



USING ONLINE ACTIVITY AS DIGITAL FINGERPRINTS TO CREATE A BETTER SPEAR PHISHER

Joaquim Espinhara & Ulisses Albuquerque



SMART SECURITY ON DEMAND

Agenda

- Introduction
- Motivation
- Background
- HowStuffWorks
- μphisher
- Demo
- Future Work
- Conclusion

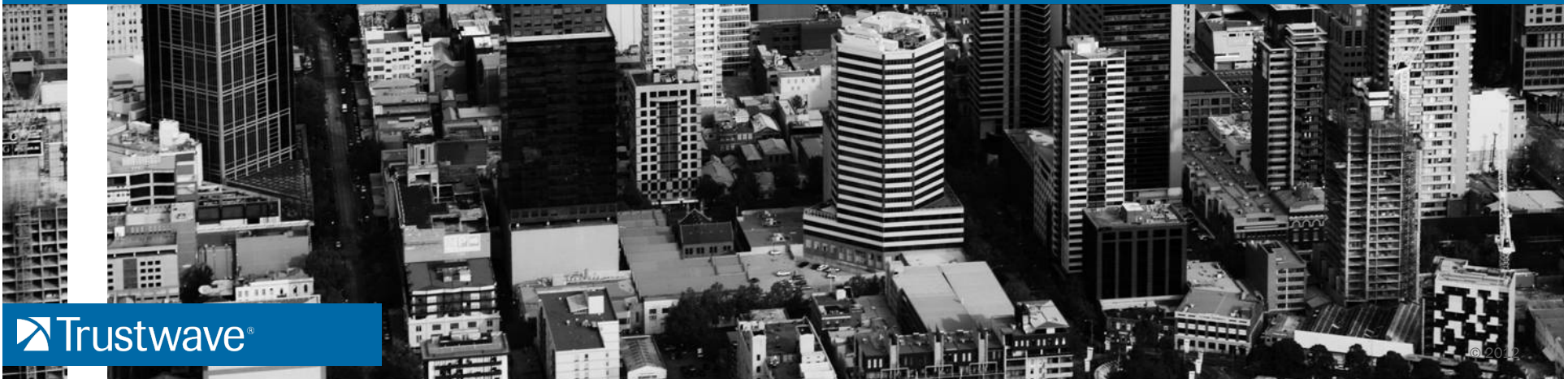


About Us

- Joaquim Espinhara
 - Security Consultant at Trustwave Spiderlabs
- Ulisses Albuquerque
 - Coder for offense & defense... as long as it's fun!
 - Lab Manager at Trustwave Spiderlabs

