I Know You

iKy

(Herramienta OSINT)

Presentada por Kenn Bro
Eterno aprendiz. Desarrollador apasionado.
Investigador anónimo. Amante de los patrones.

AGENDA

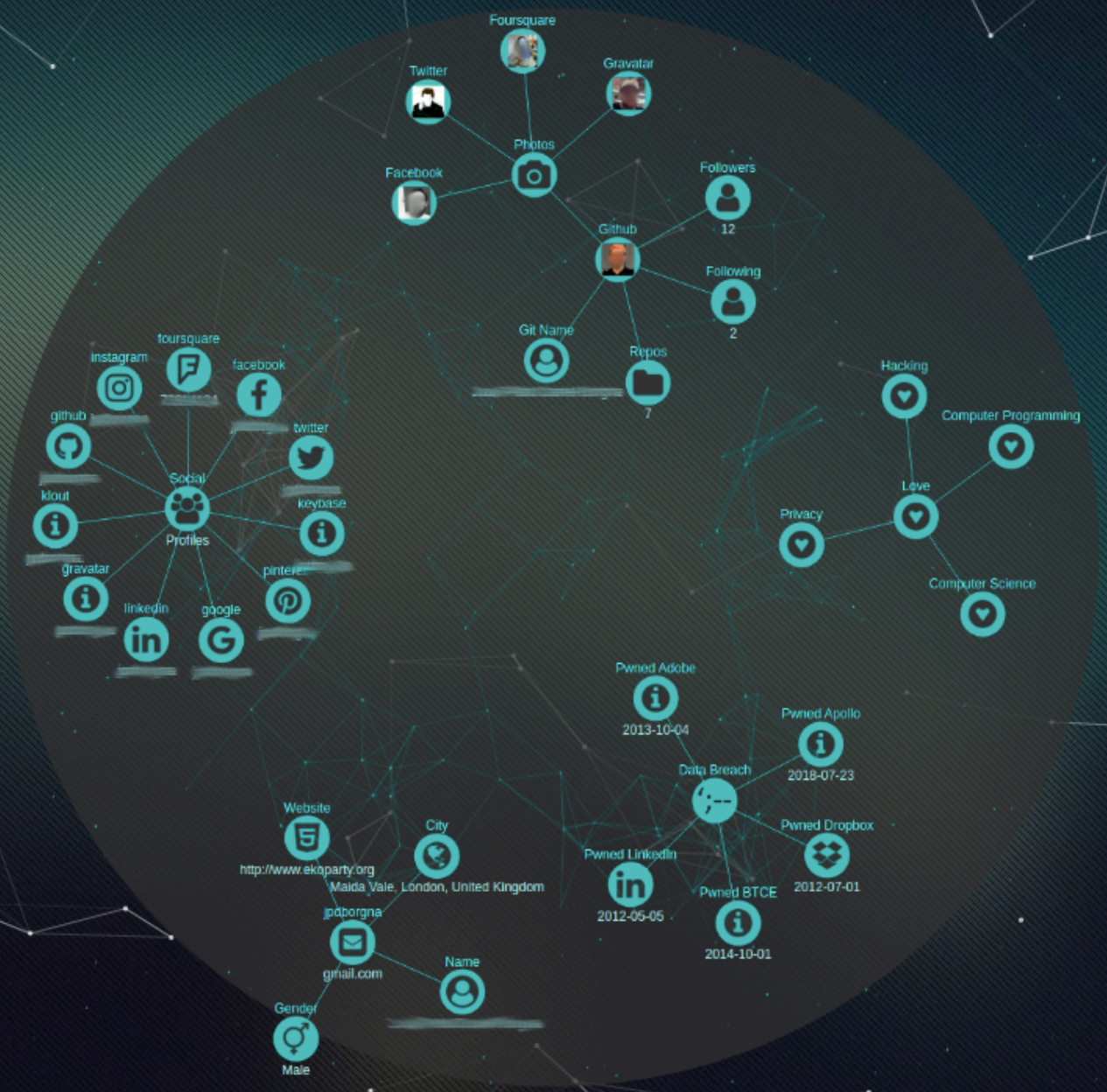
- PASADO - Porque es lo que es
- PRESENTE - Hasta donde llegamos
- DEMO - Revolución colono rectal
- FUTURO - A donde queremos llegar

