Social Networking Special Ops: Extending Data Visualization Tools for Faster Pwnage

Chris Sumner | @TheSuggmeister | www.securityg33k.com

Disclaimer

"I am not speaking on behalf of my employer.

The information and perspectives I present are personal and do not represent those of my employer."

What yer in for…

What yer in for…

1. Intro to Social Network Analysis & Visualization

What yer in for…

1. Intro to Social Network Analysis & Visualization

2. Case study using Twitter & Maltego

What yer in for…

1. Intro to Social Network Analysis & Visualization

2. Case study using Twitter & Maltego

3. Something a bit darker using facebook & Maltego

Goals

Goals

- Overview/appreciation of possibilities in this field

Goals

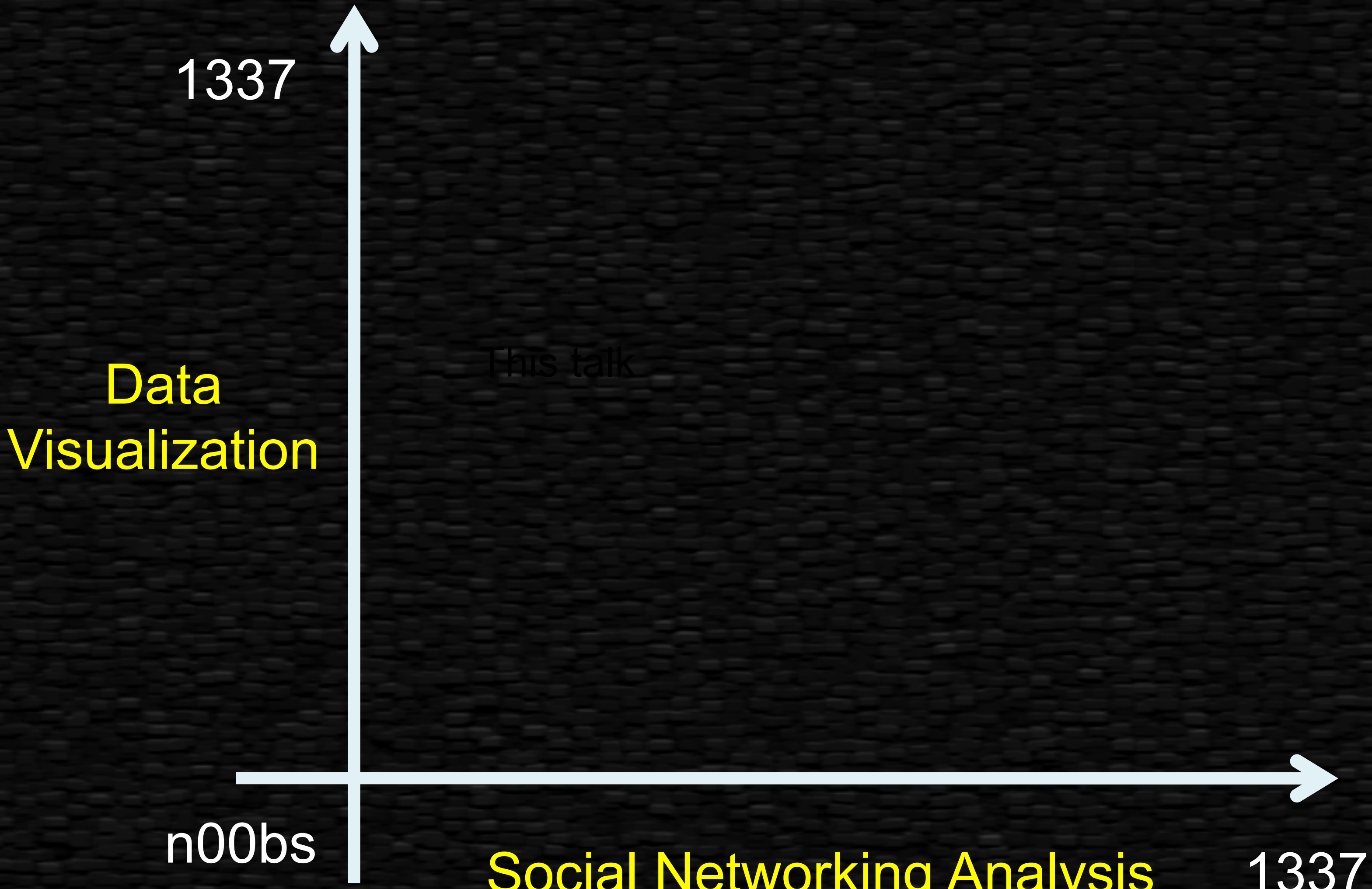
- Overview/appreciation of possibilities in this field

- Expose you to some ideas that you can apply to your specific situation

Who’s the talk aimed at?

This talk

Who’s the talk aimed at?



1337

Data Visualization

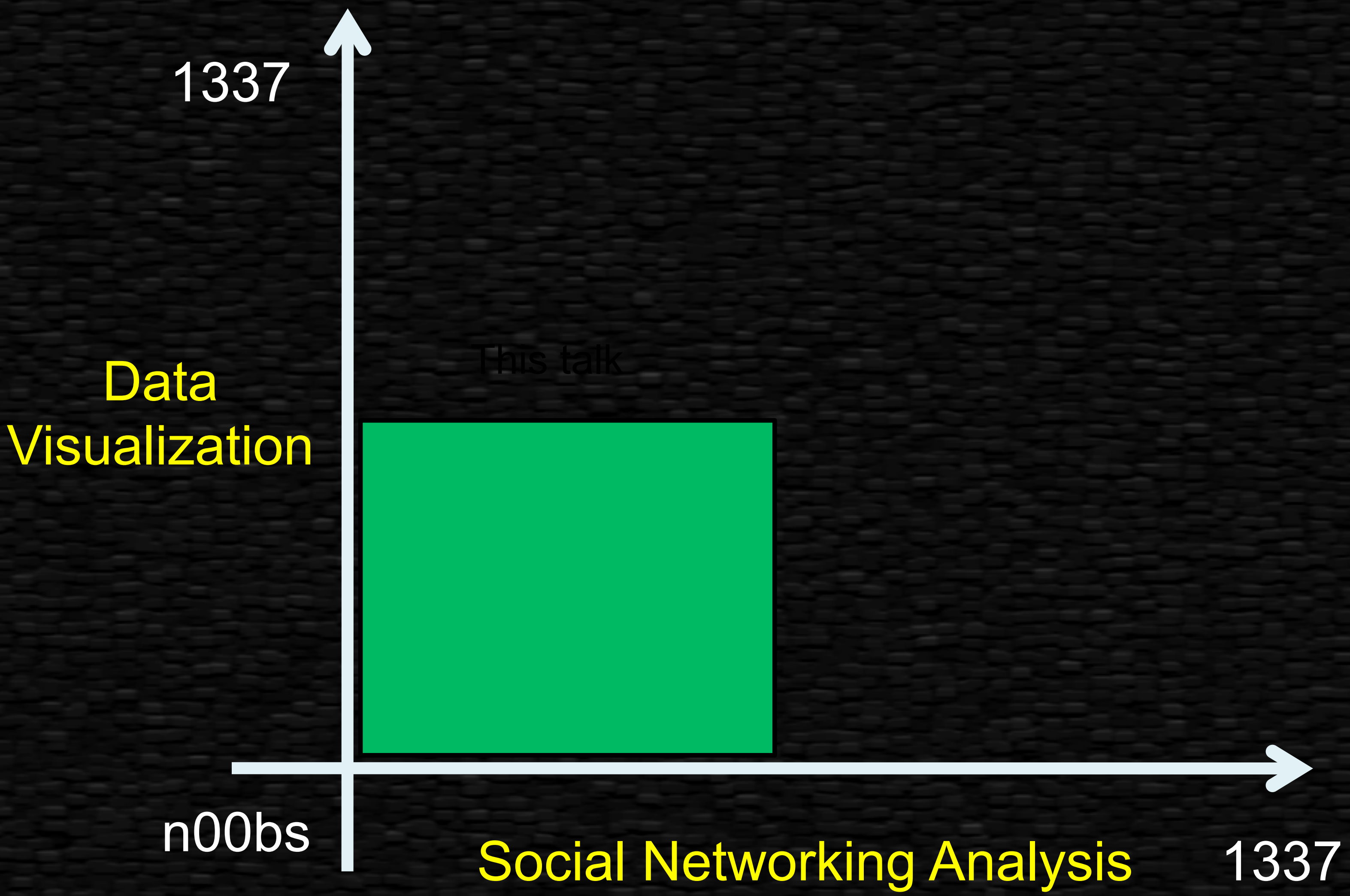
This talk

n00bs

Social Networking Analysis

1337

Who’s the talk aimed at?



1337

This talk

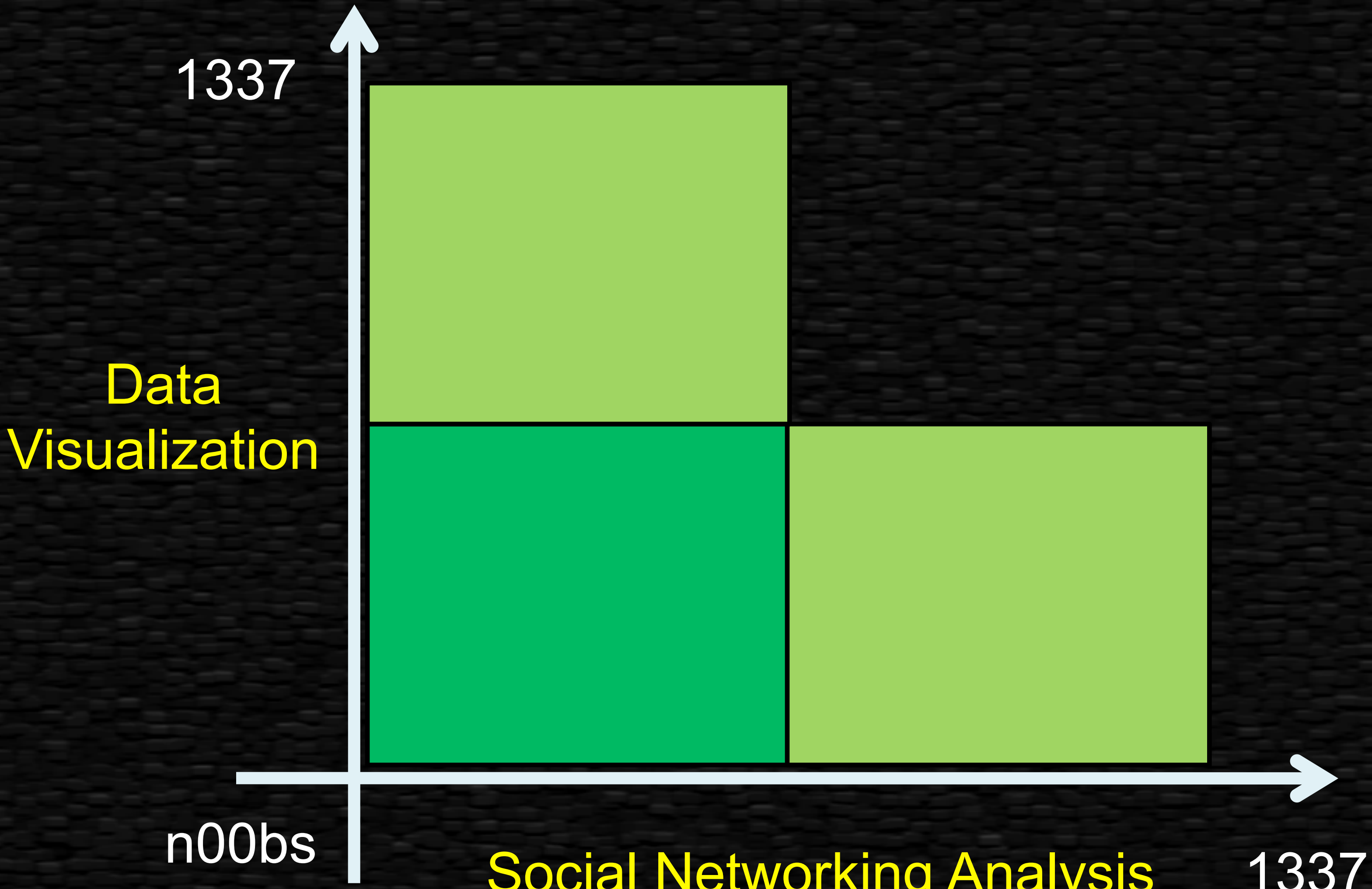
Data Visualization

n00bs

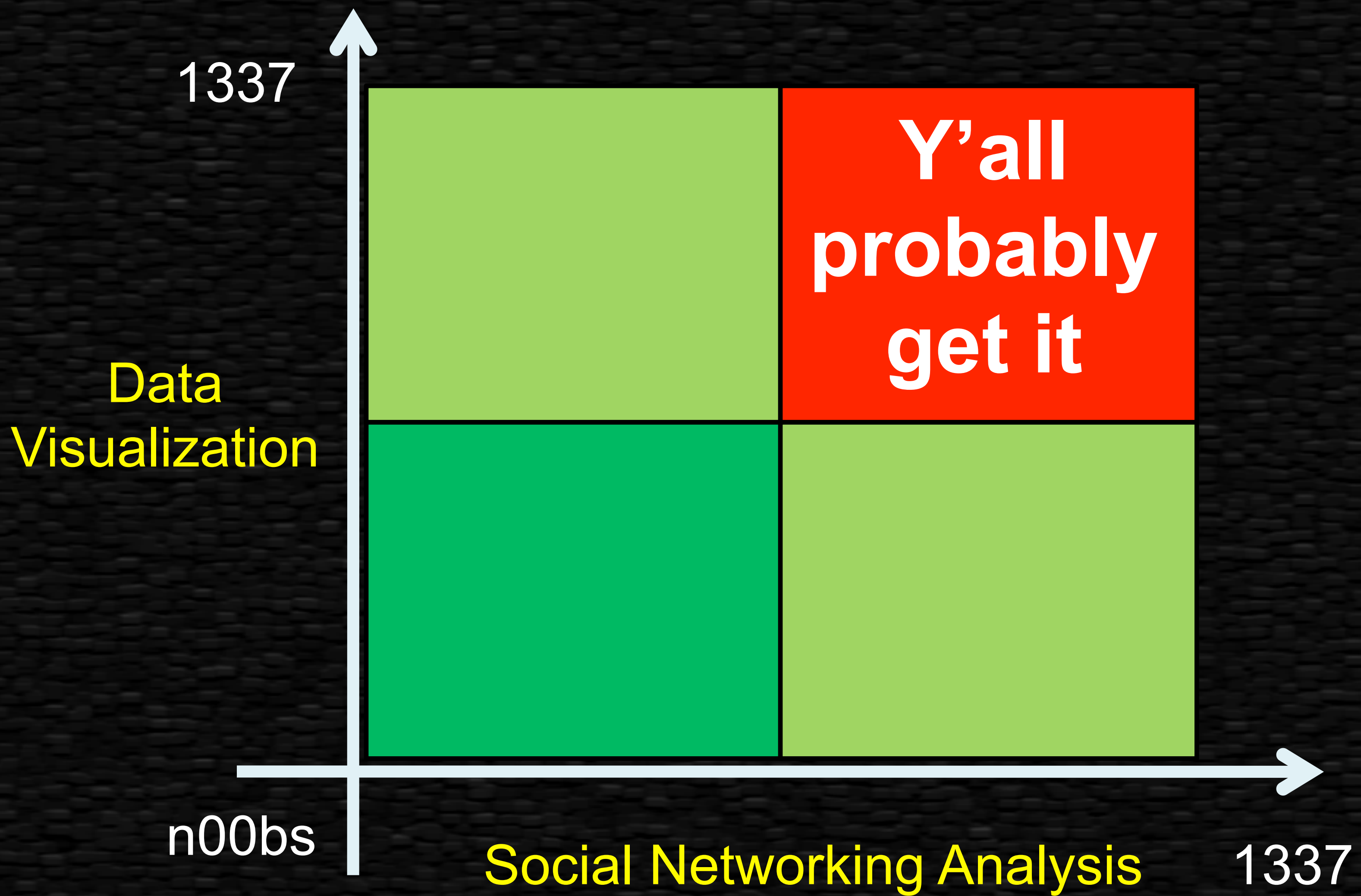
Social Networking Analysis

1337

Who’s the talk aimed at?



Who’s the talk aimed at?



1337

Y’all probably get it

Data Visualization

n00bs

Social Networking Analysis

1337

Who am I?

@TheSuggmeister

Who am I?

@TheSuggmeister

- By day
  - Corporate security

Who am I?

@TheSuggmeister

- By day
  - Corporate security
- By night | weekend
  - Data analysis
  - Data visualization
  - Social Media
  - DC4420

Who am I?

@TheSuggmeister

- By day
  - Corporate security
- By night | weekend
  - Data analysis
  - Data visualization
  - Social Media
  - DC4420
- A strange sequence of events led to me appearing here

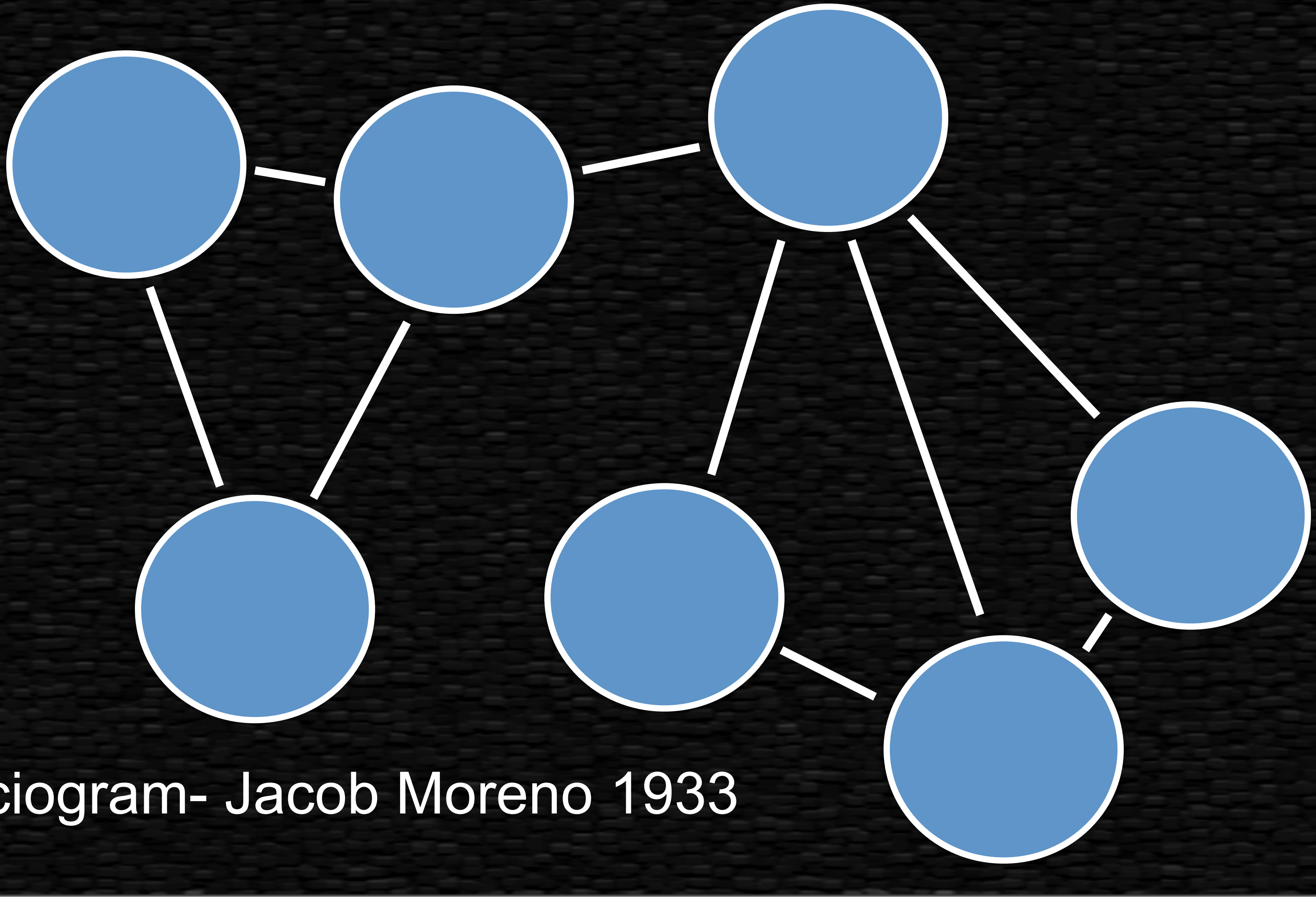
Social Network Analysis

+ Target Rich Environment

= Problem

= Opportunity

Social Network Analysis



Sociogram- Jacob Moreno 1933

Target Rich Environment

Target Rich Environment

- Data – ~21 exabytes per month

Target Rich Environment

- Data – ~21 exabytes per month
- Facebook – ~500 ish million users

Target Rich Environment

- Data – ~21 exabytes per month
- Facebook – ~500 ish million users
- Privacy paradox
  - – "I take privacy seriously"
  - – 89% use real names
  - – 61% use identifiable picture

Target Rich Environment

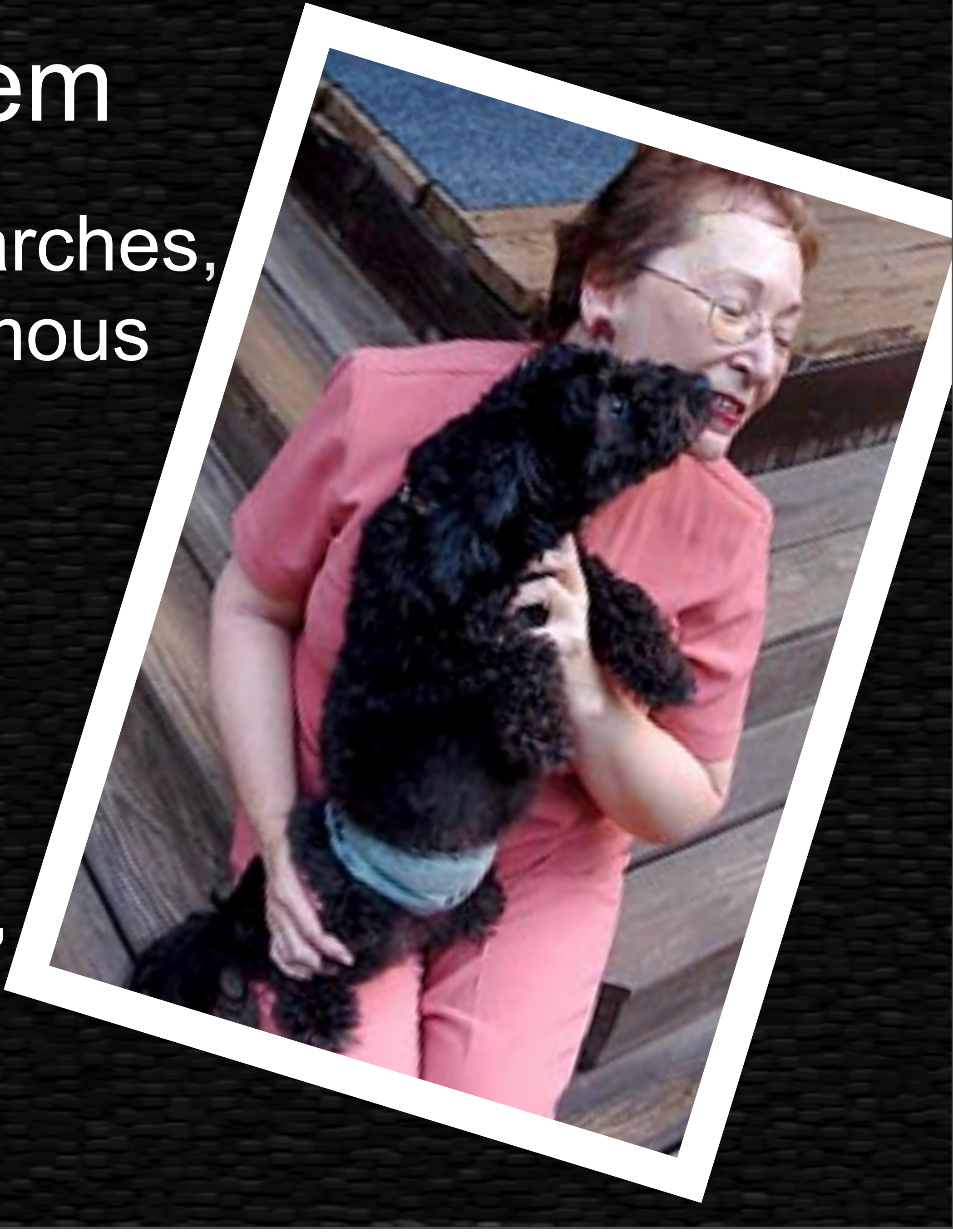
- Data – ~21 exabytes per month
- Facebook – ~500 ish million users
- Privacy paradox
  - “I take privacy seriously”
  - 89% use real names
  - 61% use identifiable picture
- “I’ve got nothing to hide and Other Misunderstandings of Privacy” – Daniel Solove

Problem

Your anonymous searches, aren’t all that anonymous

Problem

Your anonymous searches, aren't all that anonymous



- AOL user 4417749
- Ms. Thelma Arnold, Lilburn Georgia

Opportunity

- Lots of data
- Lots of noise

Opportunity

- Lots of data
- Lots of noise
- Find “interesting” stuff a bit faster….

Opportunity

- Lots of data
- Lots of noise
- Find “interesting” stuff a bit faster….

…..by combining Data Mining/Screen Scraping, Named Entity Recognition and Data Visualization

Named Entity Recognition

“Parsing data to extract & classify information”

Named Entity Recognition

“Parsing data to extract & classify information”

“Greg bought 300,000 shares of LIGATT in 2010”

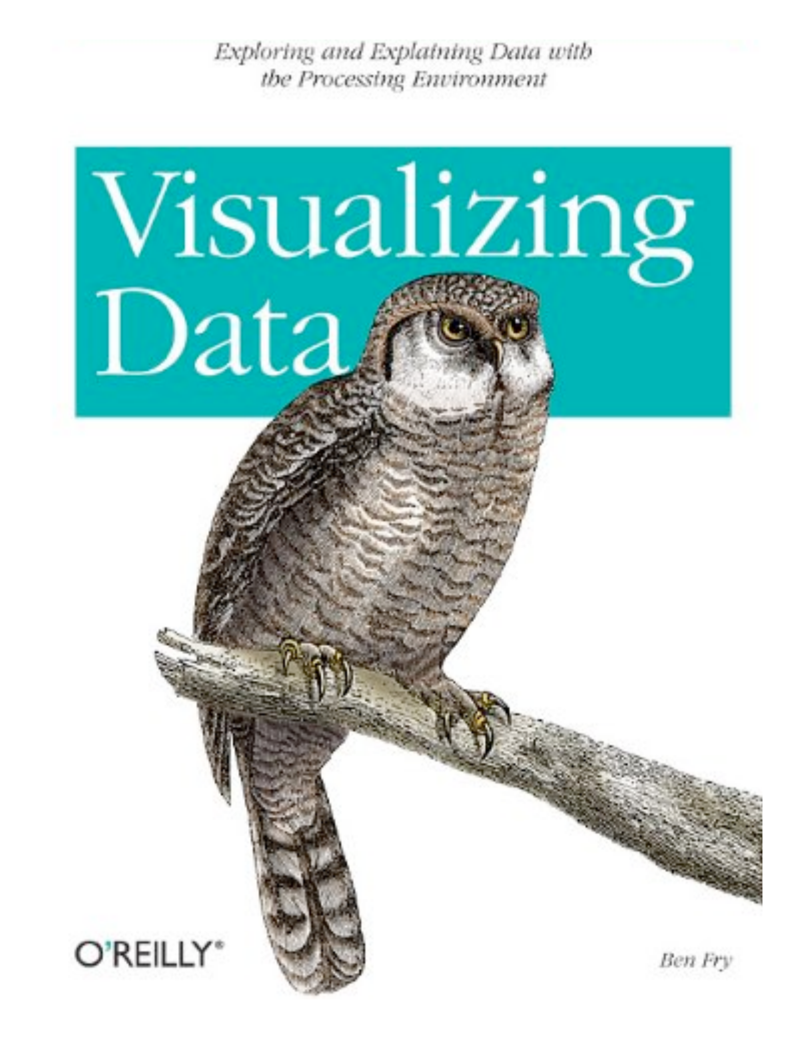
Named Entity Recognition

“Parsing data to extract & classify information”

“Greg bought 300,000 shares of LIGATT in 2010”

```
<ENAMEX TYPE="PERSON">Greg</ENAMEX> bought
<NUMEX TYPE="QUANTITY">300,000</NUMEX> shares of
<ENAMEX TYPE="ORGANIZATION">LIGATT</ENAMEX> in
<TIMEX TYPE="DATE">2010</TIMEX>.
```

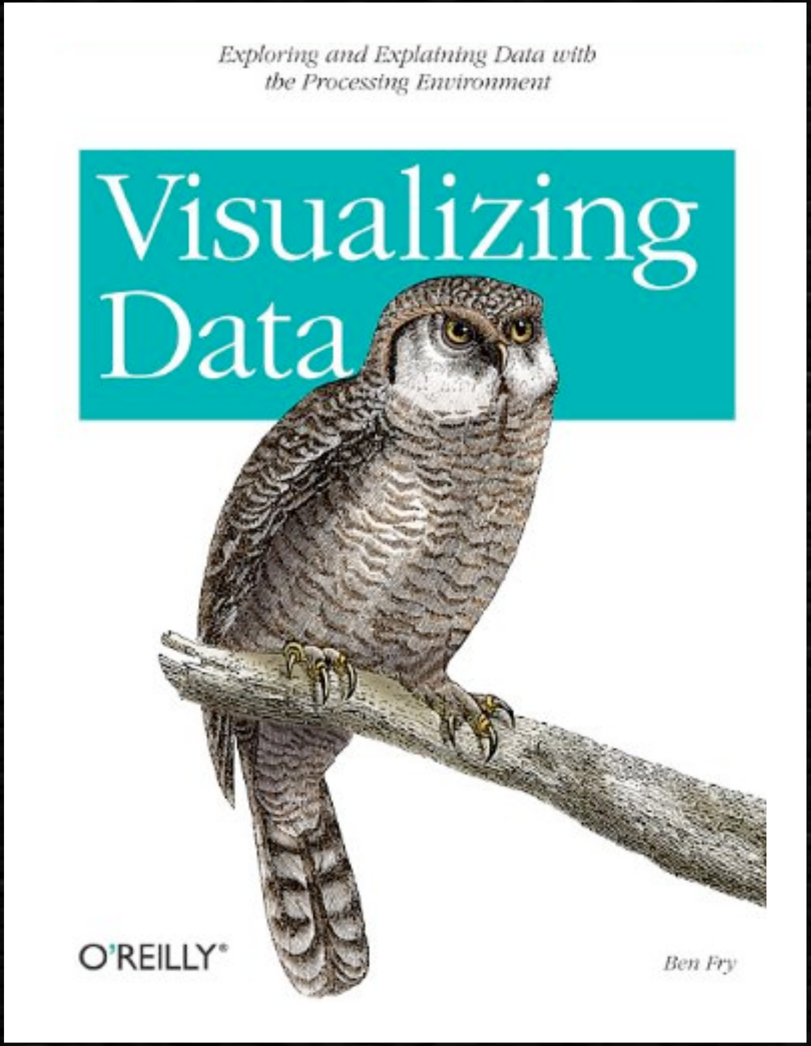
Data Visualization


Exploring and Explaining Data with the Processing Environment
Visualizing Data
O'REILLY®
Ben Fry

1. Acquire
2. Parse
3. Filter
4. Mine
5. Represent
6. Refine
7. Interact

Ben Fry

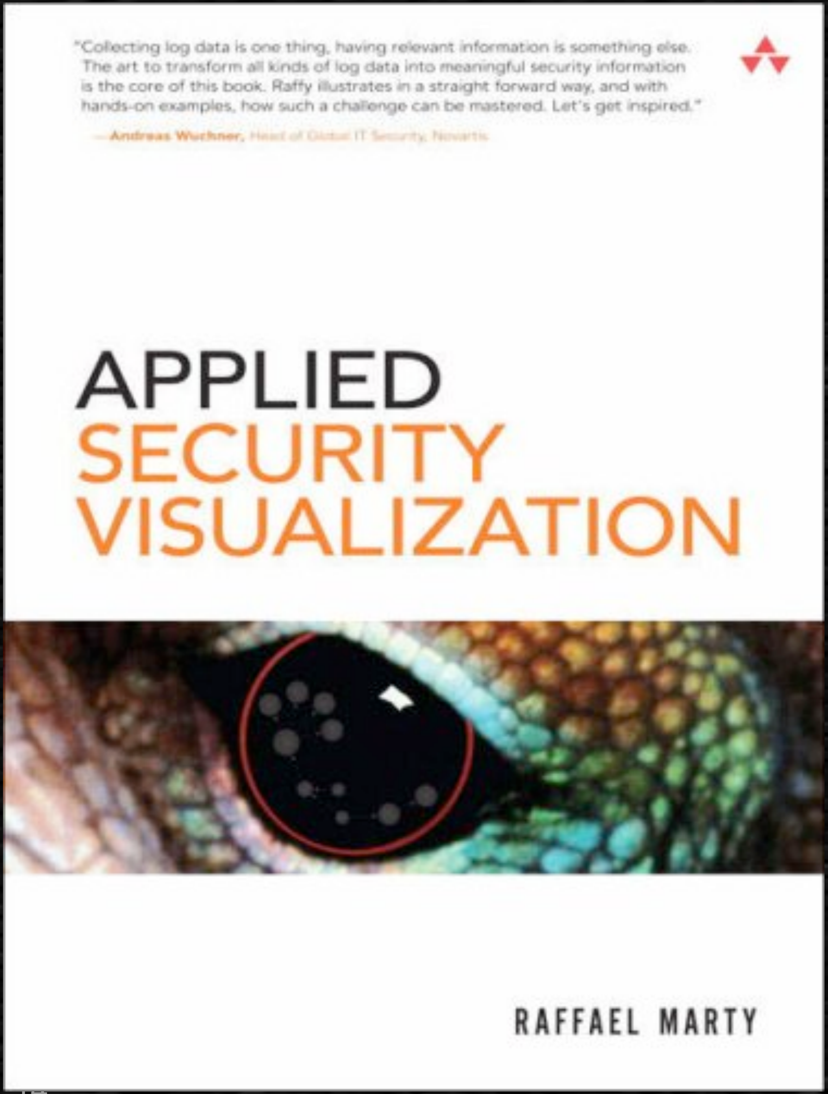
Data Visualization


Exploring and Explaining Data with the Processing Environment
Visualizing Data
O'REILLY
Ben Fry

1. Acquire
2. Parse
3. Filter
4. Mine
5. Represent
6. Refine
7. Interact

Ben Fry

Raffael Marty



"Collecting log data is one thing, having relevant information is something else. The art to transform all kinds of log data into meaningful security information is the core of this book. Raffy illustrates in a straight forward way, and with hands-on examples, how such a challenge can be mastered. Let's get inspired."

—Andreas Wuchner, Head of Global IT Security, Novartis

APPLIED
SECURITY
VISUALIZATION

RAFFAEL MARTY

Check out secviz.org

Tools

- Maltego
- Processing
- Prefuse and PrefuseFlare toolkit
- Afterglow
- DAVIX (Data Analysis & Visualization Linux)
- TouchGraph
- Vizster
- Graphviz

What the &$#@! is Maltego?

