NUNA

Digital Intelligence Gathering

Using The Powers Of OSINT For Both Blue And Red Teams

BSidesSF February 2016

Ethan Dodge

🏢 DFIR @ Nuna Health.

⚠ DFIR professional and perpetual learner.

🐦 @__eth0

💻 dodgesec.com

Nuna Health

- We work with the government and self-insured employers to understand and improve how people use healthcare.

Nuna Health

- We work with the government and self-insured employers to understand and improve how people use healthcare.

- Security is the foundation of our culture and products.

Nuna Health

- We work with the government and self-insured employers to understand and improve how people use healthcare.
- Security is the foundation of our culture and products.
- We're accepting resumes!

▸ OSINT

What is OSINT?

Using information available to everyone to gather intelligence

What is OSINT?

Using information available to everyone to gather intelligence

- Social Networks

What is OSINT?

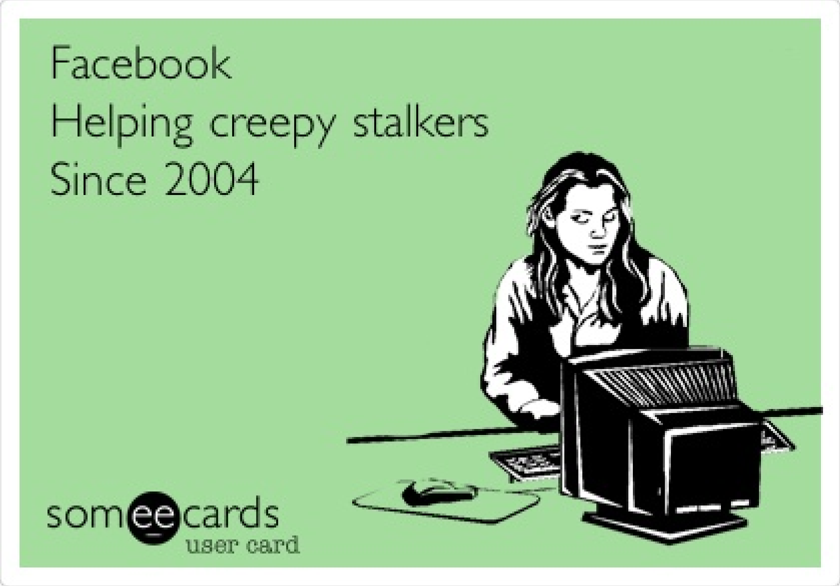
Using information available to everyone to gather intelligence

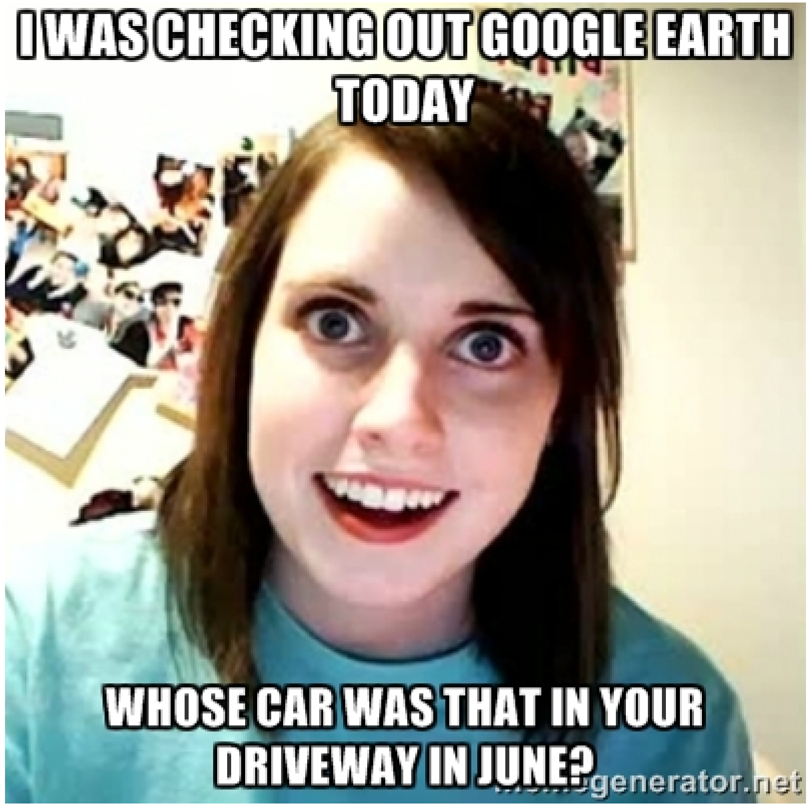
- Social Networks
- Public Data Records

What is OSINT?

Using information available to everyone to gather intelligence

- Social Networks
- Public Data Records
- Leaked Customer Data


Facebook
Helping creepy stalkers
Since 2004
someecards
user card


I WAS CHECKING OUT GOOGLE EARTH TODAY
WHOSE CAR WAS THAT IN YOUR DRIVEWAY IN JUNE?
generator.net

Why OSINT?

- Private Investigators/Detectives
- Investigative Journalism
- Criminal Activity/Law Enforcement
- Threat Intelligence

It's not stalking.
It's called being an Internet Detective.
someecards
user card

JUST KIDDING
I'M REALLY STALKING YOU!
memegenerator.net

DISCLAIMER

Basic Workflow

Identify Source

- Identify possible sources of intel
- Validate
- Automate

Basic Workflow

Identify Source

Analyze

- » Does it apply to our target?
- » Determine probability
- » Apply confidence
- » Generate new potential sources

Basic Workflow

Identify Source

Analyze

Enrich

- » Add context to target
- » Add probability, confidence level to details
- » Develop narrative

▸ Maltego

Mal...what?