PASADO

Ekoparty 2017 - Curso OSINT

Herramientas existentes

iKy (POC)


Foursquare
Twitter
Gravatar
Photos
Facebook
Followers
12
Github
Following
2
Git Name
Repos
7
foursquare
instagram
facebook
github
twitter
Social
Profiles
klout
keybase
gravatar
pinterest
linkedin
google
Hacking
Computer Programming
Love
Privacy
Computer Science
Pwned Adobe
2013-10-04
Pwned Apollo
2018-07-23
Data Breach
Pwned Dropbox
2012-07-01
Pwned LinkedIn
2012-05-05
Pwned BTCE
2014-10-01
Website
http://www.ekoparty.org
City
Maida Vale, London, United Kingdom
jpborgna
gmail.com
Name
Gender
Male

Brain Storming

Backend óptimo
Frontend futurista

Espectativa vs Realidad

PRESENTE

Y salió esto ...

iKy

- Home
- Gatherer
- Profile
- Timeline
- API Keys

HOME

Home / Home

MODULES GATHER TYPE

API modules	3
API Key modules	1
Crawlers	1
Proccess modules	2
Other	0

TO DO LIST

Task to do..

- Think about running the same module with different parameters
- Minor changes pending: grep -r -i TODO in the backend
- Use tag input to select the modules to will run
- Validation of username and email modules
- Create module Klout with crawling
- Manage multiples api keys
- List module and submodule

