Weakly Supervised Extraction of Cyber Attacks from Twitter with Turkish Tweet Analysis

Outline

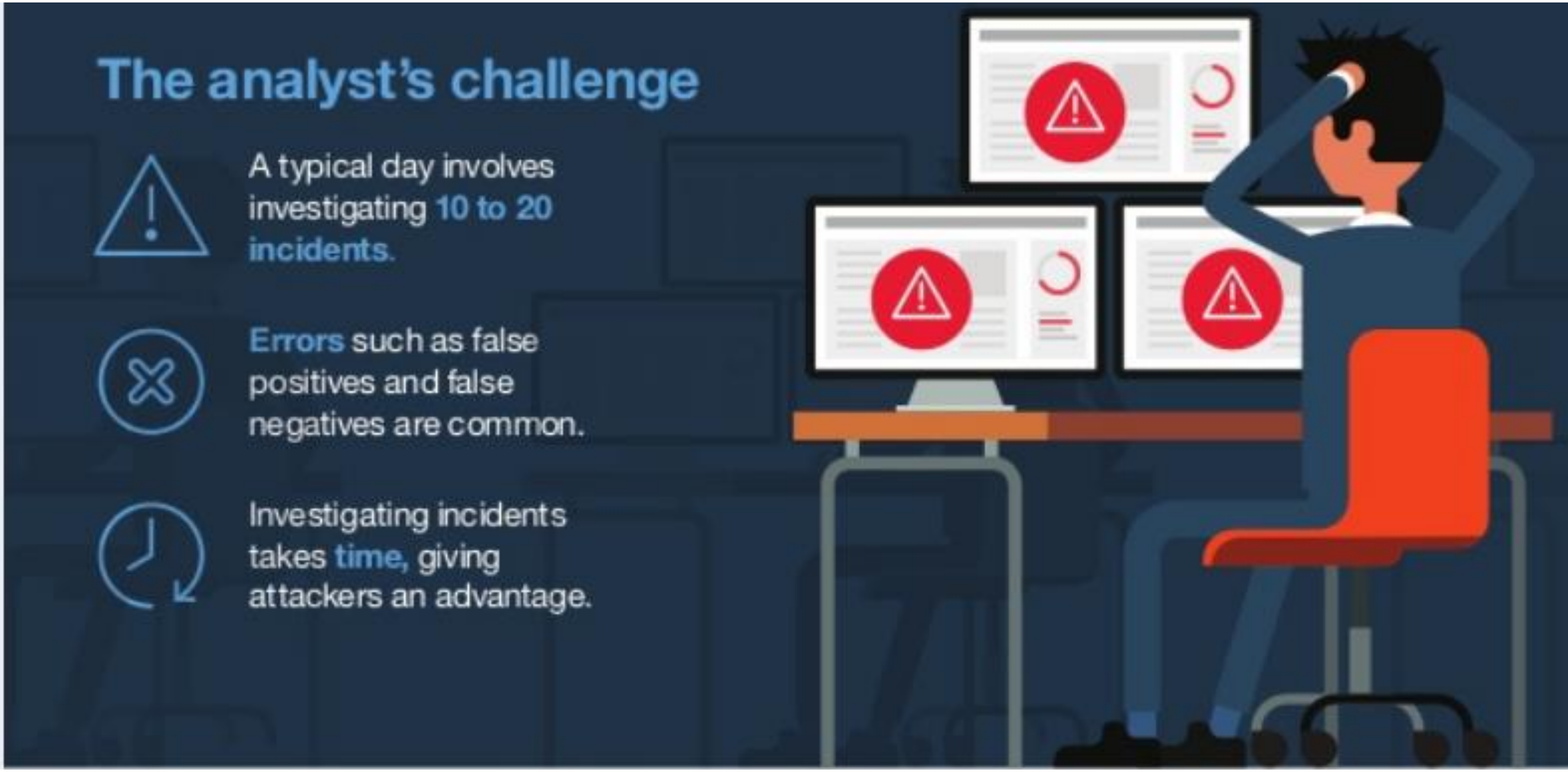
- What is an Information Security Analyst?
- What does an Information Security Analyst do?
- What is Natural Language Processing?
- Why do we need Natural Language Processing?
- Sample Tweets Related with a Security Incident
- Why is NLP Hard?
- Twitter Api
- Contributions

What is an Information Security Analyst?

Key Notes

- An information security analyst is someone who takes measures to protect a company's sensitive and mission-critical data, staying one step ahead of cyber attackers. They do this by coming up with innovative solutions to prevent critical information from being stolen, damaged or compromised by hackers.
- Note the differences between a Security Analyst and a Security Administrator:
  - Security Analysts - are responsible for analyzing data and recommending changes to higher ups, but do not authorize and implement changes. Their main job is keeping attackers out.
  - Security Administrators - ensure that systems are working as designed by making changes, applying patches and setting up new admin users. Their main job is keeping systems up.

What does an Information Security Analyst do?



The analyst's challenge

A typical day involves investigating **10 to 20 incidents**.

Errors such as false positives and false negatives are common.

Investigating incidents takes **time,** giving attackers an advantage.

A day in the life of a threat investigator

Time consuming threat analysis

Rafael
Security Analyst

1 HOUR
Gets caught up on the latest security news through bulletins and social networks in order to identify new threats

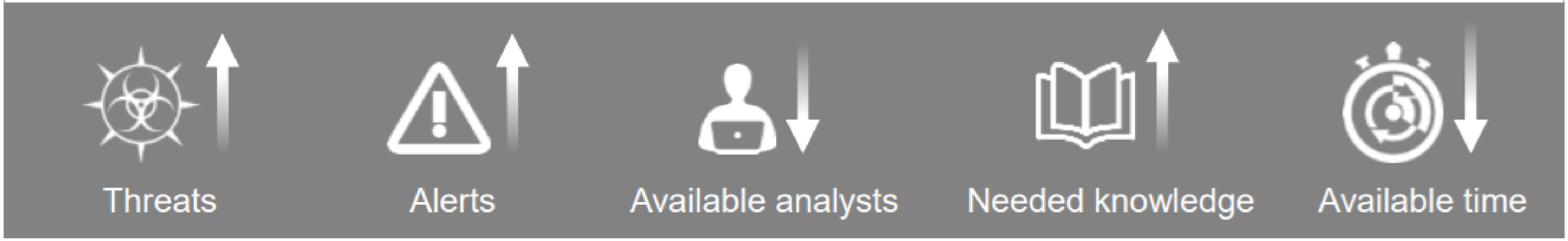
3 HOURS
Repeatedly investigates potential security incidents via online sources

4 HOURS
Manually copies and pastes information from disparate and siloed tools to correlate data

All this mundane time spent and unable to keep up with threats

Is this really sustainable?

