OSINT, OSANT CADA DÍA TE QUIERO MÁS: CASO REAL DE OSINT

INVESTIGACIONES OSINT EL PRESENTE Y FUTURO

JORGE CORONADO

WWW.QUANTIKA14.COM


#SVQTECH
SEVILLA
SVQ JS
SVQXDG
Sevilla Xamarin Developer Group
THE THINGS NETWORK SEVILLA
Qa
Sevilla
salesforce
HACKING SEVILLA
SVQ DATA BEERS
RAILS
MAKER SOCIETY
SEVILLA WASN'T BUILT ALONE
#SVQTECH
GDG Sevilla
PHPSevilla
Developers group of PHP technologies

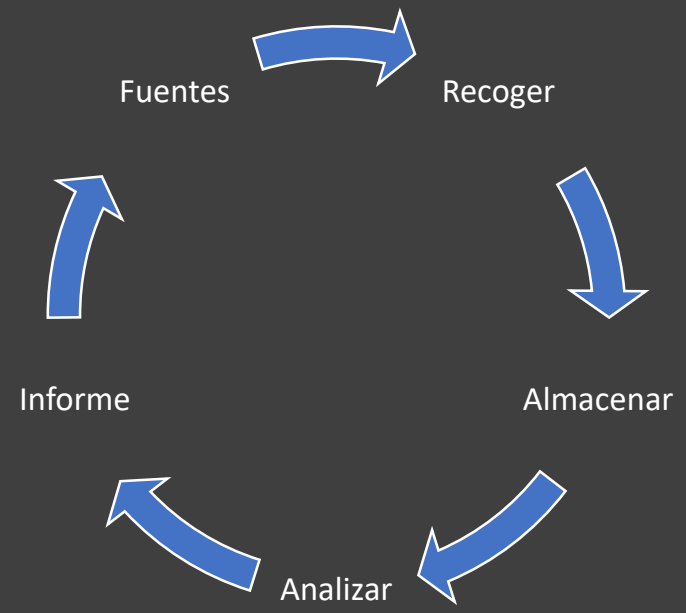
Quién es Jorge Coronado

- 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
- 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**

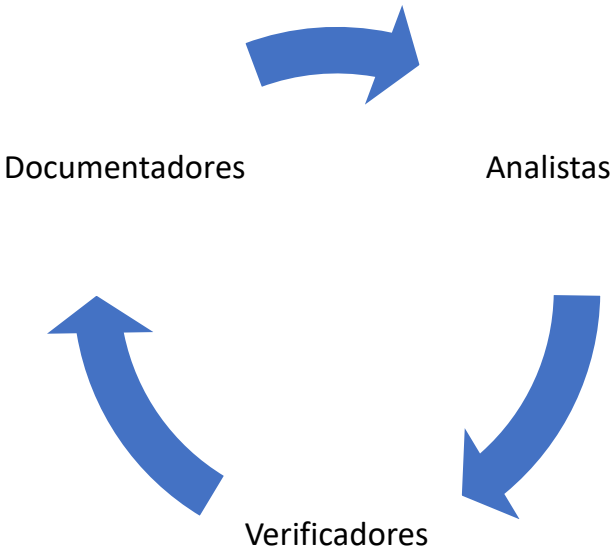
¿Qué vamos a ver?

- 1. Conceptos básicos
  - OSINT
  - SOCMINT
  - BOTS
  - CRAWLERS
- 2. Qué es Dante’s Gates Minimal Version
- 3. Cómo instalarlo
- 4. EO-ripper
- 5. Demo time

1.1 ¿Qué es el OSINT y el SOCMINT?