21 September 2009

Maltego

Maltego

- An information gathering tool that allows you to visually see relationships.

Maltego

- An information gathering tool that allows you to visually see relationships.
- Infrastructure
  - – DNS, IP Addresses, URLs, MX Records

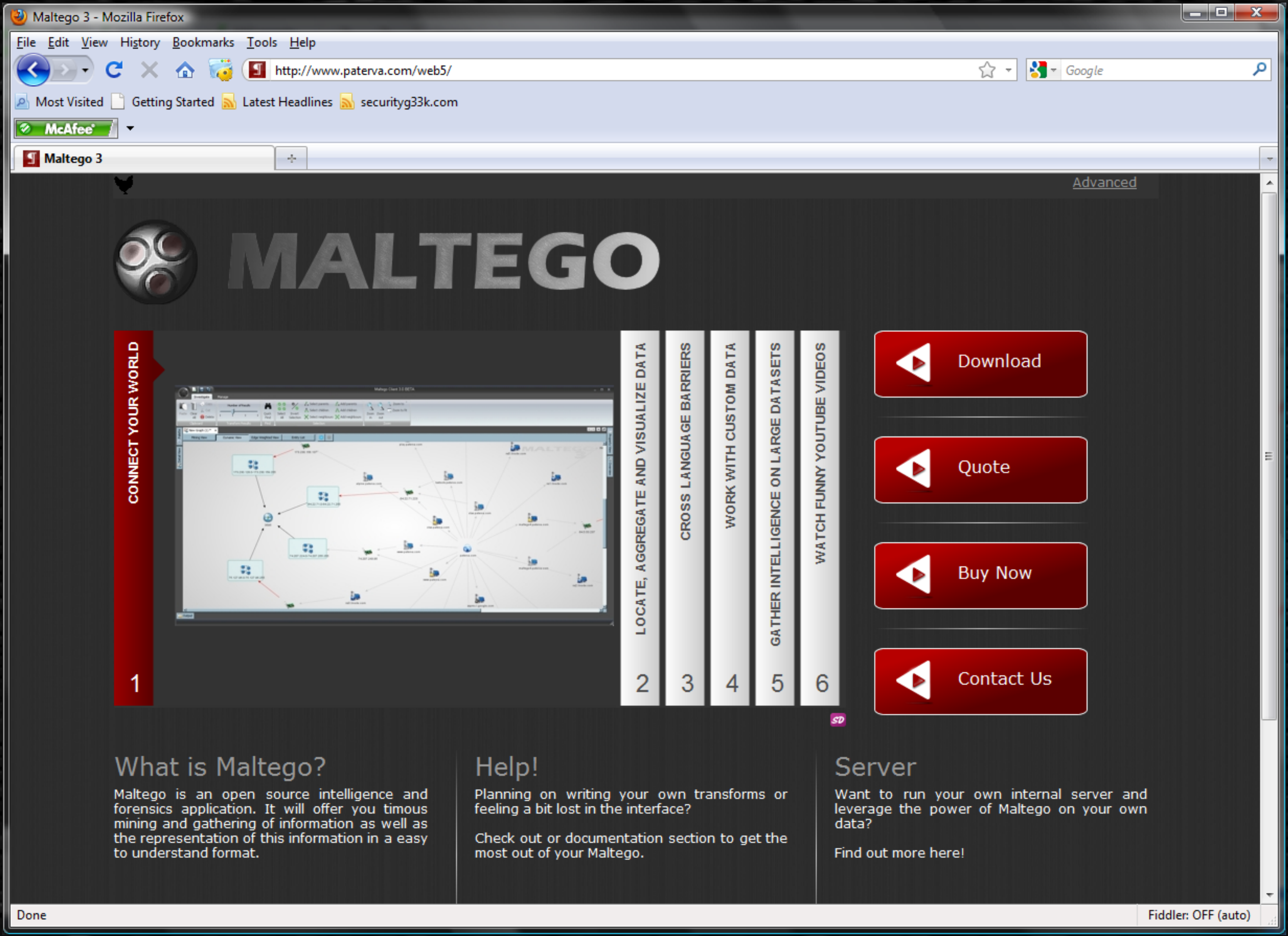
Maltego

- An information gathering tool that allows you to visually see relationships.
- Infrastructure
  - DNS, IP Addresses, URLs, MX Records
- Human
  - Email, Phone…

Maltego

- An information gathering tool that allows you to visually see relationships.
- Infrastructure
  - DNS, IP Addresses, URLs, MX Records
- Human
  - Email, Phone…
- Other… Extendable by design

www.paterva.com


Maltego 3 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.paterva.com/web5/
Google
Most Visited
Getting Started
Latest Headlines
securityg33k.com
McAfee
Maltego 3
Advanced
MALTEGO
CONNECT YOUR WORLD 1
LOCATE, AGGREGATE AND VISUALIZE DATA 2
CROSS LANGUAGE BARRIERS 3
WORK WITH CUSTOM DATA 4
GATHER INTELLIGENCE ON LARGE DATASETS 5
WATCH FUNNY YOUTUBE VIDEOS 6
Download
Quote
Buy Now
Contact Us
Done
Fiddler: OFF (auto)

What is Maltego?

Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.

Help!

Planning on writing your own transforms or feeling a bit lost in the interface?

Check out or documentation section to get the most out of your Maltego.

Server

Want to run your own internal server and leverage the power of Maltego on your own data?

Find out more here!

www.paterva.com

25%
Discount
‘BlackHat’

Maltego 3 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.paterva.com/web5/
Most Visited
Getting Started
Latest Headlines
securityg33k.com
McAfee
Maltego 3
MALTEGO
CONNECT YOUR WORLD 1
LOCATE, AGGREGATE AND VISUALIZE DATA 2
CROSS LANGUAGE BARRIERS 3
WORK WITH CUSTOM DATA 4
GATHER INTELLIGENCE ON LARGE DATASETS 5
WATCH FUNNY YOUTUBE VIDEOS 6
Quote
Buy Now
Contact Us
Done
Fiddler: OFF (auto)

What is Maltego?

Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.

Help!

Planning on writing your own transforms or feeling a bit lost in the interface?

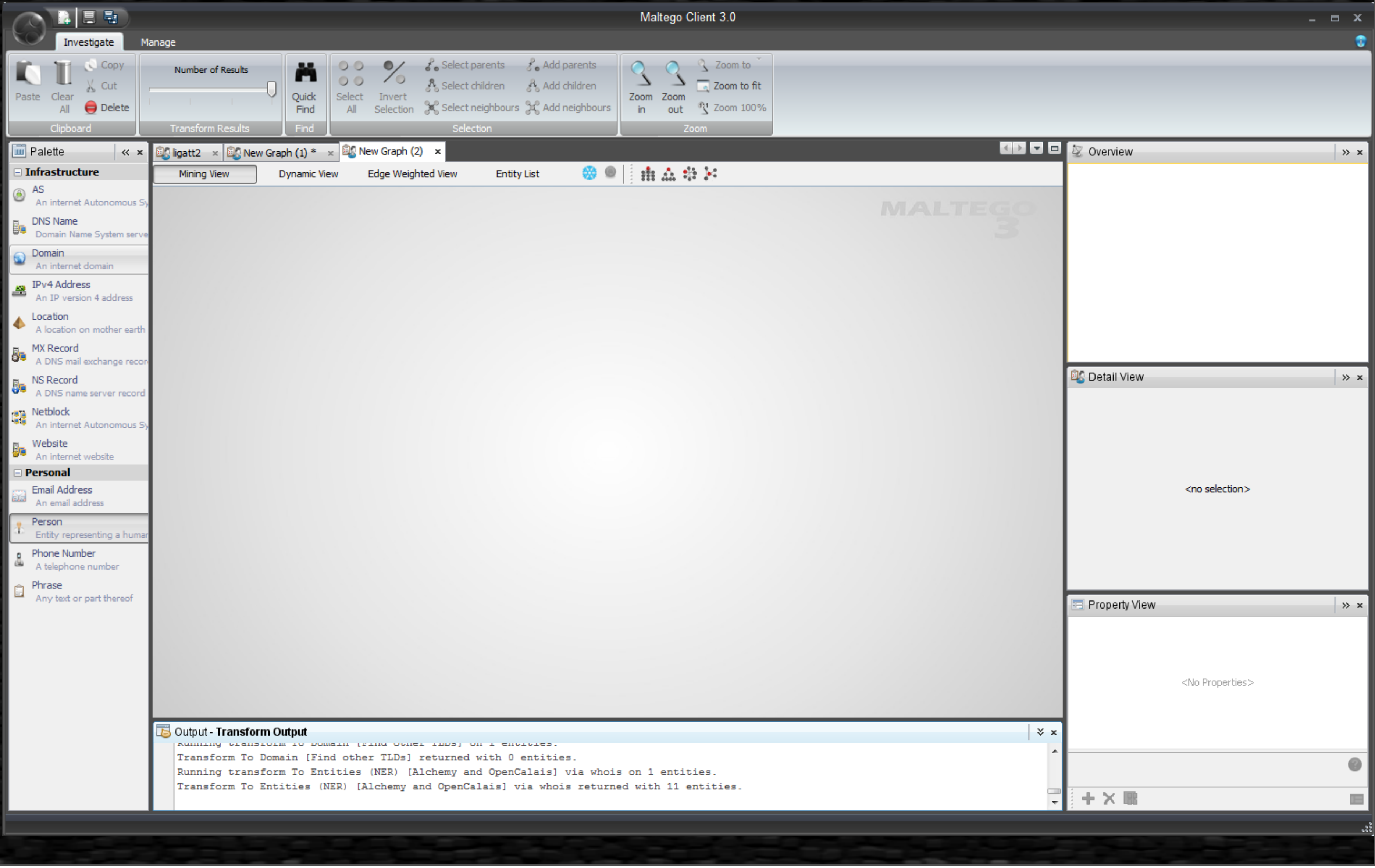
Check out or documentation section to get the most out of your Maltego.

Server

Want to run your own internal server and leverage the power of Maltego on your own data?

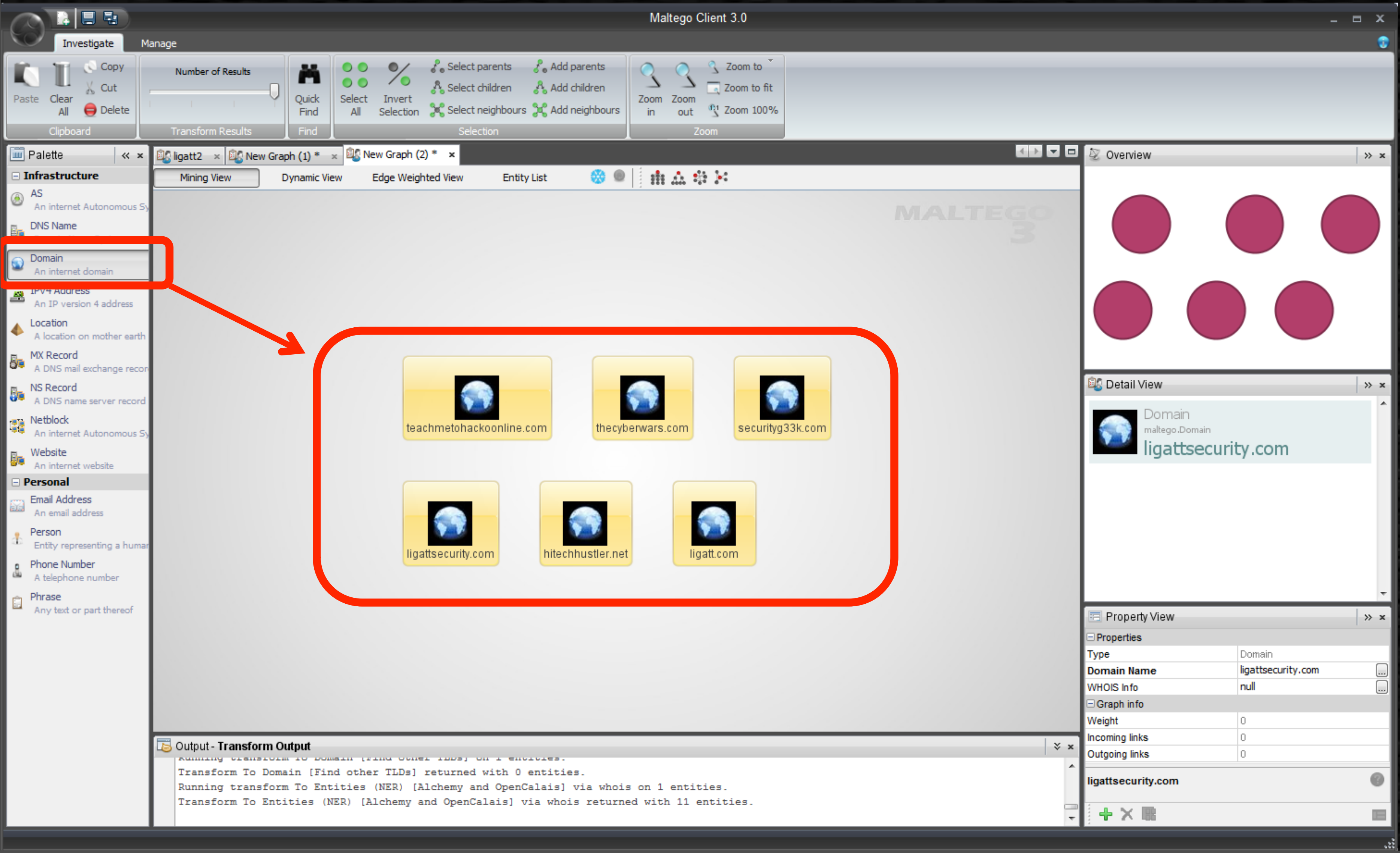
Find out more here!

E.G.



```
Running transform To Domain [Find other TLDs] on 1 entities.
Transform To Domain [Find other TLDs] returned with 0 entities.
Running transform To Entities (NER) [Alchemy and OpenCalais] via whois on 1 entities.
Transform To Entities (NER) [Alchemy and OpenCalais] via whois returned with 11 entities.
```

Domains



Properties

Type	Domain
Domain Name	ligattsecurity.com
WHOIS Info	null

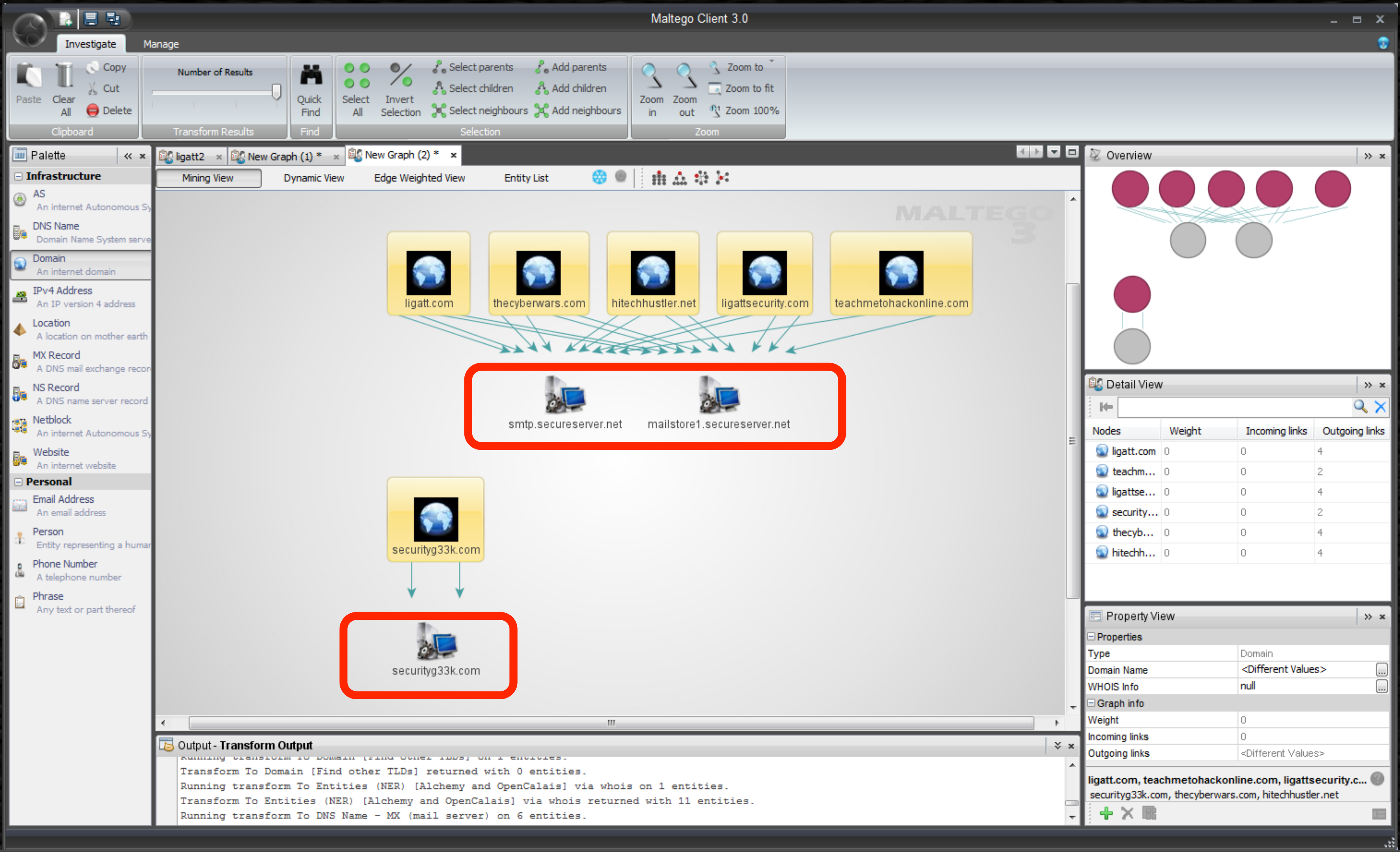
Graph info

Weight	0
Incoming links	0
Outgoing links	0

ligattsecurity.com

```
Running transform To Domain [Find other TLDs] on 1 entities.
Transform To Domain [Find other TLDs] returned with 0 entities.
Running transform To Entities (NER) [Alchemy and OpenCalais] via whois on 1 entities.
Transform To Entities (NER) [Alchemy and OpenCalais] via whois returned with 11 entities.
```

MX Records



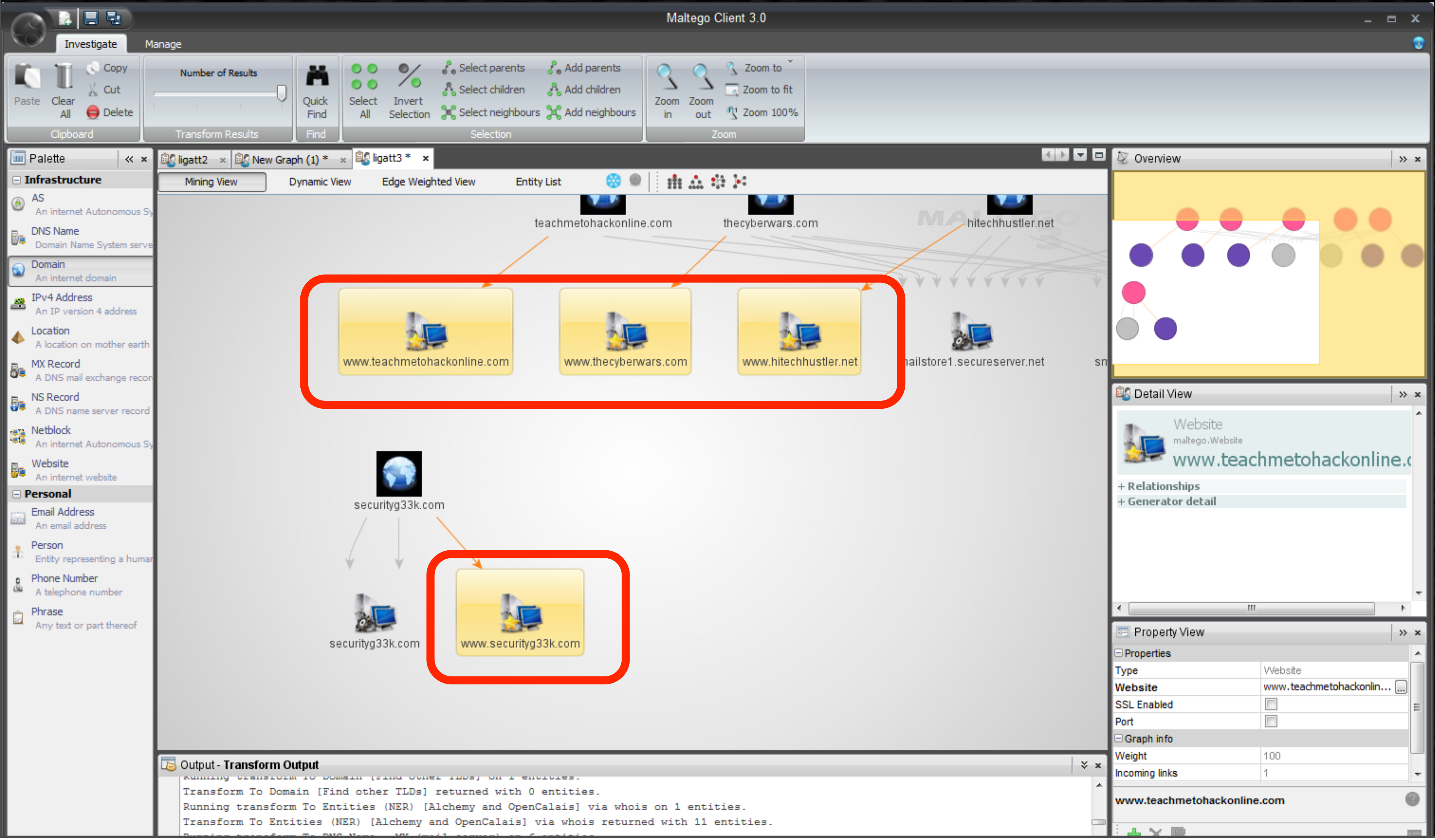
Nodes	Weight	Incoming links	Outgoing links
ligatt.com	0	0	4
teachm...	0	0	2
ligattse...	0	0	4
security...	0	0	2
thecyb...	0	0	4
hitechh...	0	0	4

Properties	
Type	Domain
Domain Name	<Different Values>
WHOIS Info	null
Graph info	
Weight	0
Incoming links	0
Outgoing links	<Different Values>

ligatt.com, teachmetohackonline.com, ligattsecurity.c...
securityg33k.com, thecyberwars.com, hitechhustler.net

```
Running transform To Domain [Find other TLDs] on 1 entities.
Transform To Domain [Find other TLDs] returned with 0 entities.
Running transform To Entities (NER) [Alchemy and OpenCalais] via whois on 1 entities.
Transform To Entities (NER) [Alchemy and OpenCalais] via whois returned with 11 entities.
Running transform To DNS Name - MX (mail server) on 6 entities.
```

Web Sites...



Website
maltego.Website
www.teachmetohackonline.c

+ Relationships
+ Generator detail

Properties

Type	Website
Website	www.teachmetohackonlin...
SSL Enabled	□
Port	□

Graph info

Weight	100
Incoming links	1

www.teachmetohackonline.com

```
Running transform To Domain [Find other TLDs] on 1 entities.
Transform To Domain [Find other TLDs] returned with 0 entities.
Running transform To Entities (NER) [Alchemy and OpenCalais] via whois on 1 entities.
Transform To Entities (NER) [Alchemy and OpenCalais] via whois returned with 11 entities.
Running transform To DNS Name - MX (mail server) on 6 entities.
```

21 September 2009

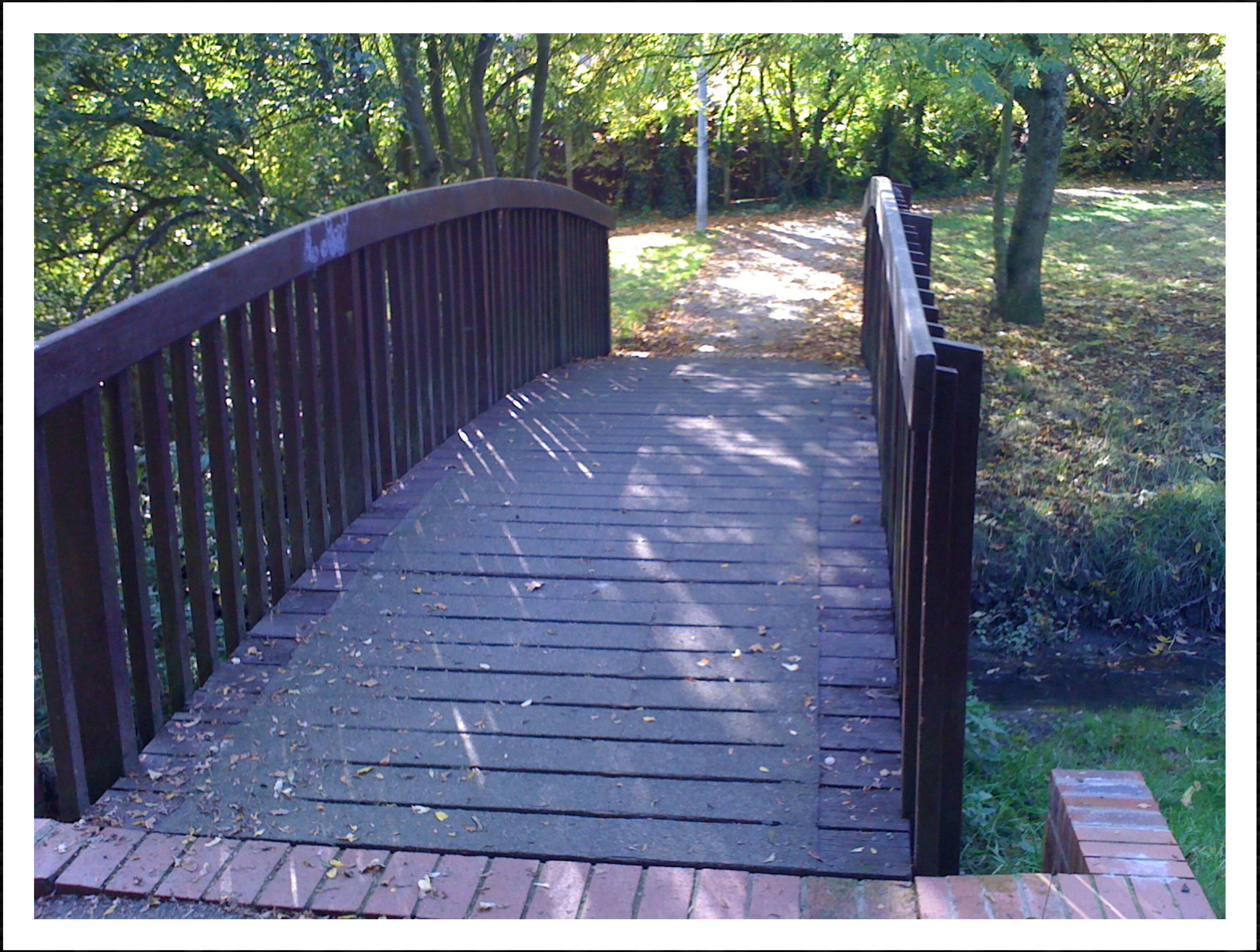
Tony Hawk Twitter Hunt versus Maltego

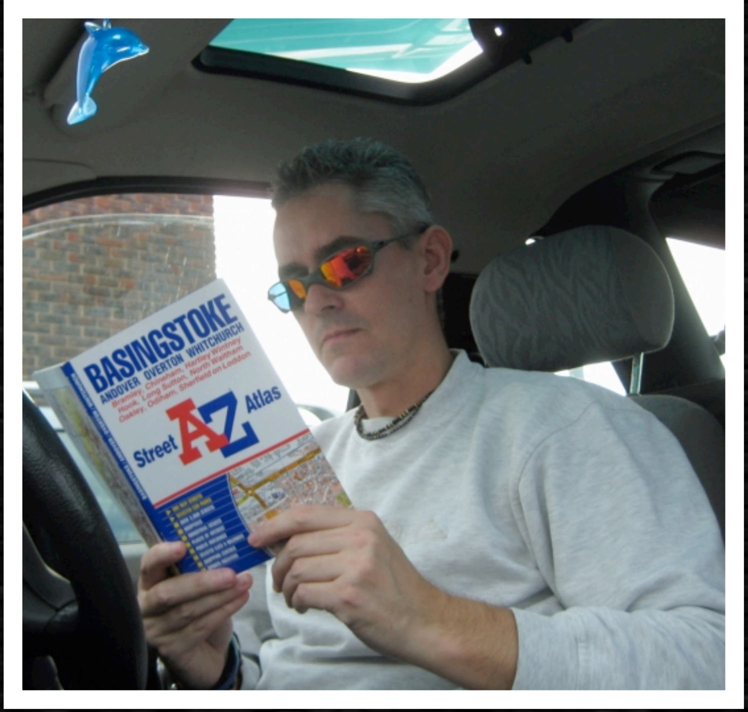
21 September 2009

#THTH

#THTH
STANFORD

“Guarded by a fearsome troll, NW from a house where you might have to pay money to pass & a sk8park”





@steven_gill

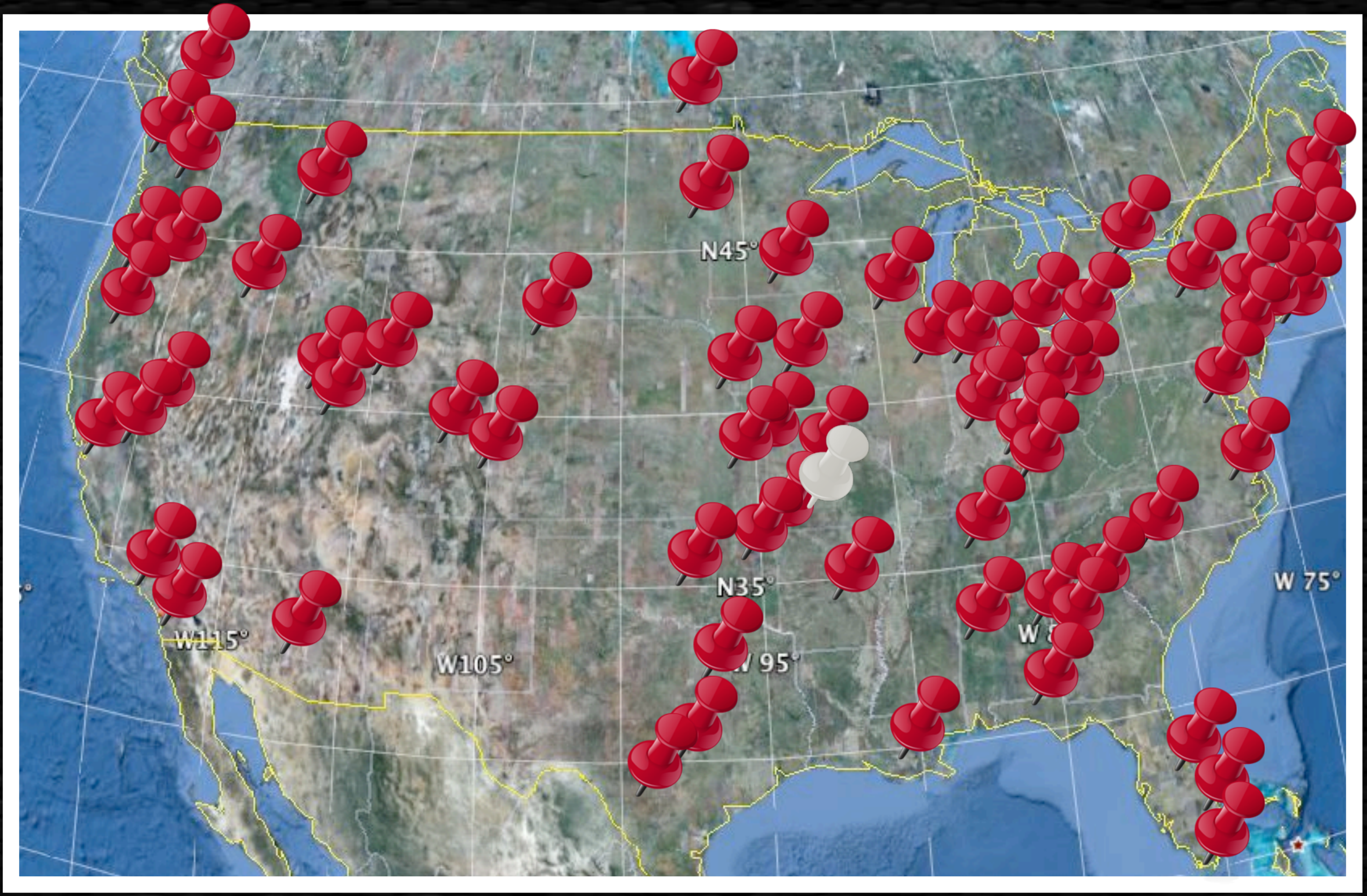
“cammo netting!
You’re a bad man”

@steven_gill

#THTH
I HACK CHARITIES.ORG
SHRED OR DIE
SHRED OR
Birdhouse
TECH DECK
birdhouse

obviously

I wanted to see a map

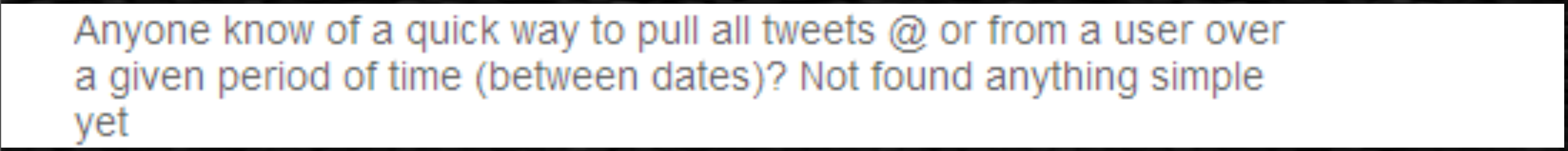


Should be easy enough

- Hiders are all friends of @hidingit
- Finders all tweet @ifoundone when they find one.
- Tony sends out “Found” tweets with #THTH

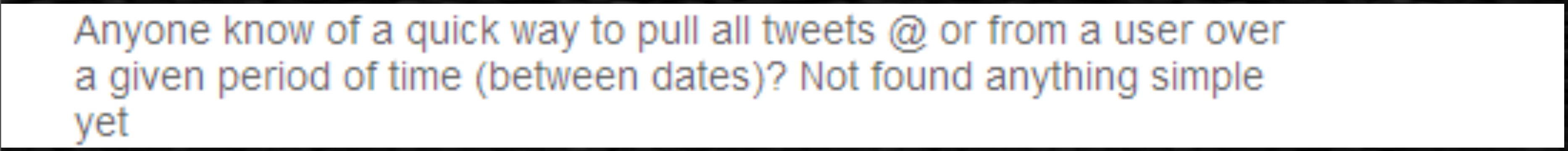
Twitter’ll fix it

Twitter’ll fix it

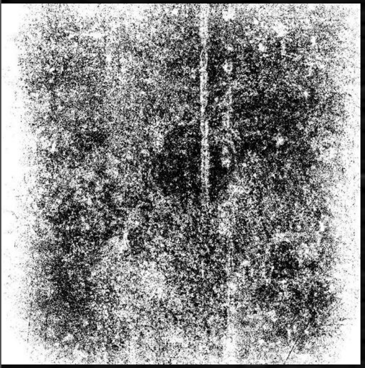


Anyone know of a quick way to pull all tweets @ or from a user over a given period of time (between dates)? Not found anything simple yet