Link Analysis Visualization Tool

- Enrich entity with other sources of information automatically
- Identify relationships between entities
- Visualize relationships

Common Terms

- Entities

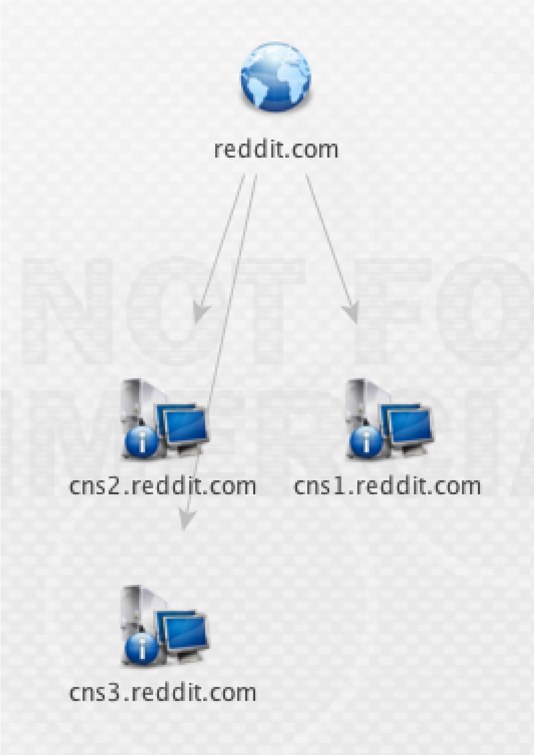
Common Terms

- Entities
- Transforms

Common Terms

- Entities
- Transforms
- Machine

Transform Example



Transform Development Primer

```
from MaltegoTransform import *
```

Transform Development Primer

```
me = MaltegoTransform()
me.parseArguments(sys.argv)
location = sys.argv[1]
```

Transform Development Primer

```
ent = me.addEntity("maltego.Location","DNA Lounge")
me.returnOutput()
```

Gavel

- Custom maltego transform we developed.

Gavel

- Custom maltego transform we developed.
- Digs up court case records from individual states.

Gavel

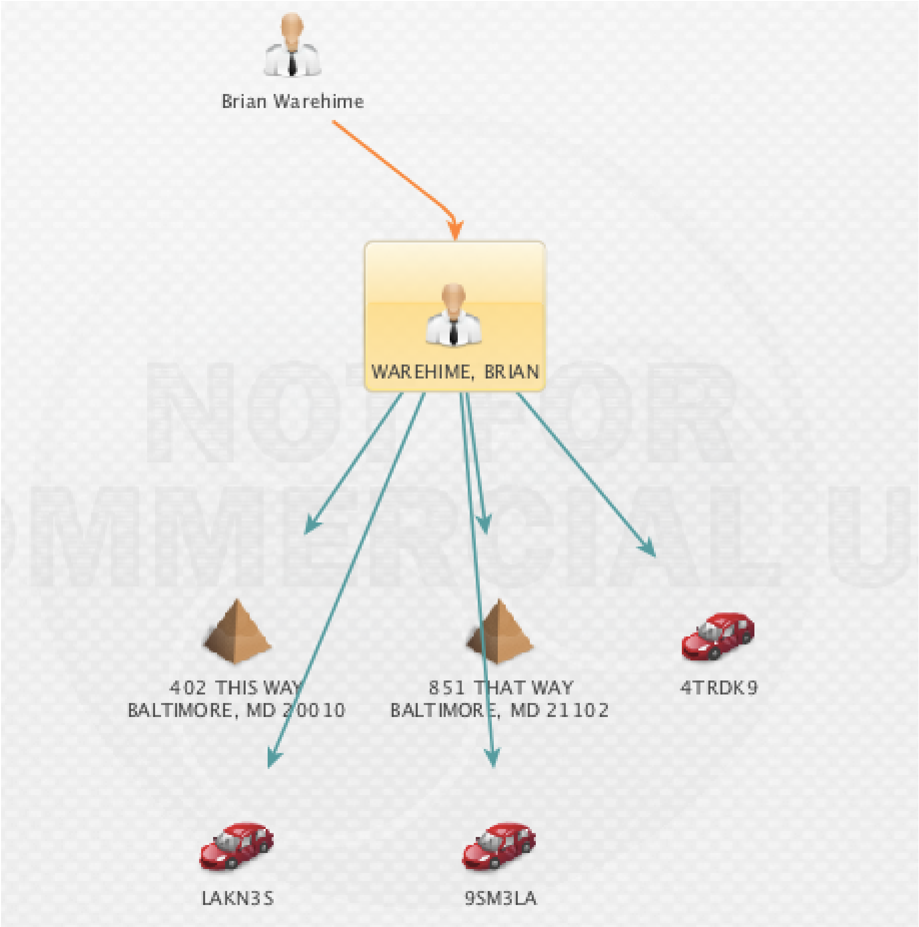
- Custom maltego transform we developed.
- Digs up court case records from individual states.
- Tons of sensitive information.

🔨 Gavel

- Custom maltego transform we developed.
- Digs up court case records from individual states.
- Tons of sensitive information.

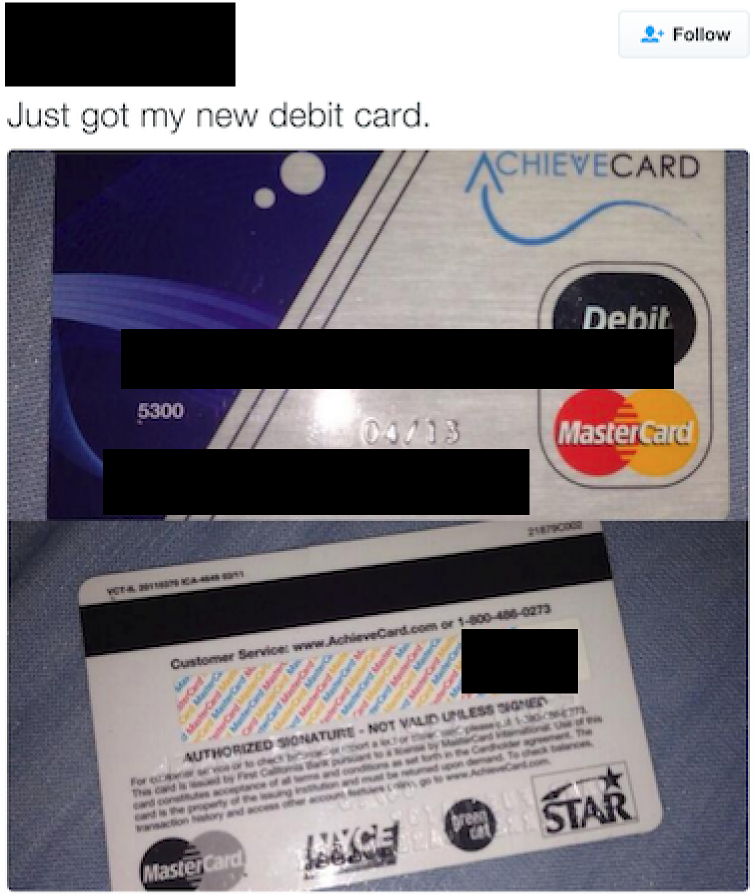
💻 https://github.com/brianwarehime/gavel

Gavel Example



▶ Story Time

Ever seen this?



