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

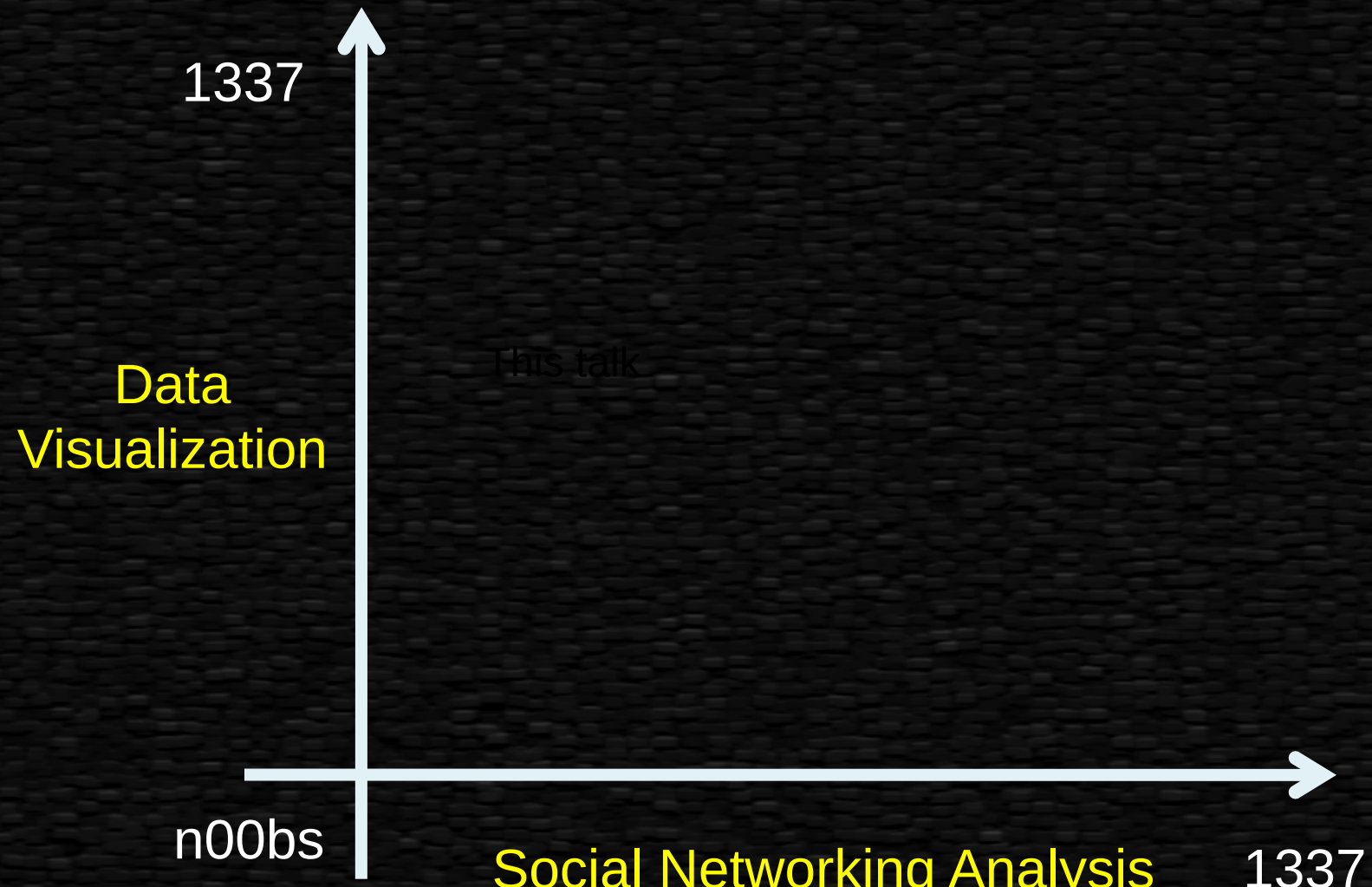
Goals

- Overview/appreciation of possibilities in this field
- Expose you to some ideas that you can apply to your specific situation

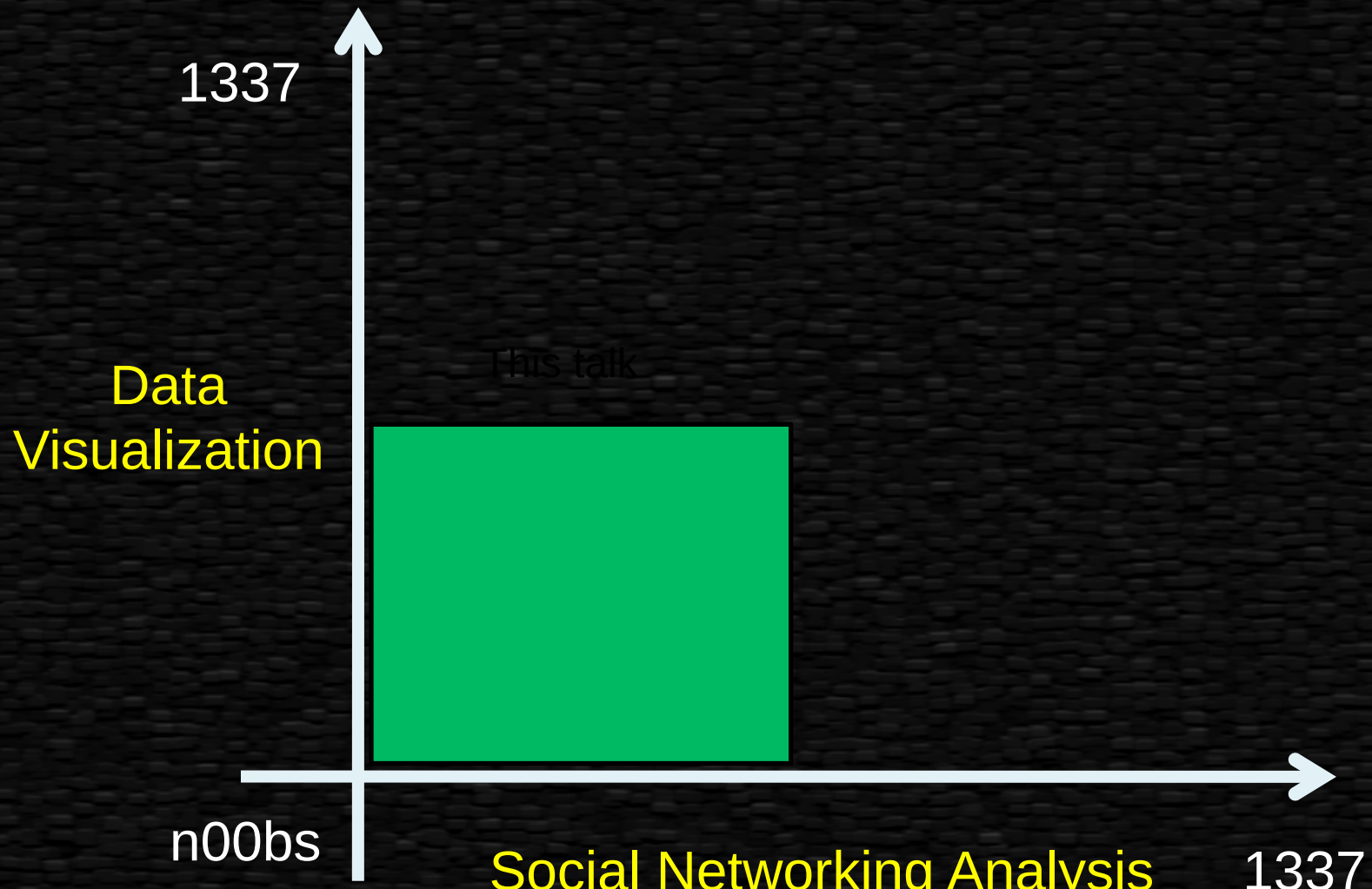
Who’s the talk aimed at?

This talk

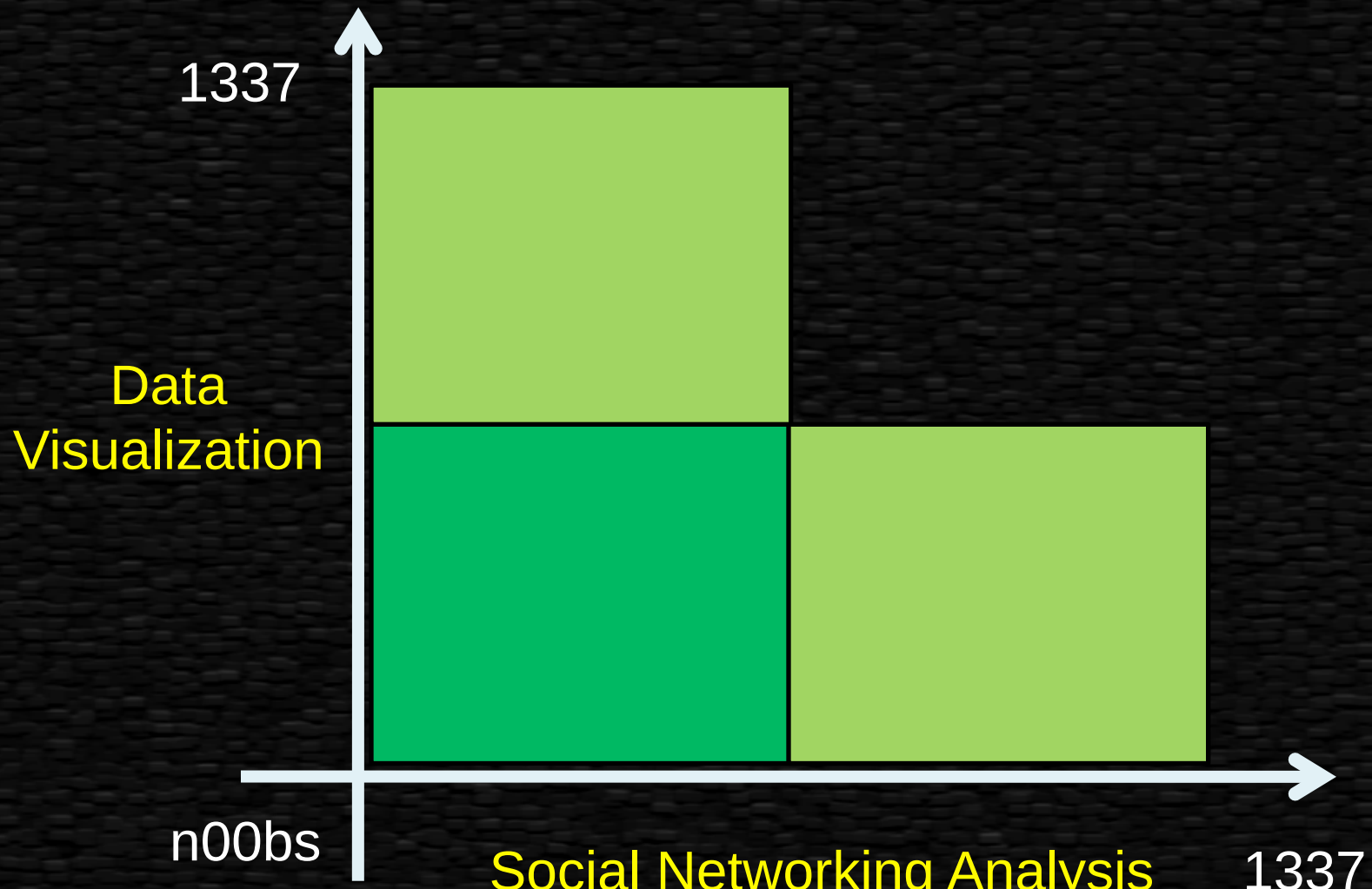
Who's the talk aimed at?



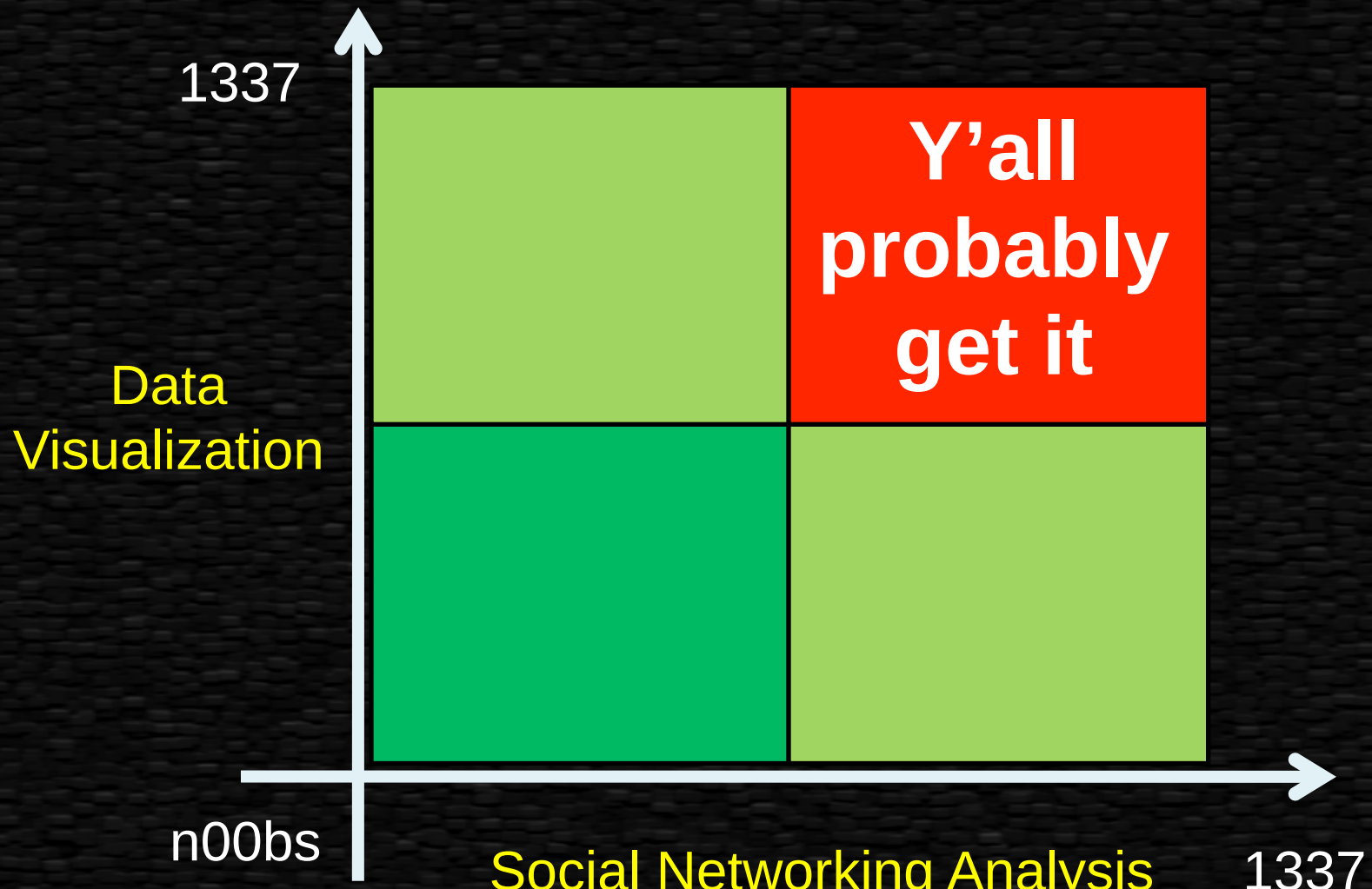
Who's the talk aimed at?



Who's the talk aimed at?



Who's the talk aimed at?



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

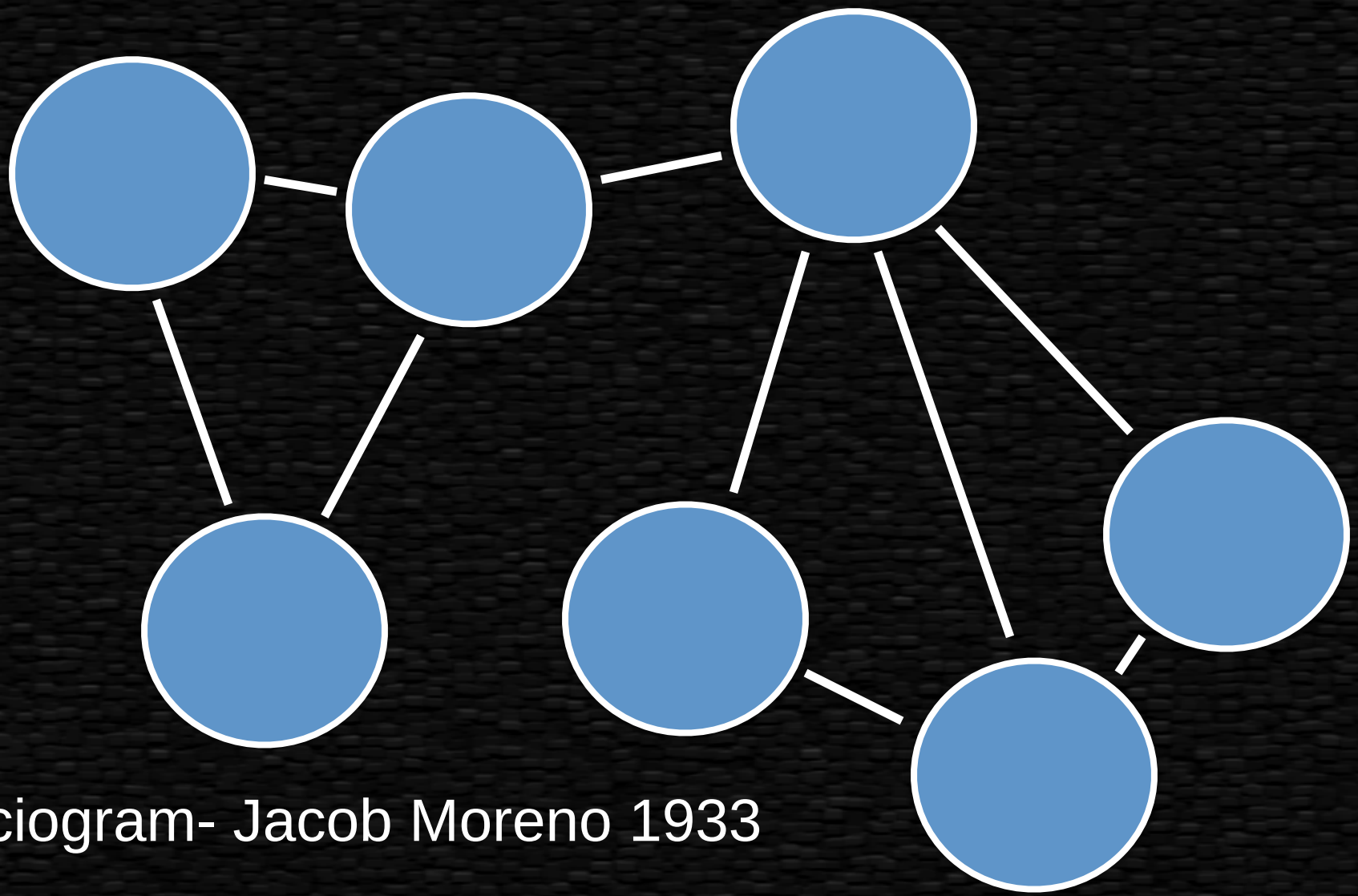
Social Network Analysis

\+ 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”

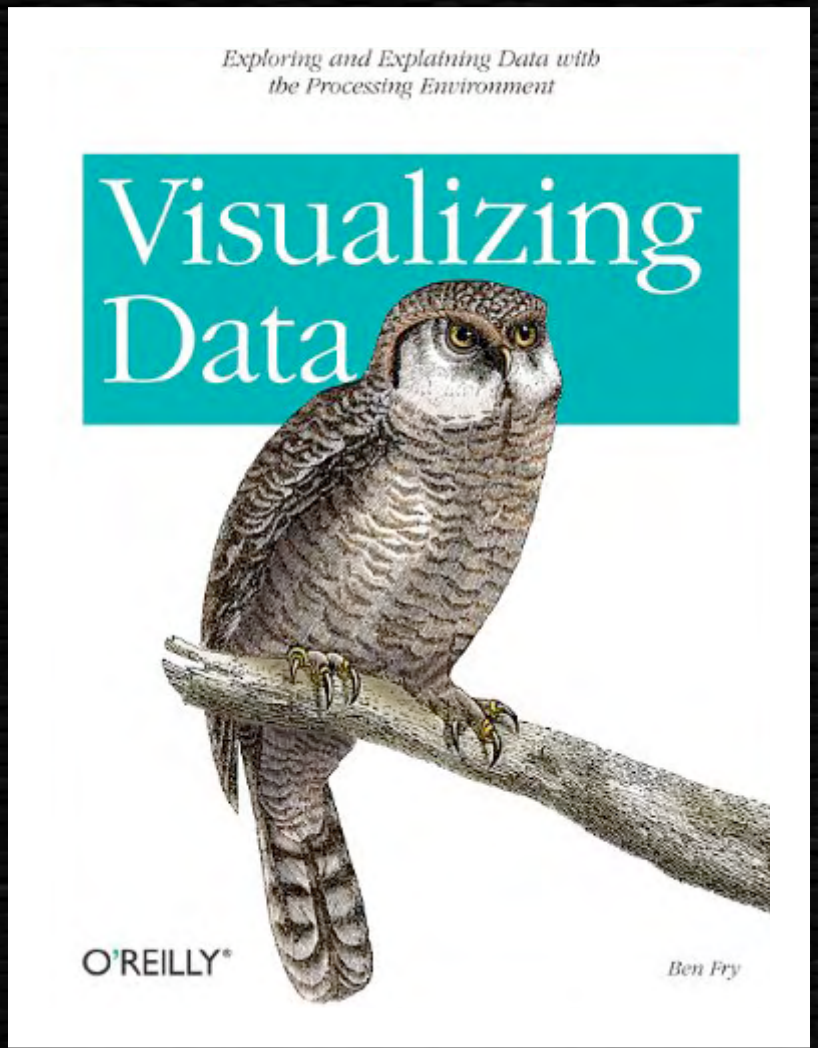
Named Entity Recognition

“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>.

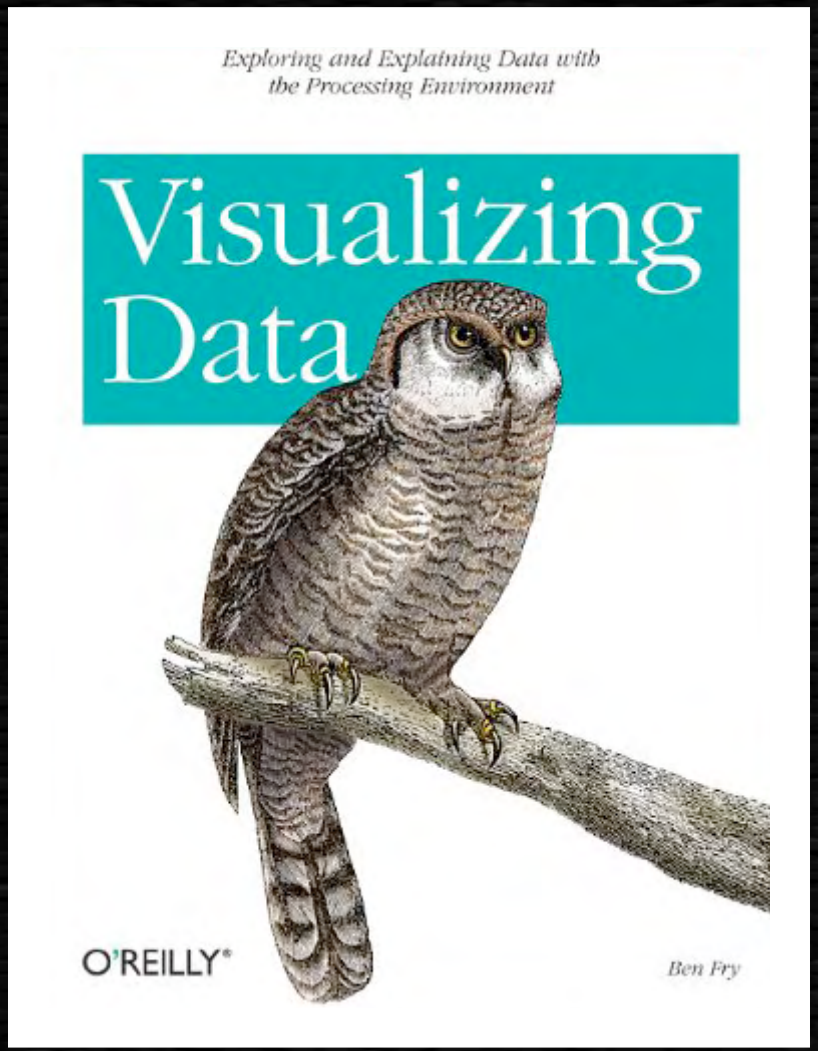
Data Visualization



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

Ben Fry

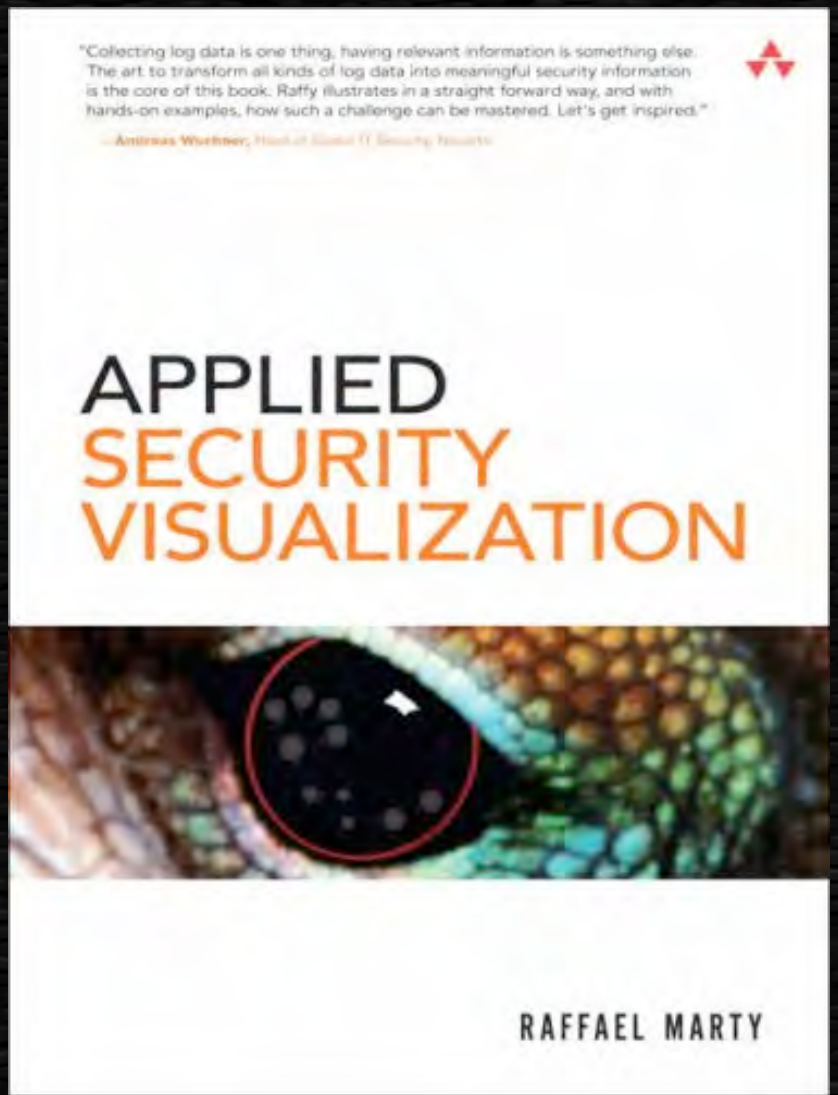
Data Visualization



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

Ben Fry

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?