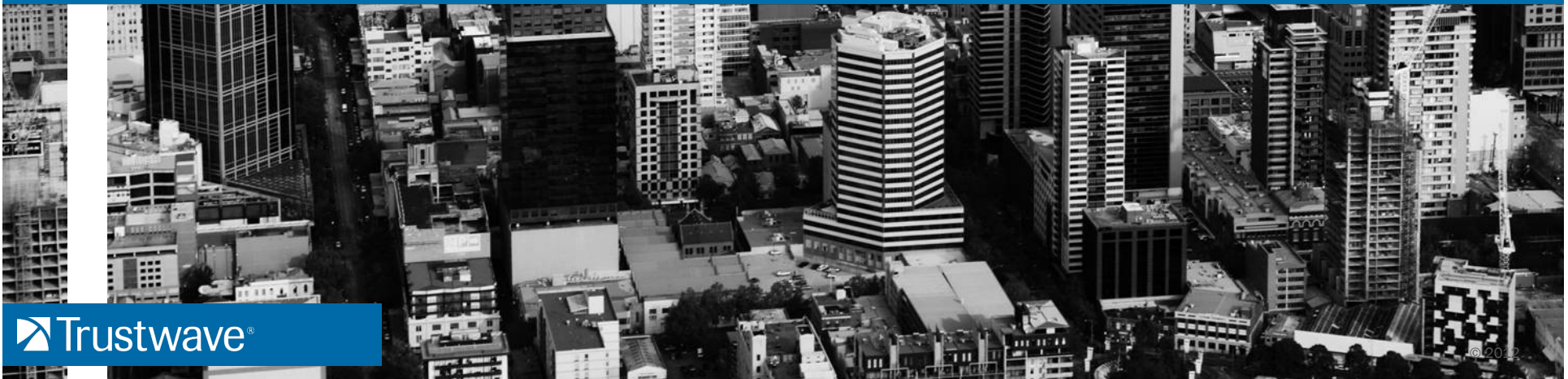


INTRODUCTION





OUR MOTIVATION



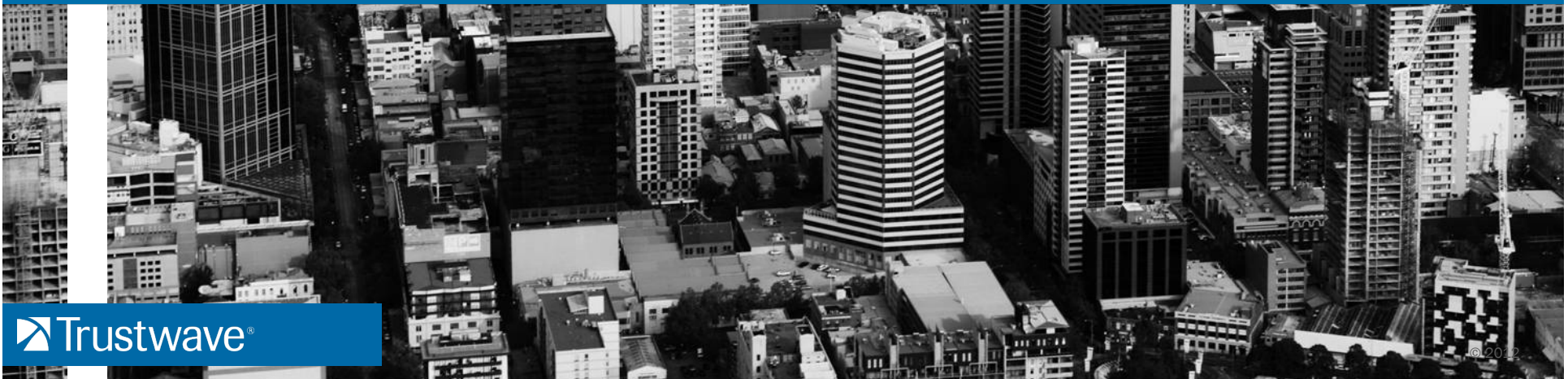


Our Motivation

- Why?
- Tools available



BACKGROUND



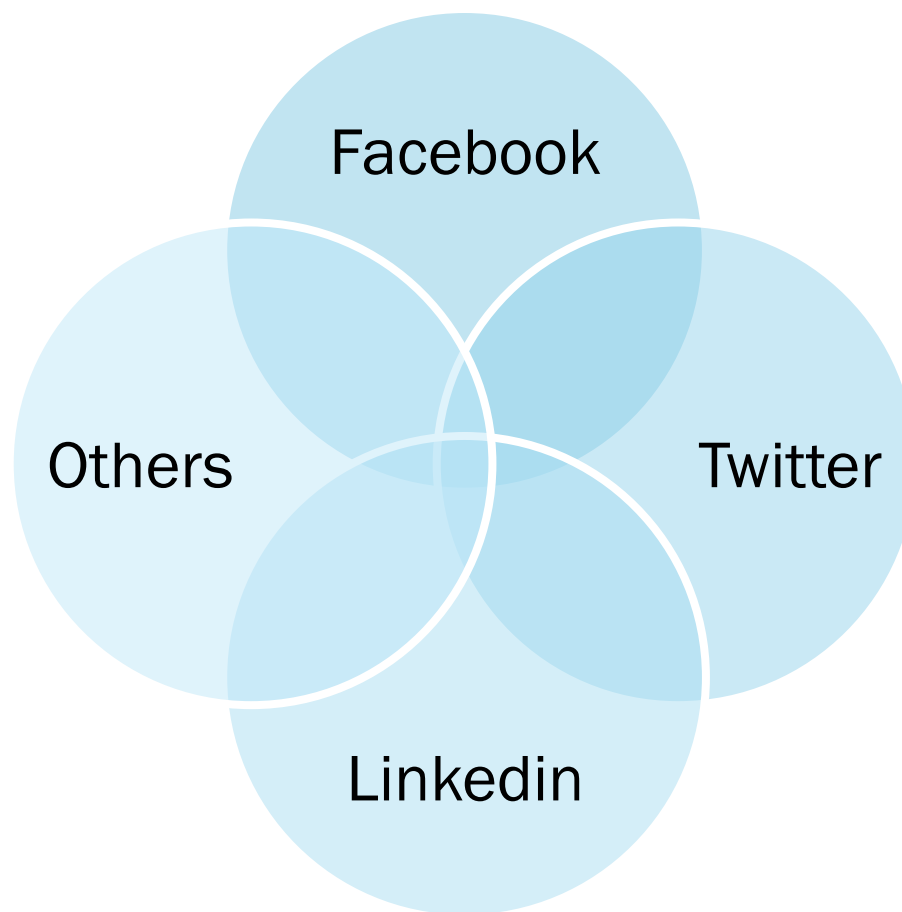


Background

- Social Networks
- Social Engineering
- Data Pre-processing
- Natural Language Processing (NLP)

Background

Social Networks





