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

Joaquim Espinhara & Ulisses Albuquerque

Trustwave®

SMART SECURITY ON DEMAND

Agenda

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

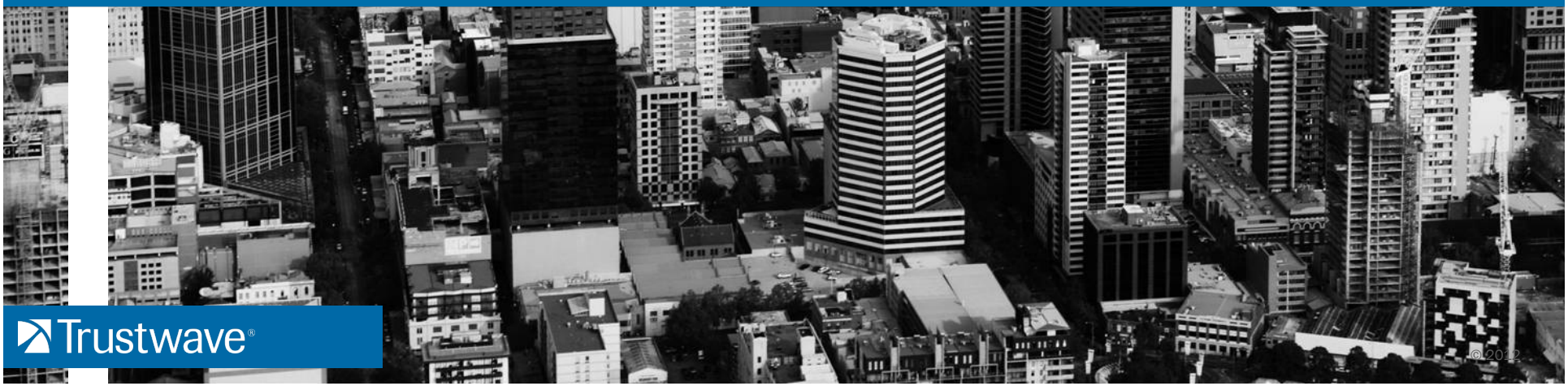
Trustwave®

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

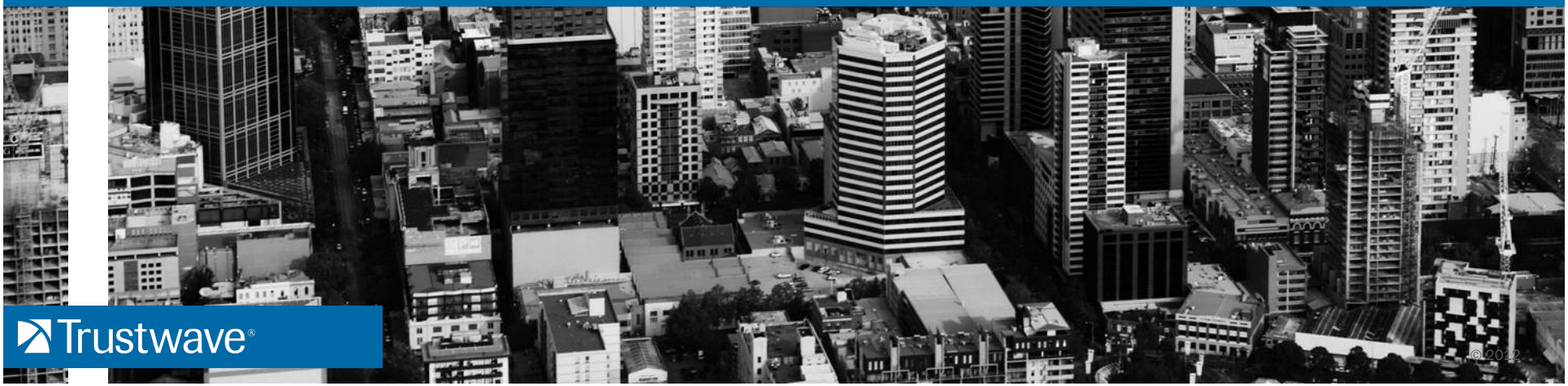
Trustwave®

INTRODUCTION



Trustwave®

OUR MOTIVATION



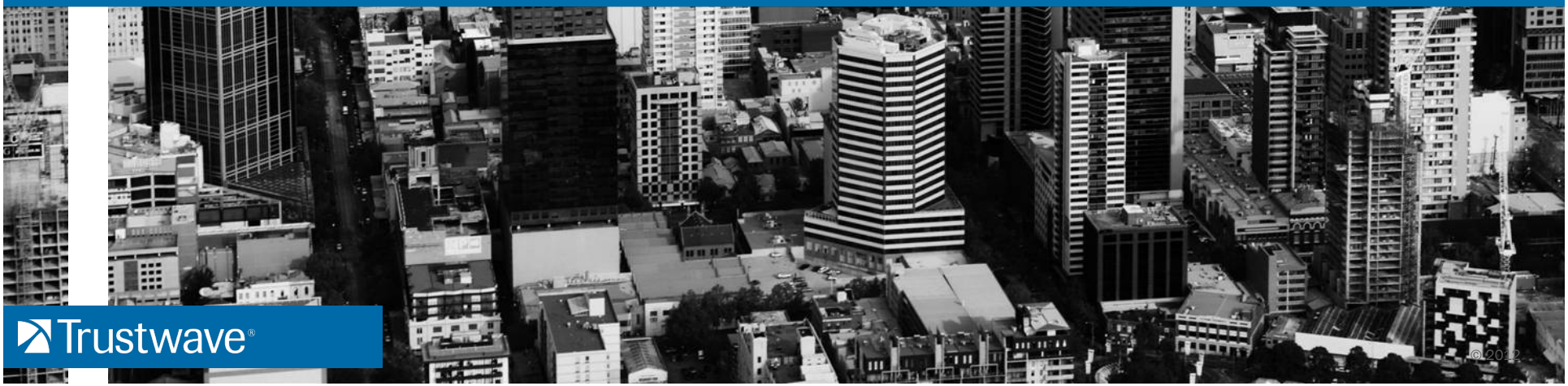
Trustwave®

Our Motivation

- Why?
- Tools available

Trustwave®