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

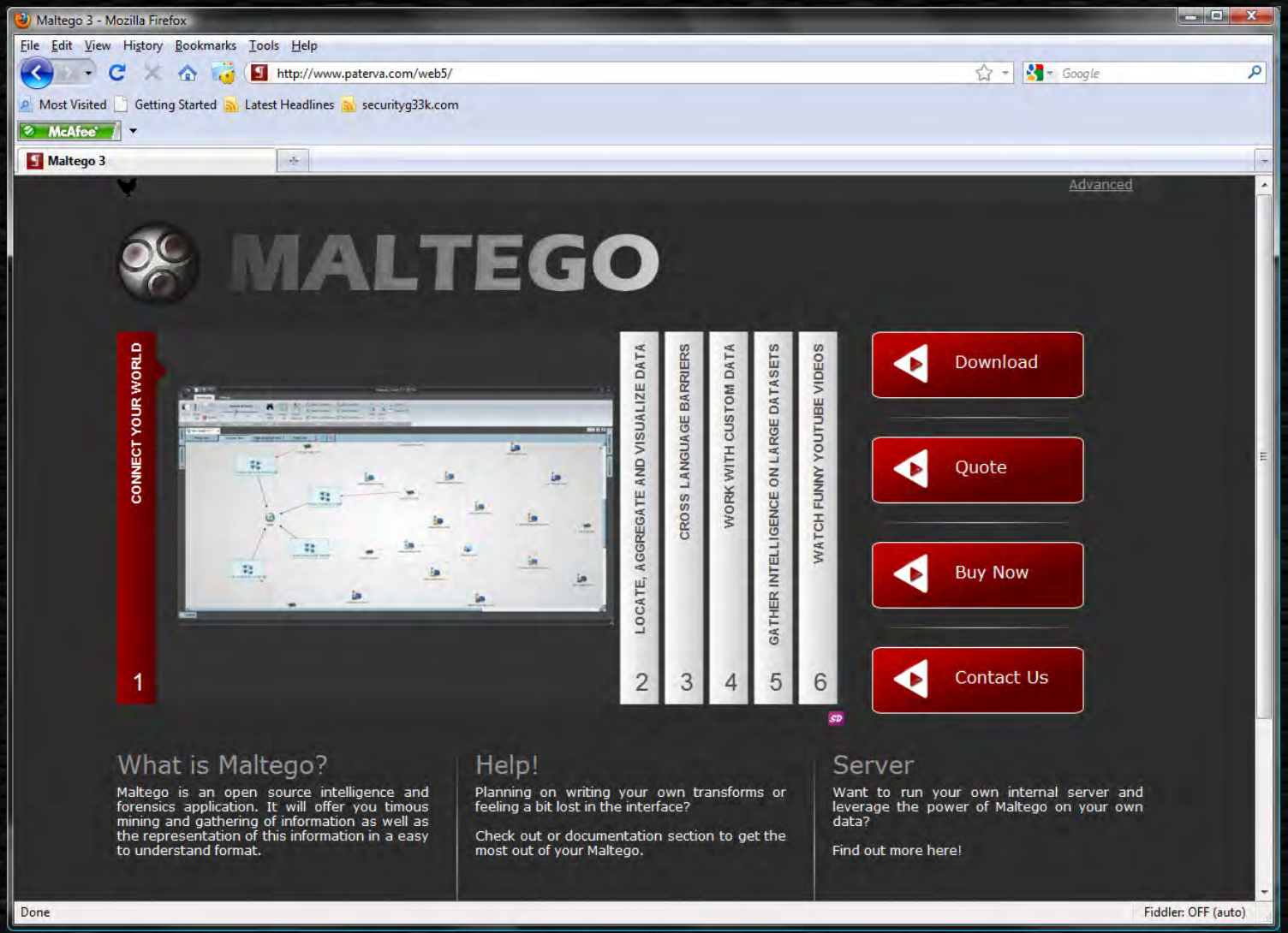
Maltego

- 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

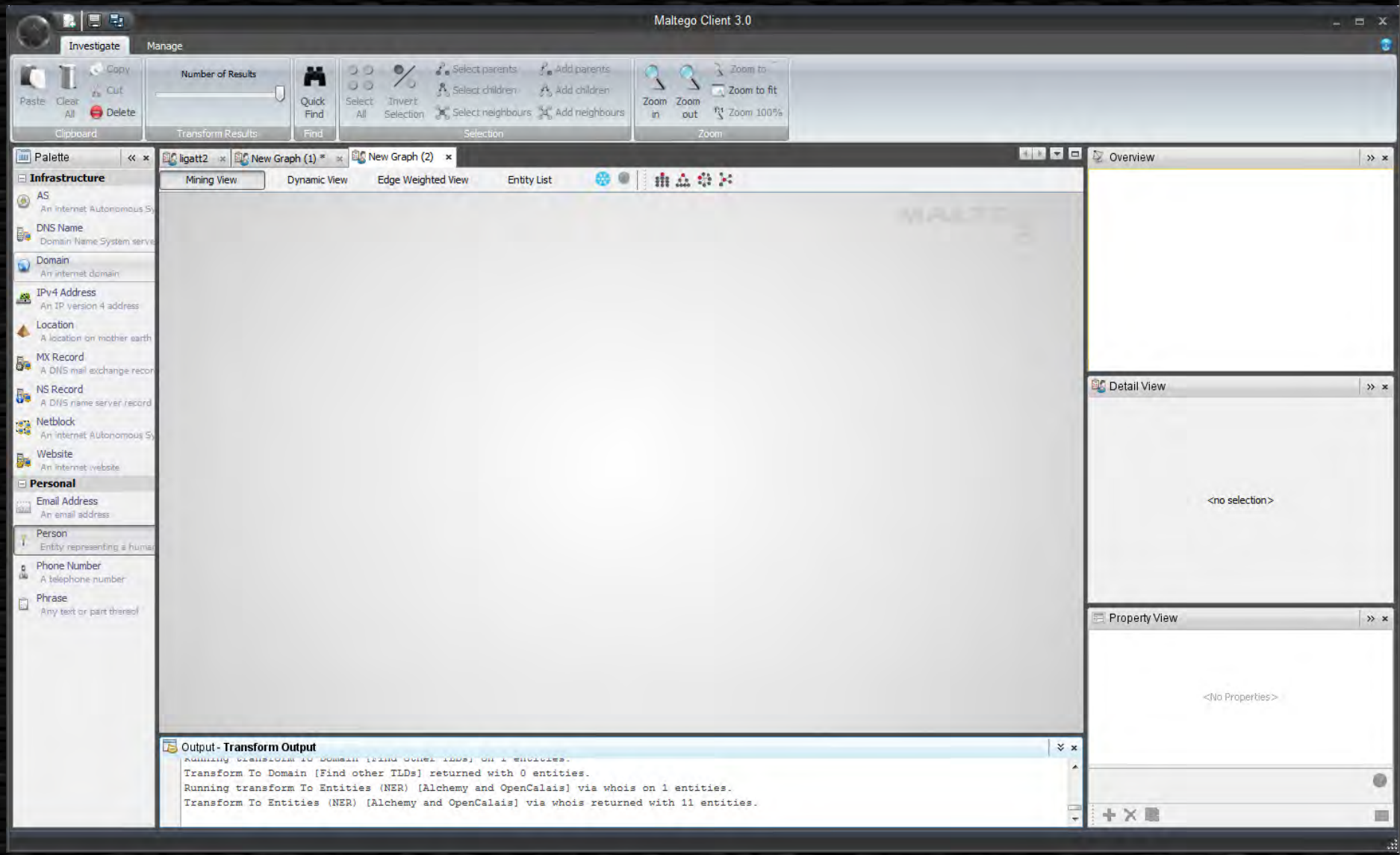


www.paterva.com

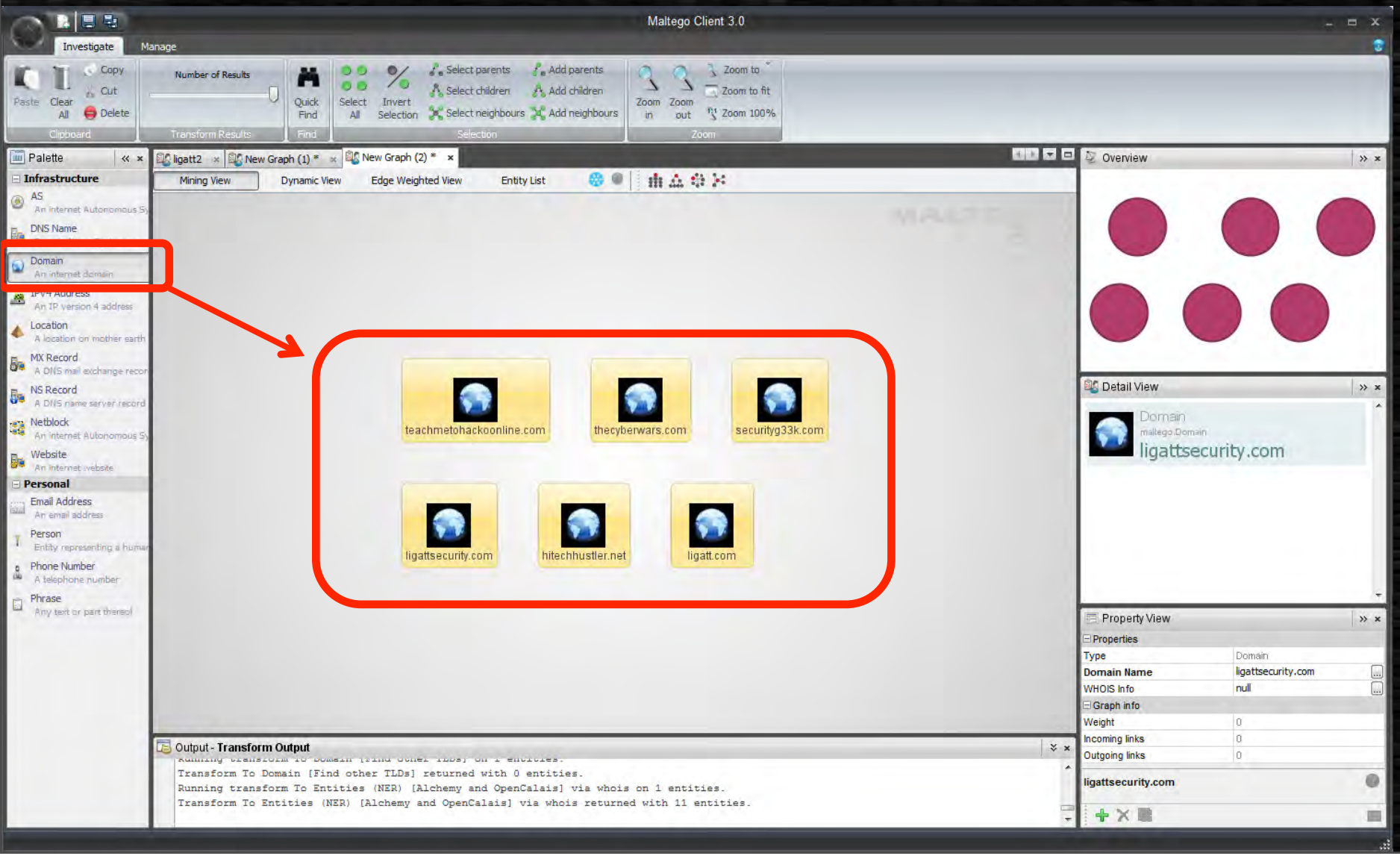


25% Discount 'BlackHat'

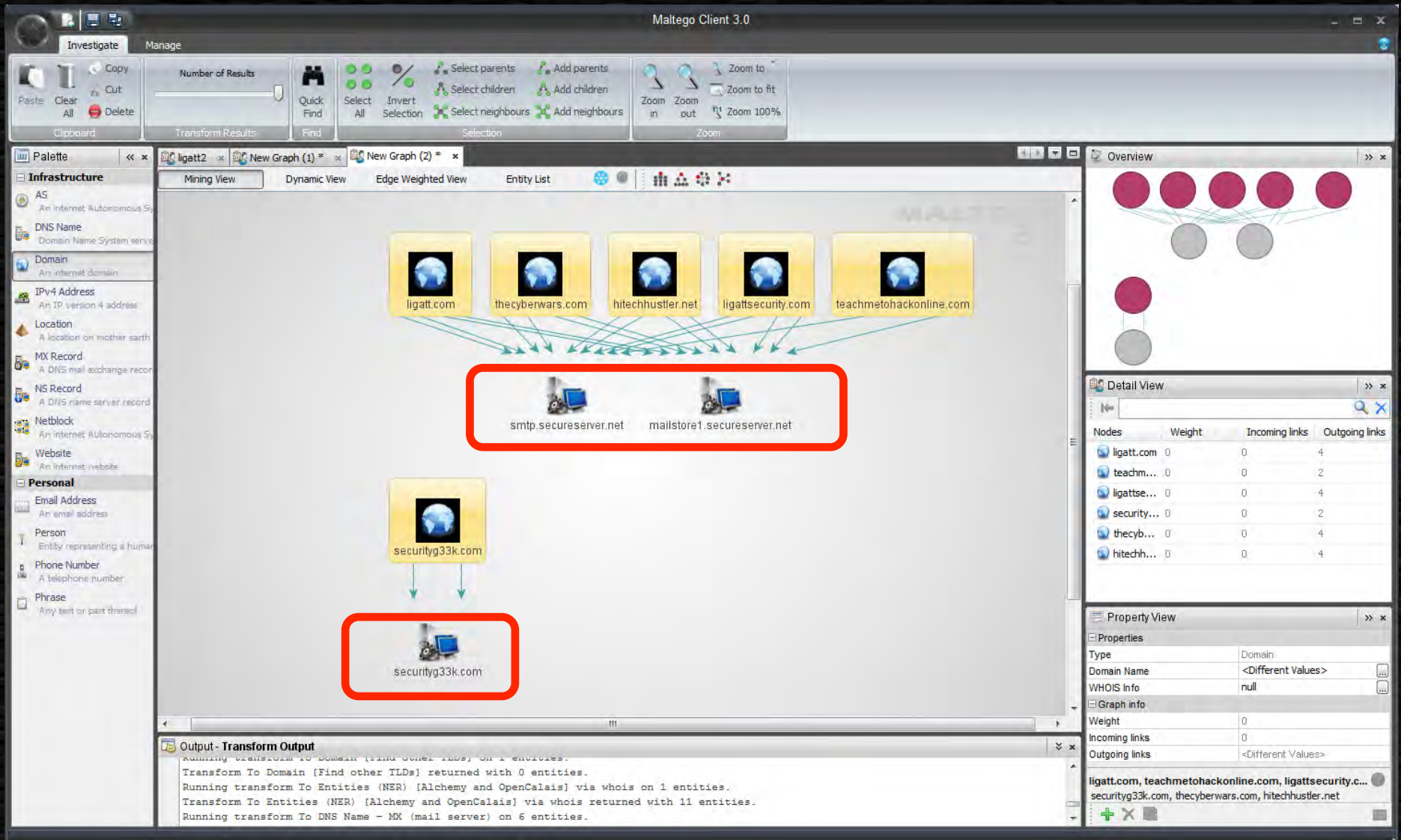
E.G.


Maltego Client 3.0
Investigate
Manage
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
Website
Personal
Email Address
Person
Phone Number
Phrase
ligatt2
New Graph (1) *
New Graph (2)
Mining View
Dynamic View
Edge Weighted View
Entity List
Overview
Detail View
<no selection>
Property View
<No Properties>
Output - Transform Output
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.

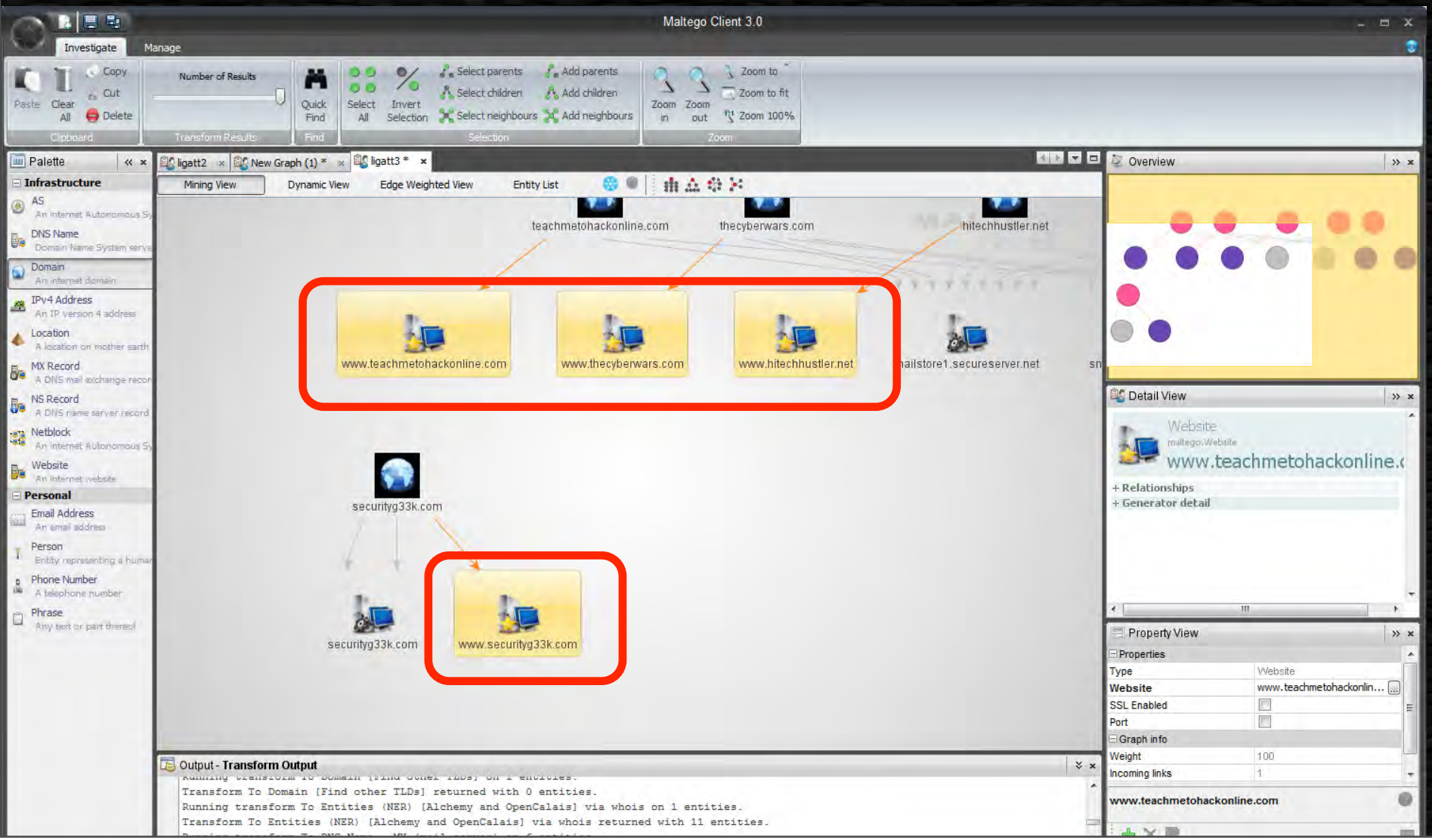
Domains


Maltego Client 3.0
Investigate
Manage
Palette
Infrastructure
AS
DNS Name
Domain
An internet domain
Location
MX Record
NS Record
Netblock
Website
Personal
Email Address
Person
Phone Number
Phrase
ligatt2
New Graph (1) *
New Graph (2) *
Mining View
Dynamic View
Edge Weighted View
Entity List
teachmetohackoonline.com
thecyberwars.com
securityg33k.com
ligattsecurity.com
hitechhustler.net
ligatt.com
Overview
Detail View
Domain
maltego.Domain
ligattsecurity.com
Property View
Properties
Type
Domain
Domain Name
ligattsecurity.com
WHOIS Info
null
Graph info
Weight
Incoming links
Outgoing links
ligattsecurity.com
Output - Transform Output
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


Maltego Client 3.0
Investigate
Manage
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
Website
Personal
Email Address
Person
Phone Number
Phrase
ligatt2
New Graph (1) *
New Graph (2) *
Mining View
Dynamic View
Edge Weighted View
Entity List
ligatt.com
thecyberwars.com
hitechhustler.net
ligattsecurity.com
teachmetohackonline.com
smtp.secureserver.net
mailstore1.secureserver.net
securityg33k.com
securityg33k.com
Overview
Detail View
Nodes
Weight
Incoming links
Outgoing links
Property View
Properties
Type
Domain
Domain Name
<Different Values>
WHOIS Info
null
Graph info
Weight
Incoming links
Outgoing links
<Different Values>
ligatt.com, teachmetohackonline.com, ligattsecurity.c...
securityg33k.com, thecyberwars.com, hitechhustler.net
Output - Transform Output
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…


Maltego Client 3.0
Investigate
Manage
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
Website
Personal
Email Address
Person
Phone Number
Phrase
Mining View
Dynamic View
Edge Weighted View
Entity List
teachmetohackonline.com
thecyberwars.com
hitechhustler.net
www.teachmetohackonline.com
www.thecyberwars.com
www.hitechhustler.net
securityg33k.com
www.securityg33k.com
Overview
Detail View
Property View
Output - Transform Output
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.


twitter

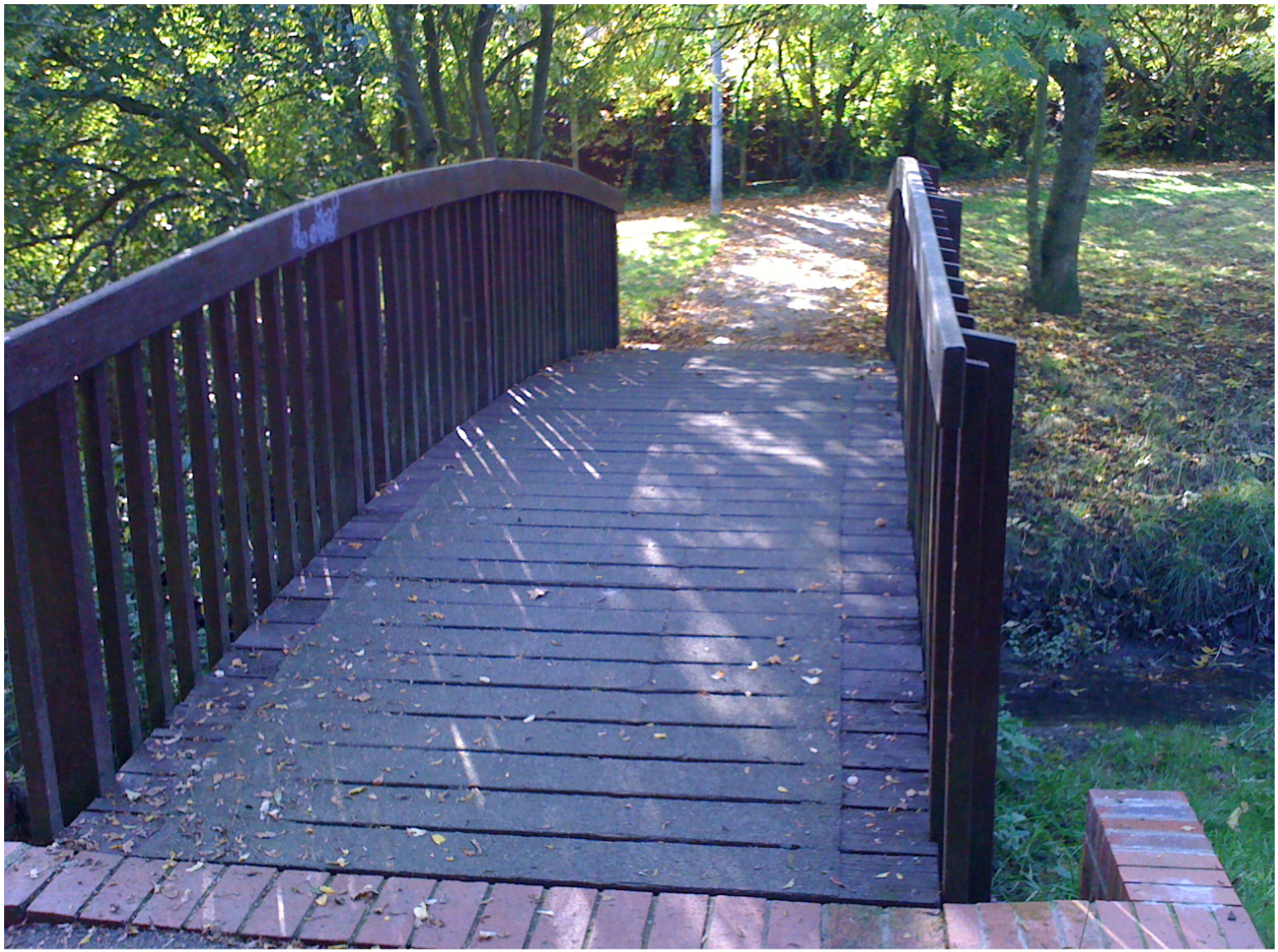
Tony Hawk Twitter Hunt versus Maltego

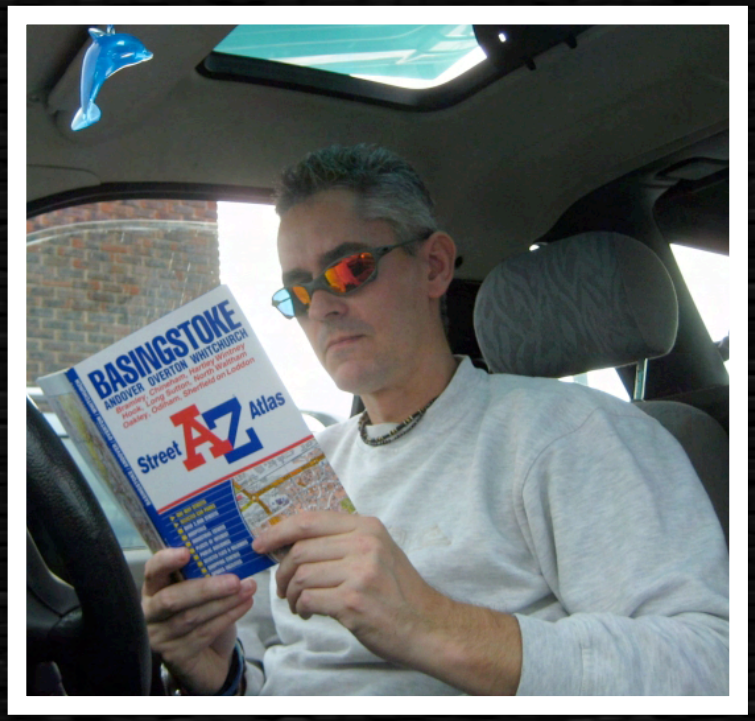



#THTH
#THTH
#THTH
#THTH


#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”

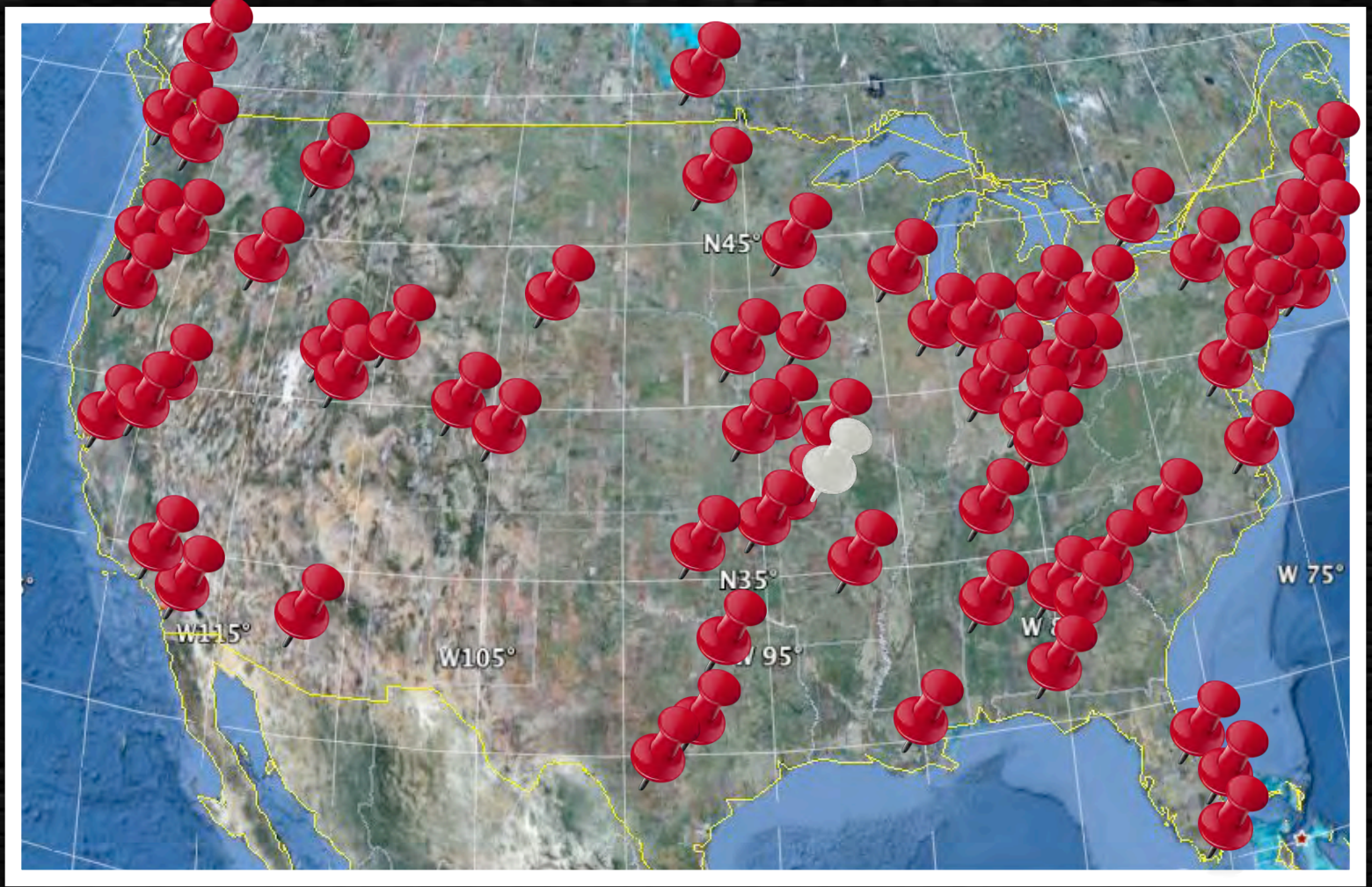


@steven_gill


#THTH
I HACK CHARITIES.ORG
SHRED OR DIE
SHRED OR DIE
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

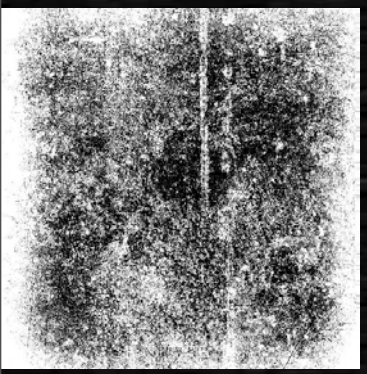
Twitter'll fix it

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

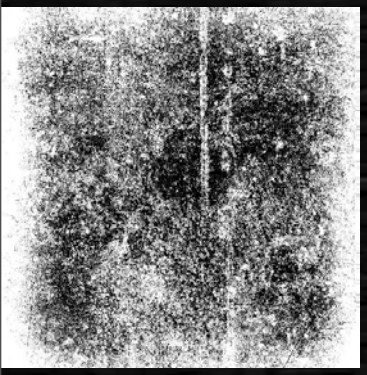
Anyone know of a quick way to pull all tweets @ or from a user over a given period of time (between dates)? Not found anything simple yet