[redacted]

Just got my new debit card.

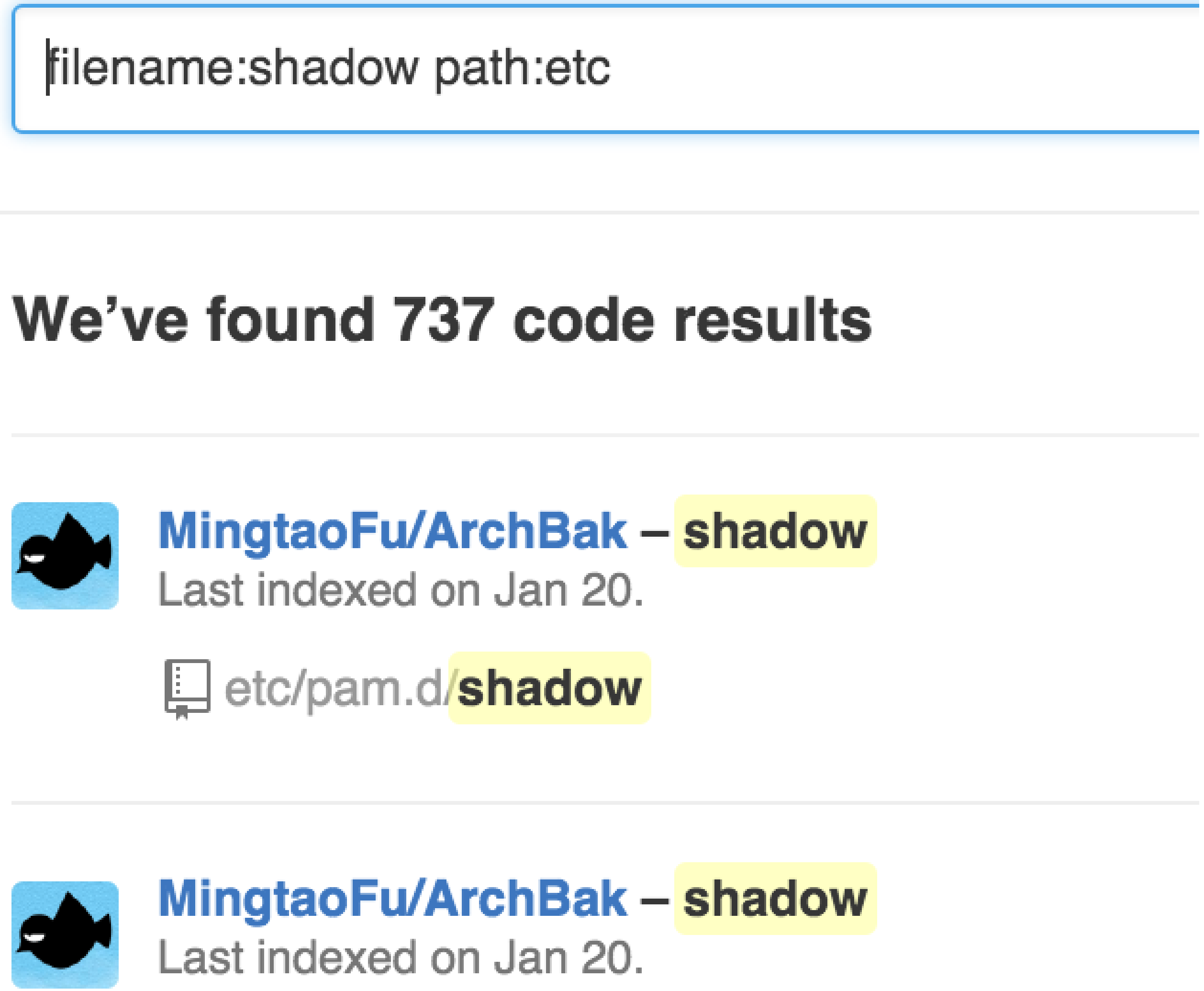
ACHIEVECARD
Debit
MasterCard
5300
04/13
Customer Service: www.AchieveCard.com or 1-800-486-0273
AUTHORIZED SIGNATURE - NOT VALID UNLESS SIGNED
STAR
MasterCard

[redacted]

[redacted]

[redacted]

Or this?



