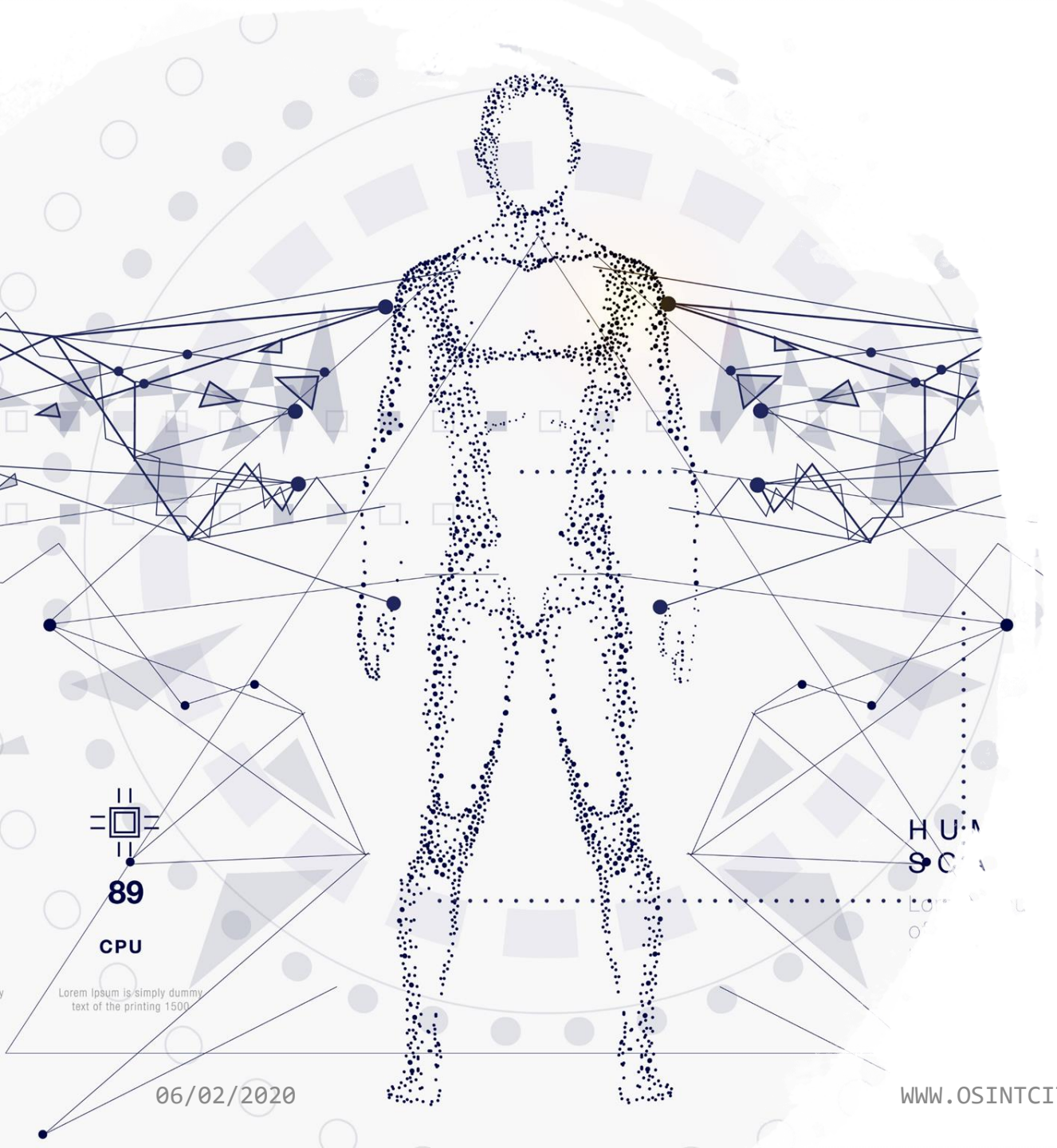


OSINT CITY

QUANTIKA14

twiana
todos los pájaros a un click

#OSINTCITY2020

OSINT, OSANT CADA DÍA TE QUIERO MÁS

IDENTIFICANDO CUENTAS ANÓNIMAS

AUTOR: JORGE CORONADO de QuantiKa14

COMUNIDAD DE APASIONADOS POR LA SEGURIDAD INFORMÁTICA EN SEVILLA

HACKING SEVILLA

ACA, APRENDE, COMPARTE + ROBOTS

GRUPO ABIERTO: HAPPY HACKING SEVILLA

¿Qué es Hacking Sevilla?

