PROYECTO ATRAPABOT

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

ATRAPABOT

por Diego Cerqueira

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

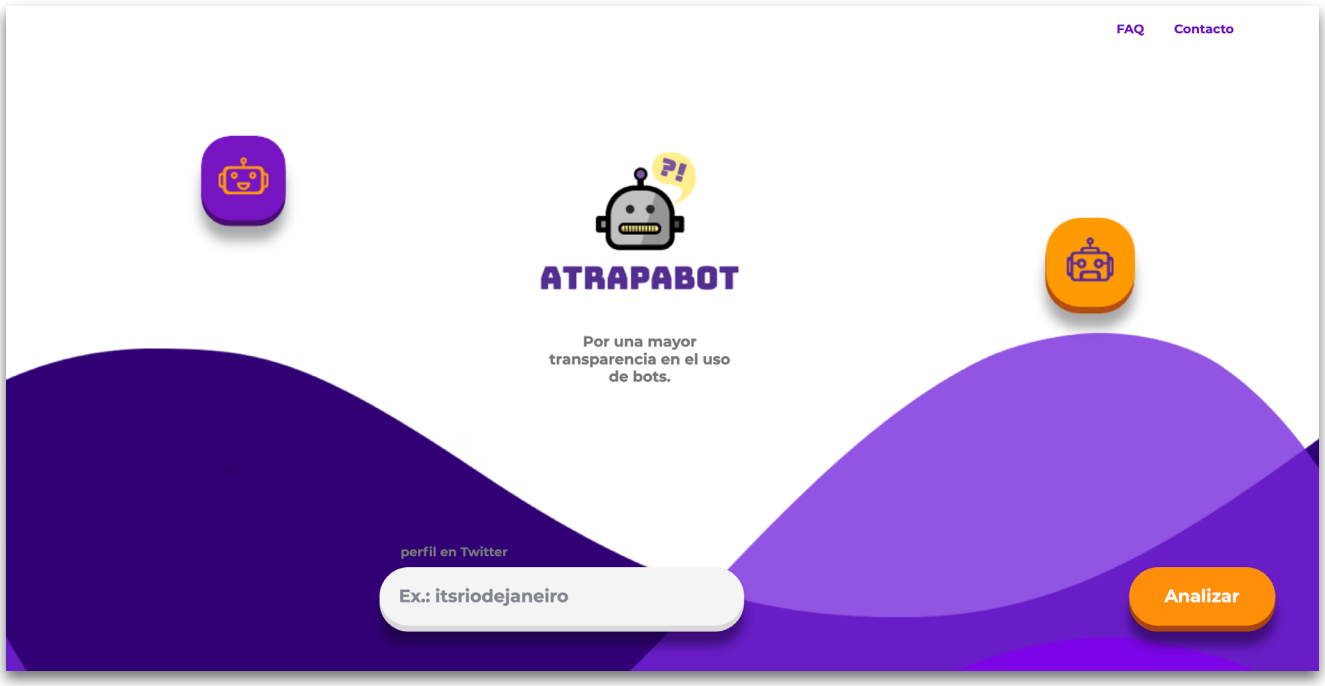
EN ESTE TUTORIAL, CONOCERÁS LA HERRAMIENTA ATRAPABOT. ¡APROVÉCHALO!

1. LO QUÉ ES

Atrapabot es una herramienta gratuita desarrollada por el Instituto de Tecnologia e Sociedade (ITS Rio) en conjunto con el Instituto de Tecnologia & Equidade (IT&E), para concientización sobre el fenómeno de bots en las redes sociales. Actúa como un instrumento de Educación Mediática sobre fenómenos de diseminación por medio de automatización en Twitter.

El Atrapabot permite la identificación de cuentas con probabilidad de que sean bots en la plataforma. Para ello, el usuario solo tiene que buscar los arrobas (conocidos como Handle) de usuarios de Twitter para obtener el resultado porcentual de lo cuán bot el perfil es considerado. De esta manera, a cada usuario buscado, el Atrapabot realiza un análisis probabilístico en relación al comportamiento del usuario en la red social. Para montar su análisis, el Atrapabot lleva en consideración diferentes criterios, que van desde el sentimiento expreso por los tuits publicados hasta la frecuencia de publicaciones del perfil analizado y los intervalos de tiempo entre las publicaciones.

La herramienta ha sido construida en código abierto y cualquier persona que tenga interés puede verificar los códigos fuentes. El Atrapabot encoraja y busca constantemente mejoras por medio de colaboraciones hechas por comunidades de desarrolladores y demás investigadores del área.