Background

Social Networks

- Communication channel for keeping in touch with someone (Facebook, Twitter)
- Media sharing (Instagram)
- Specialized networks (GetGlue, Triplt, LastFM, LinkedIn)

Background

Social Engineering

- Phishing





Background

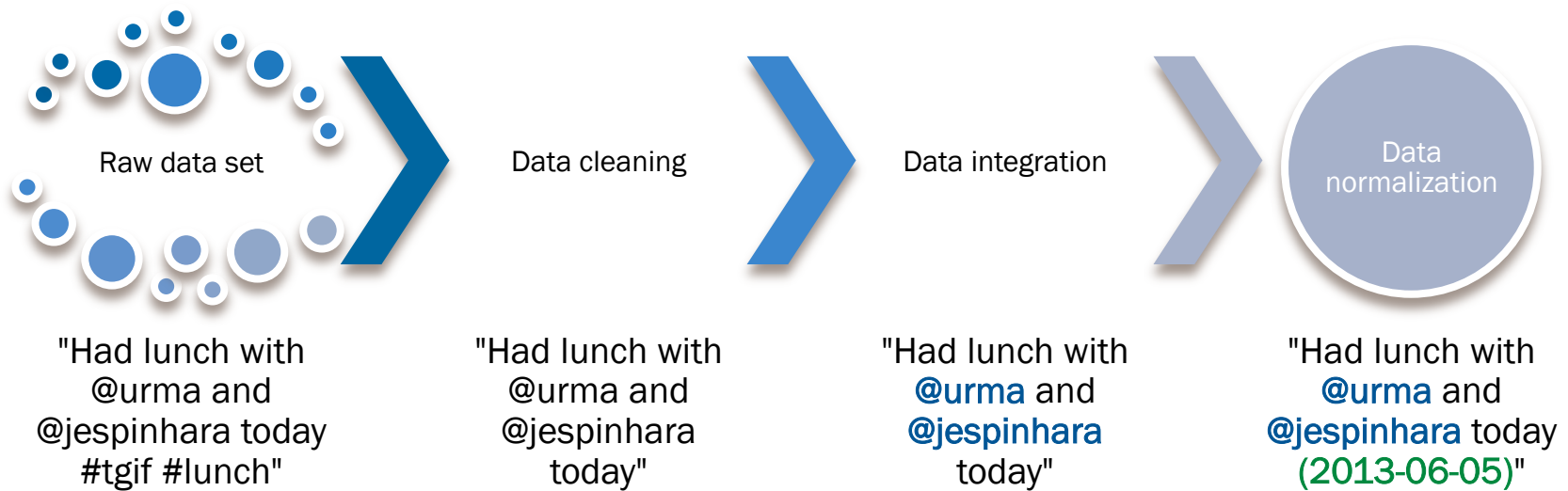
Data Pre-processing

- What is it?
- How do we use it?