BACKGROUND



Trustwave®

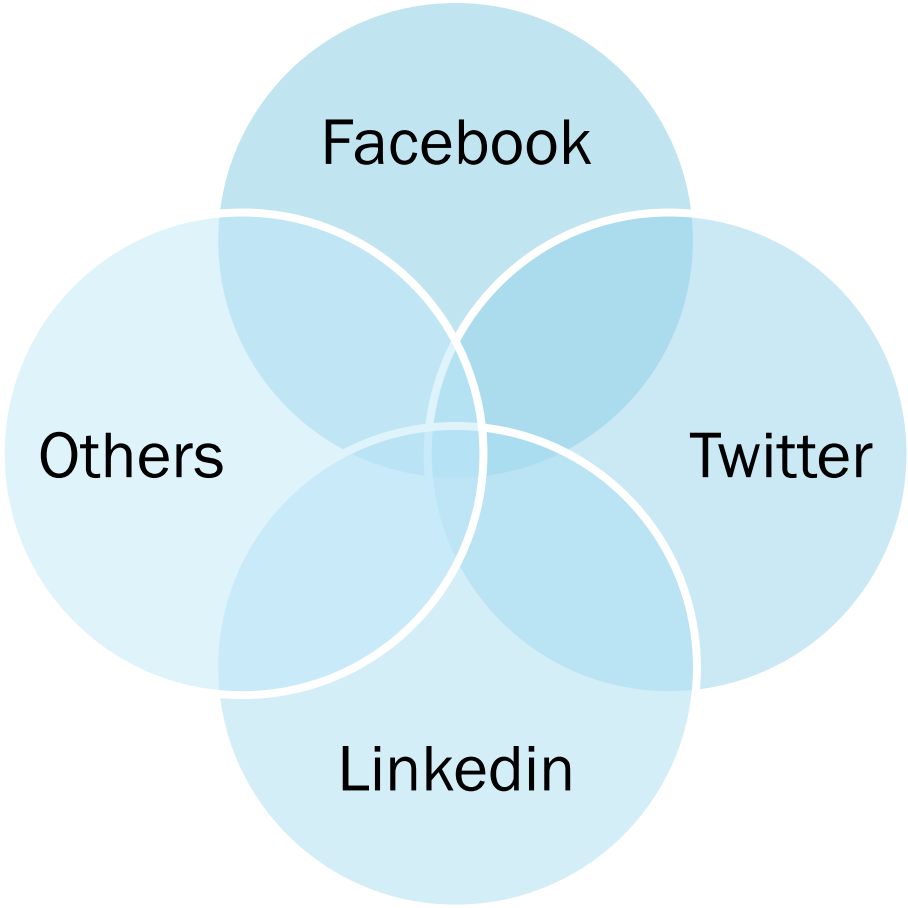
Background

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

Trustwave®

Background

Social Networks



Trustwave®

Background

Social Networks

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

Trustwave®

Background

Social Engineering

- Phishing

http://www.d00med.net/uploads/0d832c77559a2070a766f899e7eg783.png

Background

Data Pre-processing

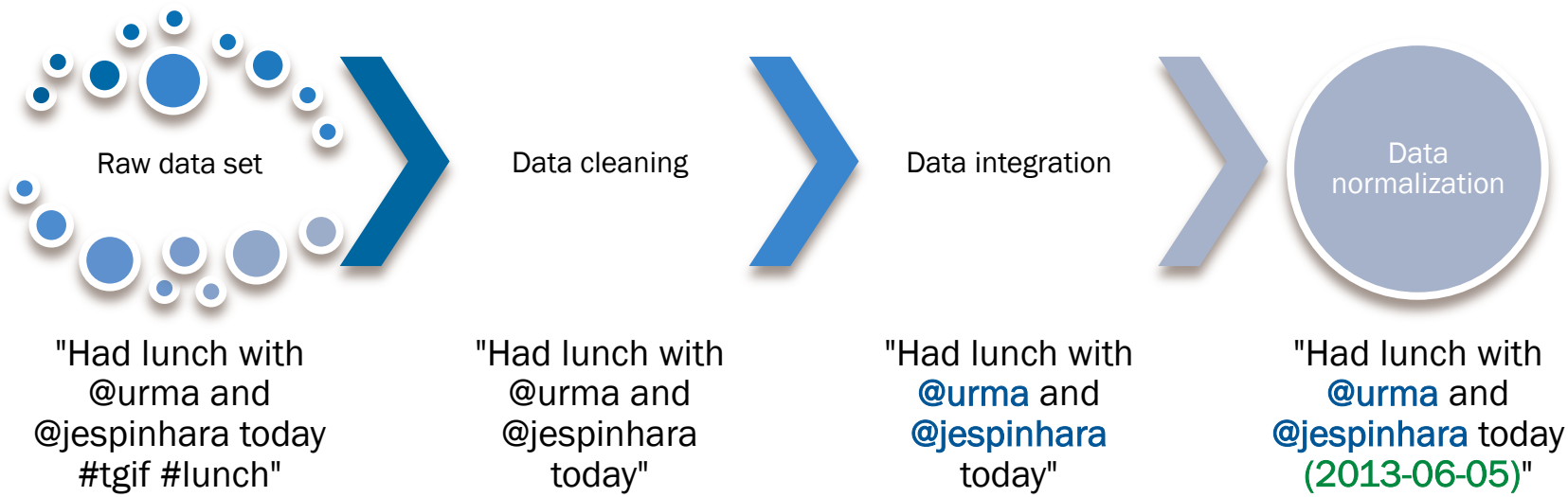
- What is it?
- How do we use it?