Twitter’ll fix it

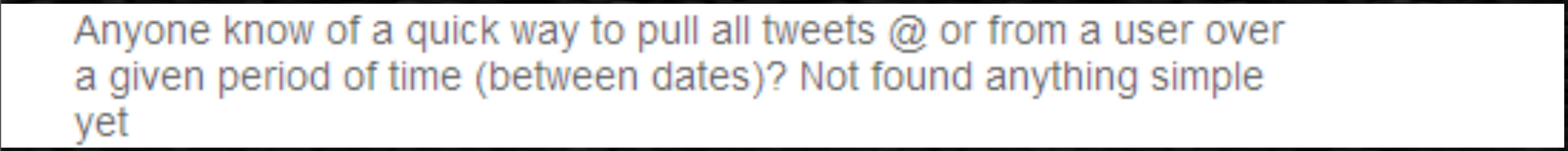


Anyone know of a quick way to pull all tweets @ or from a user over a given period of time (between dates)? Not found anything simple yet

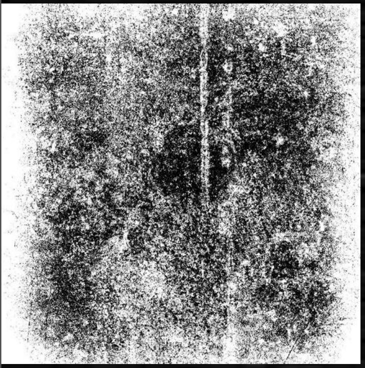


@l0sthighway

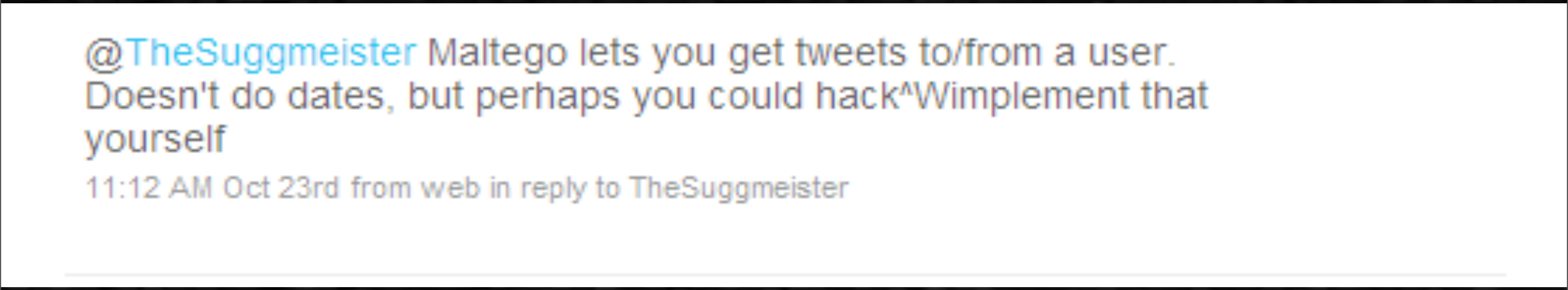
Twitter’ll fix it



Anyone know of a quick way to pull all tweets @ or from a user over a given period of time (between dates)? Not found anything simple yet



@l0sthighway



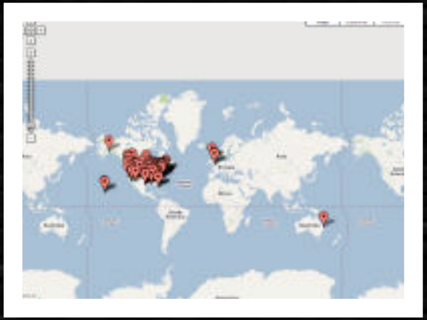
@TheSuggmeister Maltego lets you get tweets to/from a user. Doesn't do dates, but perhaps you could hack^Wimplement that yourself

11:12 AM Oct 23rd from web in reply to TheSuggmeister

Hypothesis

+

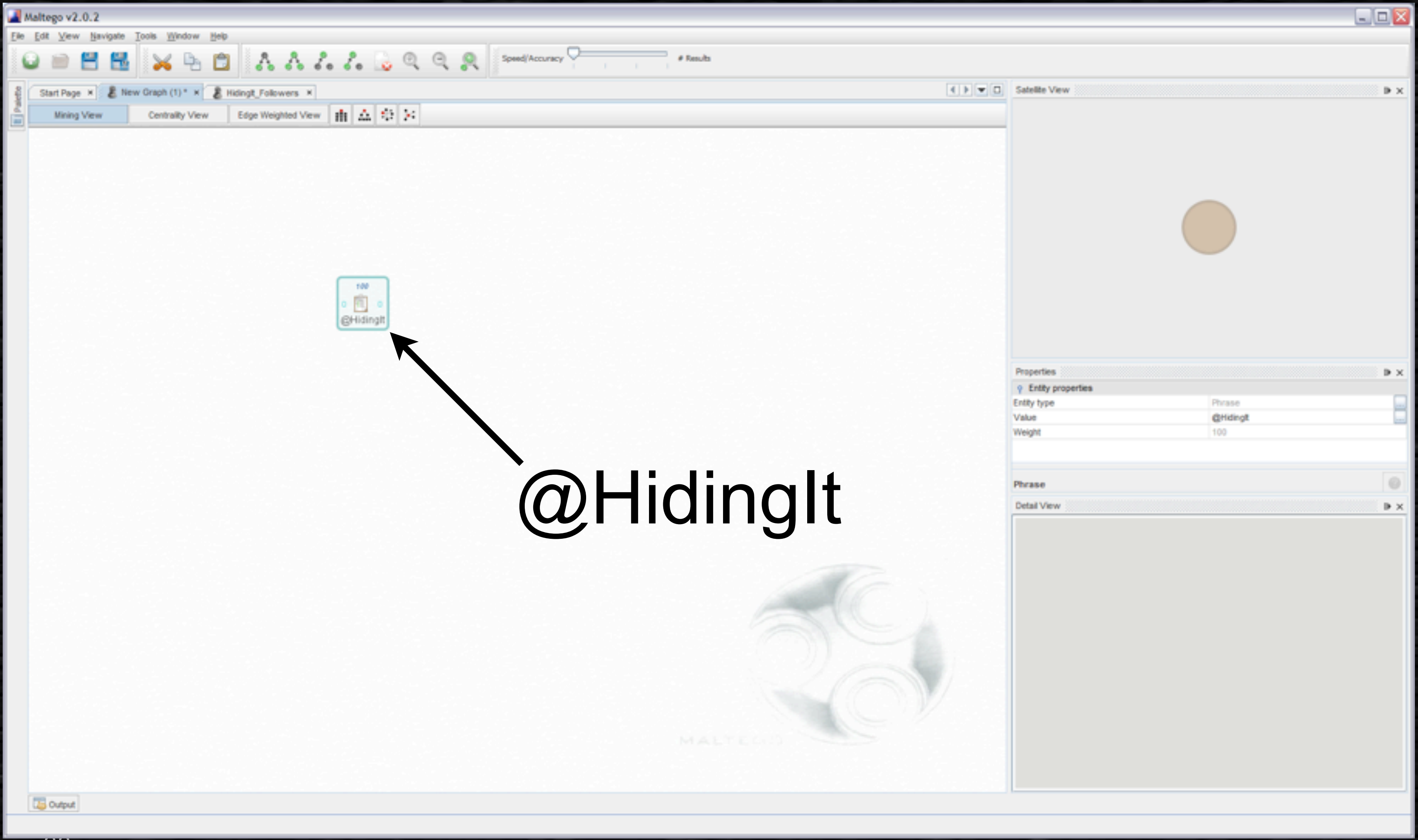
=



=

List the Hiders

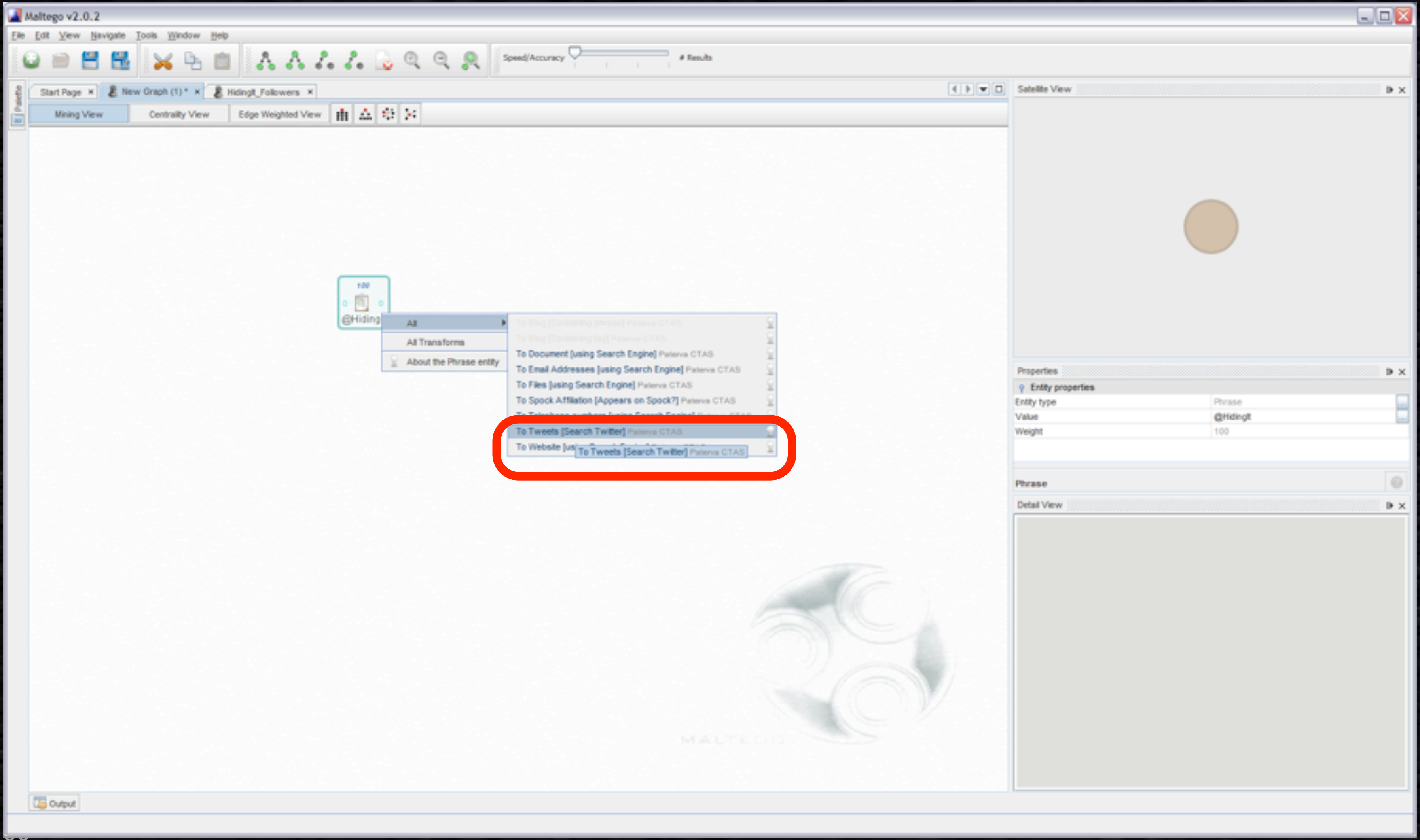
Derive @HidingIt



Entity type	Phrase
Value	@Hidingit
Weight	100

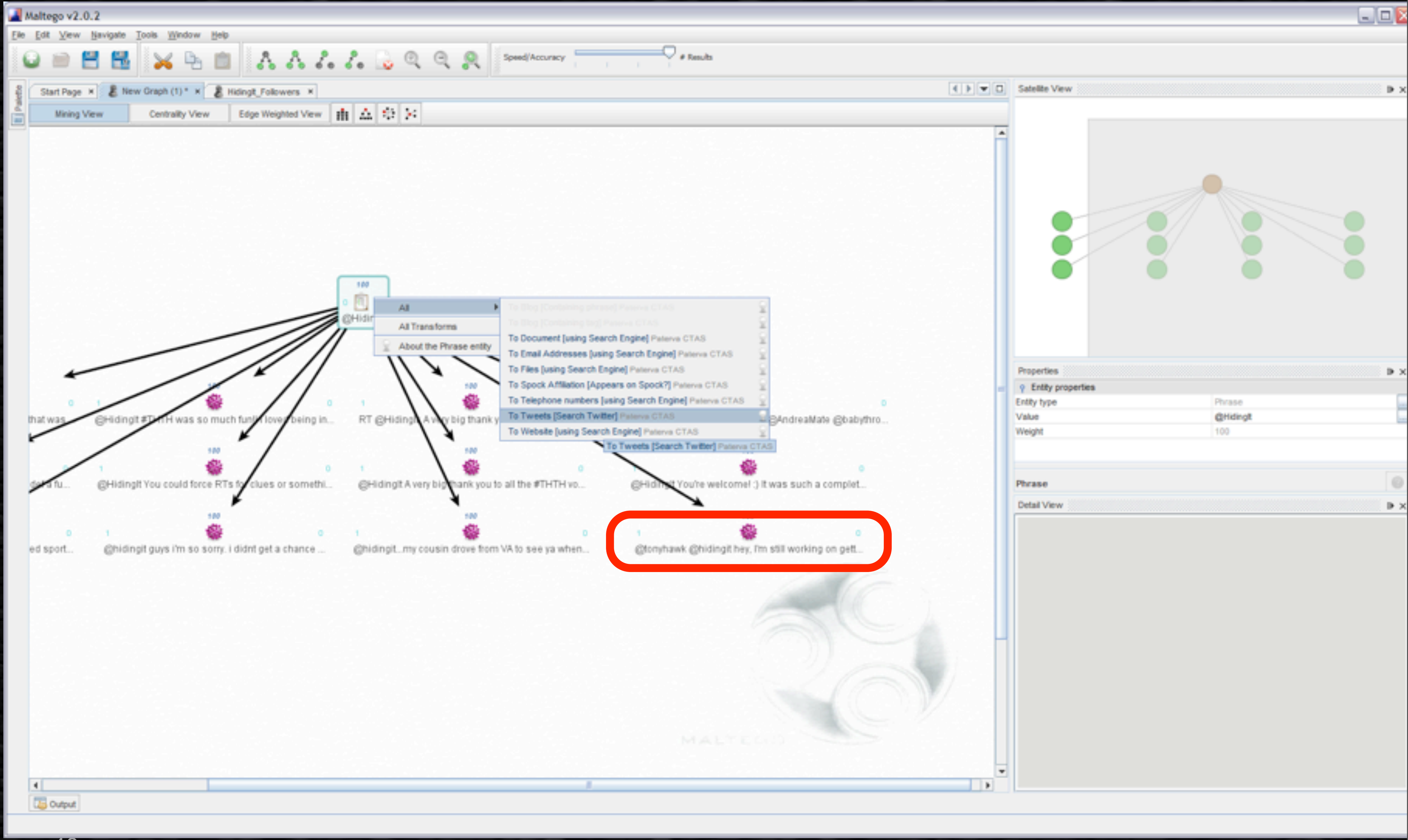
@HidingIt

To Tweets [Search Twitter]


Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
# Results
Start Page
New Graph (1) *
Hidingt_Followers
Mining View
Centrality View
Edge Weighted View
Satellite View
100
@Hiding
All
All Transforms
About the Phrase entity
To Blog [Containing phrase] Paterva CTAS
To Blog [Containing tag] Paterva CTAS
To Document [using Search Engine] Paterva CTAS
To Email Addresses [using Search Engine] Paterva CTAS
To Files [using Search Engine] Paterva CTAS
To Spock Affiliation [Appears on Spock?] Paterva CTAS
To Telephone numbers [using Search Engine] Paterva CTAS
To Tweets [Search Twitter] Paterva CTAS
To Website [us
To Tweets [Search Twitter] Paterva CTAS
Properties
Entity properties
Phrase
Detail View
MALTEGO
Output

Entity type	Phrase
Value	@Hidingt
Weight	100

Tweets


Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
# Results
Start Page
New Graph (1) *
Hidingit_Followers
Mining View
Centrality View
Edge Weighted View
All
All Transforms
About the Phrase entity
To Document [using Search Engine] Paterva CTAS
To Email Addresses [using Search Engine] Paterva CTAS
To Files [using Search Engine] Paterva CTAS
To Spock Affiliation [Appears on Spock?] Paterva CTAS
To Telephone numbers [using Search Engine] Paterva CTAS
To Tweets [Search Twitter] Paterva CTAS
To Website [using Search Engine] Paterva CTAS
To Tweets [Search Twitter] Paterva CTAS
Satellite View
Properties
Entity properties
Entity type
Phrase
Value
@Hidingit
Weight
100
Phrase
Detail View
Output
MALTEGO

that was...

@HidingIt #THTH was so much fun! I love being in...

RT @HidingIt A very big thank y...

@AndreaMate @babythro...

@HidingIt You could force RTs for clues or somethi...

@HidingIt A very big thank you to all the #THTH vo...

@HidingIt You're welcome! :) It was such a complet...

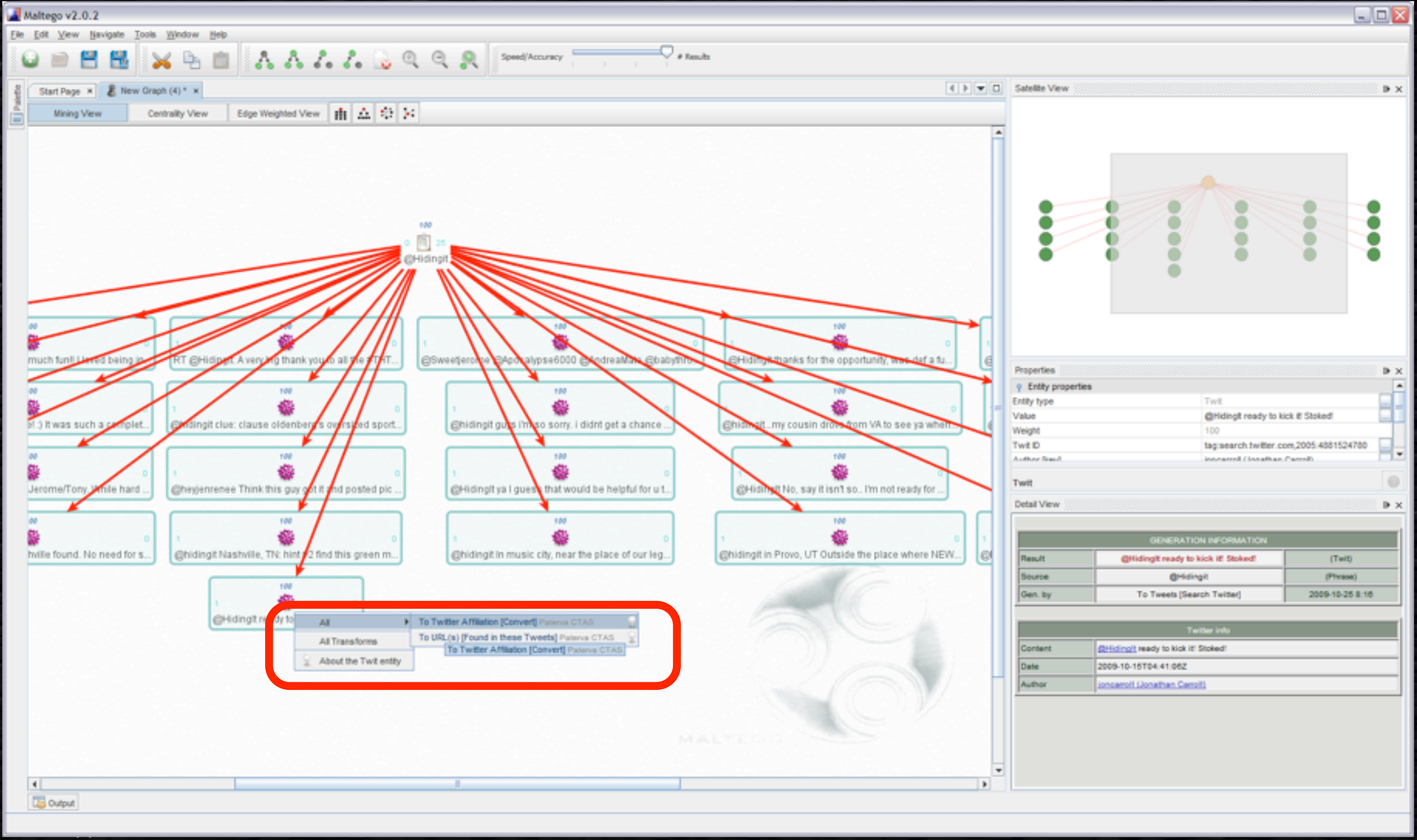
ed sport...

@hidingit guys i'm so sorry. i didnt get a chance ...

@hidingit...my cousin drove from VA to see ya when...

@tonyhawk @hidingit hey, I'm still working on gett...

To Twiiter Affiliation [Convert]


Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
# Results
Start Page
New Graph (4) *
Mining View
Centrality View
Edge Weighted View
Satellite View
@Hidingit
All
All Transforms
About the Twit entity
To Twitter Affiliation [Convert] Paterva CTAS
To URL(s) [Found in these Tweets] Paterva CTAS
To Twitter Affiliation [Convert] Paterva CTAS
Output

Properties

Entity properties

Entity type	Twit
Value	@Hidingit ready to kick it! Stoked!
Weight	100
Twit ID	tag:search.twitter.com,2005:4881524780
Author [[illegible]	joncarroll (Jonathan Carroll)

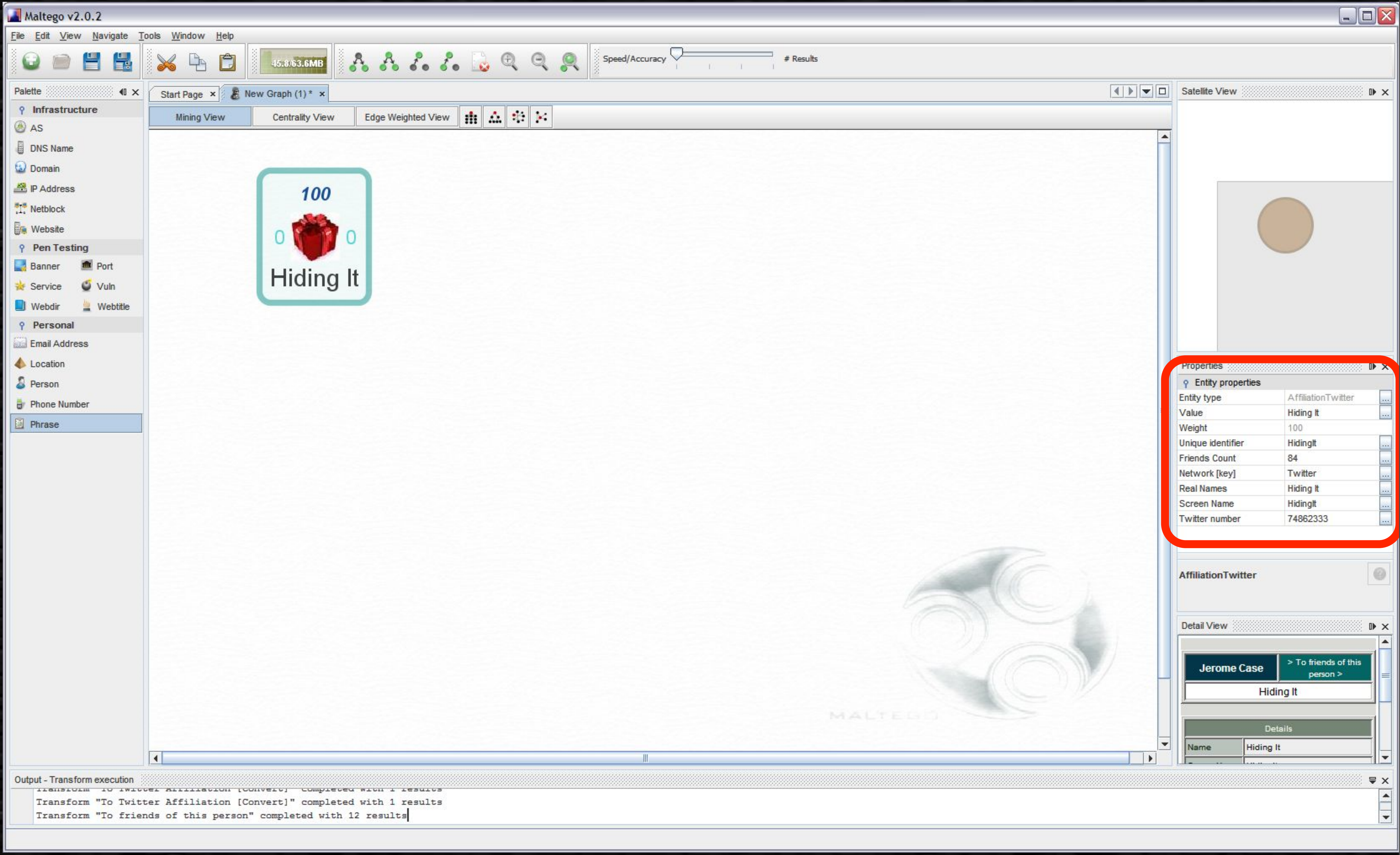
Twit

Detail View

GENERATION INFORMATION		
Result	@Hidingit ready to kick it! Stoked!	(Twit)
Source	@Hidingit	(Phrase)
Gen. by	To Tweets [Search Twitter]	2009-10-25 8:16

Twitter info	
Content	@Hidingit ready to kick it! Stoked!
Date	2009-10-15T04:41:06Z
Author	joncarroll (Jonathan Carroll)

Tuesday, 3 August 2010

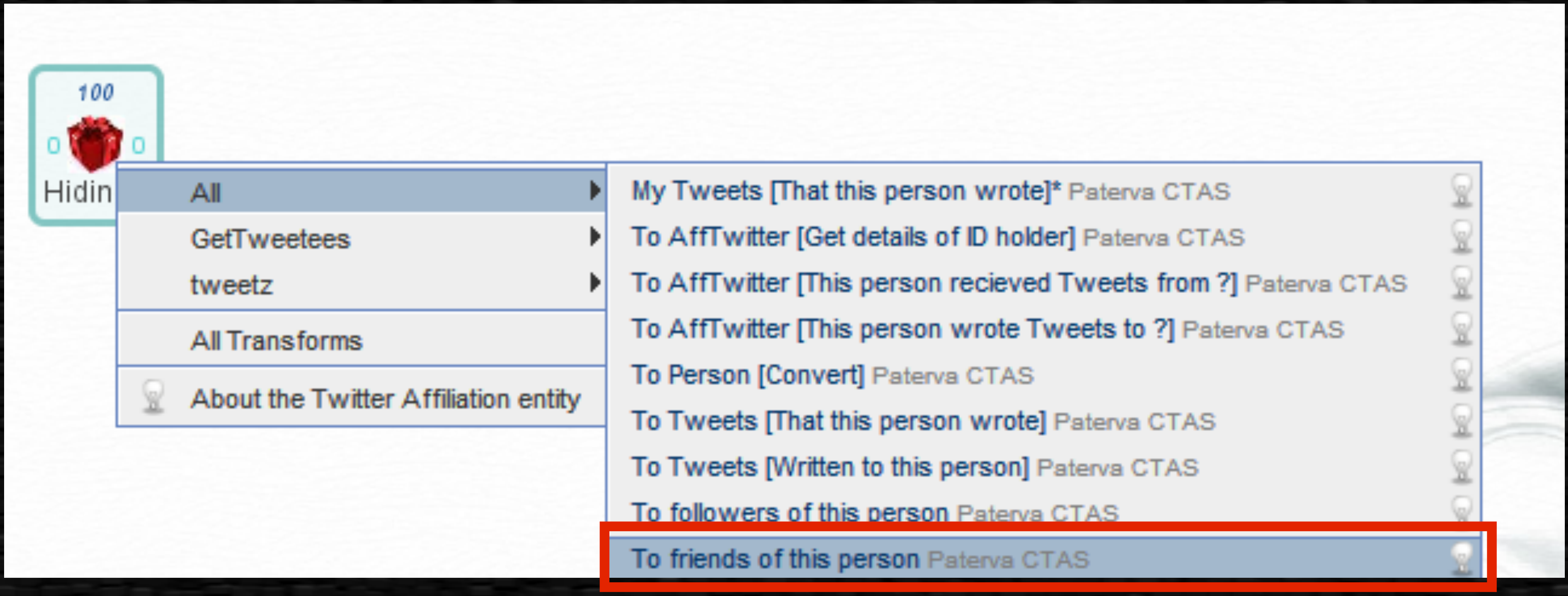


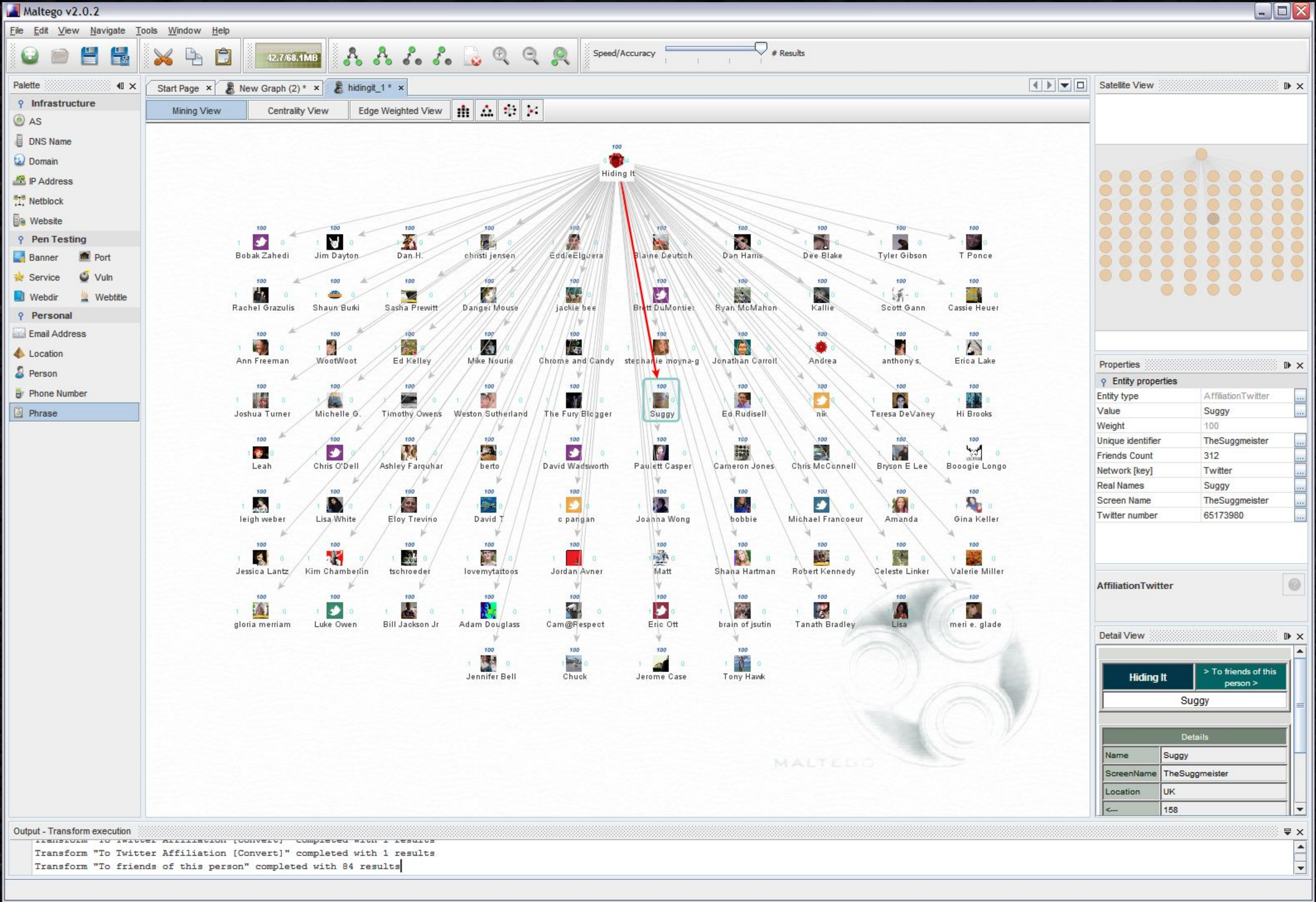
Entity properties

Entity type	AffiliationTwitter
Value	Hiding It
Weight	100
Unique identifier	HidingIt
Friends Count	84
Network [key]	Twitter
Real Names	Hiding It
Screen Name	HidingIt
Twitter number	74862333

```
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 12 results
```

To friends of this person


100
0
0
Hidin
All
GetTweetees
tweetz
All Transforms
About the Twitter Affiliation entity
My Tweets [That this person wrote]* Paterva CTAS
To AffTwitter [Get details of ID holder] Paterva CTAS
To AffTwitter [This person recieved Tweets from ?] Paterva CTAS
To AffTwitter [This person wrote Tweets to ?] Paterva CTAS
To Person [Convert] Paterva CTAS
To Tweets [That this person wrote] Paterva CTAS
To Tweets [Written to this person] Paterva CTAS
To followers of this person Paterva CTAS
To friends of this person Paterva CTAS



Entity properties

Entity type	AffiliationTwitter
Value	Suggy
Weight	100
Unique identifier	TheSuggmeister
Friends Count	312
Network [key]	Twitter
Real Names	Suggy
Screen Name	TheSuggmeister
Twitter number	65173980

AffiliationTwitter

Hiding It > To friends of this person >

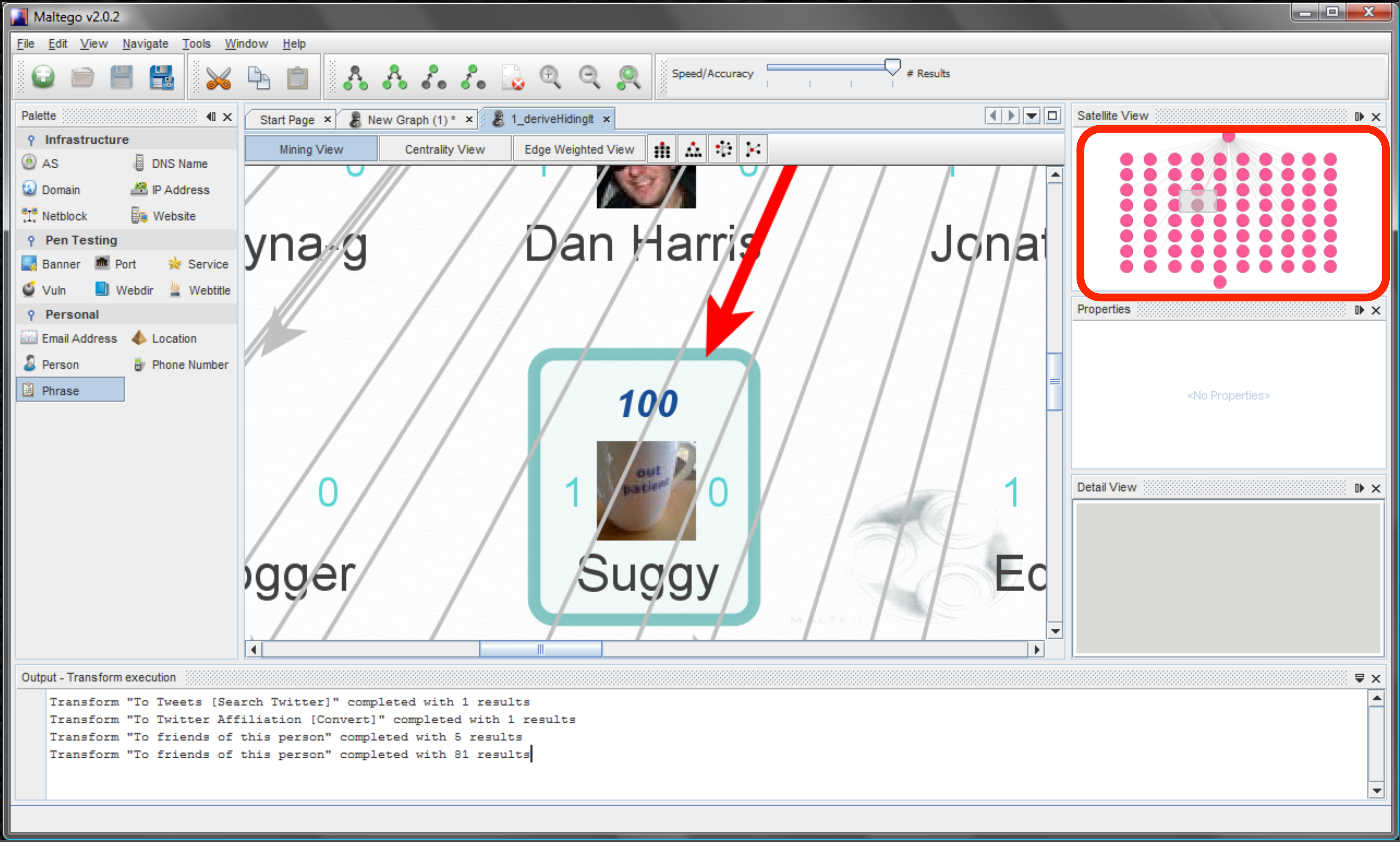
Suggy

Details

Name	Suggy
ScreenName	TheSuggmeister
Location	UK
<--	158

```
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 84 results
```