Background

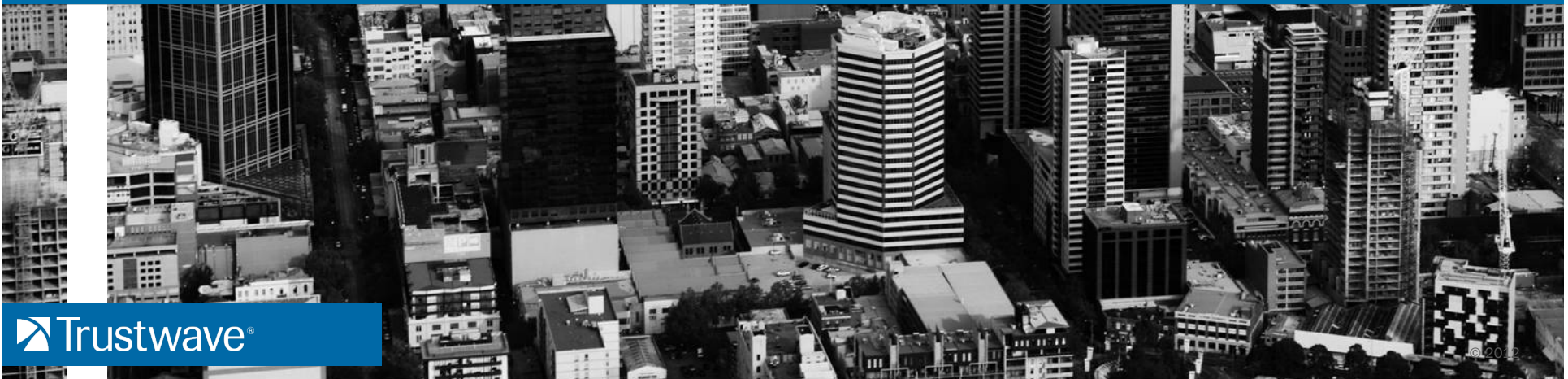
Data Pre-processing

- Data Pre-processing Flow





HOWSTUFFWORKS



HOWSTUFFWORKS

Our Approach

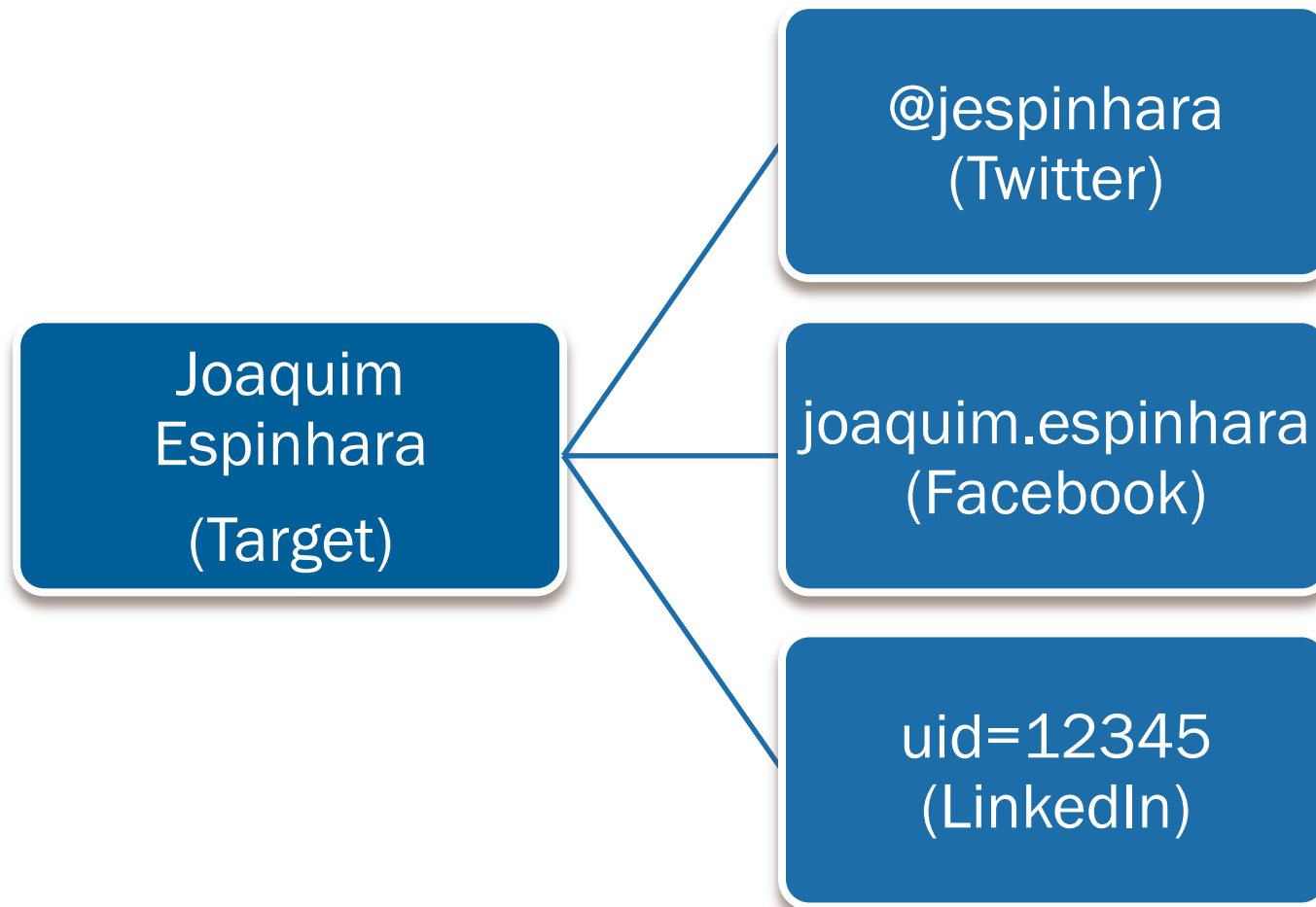
Identifying
the subject
to profile

Collecting
social
network data

Analyzing
and building
the profile

HOWSTUFFWORKS – Our Approach

The Unknown Subject (*Unsub*)