Trustwave®

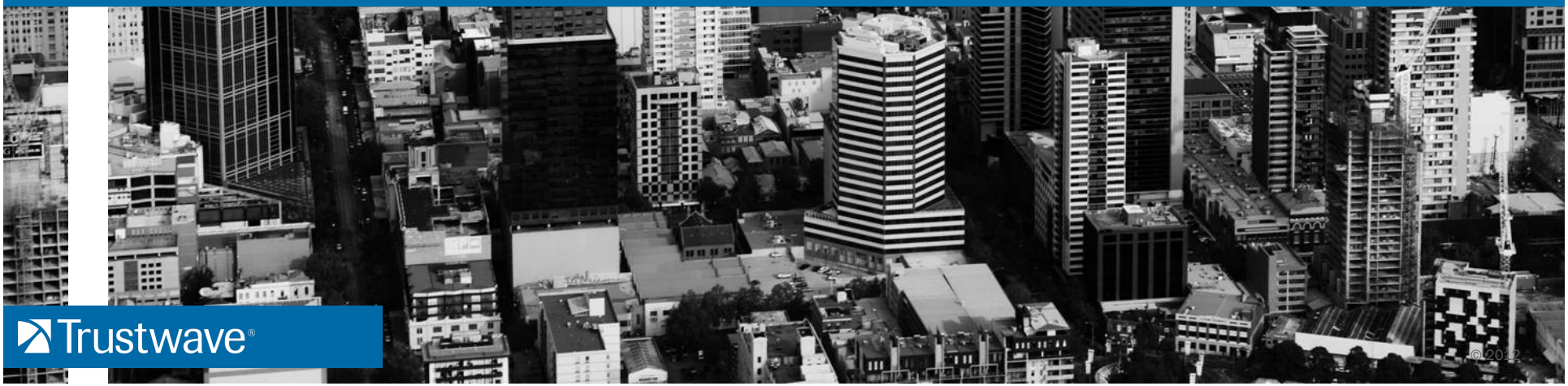
Background

Data Pre-processing

- Data Pre-processing Flow



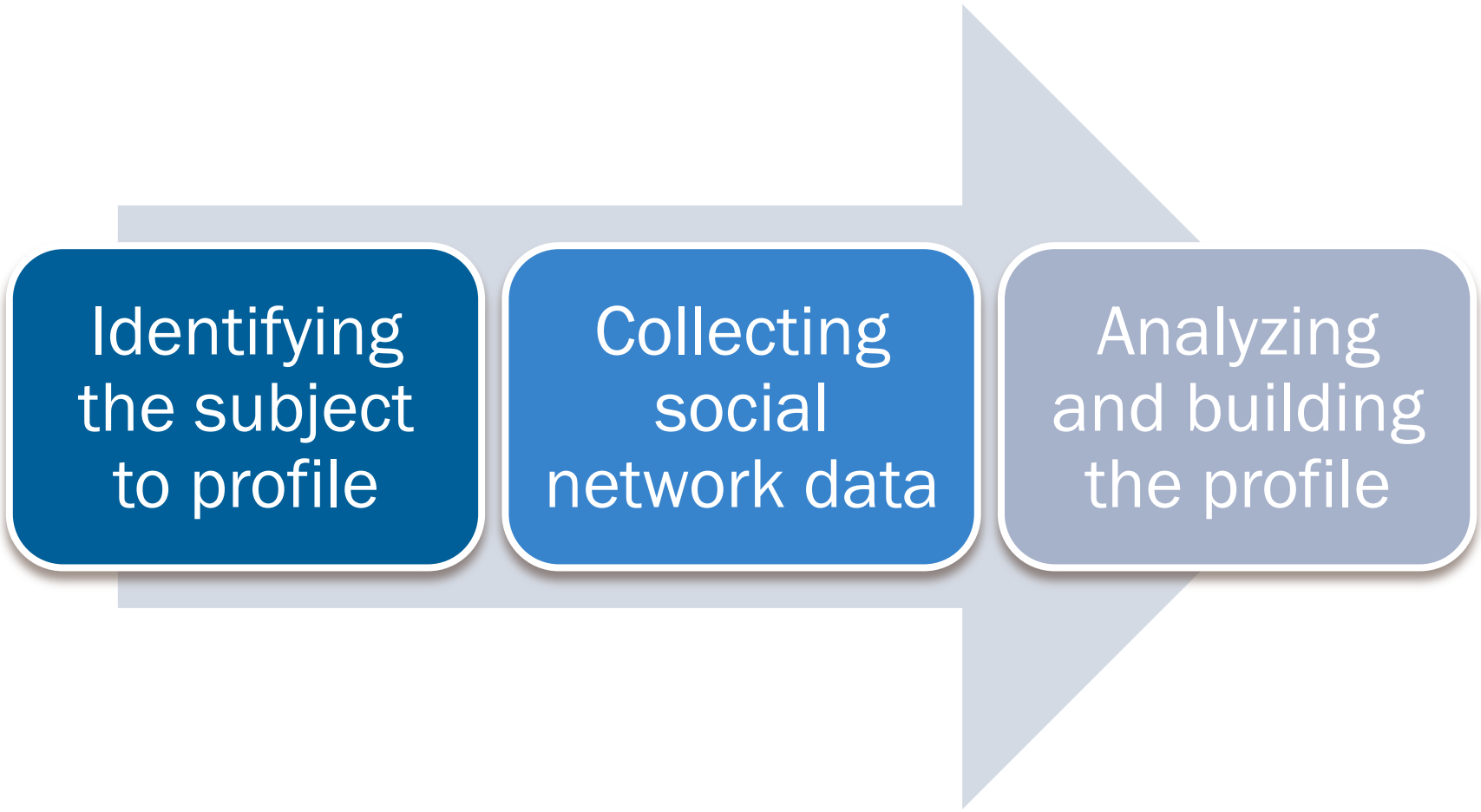
HOWSTUFFWORKS



Trustwave®

HOWSTUFFWORKS

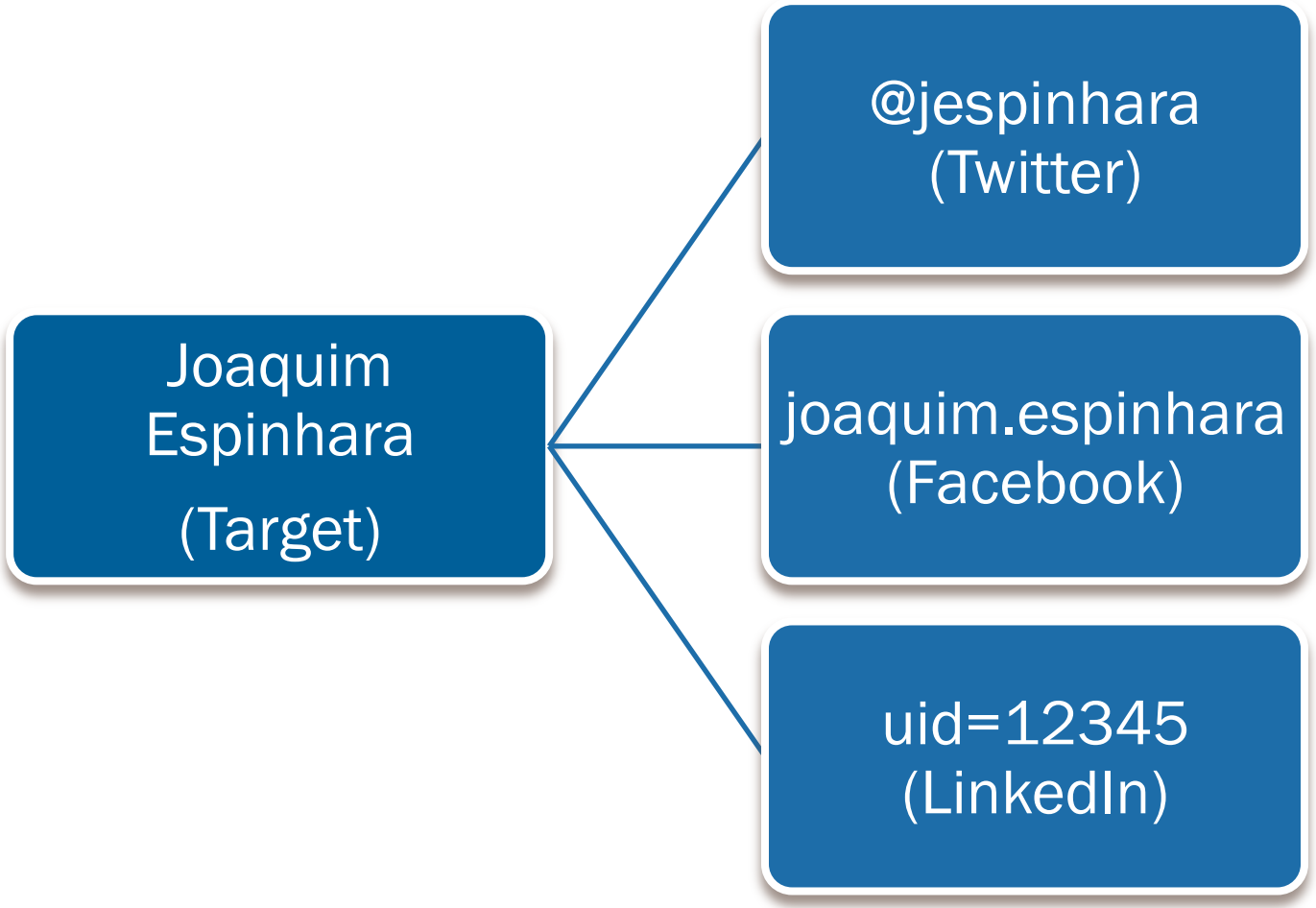
Our Approach



Trustwave®

HOWSTUFFWORKS – Our Approach

The Unknown Subject (*Unsub*)