Quick Insights: Current Security Status



Threats ↑

Alerts ↑

Available analysts ↓

Needed knowledge ↑

Available time ↓

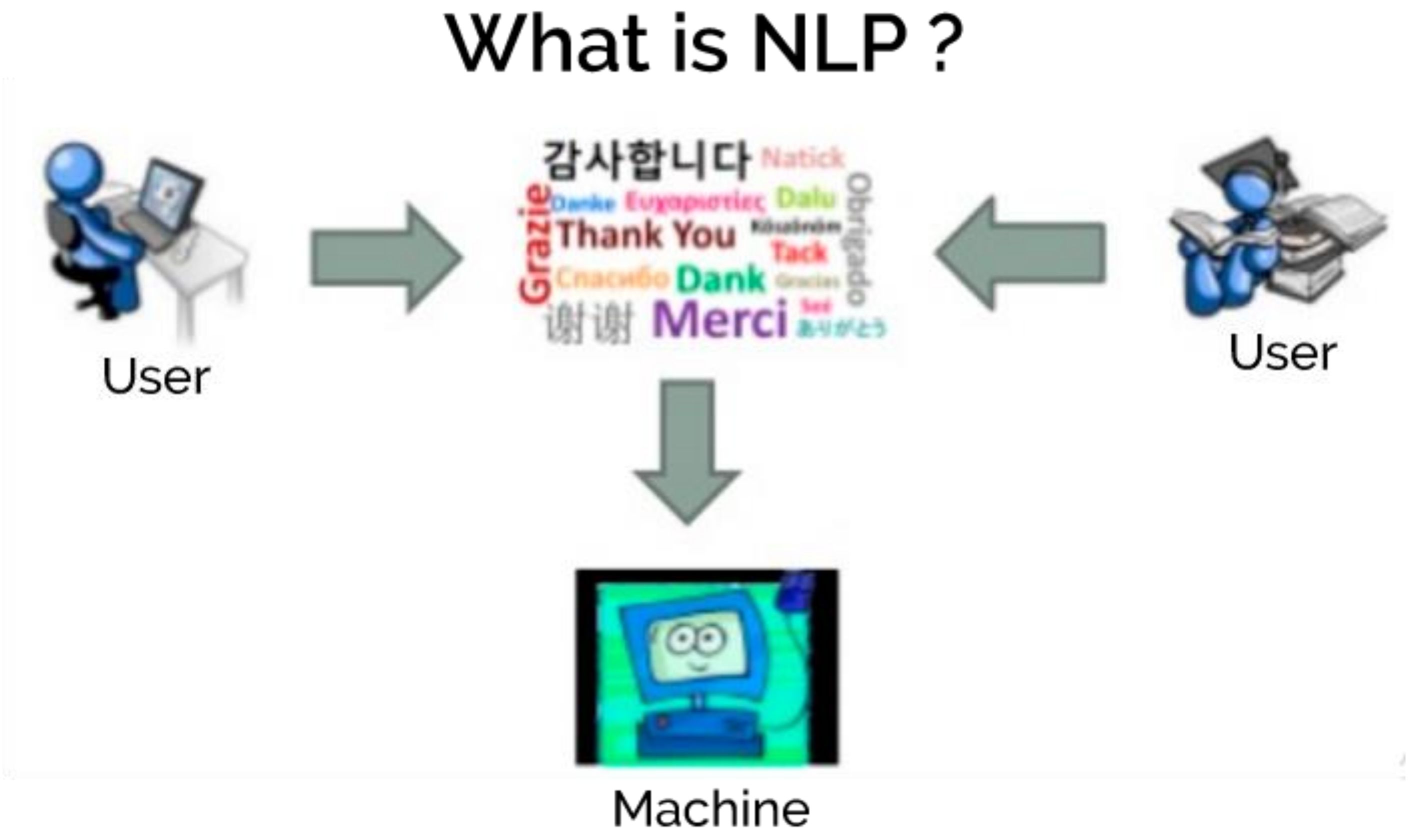
93% SOC managers are not able to triage all potential threats

42% of security professionals ignore a ‘significant number of alerts’

31% of organizations are forced to ignore **50%** or more security alerts because they can’t keep up with volume

What is Natural Language Processing?

Key Notes



Natural Language Processing (NLP) is “ability of machines to understand and interpret human language the way it is written or spoken”.

Why do we need Natural Language Processing?

20% of security data is structured data and **readable by computers.**

200K+ **security events** viewed each day

75K+ reported software **vulnerabilities**

80% of security data is unstructured—created for humans—and **inaccessible to traditional systems.**

A universe of security knowledge, dark to your defenses

Typical organizations **leverage only 8%** of this content.

Why do we need Natural Language Processing?

Intelligence

Interprets unstructured data—created for humans by humans—and correlates it with structured data to uncover new insights.

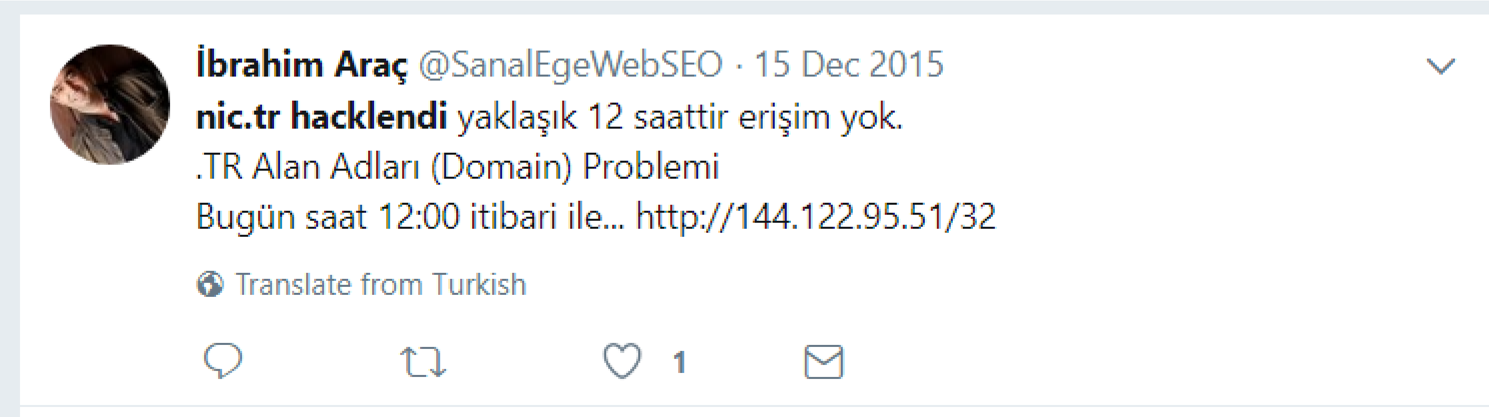
Speed

Connects obscure data points that others miss to accurately identify threats.

