A Framework for Analyzing Twitter to Detect Community Crime Activity

Safaa S. Al Dhanhani
@ssdhanhani
Outline

- Why?
- Literature review
- What is the framework
- Approach
- How?
Cont. Outline

- Investigative process
  - Finding suspicious tweets and individuals based on hashtag analysis
  - Classifying the user profile based on Twitter features
  - Identifying influencers in the FOAF networks.
  - Analyzing these influencers.

- Analysis & Results

- Validation

- Conclusion & Future work
Why? Problem Statement

- The increase use of social media increase the **risk** of controlling crimes.
- Increase use of social media for **investigation** by law enforcement agencies
- The massive severity of crime cases drive the need of **continuous monitoring**
- The **challenge** of understanding, **analyzing** and correlate data from social media by investigators.
Literature Review

- Crime detection on weblog
  - Good analytics approach, but no exposure of the tools
- Twitter user account analysis
  - Good study about the account but didn’t analyze criminals accounts
- Detection of events based on twitter communication
  - Giving a good indication about the event, but without exploring impact in the people
- Predicting crime location using linear regression
  - Detection of crime location without indication of the criminals or the time of the crime will happened
Cont. Literature Review

- Detecting crimes based on nodes analysis
  - Manually checking the profiles in Facebook
  - Case study on applying node analytics to find key roles on terrorists network with respect to NATO.
  - Relationships between criminals in the social media, with database provided from police with crimes and related individuals

- Prediction based on sentiment analysis
  - Plays, world cup 2011
  - Crime intensity in cities
    - Good to know which is the most safe cities, but can not define criminals
  - Elections
Current solutions do not support real time analysis

Most solutions used case study to apply analytics approach, but did not explore unknown suspect.

Most researches studied crimes prediction and can not predict suspects or community of interest on a crime.
  - Prediction of crimes did not cover prediction of time.

Most researches did not validate results with another data source or a tool.

Most researches did not profile suspects or criminal behavior.
What? Proposed Framework

Data Source: Twitter API

Data Collection & Sanitization

Storage

Search & Visualization
Data Processing and Analysis

**Collection**
Twitter API, keywords: locations, usernames, hashtags

**Storing Data**
Stored in Elasticsearch and then pushed to Neo4j

**Visualization**
Kibana dashboard utilizes the search, Neo4j presents graph database

**Search**
Elasticsearch, Neo4j

**Intelligence**
Ability to do statistics and prediction

**Parsing & Indexing**
sentiment analysis
Parsing
Indexing

01 02 03 04 05 06
Framework Functionality and Interactions
Approach

Statistical analysis model

Network analysis model
Statistical Analysis Model

- Sample size
- Total number of hits
- Top 15 number of hashtags
- Percentage of each hashtags
- Number of posts per used
- Top shared URLs
- Sentiment analysis for full sample
- Number of tweets per location
Network Analysis Model

- Centrality measures
- Suspicious Community Identification: Degree Centrality
  \[ C_D = d(n_i) = X_{i+} = \sum_j X_{ij} \]
- Suspicious Personal Relationship Identification: Closeness Centrality
- Suspicious Personal Identification: Betweenness Centrality
Approach in Analytics

Statistical analysis

- Sentiment Analysis
- User Classification Analysis
- Detecting automated and non automated accounts
- Verified and non verified accounts
- Personal and non personal accounts
- Hashtag analysis

Network Analysis

- Suspicious personal identification
- Suspicious community topologies
How? Implementation

Elasticsearch Logstash Kibana Stack (ELK)

- Elasticsearch-2.3.5
- Kibana-4.5.3-darwin-x64
- Logstash-2.3.0
- Python 2.7
- Py2neo 2.0.9
- Neo4j-community-3.1.0-rc1
- Alchemyapi sdk

Neo4j – Elasticsearch
Cont. Neo4j Schema

- Relationships:
  - Replies
  - Retweets
  - Mentions
  - Tags
  - Posts

- Entities:
  - Tweet
  - User
  - Hashtag
Questions come to analysts’ minds

Is my analytics accurate?
What makes analysis accurate?

Who are the unknown?
Getting the history of known criminals on Twitter helps to get the related or unknown group to this person. How?

Communication
How many relationships?
How many reply?
How many mentions?
How many posts?

Trends
Common hashtags?
Common active time?, Common posts/timestamp?
Common URLs and media shared?