Trustwave®

HOWSTUFFWORKS – Our Approach

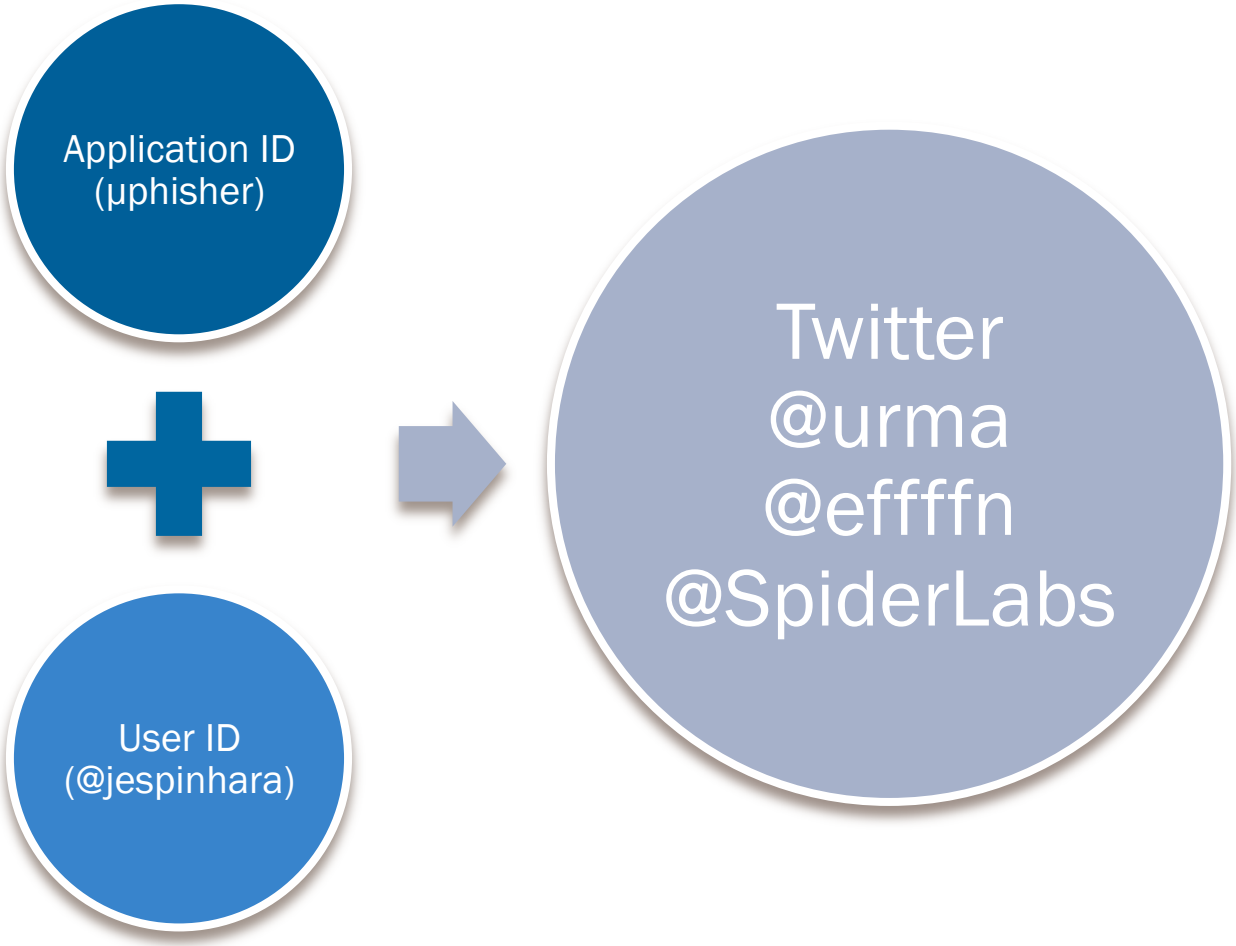
Data Collection

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

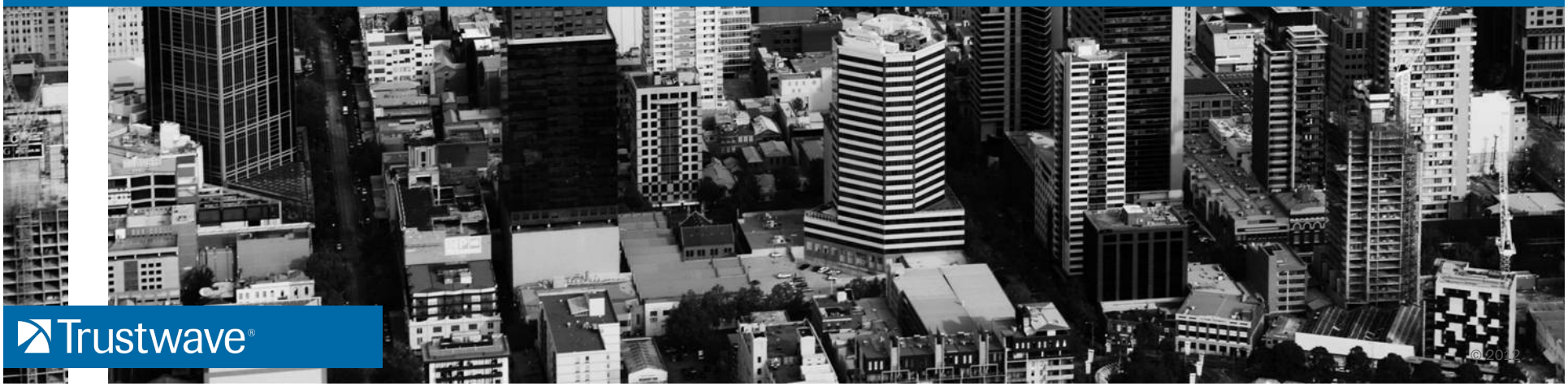
Trustwave®

HOWSTUFFWORKS – Our Approach

Data Collection - Twitter