Accuracy

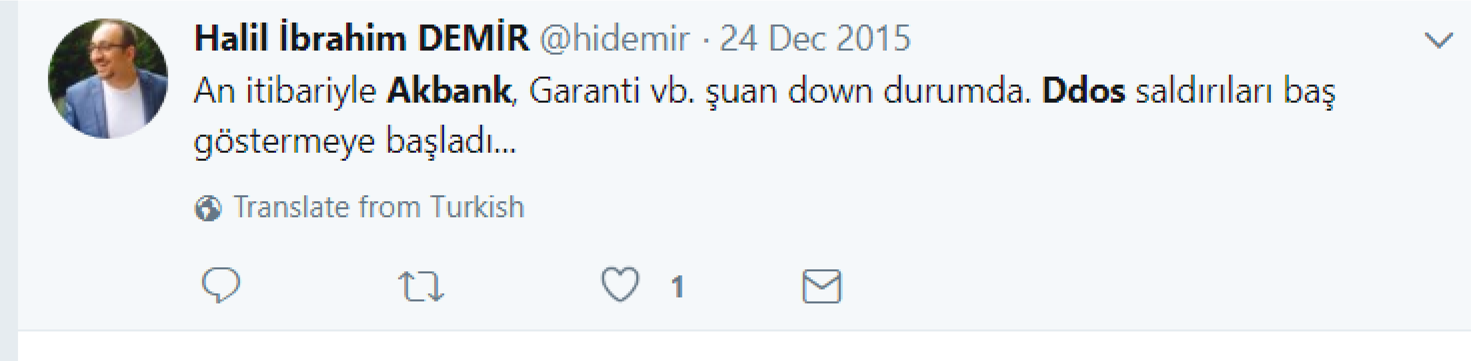
Correctly identifies malicious activity with enriched threat investigation and real-time intelligence.

Sample Tweets After an Attack



İbrahim Araç @SanalEgeWebSEO · 15 Dec 2015

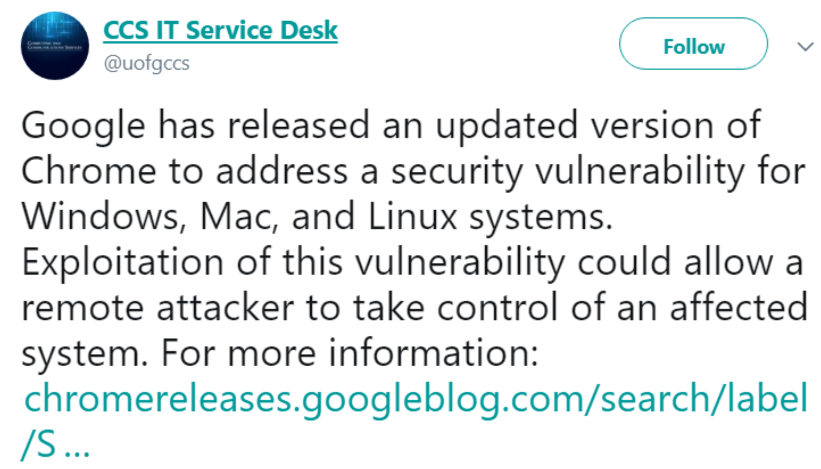
nic.tr hacklendi yaklaşık 12 saattir erişim yok.
.TR Alan Adları (Domain) Problemi
Bugün saat 12:00 itibari ile... http://144.122.95.51/32



Halil İbrahim DEMİR @hidemir · 24 Dec 2015

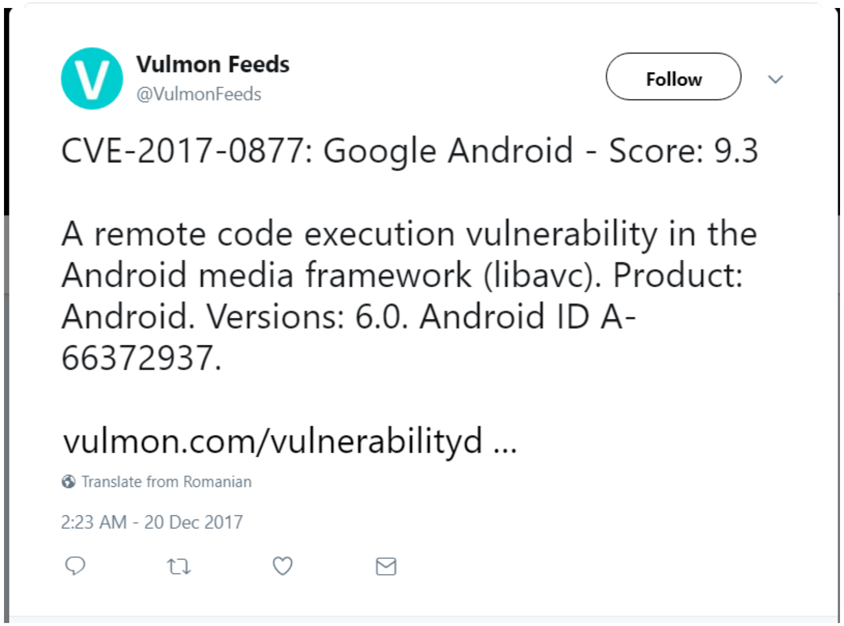
An itibariyle **Akbank**, Garanti vb. şuan down durumda. **Ddos** saldırıları baş göstermeye başladı...

Sample Tweets



CCS IT Service Desk
@uofgccs

Google has released an updated version of Chrome to address a security vulnerability for Windows, Mac, and Linux systems. Exploitation of this vulnerability could allow a remote attacker to take control of an affected system. For more information: chromereleases.googleblog.com/search/label/S ...