Gorgue de Triana

- Fundador y **CEO de QuantiKa14**
- Colaborador de **Canal Sur Radio** desde 2015
- **Profesor** en el curso de **detectives de la Universidad Pablo Olavide** de Sevilla en 2017
- Co-autor del primer **"Protocolo institucional en España ante la violencia de género en las redes sociales"**
- **Formación a cuerpos de seguridad en investigación a través de Internet** desde la ESPA y otros cursos
- Creador del **protocolo de actuación para la búsqueda de personas desaparecidas a través de las tecnologías de la información y comunicación**
- **Vocal** de la **asociación de peritos tecnológicos de Andalucía** (APTAN)
- Dinamizador del **Hack&Beers Sevilla**
- Autor del canal de Youtube **Investiga Conmigo desde el Sü**
- Creador de aplicaciones como: **Guasap Forensic, Shodita, EO-Ripper, Dante Gates, Killo.io, etc**

aptan ASOCIACIÓN DE PERITOS JUDICIALES TECNOLÓGICOS DE ANDALUCÍA

QUANTIKA14

DANTE'S GATES

¿Qué es QuantiKa14?

PERITAJE INFORMÁTICO

+

OSINT

QK14 es una empresa que nació en 2013 con el objetivo de unir el mundo legal y técnico. Actualmente es una empresa consolidada por sus proyectos y amplia experiencia. Su equipo multidisciplinar le permite realizar servicios de investigación de crímenes informáticos, peritajes informáticos, auditorías de seguridad y desarrollar sus propias aplicaciones informáticas. Además QK14 ha participado, patrocinado y organizado decenas de eventos de seguridad informática y derecho.

¿Qué vamos a ver?

I. Conceptos básicos

II. Situación del caso I
    I. Metodología
    II. Demostración

III. Situación del caso II

Objetivo de la charla

1. Enseñar conceptos básicos y funcionamiento de la red social de Twitter
2. Enseñar el Proyecto “Investiga conmigo desde el su”
3. Explicar cómo se puede hacer un big data para identificar cuentas anónimas en Twitter usando Python
4. Realizar una demostración

I. Conceptos básicos

Conceptos básicos: **¿Qué es una cuenta anónima?**

¿Qué es una cuenta anónima en Twitter?

Es una cuenta creada en la red social y que no es posible de asociar a una persona o entidad. Porque no expone ningún dato que inicialmente identificable.

Actualmente, las cuentas anónimas tienen las siguientes características:

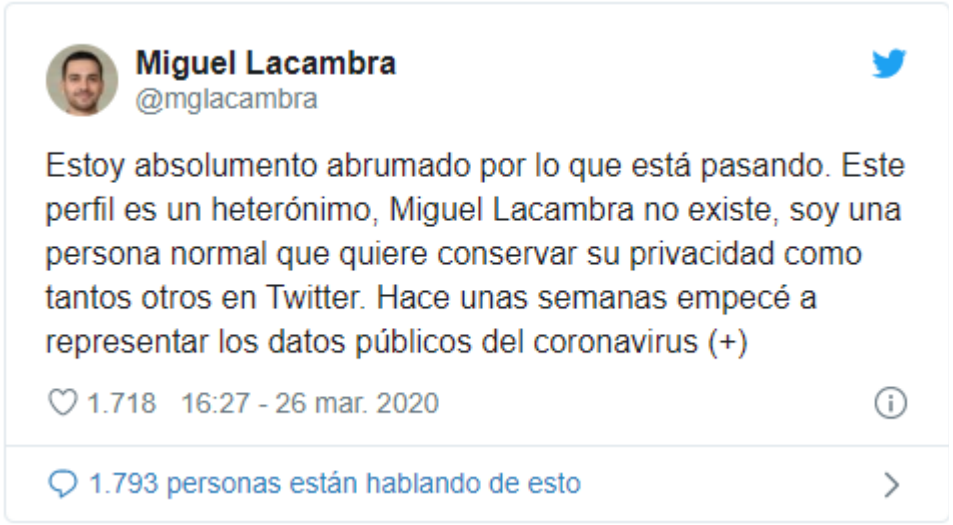
1. Username y user account no identificable
2. Imagen(portada) y de perfil aparentemente no identificable
3. Biografía con ningún dato rastreable
4. Sin o falsa ubicación