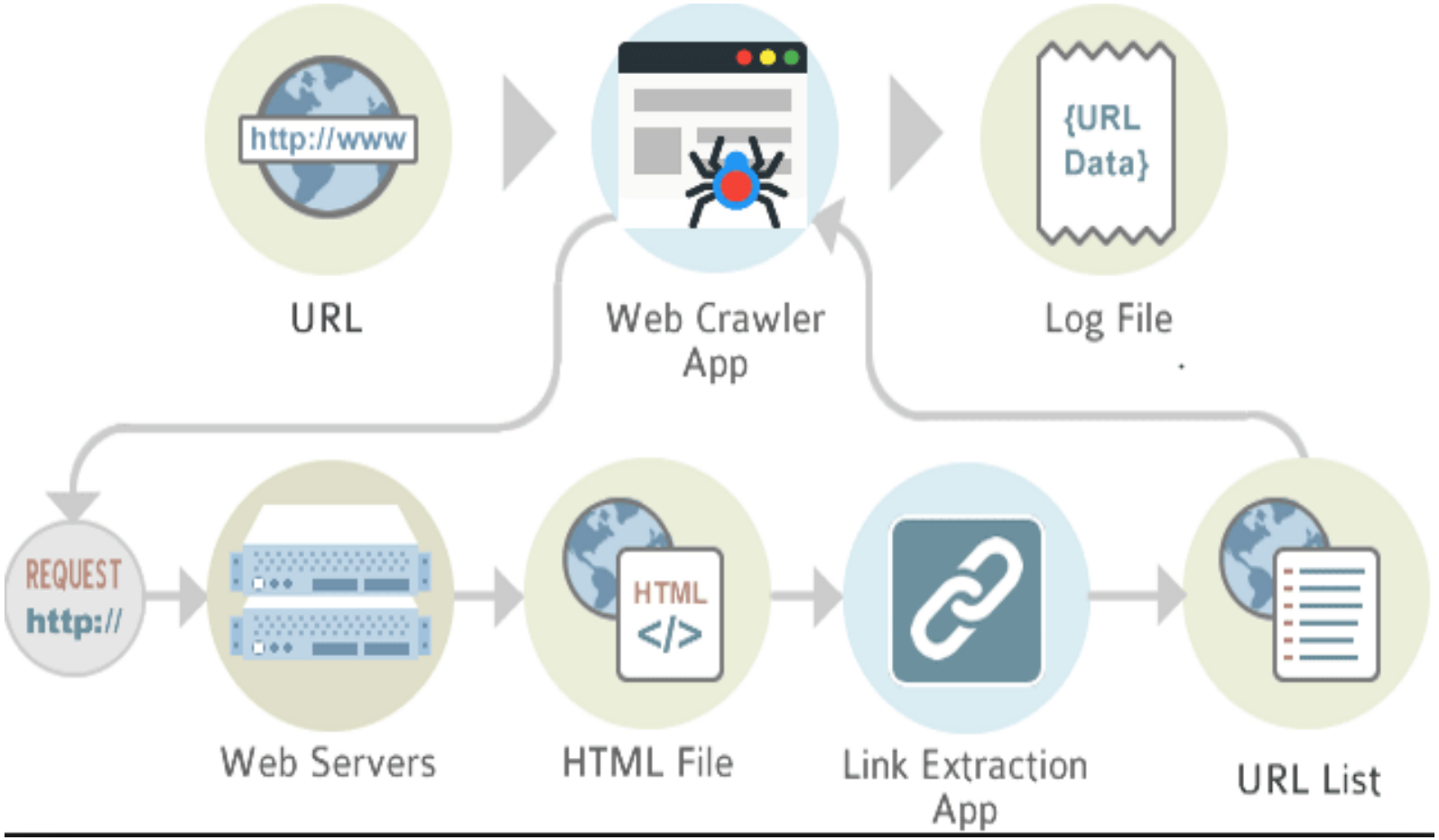


1.2 Niveles en inteligencia



1.3 ¿Qué es un bot?

1.4 ¿Qué es un Crawler?



¿Qué son los datos iniciales?

Metodología

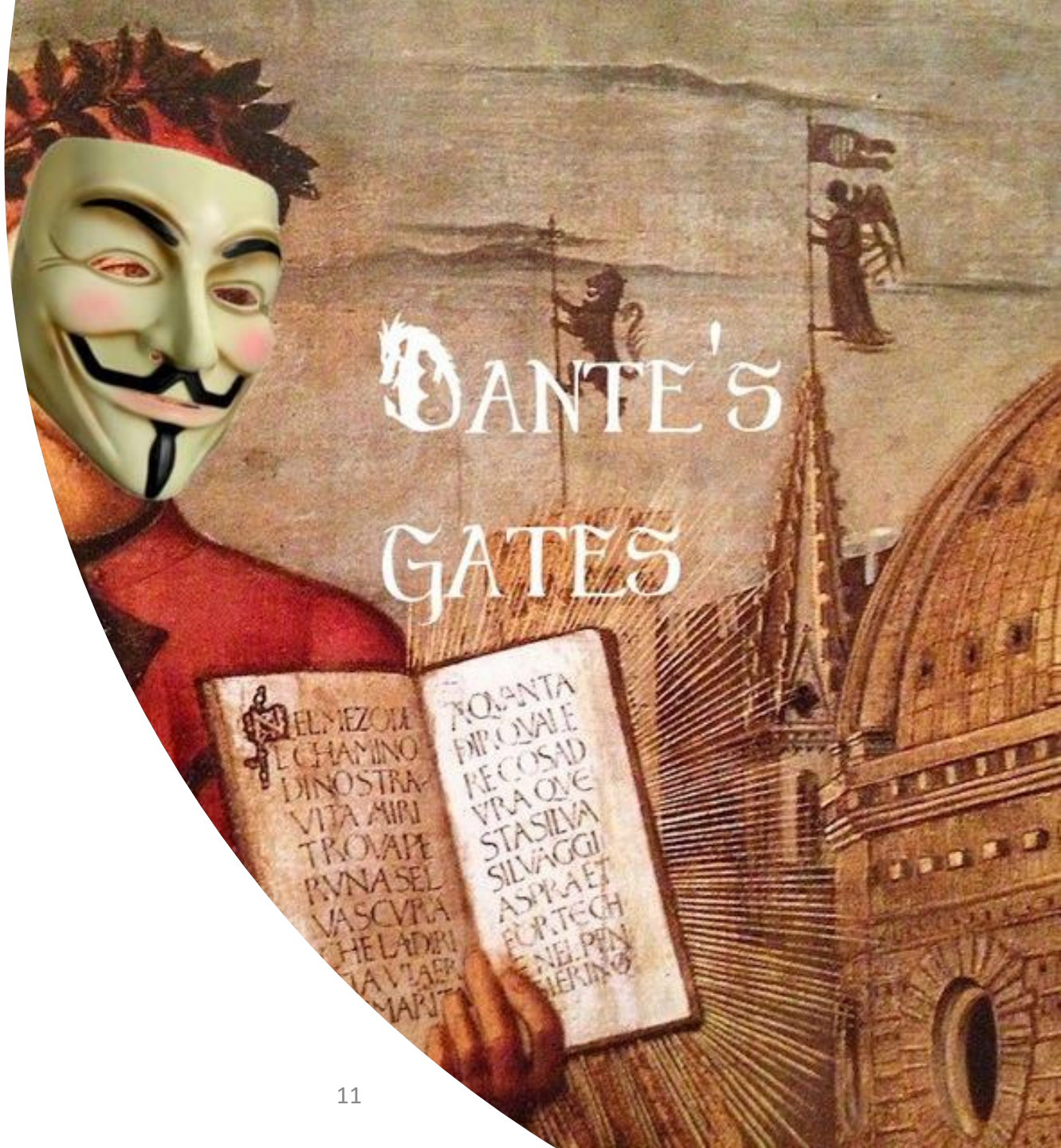
1. Identificación de datos iniciales
2. Análisis automático con buscadores (Dante's Gates Minimal Version, EO-ripper, etc)
3. Análisis manual
4. Creación de informe

Con los **datos iniciales** creamos un dataset de información que tendrá que ser verificado.