Vulmon Feeds
@VulmonFeeds

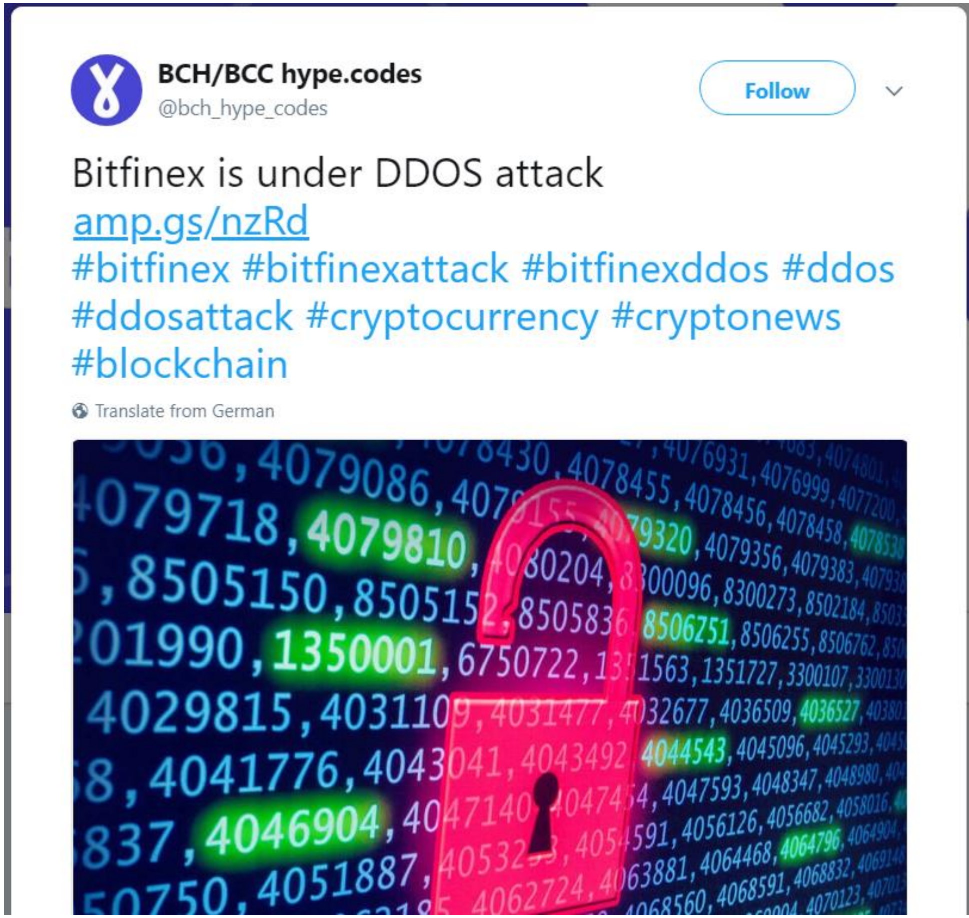
CVE-2017-0877: Google Android - Score: 9.3

A remote code execution vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0. Android ID A-66372937.

vulmon.com/vulnerabilityd ...

Translate from Romanian

2:23 AM - 20 Dec 2017

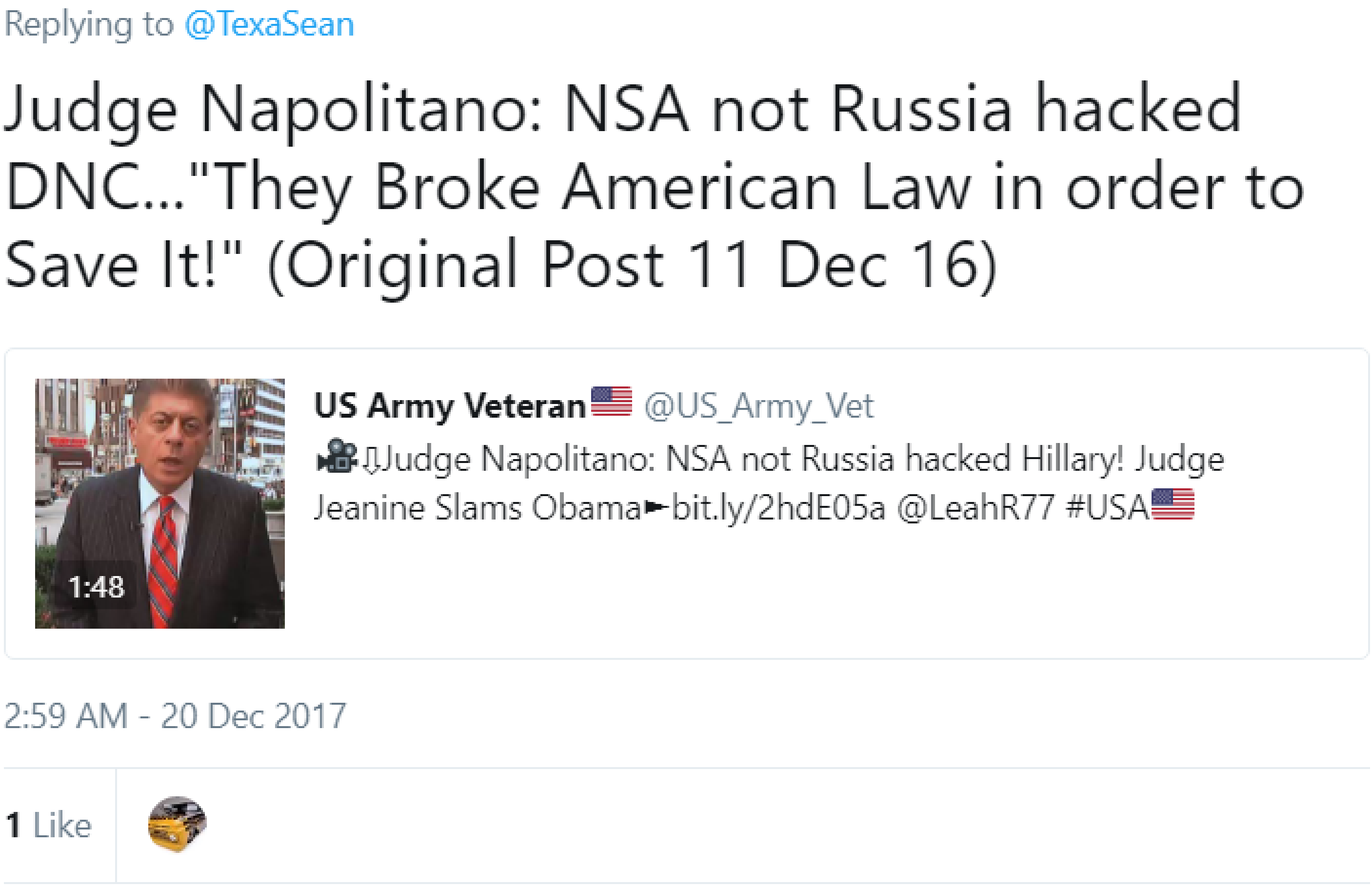


BCH/BCC hype.codes
@bch_hype_codes

Bitfinex is under DDOS attack
amp.gs/nzRd
#bitfinex #bitfinexattack #bitfinexddos #ddos #ddosattack #cryptocurrency #cryptonews #blockchain

Translate from German

Sample False Positive



Replying to @TexaSean

Judge Napolitano: NSA not Russia hacked DNC..."They Broke American Law in order to Save It!" (Original Post 11 Dec 16)

US Army Veteran🇺🇸 @US_Army_Vet

🎥⇩Judge Napolitano: NSA not Russia hacked Hillary! Judge Jeanine Slams Obama►bit.ly/2hdE05a @LeahR77 #USA🇺🇸

2:59 AM - 20 Dec 2017

1 Like

Cognitive Solution

The result

A cognitive solution that learns about security from structured and unstructured information sources, and **empowers security analysts with insights to respond to incidents with speed and accuracy like never before.**

Why is NLP Hard?