iKy

- Home
- Gatherer
- Profile
- Timeline
- API Keys

GATHERER

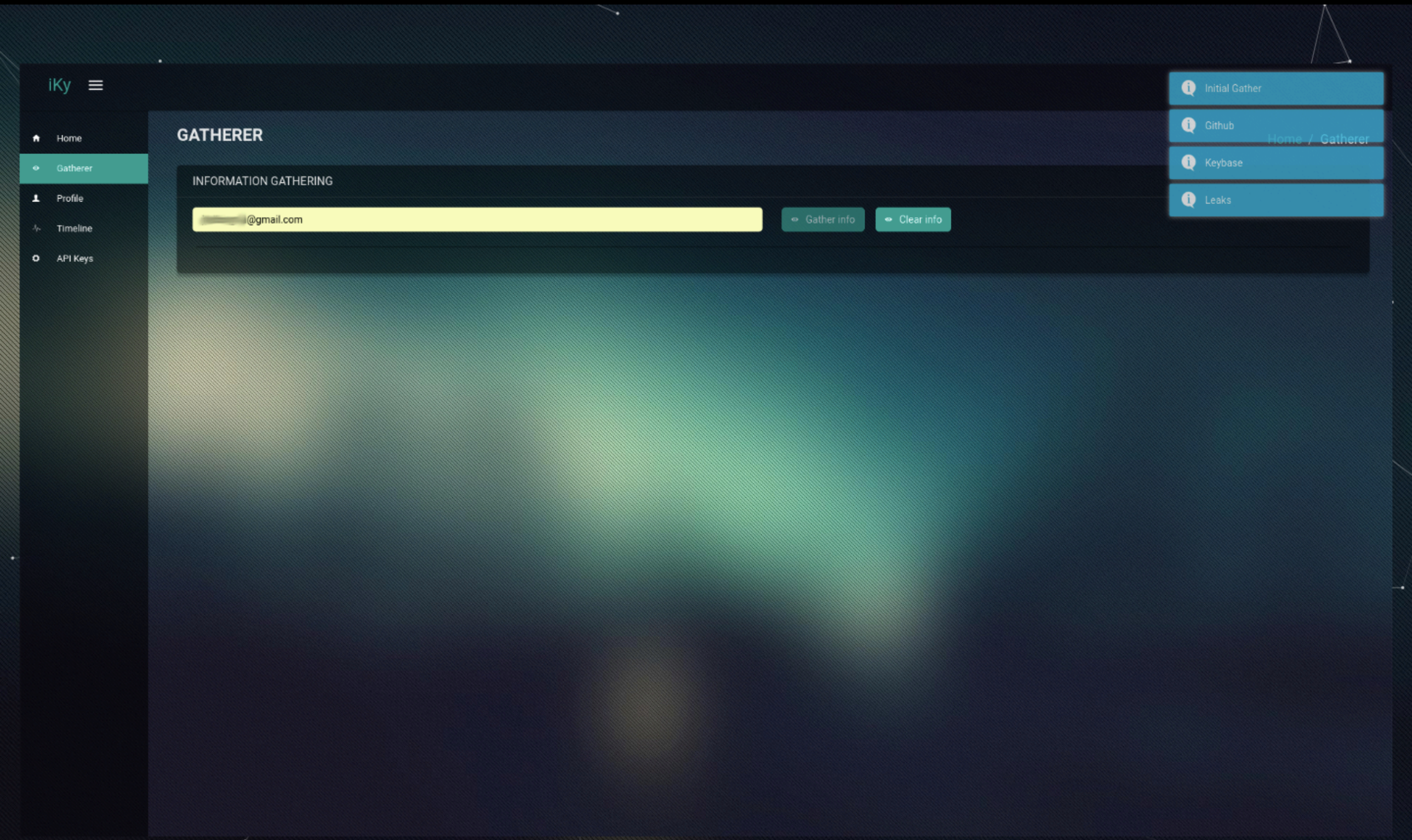
Home / Gatherer

INFORMATION GATHERING

Email

Gather info

Clear info


iKy
Home
Gatherer
Profile
Timeline
API Keys
GATHERER
Home / Gatherer
INFORMATION GATHERING
@gmail.com
Gather info
Clear info
Initial Gather
Github
Keybase
Leaks

iKy

GATHERER

Home / Gatherer

- Home
- Gatherer
- Profile
- Timeline
- API Keys

INFORMATION GATHERING

@gmail.com

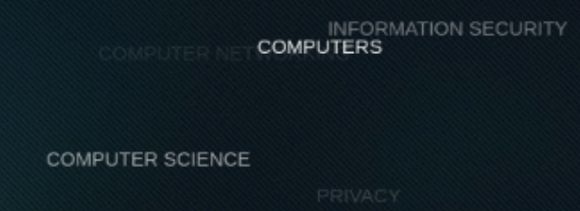
Gather info | Clear info

SOCIAL

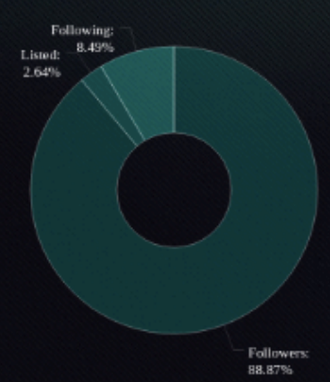
BIOS

Software/Hardware security researcher>

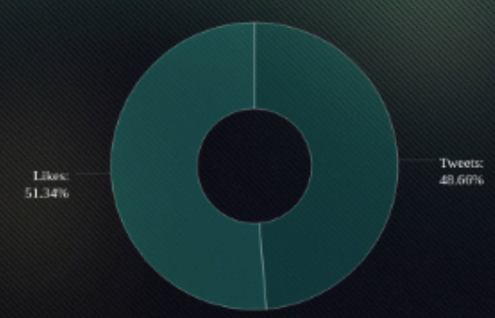
FOOTPRINT



TWITTER POPULARITY



TWITTER APPROVAL



TWITTER RESUME

iKy

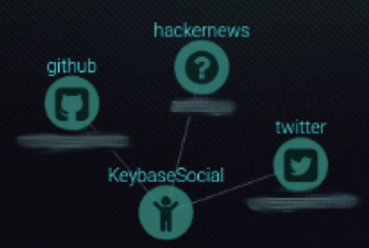
- Home
- Gatherer
- Profile
- Timeline
- API Keys

Followers:
88.87%

GITHUB

GITHUB CONTRIBUTIONS (TWO LAST YEARS)