Página inicial del Atrapabot (https://es.pegabot.com.br/)

2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES

En la versión actual del Atrapabot es posible realizar el análisis de cualquier perfil de Twitter, individualmente, para verificar el porcentaje probabilístico de que la cuenta sea un robot. Todavía no hay la posibilidad de realizar análisis de diversos perfiles simultáneamente.

3. CÓMO ACCEDER

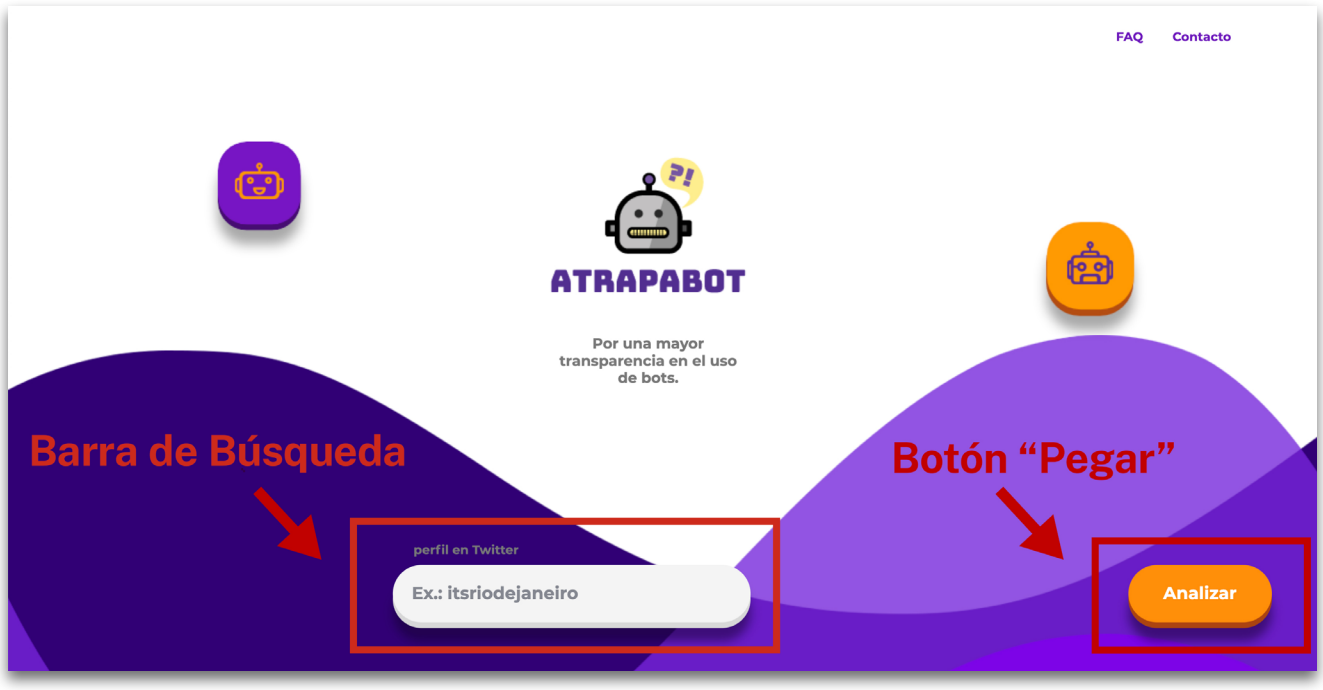
La herramienta está disponible a través del sitio es.pegabot.com.br y no es necesario instalar o descargar cualquier software adicional para utilizarla. Toda la navegación por la interfaz de la herramienta ha sido pensada para posibilitar, además, una experiencia tanto por el desktop cuanto por dispositivos mobile, o sea, por móvil.

4. CÓMO UTILIZAR

Para realizar el análisis, accede al sitio de la herramienta (es.pegabot.com.br). Observa en la pantalla inicial dos elementos importantes:

1. Barra de búsqueda: Barra donde puedes insertar el perfil (o arroba) del usuario que será analizado por la herramienta.