Key Notes

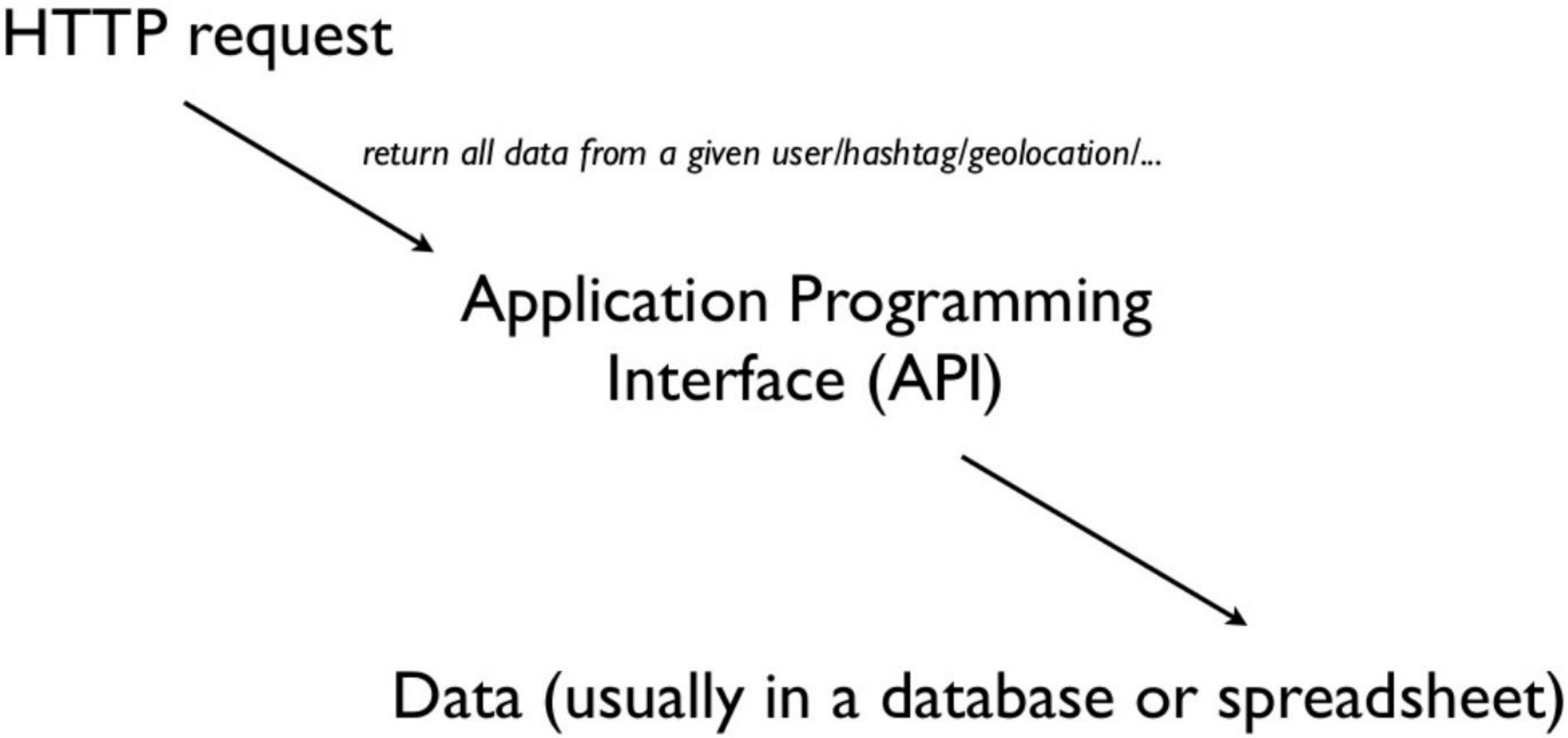
Language is highly ambiguous– it relies on subtle cues and contexts to convey meaning.

Take this simple example: “I love flying planes.”

Do I enjoy participating in the act of piloting an aircraft? Or am I expressing an appreciation for man-made vehicles engaged in movement through the air on wings?

A single sentence can carry different meanings. After thousands of years of evolution, languages have evolved to become shorter and less explicit. For humans, this is very efficient.