KEYBASE SOCIAL



KEYBASE DEVICES

LEAKS

iKy

- Home
- Gatherer
- Profile
- Timeline
- API Keys

PROFILE

Home / Profile

General Information

Pictures

Name	[redacted]	Location	London, England, United Kingdom
Gender	Male		

Social Profiles

- facebook
- foursquare
- github
- google
- gravatar
- instagram
- keybase
- klout
- linkedin
- pinterest
- twitter

iKy

- Home
- Gatherer
- Profile
- Timeline
- API Keys

TIMELINE

Home / Timeline

Github : Update Account

2018/03/17 23:19:10

2016/03/18 00:16:26

Keybase: Create Account

Keybase : Update Account

2016/03/18 00:16:26

2014-10-01

Leak : BTC-E

In October 2014, <a href="https://www.databreaches.net/bitcoin-exchange-btc-e-and-bitcointalk-forum-breaches/" target="_blank" rel="noopener">the Bitcoin exchange BTC-E was hacked</a> and 568k accounts were exposed. The data included email and IP addresses, wallet balances and hashed passwords.

Github : Create Account

2013/01/08 22:39:50

2013-10-04

Leak : Adobe

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and <a href="http://stricture-group.com/files/adobe-top100.txt" target="_blank" rel="noopener">many were quickly resolved back to plain text</a>. The unencrypted hints also <a href="http://www.troyhunt.com/2013/11/adobe-credentials-and-serious.html" target="_blank" rel="noopener">disclosed much about the passwords</a> adding further to the risk that hundreds of millions of Adobe customers already faced.

Características

- Open Source
- GitLab (https://gitlab.com/kennbroorg/iKy)
- Instalación no tan fácil
- Vagrant (https://gitlab.com/kennbroorg/iKy-vagrant)

Arquitectura

- Redis - Base de datos en memoria
- Python 2 - Lenguaje
- Celery - Procesamiento paralelo
- Flask - Interface entre backend y frontend
- AngularJS - Frontend

Agregados recientes

- Ghostproject (Colaboración)
- Corrección de errores (Constantes)
- Validaciones
- Linkedin

Las correcciones son constantes porque cada vez que las páginas o los servicios cambian, debemos cambiar la manera de obtener los datos

Reescribimos el frontend...

...de AngularJS a Angular 7

iKy

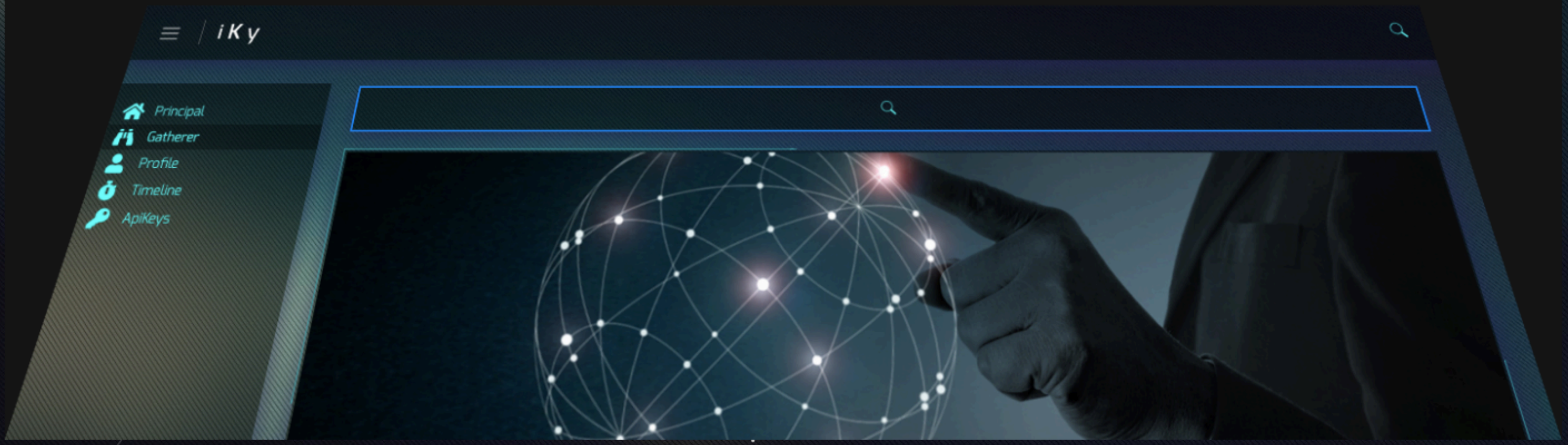
- Principal
- Gatherer
- Profile
- Timeline
- ApiKeys