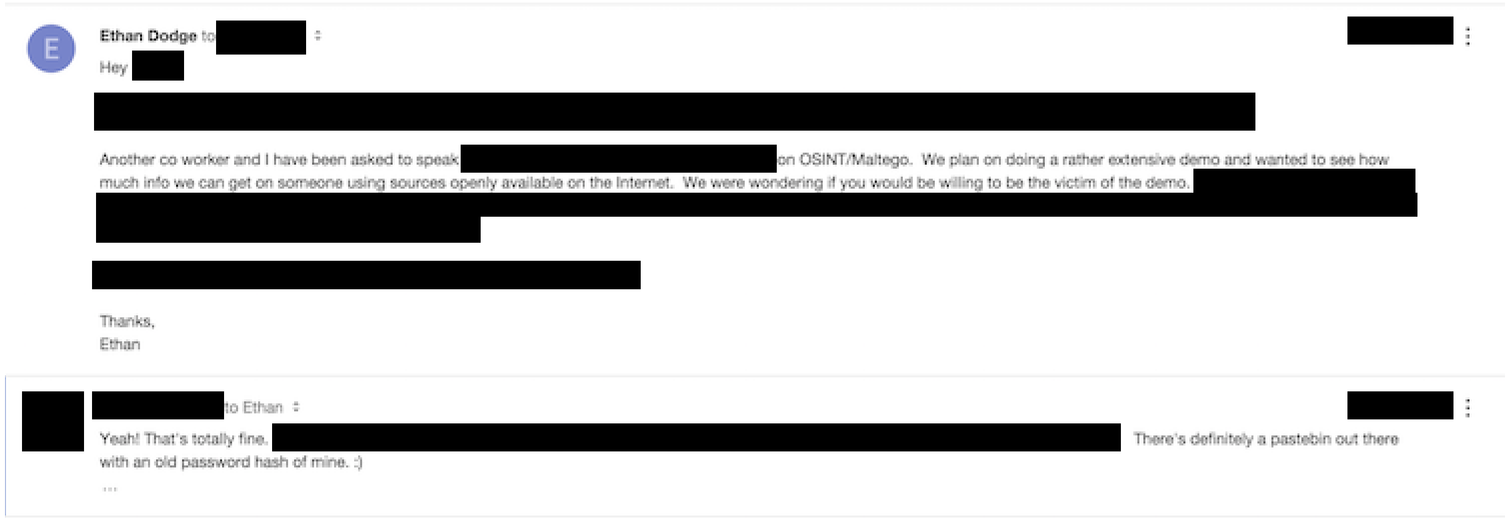
filename:shadow path:etc

We’ve found 737 code results

MingtaoFu/ArchBak – shadow
Last indexed on Jan 20.

etc/pam.d/shadow

MingtaoFu/ArchBak – shadow
Last indexed on Jan 20.



Ethan Dodge to [redacted] [redacted]

Hey [redacted]

[redacted]

Another co worker and I have been asked to speak [redacted] on OSINT/Maltego. We plan on doing a rather extensive demo and wanted to see how much info we can get on someone using sources openly available on the Internet. We were wondering if you would be willing to be the victim of the demo. [redacted]

[redacted]

Thanks,
Ethan

[redacted] [redacted] to Ethan [redacted]

Yeah! That's totally fine. [redacted] There's definitely a pastebin out there with an old password hash of mine. :)

...

Twitter Data

- Start with best source of data - Twitter

Twitter Data

- Start with best source of data - Twitter
- We needed a way to parse through all the data

Twitter Data

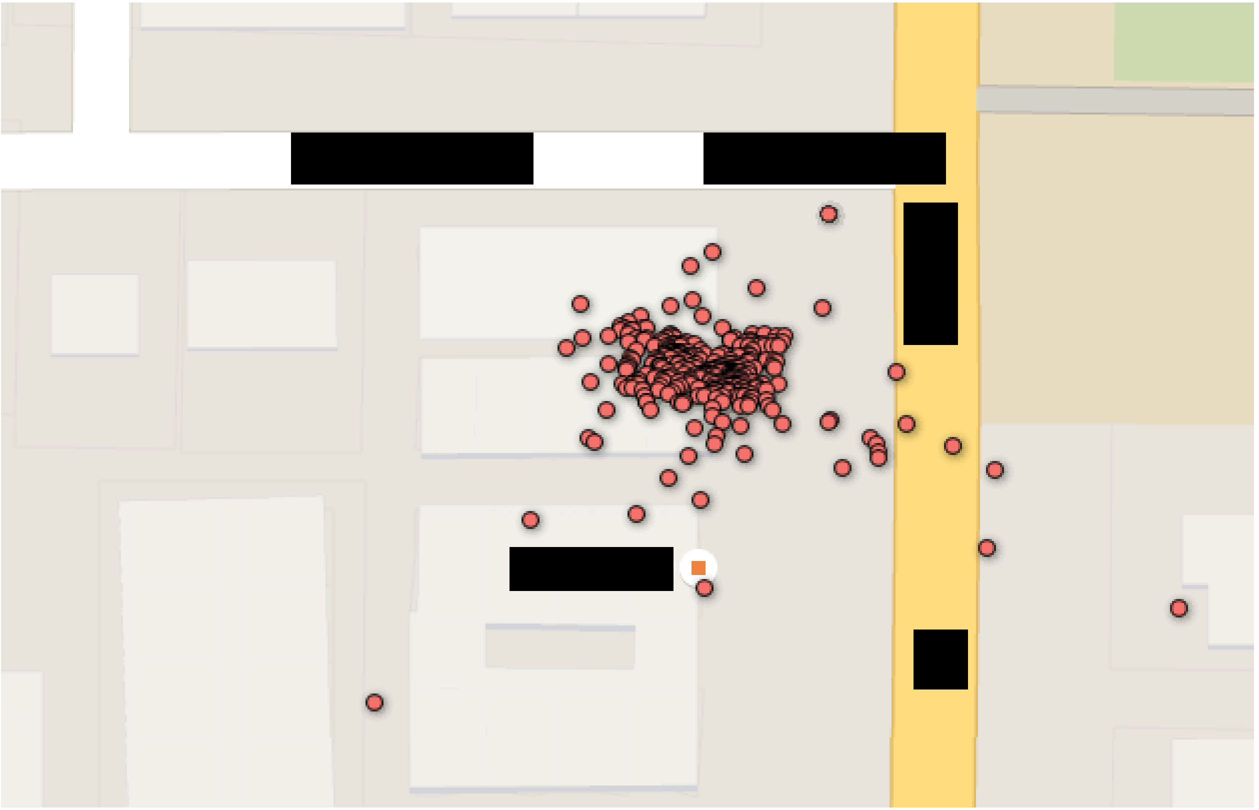
- Start with best source of data - Twitter
- We needed a way to parse through all the data
- We identified it, validated it, now we analyze...

Get the tweets

```
def download_tweets(screen_name,number_of_tweets,max_id=None):

    api_url  = "%s/statuses/user_timeline.json?" % base_twitter_url
    api_url += "screen_name=%s&" % screen_name
    api_url += "count=%d" % number_of_tweets

    if max_id is not None:
        api_url += "&max_id=%d" % max_id

    # send request to Twitter
    response = requests.get(api_url,auth=oauth)

    if response.status_code == 200:

        tweets = json.loads(response.content)

        return tweets
```

All the tweets!

```python
def download_all_tweets(username):
    full_tweet_list = []
    max_id          = 0

    tweet_list   = download_tweets(username,200)

    oldest_tweet = tweet_list[::-1][0]

    while max_id != oldest_tweet['id']:

        full_tweet_list.extend(tweet_list)

        max_id = oldest_tweet['id']

        time.sleep(3)

        tweet_list = download_tweets(username,200,max_id-1)

        if len(tweet_list):
            oldest_tweet = tweet_list[-1]

    full_tweet_list.extend(tweet_list)

    return full_tweet_list
```