2. ¿Qué es Dante's Gates Minimal Version?

- Código abierto
- Python 2.7
- Suit de herramientas para hacer OSINT en España

- CÓMO DESCARGAR: https://github.com/Quantika14/osint-suite-tools



¿De dónde viene DG MV?

Un Proyecto de QuantiKa14.

- Página web -> acceso limitado
- Bot de Telegram -> DEAD

Proyecto open source: Dante´s Gates Minimal version

DANTE GATES™
What does internet know about you?

2.1 ¿A quién le puede interesar DG.MV?

- Detectives
- Periodistas
- Peritos informáticos
- Cuerpos de seguridad
- Recursos humanos

2.2 ¿En qué puede ayudar?

- **Investigaciones privadas usando OSINT** (casos de corrupción, desfalco, terrorismo, etc)
- Auditorías de seguridad informática (proceso de footprinting y figerprinting)
- Marketing (estudios de mercados, competencia, etc)
- Prueba digital para un peritaje informático

Transparencia ciudadana

DISCLAIMER:

El autor de esta aplicación no se ha responsable de su uso. Su intención es formativa y capacitar a los ciudadanos a ejercer su derecho a la transparencia en España con el uso de herramientas OSINT.

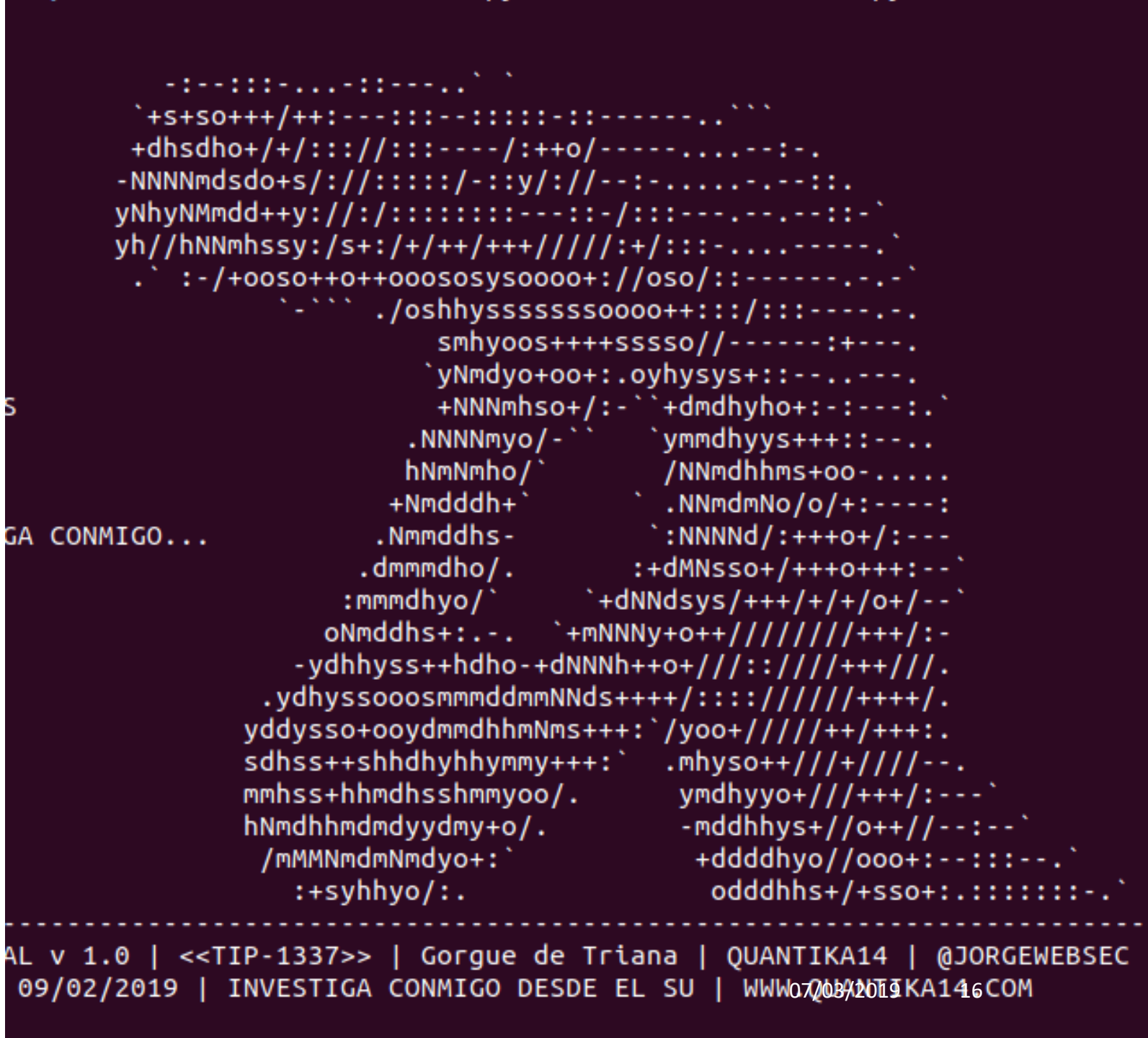
2.3 ¿Cómo se estructura Dante's Gates Minimal Version?

