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
- n00bs
- Social Networking Analysis
- This talk

Tuesday, 3 August 2010
Who’s the talk aimed at?

Data Visualization

Social Networking Analysis

n00bs

This talk

1337

1337

n00bs

Social Networking Analysis

Tuesday, 3 August 2010
Who’s the talk aimed at?

Data Visualization

n00bs

Social Networking Analysis 1337

1337

Tuesday, 3 August 2010
Who’s the talk aimed at?

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

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

• 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

What is Maltego?
Maltego is an open source intelligence and forensics application. It will offer youtimous mining and gathering of information as well as the representation of the information in an 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’
E.G.
Domains

Tuesday, 3 August 2010
MX Records
Tony Hawk Twitter Hunt versus Maltego
“Guarded by a fearsome troll, NW from a house where you might have to pay money to pass & a sk8park”
“cammo netting!
You’re a bad man”
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
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
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 some implement that yourself

11:12 AM Oct 23rd from web in reply to TheSuggmeister
List the Hiders
Derive @HidingIt
To Tweets [Search Twitter]
To Twitter Affiliation [Convert]
To friends of this person
“Suggy”
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
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
List of all @mentionee's
Found ATL by @blahblahblah

Tony’s @ mentionee’s (potential finders....)
Repeat for each of Tony’s mentionee’s
A bit less messy
Centrality layout

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

Tuesday, 3 August 2010
Edge Weighted

Tuesday, 3 August 2010
So what? What on earth have I been going on about?
@sweetjerome & @tonyhawk

Tuesday, 3 August 2010
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
“Just Landed: Processing, Twitter, MetaCarta & Hidden Data”

Jер Thorp, using processing

Tuesday, 3 August 2010
Graphs for DEC.org.uk

......Check out RowFeeder.com

Tuesday, 3 August 2010
I go chop your dollar...
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

Tuesday, 3 August 2010
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

Tuesday, 3 August 2010
webs.com visitor logs

See... Jeremiah Grossman's talk

Jul 9 2010  169.105 /apps/photos/
Lagos, Nigeria
Step #2  where did package really go?

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

Newcastle

Alice
Step #2 where did package really go?

NS

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

Alice

Newcastle
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”? 

Tuesday, 3 August 2010
Step #3 Which “Alice”??
fb -> friends
Tuesday, 3 August 2010
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
- 220 million 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

Tuesday, 3 August 2010
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
“Interesting” People
“7k in 5 days”

- Fast money
- Flashy rides
- Expensive clothes
- HOT chicks
- Luxury apartment
- “It’s 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

Tuesday, 3 August 2010
“Arrrrrrgh!”
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 SLAVER Y IN 1905(start working)”
How about something a little more nefarious?
How about something a little more nefarious?
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 Investigatons)
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!!!!
holla
about an hour ago • Comment • Like • See Wall-to-Wall
Connections

Alice

Tuesday, 3 August 2010
Connections

NS

Alice
Connections

NS  Alice  UKS

Tuesday, 3 August 2010
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

@diginnga
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
It's QUESTION TIME!!