[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

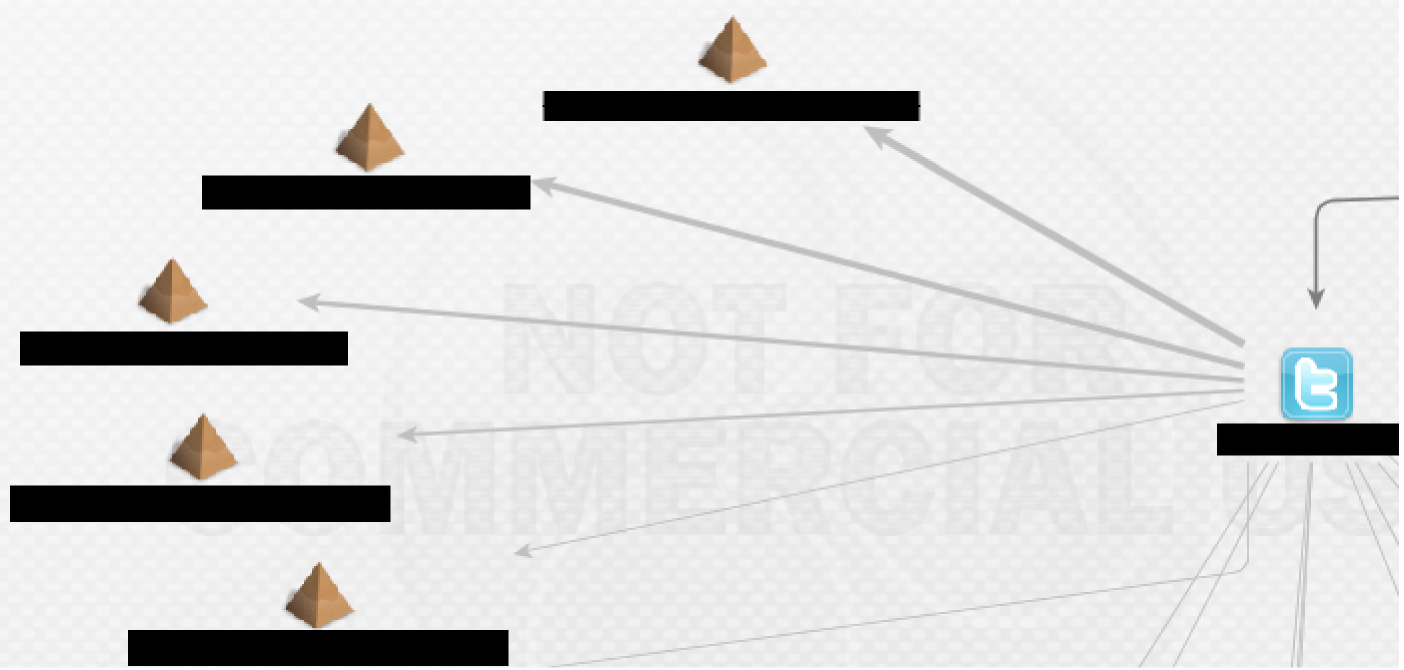
Where the tweets at?

```
for tweet in tweets:
    templist = []
    if tweet.has_key("geo") and tweet['geo']:
      latitude,longitude = tweet['geo'].get("coordinates")
      r = requests.get("http://maps.googleapis.com/maps/api/geocode/json?
      latlng="+str(latitude)+","+str(longitude)+"&sensor=true")
      res = json.loads(r.text)
      try:
        for i in res['results'][0]['address_components']:
          if "neighborhood" in i['types'] or "administrative_area_level_2"
          in i['types'] or "postal_code_suffix" in i['types'] or
           "country" in i['types'] or "postal_code" in i['types']:
            pass
          else:
            templist.append(i['long_name'])
      except:
        pass
```

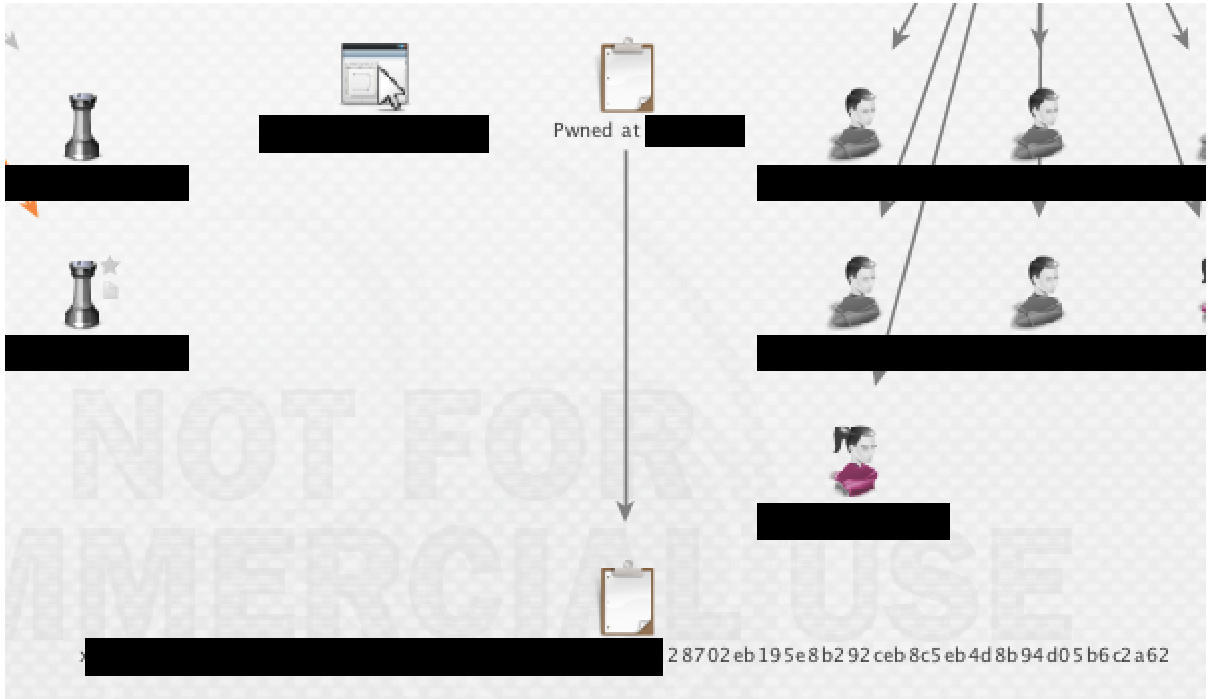
Enriching Maltego

```python
last = Counter(newlist).most_common(5)
x = 5
for address in last:
    ent = me.addEntity("maltego.Location",address[0])
    ent.addAdditionalFields('link#maltego.link.thickness','','',x)
    x = x - 1
```