@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

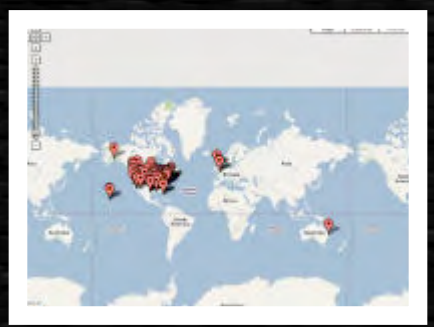
Hypothesis



+



=



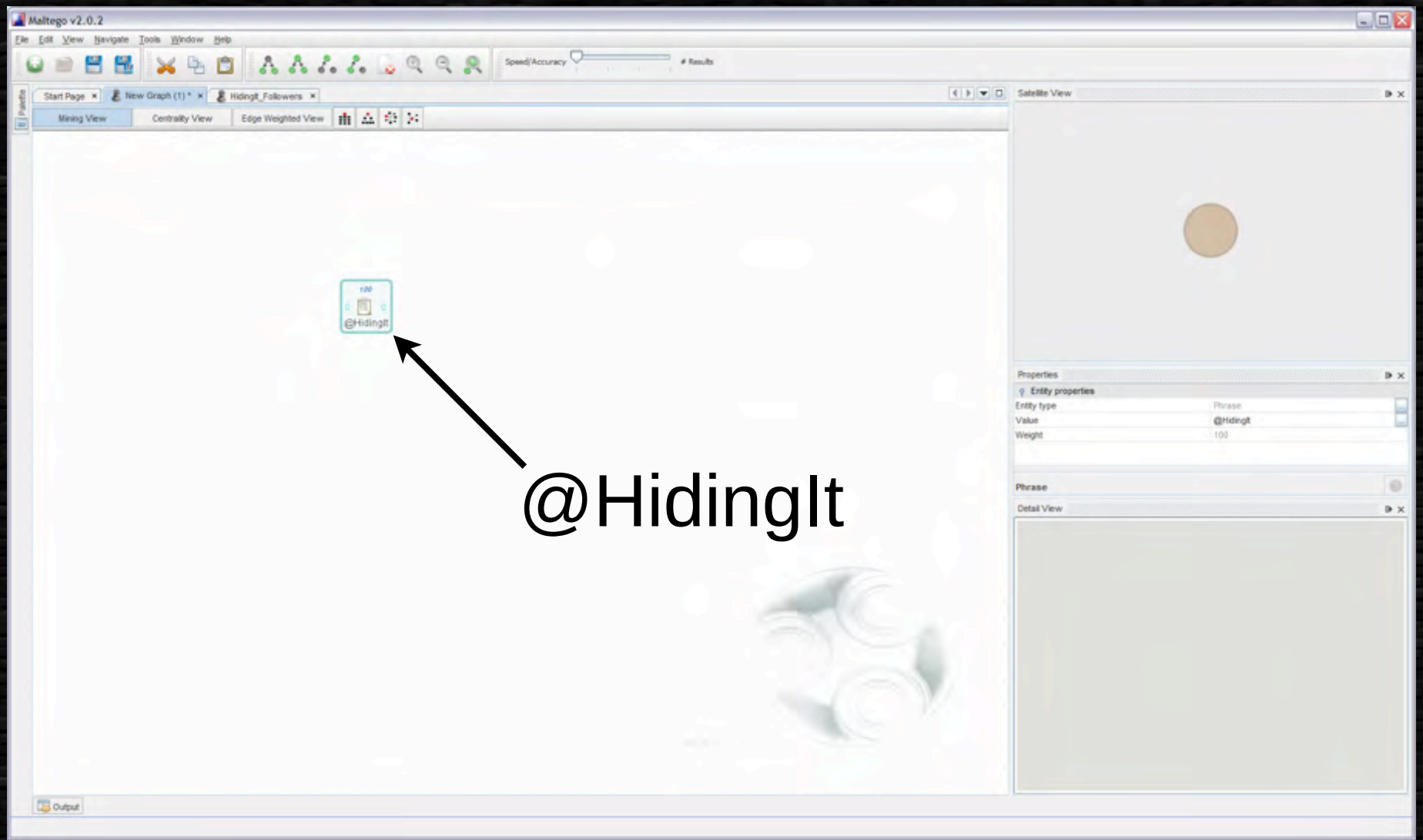
=



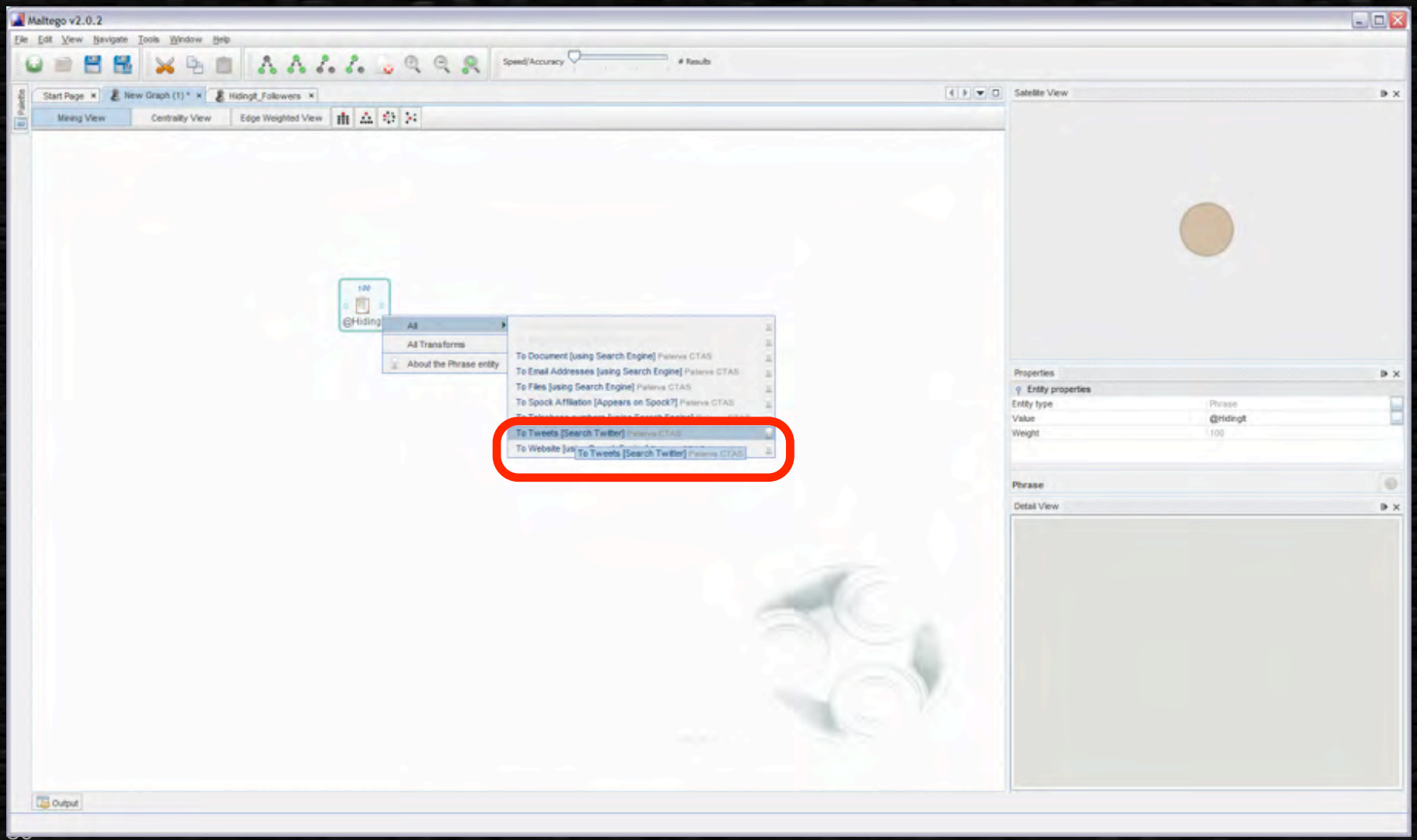
List the Hiders



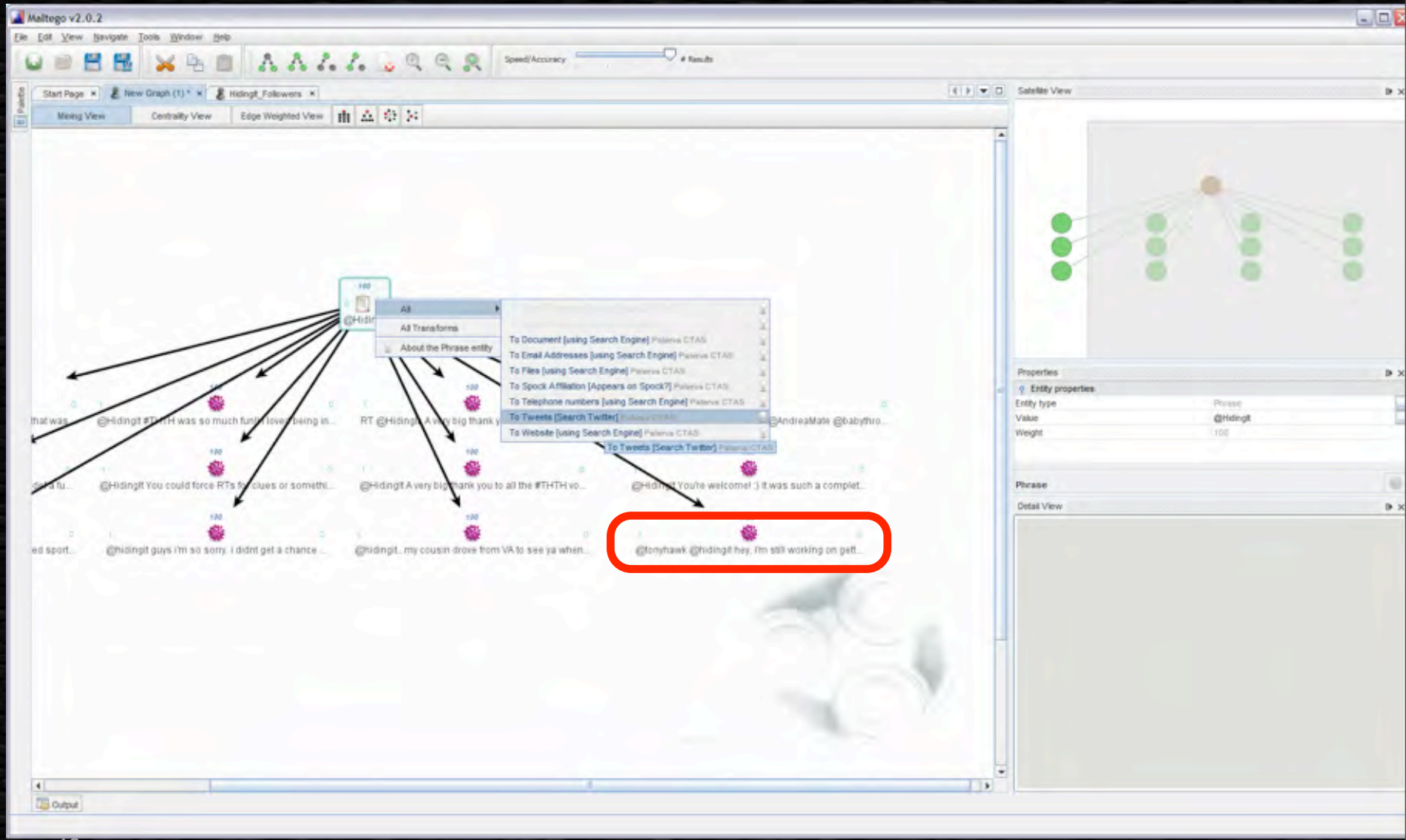
Derive @HidingIt



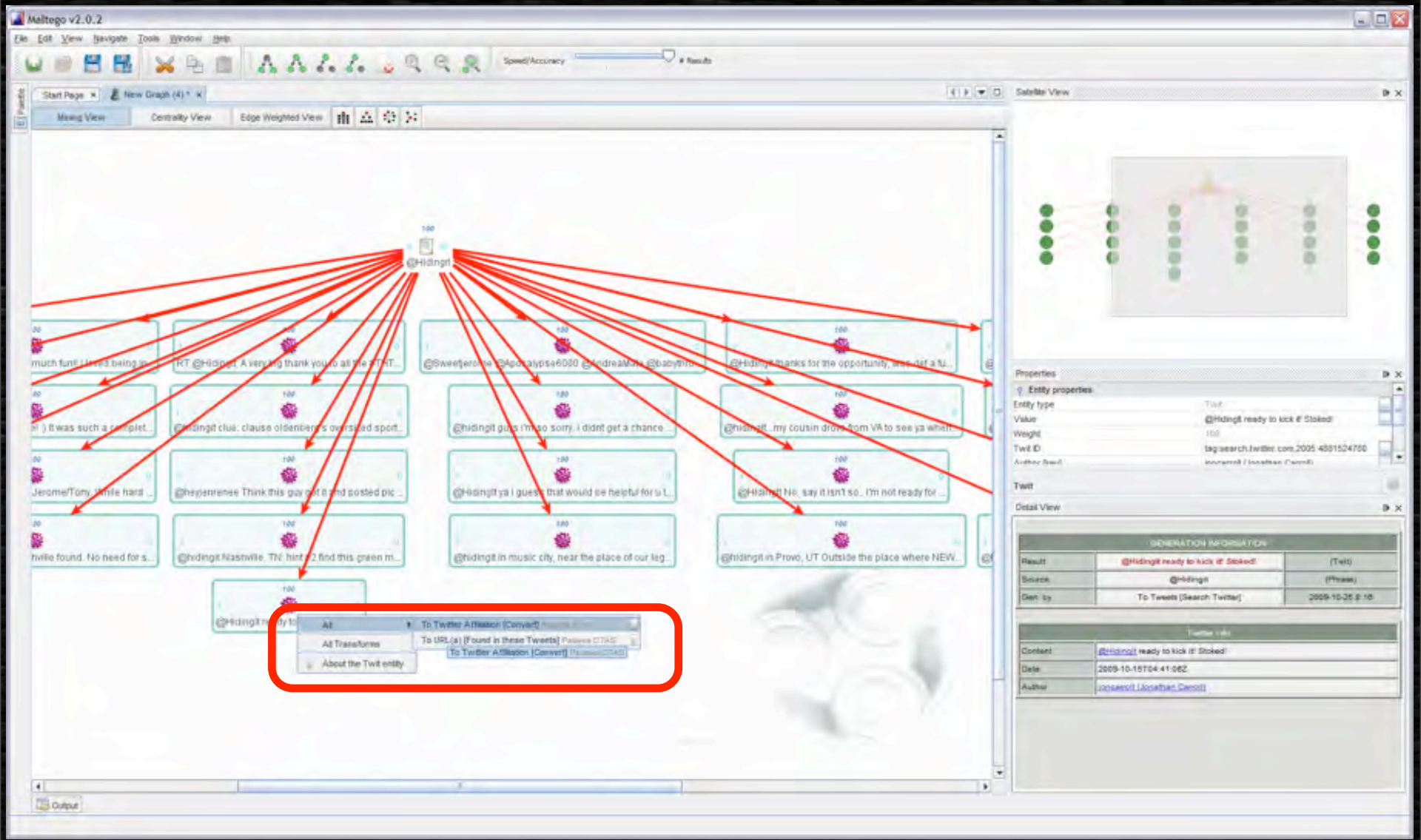
To Tweets [Search Twitter]

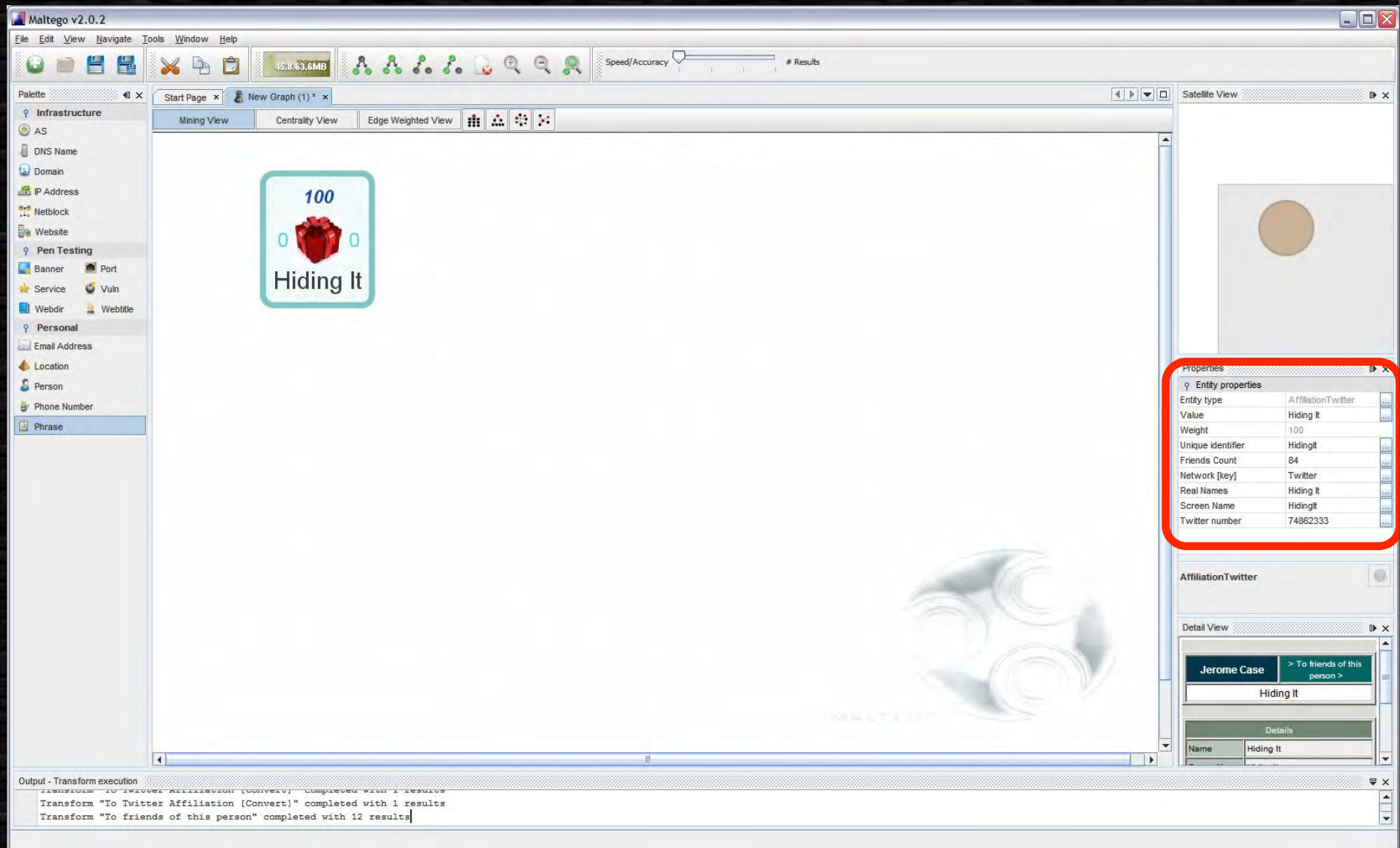


Tweets

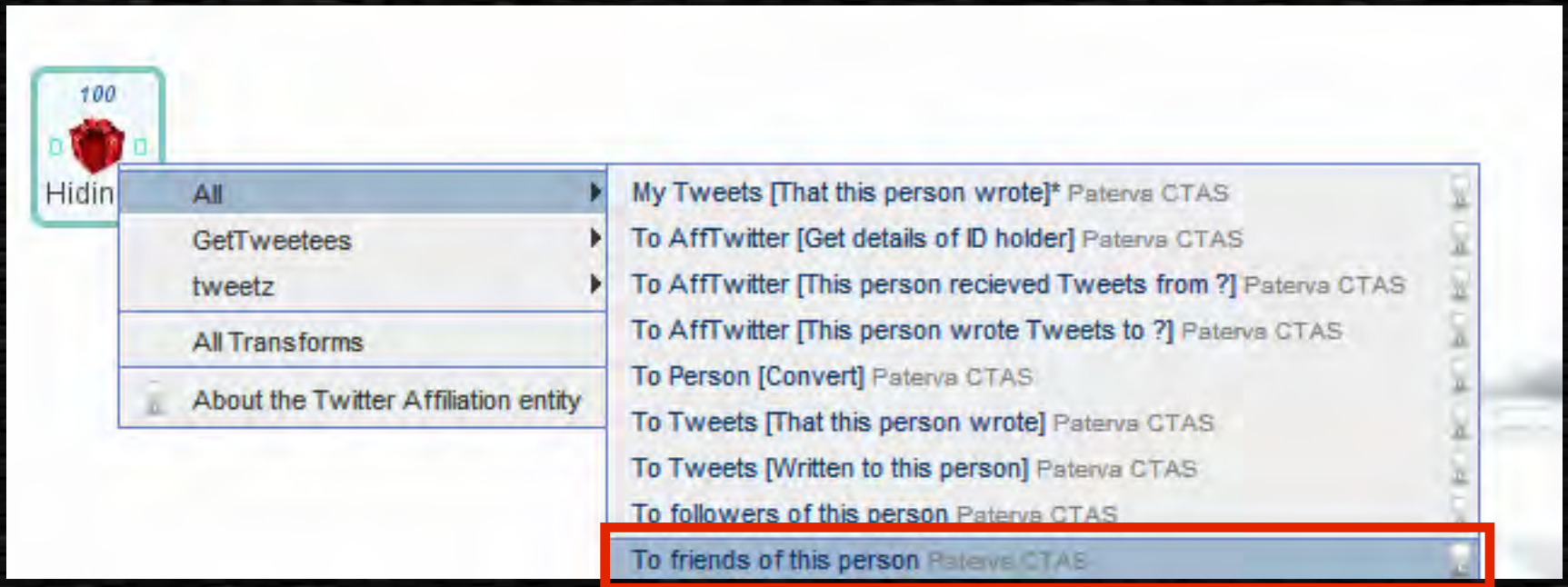

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Start Page
New Graph (1)
Hidingit_Followers
Mixing View
Centrality View
Edge Weighted View
Satellite View
All
All Transforms
About the Phrase entity
To Document [using Search Engine]
To Email Addresses [using Search Engine]
To Files [using Search Engine]
To Spock Affiliation [Appears on Spock?]
To Telephone numbers [using Search Engine]
To Tweets [Search Twitter]
To Website [using Search Engine]
To Tweets [Search Twitter]
@tonyhawk @hidingit hey, I'm still working on getl...
Properties
Entity properties
Entity type
Value
@Hidingit
Weight
Phrase
Detail View
Output

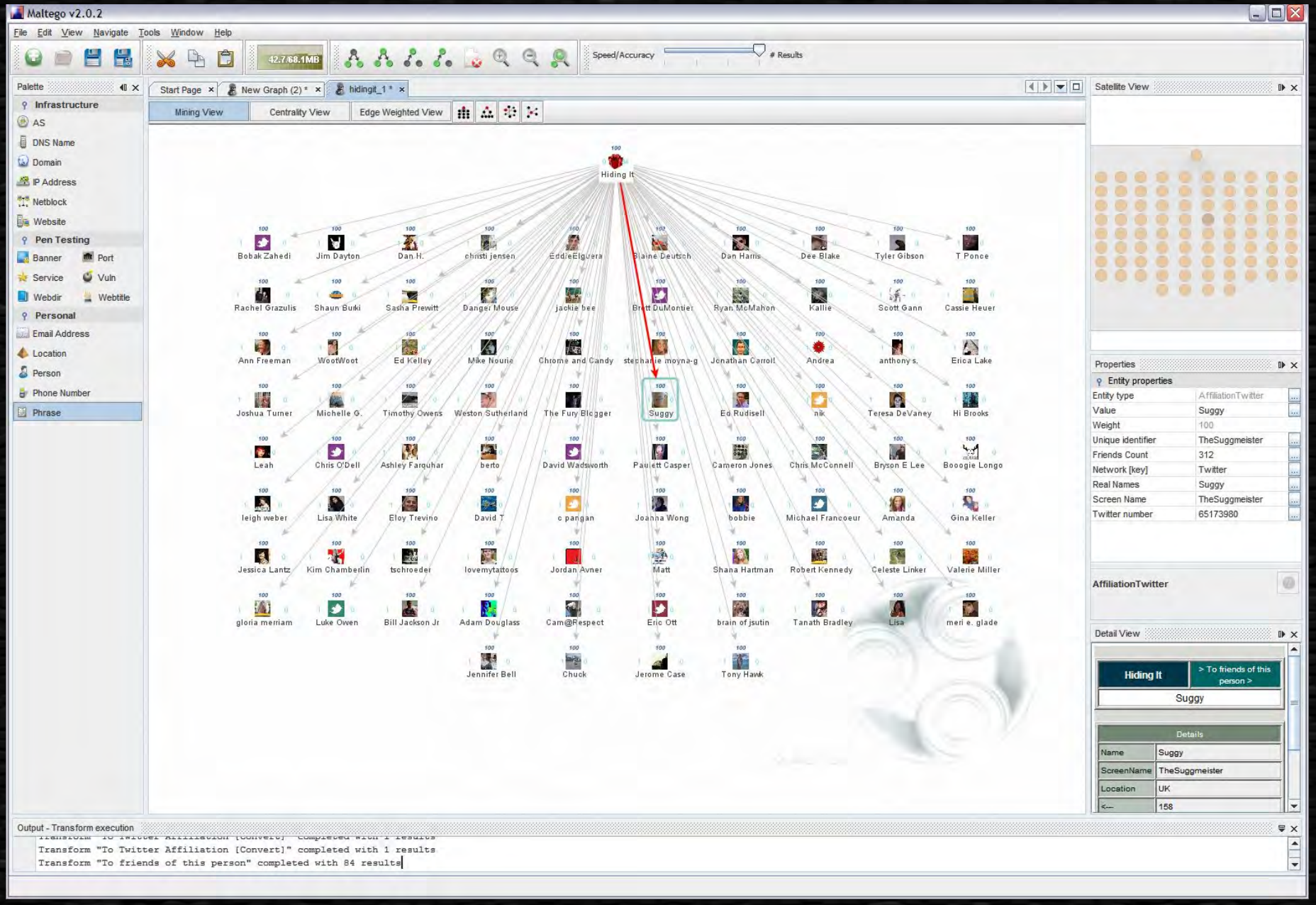
To Twiiter Affiliation [Convert]