Extracting Twitter Data



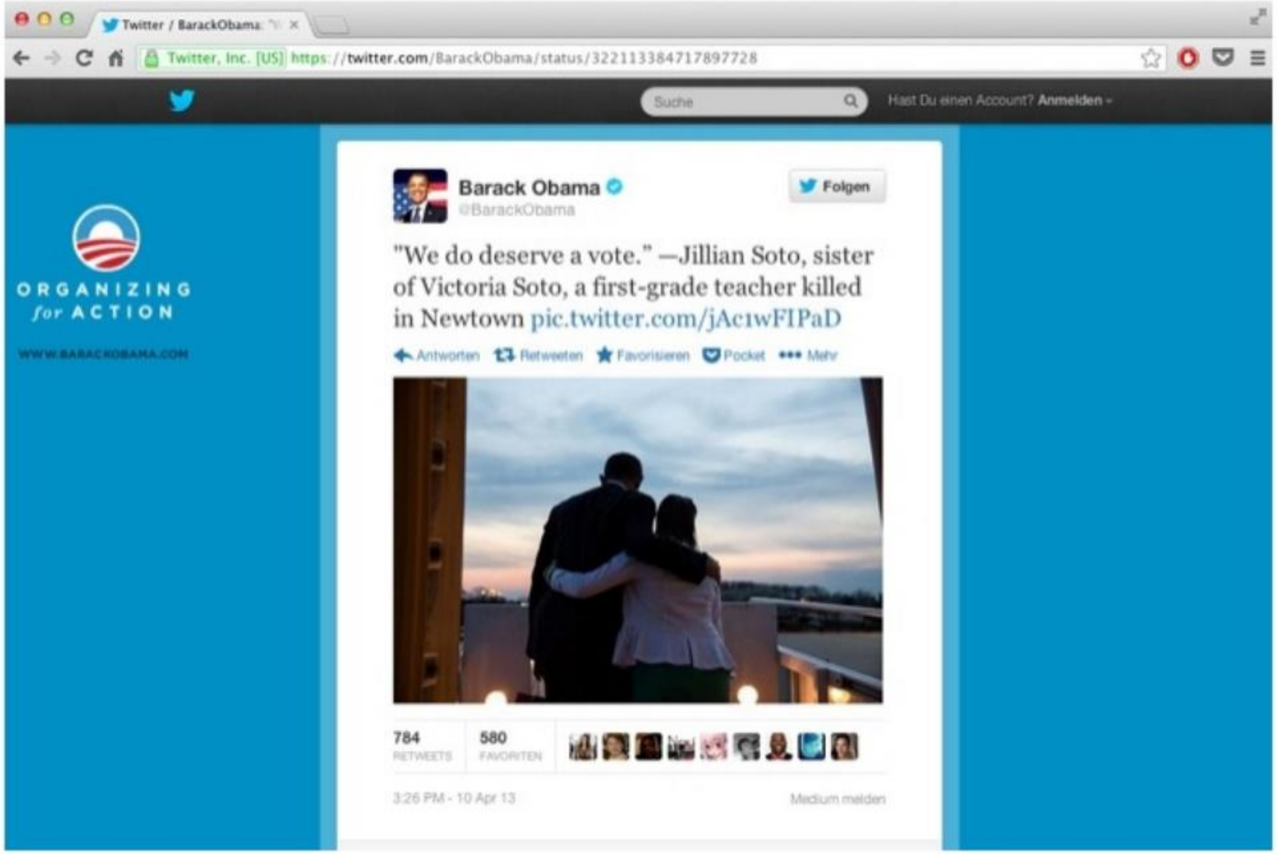
HTTP request

return all data from a given user/hashtag/geolocation/...

Application Programming Interface (API)

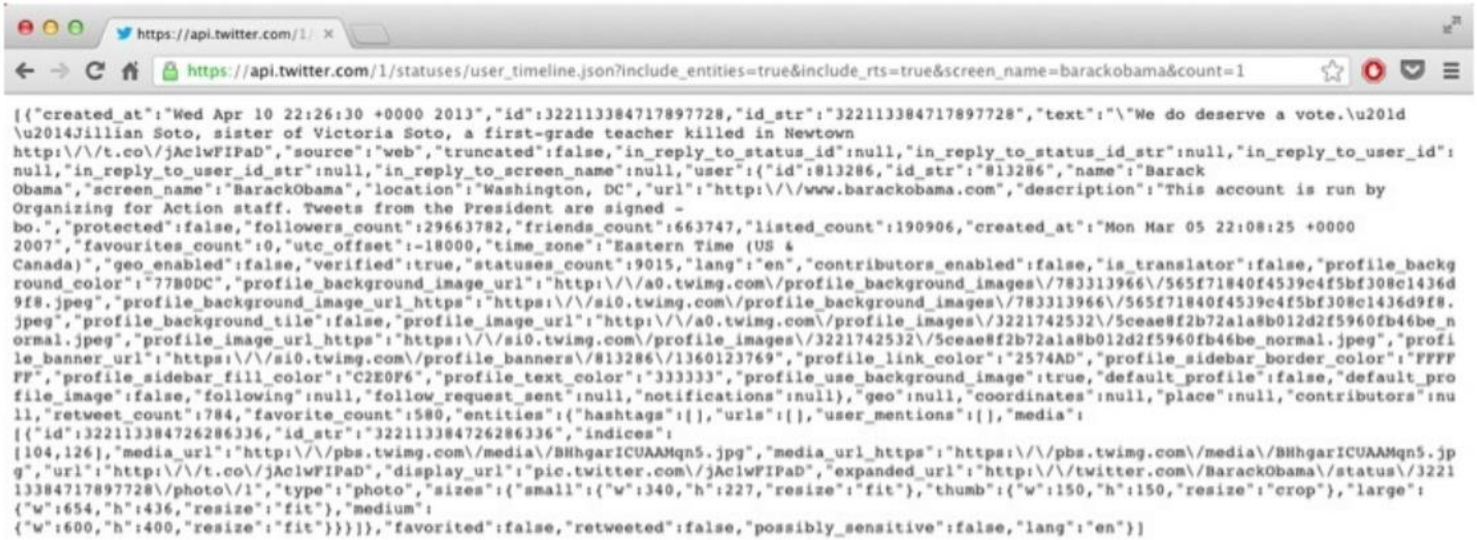
Data (usually in a database or spreadsheet)

Tweet in browser


Twitter / BarackObama
Twitter, Inc. [US] https://twitter.com/BarackObama/status/322113384717897728
Suche
Hast Du einen Account? Anmelden
ORGANIZING for ACTION
WWW.BARACKOBAMA.COM
Barack Obama
@BarackObama
Folgen

"We do deserve a vote." —Jillian Soto, sister of Victoria Soto, a first-grade teacher killed in Newtown pic.twitter.com/jAc1wFIPaD

Tweet source via API


https://api.twitter.com/1/
https://api.twitter.com/1/statuses/user_timeline.json?include_entities=true&include_rts=true&screen_name=barackobama&count=1

```
[{"created_at":"Wed Apr 10 22:26:30 +0000 2013","id":322113384717897728,"id_str":"322113384717897728","text":"\"We do deserve a vote.\u201d
\u2014Jillian Soto, sister of Victoria Soto, a first-grade teacher killed in Newtown
http:\/\/t.co\/jAc1wFIPaD","source":"web","truncated":false,"in_reply_to_status_id":null,"in_reply_to_status_id_str":null,"in_reply_to_user_id":
null,"in_reply_to_user_id_str":null,"in_reply_to_screen_name":null,"user":{"id":813286,"id_str":"813286","name":"Barack
Obama","screen_name":"BarackObama","location":"Washington, DC","url":"http:\/\/www.barackobama.com","description":"This account is run by
Organizing for Action staff. Tweets from the President are signed -
bo.","protected":false,"followers_count":29663782,"friends_count":663747,"listed_count":190906,"created_at":"Mon Mar 05 22:08:25 +0000
2007","favourites_count":0,"utc_offset":-18000,"time_zone":"Eastern Time (US &
Canada)","geo_enabled":false,"verified":true,"statuses_count":9015,"lang":"en","contributors_enabled":false,"is_translator":false,"profile_backg
round_color":"77B0DC","profile_background_image_url":"http:\/\/a0.twimg.com\/profile_background_images\/783313966\/565f71840f4539c4f5bf308c1436d
9f8.jpeg","profile_background_image_url_https":"https:\/\/si0.twimg.com\/profile_background_images\/783313966\/565f71840f4539c4f5bf308c1436d9f8.
jpeg","profile_background_tile":false,"profile_image_url":"http:\/\/a0.twimg.com\/profile_images\/3221742532\/5ceae8f2b72a1a8b012d2f5960fb46be_n
ormal.jpeg","profile_image_url_https":"https:\/\/si0.twimg.com\/profile_images\/3221742532\/5ceae8f2b72a1a8b012d2f5960fb46be_normal.jpeg","profi
le_banner_url":"https:\/\/si0.twimg.com\/profile_banners\/813286\/1360123769","profile_link_color":"2574AD","profile_sidebar_border_color":"FFFF
FF","profile_sidebar_fill_color":"C2E0F6","profile_text_color":"333333","profile_use_background_image":true,"default_profile":false,"default_pro
file_image":false,"following":null,"follow_request_sent":null,"notifications":null},"geo":null,"coordinates":null,"place":null,"contributors":nu
ll,"retweet_count":784,"favorite_count":580,"entities":{"hashtags":[],"urls":[],"user_mentions":[],"media":
[{"id":322113384726286336,"id_str":"322113384726286336","indices":
[104,126],"media_url":"http:\/\/pbs.twimg.com\/media\/BHhgarICUAAMqn5.jpg","media_url_https":"https:\/\/pbs.twimg.com\/media\/BHhgarICUAAMqn5.jp
g","url":"http:\/\/t.co\/jAc1wFIPaD","display_url":"pic.twitter.com\/jAc1wFIPaD","expanded_url":"http:\/\/twitter.com\/BarackObama\/status\/3221
13384717897728\/photo\/1","type":"photo","sizes":{"small":{"w":340,"h":227,"resize":"fit"},"thumb":{"w":150,"h":150,"resize":"crop"},"large":
{"w":654,"h":436,"resize":"fit"},"medium":
{"w":600,"h":400,"resize":"fit"}}}]},"favorited":false,"retweeted":false,"possibly_sensitive":false,"lang":"en"}]
```