- Buscadores (scripts):
  - Buscador de personas
  - Buscador de niks
  - Buscador de emails
  - Buscador de Ips (-)
  - Buscador de TLFN(-)
  - Buscador de empresas(-)
- Bots y crawlers:
  - LinkedIn
  - Web
  - Pdfs
  - BOE y BORME
  - TESTRA
  - Adjudicaciones (-)
  - Imágenes

- Archivos: JSON, CSV, PDF e imágenes (por major y guardar en DB)
- Base de datos en local con MongoDB (crear una API)

2.4 BuscadorPersonas.py

- Wikipedia
- BORME
  - Cargos actuals
  - Cargos anteriores
  - Busca adjudicaciones en “data”
  - Busca adjudicaciones en MongoDB
- Youtube
- Páginas amarillas
- Infojobs
- Búsquedas con Bing y DuckDuckGo
- “Data”



2.5 APIS y librerías

- Wikipedia: https://pypi.org/project/wikipedia/
- Libreborme API: https://libreborme.readthedocs.io/es/latest/api/
- Dryscape: para scraping en webs con JS
- BeautifulSoup: parsing
- PDFGREP: para extraer texto PDF

```
>>> import wikipedia
>>> print wikipedia.summary("Wikipedia")
# Wikipedia (/ˌwɪkɨˈpiːdiə/ or /ˌwɪkiˈpiːdiə/ WIK-i-PE

>>> wikipedia.search("Barack")
# [u'Barak (given name)', u'Barack Obama', u'Barack (
```

```
$ curl -s "https://libreborme.net/borme/api/v1/empresa/search/?q=Gowex+Malaga&page=1" | python -m
{
    "objects": [
        {
            "name": "GOWEX MALAGA",
            "resource_uri": "/borme/api/v1/empresa/gowex-malaga/",
            "slug": "gowex-malaga"
        }
    ]
}
```

2.6 Buscador de Nicks

- 90 webs
- Verificación por URL
- Mejoras:
  - Base de datos
  - Usar buscadores (DDG, Google, Bing, etc)

2.7 Tipos de bots/crawlers

- **Estáticos:** es utilizado solo una vez
- **Dinámicos:**
  - Aplicaciones que se ejecutan cada X tiempo
  - Aplicaciones que están en ejecución todo el tiempo

```
sudo crontab -e
```

Ejecutar un script de lunes a viernes a las 2:30 horas:

```
30 2 * * 1-5 /bin/ejecutar/script.sh
```

Ejecutar un script de lunes a viernes cada 10 minutos desde las 2:00 horas durante una hora:

```
0,10,20,30,40,50 2 * * 1-5 /bin/ejecutar/script.sh
```

Esto quizá puede ser largo. La sintaxis de crontab permite lo siguiente. Imaginemos que queremos ejecutarlo cada 5 minutos:

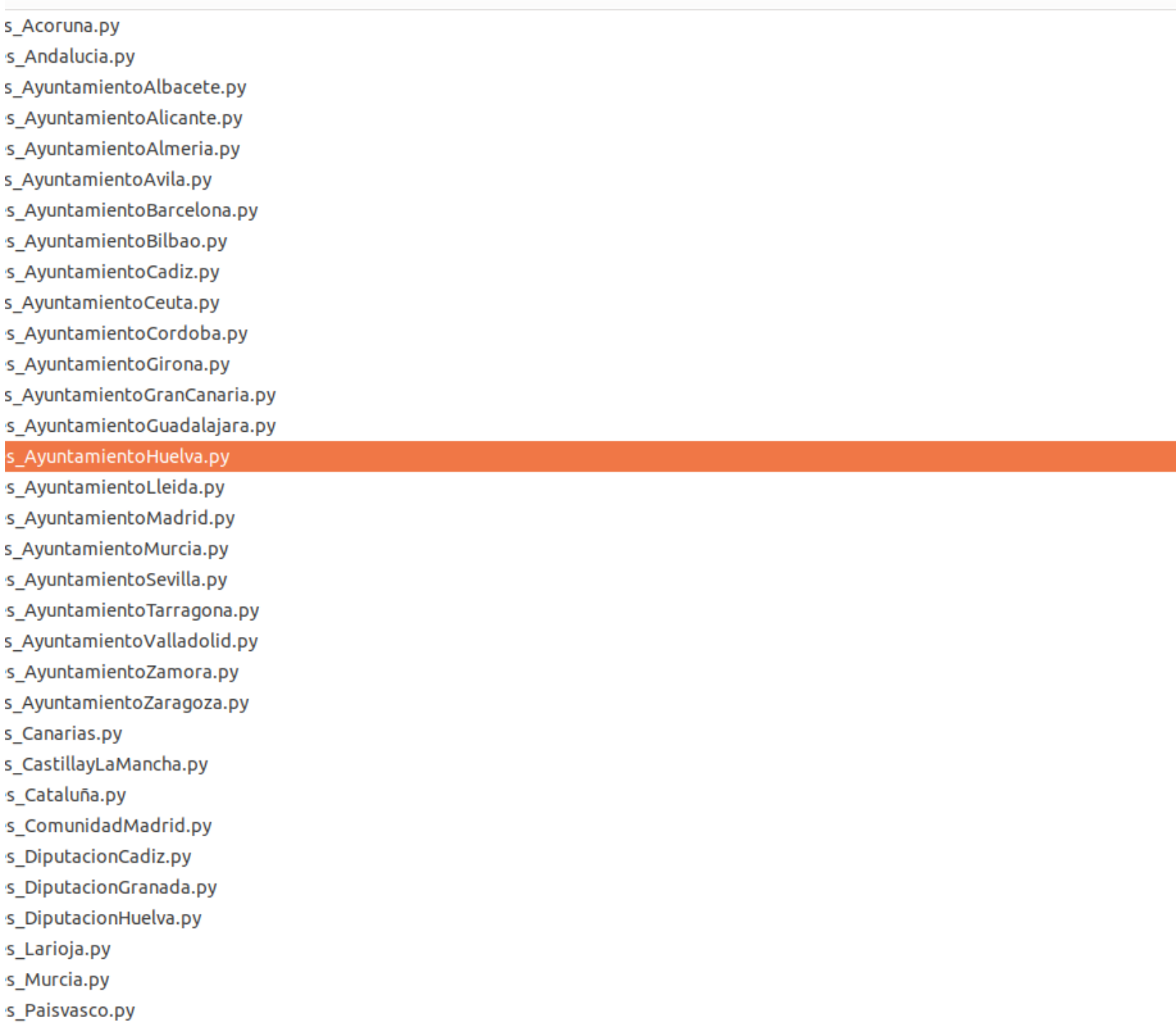
```
*/5 2 * * 1-5 /bin/ejecutar/script.sh
```