En resumen es una cuenta que no expone ningún dato que identifique a una persona o personas dueñas de la cuenta.

Casos reales:

https://twitter.com/JulianMaciasT/status/1246200508630667265

https://www.elmundo.es/f5/comparte/2020/03/27/5e7de0ee21efa072558b4586.html



https://hipertextual.com/juno/pastrana-twitter-alcalde-pp-jospastr

¿Qué debe tener un buen OSINTER?

1. Fuentes
2. Aplicaciones
3. Paciencia
4. Caminos y correlaciones (inteligencia)

El OSINT no es magia

1
2

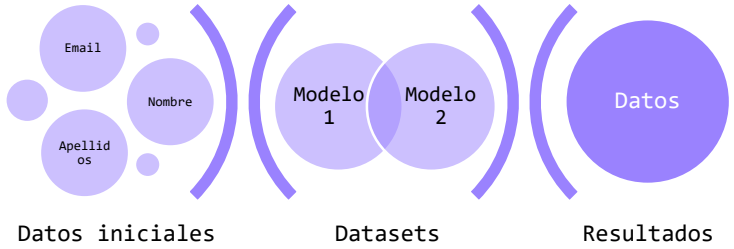
¿Qué son los datos iniciales?

DEVFEST 2019 - GDG SEVILLA

4/4/2020

II. Metodología

1. Identificación de datos iniciales
2. Análisis automático con buscadores (Dante’s Gates Minimal Version, EO-ripper, etc)
3. Análisis manual
4. Creación de informe



Con los **datos iniciales** creamos un dataset de forma recursiva.

QUANTIKA14
Intelligence for criminal investigations

https://www.youtube.com/watch?v=ra-YC6MwG3k

Situación del caso I: amenazas de muerte por Internet

WWW.OSINTCITY.COM

06/02/2020

Situación del caso real II: anónimo en Twitter…

Una cuenta insulta y acosa a otras cuentas…

Funcionalidades interesantes de Twitter:

- Cambiar el nombre de usuario
- Cambiar el número de cuenta
- Cambiar la cuenta de privado a público, y viceversa varias veces
- Eliminar un tweet que has subido
- Limitar la visualización de respuestas en hilos