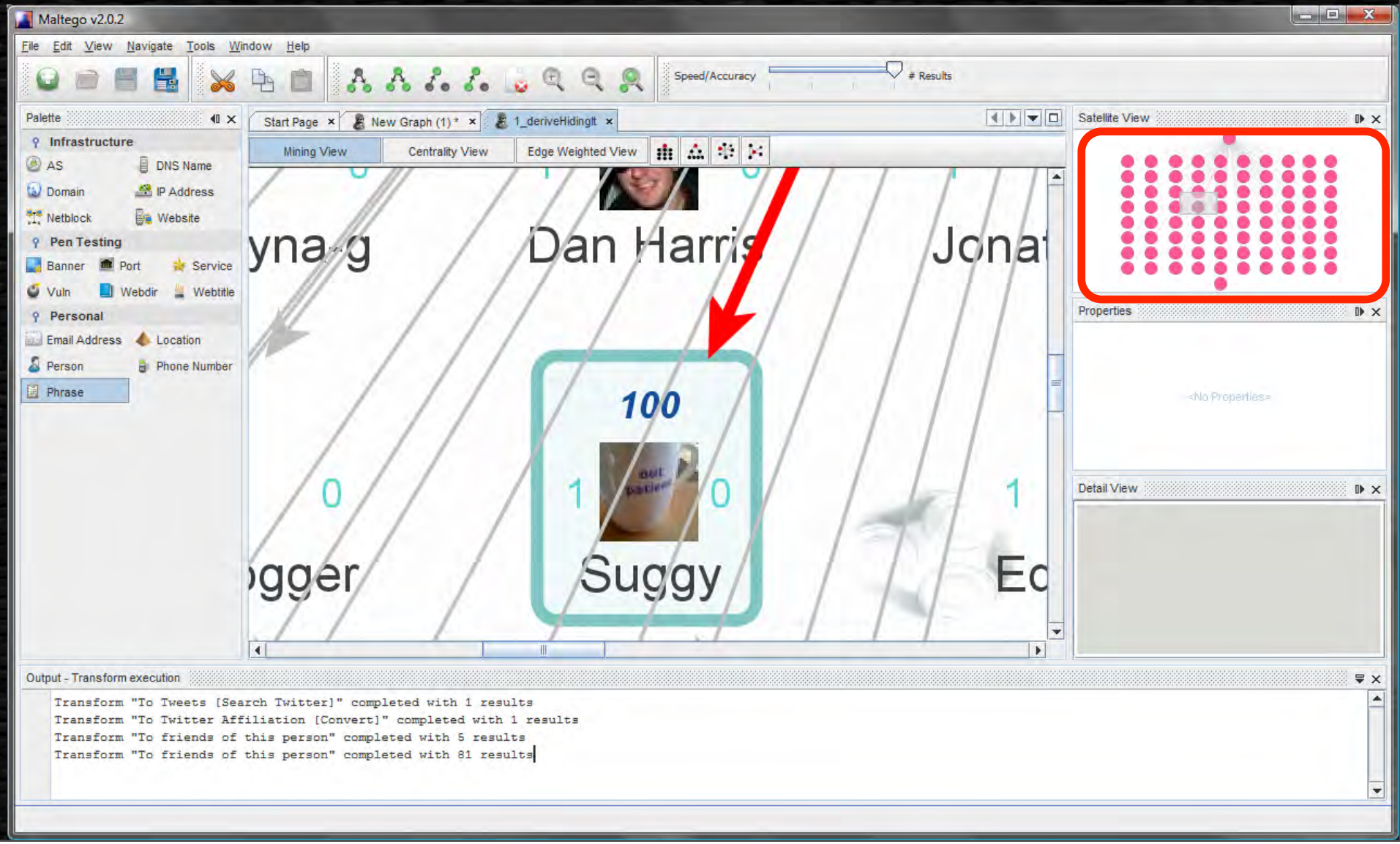

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
Start Page
New Graph (1) *
Mining View
Centrality View
Edge Weighted View
100
0
0
Hiding It
Satellite View
Properties
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
AffiliationTwitter
Detail View
Jerome Case
> To friends of this person >
Hiding It
Details
Name Hiding It
Output - Transform execution
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 12 results

To friends of this person

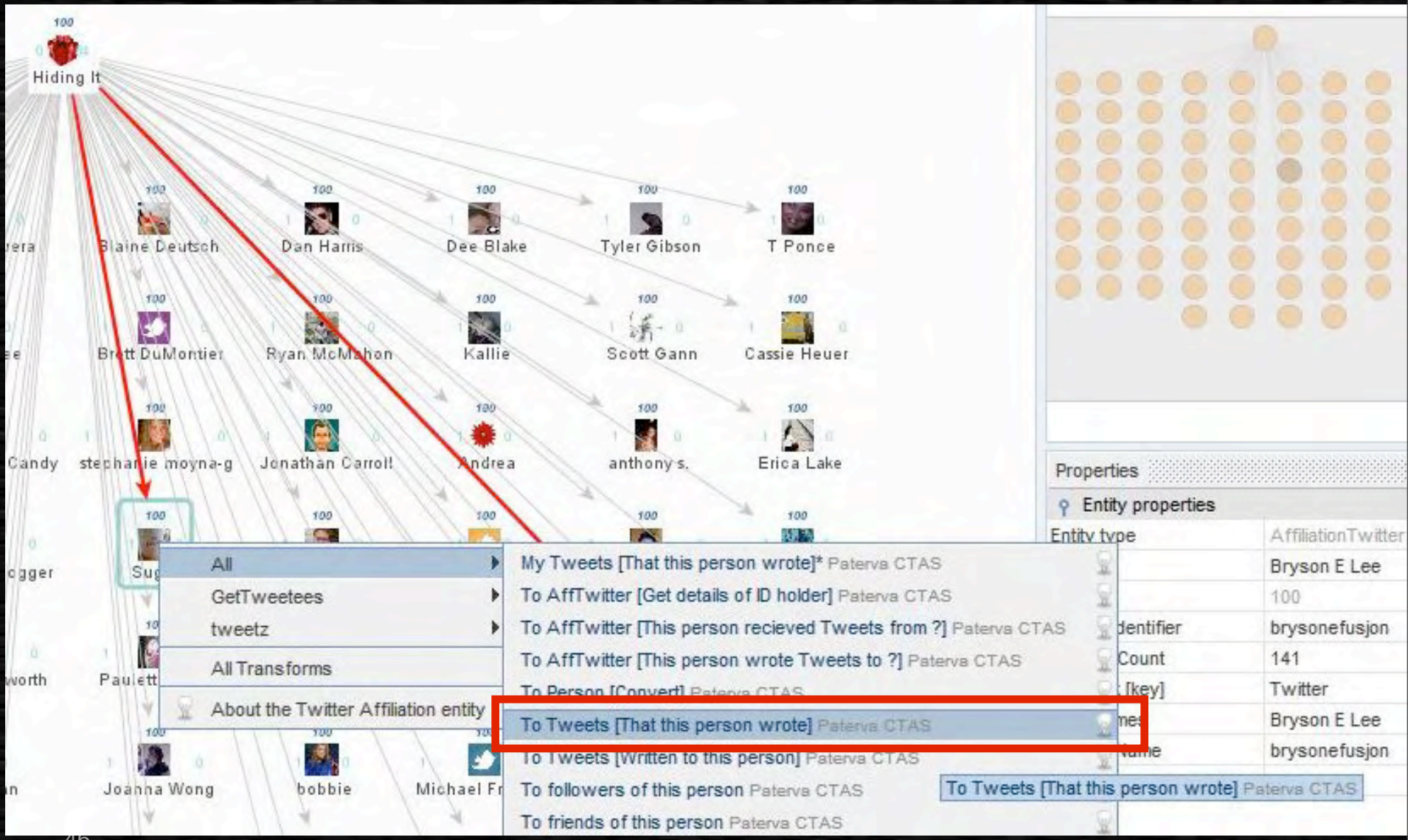


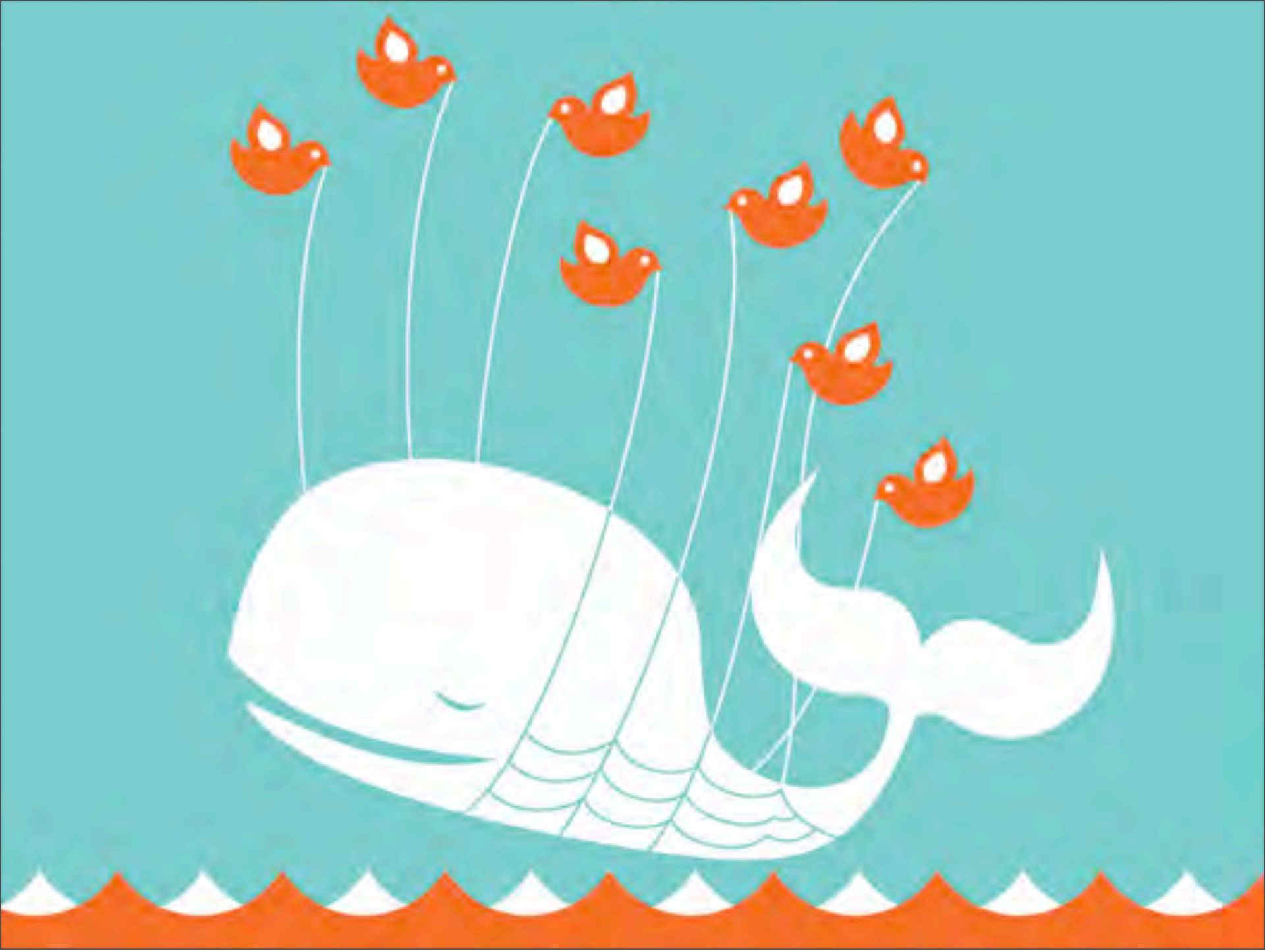

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
Start Page
New Graph (2) *
hidingit_1 *
Mining View
Centrality View
Edge Weighted View
Hiding It
Bobak Zahedi
Jim Dayton
Dan H.
christi jensen
EddieElguera
Blaine Deutsch
Dan Harris
Dee Blake
Tyler Gibson
T Ponce
Rachel Grazulis
Shaun Burki
Sasha Prewitt
Danger Mouse
jackie bee
Brett DuMontier
Ryan McMahon
Kallie
Scott Gann
Cassie Heuer
Ann Freeman
WootWoot
Ed Kelley
Mike Nourie
Chrome and Candy
stephanie moyna-g
Jonathan Carroll
Andrea
anthony s.
Erica Lake
Joshua Turner
Michelle G.
Timothy Owens
Weston Sutherland
The Fury Blogger
Suggy
Ed Rudisell
nik
Teresa DeVaney
Hi Brooks
Leah
Chris O'Dell
Ashley Farquhar
berto
David Wadsworth
Paulett Casper
Cameron Jones
Chris McConnell
Bryson E Lee
Boogie Longo
leigh weber
Lisa White
Eloy Trevino
David T
c pangan
Joanna Wong
bobbie
Michael Francoeur
Amanda
Gina Keller
Jessica Lantz
Kim Chamberlin
tschroeder
lovemytattoos
Jordan Avner
Matt
Shana Hartman
Robert Kennedy
Celeste Linker
Valerie Miller
gloria merriam
Luke Owen
Bill Jackson Jr
Adam Douglass
Cam@Respect
Eric Ott
brain of jsutin
Tanath Bradley
Lisa
meri e. glade
Jennifer Bell
Chuck
Jerome Case
Tony Hawk
Satellite View
Properties
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
Detail View
Hiding It
> To friends of this person >
Suggy
Details
Name Suggy
ScreenName TheSuggmeister
Location UK
<--- 158
Output - Transform execution
Transform "To Twitter Affiliation [Convert]" completed with 1 results
Transform "To friends of this person" completed with 84 results

“Suggy”

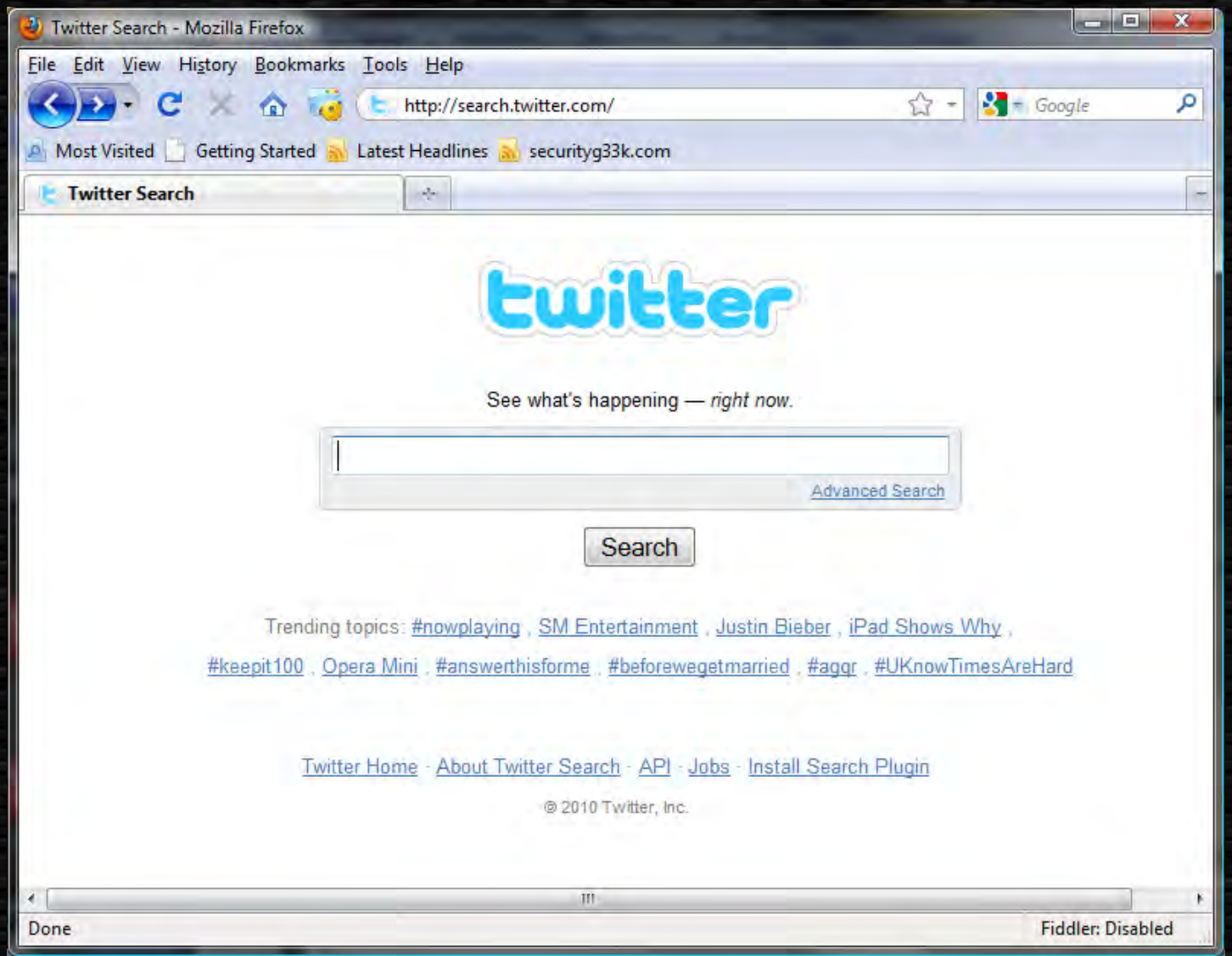

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Speed/Accuracy
Results
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
Start Page
New Graph (1) *
1_deriveHidingIt
Mining View
Centrality View
Edge Weighted View
Dan Harris
100
Suggy
Satellite View
Properties
<No Properties>
Detail View
Output - Transform execution
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

To Tweets [That this person wrote]





Twitter Search Limitations



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

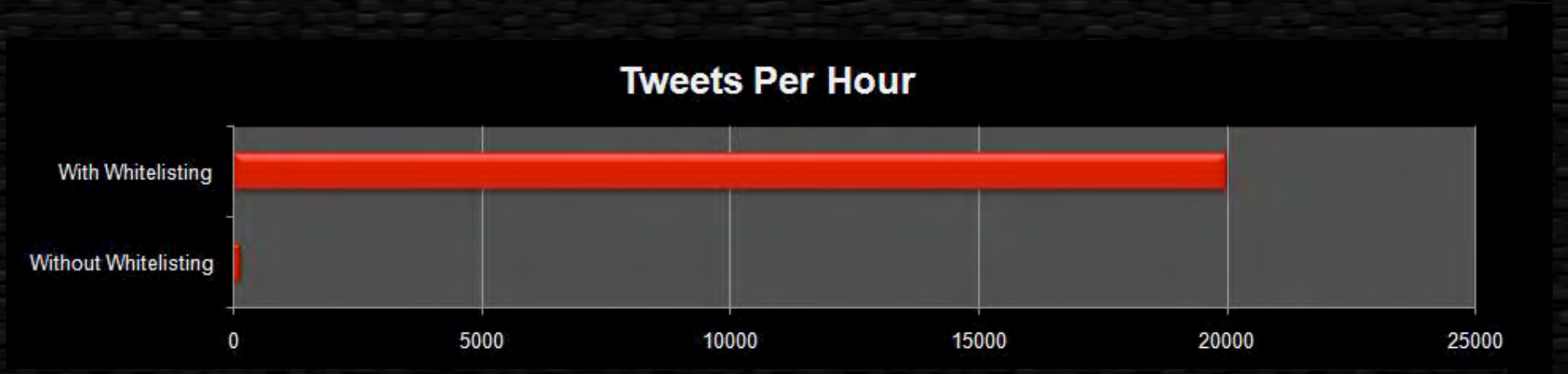
- 200 tweet limit
- Couldn't search by date
- Max history of 3200 tweets
- 150 API calls an hour