2. Botón “pegar”: Botón para iniciar el análisis del perfil.



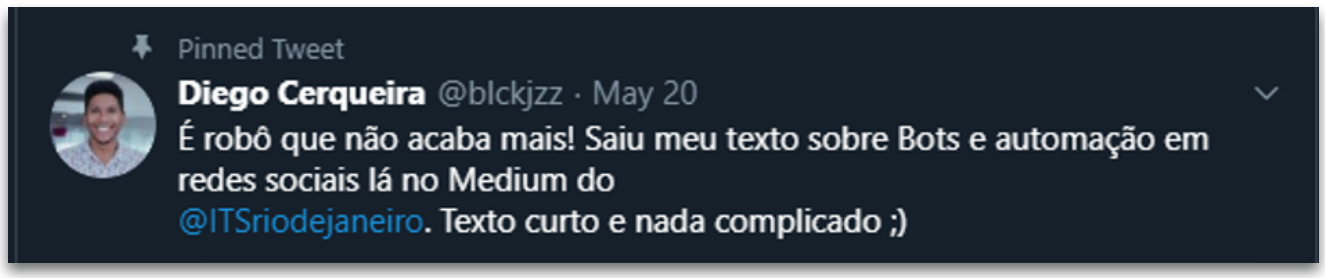
4.1. PARA OBTENER EL USUARIO

Para analizar un perfil en el Atrapabot, primero necesitas conocer el *handle* o arroba (@), que puede ser obtenido en el perfil del usuario, visto que esa información es pública.

Identificar el perfil del usuario es bastante fácil, basta con separar todo lo que viene después de la barra en la dirección de Twitter. Observa el ejemplo abajo.

ENLACE DEL PERFIL	NOMBRE DEL USUARIO
https://twitter.com/blckjzz	blckjzz

Otra manera fácil de conseguir el nombre del usuario, sin que sea necesario realizar visitas al perfil, es copiar el arroba que aparece debajo del nombre identificado. El perfil abajo se llama Diego Cerqueira, inmediatamente después podemos ver su arroba @blckjzz. Utiliza el atajo de teclado para copiar y sigue el paso siguiente del análisis.

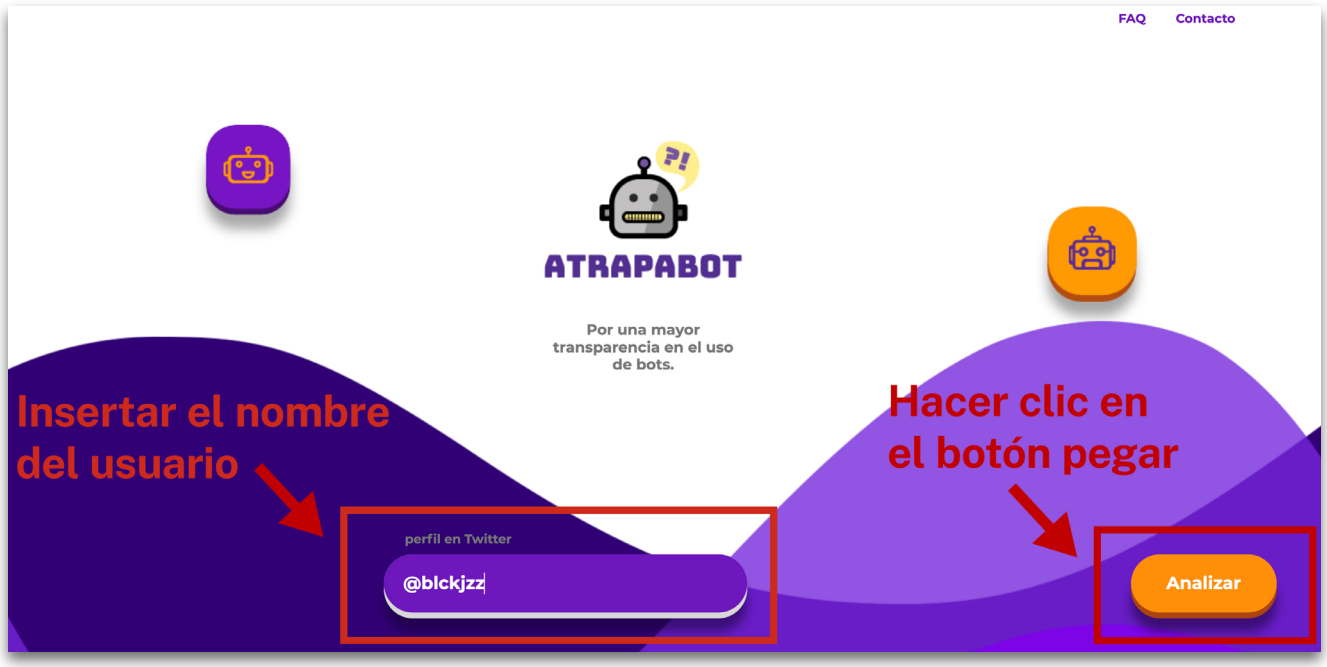


"¡Es tanto robot que no acaba nunca! Salió mi texto, sobre Bots y automatización en redes sociales, en el Medium del @ITSriodejaneiro. Texto corto y sin complicaciones ;)"

4.2. REALIZANDO UN ANÁLISIS

En posesión del nombre del usuario que será analizado, ya en la página inicial, haz clic dentro de la caja destacada en la imagen abajo y luego haz clic en el botón pegar. El perfil analizado puede contener la arroba literal o no.