2.8 Ejemplo bot estático:

- PDF_CRAWLERS WEBS: https://github.com/Zealcui/pdfcrawler
- $python pdfcraler.py %dir %URL

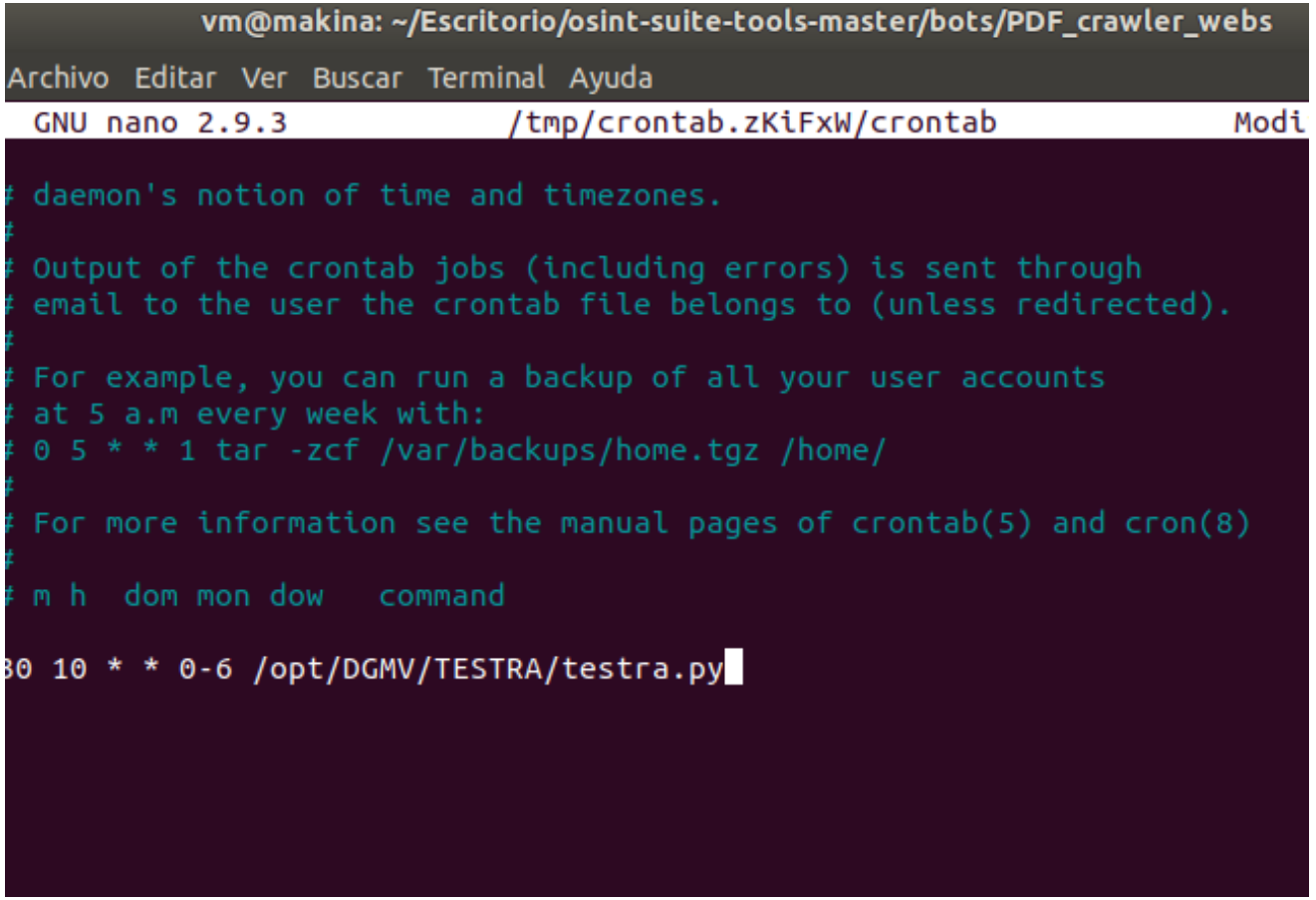
2.9 Ejemplo de bot dinámico y continuo

- Adjudicaciones
- BOE y BORME
- WEB crawler
- Redes Sociales
- Leak Offshore (https://offshoreleaks.icij.org/)