µPHISHER



Trustwave®

µphisher

Reference implementation

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

Trustwave®

µphisher

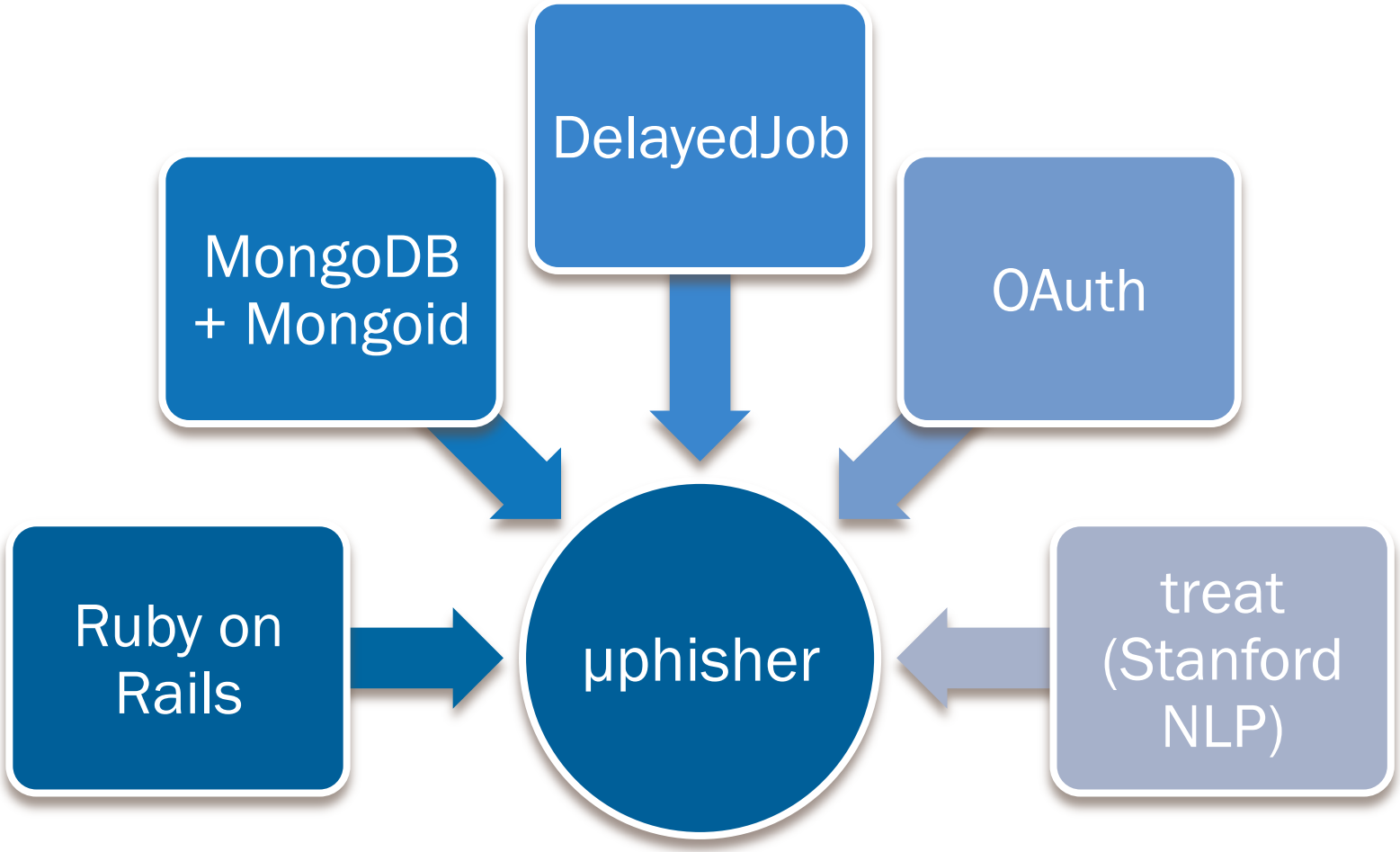
Reference implementation

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