La herramienta no funcionará o presentará errores en el caso de que insertes usuarios de otras redes sociales o incluso el enlace completo del perfil para el Twitter. Para el perfil que vamos a analizar, dos maneras podrían ser aceptadas: @blckjzz o blckjzz.



Análisis del perfil @blckjzz

Al hacer clic en el botón análisis, en la pantalla siguiente se presentará el resultado del análisis hecho por el Atrapabot, como puede observarse en la imagen abajo.

El perfil @blckjzz presenta una probabilidad de 28% de comportamiento de bot. En análisis este número presenta una baja probabilidad de que el perfil sea controlado por algún tipo de automatización.

ATENCIÓN! EL ANÁLISIS PUEDE FALLAR SI:

1. El perfil consultado no existe;
2. El perfil consultado fue suspenso;
3. El perfil consultado posee sus tuits privados;
4. La dirección para el perfil está incorrecta.

BOT SENTINEL

por Thayane Guimarães

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

EN ESTE TUTORIAL CONOCERÁS LA HERRAMIENTA BOT SENTINEL. ¡BUENA LECTURA!

1. LO QUÉ ES

2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES

3. CÓMO UTILIZAR

1. LO QUÉ ES

El Bot Sentinel es una plataforma apartidaria y gratuita desarrollada para clasificar y rastrear cuentas no auténticas y trolls tóxicos. La plataforma utiliza aprendizaje de máquina y inteligencia artificial para clasificar las cuentas de Twitter y, luego añade las cuentas a un banco de datos disponibles al público, donde cualquiera puede navegar. De la misma manera que el Pegabot y el Botometer, el Bot Sentinel indica la probabilidad de que un perfil en Twitter sea un bot o Troll, a partir de criterios preestablecidos.

La herramienta Bot Sentinel fue entrenada utilizando el modelo de aprendizaje de máquina a partir de miles de cuentas y millones de tuits que posibilitan la clasificación de las cuentas de Twitter. El sistema puede clasificar correctamente las cuentas con una precisión de 95%. Al contrario de otras herramientas de aprendizaje de máquina proyectadas para detectar “bots”, el Bot Sentinel enfoca su detección en comportamientos y actividades específicas consideradas inadecuadas por las reglas de Twitter. Se analizan centenas de de tuits para clasificar con precisión cada cuenta de Twitter y ofrecer un relatorio de fácil comprensión. Abajo explicaremos conceptos y categorías importantes para un análisis correcto de los resultados de la herramienta Bot Sentinel.

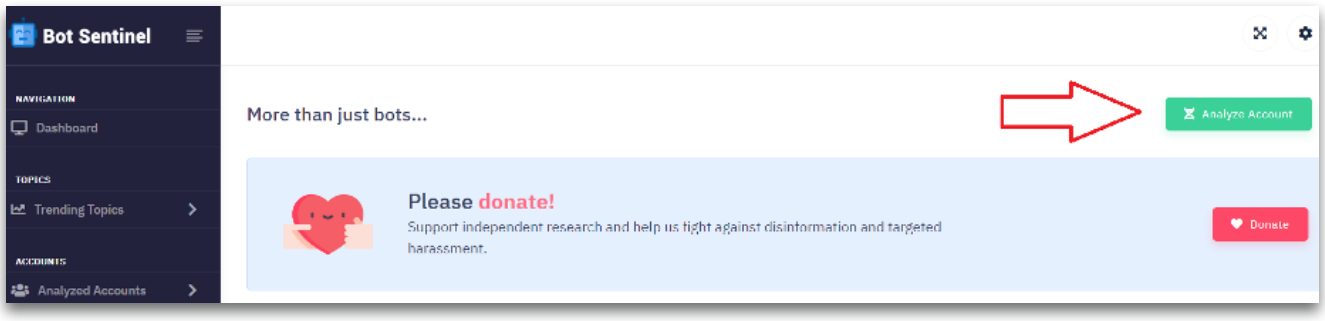
ALGUNAS DEFINICIONES IMPORTANTES PARA EL USO DEL BOT SENTINEL:

Cuentas no auténticas: son individuos con intenciones que fingen ser algo que no lo son con el propósito político de engañar a sus seguidores y público en general, o cuentas automatizadas (bots) desarrolladas para que se comporten de manera humana, también con la intención de manipular y distorsionar el debate público. Actores públicos malos utilizan cuentas no auténticas para sembrar discordia y causar caos en las plataformas de media social y esas cuentas son frecuentemente utilizadas para involucrarse en acoso direccionado y trolleo tóxico.