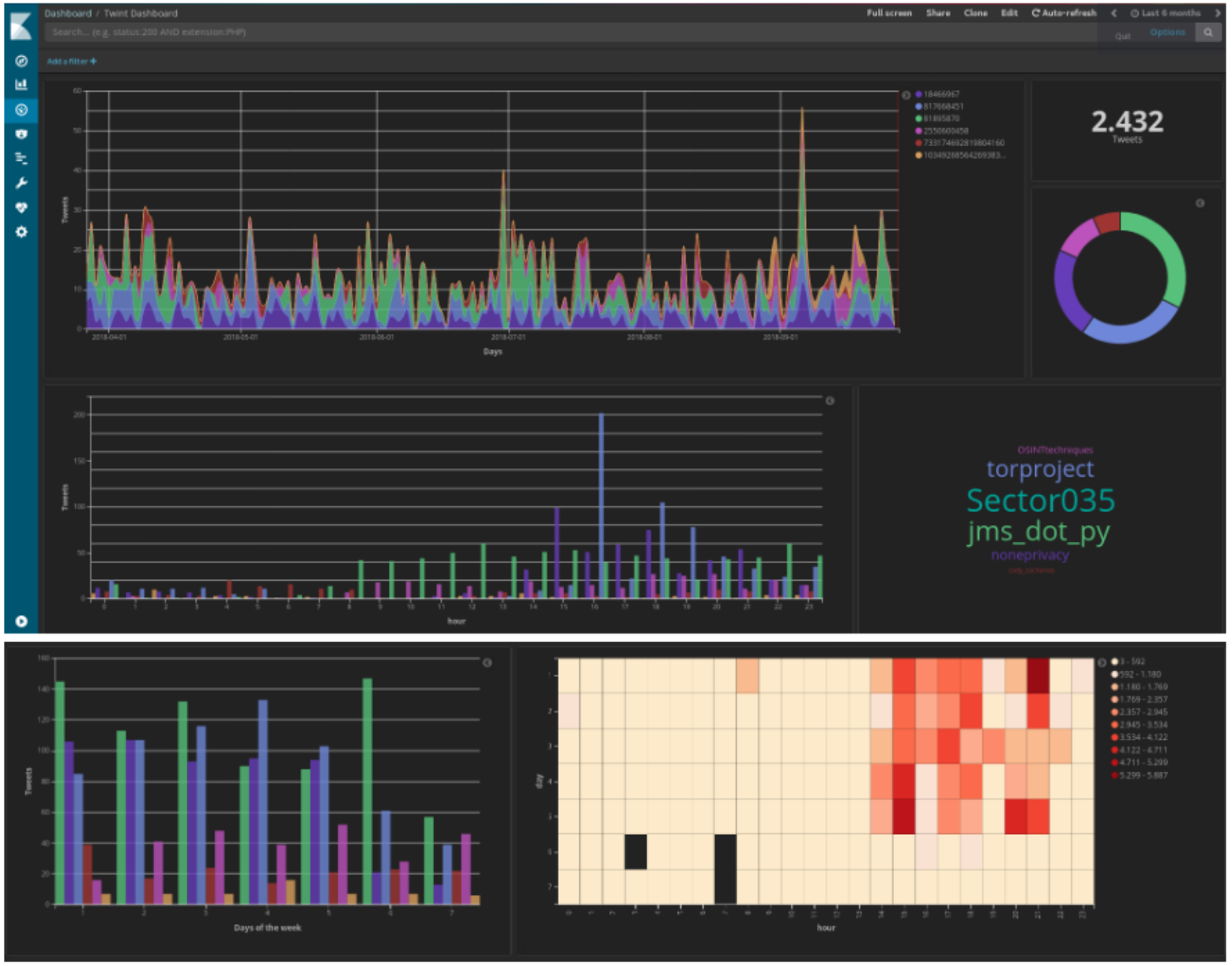
¿Qué datos iniciales tiene una cuenta de Twitter?

- Nick de username
- Nick de la cuenta
- Posible email y tlfn publicado
- Posible email y tlfn en recuperar contraseña
- Webs en descripción o contenido (time line)

¿Cómo descargar una cuenta de Twitter?

06/02/2020

TWINT - Herramienta de inteligencia de Twitter



pypi v2.1.12 | build passing | Python 3.6/3.7/3.8 | license MIT | downloads 60k | downloads/week 1k | patreon 3 patrons

Comparar dos cuentas:followers/following

```
8
9   def compare_following(u1, u2):
10
11      c.Username = u1
12      F1 = twint.run.Following(c)
13
14      c.Username = u2
15      F2 = twint.run.Following(c)
16
17      for f in F1:
18          if f in F2:
19              print(f)
20
21  compare_following("jorgewebsec", "quantika14")
```

```
21  def compare_followers(u1, u2):
22
23      c.Username = u1
24      F1 = twint.run.Followers(c)
25
26      c.Username = u2
27      F2 = twint.run.Followers(c)
28
29      for f in F1:
30          if f in F2:
31              print(f)
```