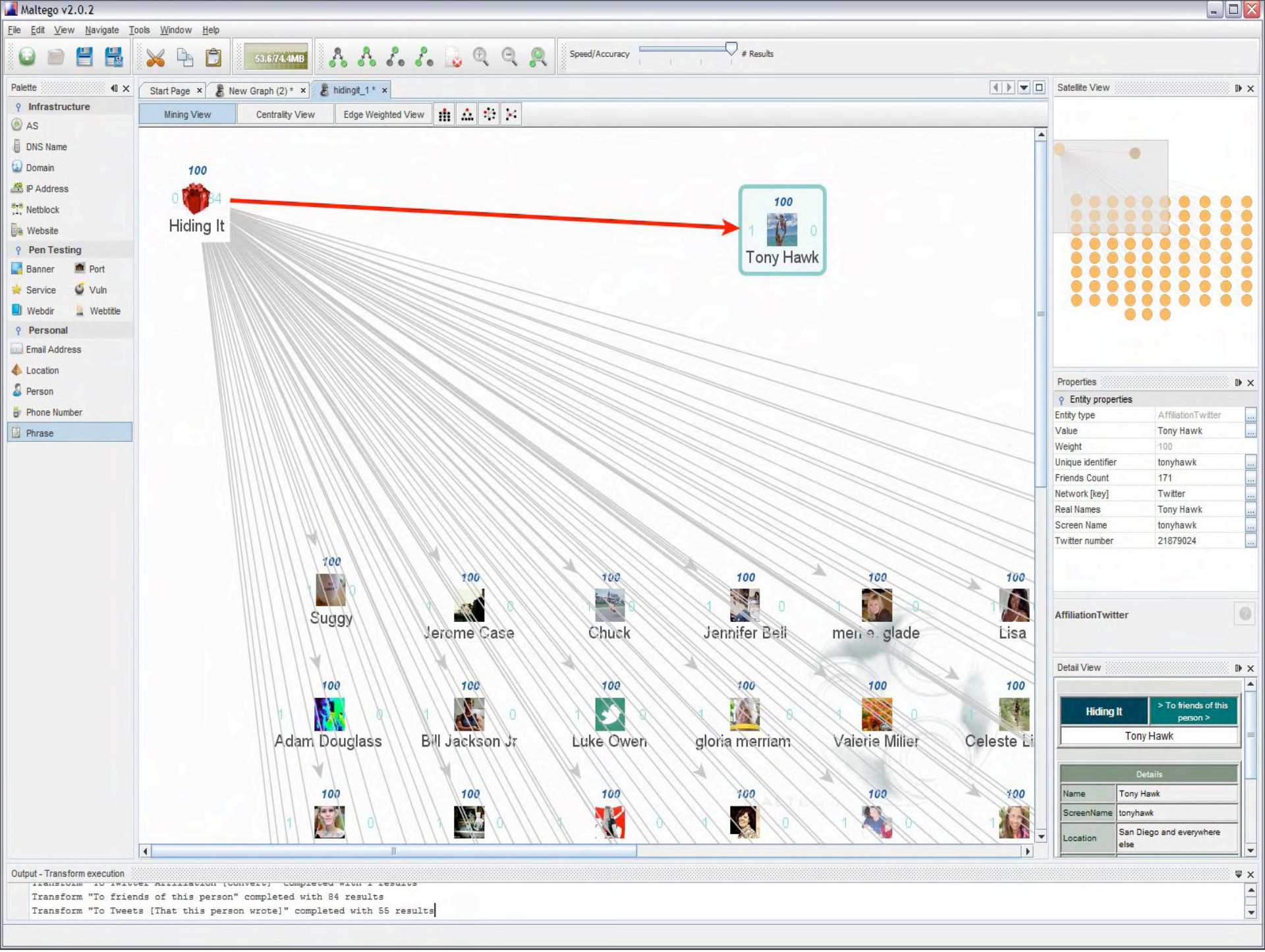
- 100 people * 3 api calls each = 300

Whitelisting

- 150 versus 20,000 per hour

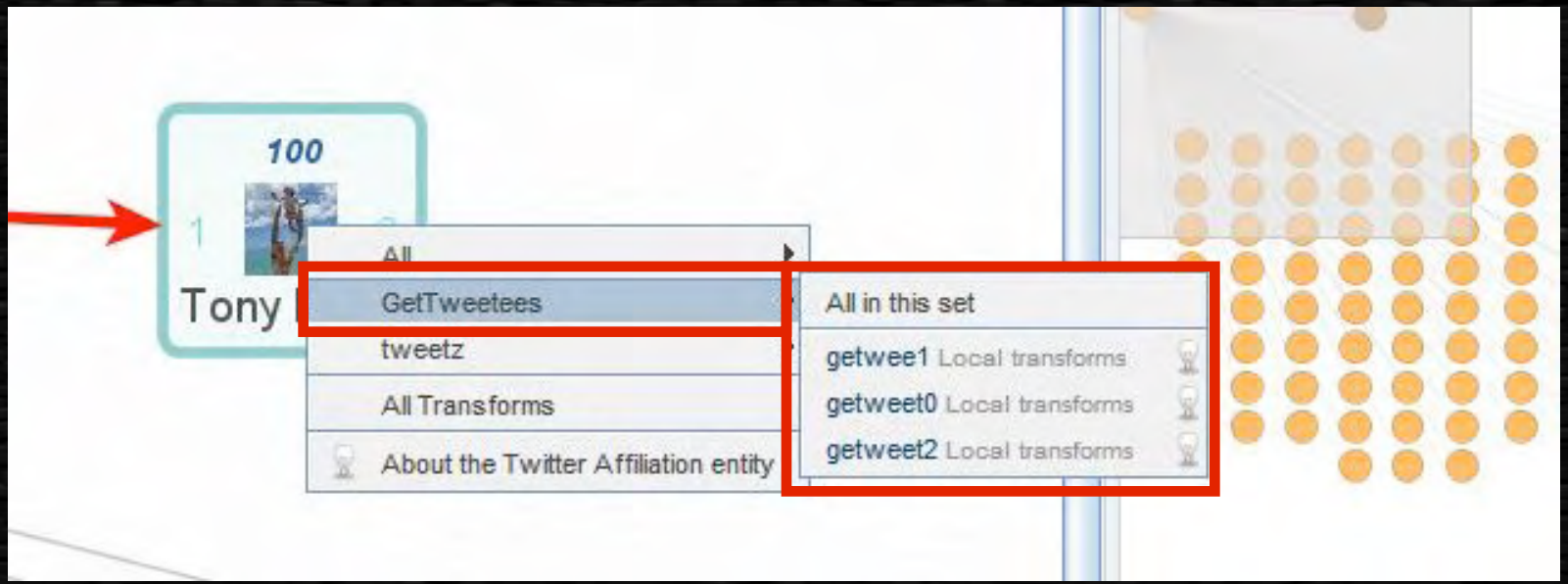


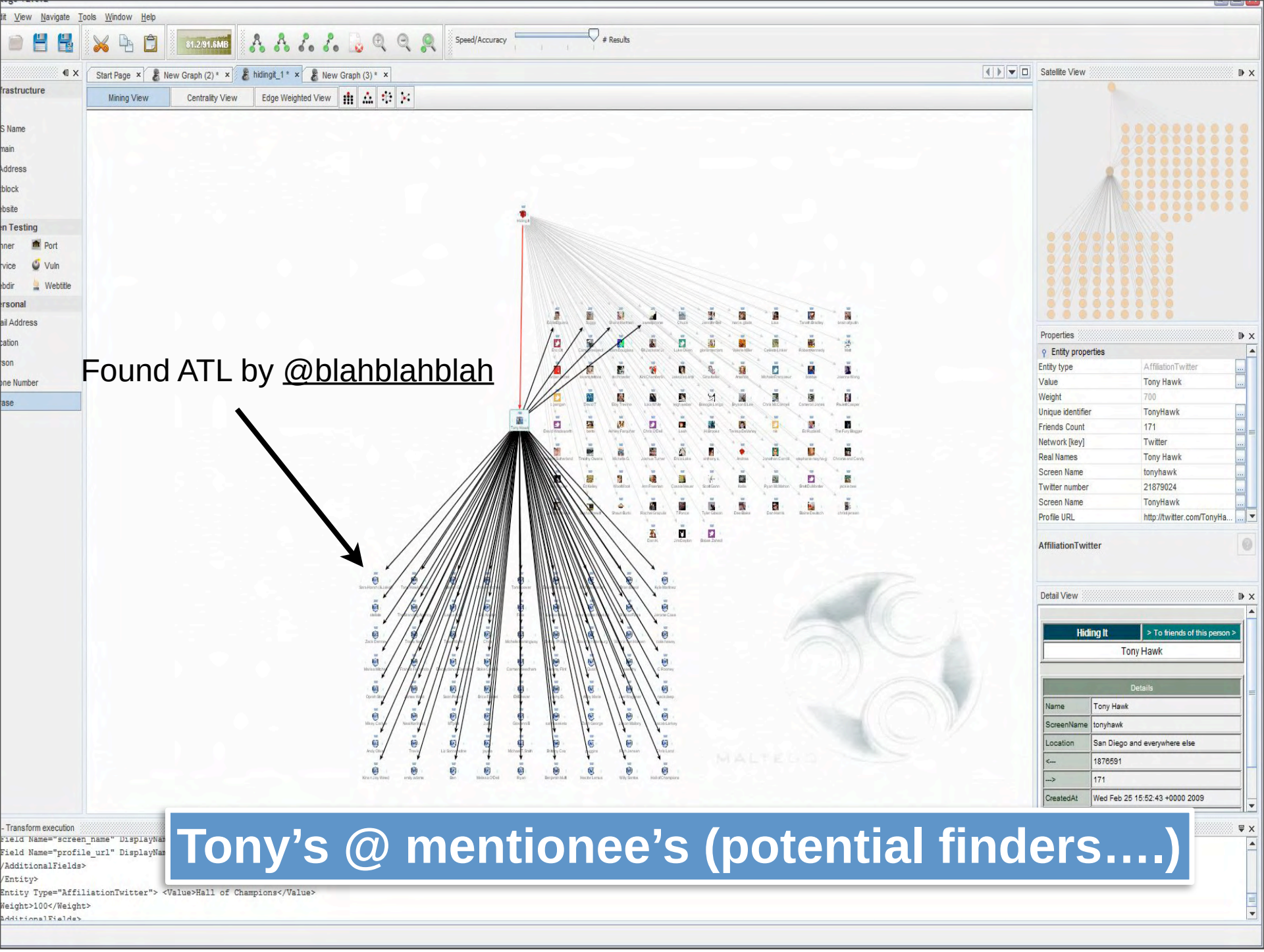
Find the winners

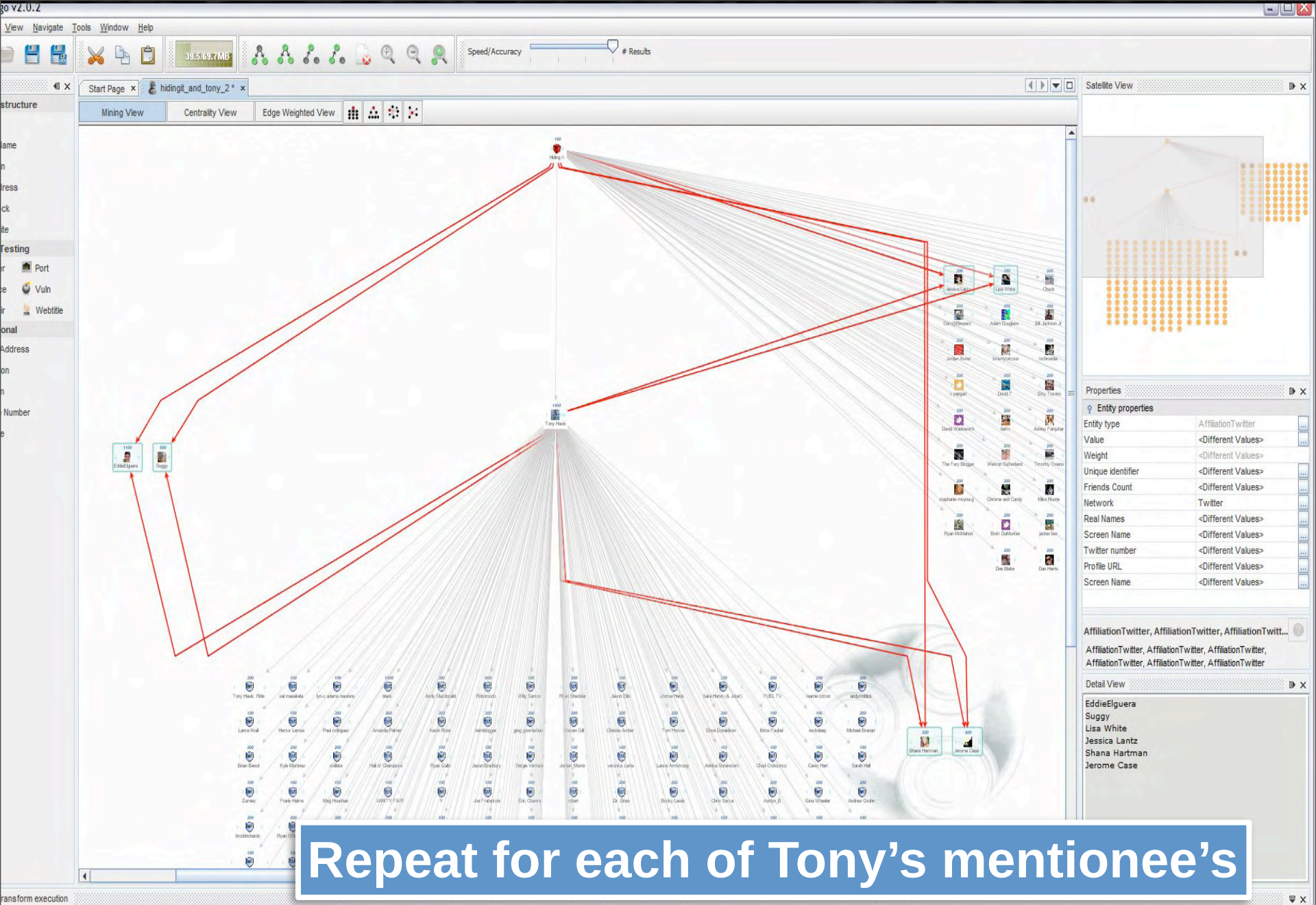


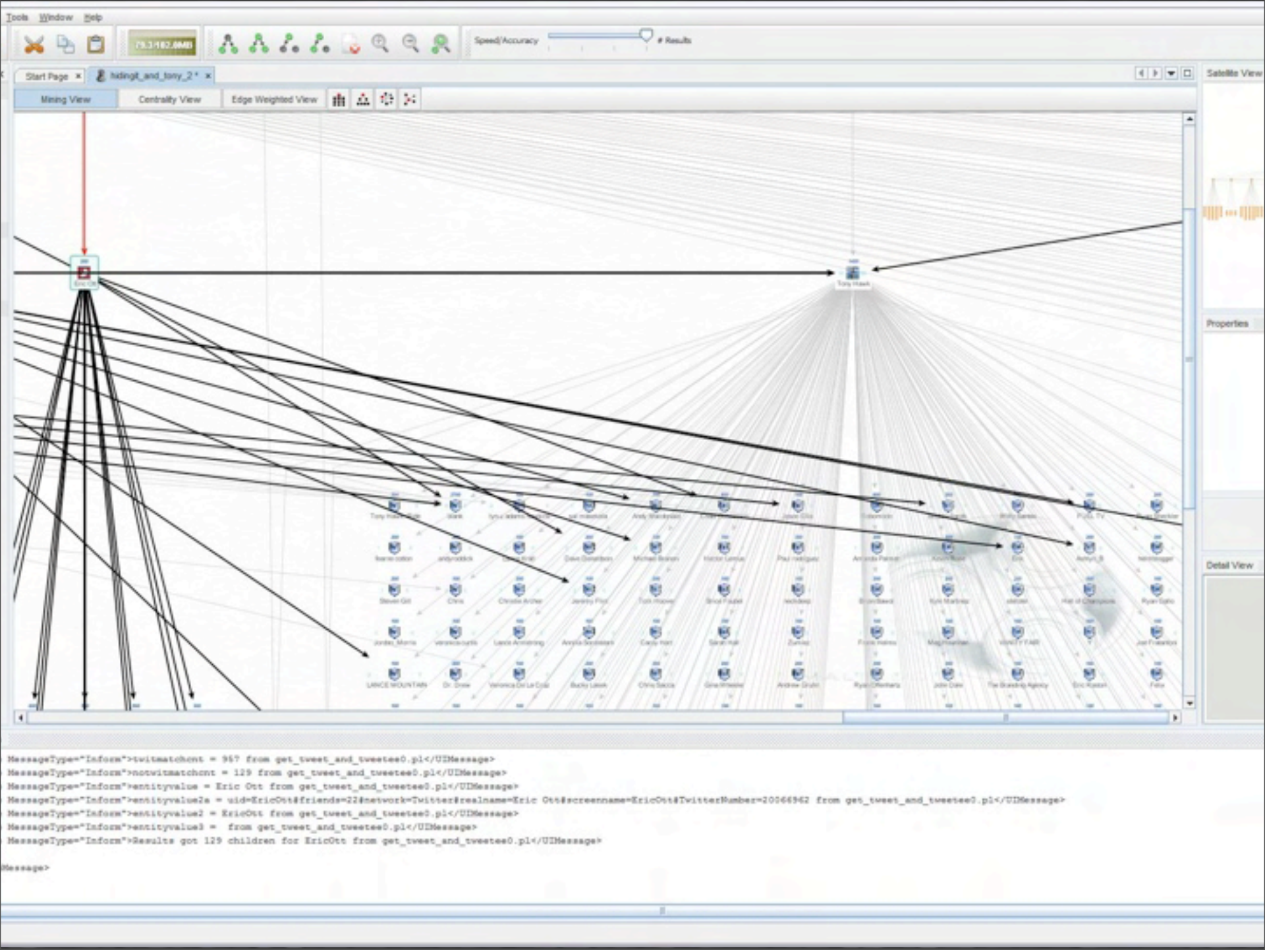
Tuesday, 3 August 2010

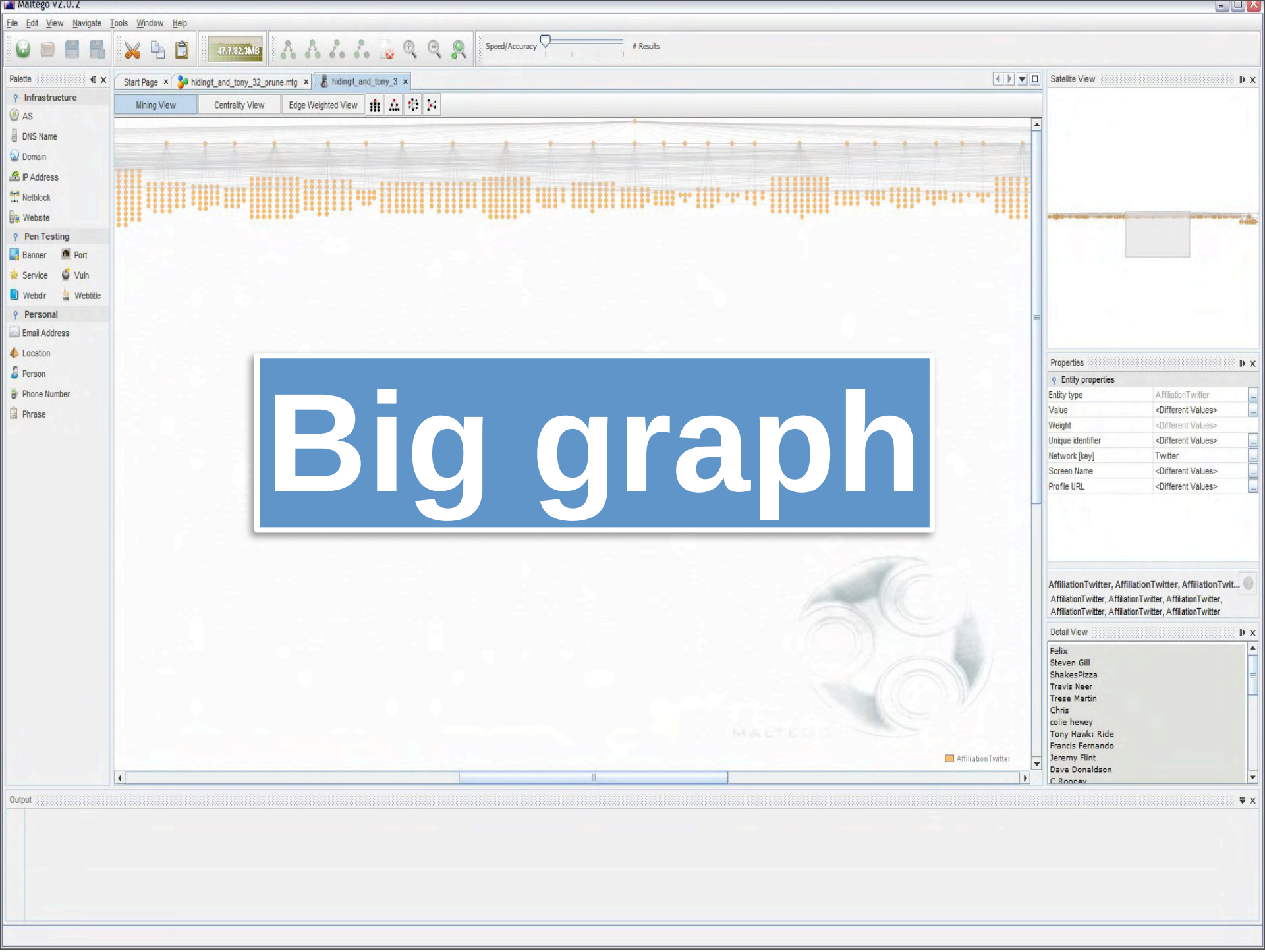
List of all @mentionee's

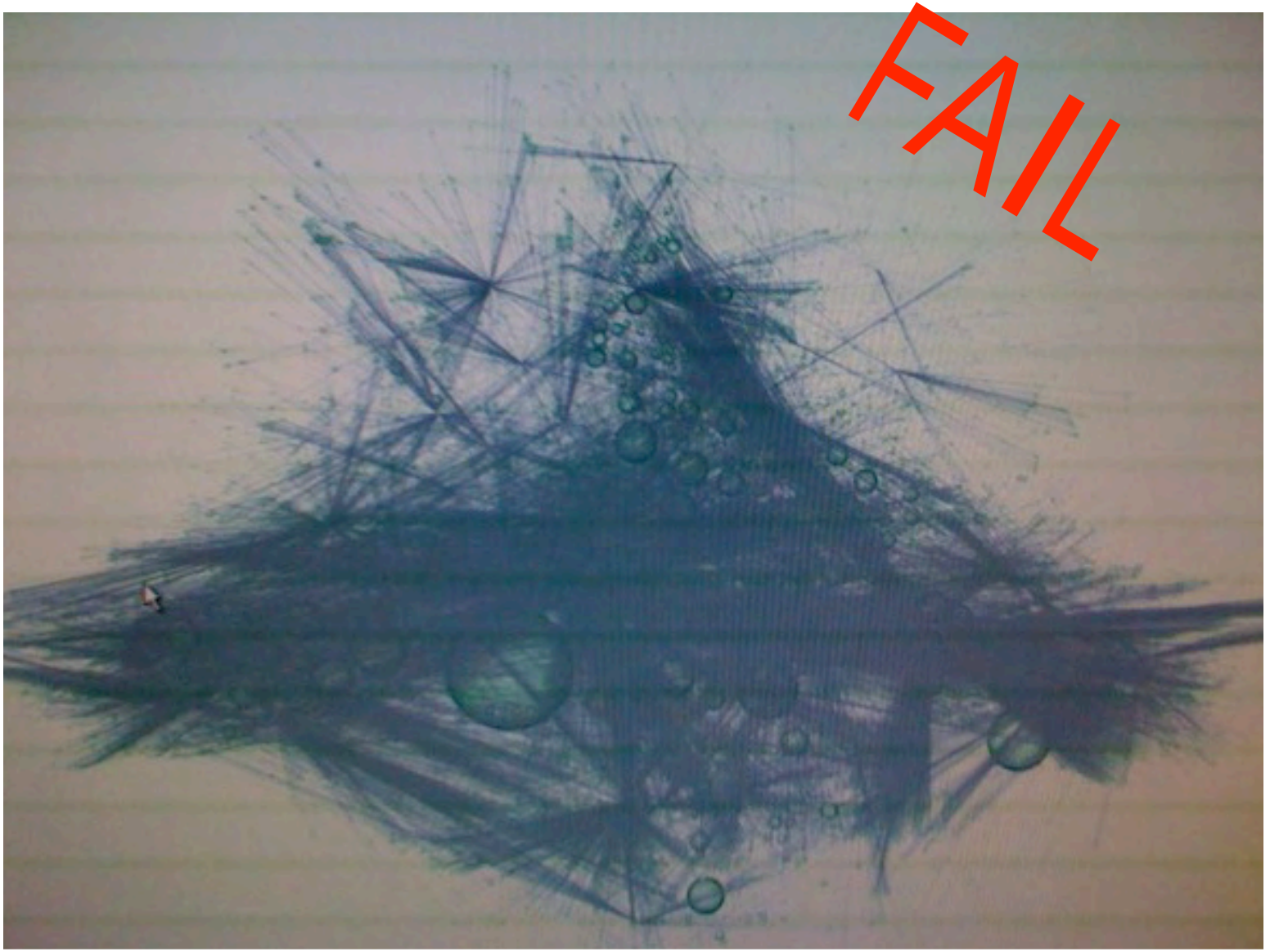



Found ATL by @blahblahblah
Tony's @ mentionee's (potential finders….)

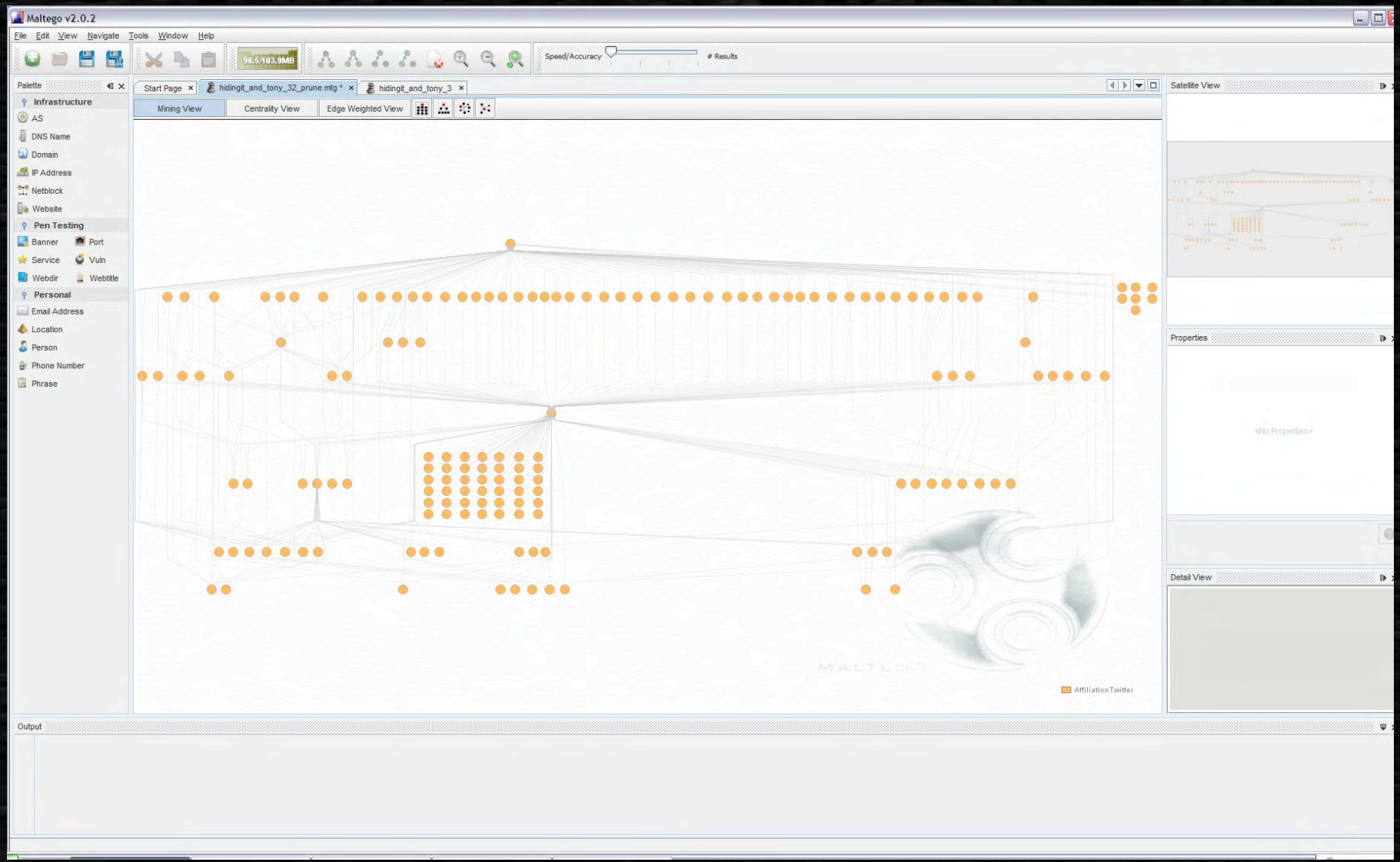

View Navigate Tools Window Help
Speed/Accuracy
Results
Start Page
hidingit_and_tony_2 *
Mining View
Centrality View
Edge Weighted View
Satellite View
Properties
Entity properties
Entity type AffiliationTwitter
Value <Different Values>
Weight <Different Values>
Unique identifier <Different Values>
Friends 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
Detail View
EddieElguera
Suggy
Lisa White
Jessica Lantz
Shana Hartman
Jerome Case
Repeat for each of Tony's mentionee's
Transform execution
<UIMessage MessageType="Inform">twitmatchcnt = 45 from get_tweet_and_tweetee2.pl</UIMessage>


Tools Window Help
Start Page
hdingit_and_tony_2 *
Mining View
Centrality View
Edge Weighted View
Satellite View
Properties
Detail View
MessageType="Inform">twitmatchcnt = 967 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>

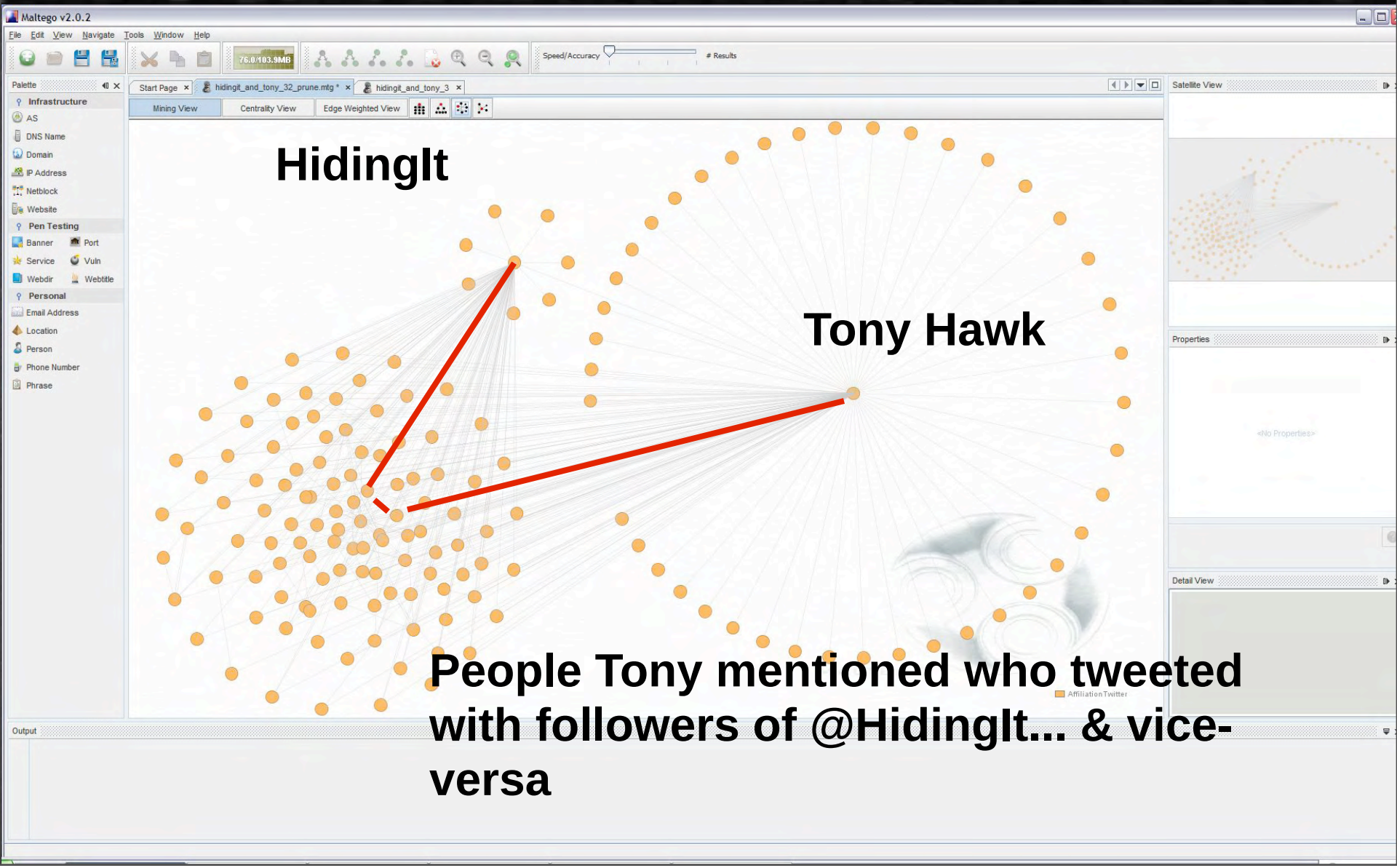

Maltego v2.0.2
File Edit View Navigate Tools Window Help
Palette
Infrastructure
AS
DNS Name
Domain
IP Address
Netblock
Website
Pen Testing
Banner
Port
Service
Vuln
Webdir
Webtitle
Personal
Email Address
Location
Person
Phone Number
Phrase
Start Page
hidingit_and_tony_32_prune.mtg
hidingit_and_tony_3
Mining View
Centrality View
Edge Weighted View
Big graph
AffiliationTwitter
Satellite View
Properties
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
Detail View
Felix
Steven Gill
ShakesPizza
Travis Neer
Trese Martin
Chris
colie hewey
Tony Hawk: Ride
Francis Fernando
Jeremy Flint
Dave Donaldson
C Rooney
Output