Psychology
Feeling positive for what?
Feeling negative for what?
Investigation Process

- Finding suspicious tweets and individuals based on hashtag analysis
- Classifying the user profile based on Twitter feature
- Identifying influencers in the FOAF networks of the senders
- Analyzing these influencers.
Example of Hashtag Analysis

Hashtag # of investigator interest
Example: #Daesh

Sentiment analysis of tweet with respect to Hashtag

Dr. Khaled: Safaa are you looking for the happy criminals?
Safaa: No 😊

Happy + #Daesh= supporter or willing to be or is Daesh

Ok, but

False positive due to: Automated account, spam, news
So many accounts to be investigated on.
Classifying Users’ Profile Using Twitter Feature

- Age of account
- Number of followers/ followings
- Number of tweets
- Verified or non-verified account
- Tweet source
Identifying influencers in the FOAF networks of the senders
Analysis and Results

Statistical Model
Analysis and Results

2016
December

2017
January

2017
February

2017
March

71,000

14%
Negative

61%
Neural

24%
Positive

1.99%
Verified accounts
News & celebrities

98.01%
Non-verified Accounts
Spams & personal

422
2287

RSAC
RSAConference 2017 Abu Dhabi
User Classification Analysis

- Number of posts by time indicates the level of activity of the account.
- A uniform pattern indicates type of automation like, API tweets everyday at the same time.
- Non uniform pattern indicates more normal user behavior.
- Random big peaks of activity like 20 or 50 per hour also indicated abnormal behavior.

Results
Analysis and Results

Verified and non verified accounts

- Most users are non verified accounts.
- Most verified accounts are non personal accounts.
- Most verified accounts are automated accounts.

Results
Analysis and Results

Network Model
Which topologies are interesting to be analyzed?

- Star topology
  - Have high degree centrality, but each node connected to one node only!

- Star topology with other connection
  - Still have high degree of centrality and have more connectivity to other nodes!
Network Analysis
Analysis and Results

Degree Centrality

<table>
<thead>
<tr>
<th>n.username</th>
<th>DegreeScore</th>
</tr>
</thead>
<tbody>
<tr>
<td>DaeshCrimes</td>
<td>181</td>
</tr>
<tr>
<td>justasender</td>
<td>163</td>
</tr>
<tr>
<td>DaeshAjl</td>
<td>149</td>
</tr>
<tr>
<td>HewarMaftuh2</td>
<td>105</td>
</tr>
<tr>
<td>iraqmedianet</td>
<td>84</td>
</tr>
<tr>
<td>saudafares</td>
<td>81</td>
</tr>
<tr>
<td>sharjah24</td>
<td>80</td>
</tr>
<tr>
<td>xHollyray</td>
<td>78</td>
</tr>
<tr>
<td>7amdaaah_</td>
<td>65</td>
</tr>
<tr>
<td>ALWATAN_BARQ</td>
<td>65</td>
</tr>
</tbody>
</table>

Query

- Calculating top 10 highest degree on the network.

Neo4j Query: match(n:User)-[r:MENTIONS]-(m:Tweet) return n.username, count(r) as DegreeScore order by DegreeScore desc limit 10;
Analysis and Results

Betweenness Centrality

Query

- Shortest path between users with mentions communication betweenness.

Neo4j Query: MATCH p=allShortestPaths((u:User {username: "A"})-[:Mentions*0..10]-(u2:User {username: "B"})) RETURN p
Betweenness Centrality:

Query

- Shortest path between users with **indirect** communication betweenness.

Neo4j Query: MATCH (cs:User { username:"A" }), (ms:User { username:"B" }), p = shortestPath((cs)-[*] (ms)) WITH p WHERE length(p)> 1 RETURN p;
Betweenness Centrality:

Query

• Shortest path between users with exhausted search for all paths between users (betweenness).

Neo4j Query: MATCH (cs:User { username:"A" }), (ms:User { username:"B" }), p = shortestPath((cs)-[*] (ms)) WITH p WHERE length(p)> 1 RETURN p;
Dr Ernesto: Safaa are the criminals too stupid to say I’m criminal Or posting about themselves?
Safaa: Yes & No
Dr. Ernesto: ok validate it.
A reply from known activist mentioning unknown suspect “I feel bad about “@Suspect”, such a country #UAE against public freedom”

Resulting: UAE hashtag + Negative sentiment results
Validation

Maltego Validation

- Using another communication channel to validate if the twitter analysis is correct.
- Email communication inspection using Maltego
Conclusion & Future work

- Two analytical methodologies to identify influencers in the Twitter network and the relationships between the people of community interest.
- Sentiment improve the quality of data inspection for investigation.
- Having different data sources of communication such as email provides better profiling of the suspects.
- Having different tools of validation provides precise results.
Future Work

- Smart detection of codes used by criminals
- NLP
- Personality analysis
- Adding other data sources (Facebook, LinkedIn, Instagram)
- Better user friendly web interface
- Simpler searching techniques
Demo
Q & A

Thank you