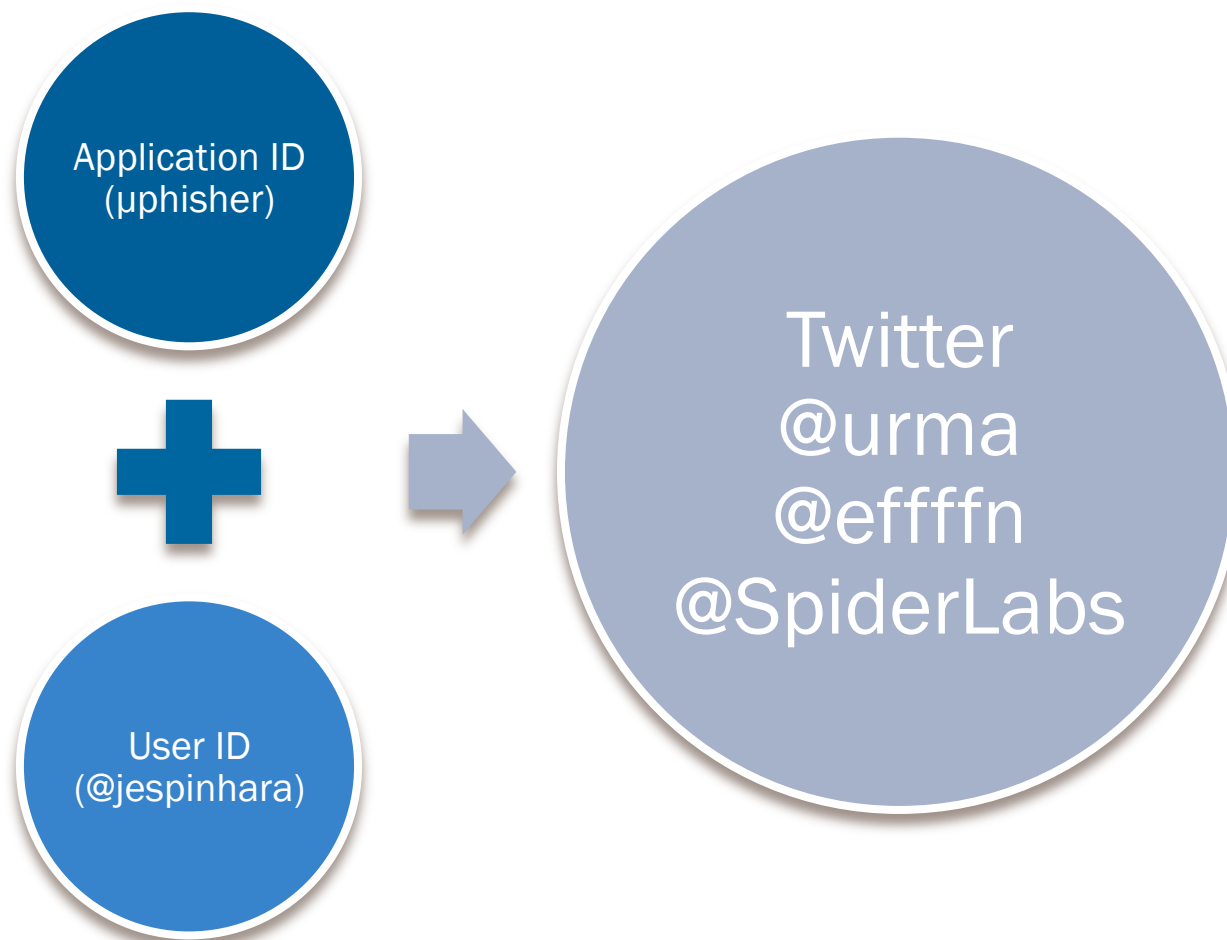
HOWSTUFFWORKS – Our Approach

Data Collection

- Social Network IDs
- Official APIs
- Web Scraping
- OAuth

HOWSTUFFWORKS – Our Approach

Data Collection - Twitter





μPHISHER



 Trustwave®

© 2012



μphisher

Reference implementation

- Goals
 - Validate potential unsub content (Defense)
 - Assisted textual content input (Attack)



