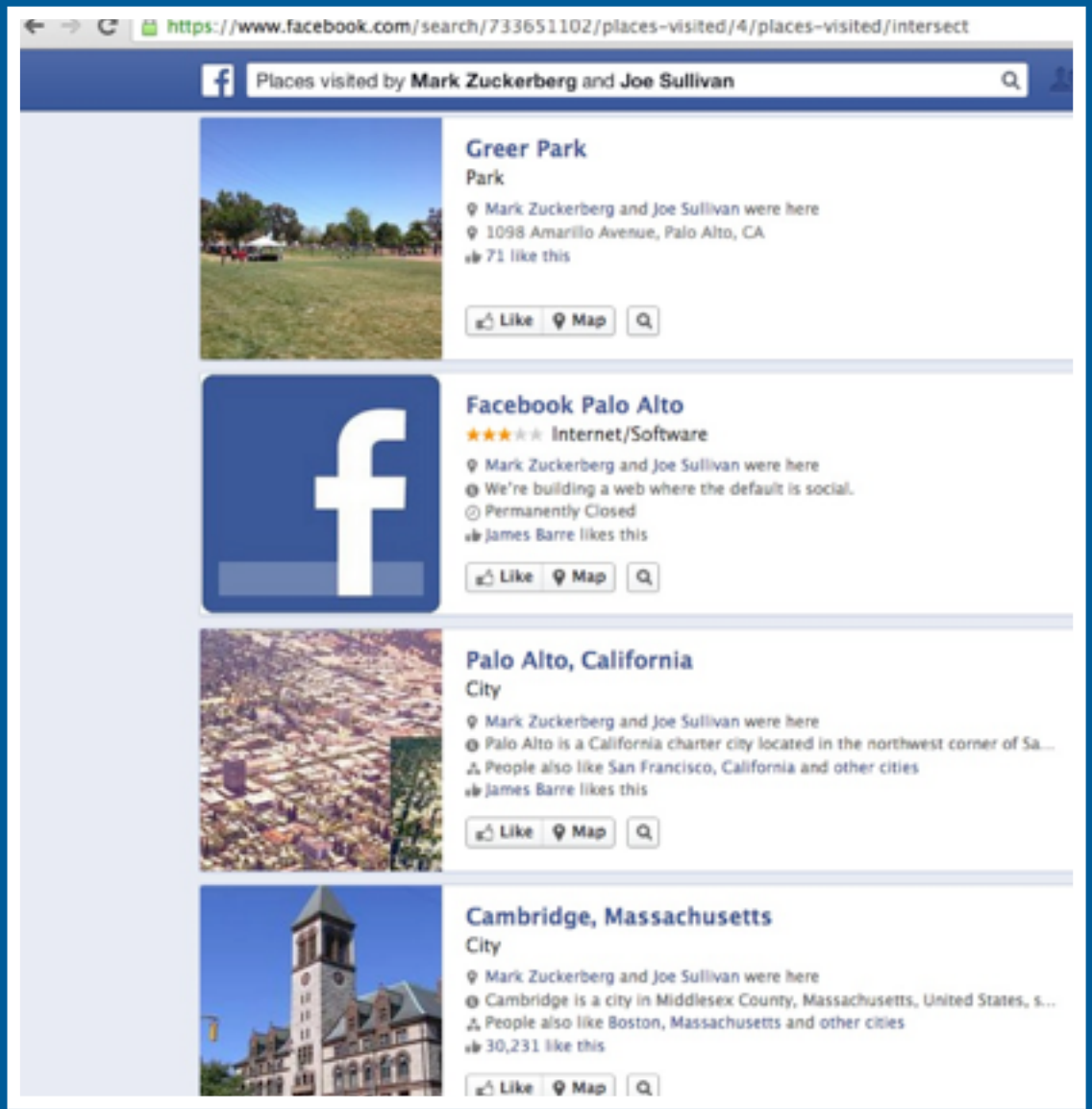
FACEBOOK GRAPH KEYWORDS

UNDERSTAND HOW 2 INDIVIDUALS ARE CONNECTED / RELATED



FBSTALKER - GRAPH SEARCH EXAMPLE

FBSTALKER - GRAPH SEARCH EXAMPLE