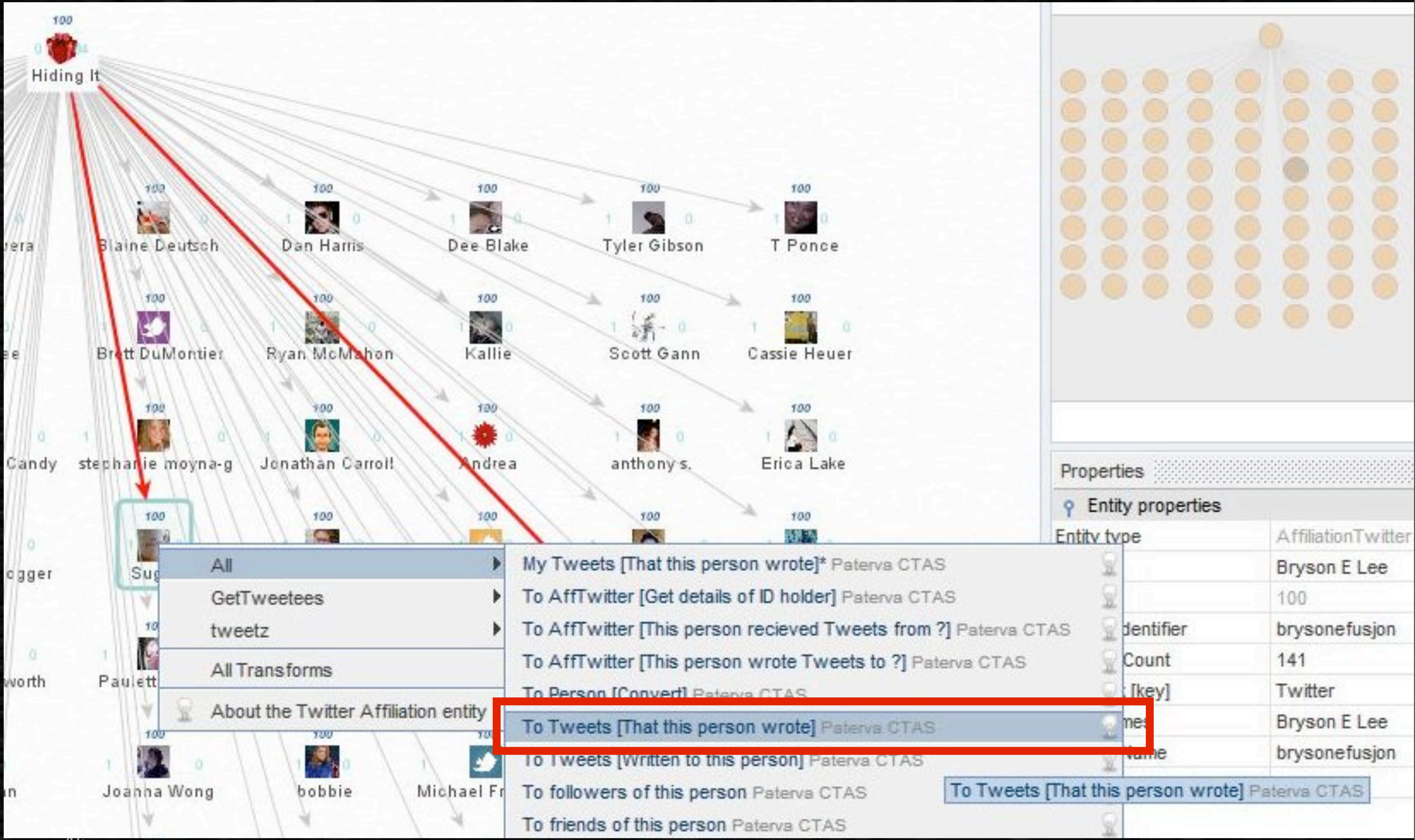
“Suggy”



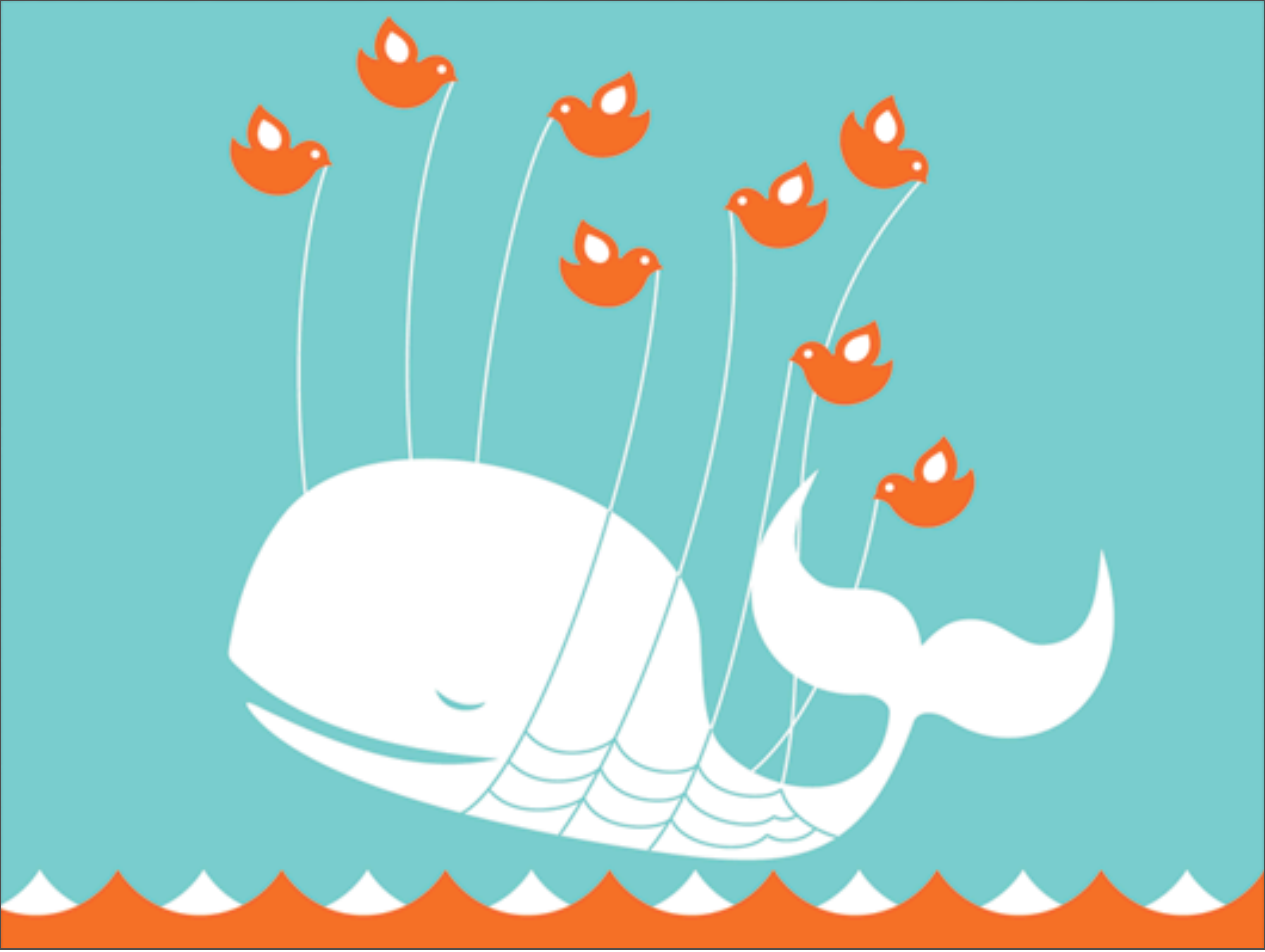
```
Transform "To Tweets [Search Twitter]" completed with 1 results
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 5 results
Transform "To friends of this person" completed with 81 results
```

Tuesday, 3 August 2010

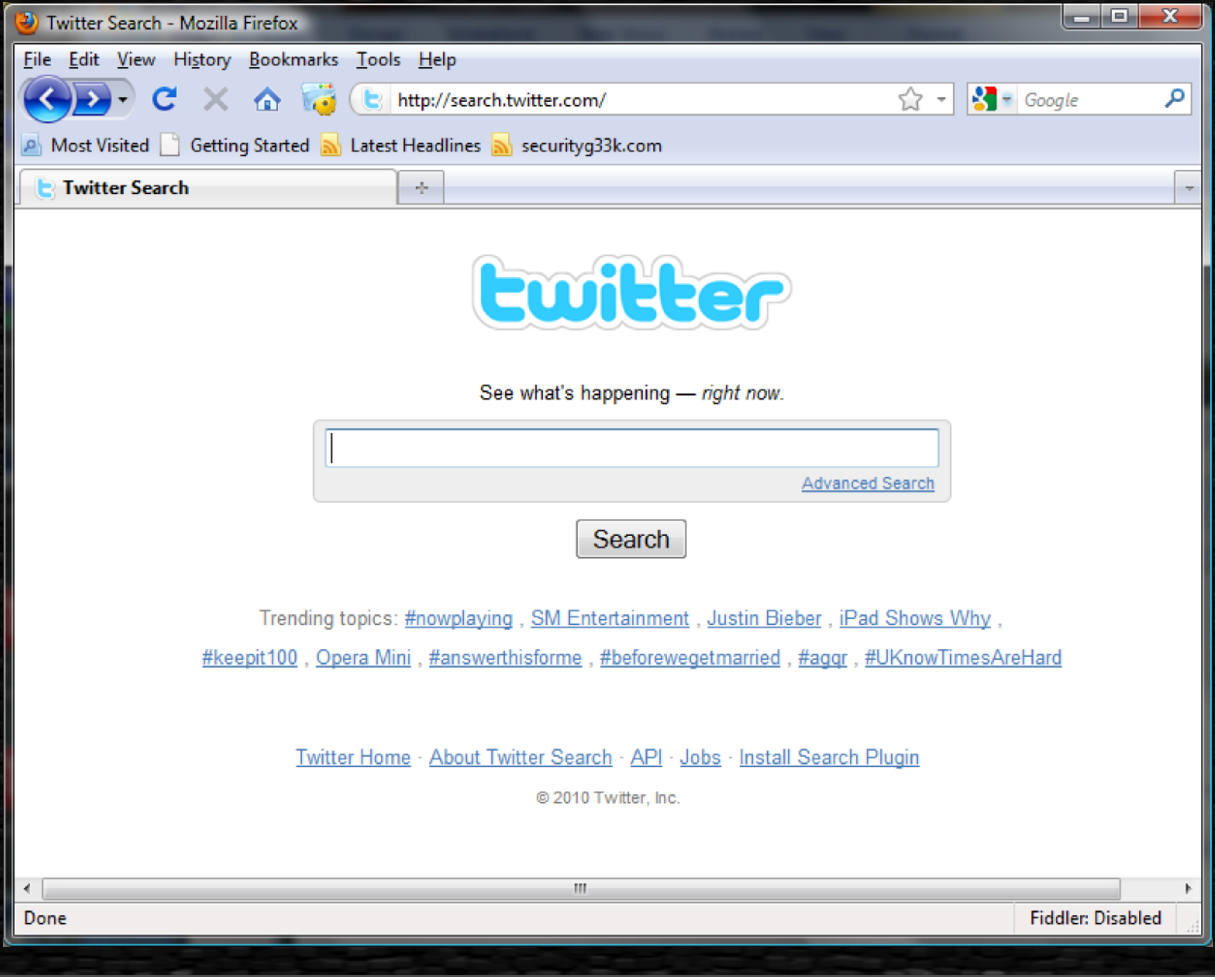
To Tweets [That this person wrote]


Hiding It
Blaine Deutsch
Dan Harris
Dee Blake
Tyler Gibson
T Ponce
Brett DuMontier
Ryan McMahon
Kallie
Scott Gann
Cassie Heuer
Candy
stephanie moyna-g
Jonathan Carroll
Andrea
anthony s.
Erica Lake
Sug
Paulett
Joanna Wong
bobbie
Michael Fr
All
GetTweetees
tweetz
All Transforms
About the Twitter Affiliation entity
My Tweets [That this person wrote]* Paterva CTAS
To AffTwitter [Get details of ID holder] Paterva CTAS
To AffTwitter [This person recieved Tweets from ?] Paterva CTAS
To AffTwitter [This person wrote Tweets to ?] Paterva CTAS
To Person [Convert] Paterva CTAS
To Tweets [That this person wrote] Paterva CTAS
To Tweets [Written to this person] Paterva CTAS
To followers of this person Paterva CTAS
To friends of this person Paterva CTAS
To Tweets [That this person wrote] Paterva CTAS
Properties
Entity properties

Entity type	AffiliationTwitter
	Bryson E Lee
	100
dentifier	brysonefusjon
Count	141
[key]	Twitter
me	Bryson E Lee
ame	brysonefusjon



Twitter Search Limitations



See what's happening — *right now.*

Trending topics: #nowplaying , SM Entertainment , Justin Bieber , iPad Shows Why , #keepit100 , Opera Mini , #answerthisforme , #beforewegetmarried , #aggr , #UKnowTimesAreHard

Twitter Home · About Twitter Search · API · Jobs · Install Search Plugin

© 2010 Twitter, Inc.

Local Transforms

If you can call script/program and pass input… AND

If you can get your output to STDOUT, THEN

you can write a local transform

Learn How to Build Applications with the Twitter API

Twitter API

Up and Running

O'REILLY®

Kevin Makice

3 x API's

- 2 x REST
- 1 x Streaming

- PERL & ::LWP e.g. from latest tweet

```
$url = "http://twitter.com/statuses/
  user_timeline.xml?count=200&id=" .
  $entityValue2;
```

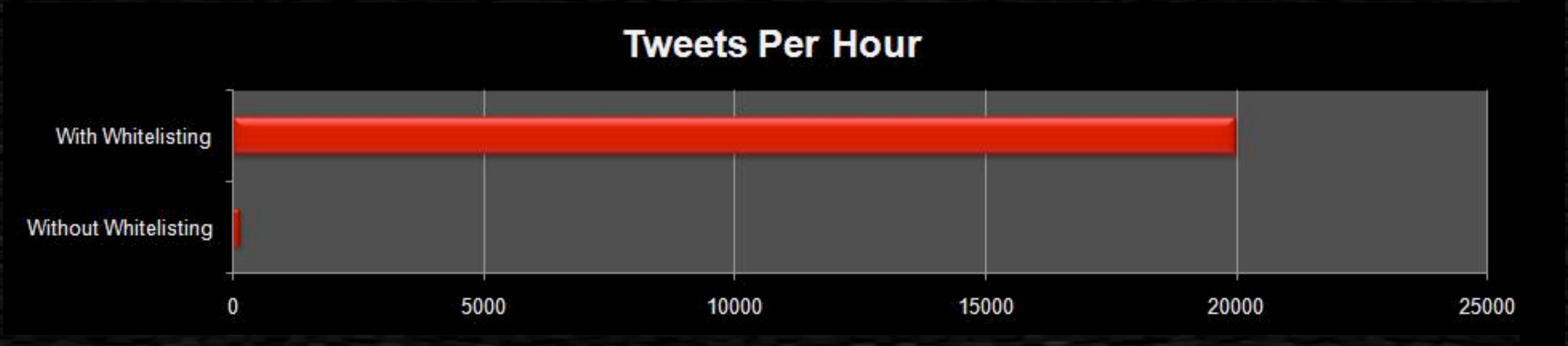
Gotcha’s

- 200 tweet limit
- Couldn’t search by date
- Max history of 3200 tweets
- 150 API calls an hour

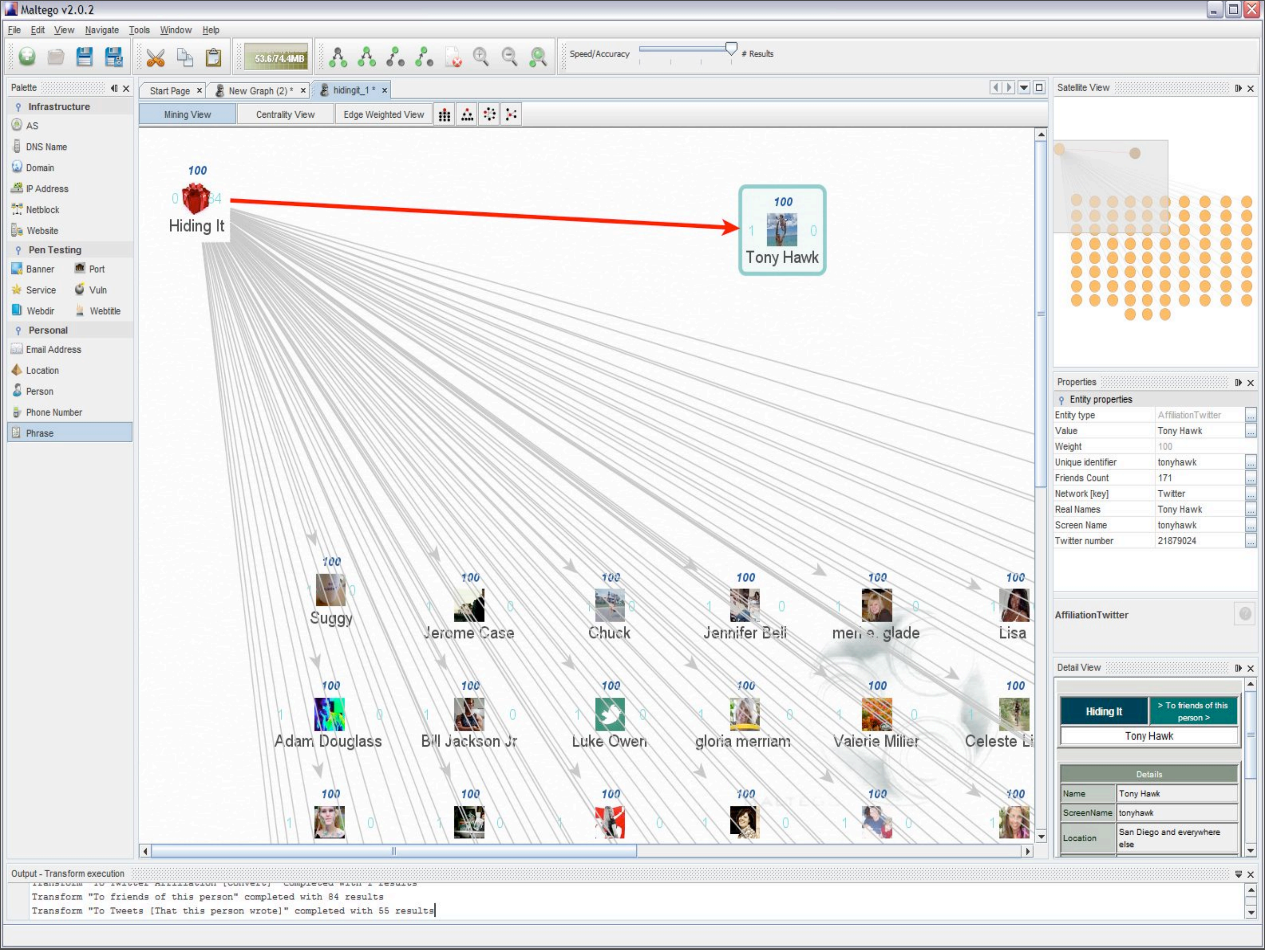
- 100 people * 3 api calls each = 300

Whitelisting

- 150 versus 20,000 per hour



Find the winners



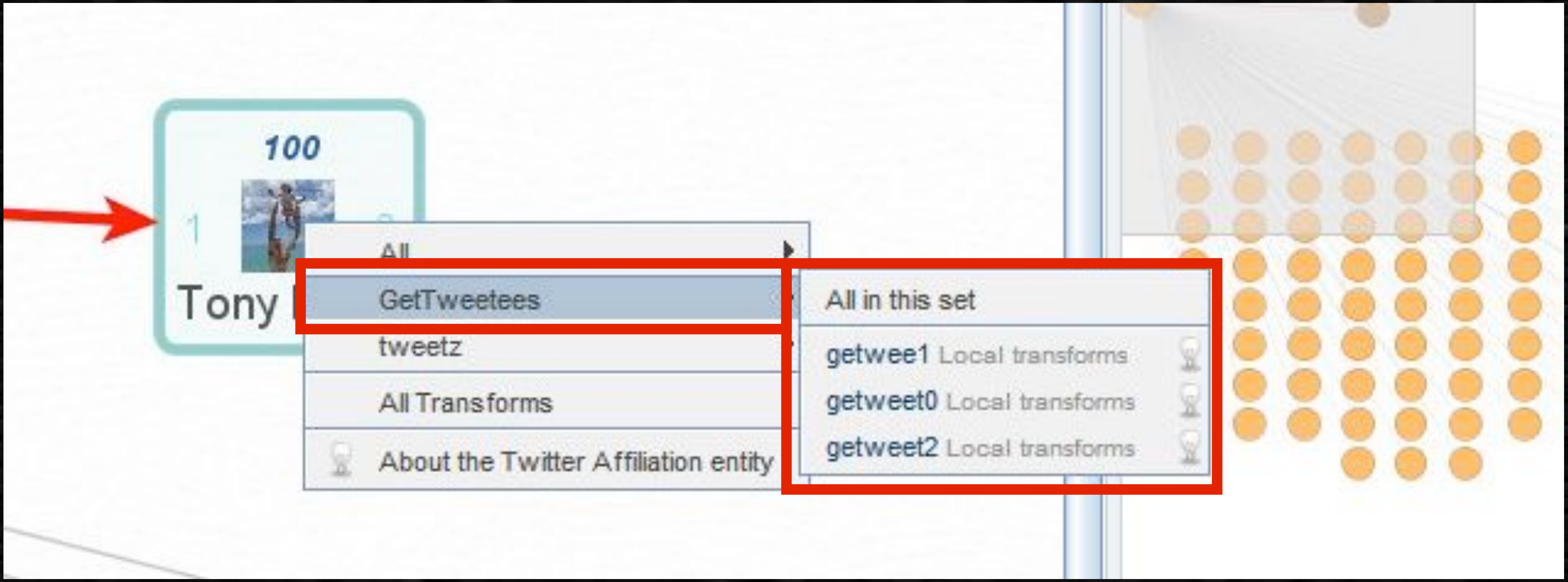
Entity type	AffiliationTwitter
Value	Tony Hawk
Weight	100
Unique identifier	tonyhawk
Friends Count	171
Network [key]	Twitter
Real Names	Tony Hawk
Screen Name	tonyhawk
Twitter number	21879024

Hiding It > To friends of this person > Tony Hawk

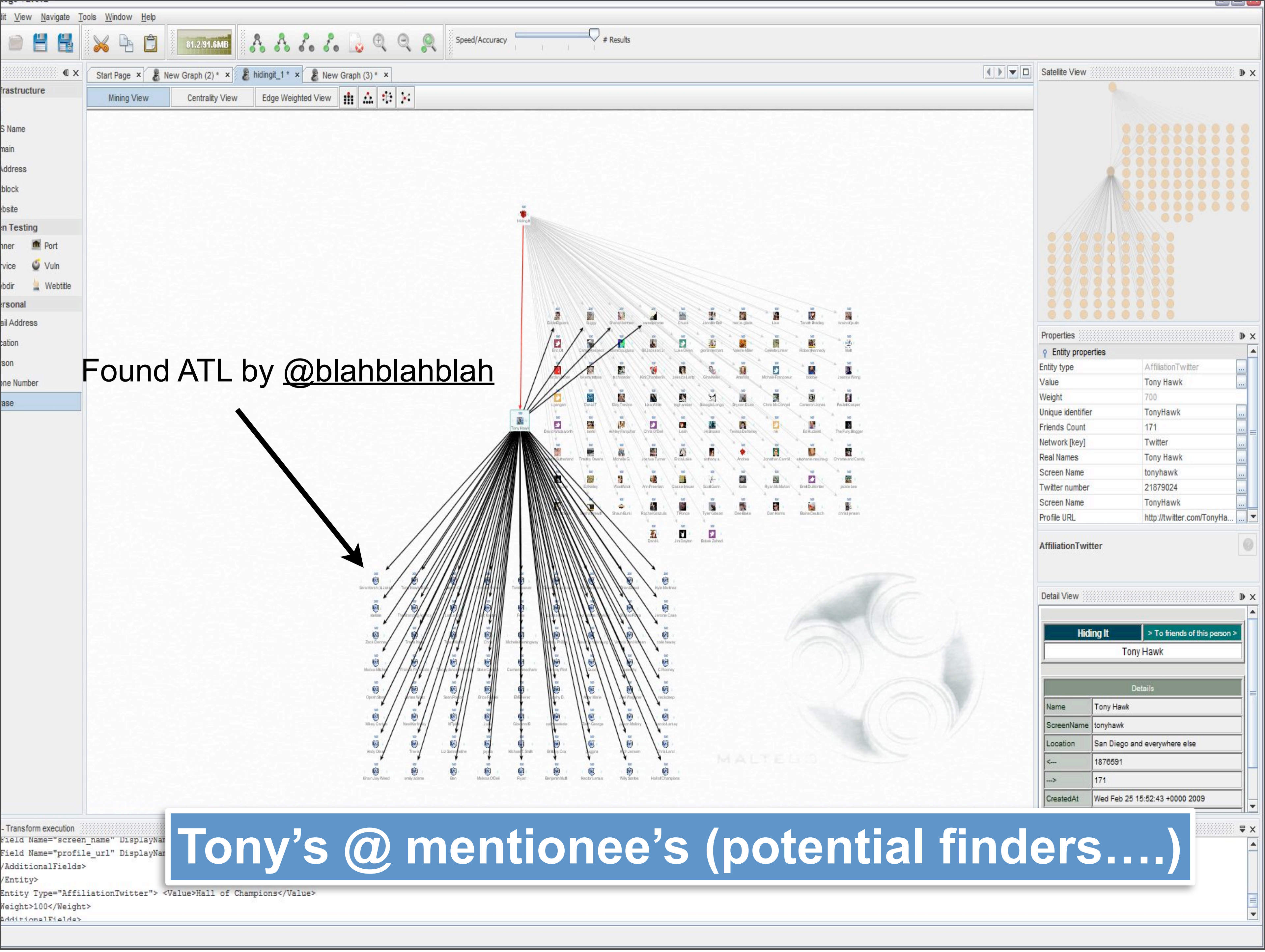
Details	
Name	Tony Hawk
ScreenName	tonyhawk
Location	San Diego and everywhere else

```
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 84 results
Transform "To Tweets [That this person wrote]" completed with 55 results
```

List of all @mentionee's



100
1
Tony
All
GetTweetees
tweetz
All Transforms
About the Twitter Affiliation entity
All in this set
getwee1 Local transforms
getweet0 Local transforms
getweet2 Local transforms



Found ATL by @blahblahblah

Tony's @ mentionee's (potential finders….)

Properties

Entity properties

Entity type	AffiliationTwitter
Value	Tony Hawk
Weight	700
Unique identifier	TonyHawk
Friends Count	171
Network [key]	Twitter
Real Names	Tony Hawk
Screen Name	tonyhawk
Twitter number	21879024
Screen Name	TonyHawk
Profile URL	http://twitter.com/TonyHa...

AffiliationTwitter

Detail View

Hiding It > To friends of this person >

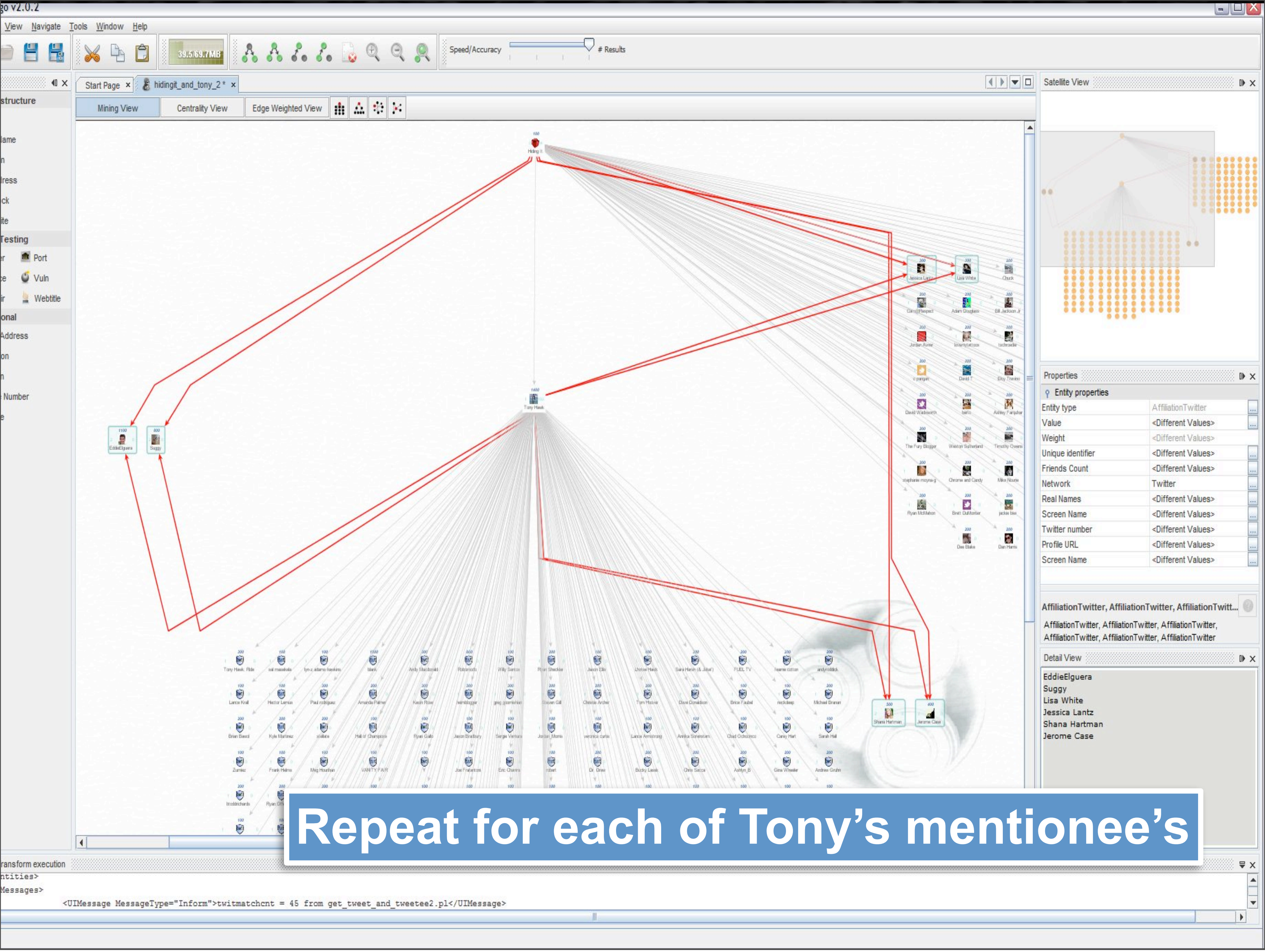
Tony Hawk

Details

Name	Tony Hawk
ScreenName	tonyhawk
Location	San Diego and everywhere else
<---	1876591
--->	171
CreatedAt	Wed Feb 25 15:52:43 +0000 2009

- Transform execution

```
Field Name="screen_name" DisplayNam
Field Name="profile_url" DisplayNam
/AdditionalFields>
/Entity>
Entity Type="AffiliationTwitter"> <Value>Hall of Champions</Value>
Weight>100</Weight>
AdditionalFields>
```



Entity type	AffiliationTwitter
Value	<Different Values>
Weight	<Different Values>
Unique identifier	<Different Values>
Friends Count	<Different Values>
Network	Twitter
Real Names	<Different Values>
Screen Name	<Different Values>
Twitter number	<Different Values>
Profile URL	<Different Values>
Screen Name	<Different Values>

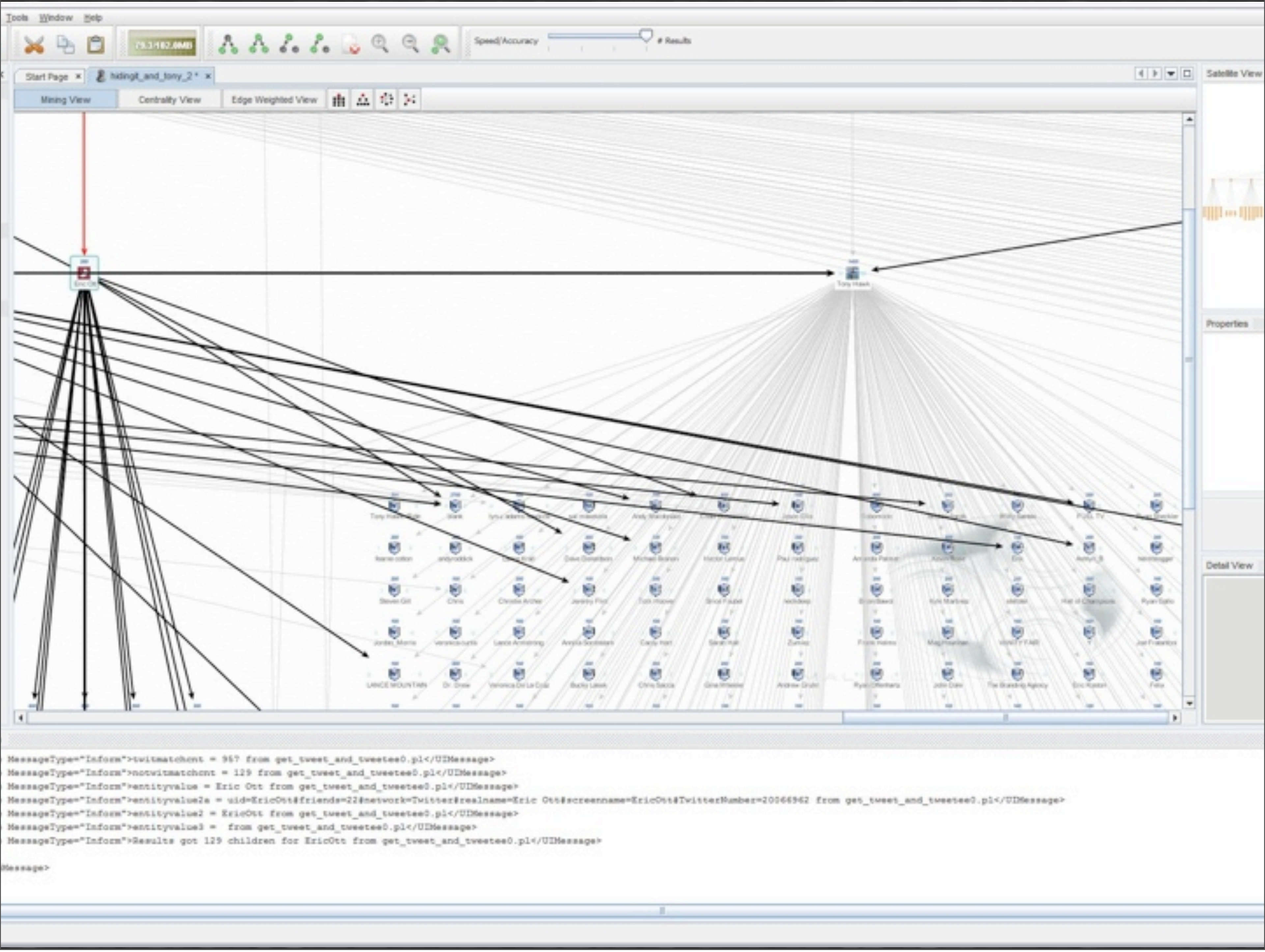
AffiliationTwitter, AffiliationTwitter, AffiliationTwitt...