Gathering information

To collect information it is necessary to enter an e-mail address in the search window that can be activated from the magnifying glass present in the button above or from the magnifying glass located in the upper right corner.

email@address

Hit enter to search



iKy

Principal
Gatherer
Profile
Timeline
ApiKeys

SEARCH | REPORT

SEARCH | REPORT

Tasklist
Process ended

Keybase
Send information gathering

Linkedin
Send information gathering

GitHub
Send information gathering

Fullcontact
Send information gathering

Tasklist
Send Tasklist process

iKy

- Principal
- Gatherer
- Profile
- Timeline
- ApiKeys

SEARCH | REPORT | JSON

FULLCONTACT Graphs

Validation

FULLCONTACT Bios

Validation

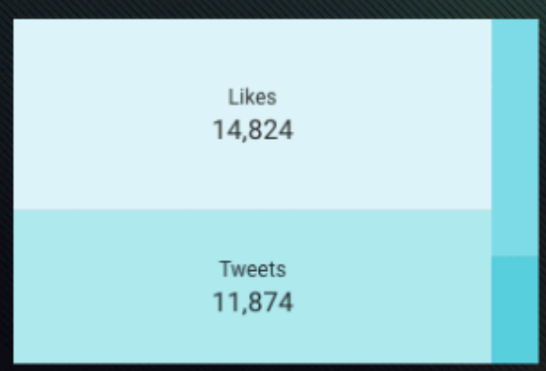
When it's all said and done, the Wired is just a medium of communication and the transfer of information. You mustn't confuse it with the real world.