FAIL

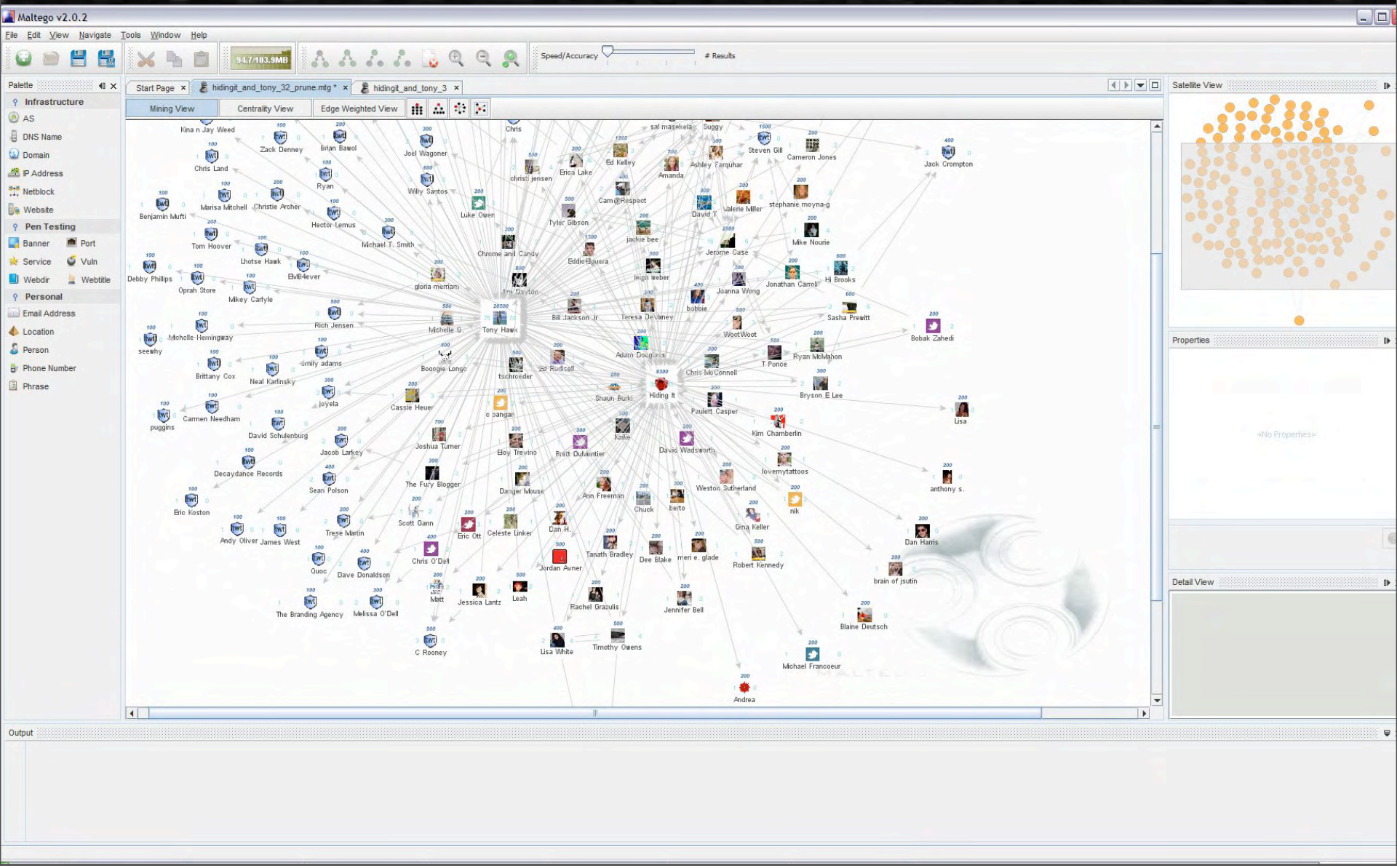
A bit less messy



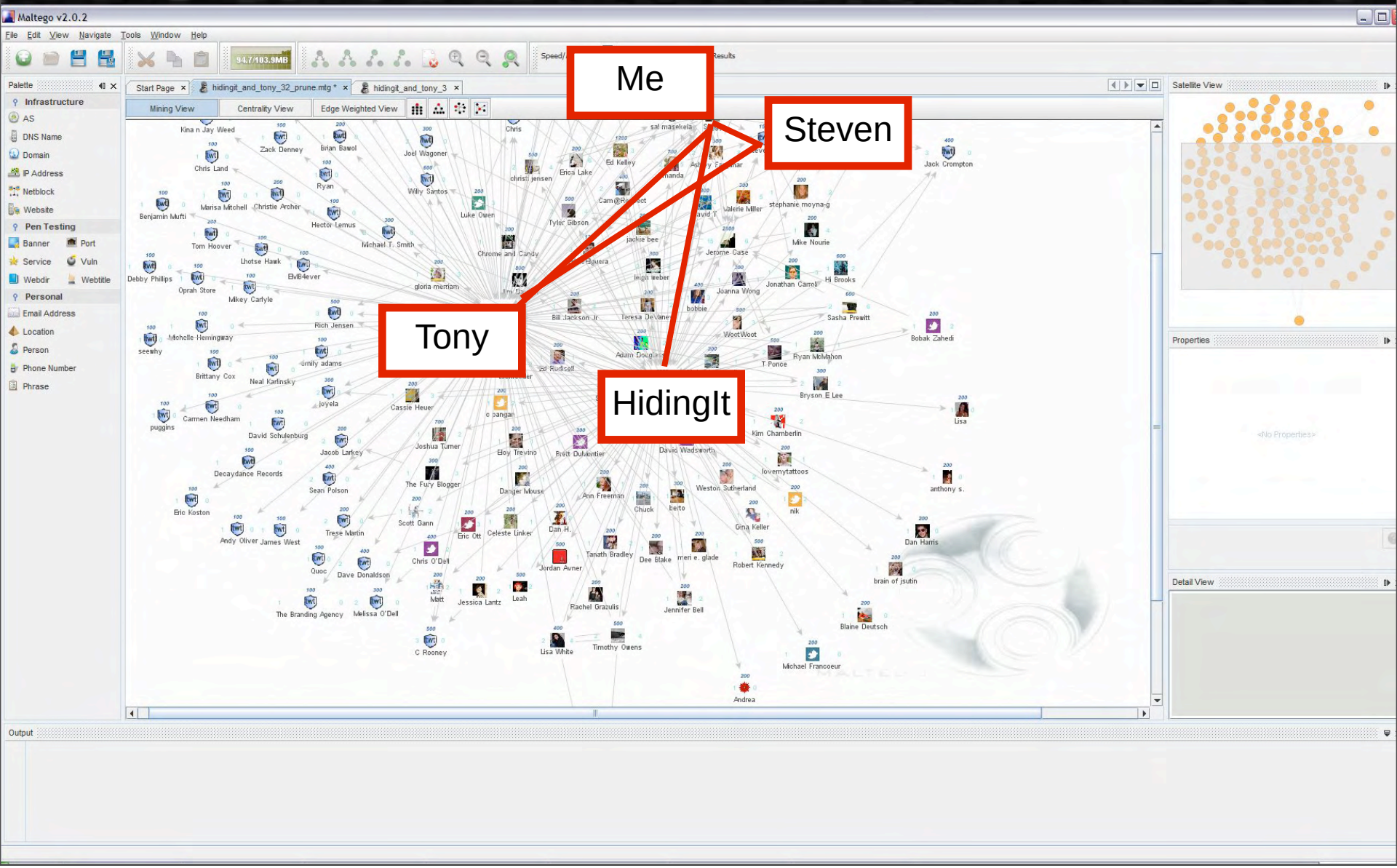
Centrality layout



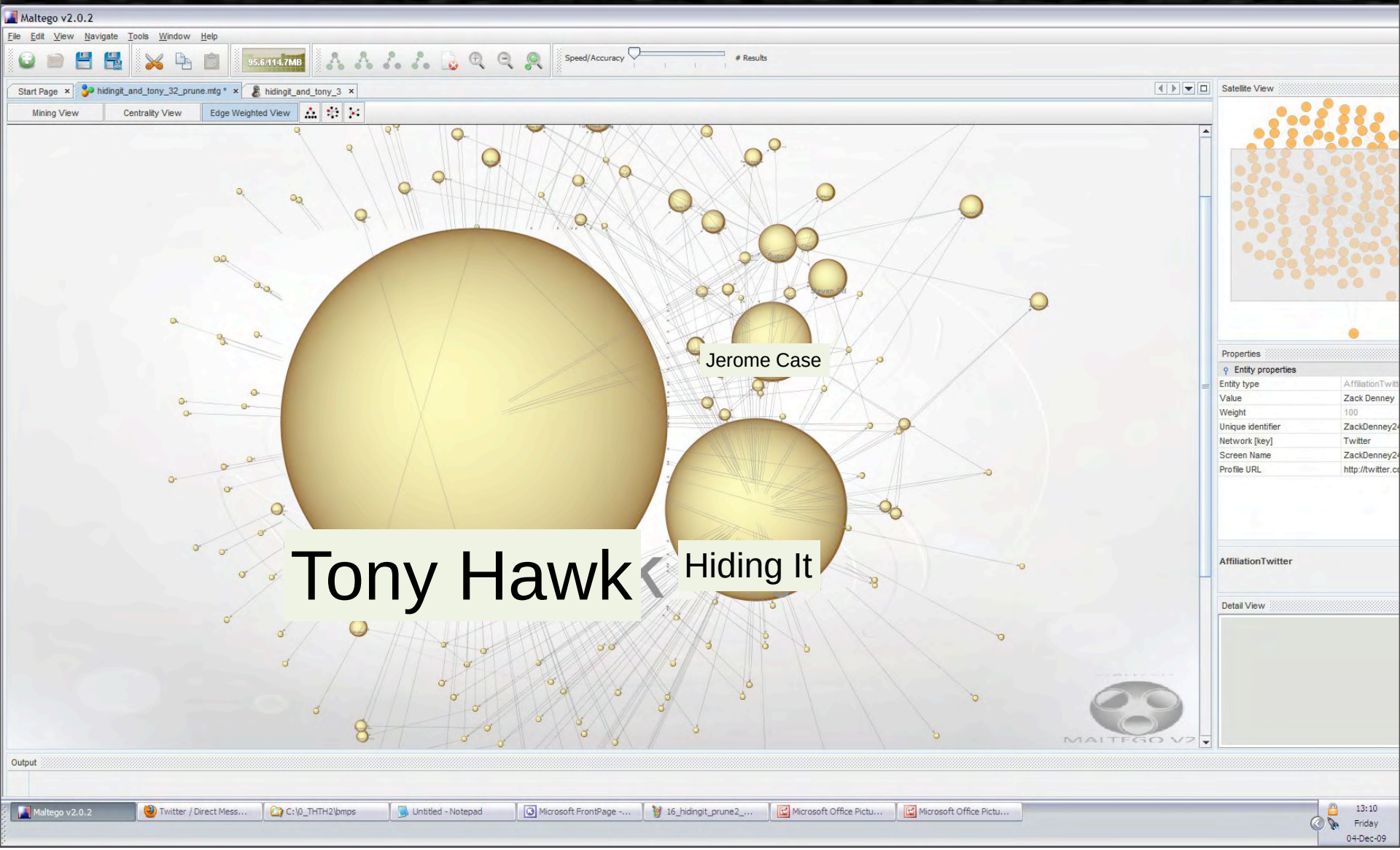
Organic


Maltego v2.0.2
File Edit View Navigate Tools Window Help
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
Detail View
Output
Tony Hawk
Hiding It
Michelle G.
Rich Jensen
Michelle Hemingway
Brittany Cox
Neal Karlinsky
Carmen Needham
David Schulenburg
Jacob Larkey
Sean Polson
Eric Koston
Andy Oliver
James West
Trese Martin
Quoc
Dave Donaldson
The Branding Agency
Melissa O'Dell
C Rooney
Chris O'Dell
Matt
Jessica Lantz
Leah
Lisa White
Timothy Owens
Rachel Grazulis
Jennifer Bell
Jordan Avner
Tanath Bradley
Dee Blake
Robert Kennedy
Gina Keller
Weston Sutherland
Ann Freeman
Danger Mouse
Joshua Turner
The Fury Blogger
Scott Gann
Eric Ott
Celeste Linker
Dan H.
Eloy Trevino
Preit Dulkontier
Kallie
David Wadsworth
Paulett Casper
Kim Chamberlin
Shaun Burke
Adam Douglass
Chris McConnell
T Ponce
Ryan McMahon
Bryson E Lee
Lisa
Bobak Zahedi
Sasha Prewitt
WootWoot
Jack Crompton
Cameron Jones
Steven Gill
Ashley Farquhar
Amanda
Ed Kelley
Erica Lake
christi jensen
Willy Santos
Joel Wagoner
Brian Bawol
Zack Denney
Kina n Jay Weed
Chris Land
Ryan
Hector Lemus
Michael T. Smith
Luke Owen
Tyler Gibson
Cam@Respect
David T
Valerie Miller
stephanie moyna-g
Mike Nourie
Jerome Case
jackie bee
Eddie Elguera
Chrome and Candy
Tom Hoover
Lhotse Hawk
Christie Archer
Marisa Mitchell
Benjamin Mufti
Debby Phillips
Oprah Store
Mikey Carlyle
ElvB4ever
gloria merriam
Jonathan Carroll
Hi Brooks
Joanna Wong
bobbie
Teresa DeVaney
Bill Jackson Jr
Adam Douglass
Ed Rudisell
tschroeder
Boogie Longo
Cassie Heuer
c pangan
Shaun Burke
Chris McConnell
Paulett Casper
Kim Chamberlin
Lisa
Bryson E Lee
Ryan McMahon
T Ponce
Sasha Prewitt
WootWoot
Bobak Zahedi

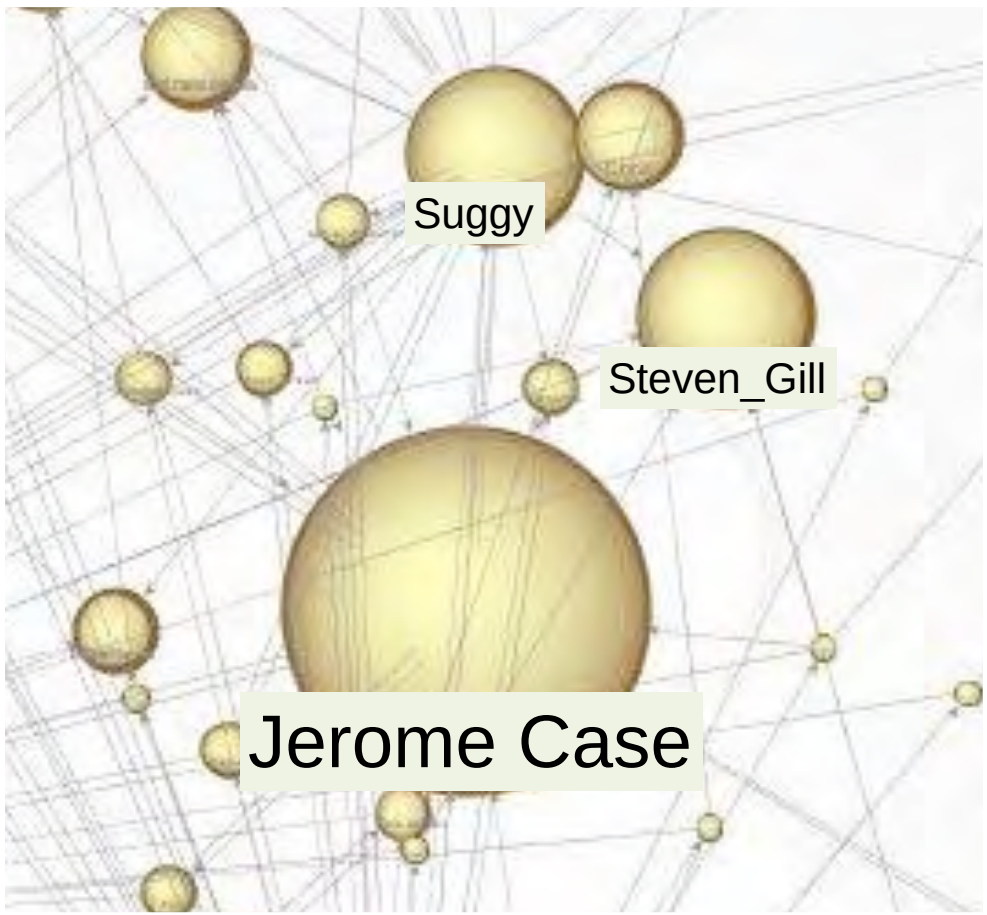
Organic



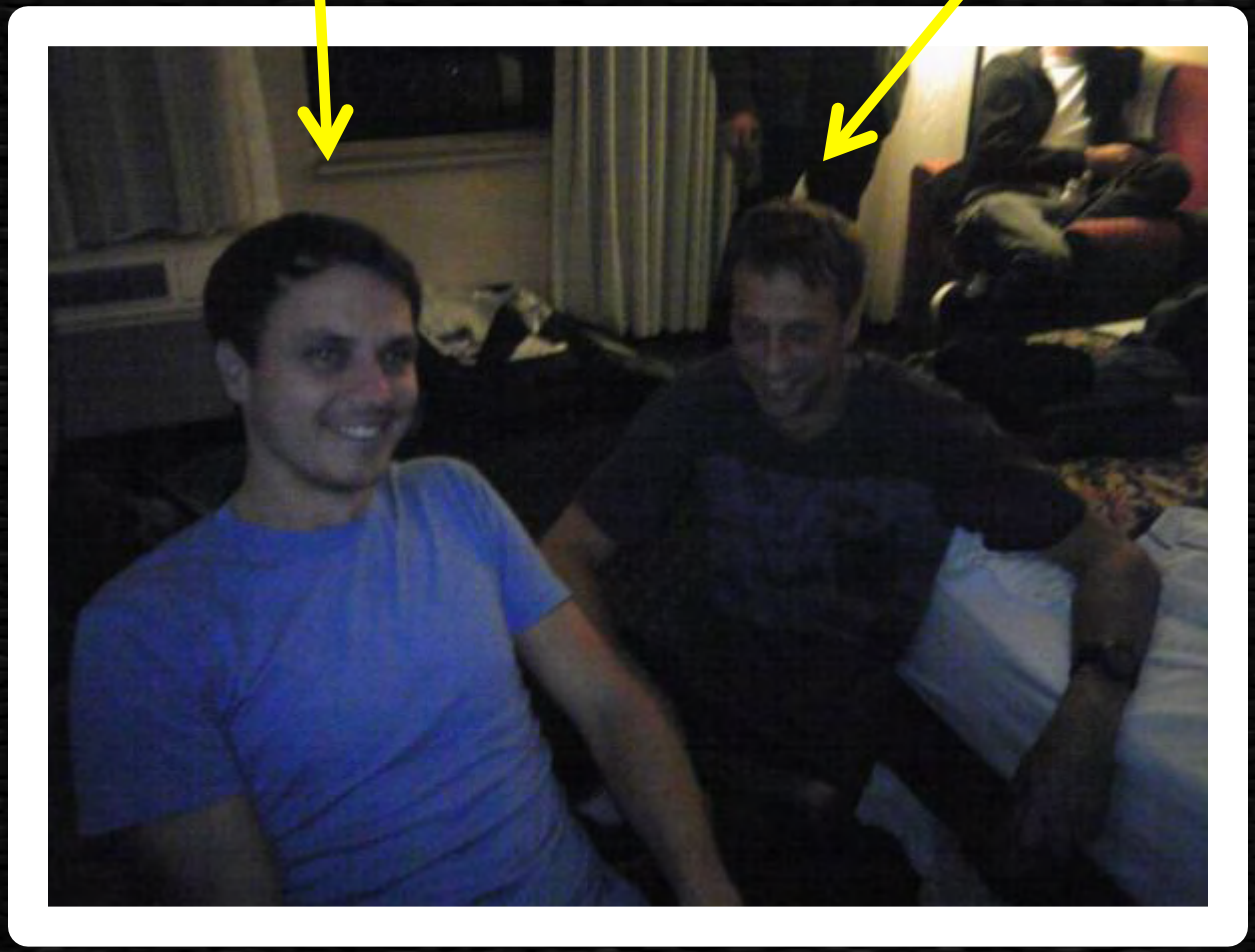
Edge Weighted



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



@sweetjerome & @tonyhawk



Lessons learned #1

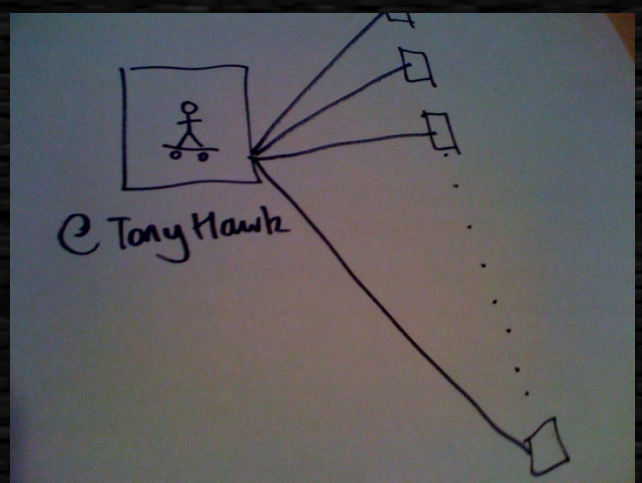
- Plan

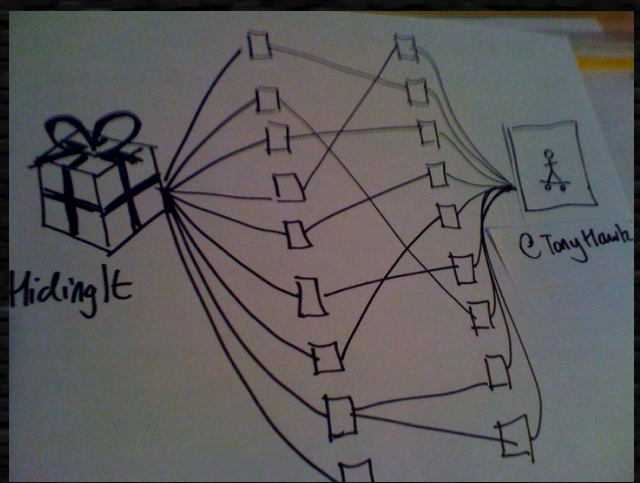






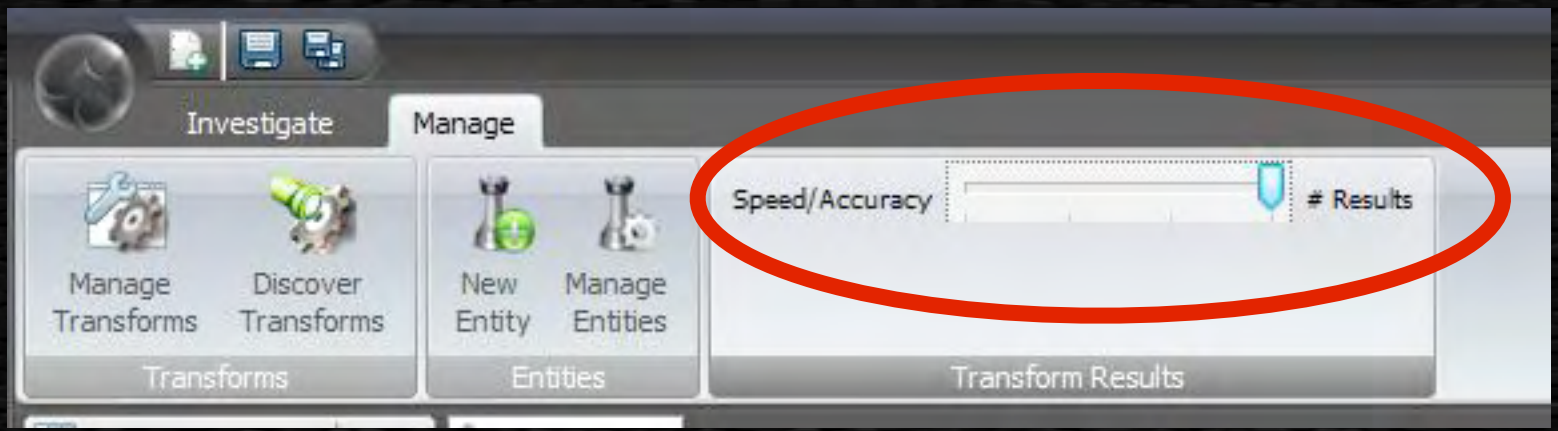






Lessons learned #2

- 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



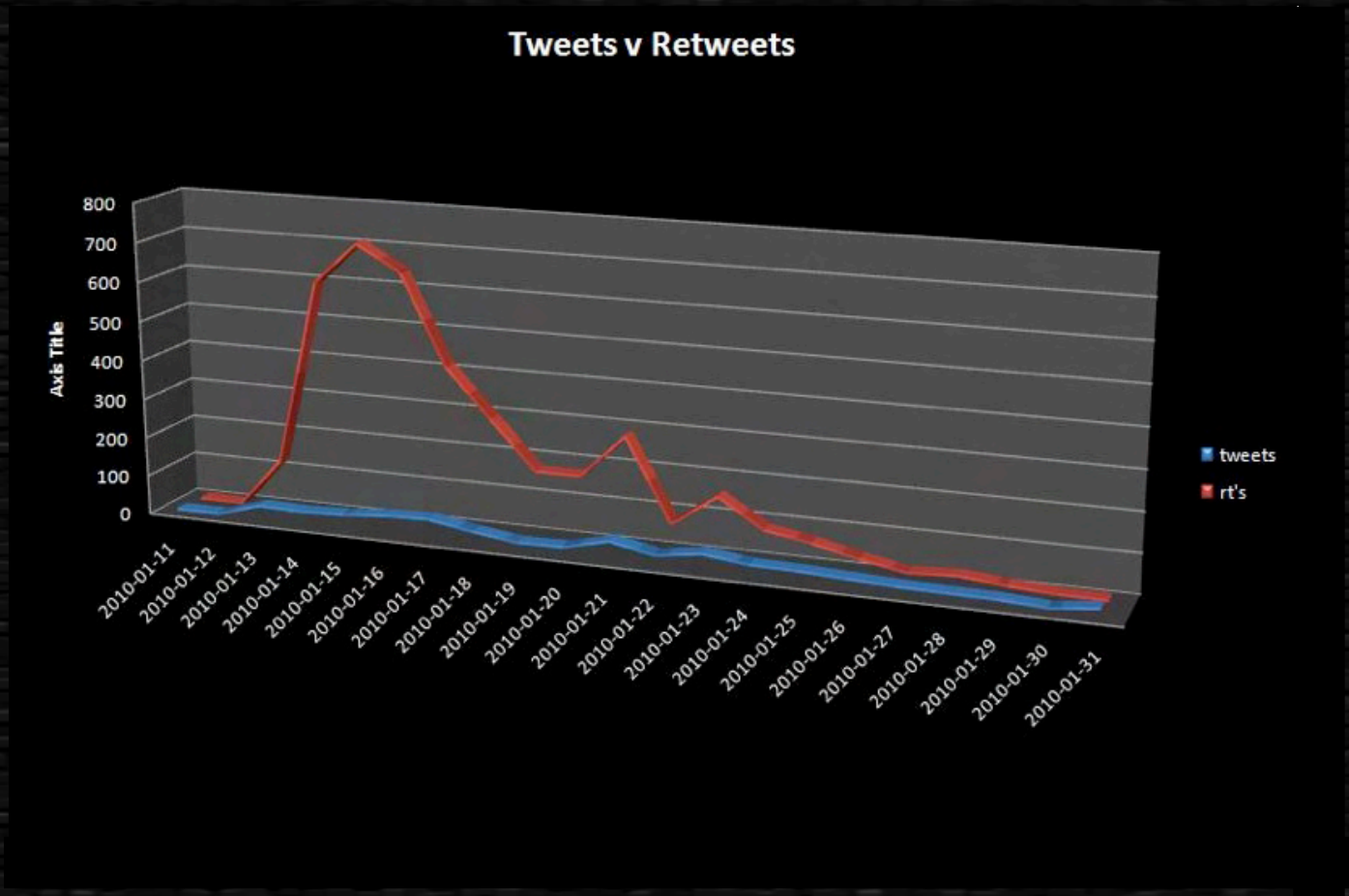
Tuesday, 3 August 2010



"**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”



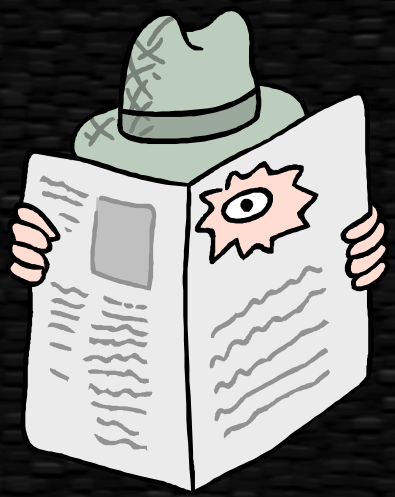
- Laptop on auction site
- Gets bought quickly at “Buy now price”
- Jess exchanges emails with the buyer
- Notification from “paypal”
- Jess sends laptop to valid address in UK
- Notice from auction site that buy account had been hacked

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.

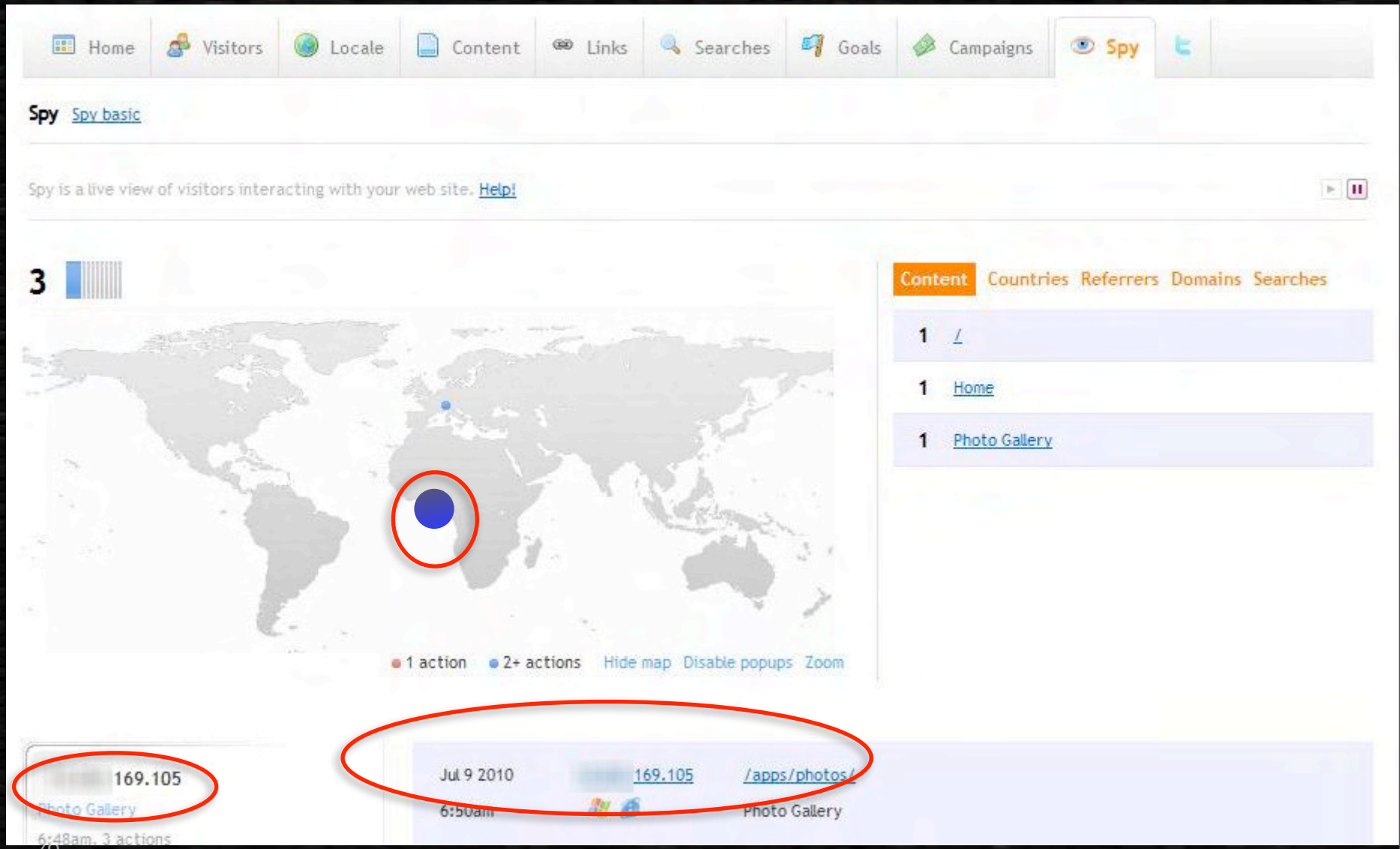
Step #1 Where is our scammer?