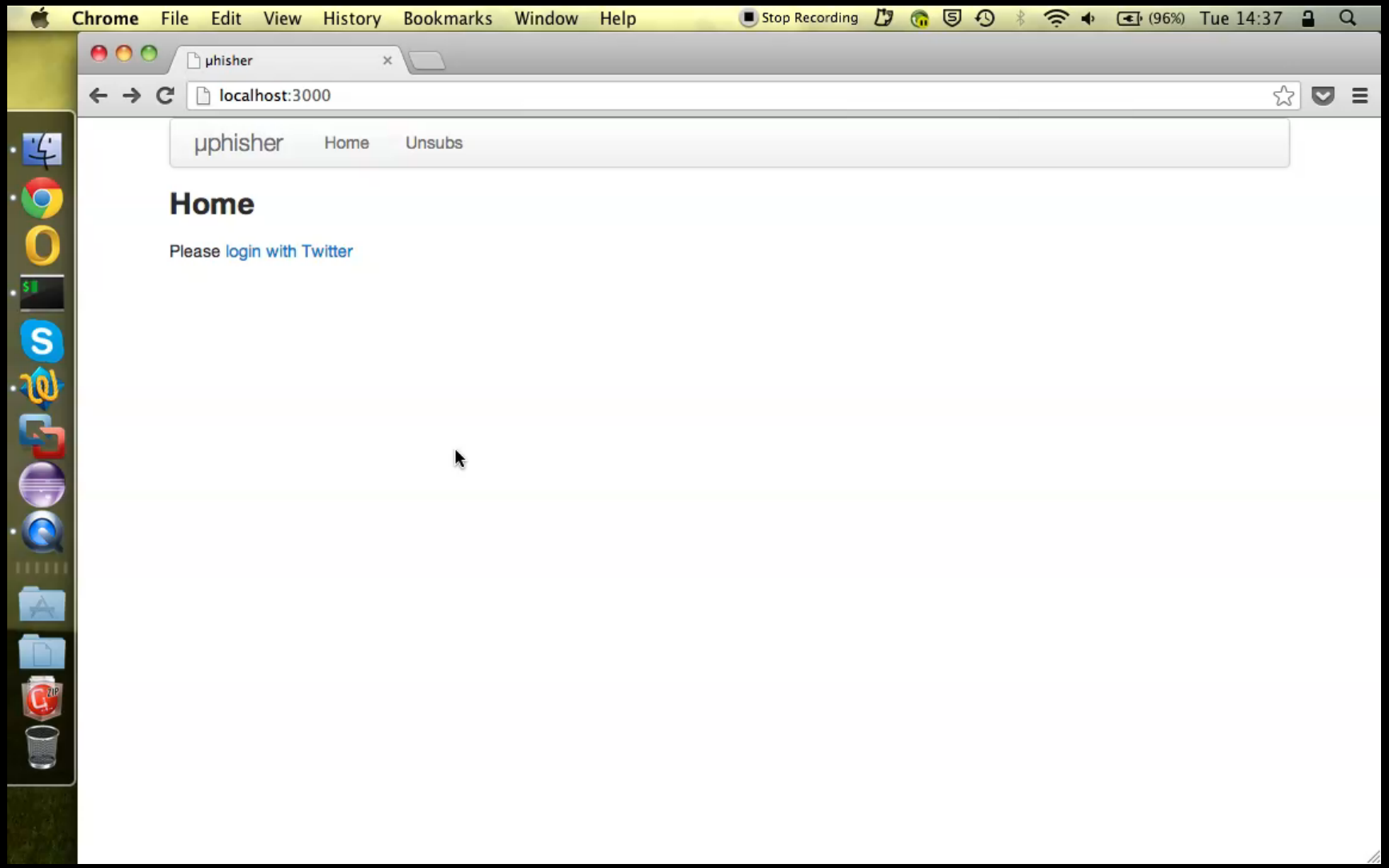
Trustwave®

µphisher

Reference implementation



Unsub Registration Demo



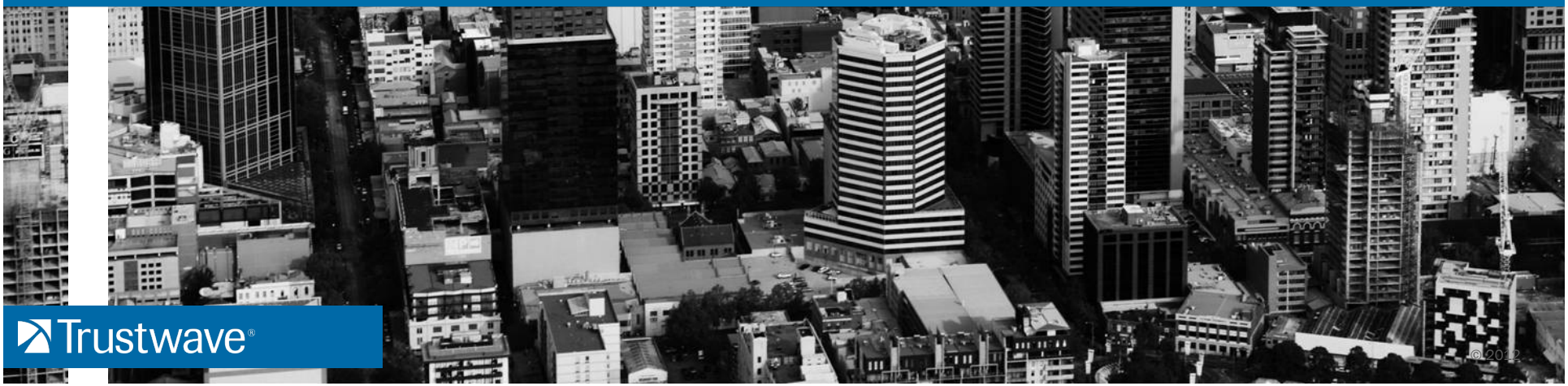
Trustwave®

µphisher

Reference implementation

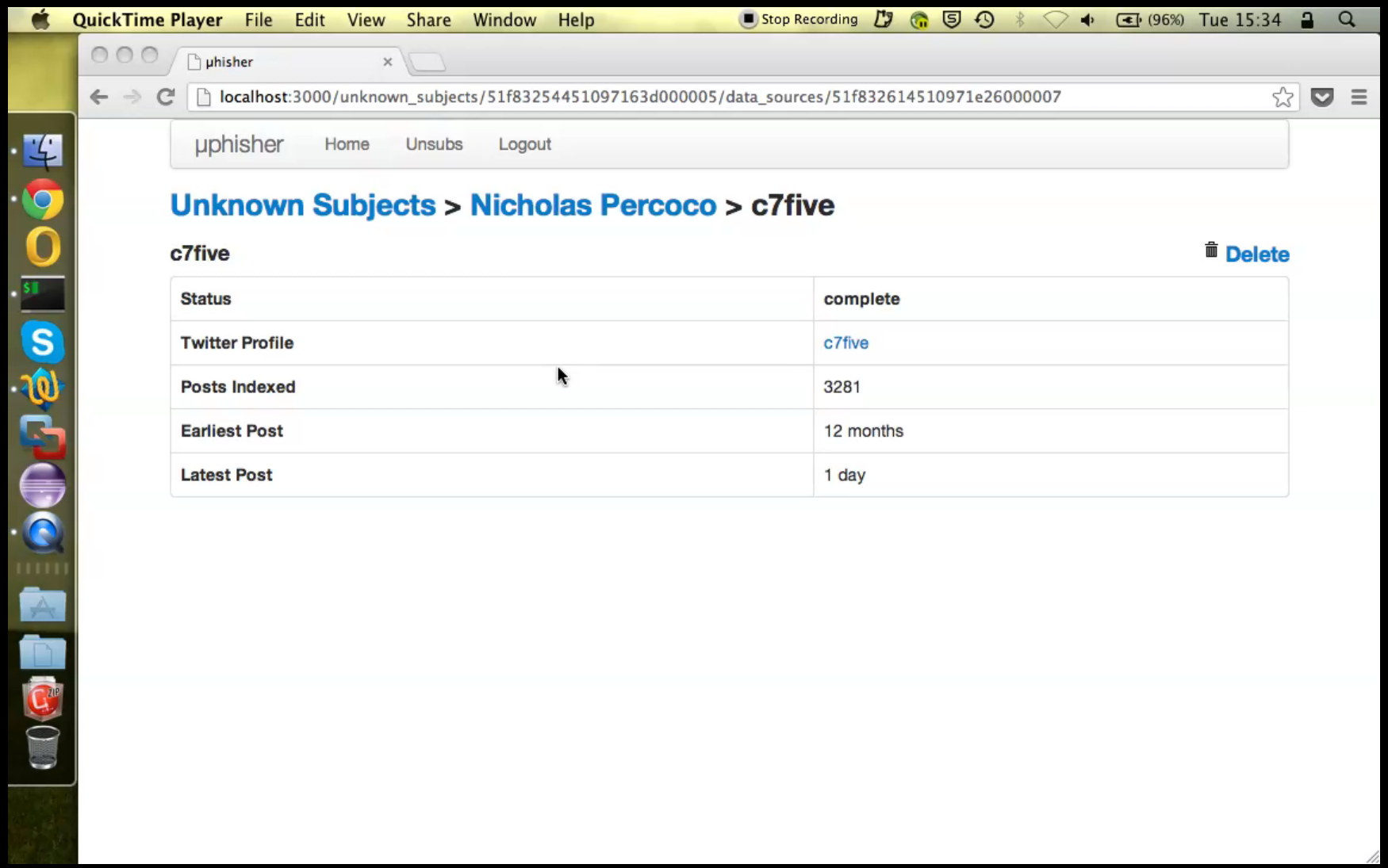
Trustwave®

DEMO (FINGERS CROSSED)