Comparar menciones y hashtags

```
- {id}
- {conversation_id}
- {created_at}
- {date}
- {time}
- {timezone}
- {user_id}
- {username}
- {name}
- {place}
- {tweet}
- {mentions}
- {urls}
- {photos}
- {replies_count}
- {retweets_count}
- {likes_count}
- {hashtags}
- {cashtags}
- {link}
- {retweet}
- {quote_url}
- {video}
- {user_rt_id}
- {near}
- {geo}
- {source}
- {retweet_date}
```

- Podemos configurar el análisis de los tweets según sus atributos: hashtags, menciones, fechas, urls, etc

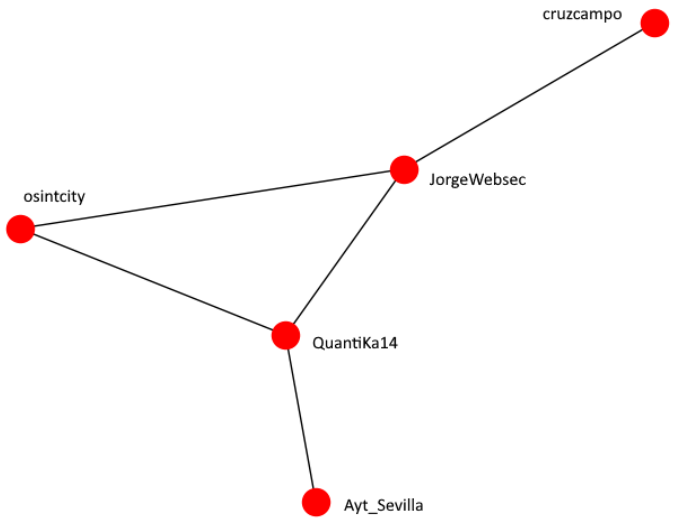
```
import twint

c = twint.Config()
c.Username = "username"
c.Custom["tweet"] = ["id", "username"]
c.Output = "tweets.csv"
c.Store_csv = True

twint.run.Search(c)
```

¿Cómo dibujamos los datos de comparación de followings?

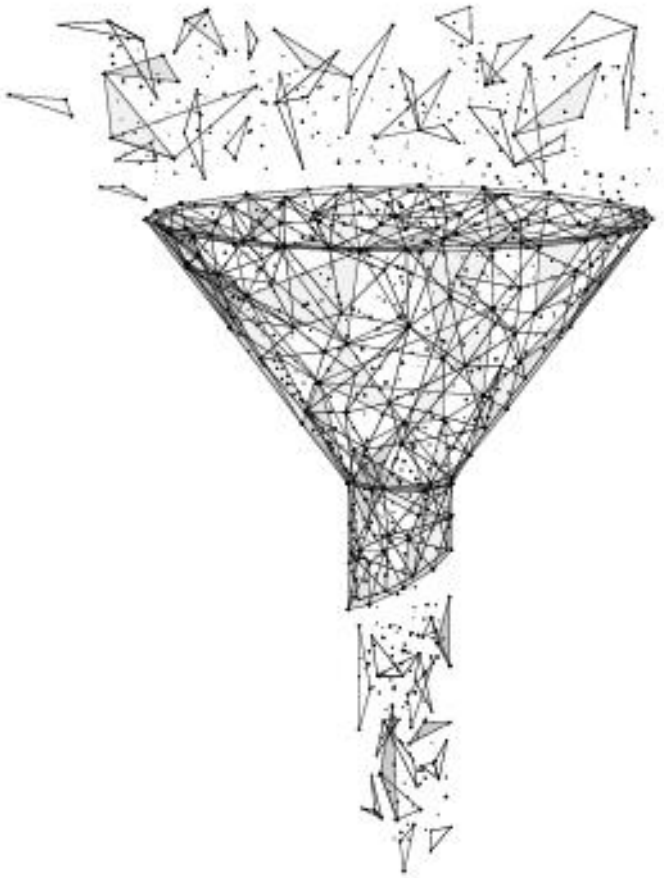
06/02/2020

```
#Se importa la libreria networkx como nx

import networkx as nx

#Se importa la libreria pyplot de matplotlib como plt

import matplotlib.pyplot as plt

#Se crea un grafo vacio

G=nx.Graph()
```

```
#Cada nodo son las cuentas que vamos a comparar

G.add_node("jorgewebsec")

G.add_node("quantika14")

#Se crean los nodos de las cuentas a las que sigue Jorge Websec

G.add_nodes_from(["quantika14","osintcity", "cruzcampo"])

#Se crean los nodos de las cuentas a las que sigue quantika14

G.add_nodes_from(["jorgewebsec","osintcity", "ayt_sevilla"])

#Se crean los enlaces

G.add_edge("quantika14","jorgewebsec")

G.add_edge("jorgewebsec","quantika14")

G.add_edge("osintcity","jorgewebsec")

G.add_edge("osintcity","quantika14")

G.add_edge("cruzcampo","jorgewebsec")

G.add_edge("ayt_sevilla","quantika14")
```