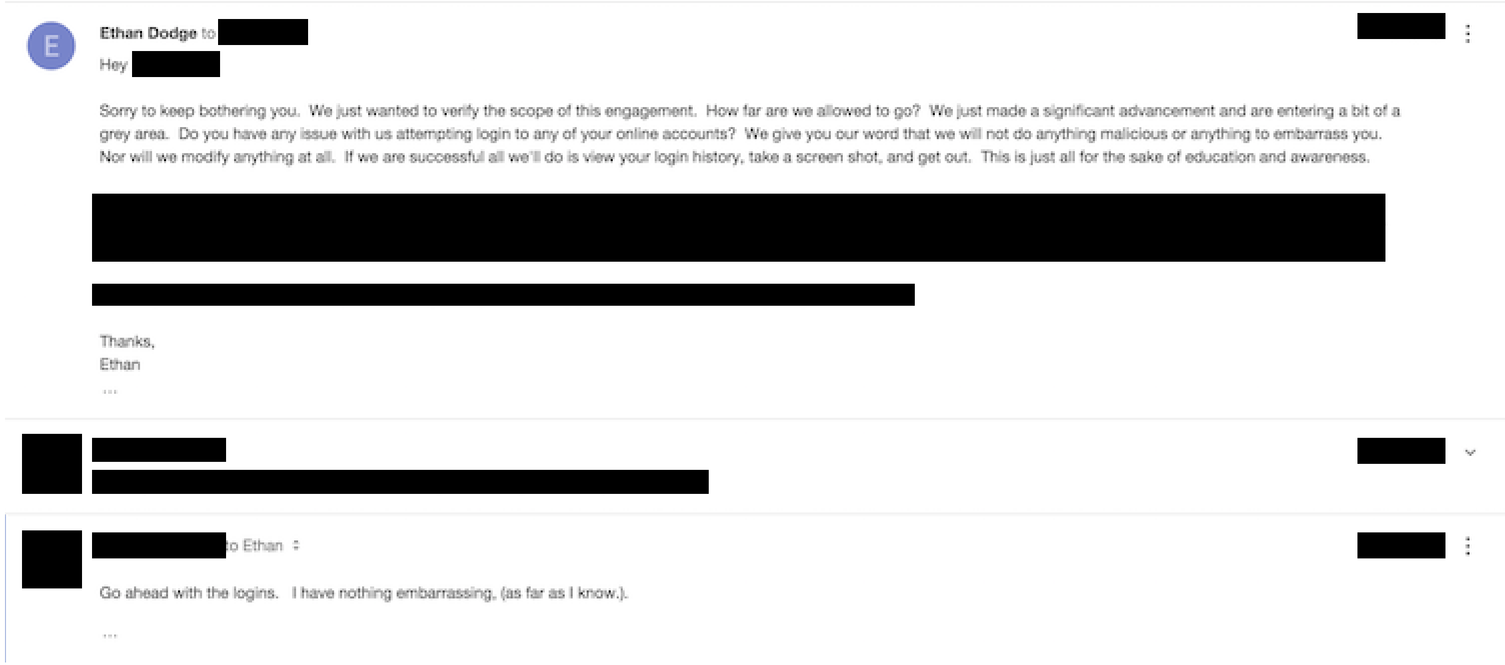
Transform in Action



Then we found this...



```
28702eb195e8b292ceb8c5eb4d8b94d05b6c2a62 SHA1 : 3nd3rwiggin
```



Ethan Dodge to [redacted] [redacted]

Hey [redacted]

Sorry to keep bothering you. We just wanted to verify the scope of this engagement. How far are we allowed to go? We just made a significant advancement and are entering a bit of a grey area. Do you have any issue with us attempting login to any of your online accounts? We give you our word that we will not do anything malicious or anything to embarrass you. Nor will we modify anything at all. If we are successful all we'll do is view your login history, take a screen shot, and get out. This is just all for the sake of education and awareness.

[redacted]

[redacted]

Thanks,
Ethan

...

[redacted] [redacted] [redacted]