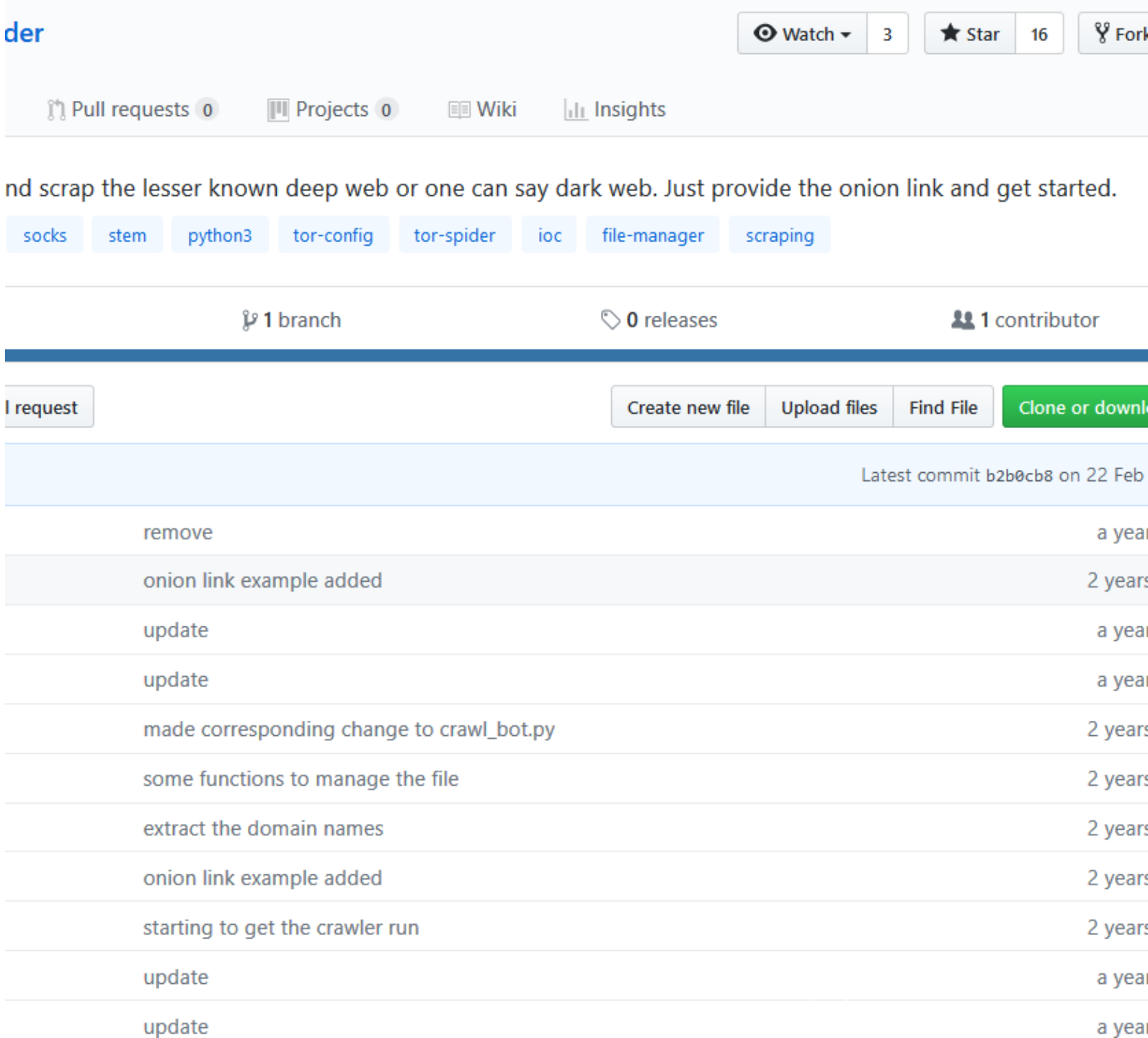
2.10 Ejemplo de bot dinámico

- **TESTRA:** ejecutar la aplicación todos los días a las 10:30 de la mañana



2.11 Tor Spider:

- Enlace: https://github.com/absingh31/Tor_Spider
- En el archive onions copiamos las rutas que queremos descargar
- Copiamos los archivos generados dentro de la carpeta data



2.12 Problemas actuales

- Python 2.7
- Buscadores como Google, DuckDuckGo, Bing, Shodan, etc.
- Open data de la administración
- Lento

2.13 Mejoras

- Python 3
- Configurar conexiones y búsquedas por base de datos
- Disminuir archivos en data, insertarlos y crear un índice
- Multihilos
- Expresiones regulares
- Sistema de informes
- Interfaz web
- Paraisos fiscales
- Registros mercantiles de otros paises