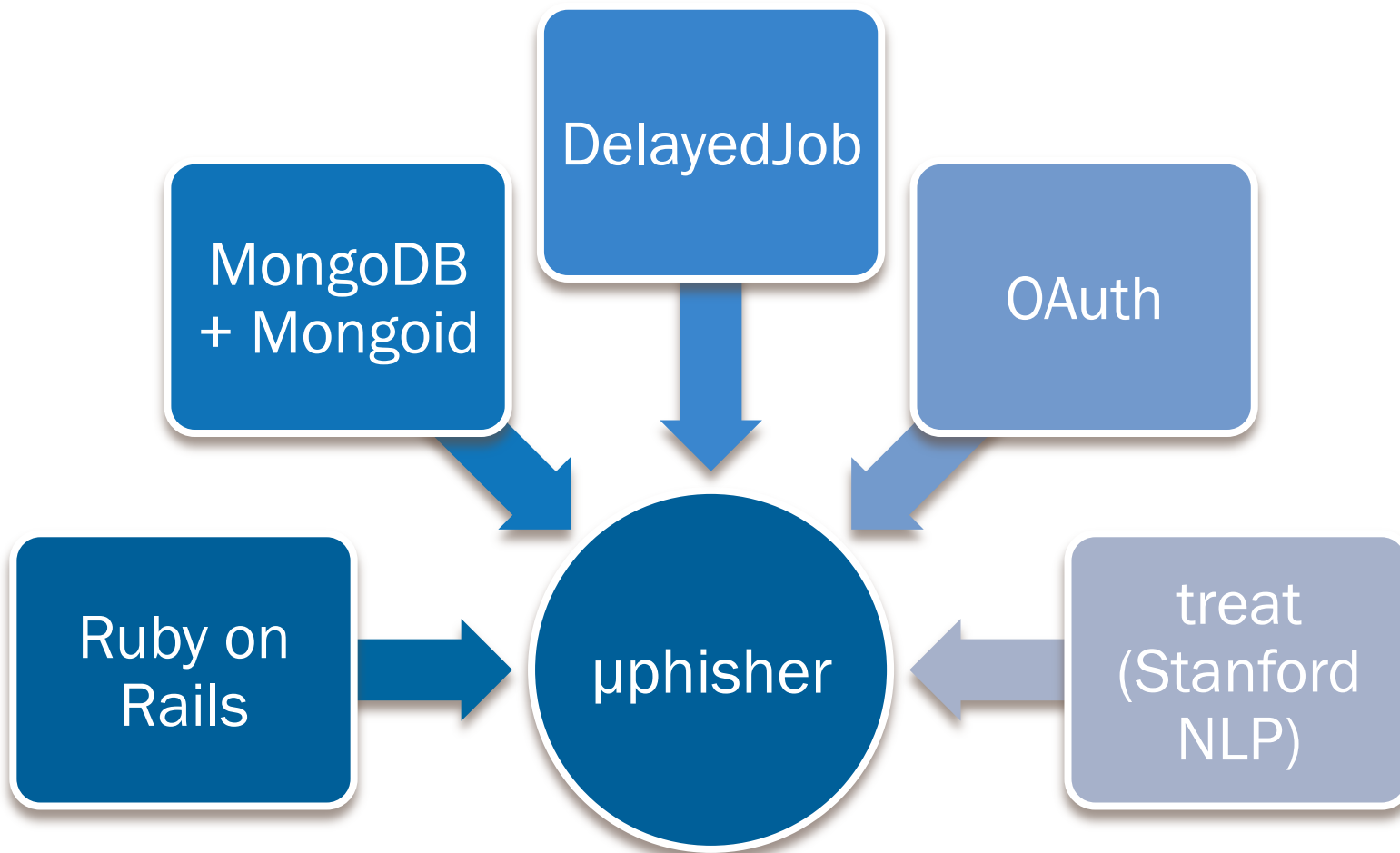
μphisher

Reference implementation

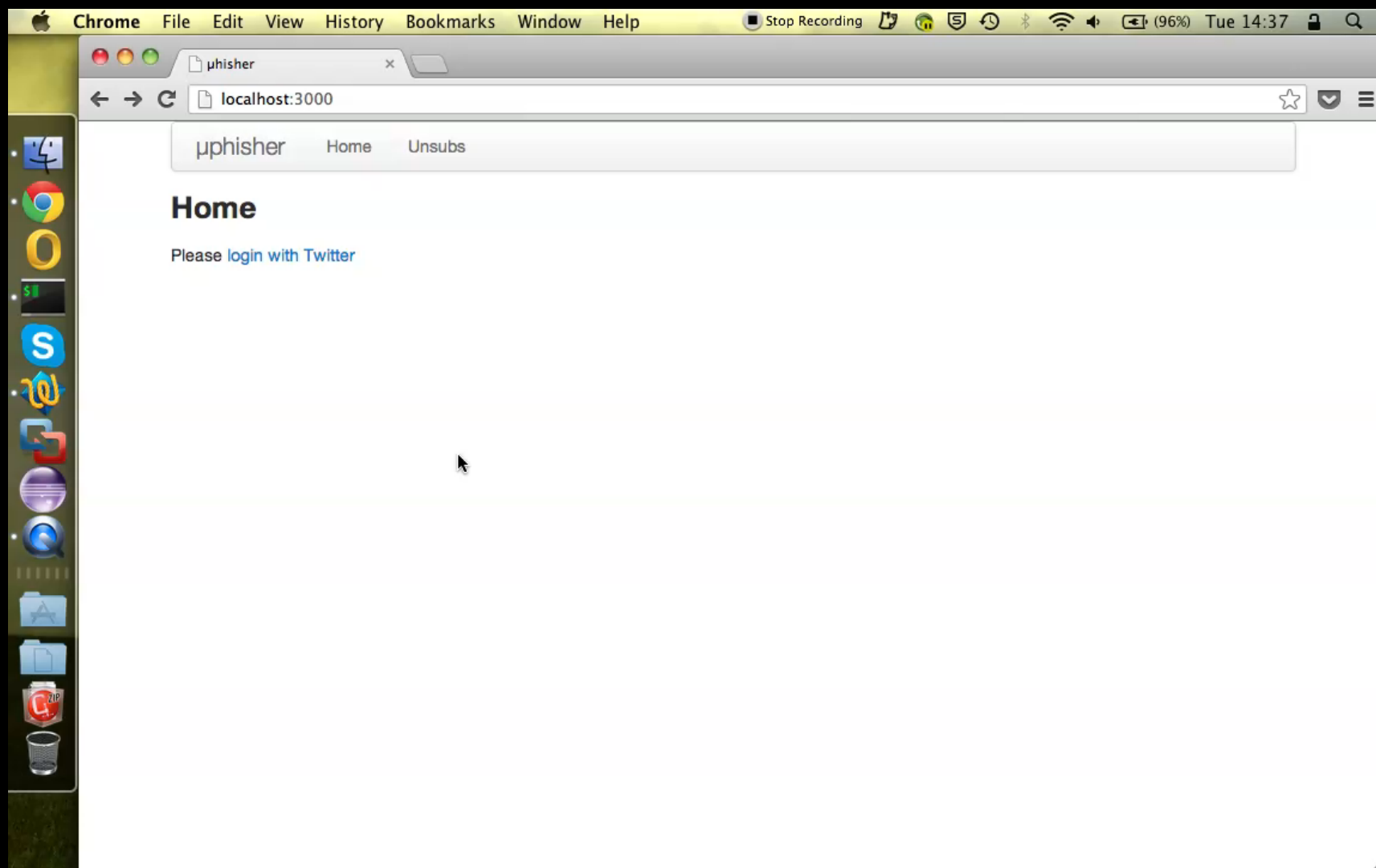
- Web Application
- Console Application
- Twitter only (for now)
- Open Source (GPLv3)