- 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



webs.com visitor logs



Add Google Toolbar Button | Add Search Plugin

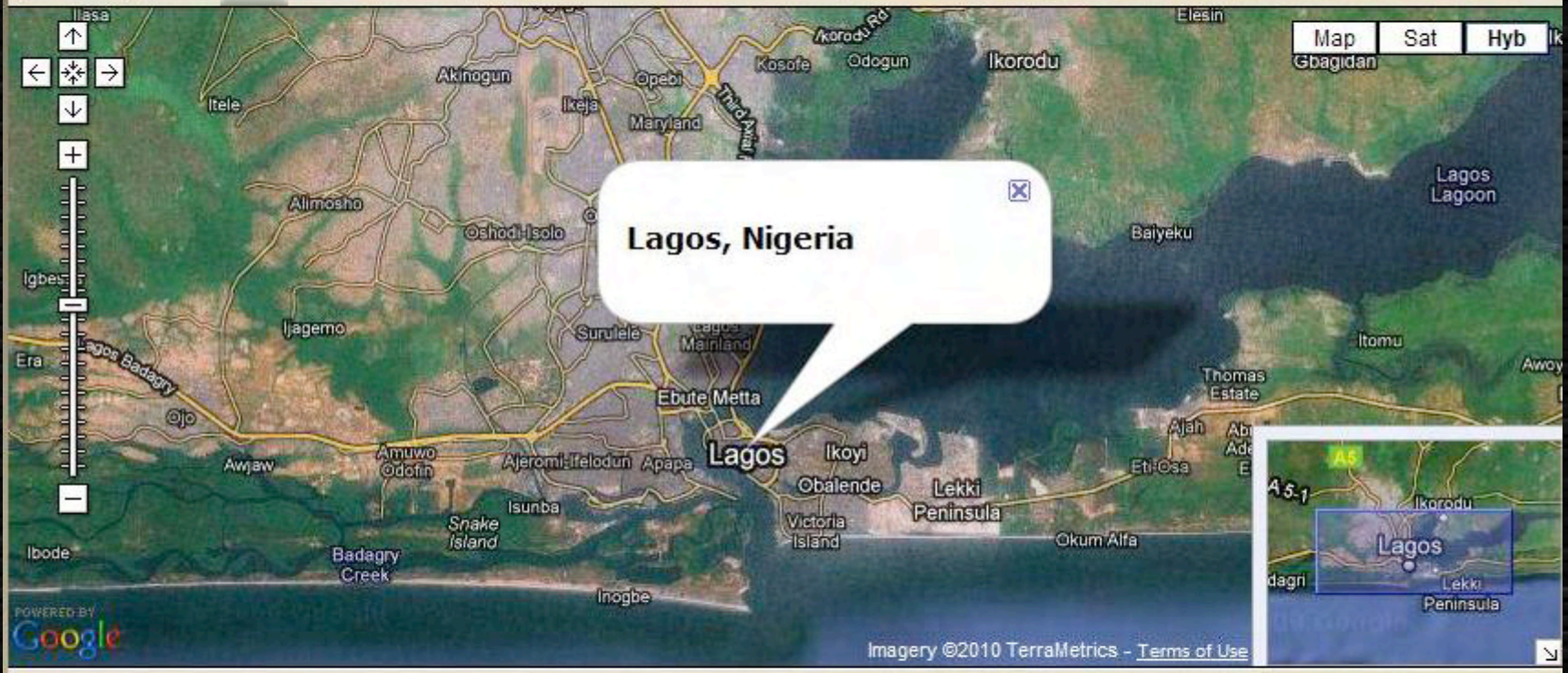
INFO SNIPER
Geolocation Service

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.

Ads by Google | IP Whois | Map | Whois com Search | Better Whois | Domain Whois

HOME | SERVICE | URL PARAMETER | API | LIVEVISITS | GADGETS | WORLDMAP | SCRIPTS

Check 41.220. Google Maps™ Windows Live Maps™ Yahoo Maps™ Two Maps Overview Map



IP Address 41.220.	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	Country Nigeria	Longitude 3.3958	Postal Code n/a
Timezone Africa/Lagos	Continent Africa	TLD NG	GMT Offset 1

Show Whois Results

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





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

Info Gathering

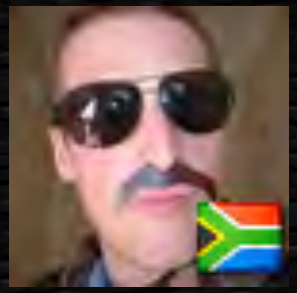




- Email addresses
- Nick names
- Friends
- Addresses
- Schools
- Pictures… lots of pictures



Dominic @Singe White

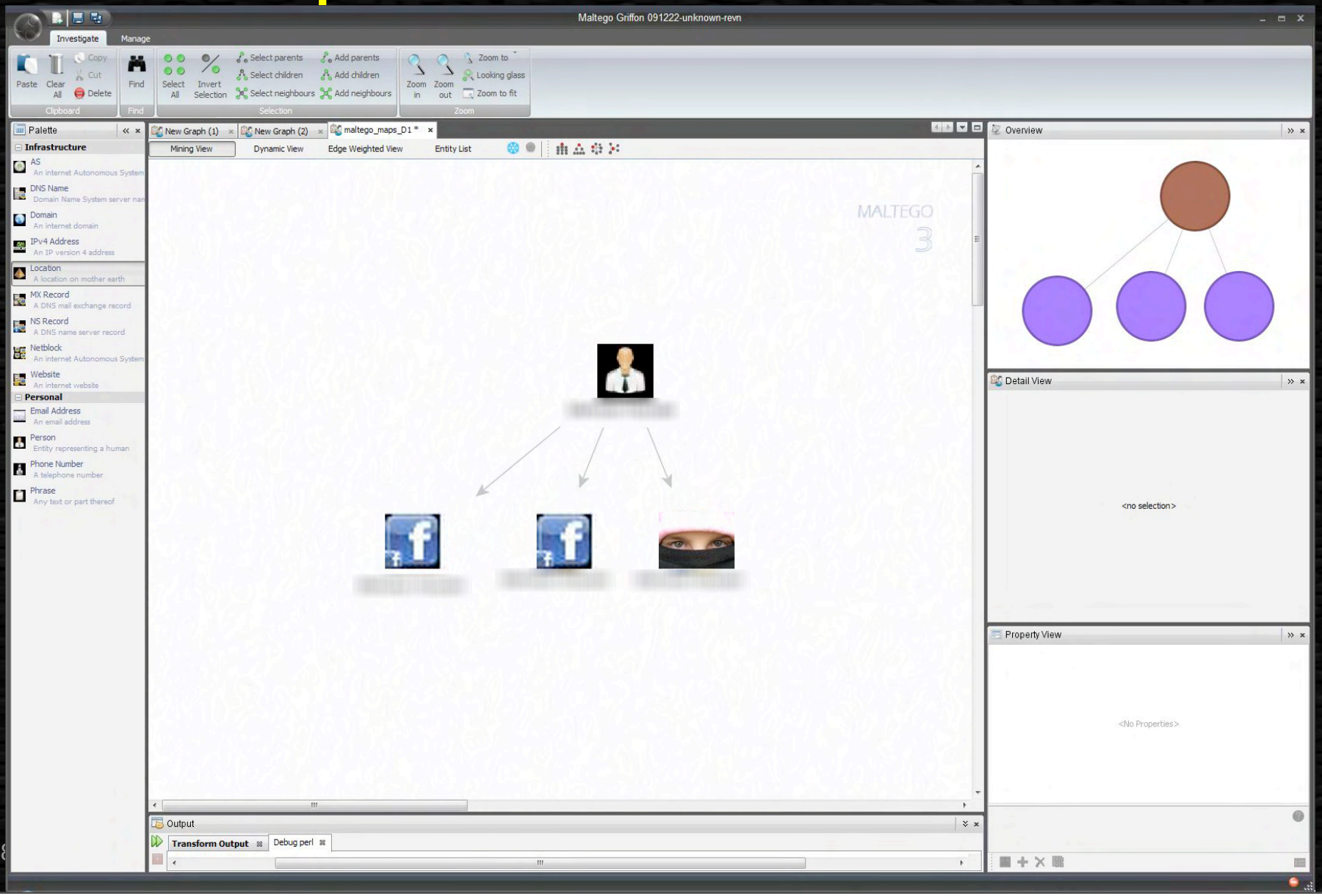


...wrote some useful facebook transforms for Maltego

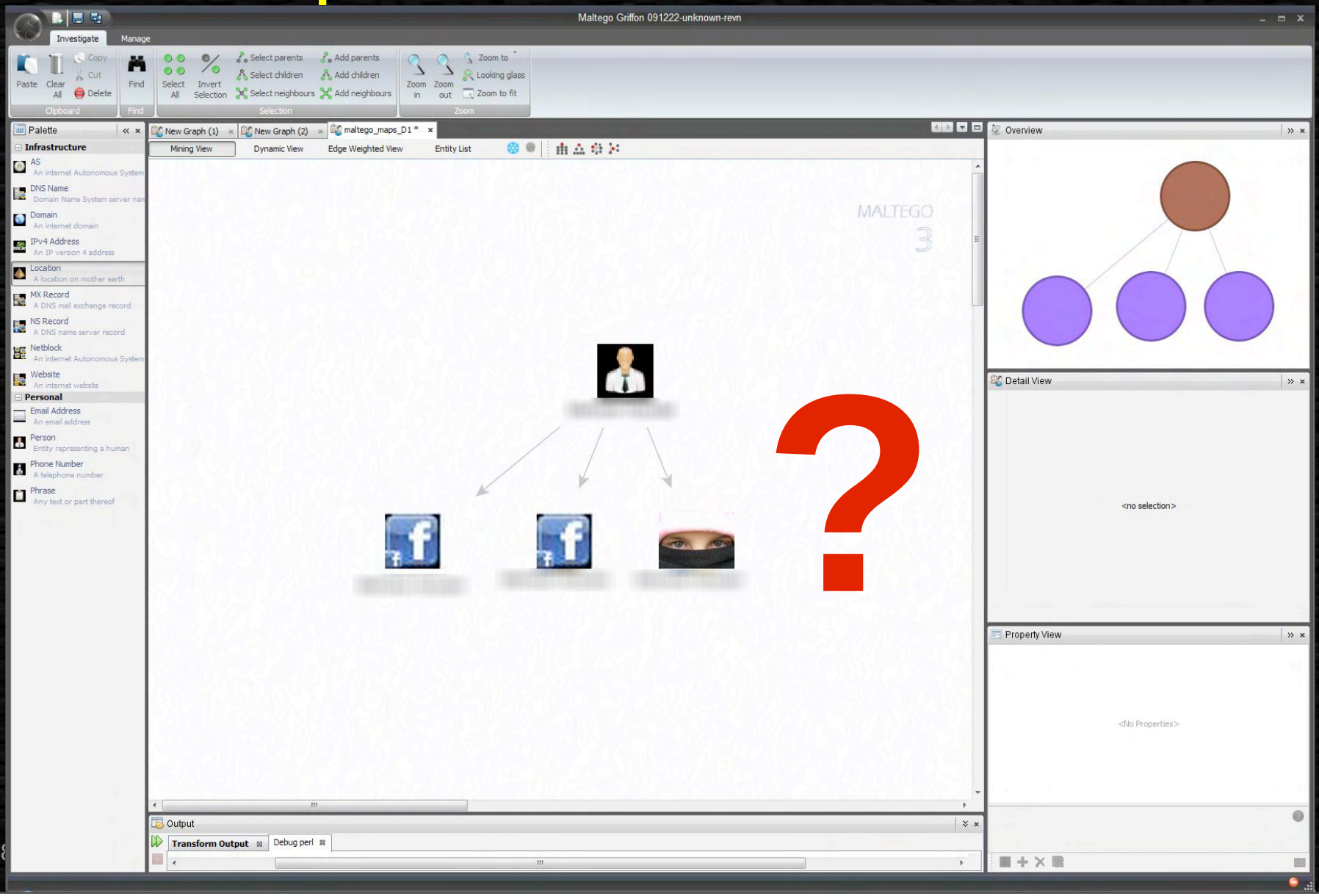
Python
Mechanize
Beautiful Soup

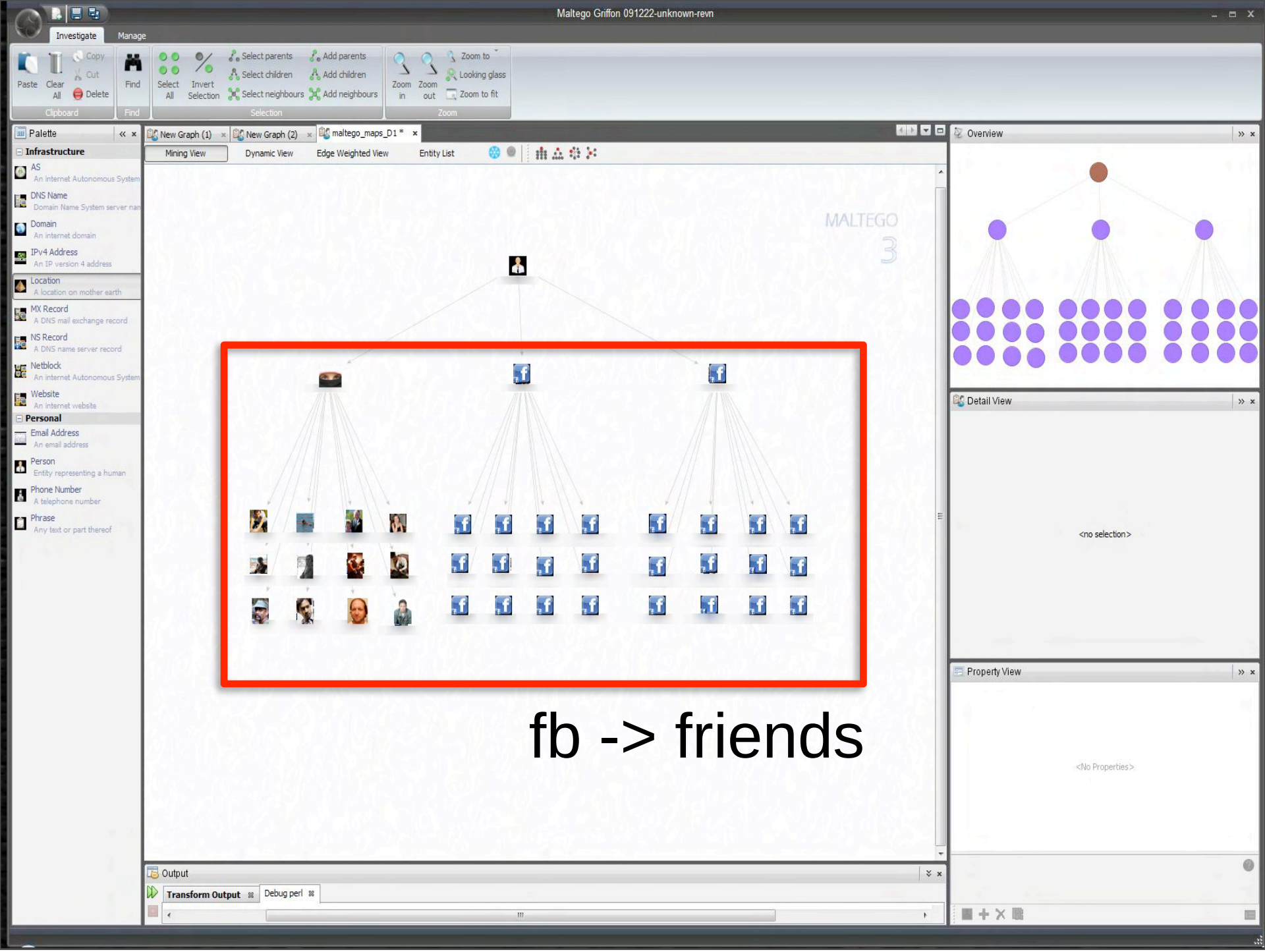
They'd break Facebook ToS so don't use them.

Step #3 Which “Alice” ?

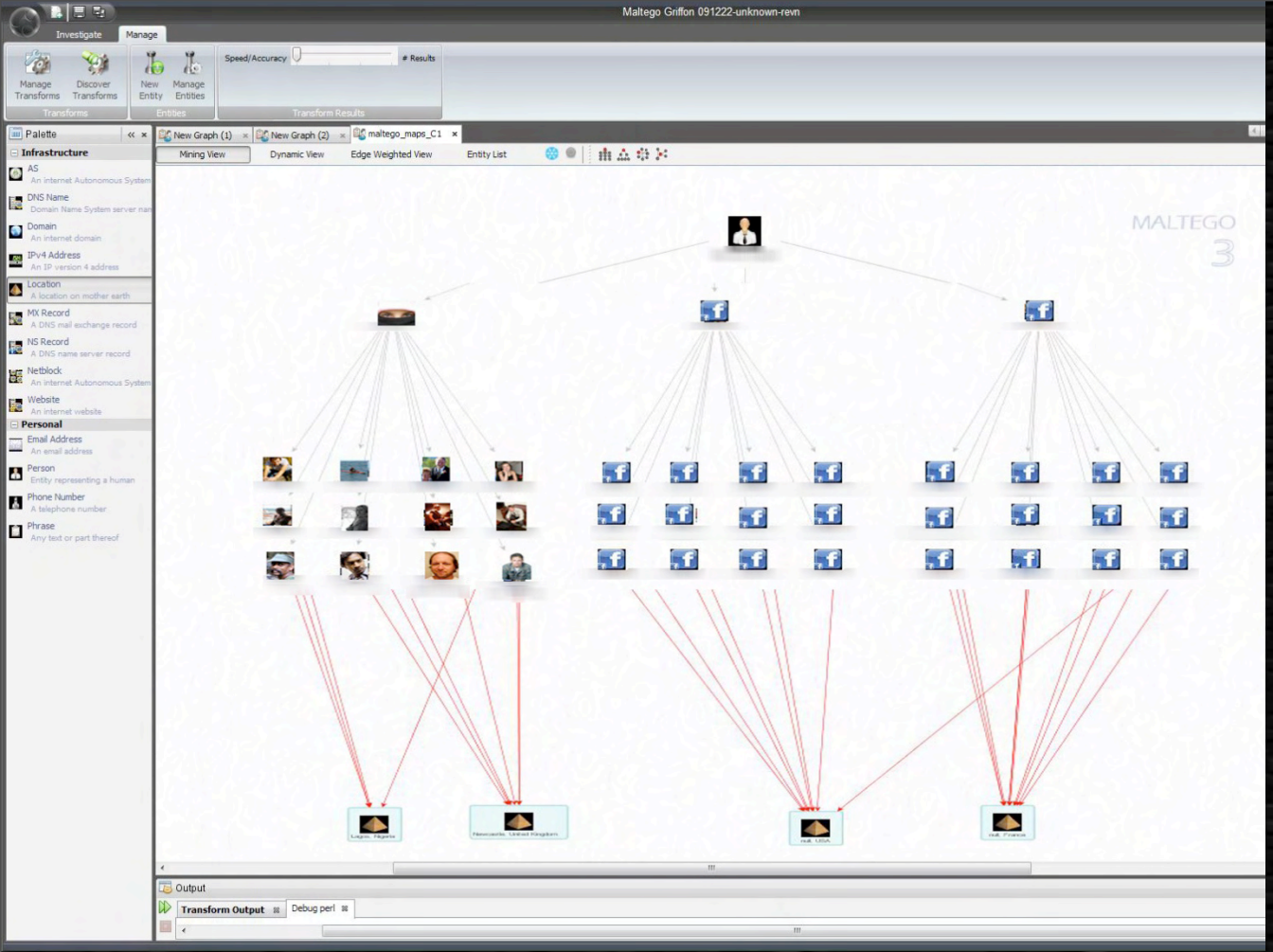


Step #3 Which “Alice” ?

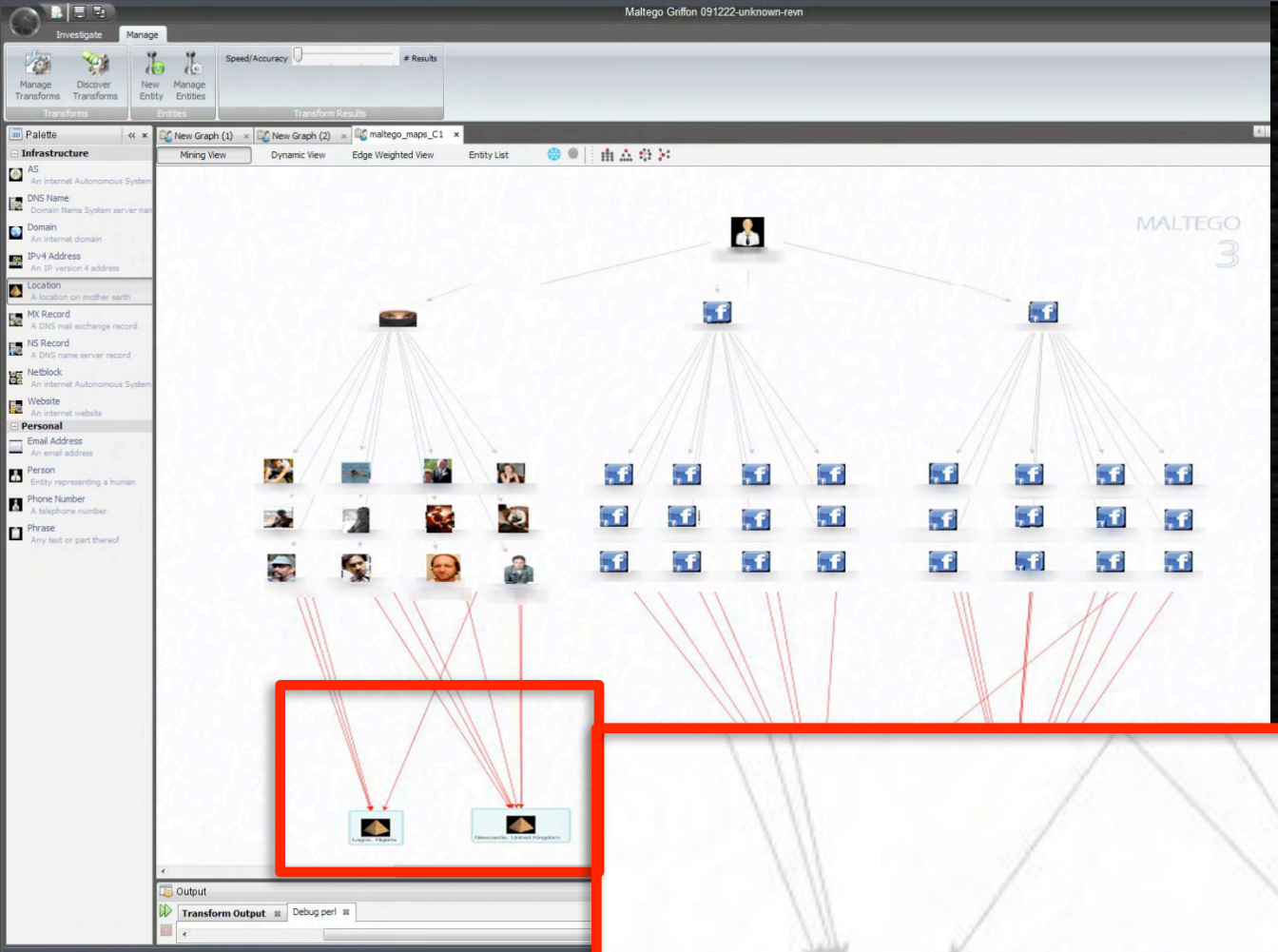


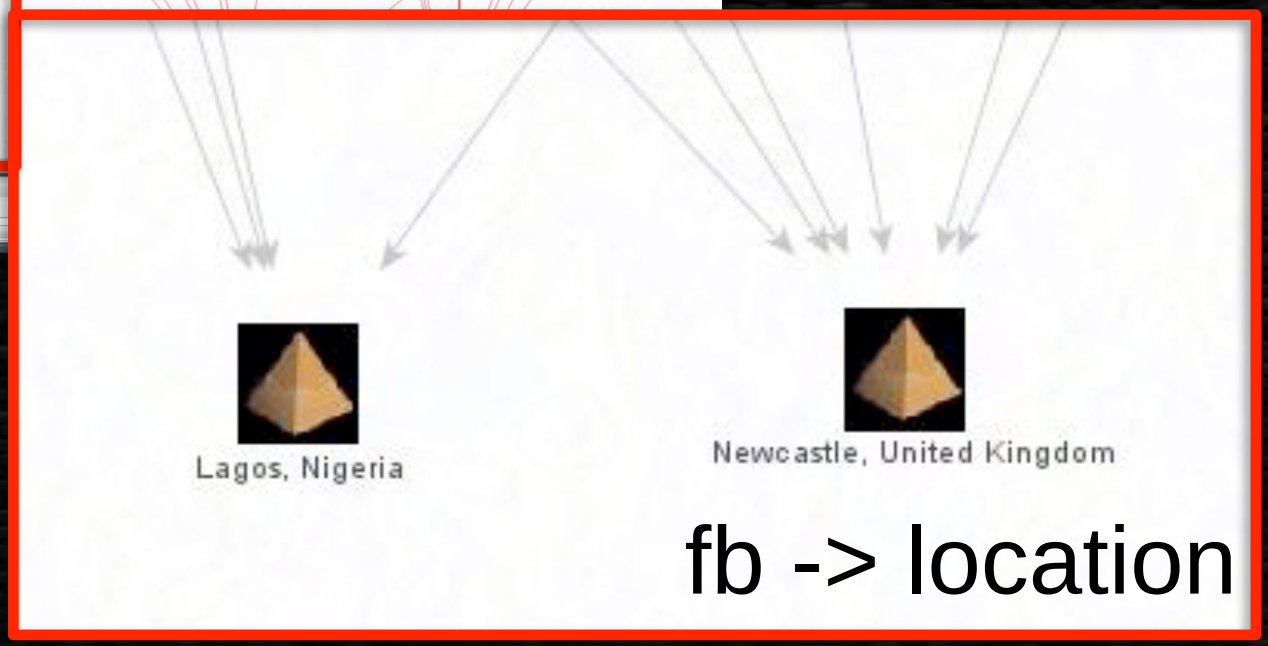


Tuesday, 3 August 2010


Maltego Griffon 091222-unknown-revn
Investigate
Manage
Manage Transforms
Discover Transforms
New Entity
Manage Entities
Speed/Accuracy
Results
Transforms
Entities
Transform Results
Palette
Infrastructure
AS
An internet Autonomous System
DNS Name
Domain Name System server nam
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

fb -> location


Maltego Griffon 091222-unknown-revn
Investigate
Manage
Manage Transforms
Discover Transforms
New Entity
Manage Entities
Speed/Accuracy
Results
Transforms
Entities
Transform Results
Palette
Infrastructure
AS
DNS Name
Domain
IPv4 Address
Location
MX Record
NS Record
Netblock
Website
Personal
Email Address
Person
Phone Number
Phrase
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