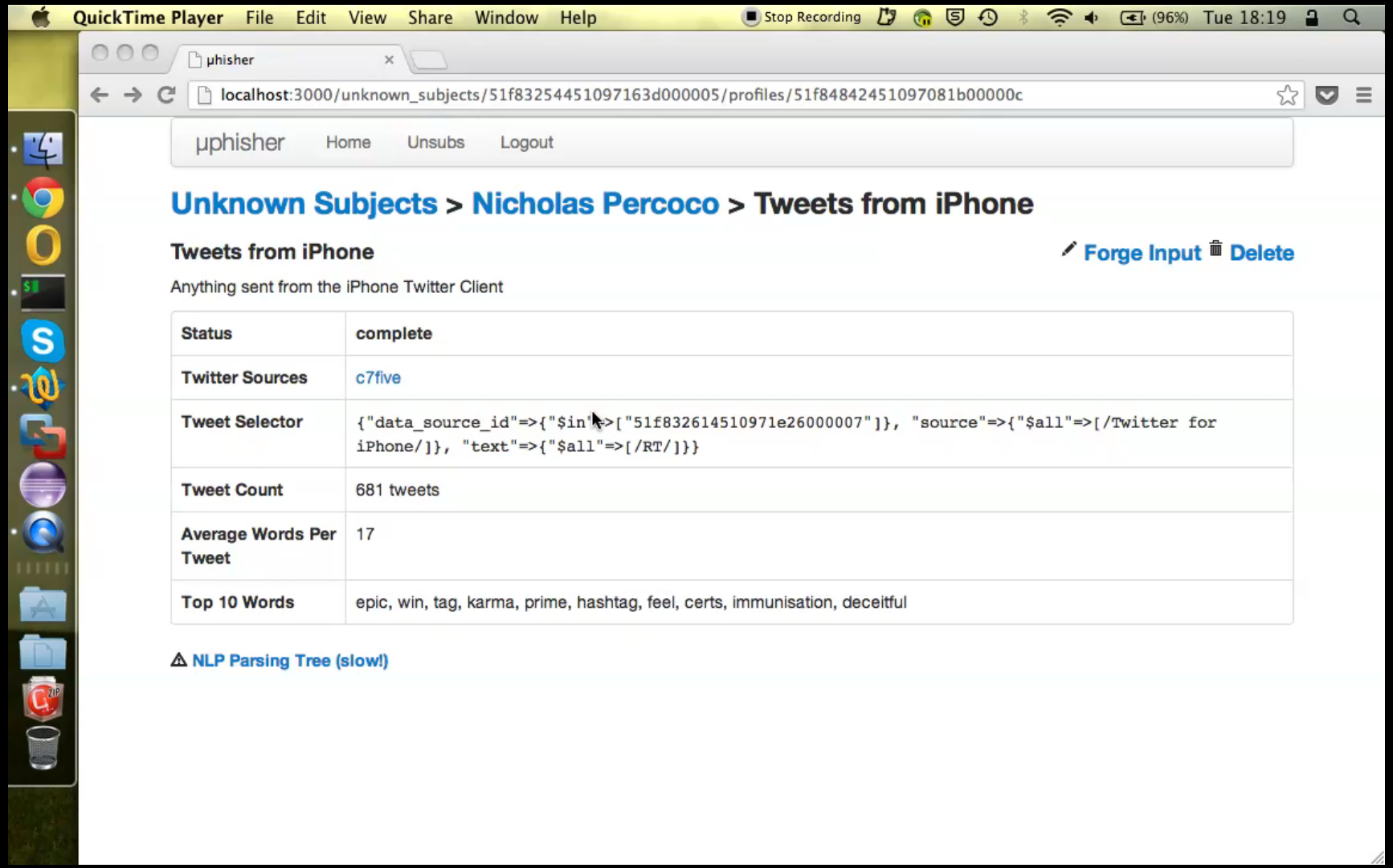
Trustwave®

New Profile Demo



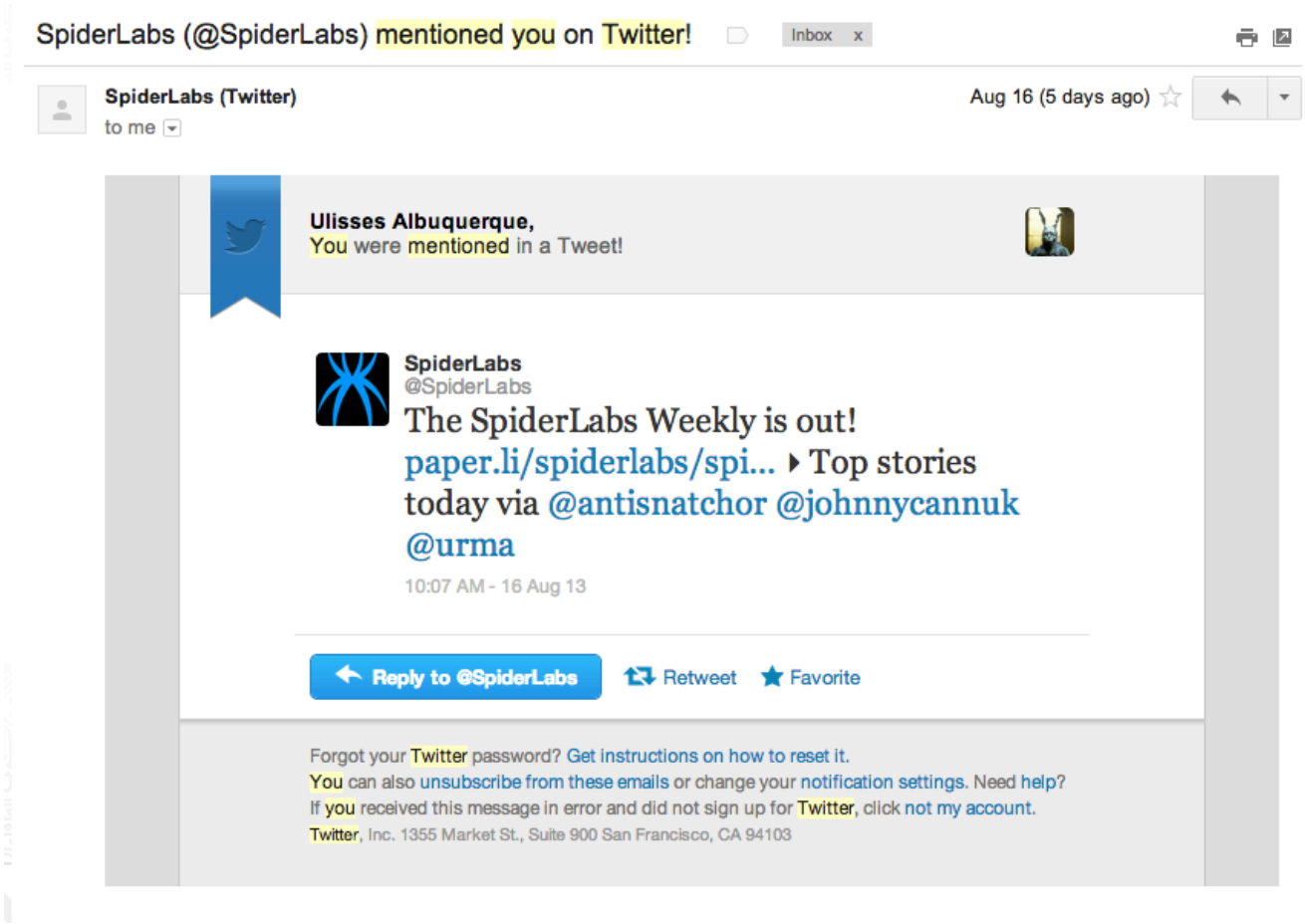
Trustwave®

Assisted Input Demo



µphisher

- How to use forged content?



Personal email screenshot

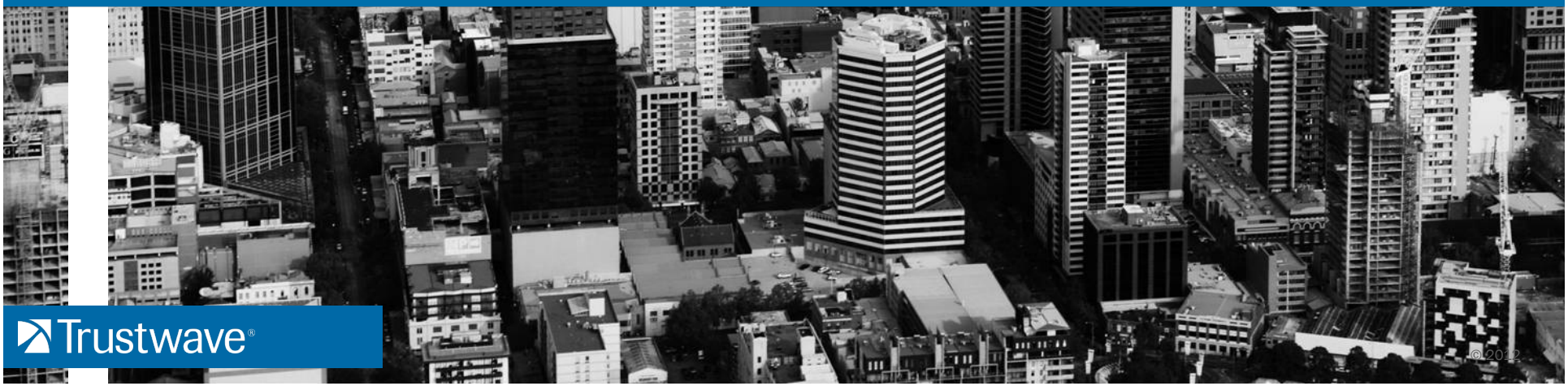
µphisher – Future Work