μphisher

Reference implementation



Unsub Registration Demo



μphisher

Reference implementation





DEMO (FINGERS CROSSED)



New Profile Demo

The screenshot shows a web browser window with the following elements:

- QuickTime Player menu bar: File, Edit, View, Share, Window, Help
- System status bar: Stop Recording, network icons, (96%), Tue 15:34
- Browser tab: μphisher
- Address bar: localhost:3000/unknown_subjects/51f83254451097163d000005/data_sources/51f832614510971e26000007
- Navigation: Home, Unsubs, Logout
- Breadcrumbs: Unknown Subjects > Nicholas Percoco > c7five
- Profile Name: c7five (with a Delete button)
- Table of profile details:

Status	complete
Twitter Profile	c7five
Posts Indexed	3281
Earliest Post	12 months
Latest Post	1 day

Assisted Input Demo

The screenshot shows a web browser window with the following elements:

- Browser Title:** μphisher
- Address Bar:** localhost:3000/unknown_subjects/51f83254451097163d000005/profiles/51f84842451097081b00000c
- Navigation:** μphisher Home Unsubs Logout
- Breadcrumbs:** Unknown Subjects > Nicholas Percoco > Tweets from iPhone
- Actions:** Forge Input Delete
- Text:** Tweets from iPhone
Anything sent from the iPhone Twitter Client
- Table:**

Status	complete
Twitter Sources	c7five
Tweet Selector	<code>{"data_source_id"=>{"\$in"=>["51f832614510971e26000007"]}, "source"=>{"\$all"=>[/Twitter for iPhone/]}, "text"=>{"\$all"=>[/RT/]}}</code>
Tweet Count	681 tweets
Average Words Per Tweet	17
Top 10 Words	epic, win, tag, karma, prime, hashtag, feel, certs, immunisation, deceitful

[NLP Parsing Tree \(slow!\)](#)

phisher

- How to use forged content?





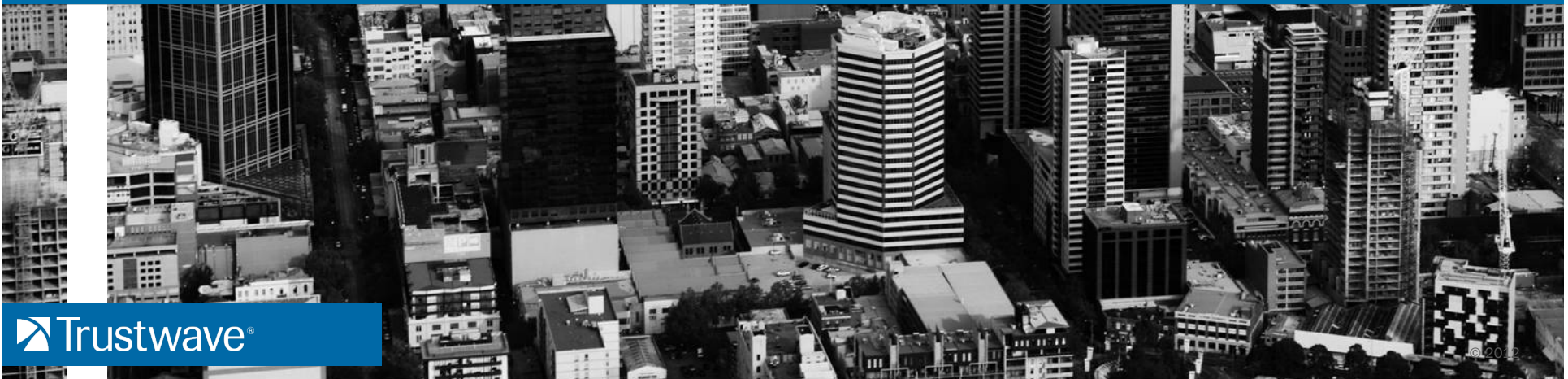
μphisher – Future Work

Coming Soon

- Support for additional data sources
- Topic clustering customized per data source
- More metrics and feedback for assisted input
- Usability (UX help very much needed)



CONCLUSION





[HTTPS://GITHUB.COM/URMA/
MICROPHISHER](https://github.com/URMA/MICROPHISHER)

Download, test, & contribute – any feedback is welcome

An aerial, black and white photograph of a dense urban skyline, likely New York City, showing numerous high-rise buildings with many windows and rooftop structures. A solid blue horizontal banner is overlaid at the top of the image.

Thank You!