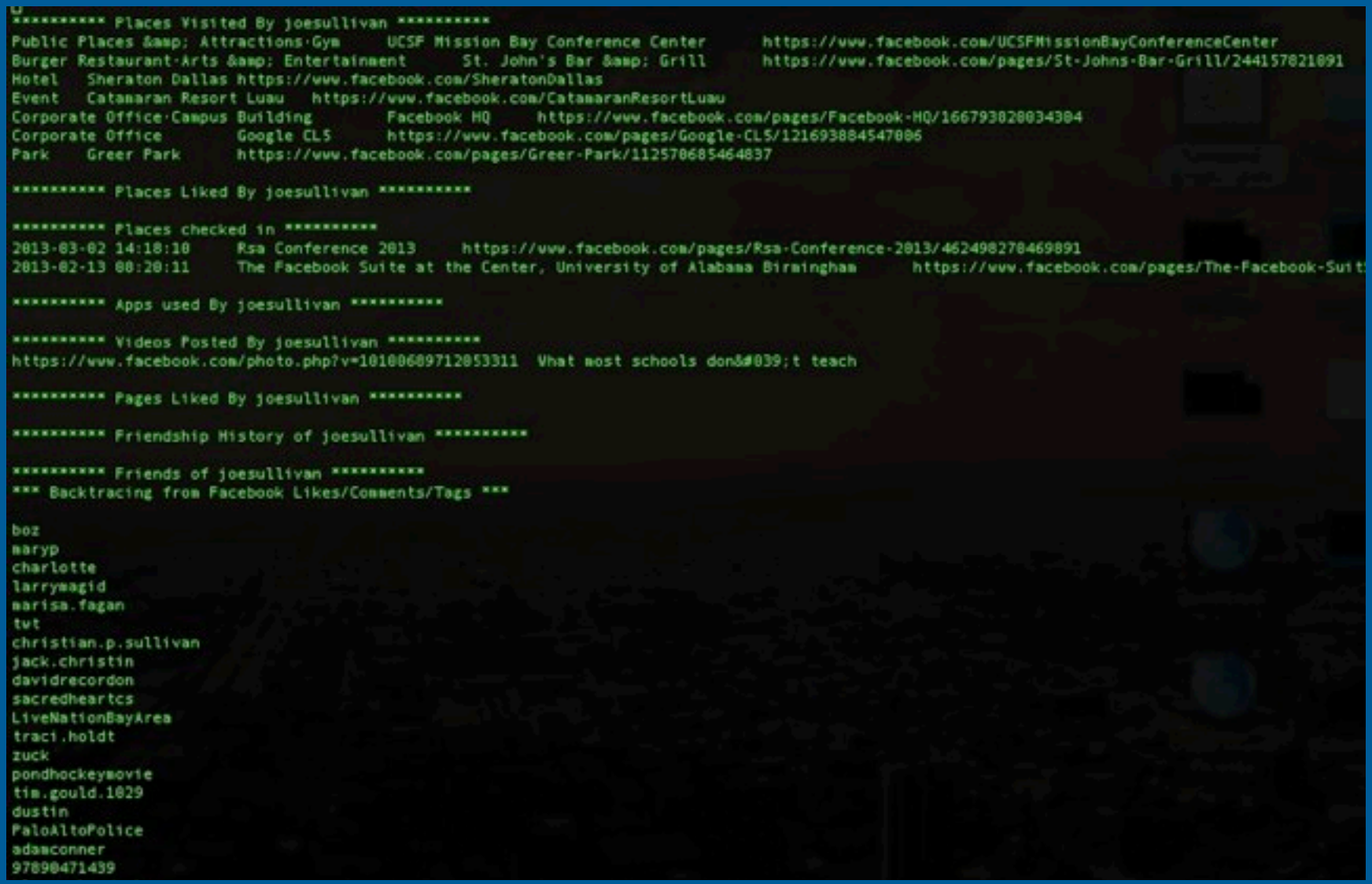
DEMO

FBSTALKER

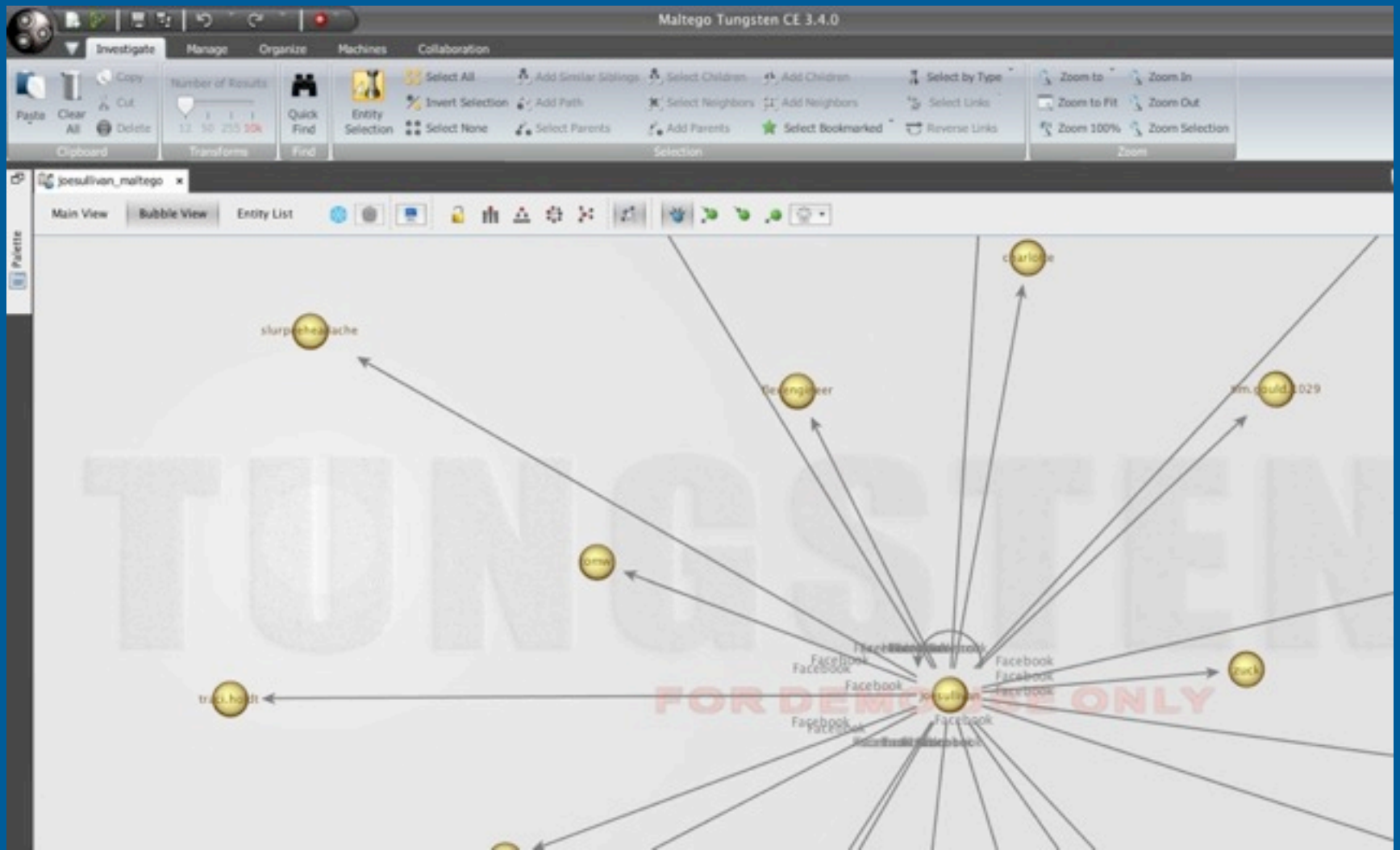
FBSTALKER - INPUT

```
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: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] Extracting Data from Photo Page: joesullivan
[*] 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



FBSTALKER - MALTEGO EXPORT



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®