AffiliationTwitter, AffiliationTwitter, AffiliationTwitter, AffiliationTwitter, AffiliationTwitter, AffiliationTwitter

EddieElguera
Suggy
Lisa White
Jessica Lantz
Shana Hartman
Jerome Case

```
ntities>
Messages>
        <UIMessage MessageType="Inform">twitmatchcnt = 45 from get_tweet_and_tweetee2.pl</UIMessage>
```

Repeat for each of Tony’s mentionee’s

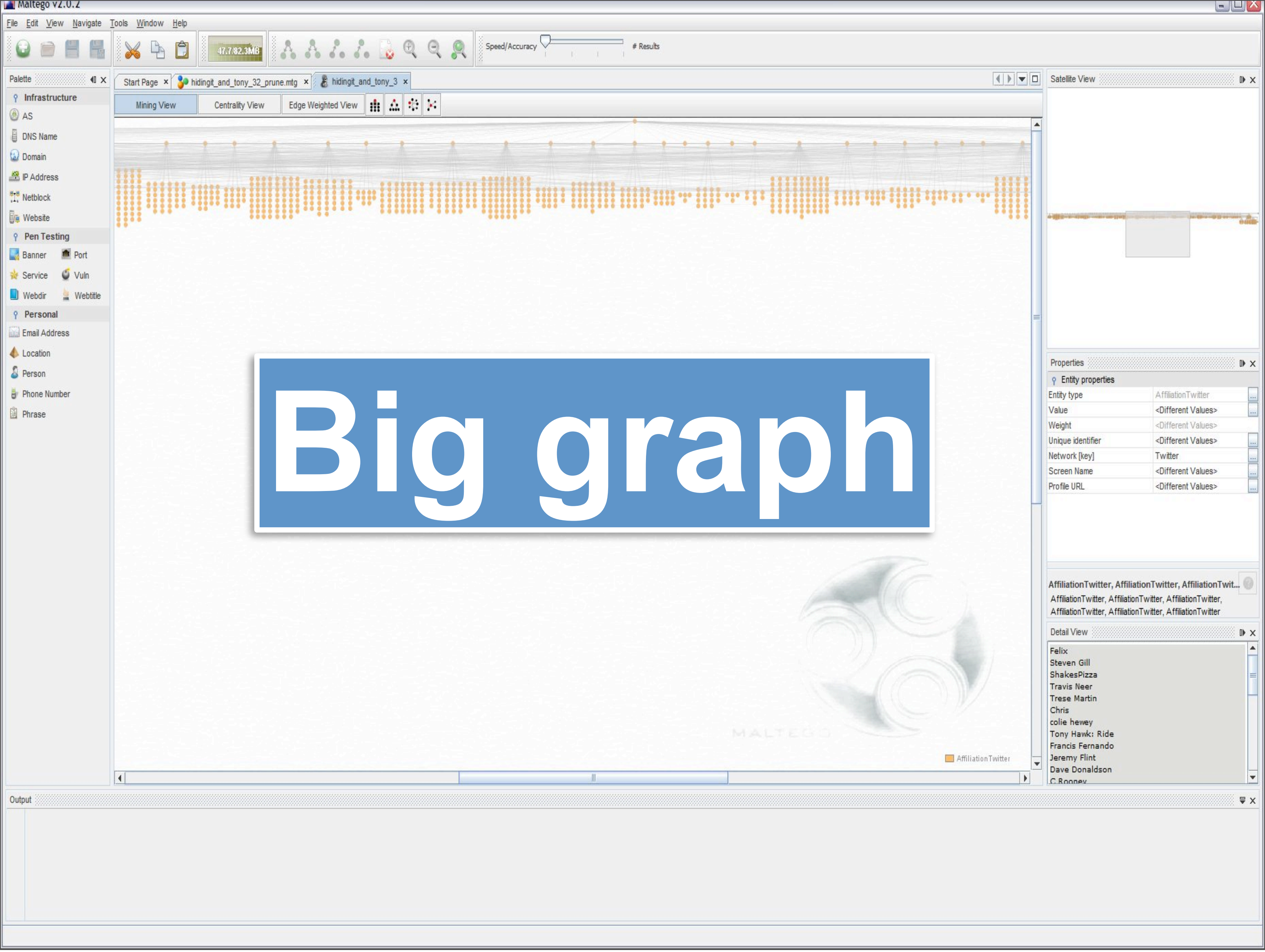


```
 MessageType="Inform">twitmatchcnt = 957 from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">notwitmatchcnt = 129 from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">entityvalue = Eric Ott from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">entityvalue2a = uid=EricOtt#friends=22#network=Twitter#realname=Eric Ott#screenname=EricOtt#TwitterNumber=20066962 from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">entityvalue2 = EricOtt from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">entityvalue3 =  from get_tweet_and_tweetee0.pl</UIMessage>
 MessageType="Inform">Results got 129 children for EricOtt from get_tweet_and_tweetee0.pl</UIMessage>

Message>
```

Tuesday, 3 August 2010

Big graph



Entity properties

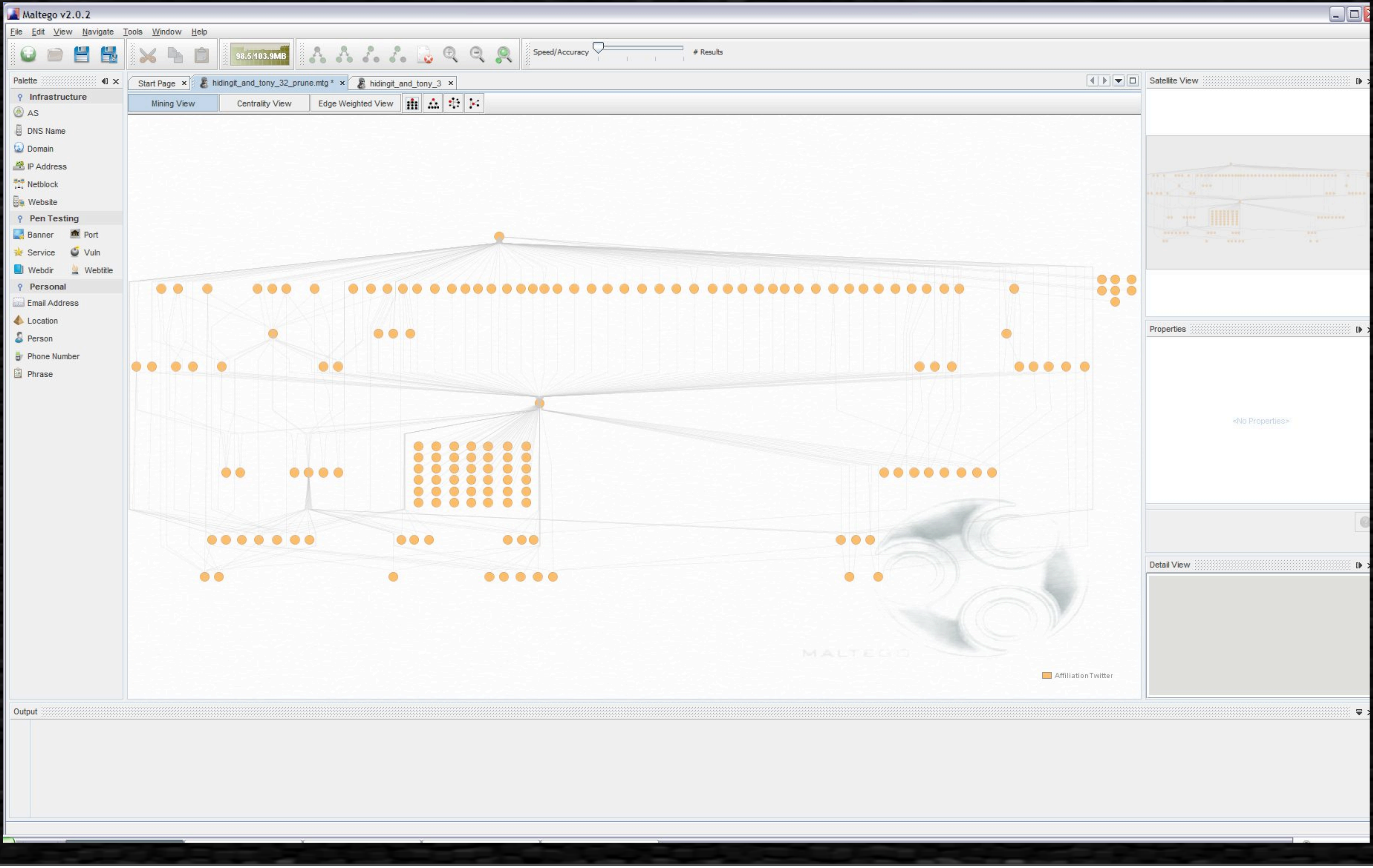
Entity type	AffiliationTwitter
Value	<Different Values>
Weight	<Different Values>
Unique identifier	<Different Values>
Network [key]	Twitter
Screen Name	<Different Values>
Profile URL	<Different Values>

AffiliationTwitter, AffiliationTwitter, AffiliationTwit...
AffiliationTwitter, AffiliationTwitter, AffiliationTwitter,
AffiliationTwitter, AffiliationTwitter, AffiliationTwitter

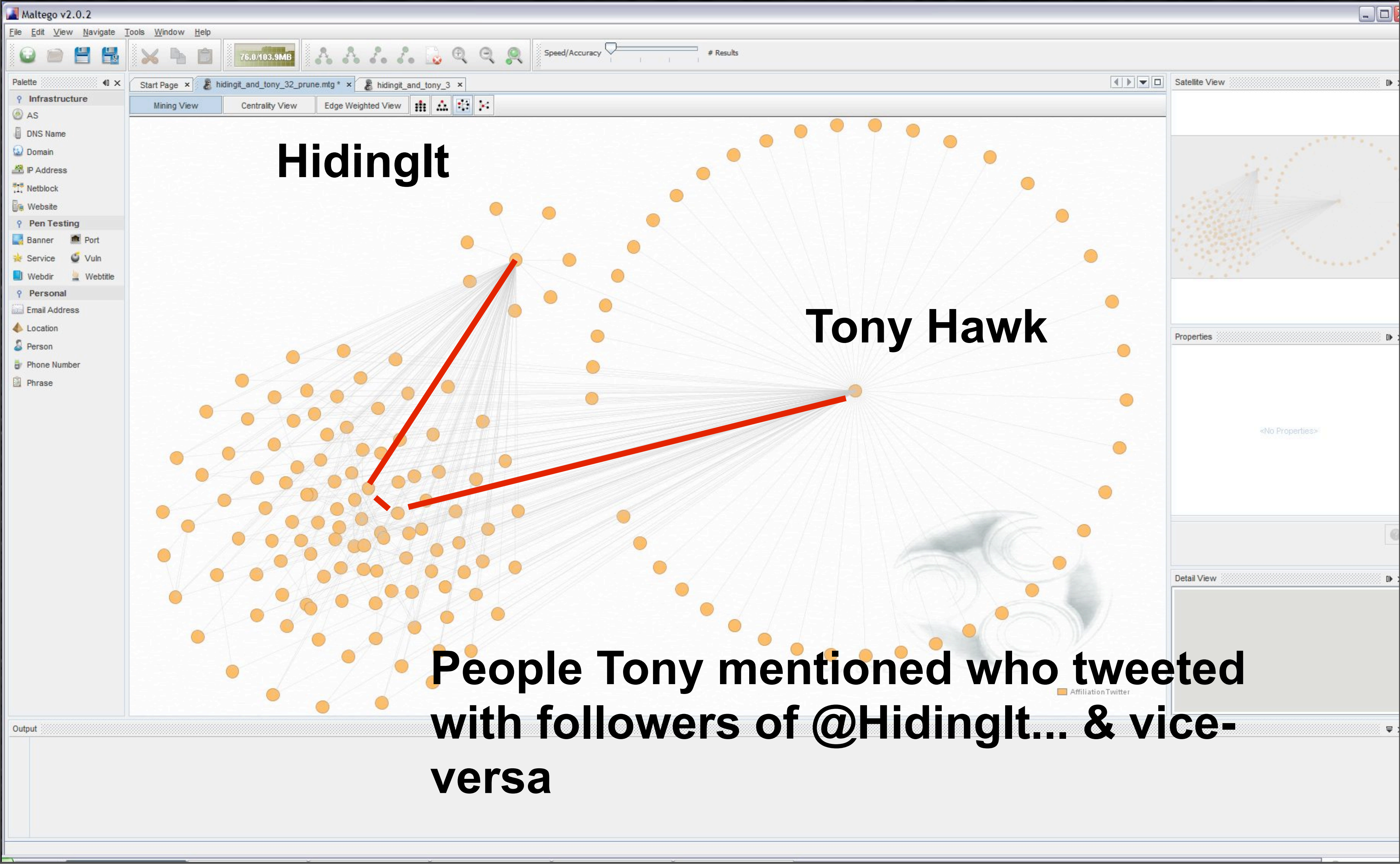
Felix
Steven Gill
ShakesPizza
Travis Neer
Trese Martin
Chris
colie hewey
Tony Hawk: Ride
Francis Fernando
Jeremy Flint
Dave Donaldson
C Rooney

FAIL

A bit less messy



Centrality layout

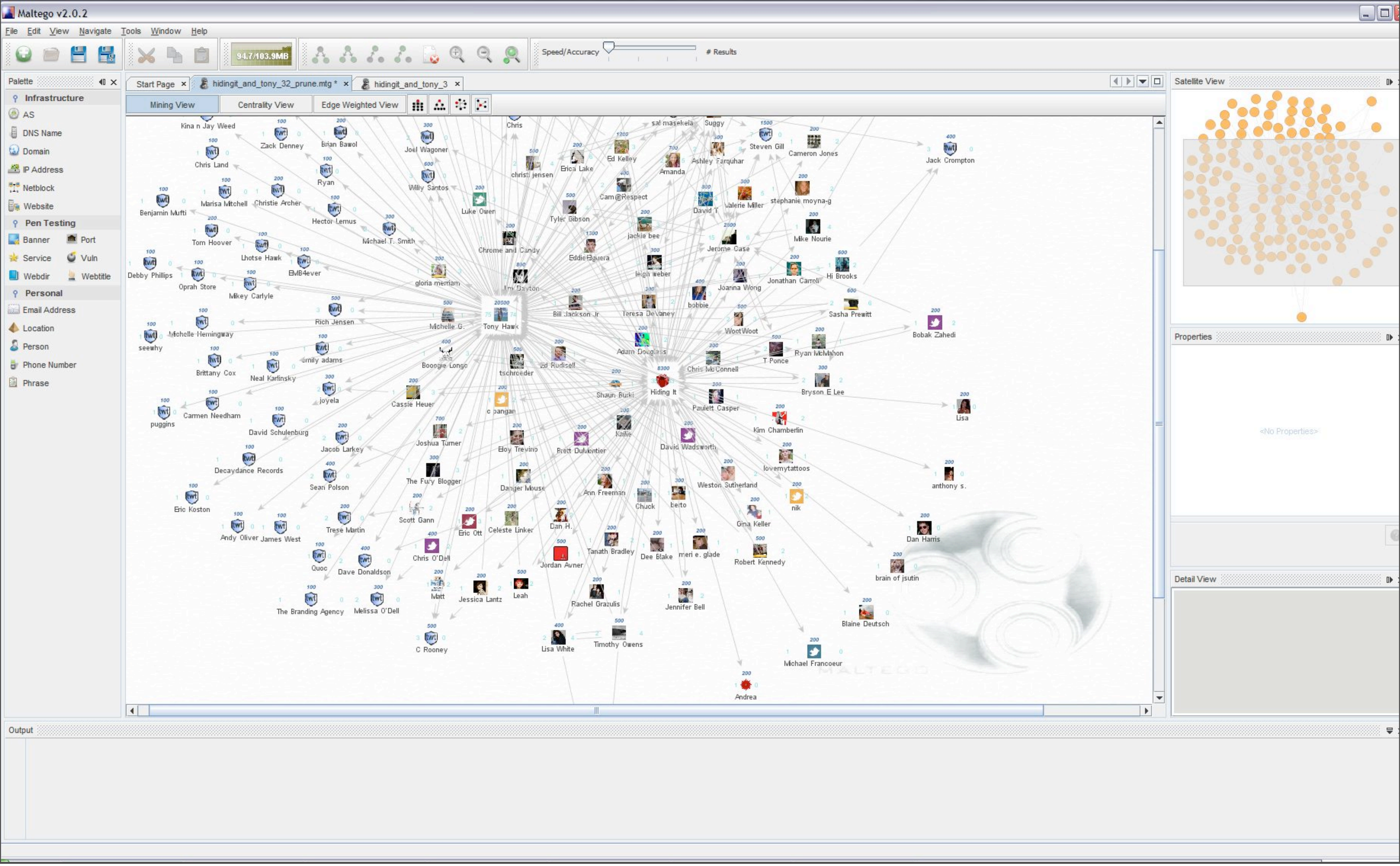


HidingIt

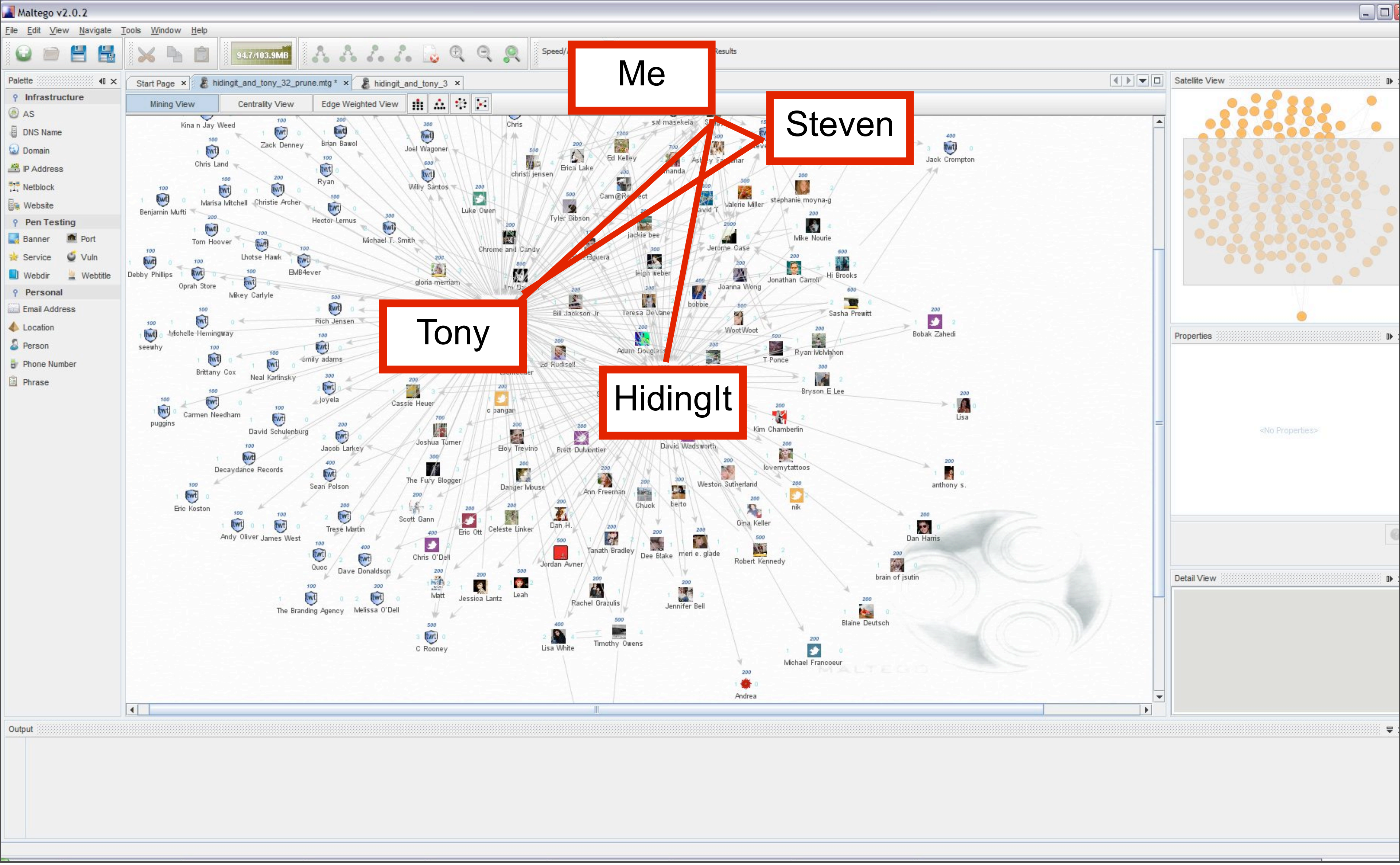
Tony Hawk

People Tony mentioned who tweeted with followers of @HidingIt... & vice-versa

Organic


Maltego v2.0.2
File Edit View Navigate Tools Window Help
94.7/103.9MB
Speed/Accuracy
# Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
Start Page
hidingit_and_tony_32_prune.mtg *
hidingit_and_tony_3
Mining View
Centrality View
Edge Weighted View
Satellite View
Properties
<No Properties>
Detail View
Output
Tony Hawk
Hiding It
Kina n Jay Weed
Zack Denney
Brian Bawol
Joel Wagoner
Chris
sal masekela
Suggy
Steven Gill
Cameron Jones
Jack Crompton
Chris Land
Ryan
Willy Santos
christi jensen
Erica Lake
Ed Kelley
Amanda
Ashley Farquhar
Benjamin Mufti
Marisa Mitchell
Christie Archer
Hector Lemus
Luke Owen
Tyler Gibson
Cam@Respect
David T
Valerie Miller
stephanie moyna-g
Tom Hoover
Lhotse Hawk
Michael T. Smith
Chrome and Candy
Eddie Elguera
jackie bee
Jerome Case
Mike Nourie
Debby Phillips
Oprah Store
EMB4ever
gloria merriam
Ivy Dayton
leigh weber
Joanna Wong
Jonathan Carroll
Hi Brooks
Mikey Carlyle
Bill Jackson Jr
Teresa DeVaney
bobbie
Sasha Prewitt
Rich Jensen
Michelle G.
Woot Woot
Bobak Zahedi
Michelle Hemingway
seewhy
Adam Douglass
Ryan McMahon
Brittany Cox
emily adams
Boogie Longo
tschroeder
Ed Rudisell
Chris McConnell
T Ponce
Neal Karlinsky
joyela
Cassie Heuer
c pangan
Shaun Burki
Bryson E Lee
Paulett Casper
Lisa
puggins
Carmen Needham
David Schulenburg
Kallie
Kim Chamberlin
Jacob Larkey
Joshua Turner
Eloy Trevino
Brett Dumontier
David Wadsworth
Decaydance Records
Sean Polson
The Fury Blogger
Danger Mouse
lovemytattoos
anthony s.
Ann Freeman
Weston Sutherland
Eric Koston
Chuck
berto
nik
Andy Oliver
James West
Trese Martin
Scott Gann
Eric Ott
Celeste Linker
Dan H.
Gina Keller
Dan Harris
Quoc
Dave Donaldson
Chris O'Dell
Tanath Bradley
Dee Blake
meri e. glade
Robert Kennedy
brain of jsutin
Jordan Avner
Matt
Jessica Lantz
Leah
Rachel Grazulis
Jennifer Bell
The Branding Agency
Melissa O'Dell
Blaine Deutsch
C Rooney
Lisa White
Timothy Owens
Michael Francoeur
Andrea

Organic



Me

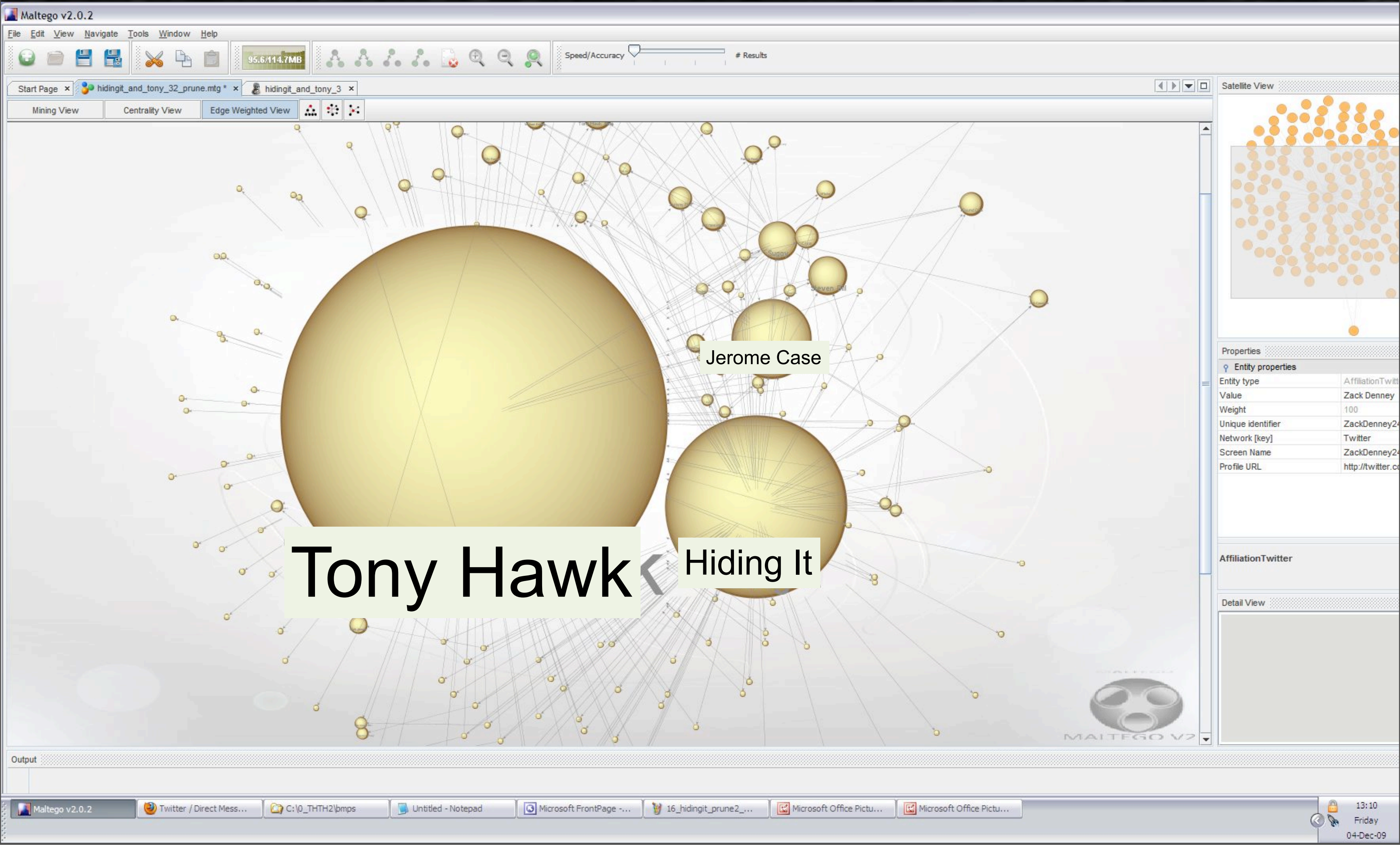
Steven

Tony

HidingIt

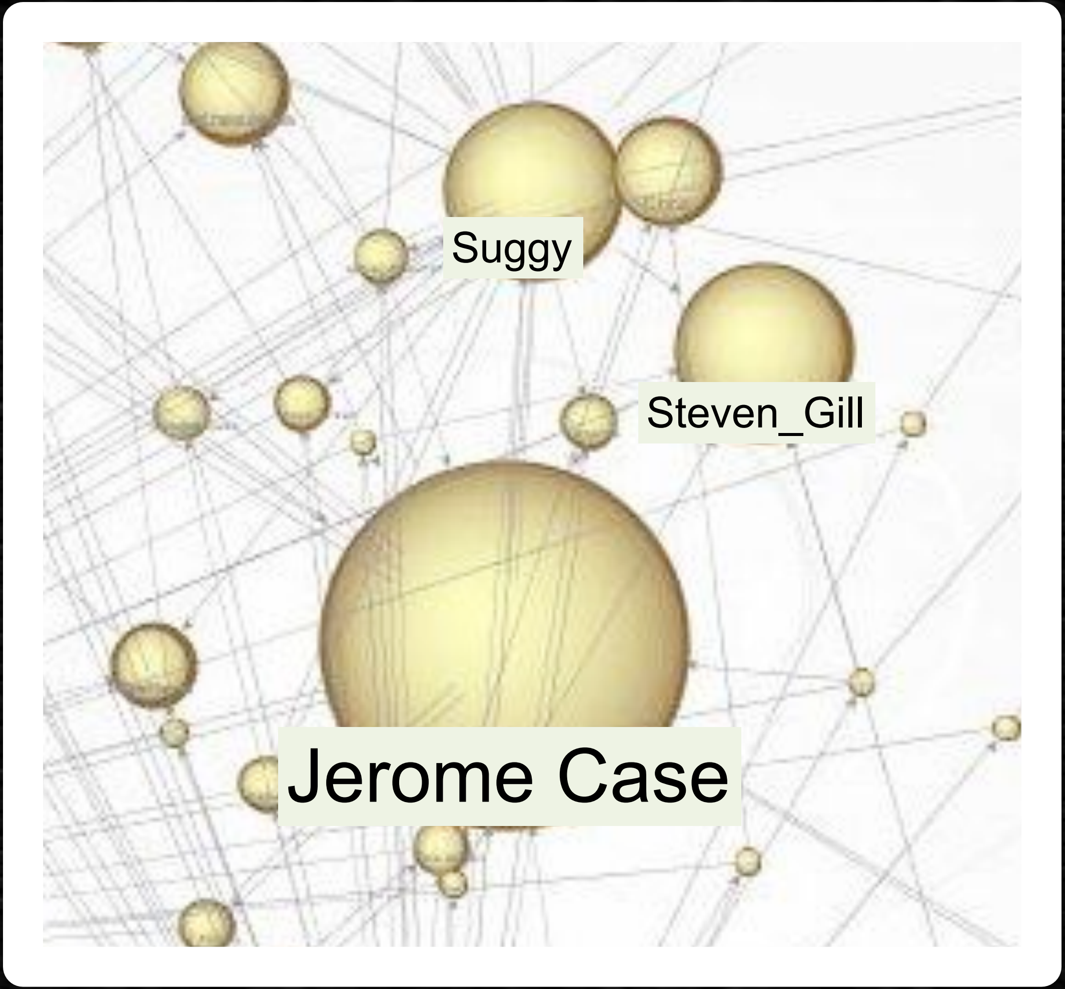
Tuesday, 3 August 2010

Edge Weighted

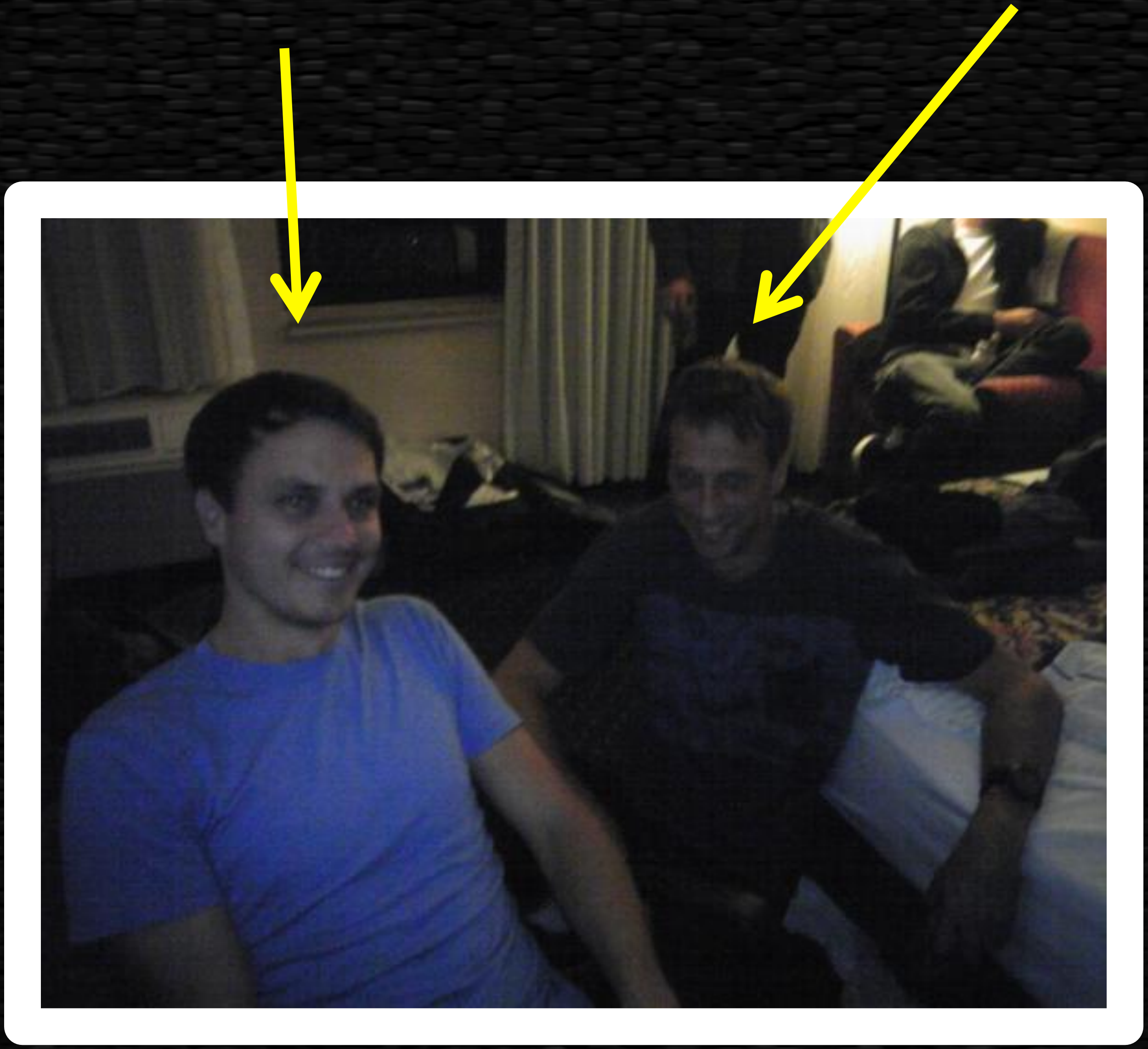


Entity type	AffiliationTwitt
Value	Zack Denney
Weight	100
Unique identifier	ZackDenney2
Network [key]	Twitter
Screen Name	ZackDenney2
Profile URL	http://twitter.c

So what? What on earth have I been going on about?