Sampling approaches

Strategy #1: Sample by hashtag, keyword, user, geographical location, or other filtering parameters

+ representativeness unclear on multiple levels

- time frame and parameters have to be carefully chosen

Strategy #2: Use the 1% or 10% sample provided by the Streaming API

+ generally assumed to be representative (of Twitter)

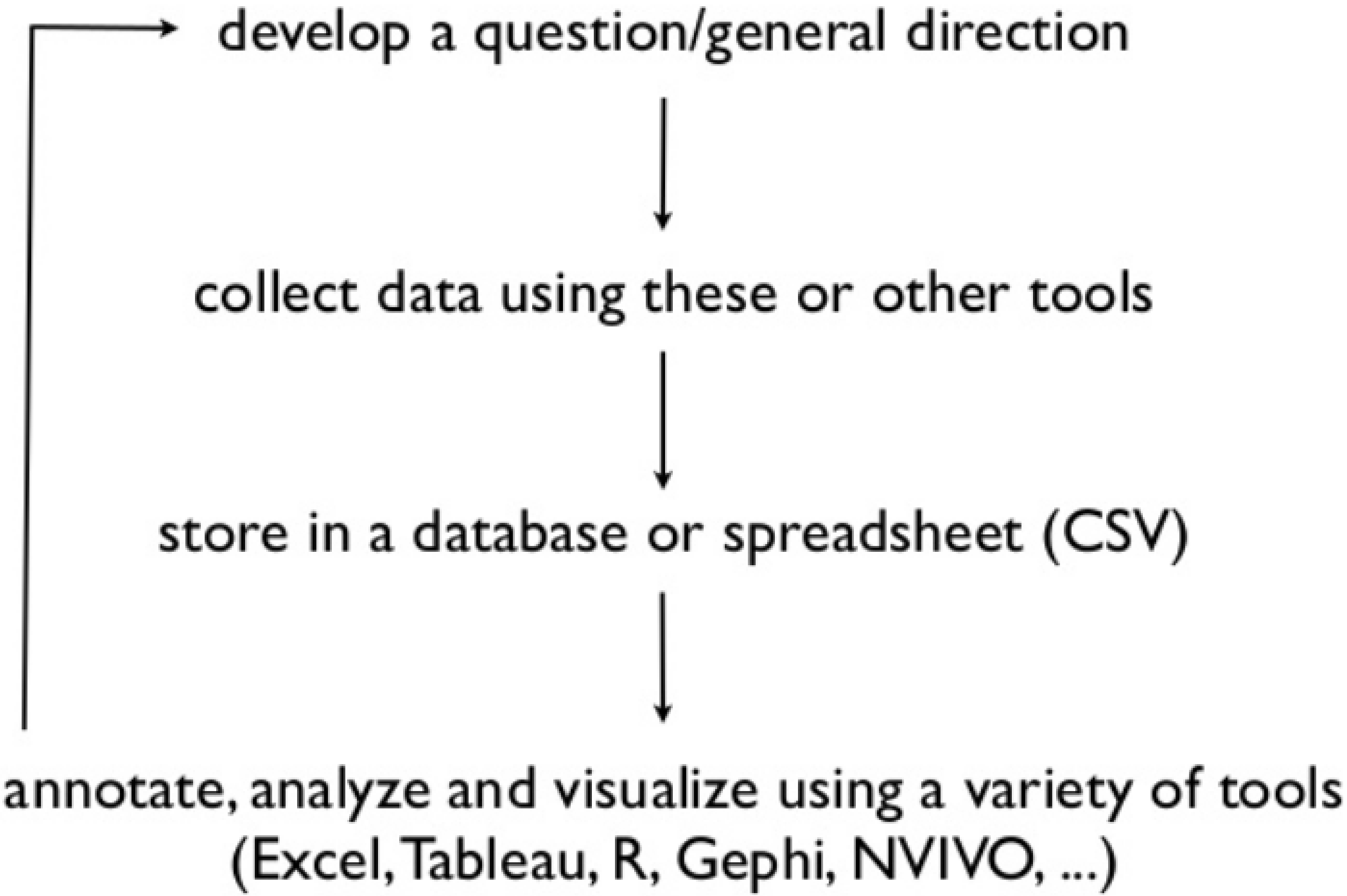
- time frame has to be carefully chosen

Strategy #3: Capture Twitter's entire throughput

+ highly representative (of Twitter)