TWITTER Popularity

Validation

TWITTER Resume

Validation

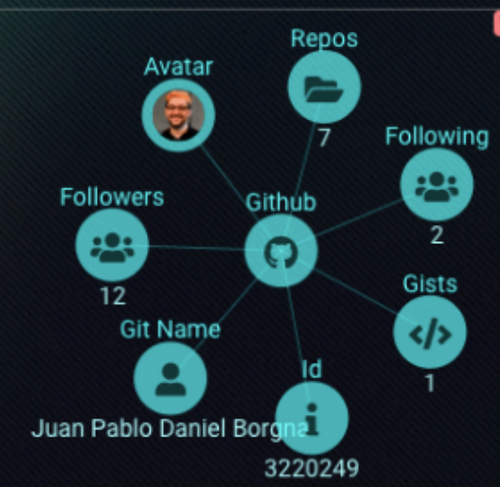


TWITTER Approval

Validation

GITHUB Graphs

Validation



iKy

3220249

- Principal
- Gatherer
- Profile
- Timeline
- ApiKeys

GITHUB Calendar

Validation

Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar

Mon
Wed
Fri

Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr

Mon
Wed
Fri

LINKEDIN Graphs

Validation

LINKEDIN Skill

Validation

LINKEDIN Certs

validation

LINKEDIN Positions

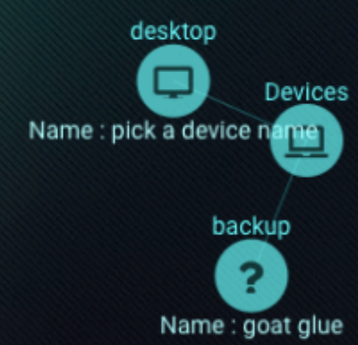
validation

UT **Universidad Tecnológica Nacional -**
EDUCATION

EN **EET Nro 4 -**
EDUCATION : TÉCNICO EN ELECTRÓNICA

KEYBASE Devices

Validation



KEYBASE Social

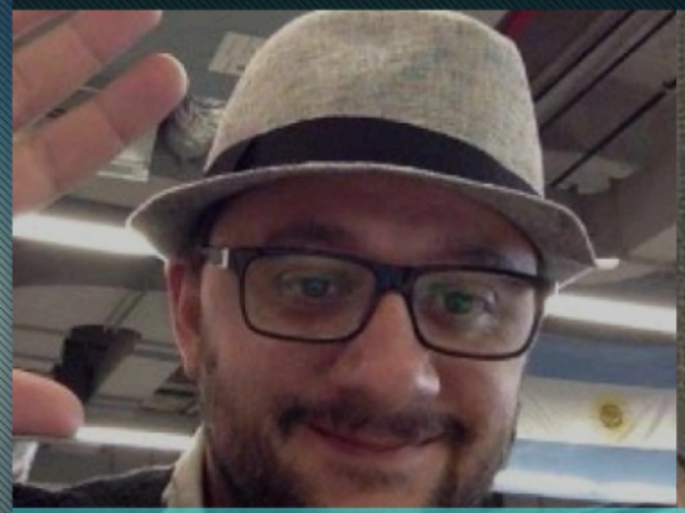
Validation

github

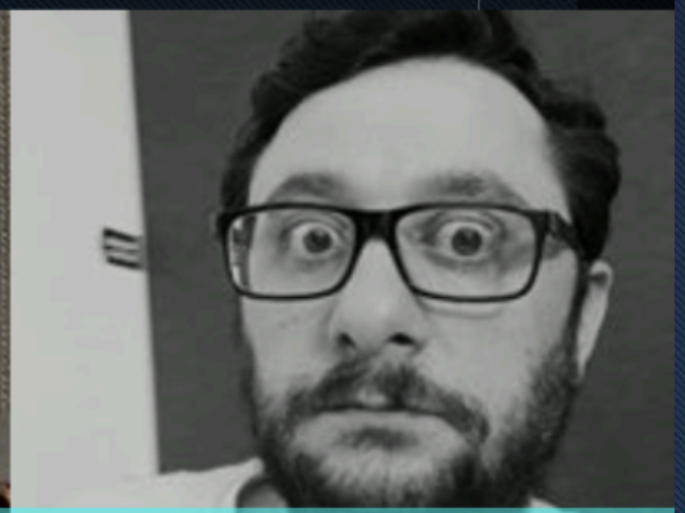
iKy

- Principal
- Gatherer
- Profile
- Timeline
- ApiKeys

Profile Photos


Gravatar

Github


Facebook

Foursquare

Twitter

Profile Data

iKy

Principal
Gatherer
Profile
Timeline
ApiKeys

Profile Data

Posible Name

JUAN PABLO DANIEL
BORGNA
JUAN PABLO DANIEL BOR(
BORGNA
JUAN

Posible Location

UNITED KINGDOM
[redacted]
LONDON, ENGLAND, UNITED KINGDOM

Posible Organization

N ENGINEER, SOMETHING LIKE DEVOPS, E

Profile Social

- facebook
- foursquare
- github
- google
- gravatar
- instagram
- keybase
- linkedin

iKy

- Principal
- Gatherer
- Profile
- Timeline
- ApiKeys

TIMELINE

Consultor

Twitter : Create Account — 2008/07/23 14:21:42

2008 — End :

Universidad Tecnológica Nacional -

Start : ekoparty security conference — 2007-01

organizer

2001 — Start :

Universidad Tecnológica Nacional - -

Reporting

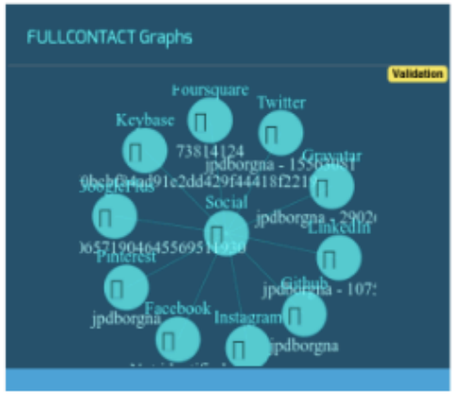
iKy
Principal
Gatherer
Profile
Timeline
Report
ApiKeys
SEARCH
REPORT
JSON
FULLCONTACT Graphs
Validation
Foursquare
Keybase
Twitter
FULLCONTACT Bios
Validation
TWITTER Popularity
Validation