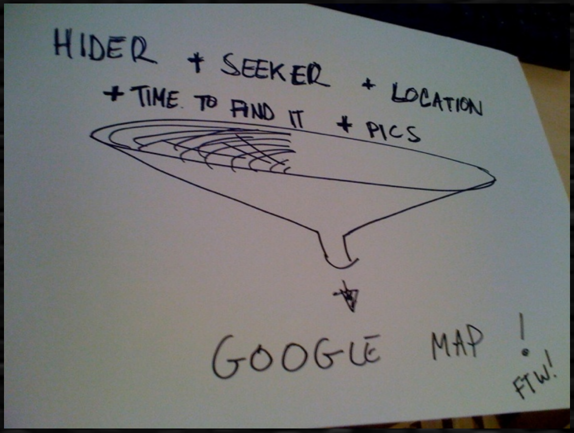


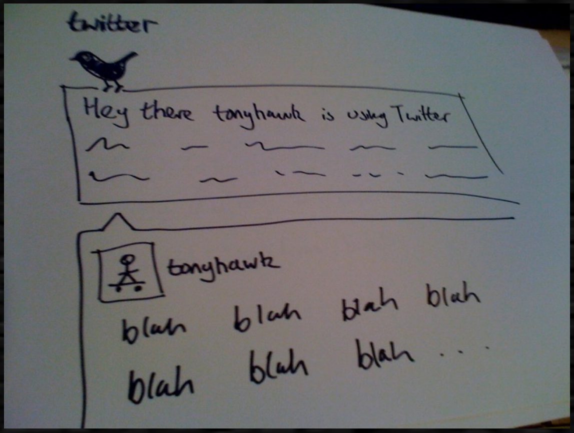
@sweetjerome & @tonyhawk

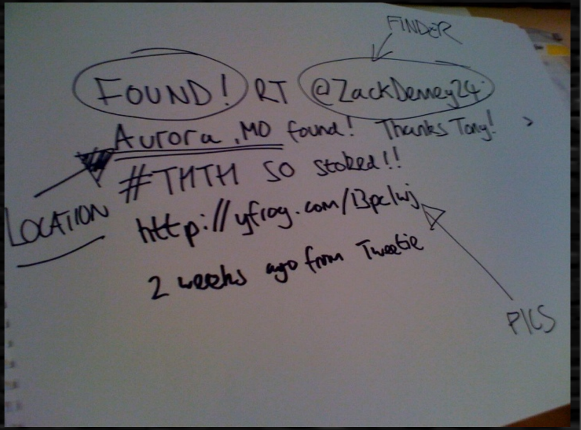


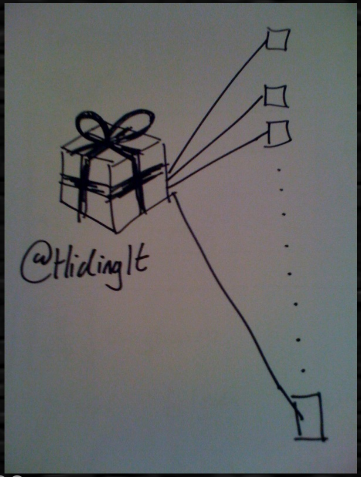
Lessons learned #1

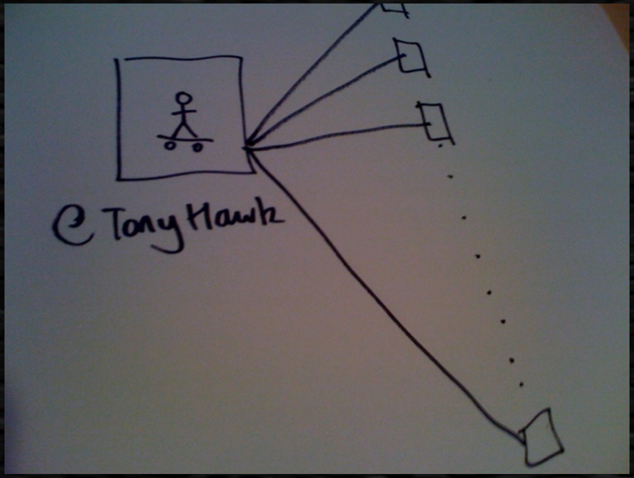
- Plan

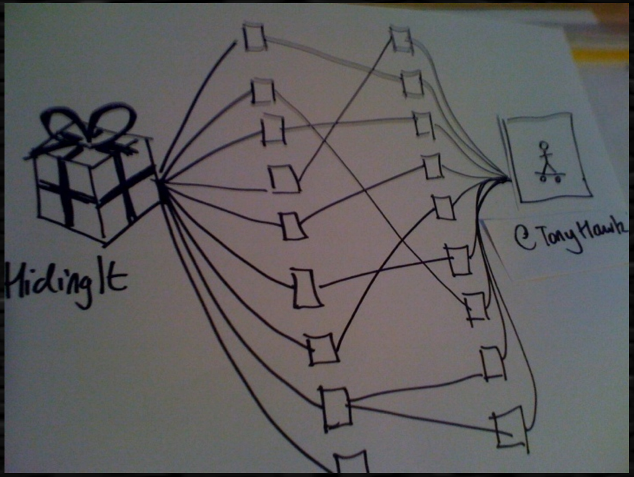






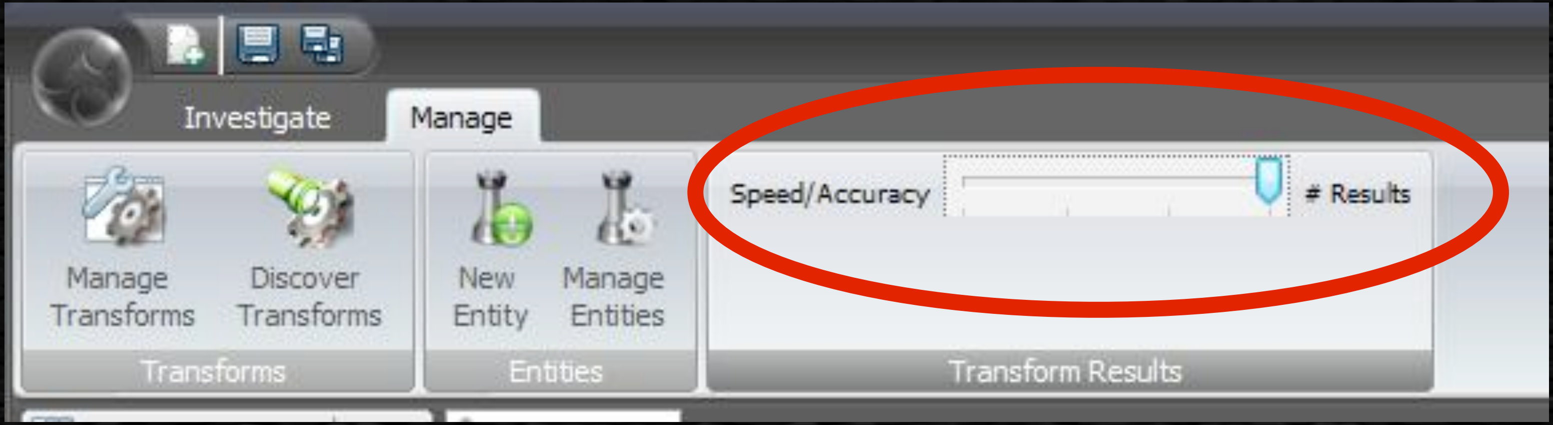






Lessons learned #2

- Speed/Accuracy bar set to left until you know it works



- If you ever think, “that’s weird. Not many results”, it’s probably because your Speed/Accuracy bar isn’t over to the right.

Lessons learned #3

Lessons learned #3

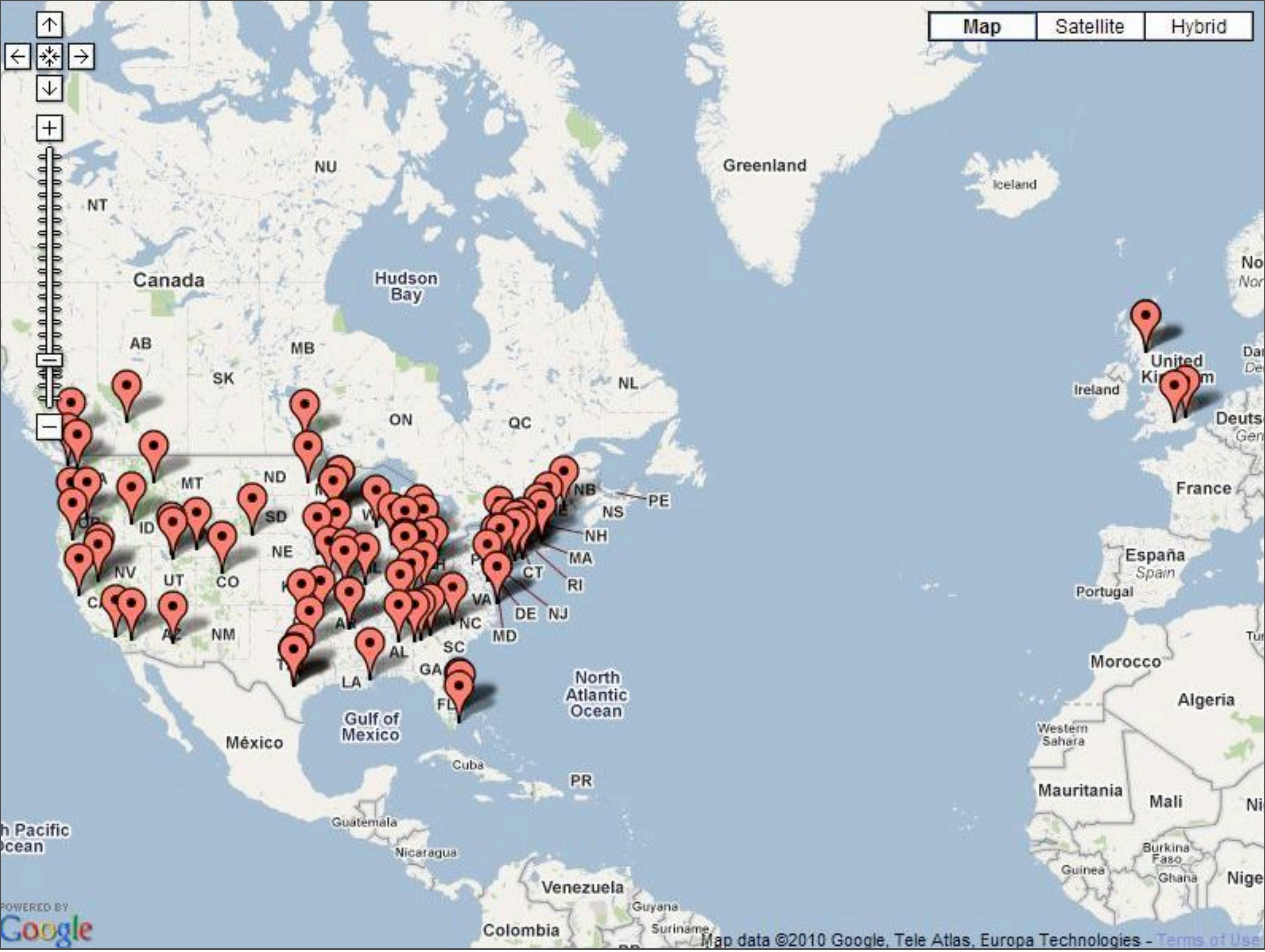
- Local transforms open up a world of opportunity

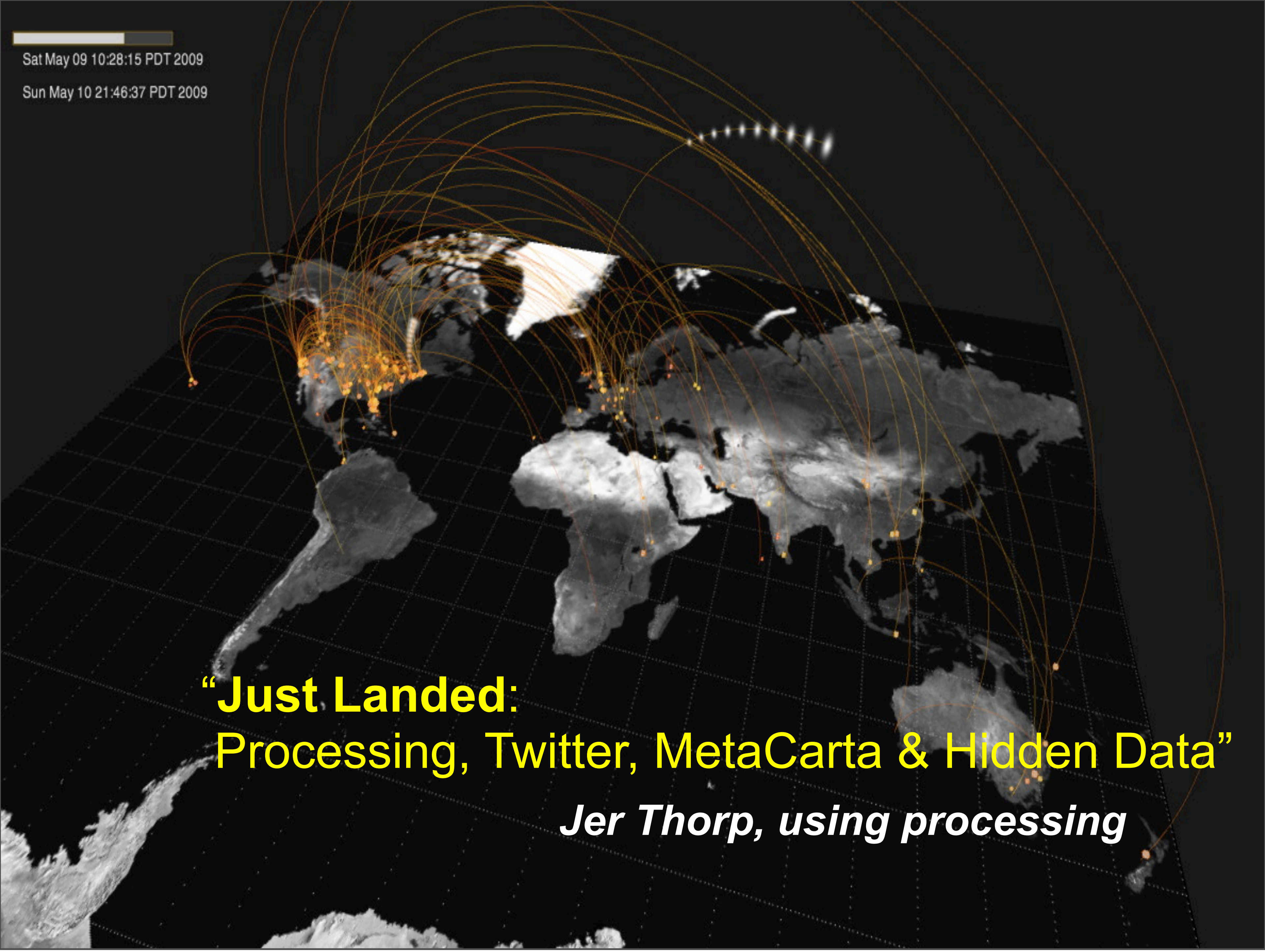
Lessons learned #3

- Local transforms open up a world of opportunity
- Enterprise? Consider the server platform.

Lessons learned #3

- Local transforms open up a world of opportunity
- Enterprise? Consider the server platform.
- If you’re going to leverage Twitter API heavily, you should really consider making a whitelisting request

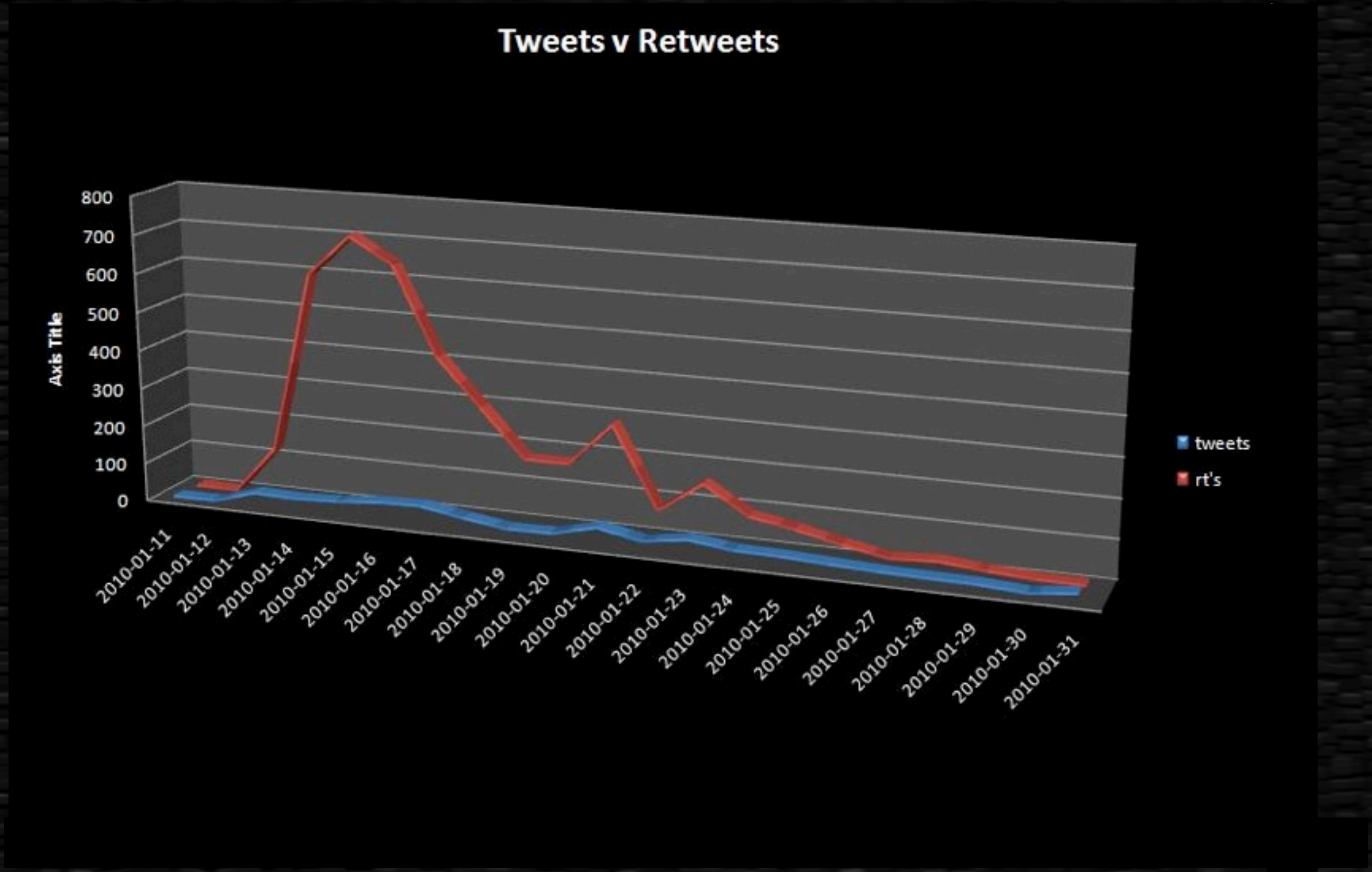

Map
Satellite
Hybrid
NU
Greenland
Iceland
NT
Canada
Hudson Bay
AB
MB
SK
NL
ON
QC
Ireland
United Kingdom
Deuts
France
España
Spain
Portugal
MT
ND
SD
ID
NE
NV
UT
CO
CA
AZ
NM
NB
PE
NS
NH
MA
CT
RI
VA
DE
NJ
MD
NC
SC
GA
AL
LA
FL
TX
Morocco
Algeria
North Atlantic Ocean
Gulf of Mexico
México
Cuba
PR
Western Sahara
Mauritania
Mali
Guatemala
Nicaragua
Burkina Faso
Guinea
Ghana
Venezuela
Guyana
Suriname
Colombia
Pacific Ocean
POWERED BY Google
Map data ©2010 Google, Tele Atlas, Europa Technologies - Terms of Use



“**Just Landed**: Processing, Twitter, MetaCarta & Hidden Data”

Jer Thorp, using processing

Graphs for DEC.org.uk



……Check out RowFeeder.com

419

419

419

Disclaimer

“The only way you can tell the truth is through fiction”

Via Richard Thieme/his friend at NSA

“Events, Names, dates, images etc all changed to protect the innocent and the not so innocent”

Meet “Jess”

Meet “Jess”

- Laptop on auction site

Meet “Jess”

- Laptop on auction site
- Gets bought quickly at “Buy now price”

Meet "Jess"

- Laptop on auction site
- Gets bought quickly at "Buy now price"
- Jess exchanges emails with the buyer

Meet “Jess”

- Laptop on auction site
- Gets bought quickly at “Buy now price”
- Jess exchanges emails with the buyer
- Notification from “paypal”

Meet “Jess”

- Laptop on auction site
- Gets bought quickly at “Buy now price”
- Jess exchanges emails with the buyer
- Notification from “paypal”
- Jess sends laptop to valid address in UK

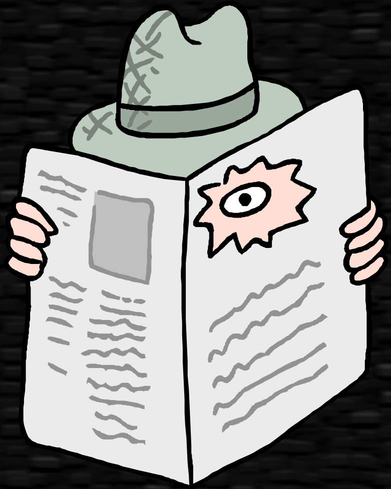
Meet “Jess”

- Laptop on auction site
- Gets bought quickly at “Buy now price”
- Jess exchanges emails with the buyer
- Notification from “paypal”
- Jess sends laptop to valid address in UK
- Notice from auction site that buy account had been hacked

Meet “Jess”

- Laptop on auction site
- Gets bought quickly at “Buy now price”
- Jess exchanges emails with the buyer
- Notification from “paypal”
- Jess sends laptop to valid address in UK
- Notice from auction site that buy account had been hacked
- Jess contacts police

Hypothesis

 +

= =

Step #1 Where is our scammer?

Step #1 Where is our scammer?

- Need to get email header, but he/she uses webmail……

Step #1 Where is our scammer?

- Need to get email header, but he/she uses webmail……
- …. So sign up for a blog site like webs.com that also provides logs.

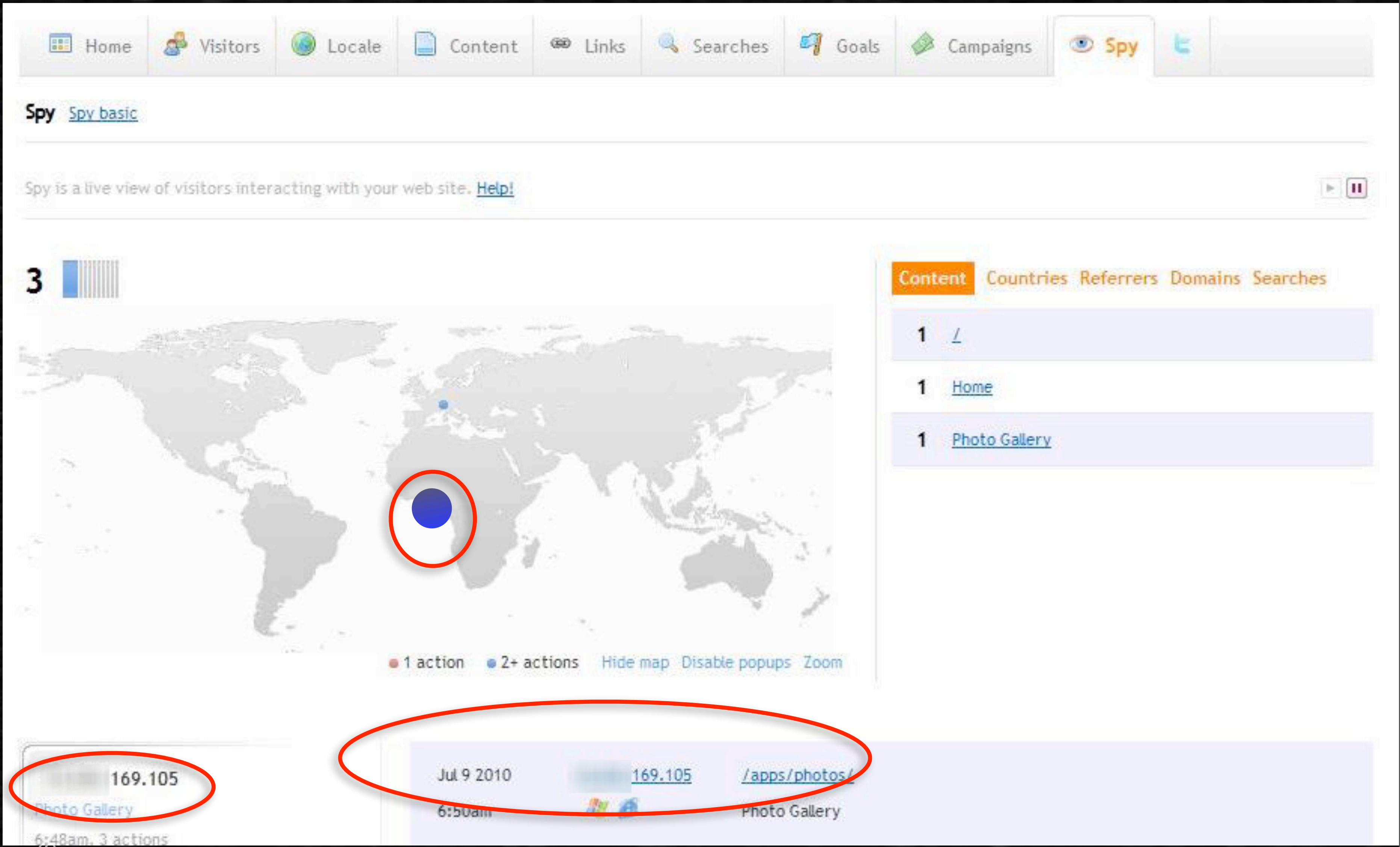
Step #1 Where is our scammer?

- Need to get email header, but he/she uses webmail……
- …. So sign up for a blog site like webs.com that also provides logs.
- Send spammer an email message with embedded image.

Step #1 Where is our scammer?

- Need to get email header, but he/she uses webmail……
- …. So sign up for a blog site like webs.com that also provides logs.
- Send spammer an email message with embedded image.
- Wait

webs.com visitor logs



Spy Spy basic

Spy is a live view of visitors interacting with your web site. Help!

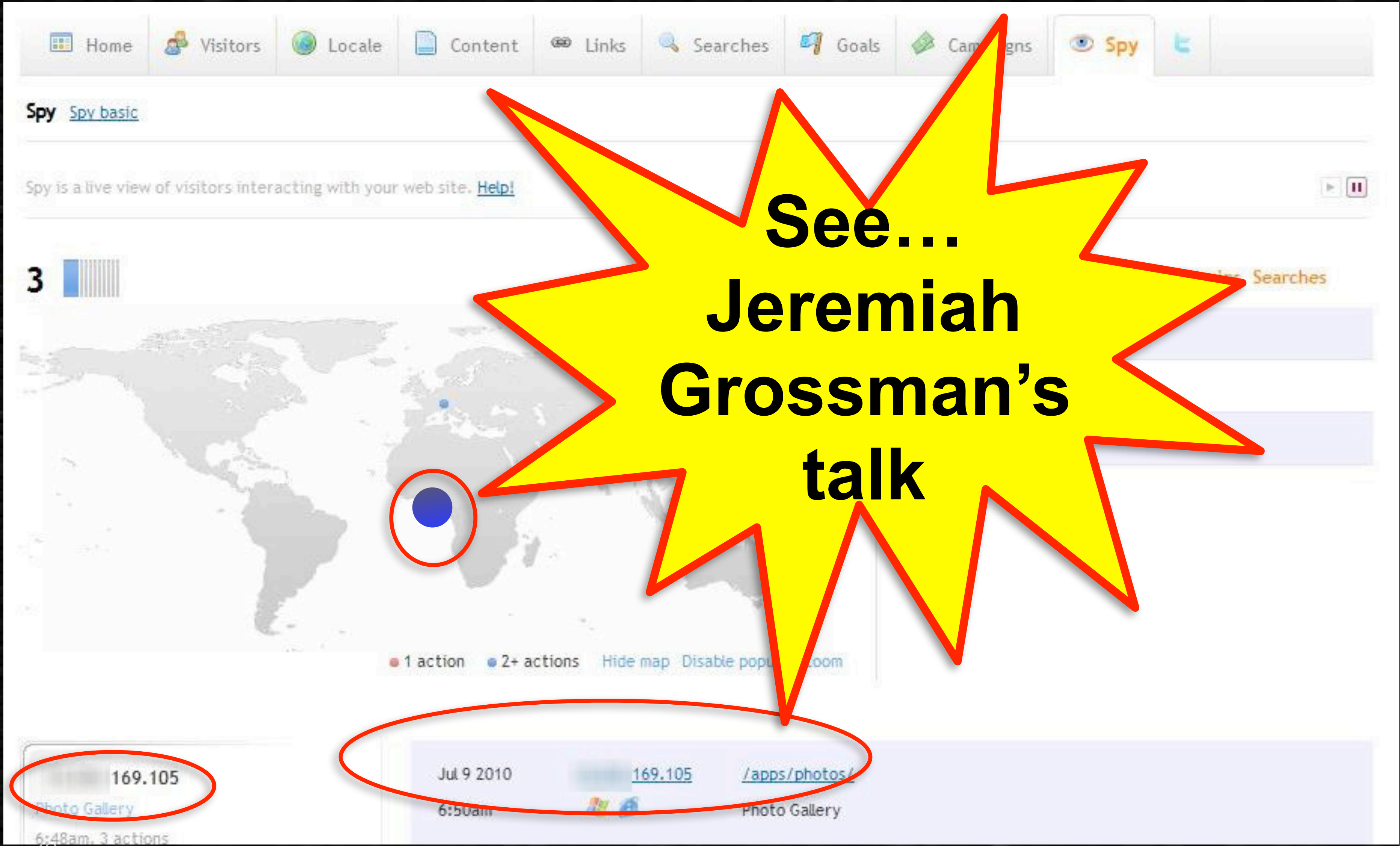
3

1	/
1	Home
1	Photo Gallery

[redacted] 169.105
Photo Gallery
6:48am, 3 actions

Jul 9 2010 6:50am [redacted]169.105 /apps/photos/ Photo Gallery

webs.com visitor logs



Spy Spy basic

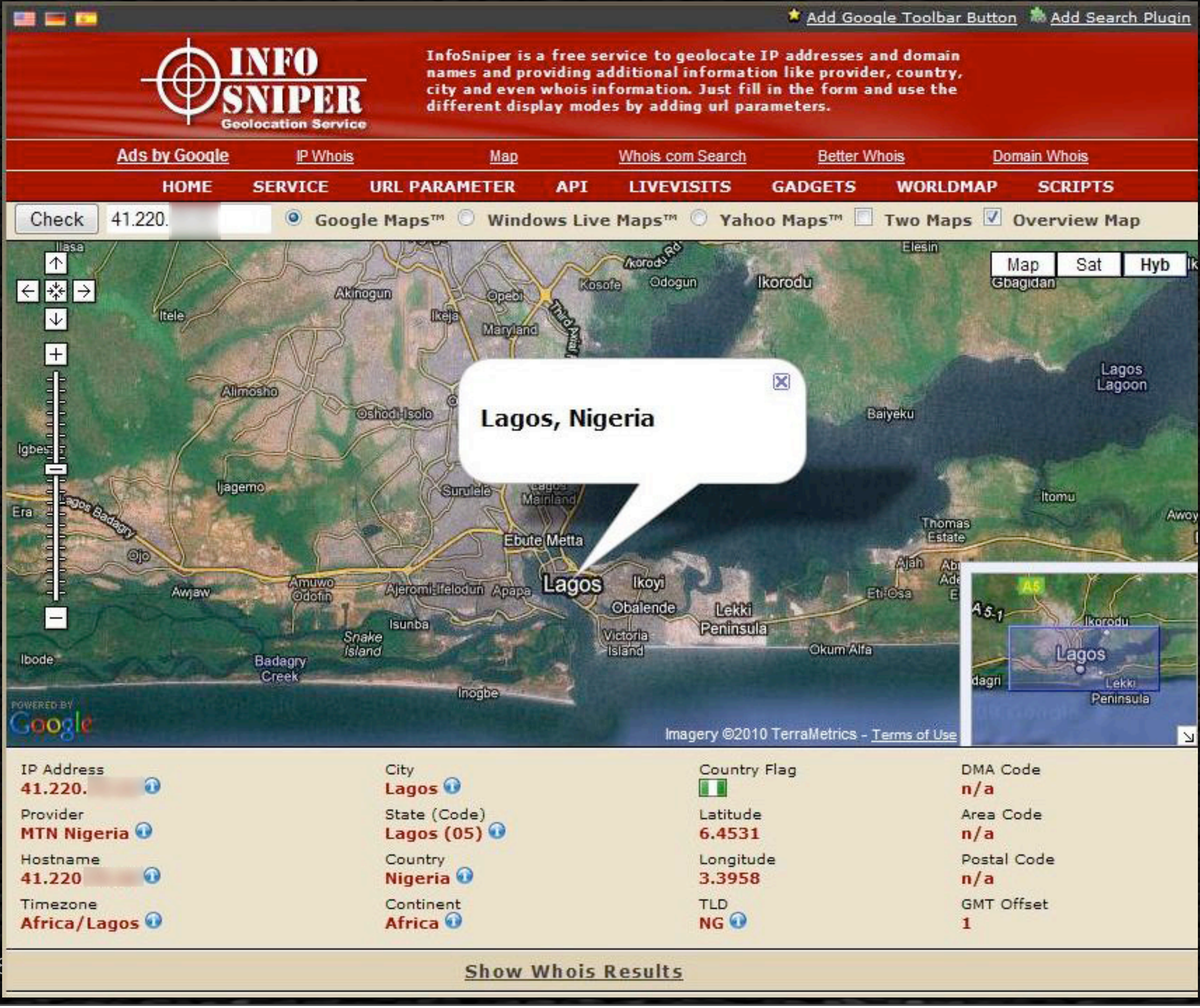
Spy is a live view of visitors interacting with your web site. Help!

3

[redacted] 169.105
Photo Gallery
6:48am, 3 actions

Jul 9 2010 6:50am [redacted] 169.105 /apps/photos/ Photo Gallery

See… Jeremiah Grossman's talk



InfoSniper is a free service to geolocate IP addresses and domain names and providing additional information like provider, country, city and even whois information. Just fill in the form and use the different display modes by adding url parameters.