- technically very difficult/costly

Extracting Twitter Data

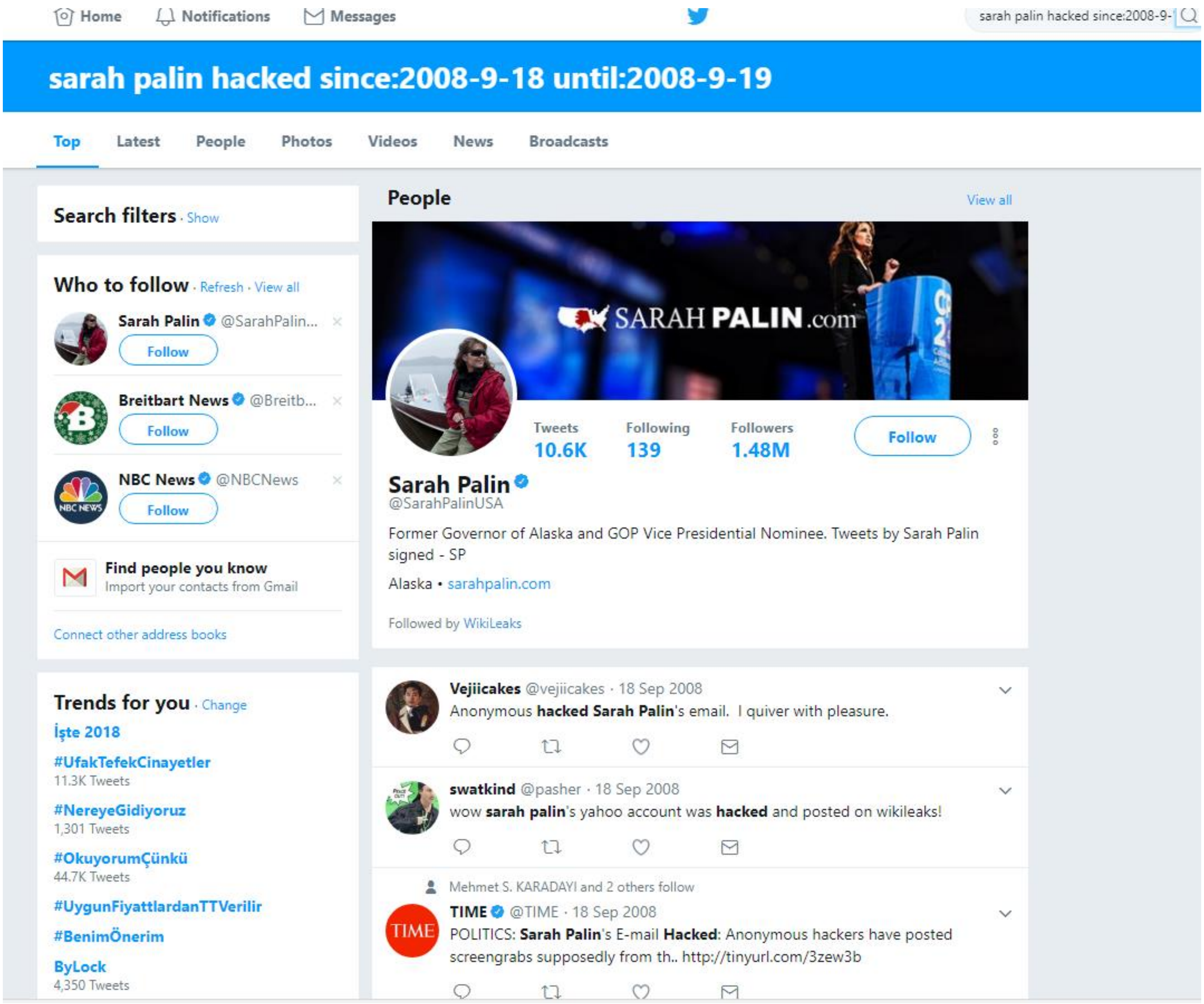


develop a question/general direction

collect data using these or other tools

store in a database or spreadsheet (CSV)

annotate, analyze and visualize using a variety of tools
(Excel, Tableau, R, Gephi, NVIVO, ...)



sarah palin hacked since:2008-9-18 until:2008-9-19

Search filters · Show

Who to follow · Refresh · View all

Sarah Palin @SarahPalin...
Follow

Breitbart News @Breitb...
Follow

NBC News @NBCNews
Follow

Find people you know
Import your contacts from Gmail

Connect other address books

Trends for you · Change

İşte 2018

#UfakTefekCinayetler
11.3K Tweets

#NereyeGidiyoruz
1,301 Tweets

#OkuyorumÇünkü
44.7K Tweets

#UygunFiyattlardanTTVerilir

#BenimÖnerim

ByLock
4,350 Tweets

People · View all

Tweets	Following	Followers
10.6K	139	1.48M

Follow

Sarah Palin
@SarahPalinUSA

Former Governor of Alaska and GOP Vice Presidential Nominee. Tweets by Sarah Palin signed - SP

Alaska • sarahpalin.com

Followed by WikiLeaks

Vejiicakes @vejiicakes · 18 Sep 2008
Anonymous **hacked Sarah Palin**'s email. I quiver with pleasure.

swatkind @pasher · 18 Sep 2008
wow **sarah palin**'s yahoo account was **hacked** and posted on wikileaks!

Mehmet S. KARADAYI and 2 others follow

TIME @TIME · 18 Sep 2008
POLITICS: **Sarah Palin**'s E-mail **Hacked**: Anonymous hackers have posted screengrabs supposedly from th.. http://tinyurl.com/3zew3b

Weekly Supervised Relation Extraction

Related Work

- There has been substantial amount of work on weakly supervised relation extraction.

- Most previous work has focused on extracting static relations which remain relatively constant over time, for instance book authors, class/instance pairs, named entities or hypernyms.

- Previous work on relation extraction has also addressed the challenge of false-negatives in weakly supervised learning.

Related Work

Weekly Supervised Relation Extraction

- There has been much less work in contrast on weakly supervised event extraction
- There are hundreds of thousands of sentences on the web which mention William Shakespeare as the author of Comedy of Errors, or that Nirvana plays grunge music, however there are typically only one or a handful of news articles that report on a specific event, such as a DoS attack.
- Social media, however greatly lowers the barrier to publishing making it easy for anyone to comment on events as they take place. This leads to substantial redundancy of information, as many users will typically comment on events of interest.
- This redundancy on Twitter makes seed-based weakly supervised event extraction a feasible task because it is easy to find a large number of event mentions for an event category given a few seed instances.

Related Work

Event Extraction

- There has been growing interest in information extraction and event identification in Social Media

- In contrast to previous work on event identification in social media, we take a weakly supervised approach to extracting focused event categories where only a few seed instances are provided. We also are the first to demonstrate the prevalence of security-related events reported on Twitter, and investigate how to automatically detect them.

- A small amount of recent work has explored extracting security related information from text, such as understanding software vulnerability ontologies.

Contributions

Key Notes

- Demonstrate that social media is a valuable resource for information on security related events.

- Present a novel approach to extracting focused events from Twitter which requires only minimal supervision for each new event category.

- **Turkish** Tweet Analysis

- What is an Information Security Analyst?
- What does an Information Security Analyst do?
- What is Natural Language Processing?
- Why do we need Natural Language Processing?
- Sample Tweets Related with a Security Incident.
- Why is NLP Hard?
- Twitter Api
- Contributions

Thank you!

Questions and Answers

References

- R. Heatherly, M. Kantarcioglu, and B. Thuraisingham. Preventing private information inference attacks on social networks. Knowledge and Data Engineering, IEEE Transactions on, 25(8):1849–1862, 2013.
- https://www.ibm.com/security/cognitive
- https://securityintelligence.com/events/cybersecurity-cognitive-era-priming-digital-immune-system/
- http://www.ling.helsinki.fi/kit/2008s/clt231/nltk-0.9.5/doc/en/book.html
- https://adeshpande3.github.io/adeshpande3.github.io/Deep-Learning-Research-Review-Week-3-Natural-Language-Processing