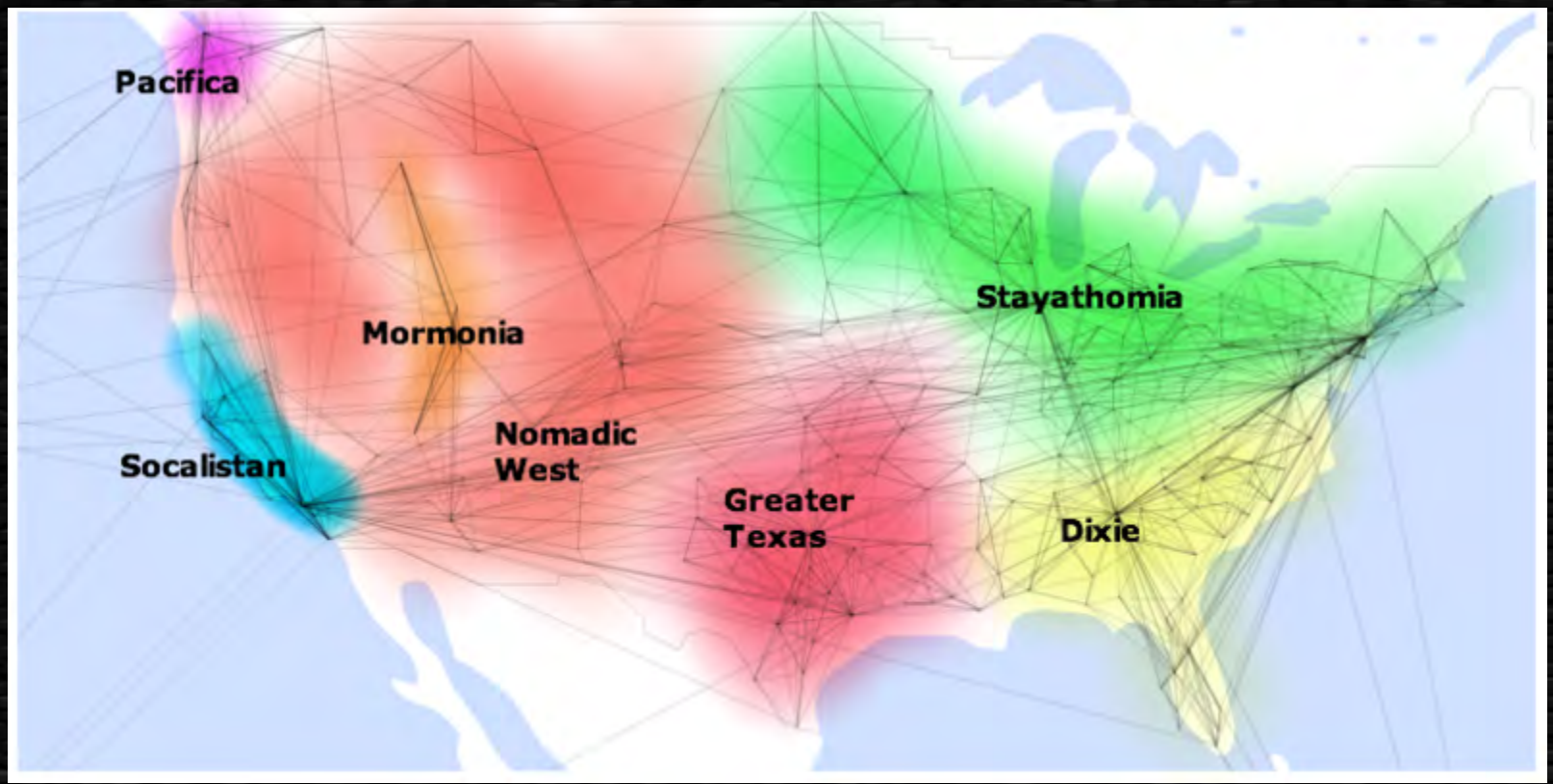
How to get sued by Facebook

- 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 !!! >

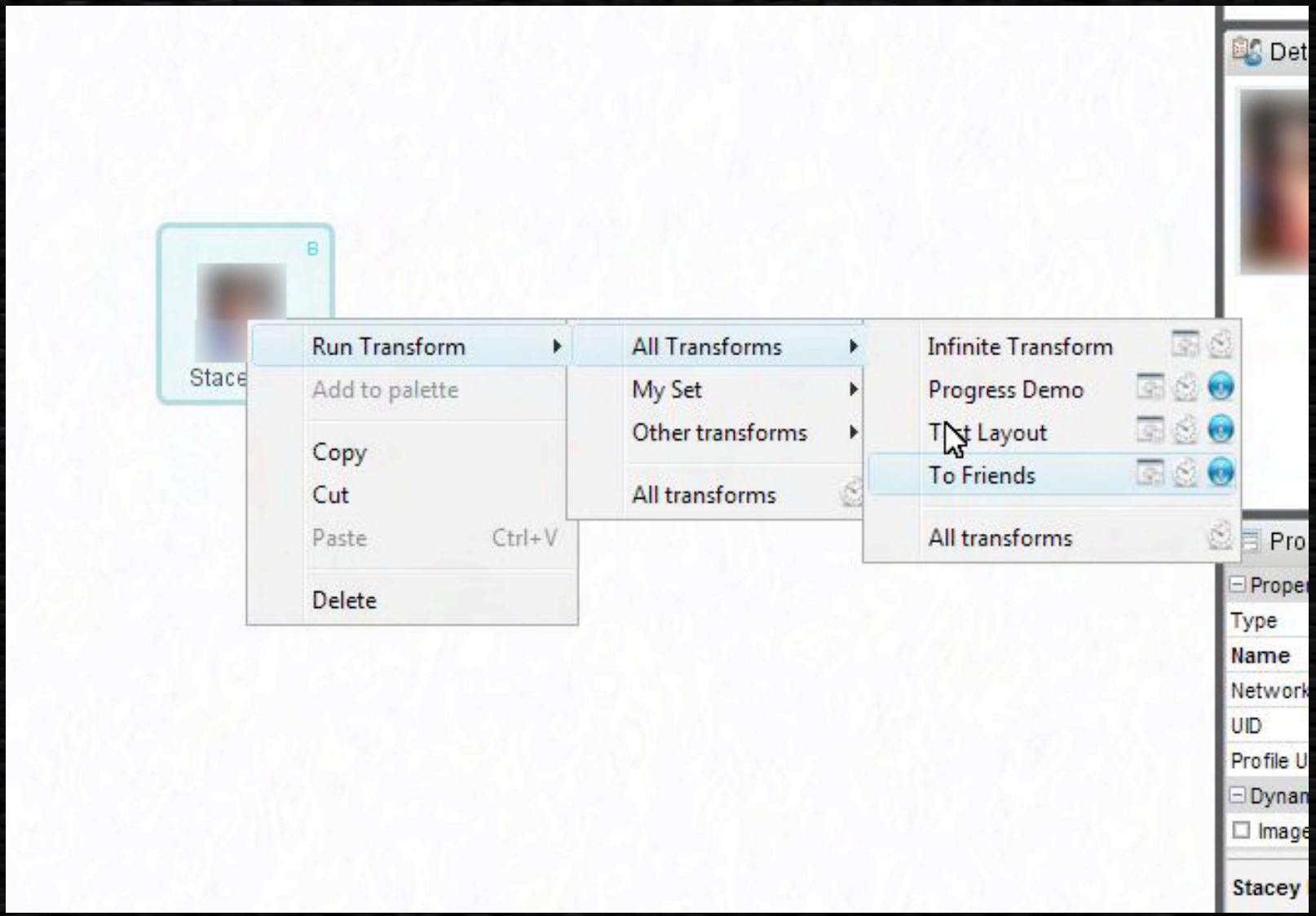
I'm a friend of "Alice"'s, just getting started and that. I added a few people and might have added too many.

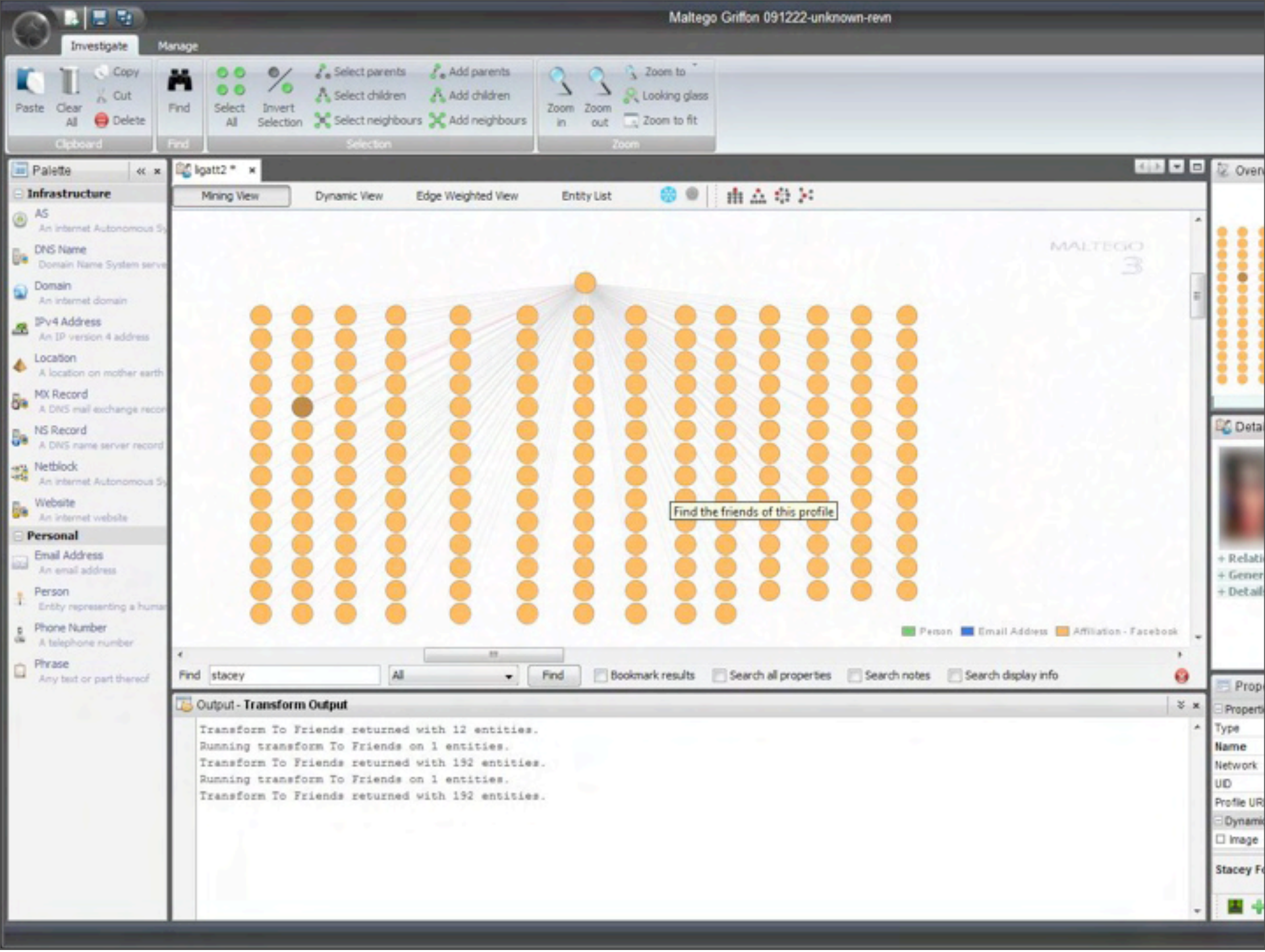
hehehe man cool, well "Alice"'s my best friend lol

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}
}
```

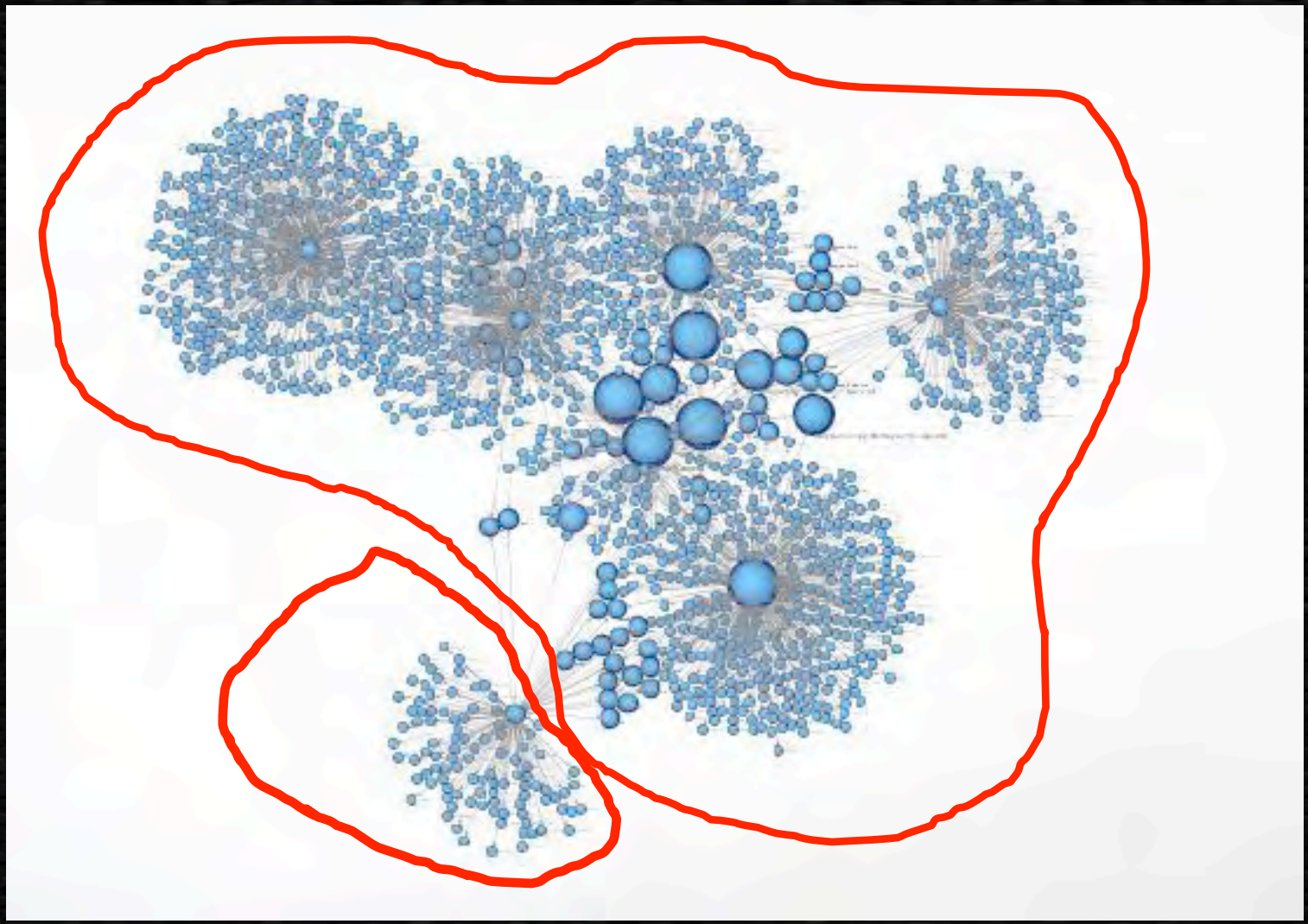
To Facebook Friends

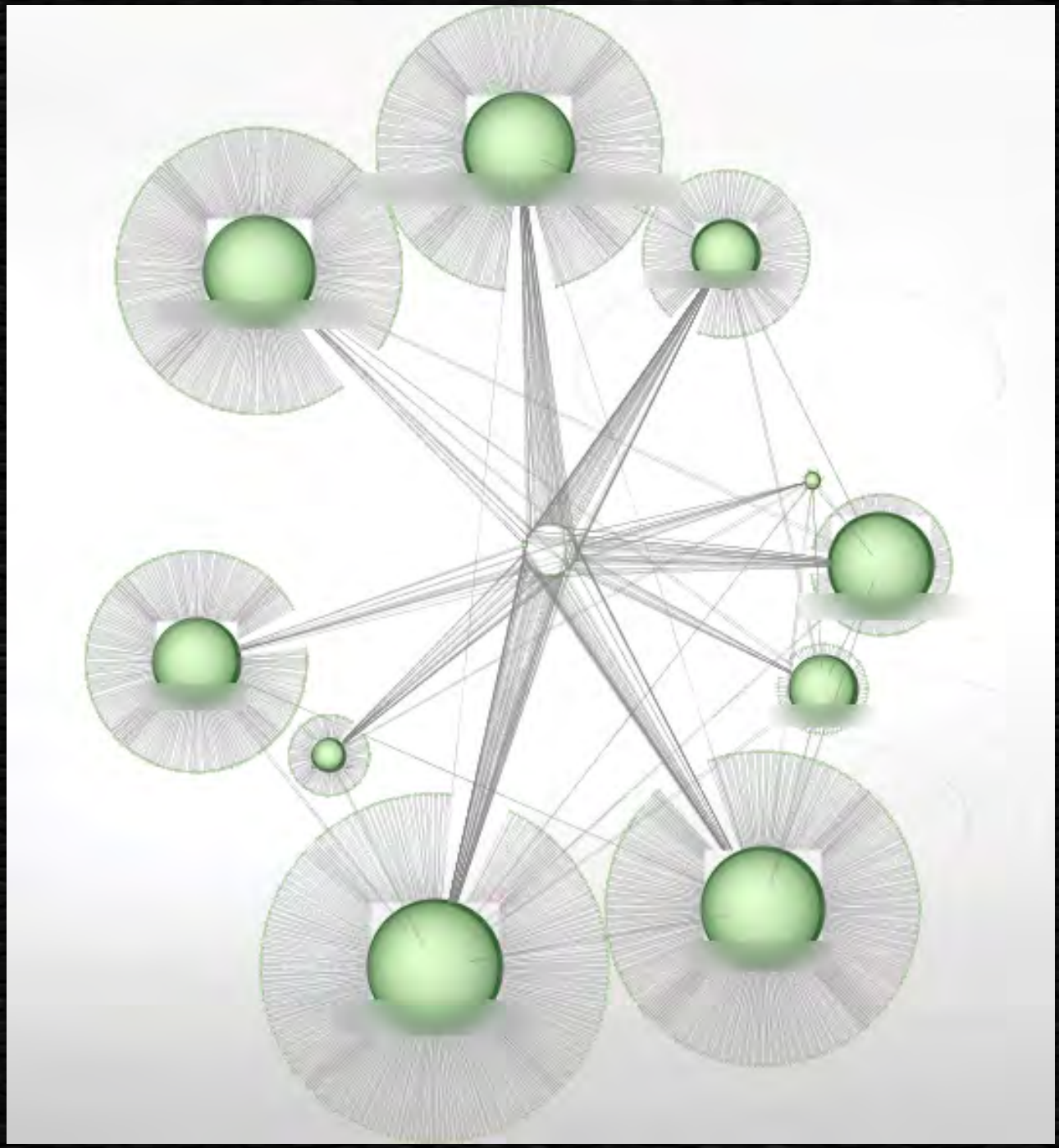




Tuesday, 3 August 2010

“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”

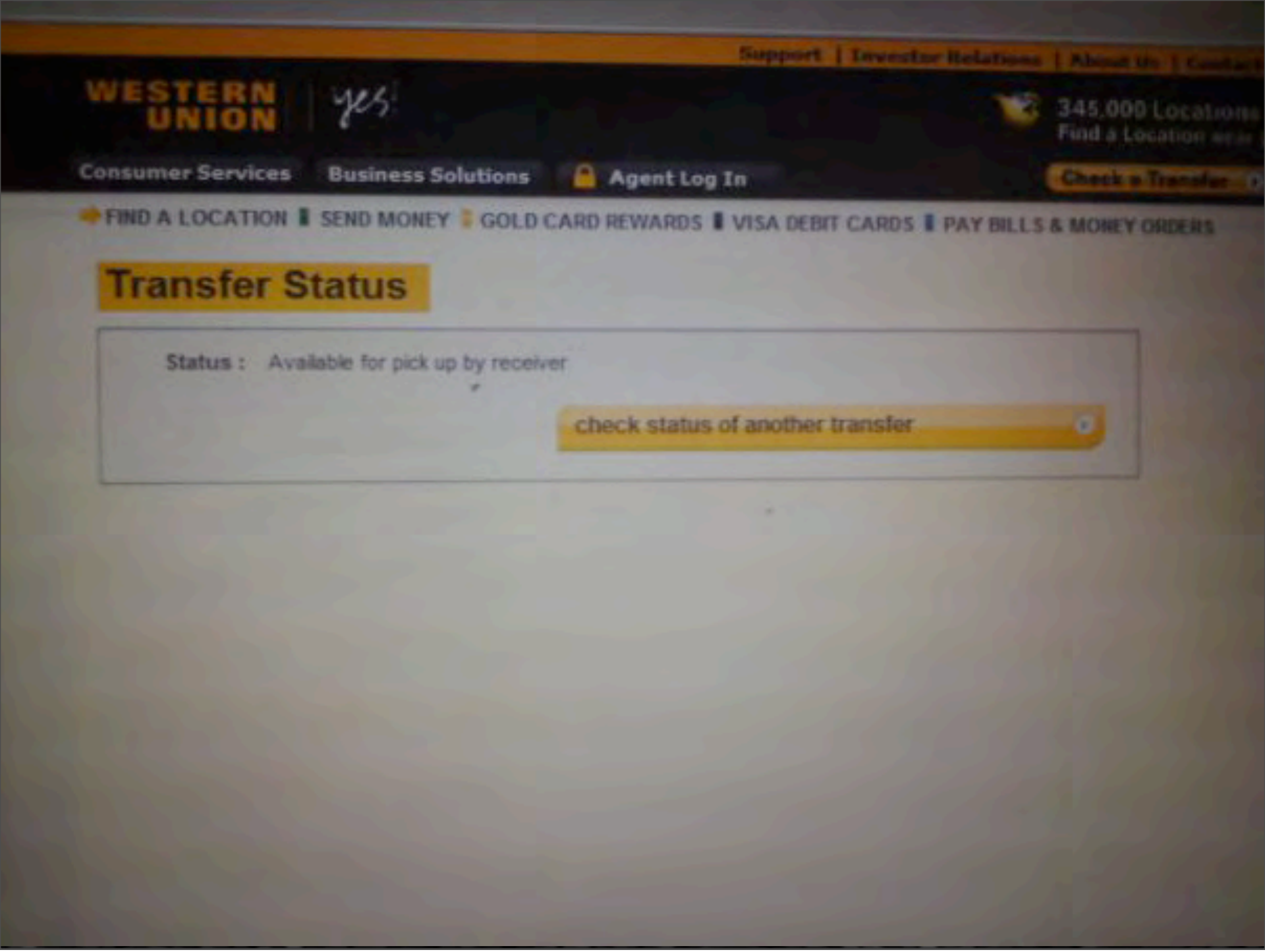
PS3 4 SALE....UK PAL.NEW




OPEN
24 HOURS
WESTERN UNION
WESTERN UNION

“Arrrrrgh!”




Support | Investor Relations | About Us | Contact
WESTERN UNION
345,000 Locations
Find a Location
Consumer Services
Business Solutions
Agent Log In
Check a Transfer
FIND A LOCATION | SEND MONEY | GOLD CARD REWARDS | VISA DEBIT CARDS | PAY BILLS & MONEY ORDERS
Transfer Status
Status : Available for pick up by receiver
check status of another transfer

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)"

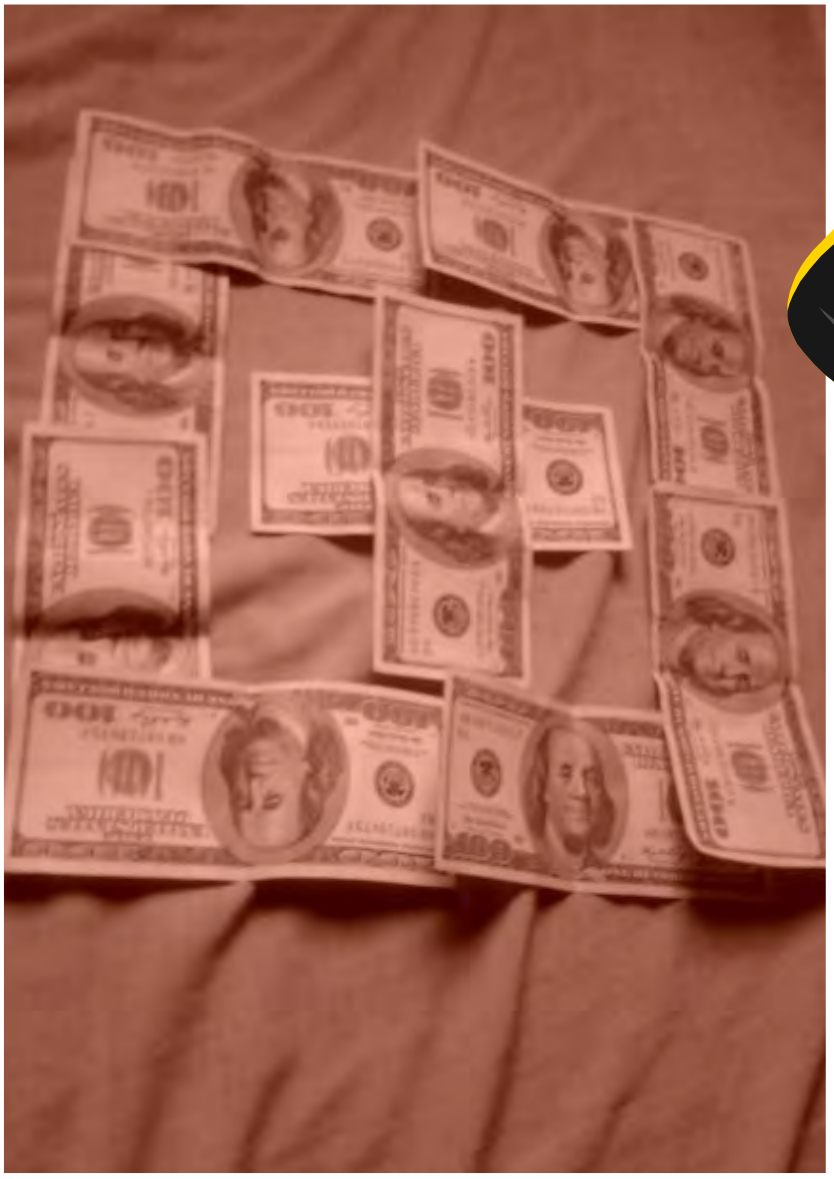
How about something a little more nefarious?



How about something a little more nefarious?









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

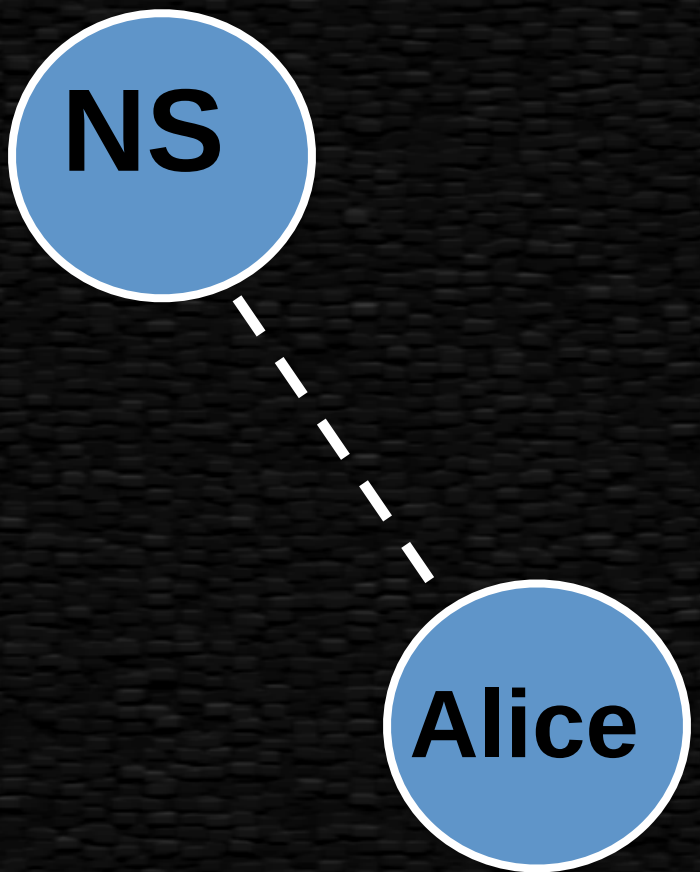
BONUS!!!!


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

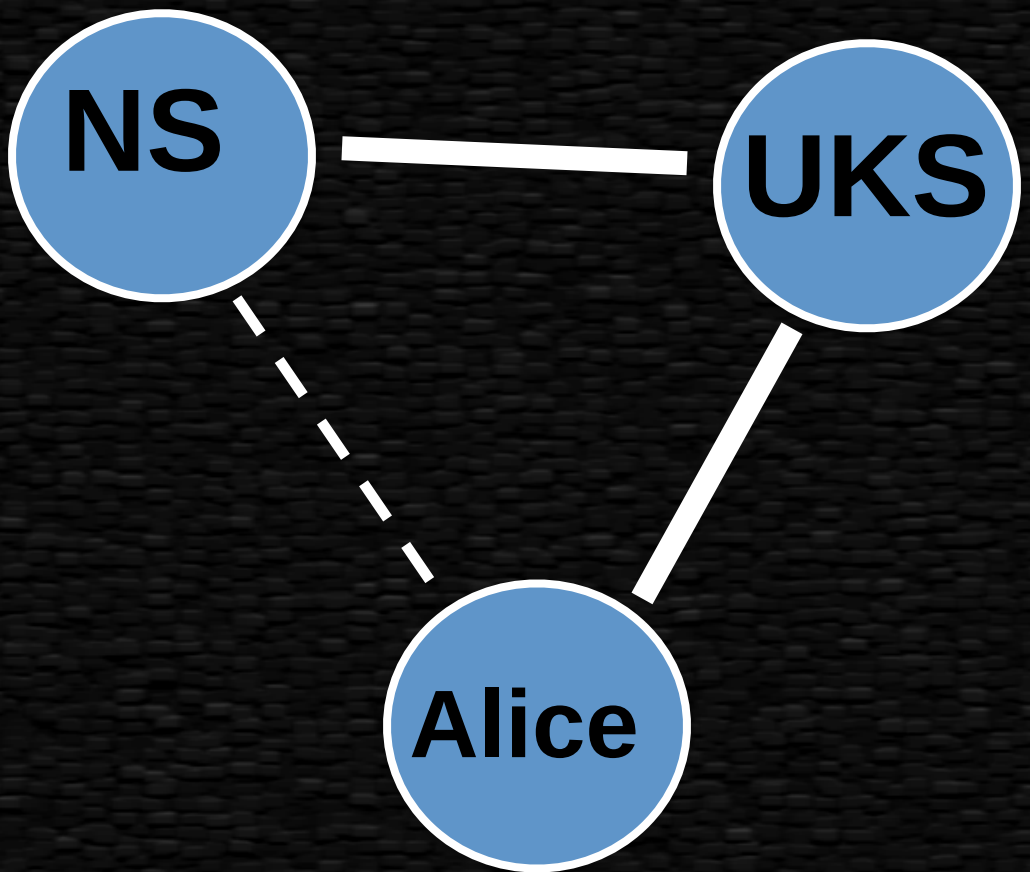
Connections



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

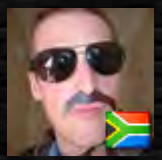
Wrappin’ up

- 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

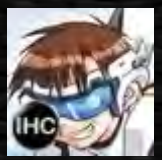
Maltego Tweeters



@Paterva



@Singe
Dominic White

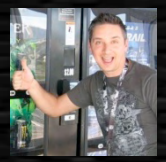


@mubix
Rob Fuller



@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



@neilkod
Neil Kodner



@PeteWarden
Pete Warden



@zrlram @secviz
Raffael Marty



@secviz
Raffael Marty


33
SecurityG33k .com



It's QUESTION TIME!!