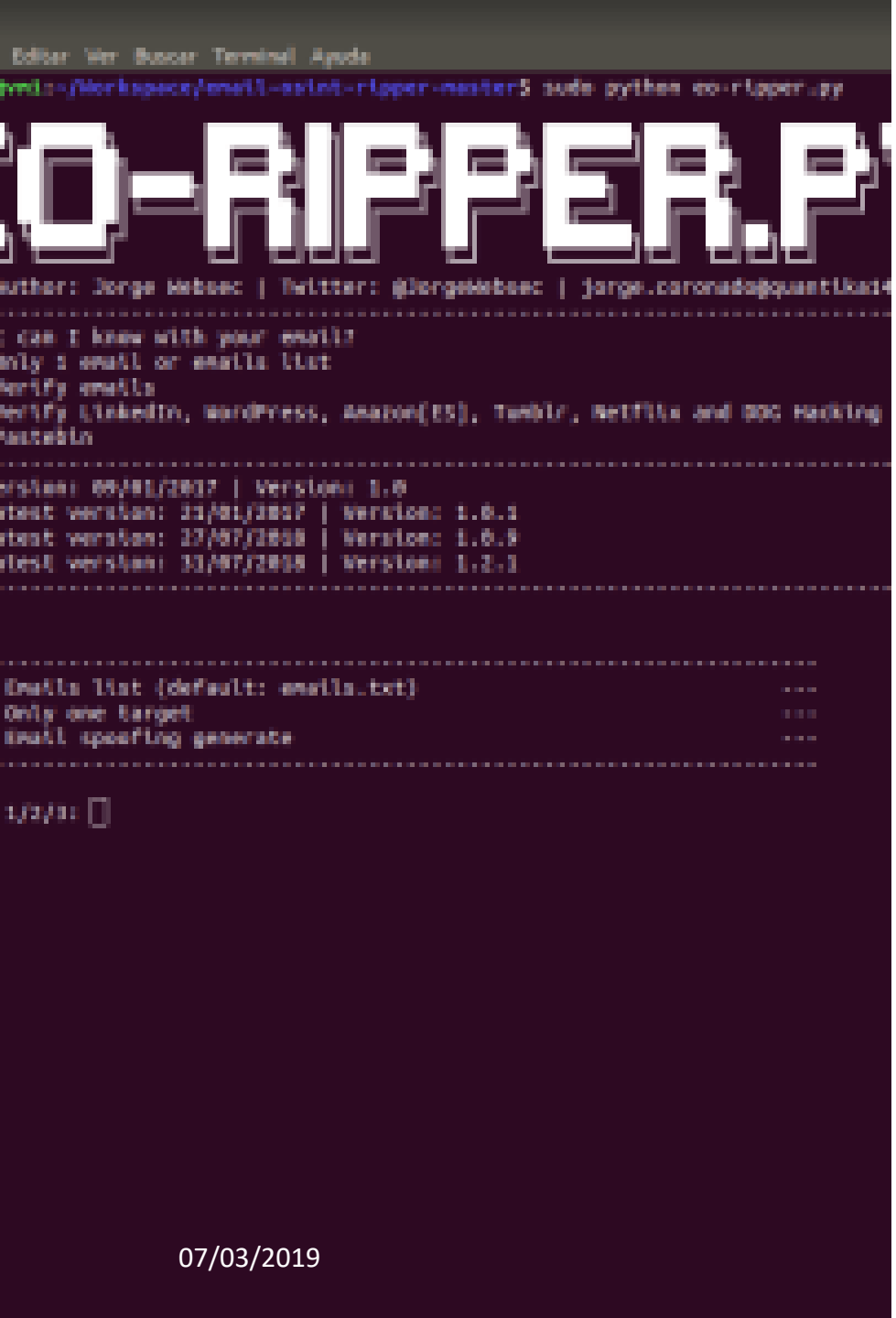
3. ¿Cómo instalar Dante's Gates Minimal Version?

1. En Linux descargamos el repositorio: https://github.com/Quantika14/osint-suite-tools
2. Lo descomprimimos en /opt/
3. Instalamos PDFgrep: "sudo apt install pdfgrep"
4. Instalamos las librerías: "sudo pip install –r requeriments.txt"

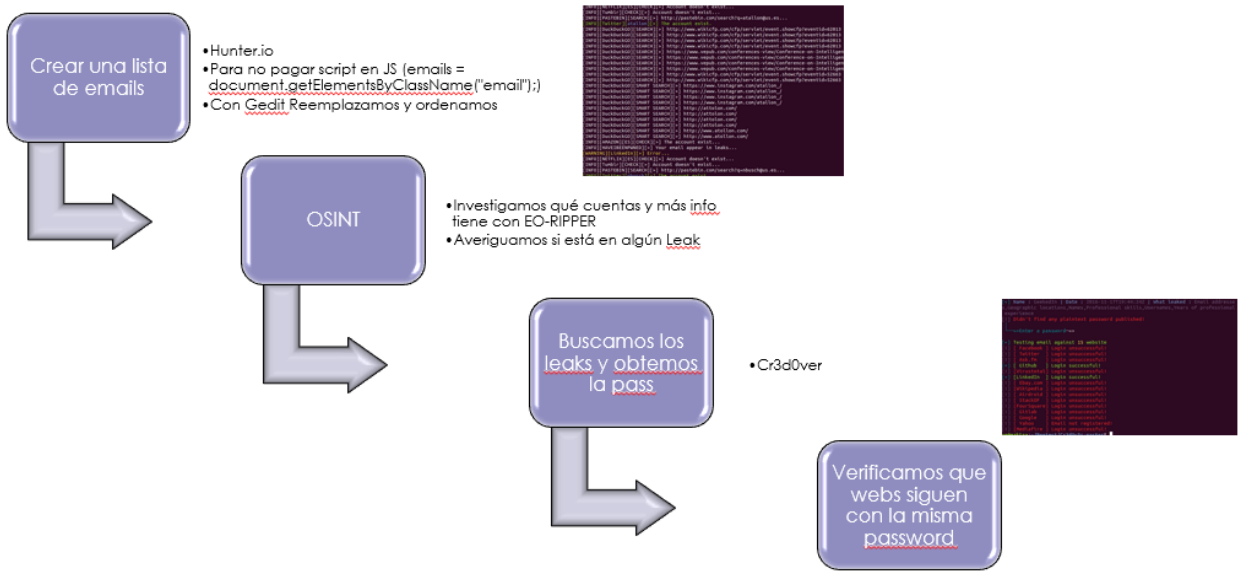
- 5. Ejecutamos nuestros bots para obtener información
- 6. Ejecutamos el buscador que queramos:
  - BuscadorPersonas.py
  - BuscadorNiks.py

4. ¿Cómo crear un buscador de la Deepweb?