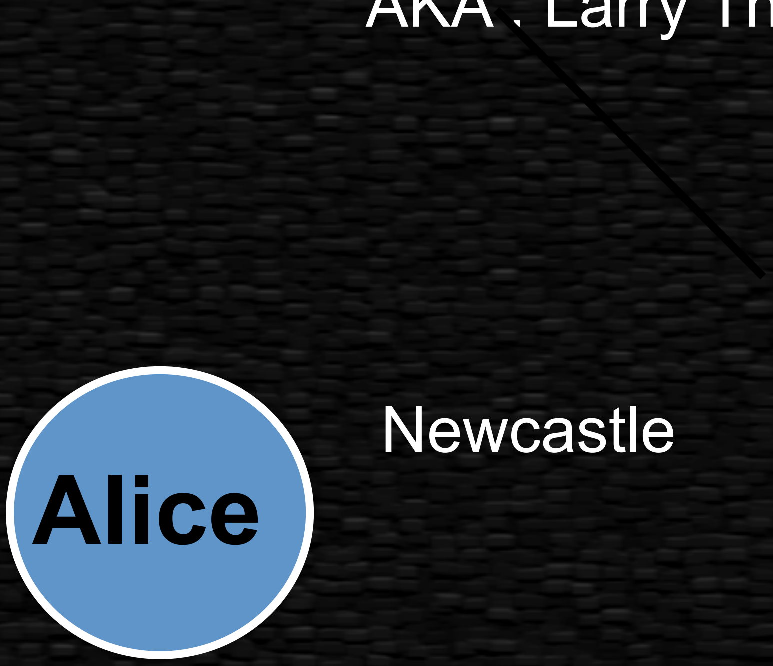
Check 41.220.[redacted] ● Google Maps™ ○ Windows Live Maps™ ○ Yahoo Maps™ □ Two Maps ☑ Overview Map

Lagos, Nigeria

IP Address 41.220.[redacted]	City Lagos	Country Flag 🇳🇬	DMA Code n/a
Provider MTN Nigeria	State (Code) Lagos (05)	Latitude 6.4531	Area Code n/a
Hostname 41.220[redacted]	Country Nigeria	Longitude 3.3958	Postal Code n/a
Timezone Africa/Lagos	Continent Africa	TLD NG	GMT Offset 1

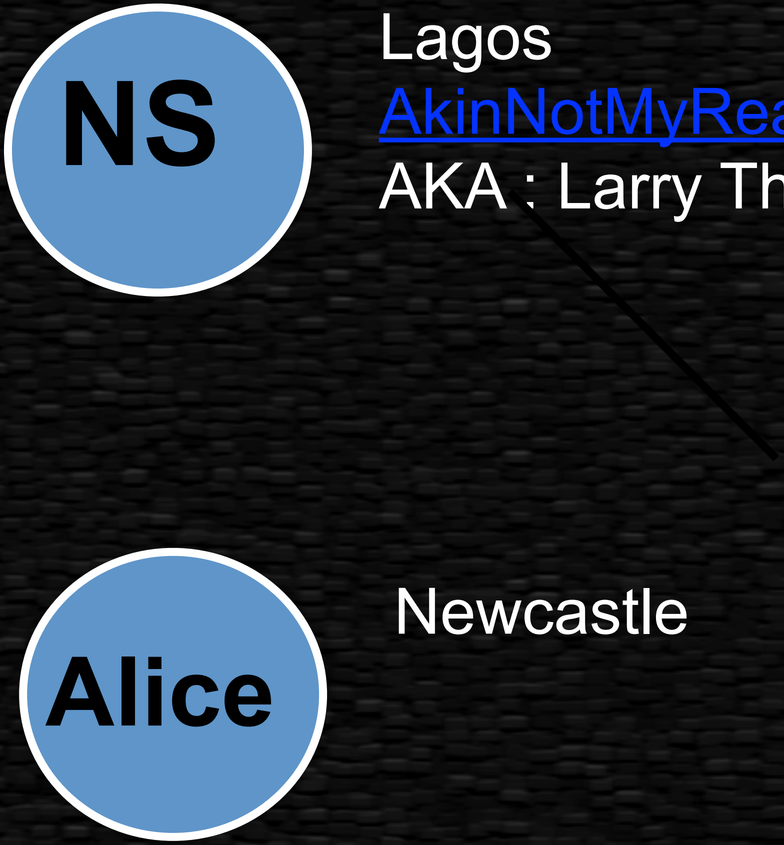
Step #2 where did package really go?

Lagos
AkinNotMyRealName@someemail.com
AKA : Larry The Cable Guy



Newcastle

Step #2 where did package really go?



Lagos
AkinNotMyRealName@someemail.com
AKA : Larry The Cable Guy

Newcastle

192.COM

192.COM

FAIL

Alice, Alice, who the &$#@! is Alice?

Info Gathering

bebo myspace.com™

a place for friends

- Email addresses
- Nick names
- Friends
- Addresses
- Schools
- Pictures… lots of pictures

Info Gathering

bebo

myspace.com™
a place for friends

- Email addresses
- Nick names
- Friends
- Addresses
- Schools
- Pictures… lots of pictures

facebook®

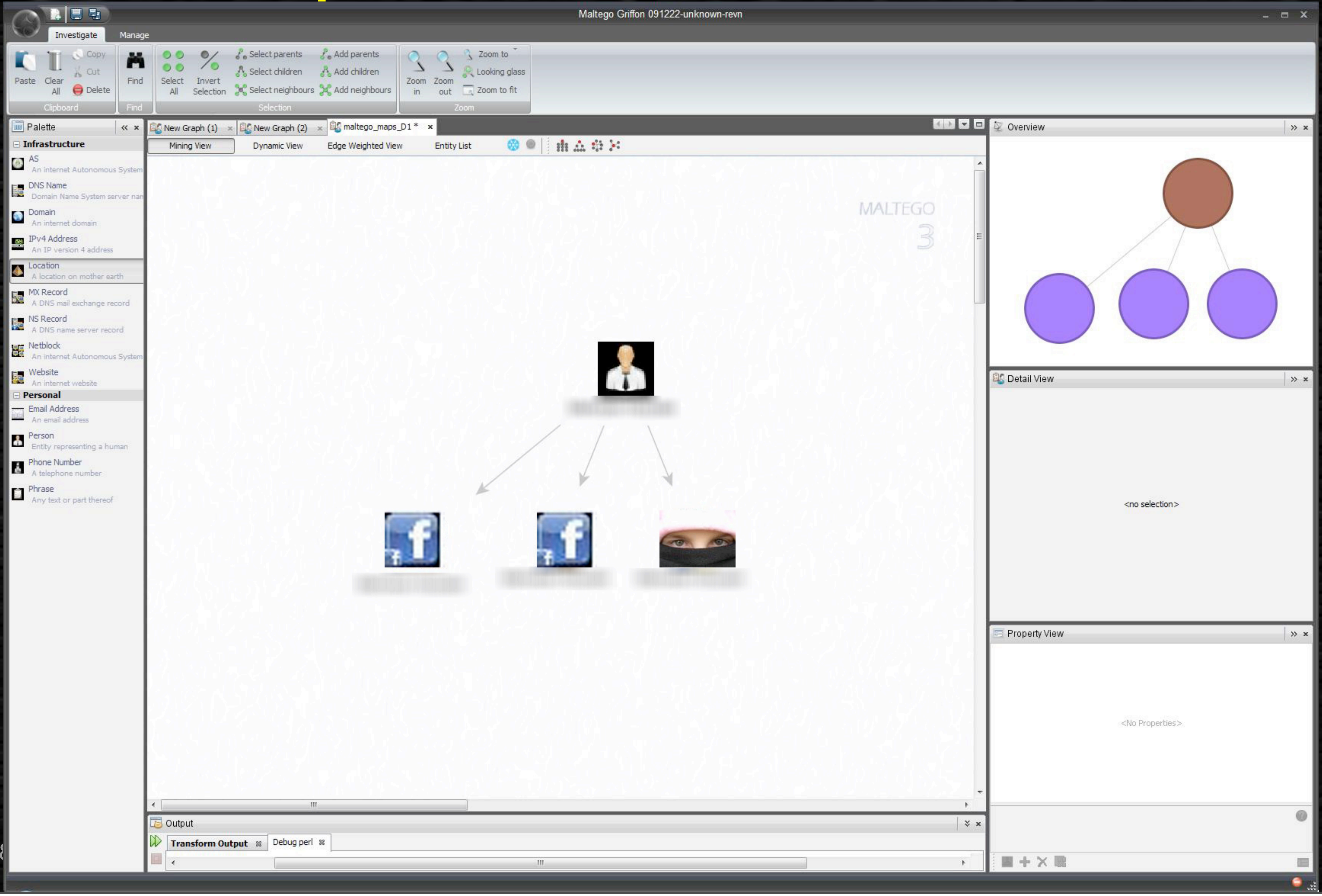
Dominic @Singe White

...wrote some useful facebook transforms for Maltego

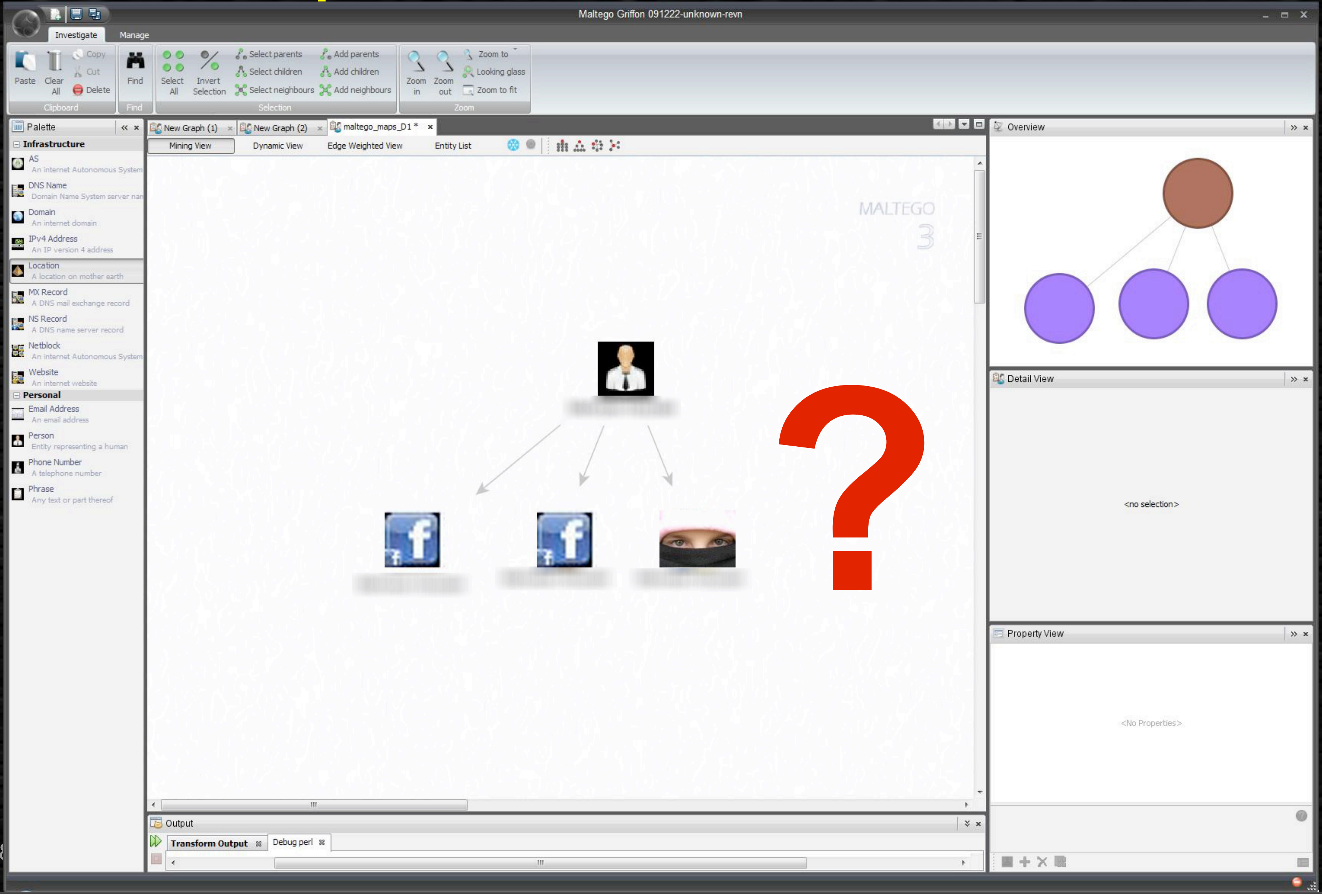
Python
Mechanize
Beautiful Soup

They'd break Facebook ToS so don't use them.

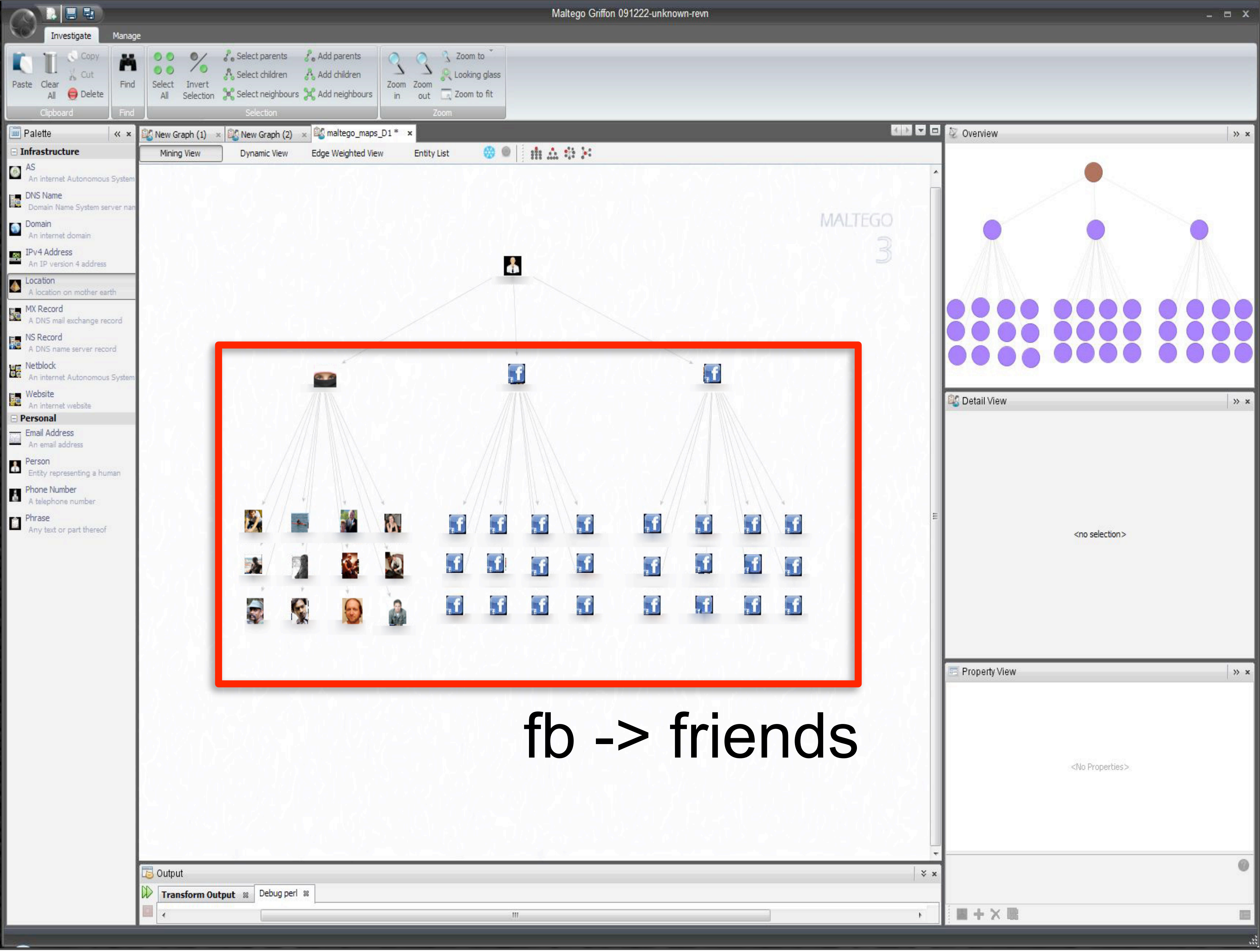
Step #3 Which “Alice” ?



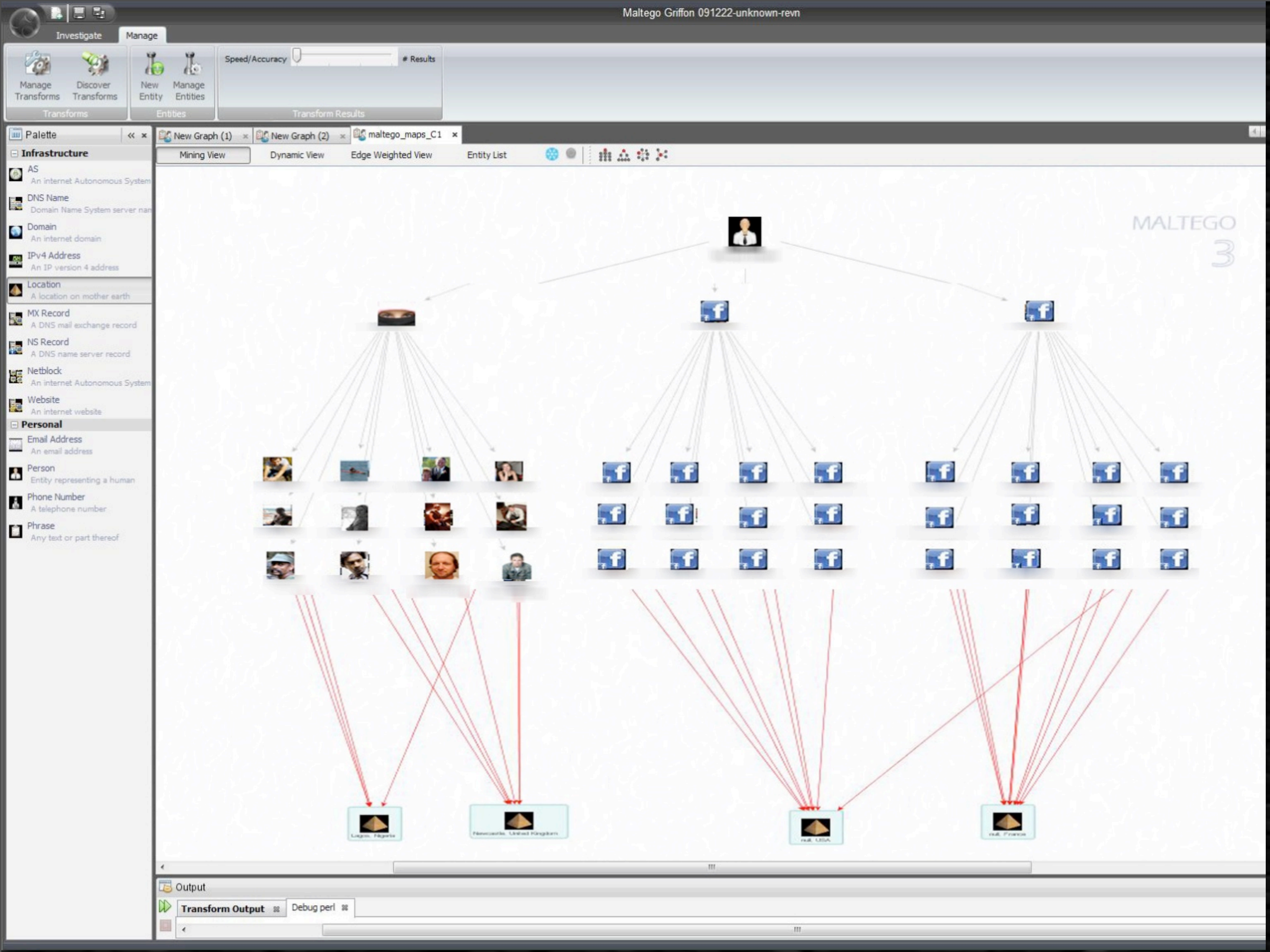
Step #3 Which "Alice" ?



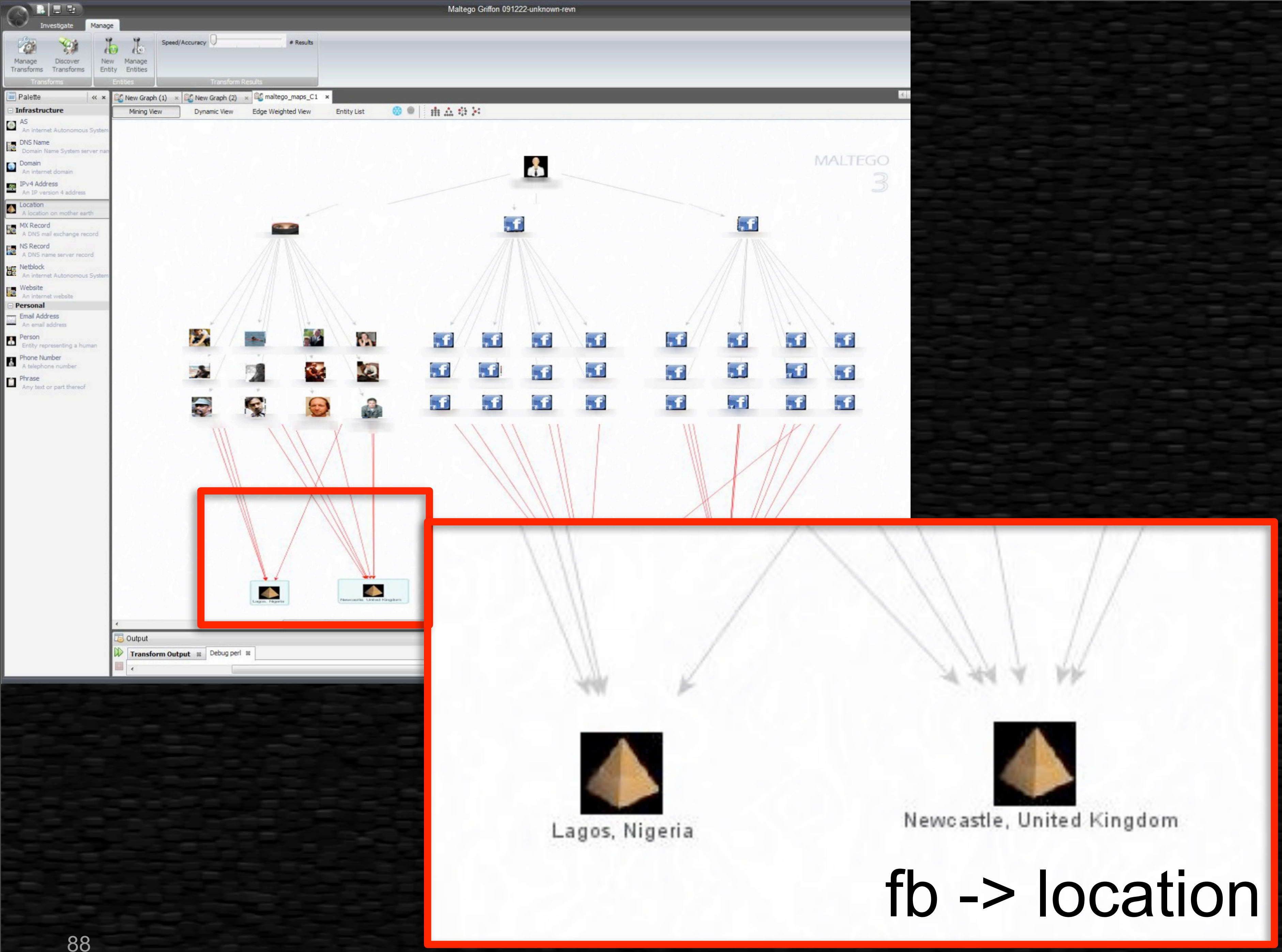
Tuesday, 3 August 2010


Maltego Griffon 091222-unknown-revn
Investigate
Manage
Paste
Clear All
Copy
Cut
Delete
Clipboard
Find
Select All
Invert Selection
Select parents
Select children
Select neighbours
Add parents
Add children
Add neighbours
Selection
Zoom in
Zoom out
Zoom to
Looking glass
Zoom to fit
Zoom
Palette
Infrastructure
AS
An internet Autonomous System
DNS Name
Domain Name System server nan
Domain
An internet domain
IPv4 Address
An IP version 4 address
Location
A location on mother earth
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
An internet Autonomous System
Website
An internet website
Personal
Email Address
An email address
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
New Graph (1)
New Graph (2)
maltego_maps_D1 *
Mining View
Dynamic View
Edge Weighted View
Entity List
MALTEGO 3
Overview
Detail View
<no selection>
Property View
<No Properties>
Output
Transform Output
Debug perl

fb -> friends


Maltego Griffon 091222-unknown-revn
Investigate
Manage
Manage Transforms
Discover Transforms
Transforms
New Entity
Manage Entities
Entities
Speed/Accuracy
# Results
Transform Results
Palette
Infrastructure
AS
An internet Autonomous System
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
Location
A location on mother earth
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
An internet Autonomous System
Website
An internet website
Personal
Email Address
An email address
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
New Graph (1)
New Graph (2)
maltego_maps_C1
Mining View
Dynamic View
Edge Weighted View
Entity List
MALTEGO
3
Lagos, Nigeria
Newcastle, United Kingdom
null, USA
null, France
Output
Transform Output
Debug perl

fb -> location


Maltego Griffon 091222-unknown-revn
Investigate
Manage
Manage Transforms
Discover Transforms
Transforms
New Entity
Manage Entities
Entities
Speed/Accuracy
# Results
Transform Results
Palette
Infrastructure
AS
An internet Autonomous System
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
Location
A location on mother earth
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
An internet Autonomous System
Website
An internet website
Personal
Email Address
An email address
Person
Entity representing a human
Phone Number
A telephone number
Phrase
Any text or part thereof
New Graph (1)
New Graph (2)
maltego_maps_C1
Mining View
Dynamic View
Edge Weighted View
Entity List
MALTEGO 3
Output
Transform Output
Debug perl
Lagos, Nigeria
Newcastle, United Kingdom

fb -> location

How to get sued by Facebook

How to get sued by Facebook

- Pete Warden

How to get sued by Facebook

- Pete Warden
- Built his own search engine

How to get sued by Facebook

- Pete Warden
- Built his own search engine
- 100 machine cluster (running Hadoop) for $10 per hour

How to get sued by Facebook

- Pete Warden
- Built his own search engine
- 100 machine cluster (running Hadoop) for $10 per hour
- Crawled Facebook

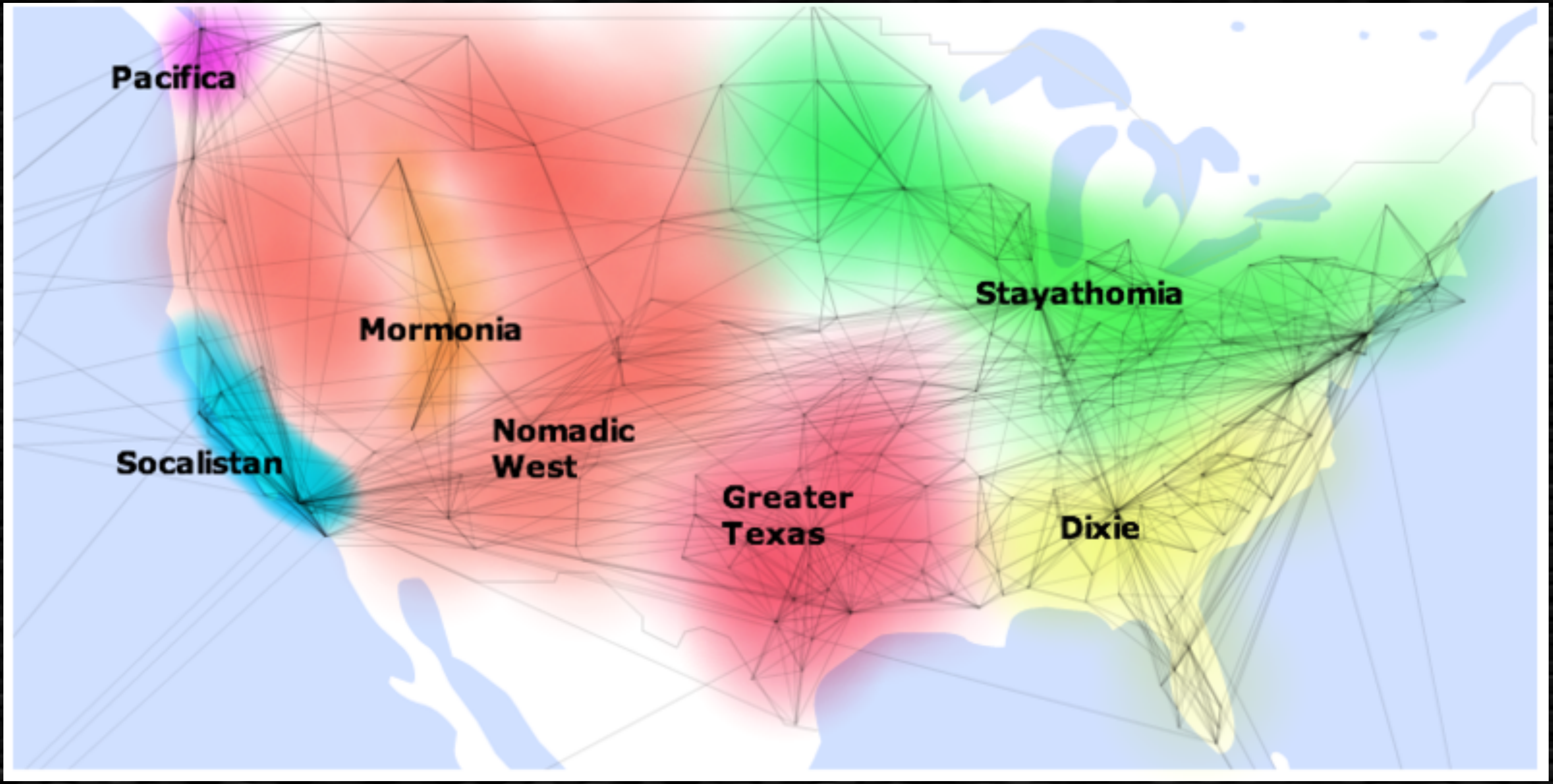
How to get sued by Facebook

- Pete Warden
- Built his own search engine
- 100 machine cluster (running Hadoop) for $10 per hour
- Crawled Facebook
- 220million profiles (name, location, email) in 10 hours for $100

How to get sued by Facebook

- Pete Warden
- Built his own search engine
- 100 machine cluster (running Hadoop) for $10 per hour
- Crawled Facebook
- 220million profiles (name, location, email) in 10 hours for $100
- So don’t do it without asking them nicely, even if you’re Law Enforcement

220 freakin' million



Information Available to All

Information Available to All

- If their privacy is “Everyone”, you’re in.

Information Available to All

- If their privacy is “Everyone”, you’re in.
- If not, you can only do so much without being a friend...sort of

Show me the good stuff

Show me the good stuff

- You could create bad apps & get people to use them,then FQL works nicely with Maltego.
  - See “Social Zombies”

Show me the good stuff

- You could create bad apps & get people to use them,then FQL works nicely with Maltego.
    - See “Social Zombies”

- You could just make friends with people and adopt @singe’s approach
    - See “Satan is on your friends list”

Show me the good stuff

- You could create bad apps & get people to use them,then FQL works nicely with Maltego.
  - See "Social Zombies"
- You could just make friends with people and adopt @singe's approach
  - See "Satan is on your friends list"
- Or maybe you're smart, like TheHarmonyGuy

Step #4 Making New Friends

Step #4 Making New Friends

- Create a credible account

Step #4 Making New Friends

- Create a credible account
- Build up your identity

Step #4 Making New Friends

- Create a credible account
- Build up your identity
- Don’t go directly for your target
  - Join similar Groups/Universities/Schools etc
  - Friends of friends
  - Target

Step #4 Making New Friends

- Create a credible account
- Build up your identity
- Don’t go directly for your target
  - Join similar Groups/Universities/Schools etc
  - Friends of friends
  - Target
- Over 1000 friends? They’re “easy”

Step #4 Making New Friends

- Create a credible account
- Build up your identity
- Don’t go directly for your target
  - Join similar Groups/Universities/Schools etc
  - Friends of friends
  - Target
- Over 1000 friends? They’re “easy”
- Take your time

Step #4 Making New Friends

- Create a credible account
- Build up your identity
- Don’t go directly for your target
  - Join similar Groups/Universities/Schools etc
  - Friends of friends
  - Target
- Over 1000 friends? They’re “easy”
- Take your time
- or automate it and get the nasty business over with

Will you be my friend?

Will you be my friend?

Hey, do I know you?

Will you be my friend?

Hey, do I know you?

< SHIT !!! >

Will you be my friend?

Hey, do I know you?

< SHIT !!! >

I’m a friend of “Alice”’s, just getting started and that. I added a few people and might have added too many.

Will you be my friend?

Hey, do I know you?

< SHIT !!! >

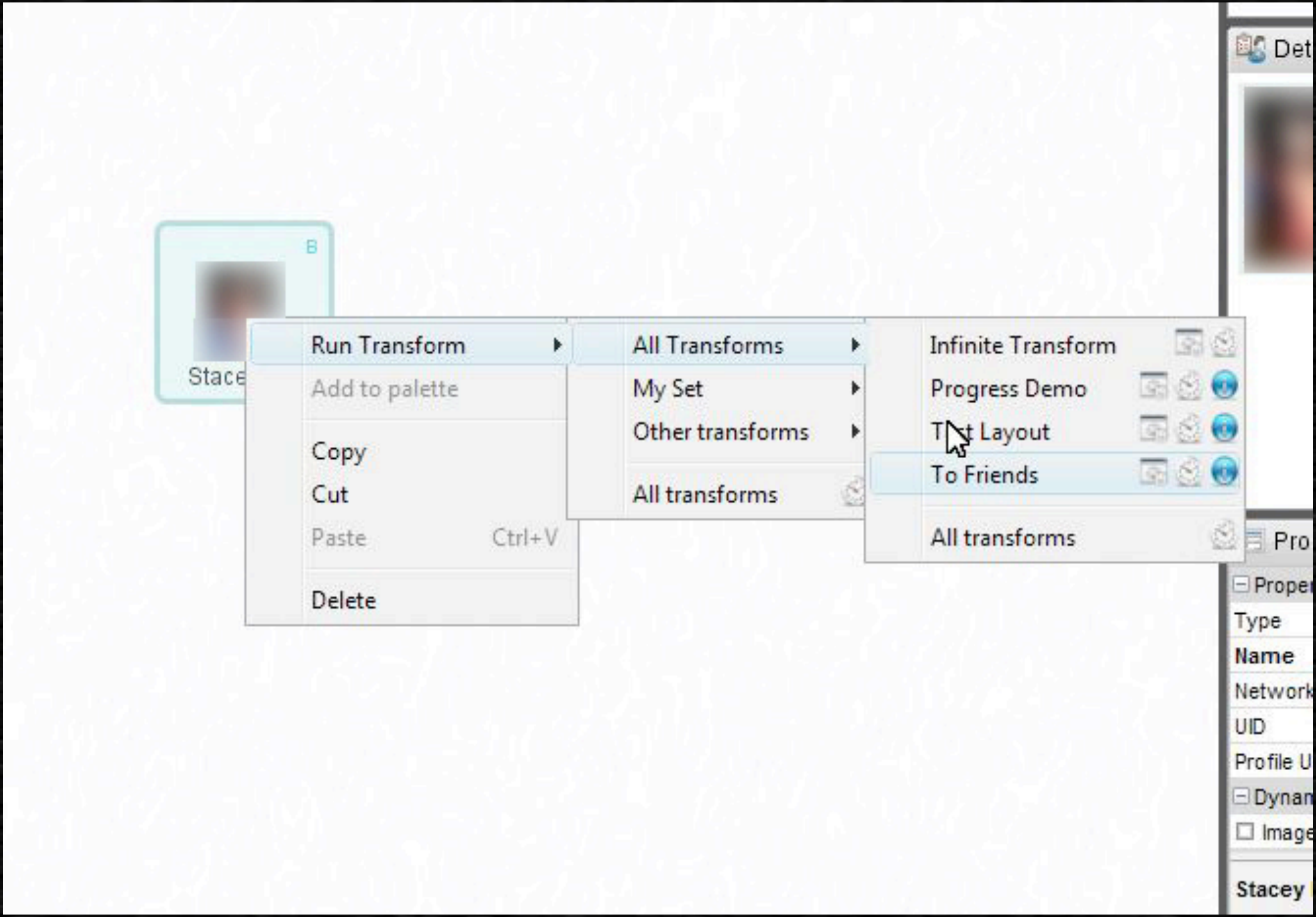
I’m a friend of “Alice”’s, just getting started and that. I added a few people and might have added too many.