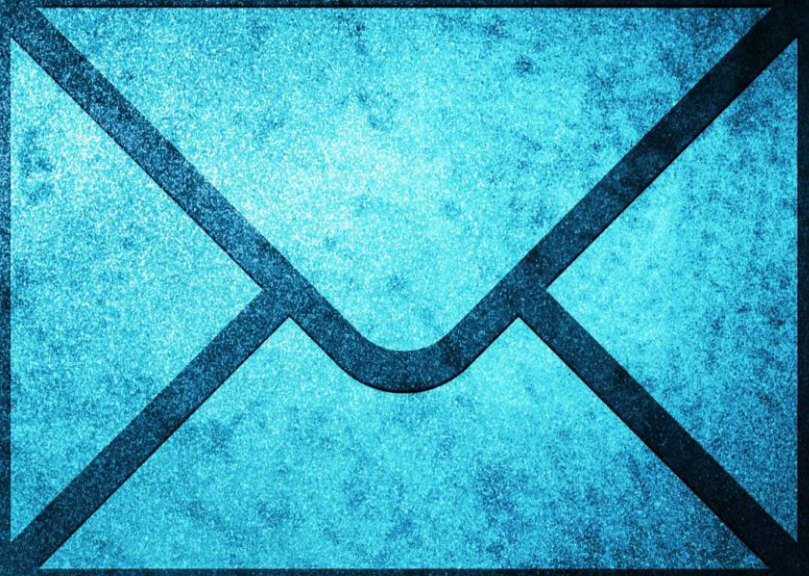
Big data + Twitter data clustering



Lectura recomendada:

- http://homepages.vub.ac.be/~ndeligia/pubs/TwitterDataClusteringVisual.pdf
- https://upcommons.upc.edu/bitstream/handle/2117/82434/113257.pdf?sequence=1&isAll
- https://github.com/albarji/curso-analisis-textos

El email es una gran fuente de información



Cruces de datos:

- Nick > Facebook > nombre real
- Twitter > email > Facebook > nombre real
- Twitter > Nº Teléfono > Facebook > nombre real