- Darksearch api
- Intelx.io
- Crawlers buscando .onion
- Crawler recursive buscando .onion en la deepweb



5. Buscador de Email: EO-Ripper https://github.com/Quantika14/email-osint-ripper



¿Investigas conmigo?
DEMO TIME

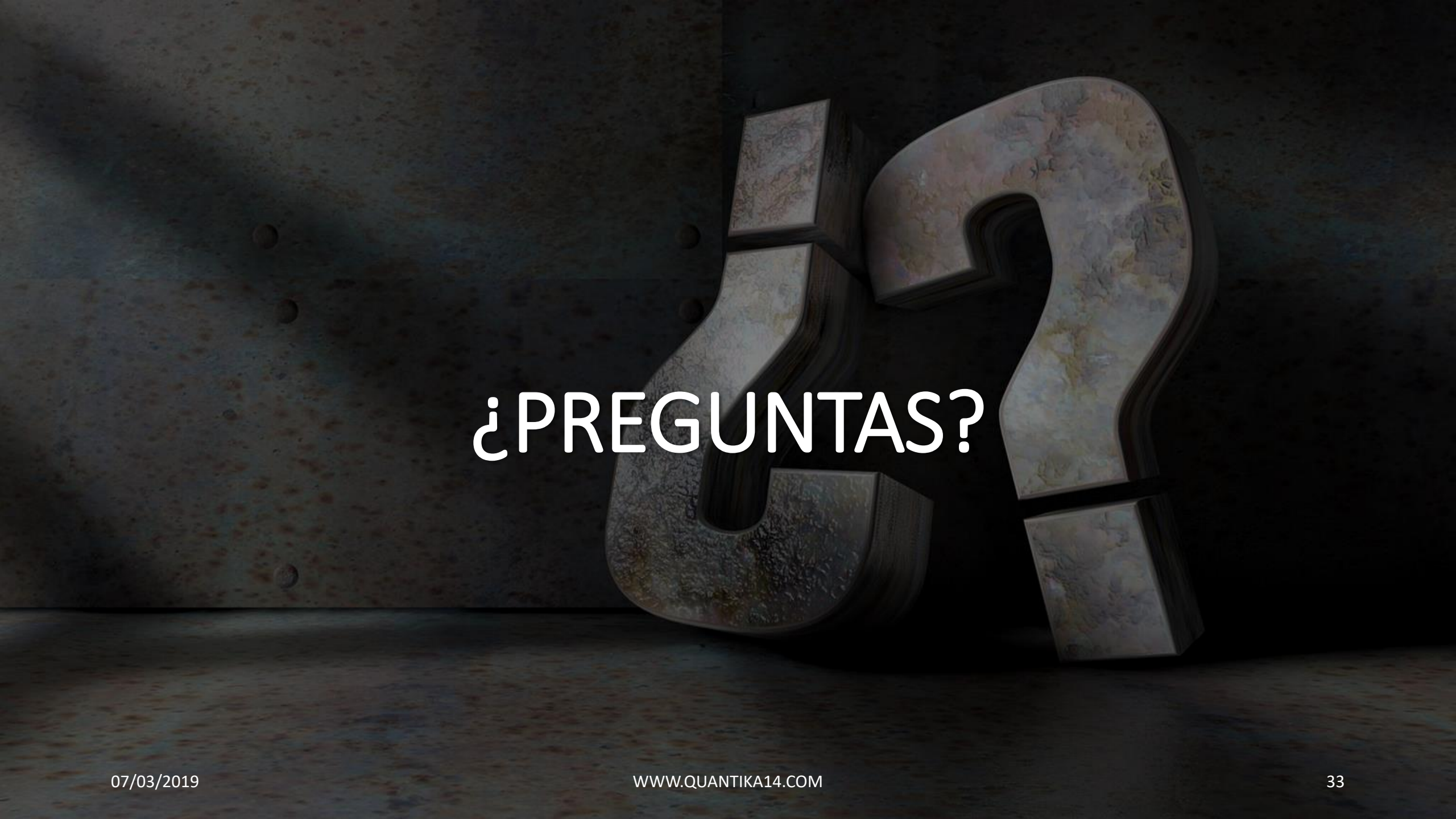
Investiga conmigo desde el Sü: capítulo I

- https://www.youtube.com/watch?v=zI11NiQcx-I

CONGRESO SOBRE #OSINTCITY2020

WWW.OSINTCITY.COM

Las investigaciones OSINT no son solo buscar en Google, es crear inteligencia con fuentes abiertas. Por ello, el big data y data science es parte del OSINT usando Internet.


¿PREGUNTAS?

¡MUCHAS GRACIAS!

INVESTIGA CONMIGO DESDE EL SÜ

https://www.youtube.com/channel/UCotPHyHsSSyhlyRN02jvSg