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)

Trustwave®

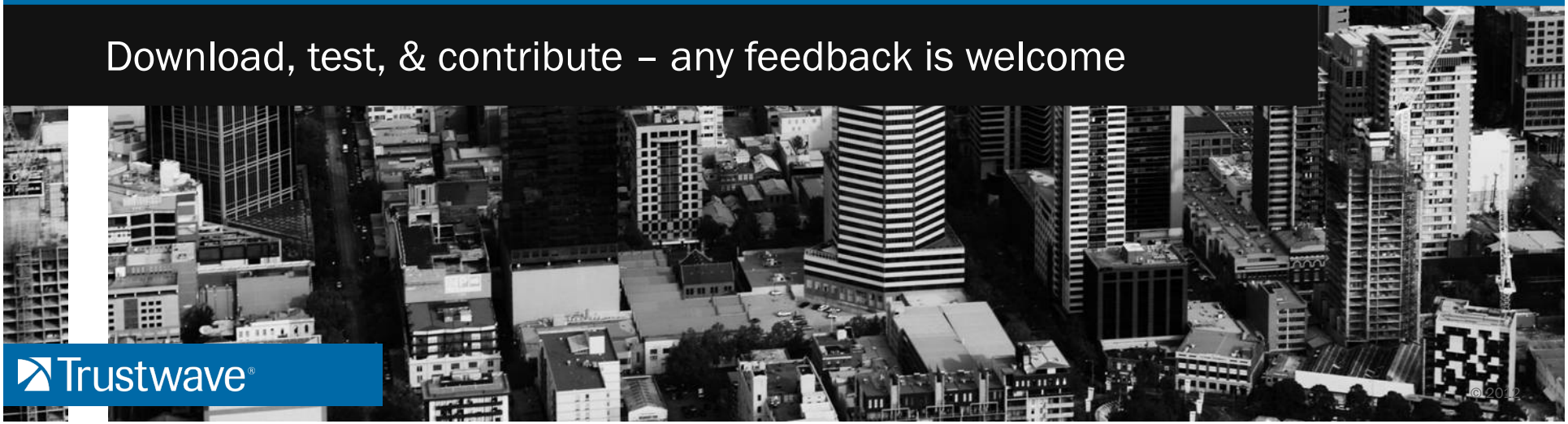
CONCLUSION



Trustwave®

HTTPS://GITHUB.COM/URMA/MICROPHISHER

Download, test, & contribute – any feedback is welcome



Trustwave®

Thank You!

Trustwave®