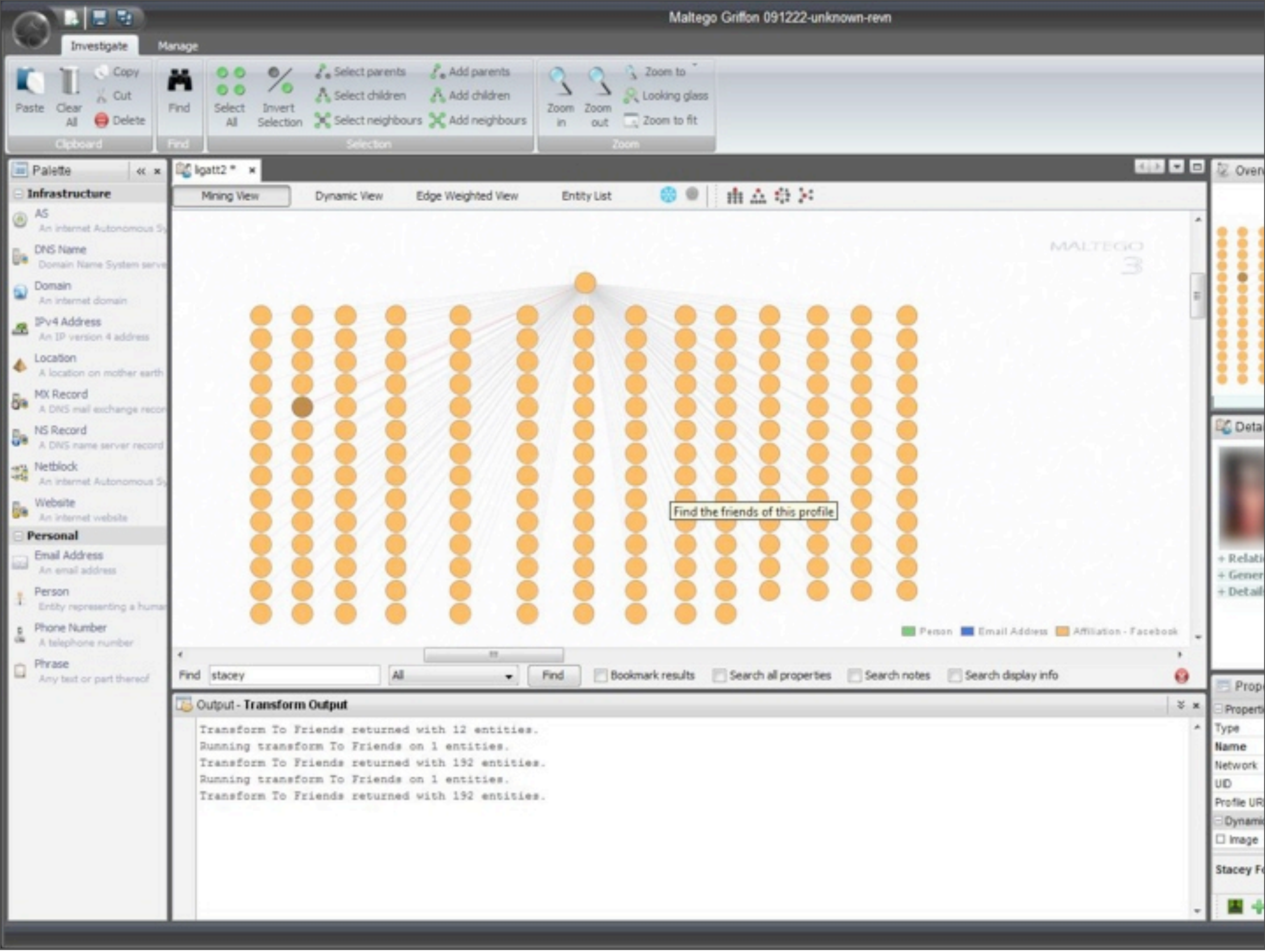
hehehe man cool, well “Alice”’s my best friend lol

Step #5 Building a map of interesting peoples

```
Until EOFriends {
        Get friend
        Get location
        IF (location = Nigeria|Lagos|…) {
                        Scrape & Parse wall posts }
        Download photos
        IF (wallPosts contain “phrases”) {
                        Download interesting wall posts }
        IF (“interesting”) {
                        Pipe back to Maltego}
}
```

To Facebook Friends



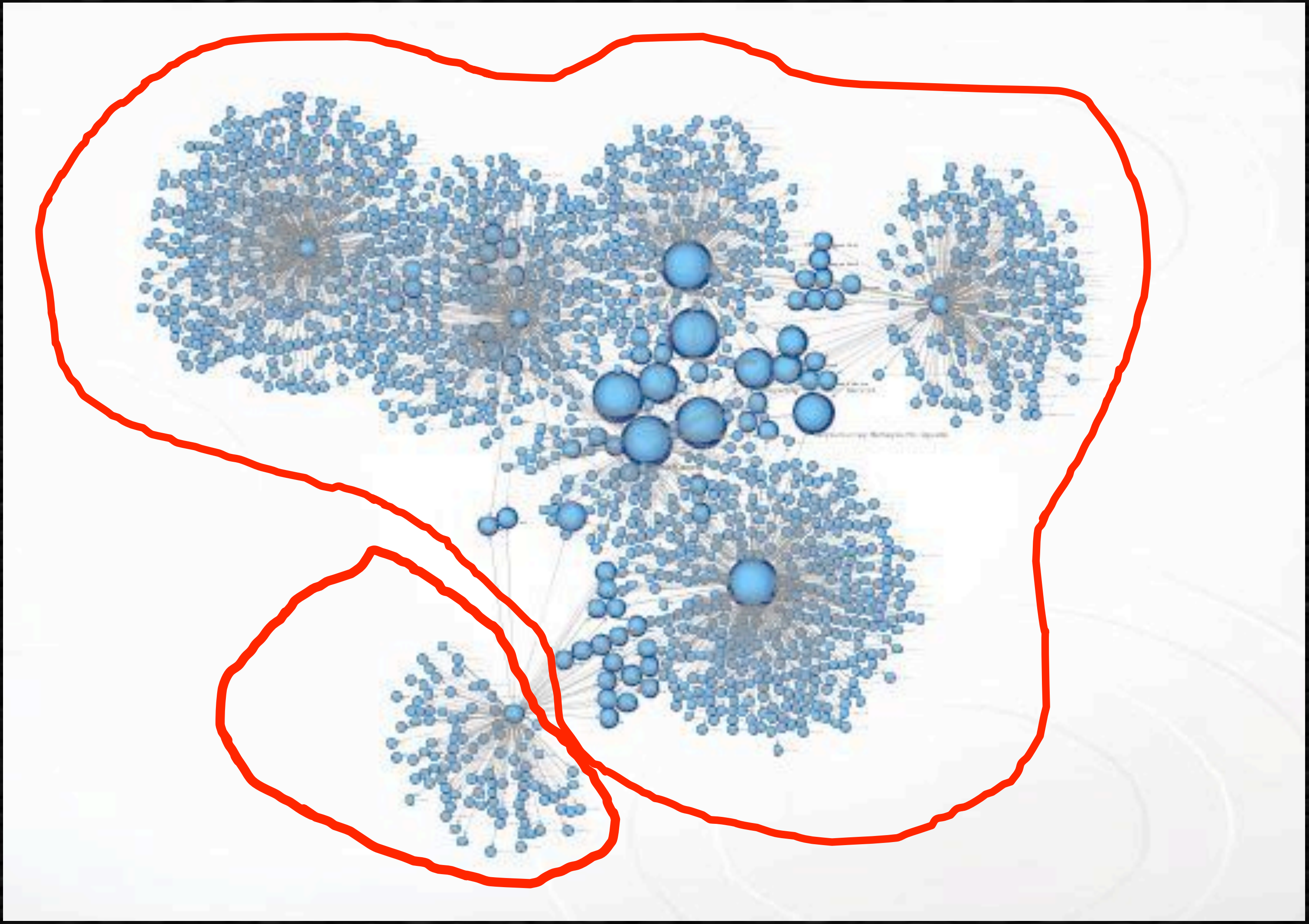


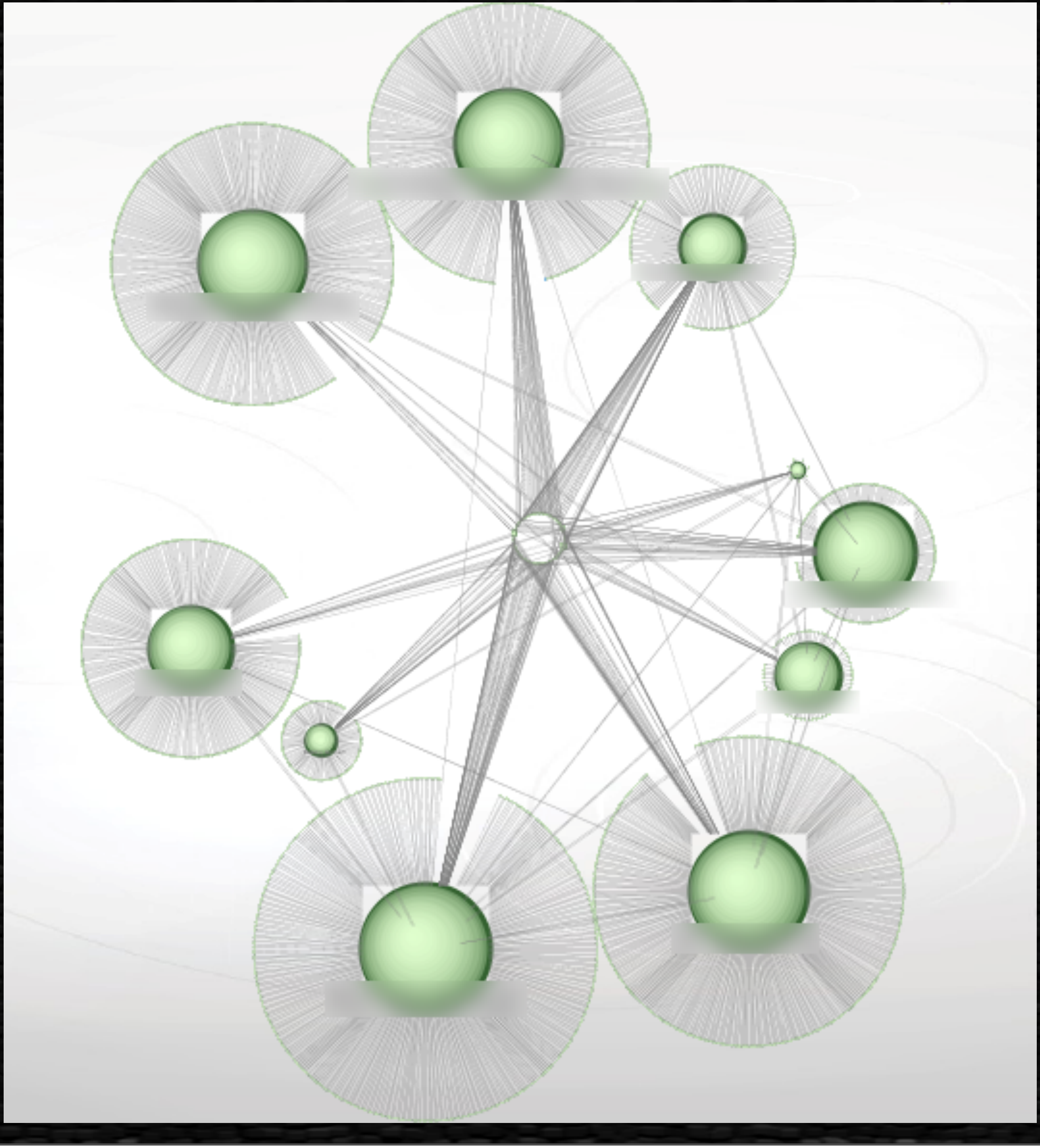
Find stacey All Find □ Bookmark results □ Search all properties □ Search notes □ Search display info

Output - **Transform Output**

```
Transform To Friends returned with 12 entities.
Running transform To Friends on 1 entities.
Transform To Friends returned with 192 entities.
Running transform To Friends on 1 entities.
Transform To Friends returned with 192 entities.
```

“Interesting” People





“7k in 5 days”

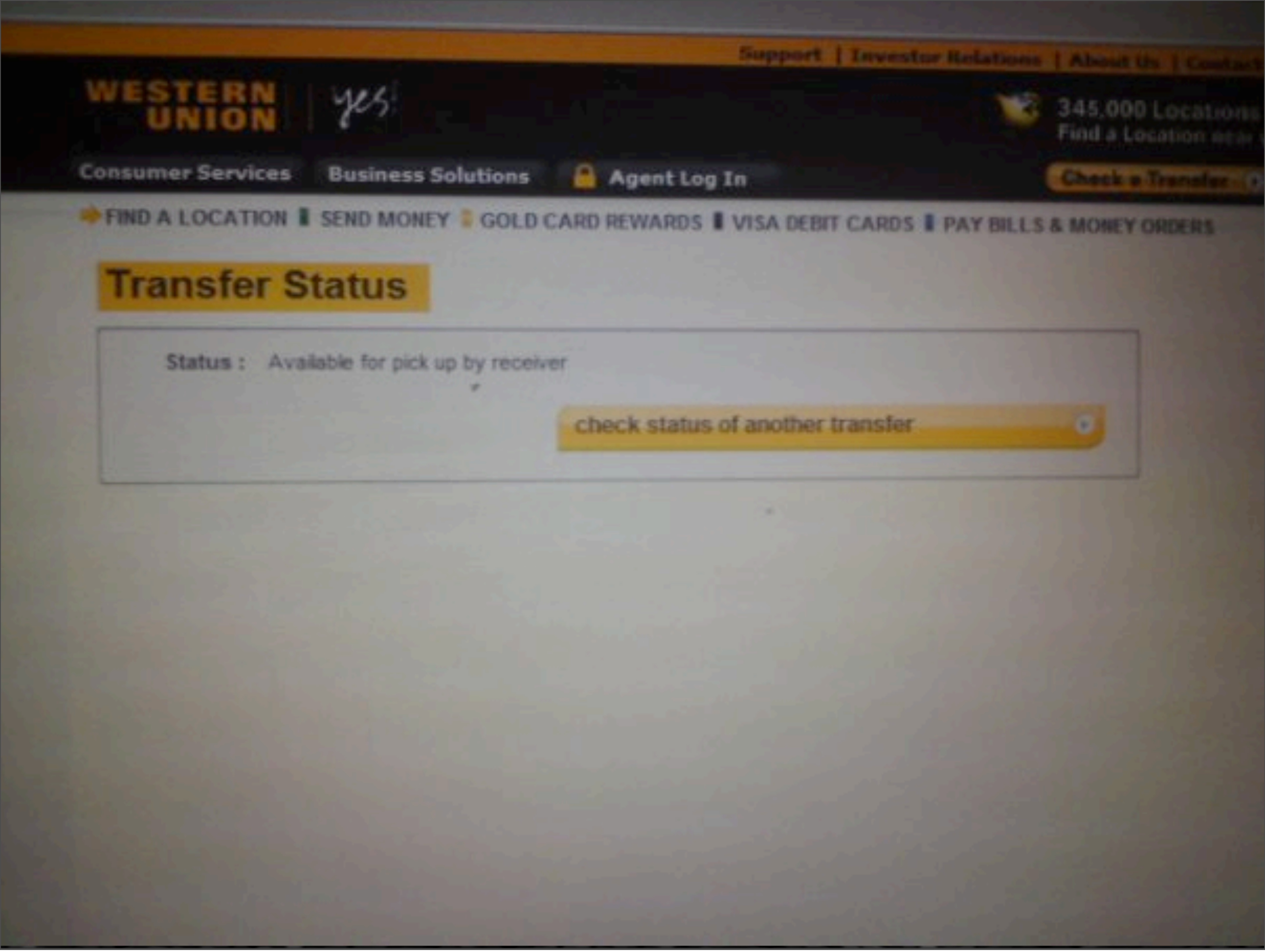
- Fast money
- Flashy rides
- Expensive clothes
- HOT chicks
- Luxury apartment
- “Its really easy to spot a yahoo boy in Nigeria, their lifestyle is pretty much the same, living the young Nigerian dream”

“I GET PAID IN POUNDS BUT I COLLECTED IN NAIRA CASH”

PS3 4 SALE....UK PAL.NEW

OPEN
24 HOURS
WESTERN UNION®
WESTERN UNION

“Arrrrgh!”



Transfer Status

Status : Available for pick up by receiver

What’s the attraction?

- Avg month salary
  - – $4,000 USA
  - – ~$200 Nigeria

- Scamming pays roughly $700 to $6,000 per/month*

Call to Action

“12.4 MILLION PEOPLE RECORDED DEAD AFTER BEING SCAMMED BY NIGERIA SCAMMERS 2009. 919 MILLION DOLLARS RECORD SCAMMED FOR THE YEAR 2009 BY SAME NIGERIA SCAMMERS. WE ARE TRYING OHH THIS 2010 LETS SCAM 20 BILLION POUNDS AFTER ALL IS NOT YET UP TO AMOUNT OF NIGERIANS TRADED FOR SLAVERY IN 1905(start working)”

How about something a little more nefarious?

21 September 2009

How about something a little more nefarious?

21 September 2009

B…………………….LING BLING

Gats

Links with terror?

- In 2008 and 2009 there was evidence directly linking 419 AFF networks to (attempted) attacks

419 Advance Fee Fraud Statistics 2009
(Ultrascan Advanced Global Investiagtions)

Step #6 The true identity of the scammer?

Step #6 The true identity of the scammer?

Hey, it’s Alice, this is my new email address... can you help? my facebook is weird, can you send me a wall post?

Step #6 The true identity of the scammer?

Hey, it's Alice, this is my new email address... can you help? my facebook is weird, can you send me a wall post?

Sure

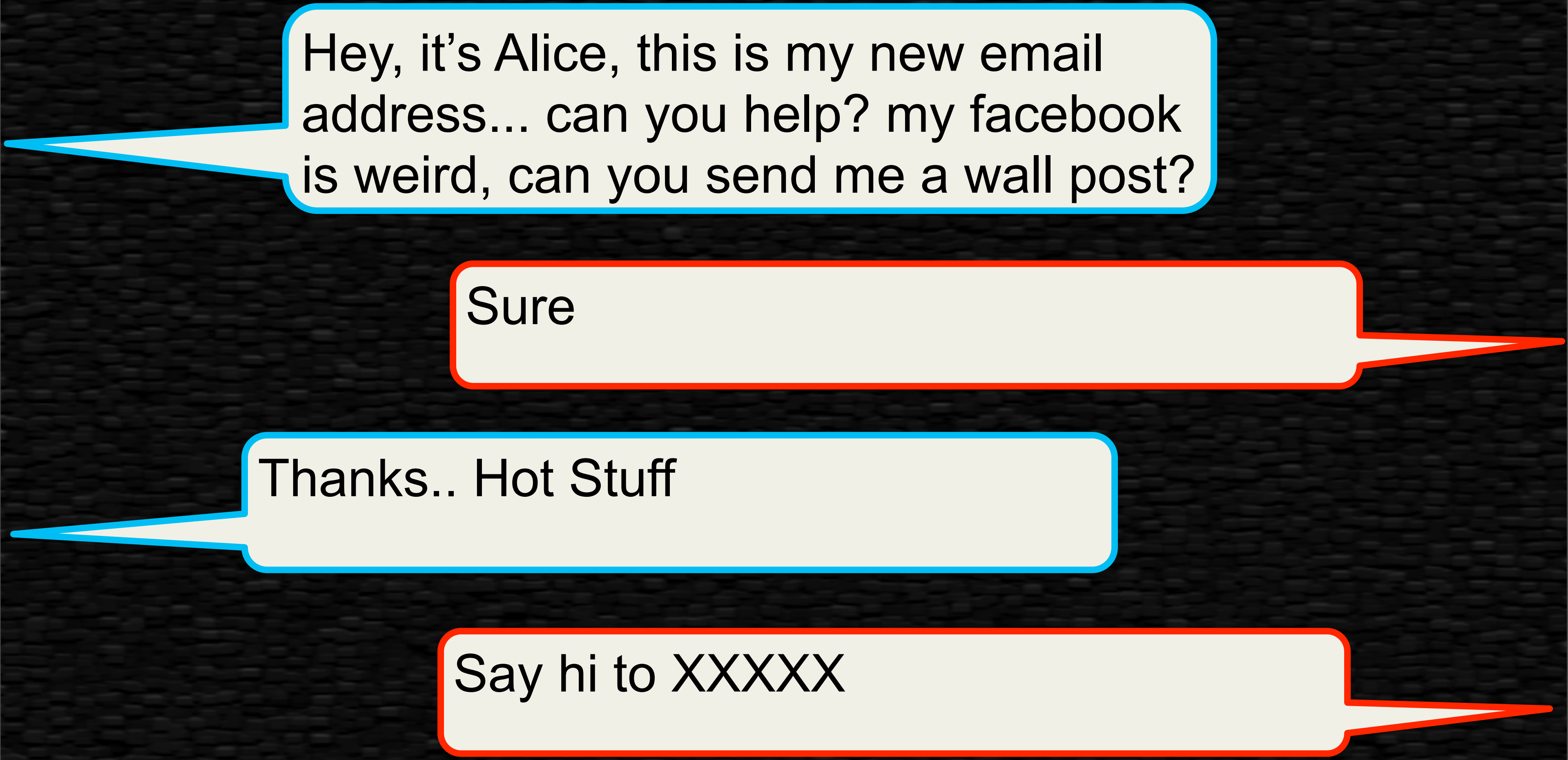
Step #6 The true identity of the scammer?

Hey, it’s Alice, this is my new email address... can you help? my facebook is weird, can you send me a wall post?

Sure

Thanks.. Hot Stuff

Step #6 The true identity of the scammer?



Hey, it’s Alice, this is my new email address... can you help? my facebook is weird, can you send me a wall post?

Sure

Thanks.. Hot Stuff

Say hi to XXXXX

Step #6 The true identity of the scammer?

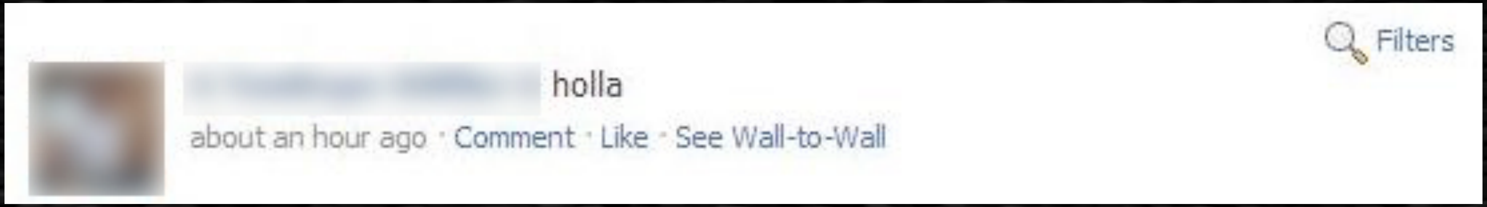
Hey, it’s Alice, this is my new email address... can you help? my facebook is weird, can you send me a wall post?

Sure

Thanks.. Hot Stuff

Say hi to XXXXX

BONUS!!!!>

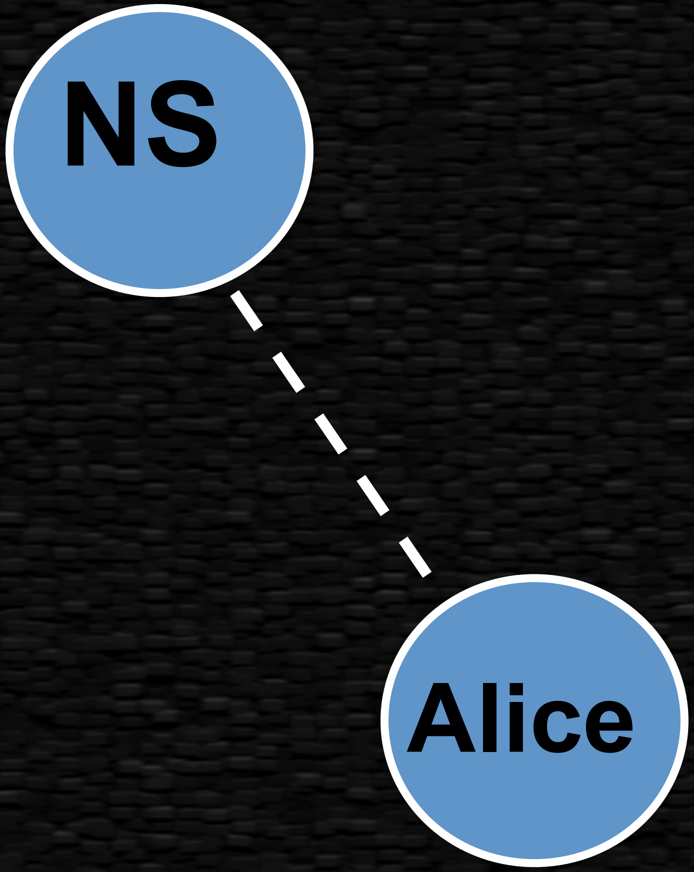


[redacted] holla

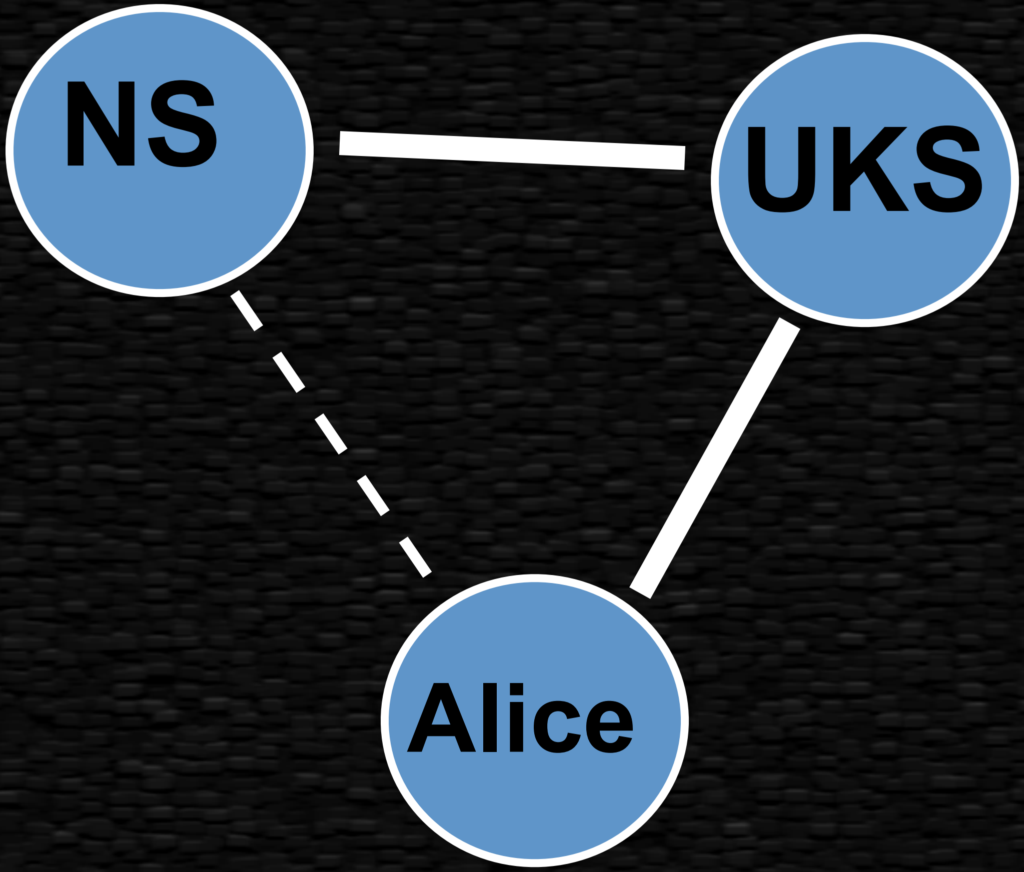
about an hour ago · Comment · Like · See Wall-to-Wall

Connections

Connections



Connections



Scammer Networks (on record)

Scammer Networks (on record)

- 62 in UK alone

Scammer Networks (on record)

- 62 in UK alone
- Spain highest with 72

Scammer Networks (on record)

- 62 in UK alone
- Spain highest with 72
- USA have 53

Scammer Networks (on record)

- 62 in UK alone
- Spain highest with 72
- USA have 53
- 916 around the world

Scammer Networks (on record)

- 62 in UK alone
- Spain highest with 72
- USA have 53
- 916 around the world
- with 16,626 members

Scammer Networks (on record)

- 62 in UK alone
- Spain highest with 72
- USA have 53
- 916 around the world
- with 16,626 members
- Raking in $9.3 billion dollars in 2009

Step #7 Gettin paid *(in full)*

Step #7 Gettin paid *(in full)*

- The Carrot/Stick
  - – Compile all info into a blog post
  - – Create a facebook fan site

Step #7 Gettin paid *(in full)*

- The Carrot/Stick
  - Compile all info into a blog post
  - Create a facebook fan site
- Email the scammers
  - Remind them that google will soon index them

Step #7 Gettin paid *(in full)*

- The Carrot/Stick
  - – Compile all info into a blog post
  - – Create a facebook fan site
- Email the scammers
  - – Remind them that google will soon index them
- Follow up with a call

Step #7 Gettin paid *(in full)*

- The Carrot/Stick
  - Compile all info into a blog post
  - Create a facebook fan site
- Email the scammers
  - Remind them that google will soon index them
- Follow up with a call
- Agree amicable terms

$ mv <scammers$> <my bank>

- Cash?
- Bank?
- paypal?
- Western union?
- Amazon Gift Certificates?

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

To do this you are either:

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

To do this you are either:

- Limited to public info (due to Terms of service)

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

To do this you are either:

- Limited to public info (due to Terms of service)
- Friend up (with your own account) the other potential bad guys and follow their links. You’d need “balls of steel” to do this.

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

To do this you are either:

- Limited to public info (due to Terms of service)
- Friend up (with your own account) the other potential bad guys and follow their links. You'd need "balls of steel" to do this.
- Work with Law Enforcement

HEALTH WARNING:

Messing With Criminals Can Reduce Your Life Expectancy

To do this you are either:

- Limited to public info (due to Terms of service)
- Friend up (with your own account) the other potential bad guys and follow their links. You’d need “balls of steel” to do this.
- Work with Law Enforcement
- You’d have to break ToS. Which will likely have facebook on your back as well as the bad guys.

Wrappin’ up

- Mining data more accessible than ever before
- Visualization can help you home in on interesting relationships

Wrappin’ up

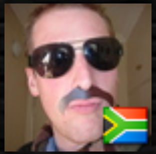
- Mining data more accessible than ever before
- Visualization can help you home in on interesting relationships
- NER can help classify information

Wrappin' up

- Mining data more accessible than ever before
- Visualization can help you home in on interesting relationships
- NER can help classify information
- Combination of the three to speed up pwnage

Maltego Tweeters

@Paterva



@Singe
Dominic White

@mubix
Rob Fuller

@carnal0wnage
Chris Gates

Social Network Tweeter

@agent0x0
Tom Eston

@digininga
Robin Wood

@theharmonyguy
Social Hacking

@SocialMediaSec
Social Media Security

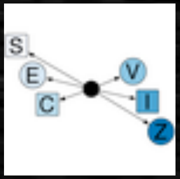
Data Mining & Visualization Tweeters

@dacort
Damon Cortesi

@PeteWarden
Pete Warden

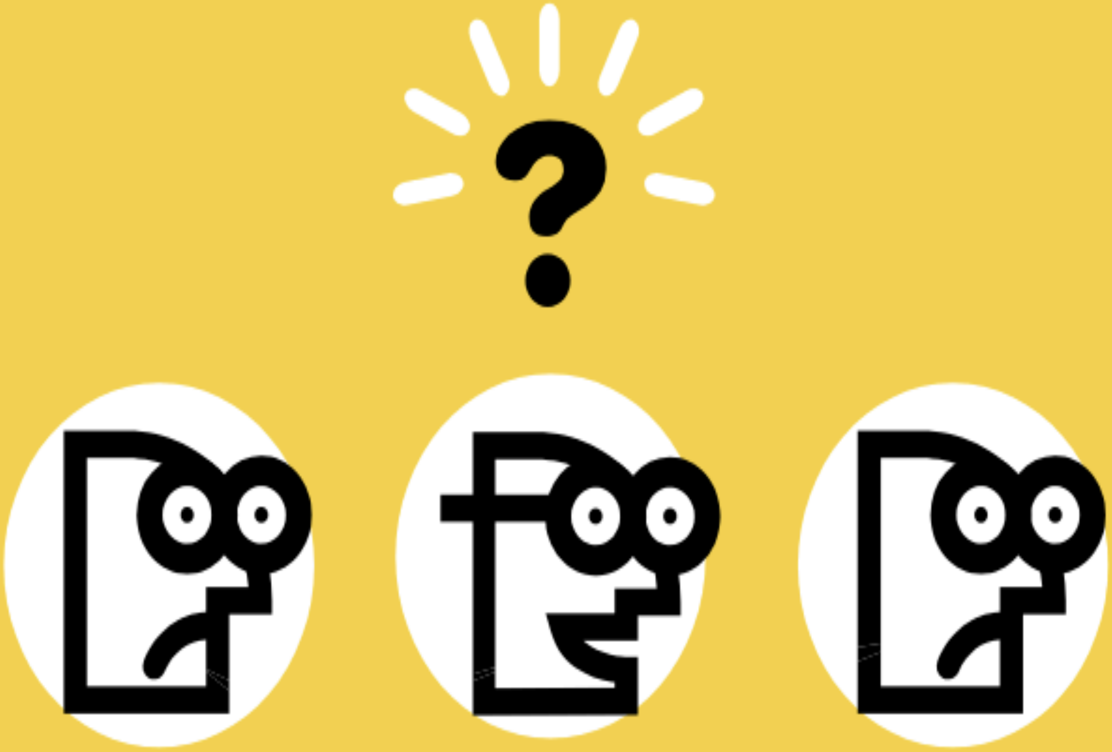
@neilkod
Neil Kodner

@zrlram @secviz
Raffael Marty



@secviz
Raffael Marty

33
SecurityG33k .com



It's QUESTION TIME !!