Análisis de emails

https://play.google.com/store/apps/details?id=com.quantika14.dantes_gates_mobile

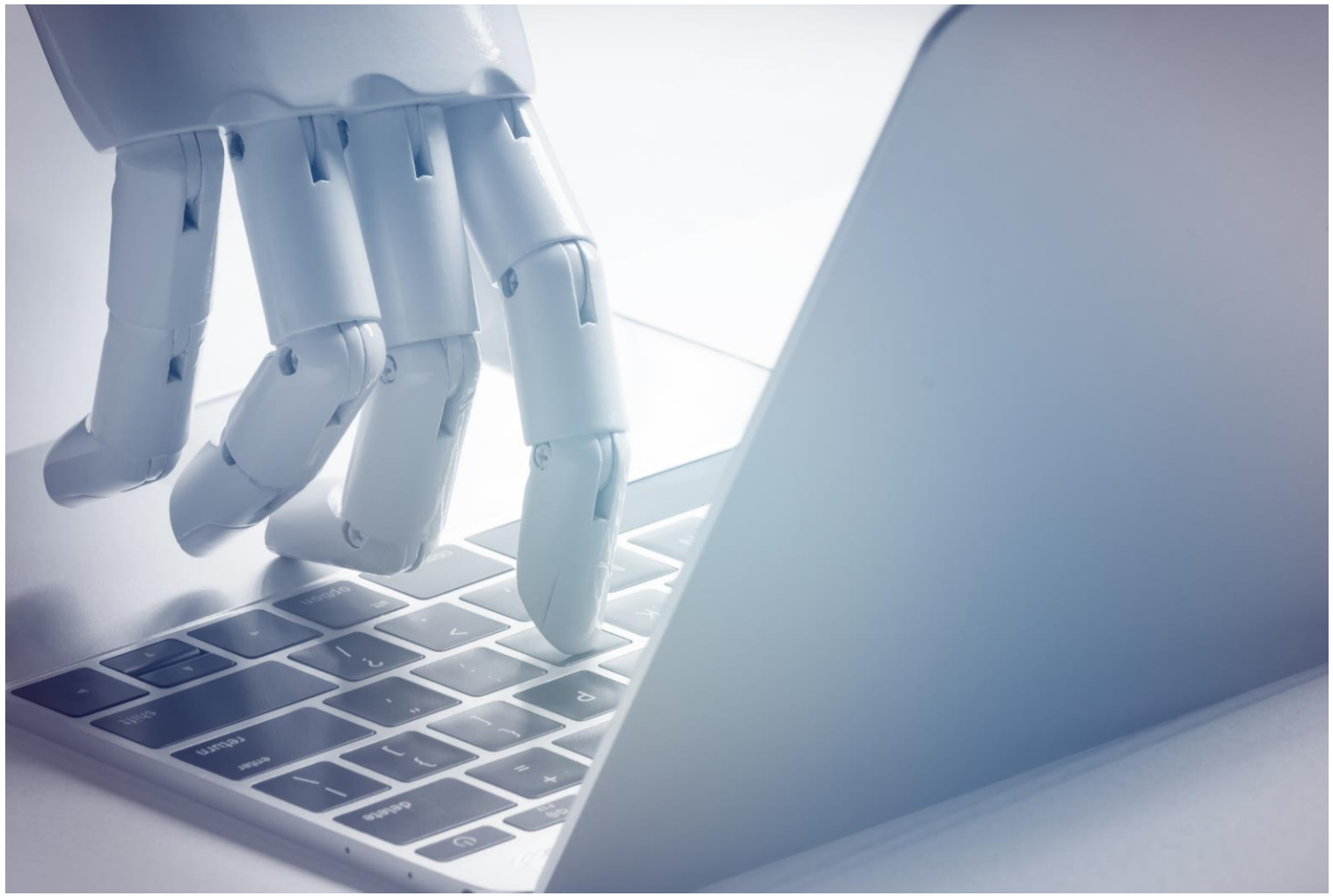
https://quantika14.com/dantes-gates-minimal-version/

Dante’s Gates Minimal versión

Análisis de Nicks y de personas

¿Qué vamos hacer?