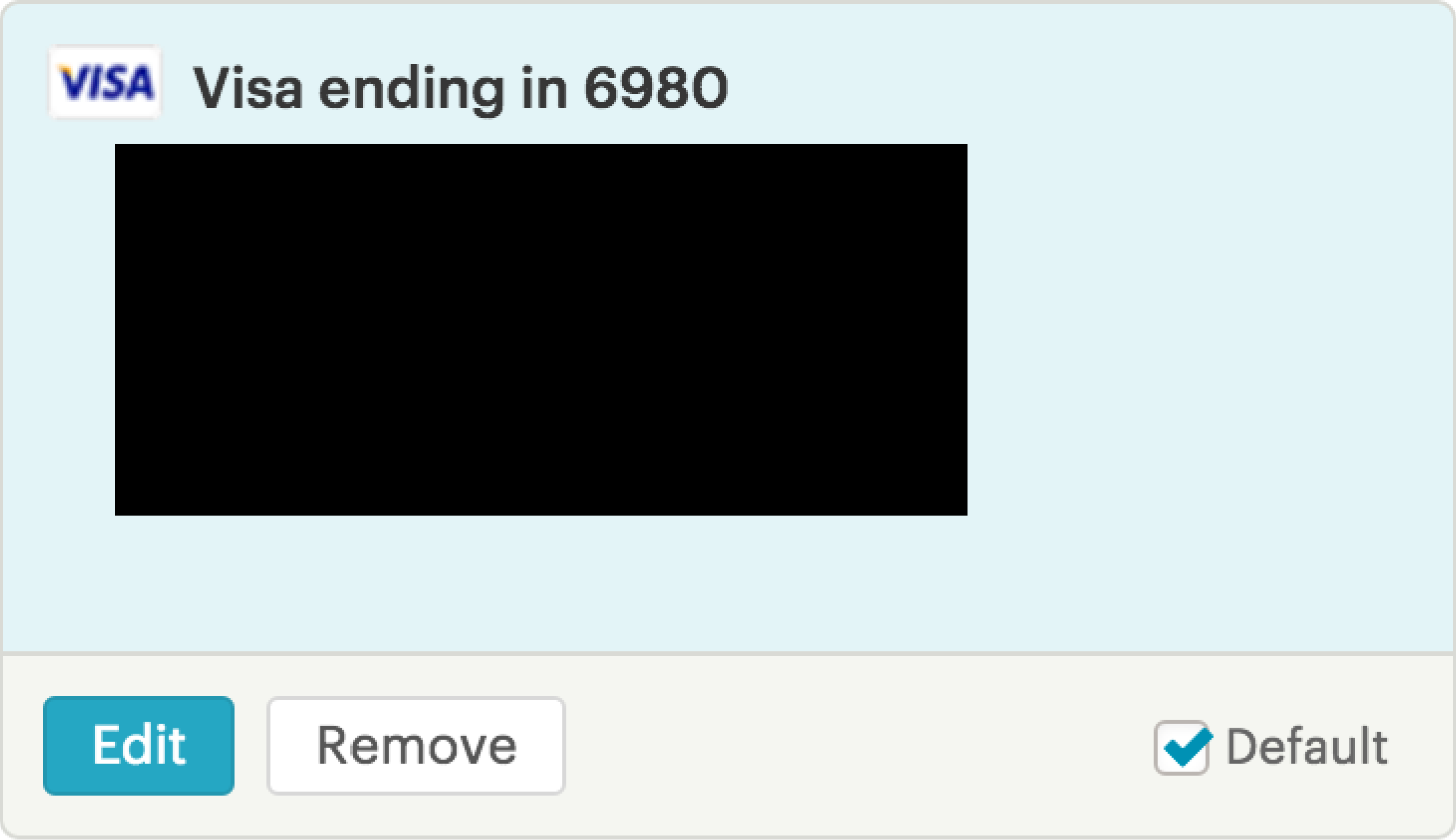
[redacted]

[redacted] [redacted]to Ethan [redacted]

Go ahead with the logins. I have nothing embarrassing, (as far as I know.).

...

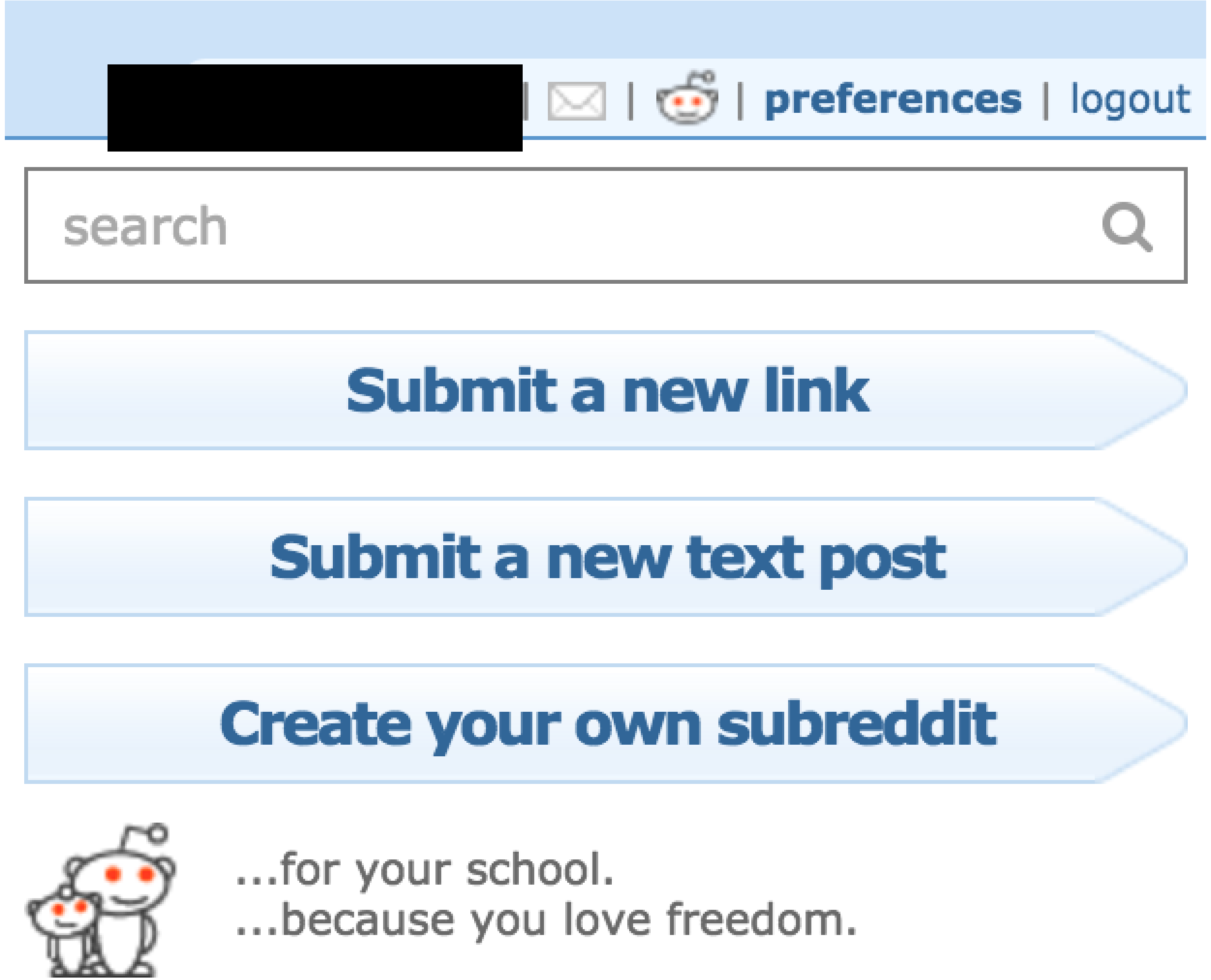
Unique Username = *Win*



Visa ending in 6980

[redacted]

☑ Default


[redacted] | ✉ | | preferences | logout
search
Submit a new link
Submit a new text post
Create your own subreddit

...for your school.
...because you love freedom.