Analyzed email

jpdborgna@gmail.com

Information gathered

Module fullcontact

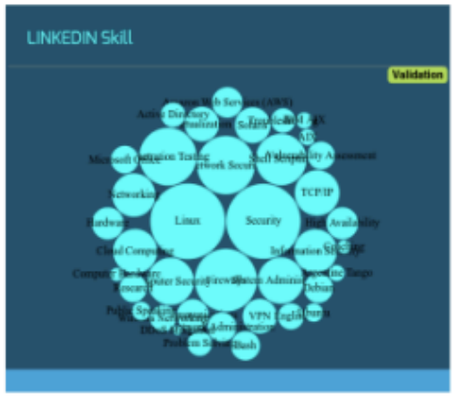


The information collected by the fullcontact module represented in the graph on the left shows the RRSS related to the e-mail analyzed.

The graph shows nodes, which have the name of the RRSS as upper title and the username in the lower part.

The information shown in the graph is shown in the table below.

RRSS	Username	Link
facebook		https://www.facebook.com/jpdborgna
foursquare		https://foursquare.com/user/73814124
github	jpdborgna	https://github.com/jpdborgna
google	jpdborgna	https://plus.google.com/106571904645569511930
gravatar	jpdborgna	https://gravatar.com/jpdborgna
instagram		https://instagram.com/jpdborgna
keybase	jpdborgna	https://keybase.io/jpdborgna
linkedin	jpdborgna	https://www.linkedin.com/in/jpdborgna
pinterest	jpdborgna	http://www.pinterest.com/jpdborgna/
twitter	jpdborgna	https://twitter.com/jpdborgna



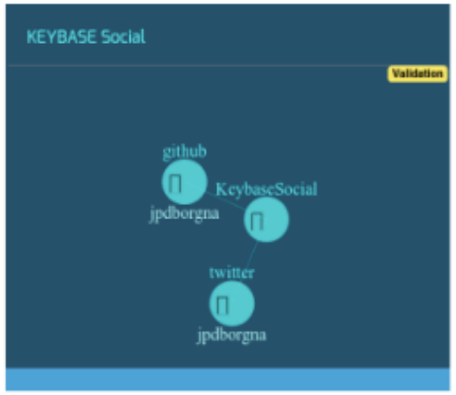
Principal skill.

Linux	67
Security	66
Firewalls	46
Network Security	40
Penetration Testing	39
Shell Scripting	31

Certifications	
Education :	Universidad Tecnológica Nacional -
Education : Técnico en electrónica	EET Nro 4 -

Positions
Facebook - Production Engineer
ekoparty security conference - organizer
spotflux - DevOps
GoIntegro - IT Infrastructure Leader
BASE4 Security - Consultor

Module keybase



The information of the chart is shown in the following table.

twitter	jpdborgna
github	jpdborgna

Timeline

2019/01/29 07:52:42
Github : Update Account -

2016/03/18 00:16:26
Keybase: Create Account -

2016/03/18 00:16:26
Keybase : Update Account -

2015-01
Start : Facebook - Production Engineer

2015-01
End : spotflux - DevOps

2013/01/08 22:39:50
Github : Create Account -

2013-03
End : GoIntegro - IT Infrastructure Leader

DEMO

FUTURO

Agregar muchas más RRSS (Sin autenticar, autenticando, con APIs)

Search Dorks (Google, Bing, Yandex, DuckDuckGo, Searx, etc)

Image Reverse Search (Yandex Image Search with facial recognition)

Social Mapper - A Social Media Enumeration and Correlation Tool

Free Public Record Search

Leer mucho código y hacer mucha investigación

Correcciones constantes porque cada vez que las páginas o los servicios cambian, debemos cambiar la manera de obtener los datos. Este tipo de aplicaciones envejecen más rápido de lo normal

Agradecimientos

ParanaConf

ekoparty security conference

+GiBa

OSINT Latam Group

Secure Podcast

Nebular framework

datasploit

tinfoleak - Vicente Aguilera Díaz

Contributors

@emips_sk

@jiannelli

@sebabeva

Contacto

https://gitlab.com/kennbroorg/iKy

@kennbroorg

kennbro <at> protonmail <dot> com

https://kennbroorg.gitlab.io/ikyweb/

https://vimeo.com/326114716

https://gitlab.com/kennbroorg/iKy-vagrant

GRACIAS