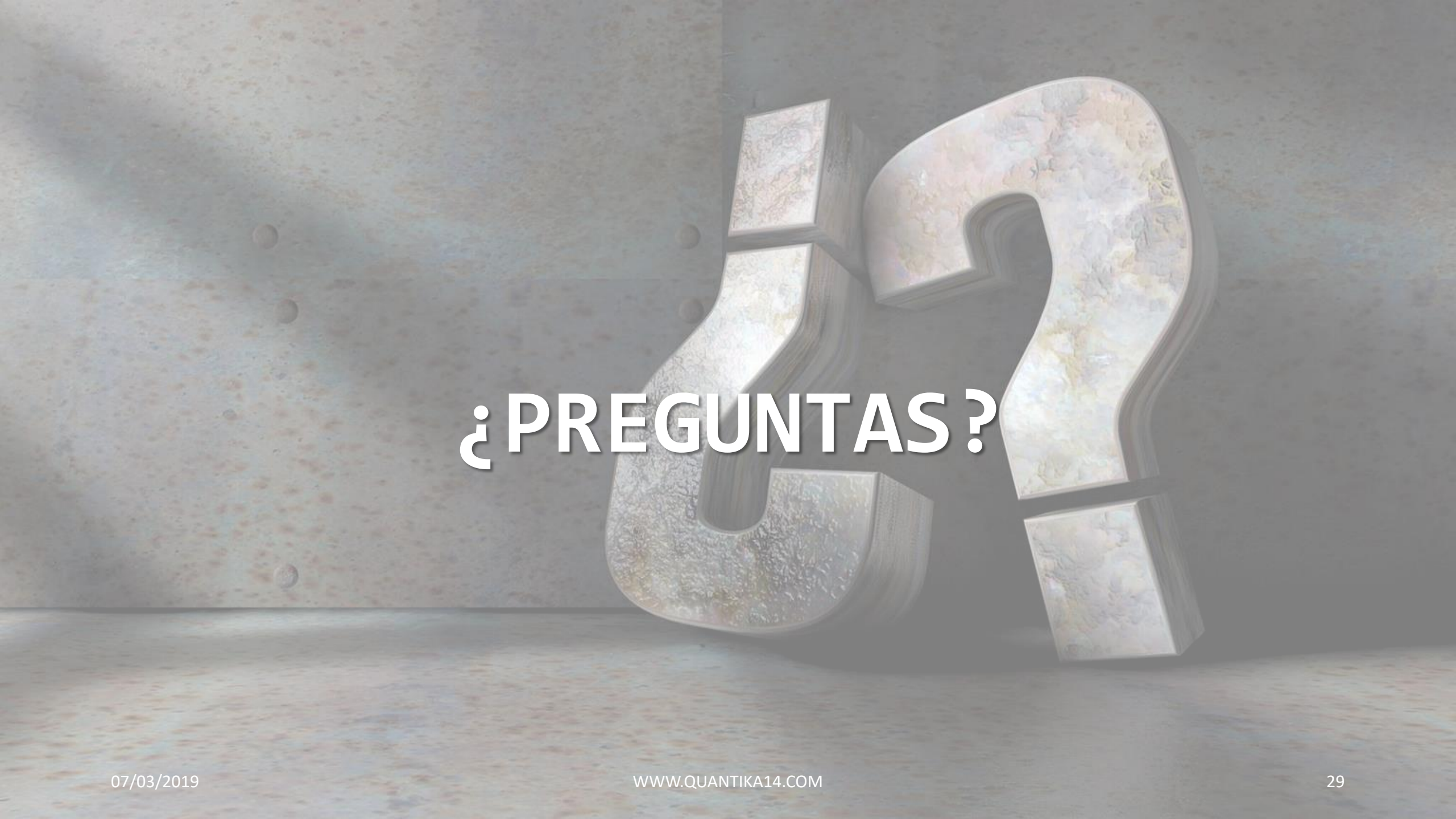
1. Extraer un JSON de un Hashtag Twitter
2. Crear un listado de las cuentas que han hecho tweet
3. Extraer el time line de todas las cuentas y generar un dataset
4. Encontrar emails y tlfn de los timelines
5. Investigar de forma automática cada Email y TLFN. Y obtener las redes sociales. Por último, crear una DB con todo.



DEMO TIME

Conclusión:

- Podemos buscar otros usuarios similares o con características parecidas.
- Big data con un perfilado de cuentas de Twitter
- **Analisis del time line del perfil es fundamental (pero lleva mucho tiempo)**


¿PREGUNTAS?

¡MUCHAS GRACIAS!

INVESTIGA CONMIGO DESDE EL SÜ

https://www.youtube.com/channel/UCotPHyHsSSyhly_RN02jvSg