What we found:

Personal

- Home address (Twitter & Etsy)
- Class locations (Twitter)
- Password (Have I Been Pwnd?)
- Close Friends (Twitter & Instagram)
- Job History (LinkedIn & Facebook)
- Home IP Address (Reddit Login History)
- Birthdate (Etsy)
- Barber (Twitter)

What we found:

Personal

Family

- Addresses (Whitepages & Property Records)
- Members (Google+)
- Names (Maltego)

Use Cases

Red Team

PHISH
ALL THE THINGS!
memegenerator.net

ONLY YOU
SMOKEY
CAN PREVENT SOCIAL ENGINEERING
made on imgur

▶ Use Cases

Blue Team

WALK THE LINE

Blue Team

Twitter

- See if public activity is malicious
- Following with competitors?
- Talking with competitors?
- Talking about your brand?

Blue Team

Twitter

Instagram

- Work badges
- Passwords
- Network Diagrams

Blue Team

Twitter

Instagram

Github

» Committed sensitive files

» Committed proprietary code

» Committed company info

Blue Team

Twitter

Instagram

Github

Facebook

» See if public activity is malicious

» Friends with competitors?

» Talking about your brand?

Blue Team

Twitter

Instagram

Github

Facebook

Brand Monitoring

- » Scumblr by Netflix
- » Monitor Forum Chatter
- » Monitor Your Name

Blue Team

Twitter

Instagram

Github

Facebook

Brand Monitoring

Rate Employees

- » Most is going to be accidental
- » Who's your most active employee?
- » Monitor them closer

Blue Team

Twitter

Instagram

Github

Facebook

Brand Monitoring

Rate Employees

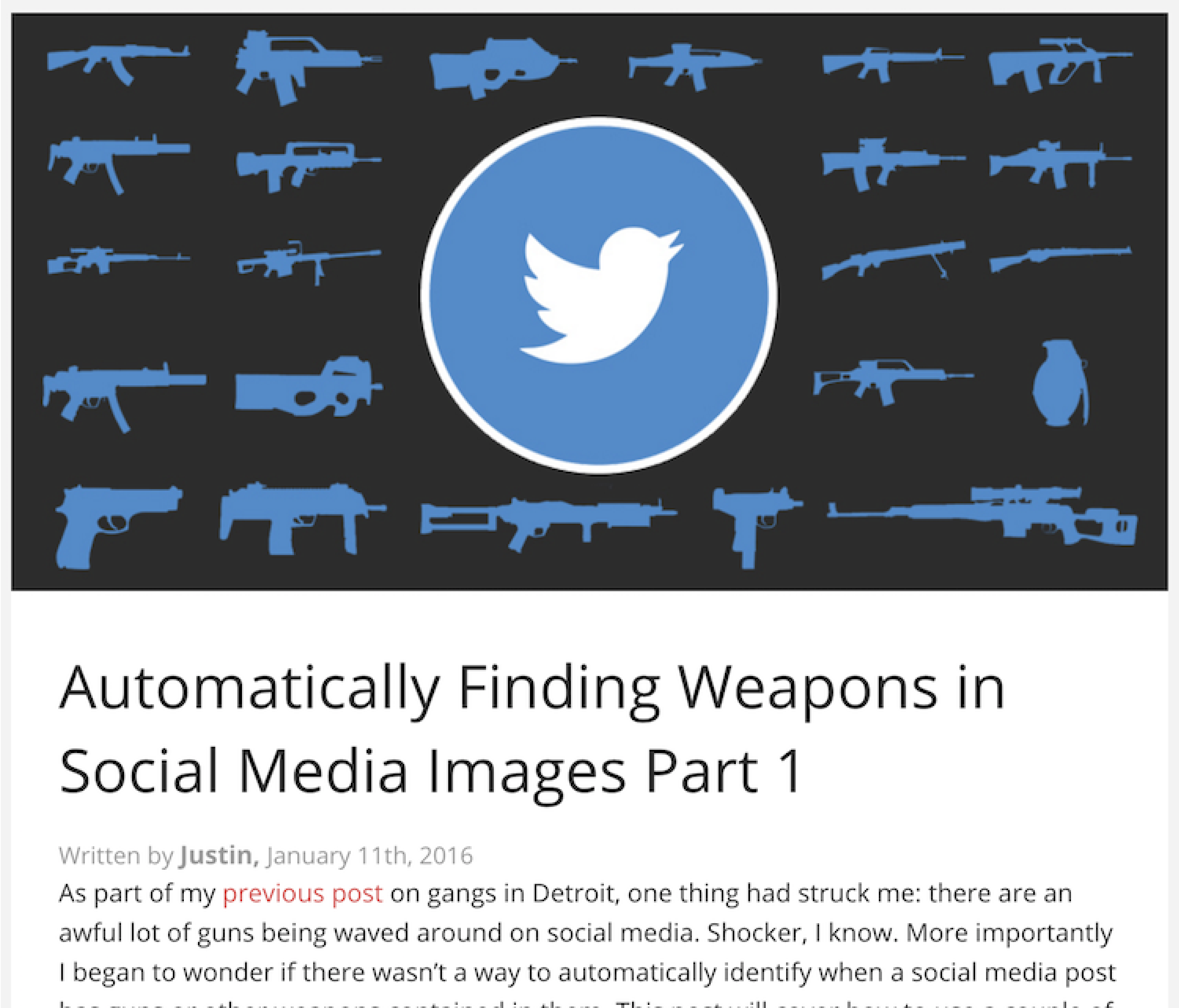
SEIM

» Alert

» Correlate

Interrogator

- Web Application
- Continuous OSINT Monitoring of Workforce
- Visualize relationships with a Graph Database
- Coming mid 2016!



Automatically Finding Weapons in Social Media Images Part 1

Written by **Justin,** January 11th, 2016

As part of my previous post on gangs in Detroit, one thing had struck me: there are an awful lot of guns being waved around on social media. Shocker, I know. More importantly I began to wonder if there wasn't a way to automatically identify when a social media post has guns or other weapons contained in them. This post will cover how to use a couple of

Reccomendations

- Justin Seitz - @jms_dot_py
- The Grugq - @thegrugq
- automatingosint.com
- bellingcat.com

- **Q&A**

Ethan Dodge

@__eth0

ethan@nuna.com

dodgesec.com