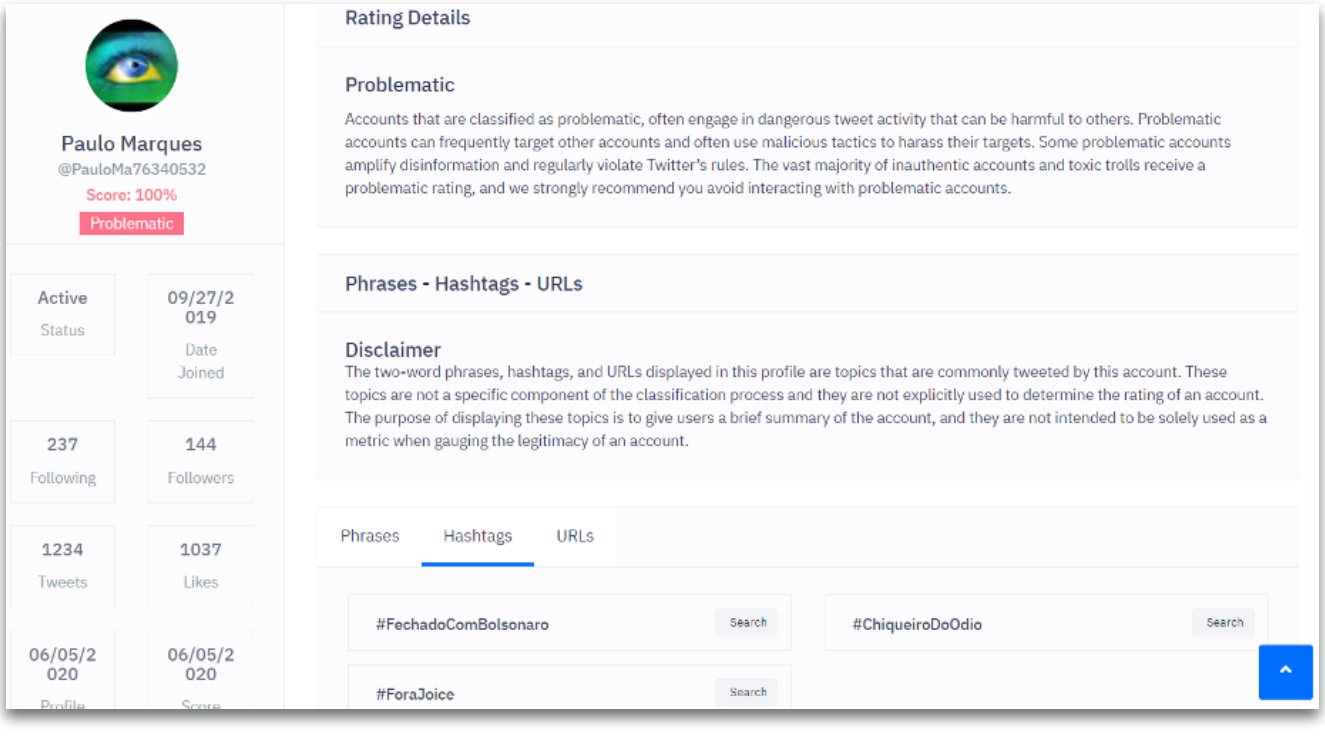
Las cuentas son clasificadas con base en un sistema de puntuación de 0% a 100%, cuanto mayor la puntuación, mayor la probabilidad de que la cuenta participe de actividades maliciosas. Incluso varias centenas de tuits son analizados por cuenta y, cuanto más uno se involucra en un comportamiento que viola las reglas de Twitter, mayor es su clasificación en el Bot Sentinel.

2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES

Análisis de perfiles de Twitter: Inicialmente, la herramienta Bot Sentinel solo tenía la capacidad de analizar individualmente un perfil y dar como resultado un “score” sobre la probabilidad de que la cuenta sea un bot o troll, con base en su comportamiento. Esa funcionalidad todavía es central en la herramienta, una vez que es a partir de ella que todas las otras se derivaron.



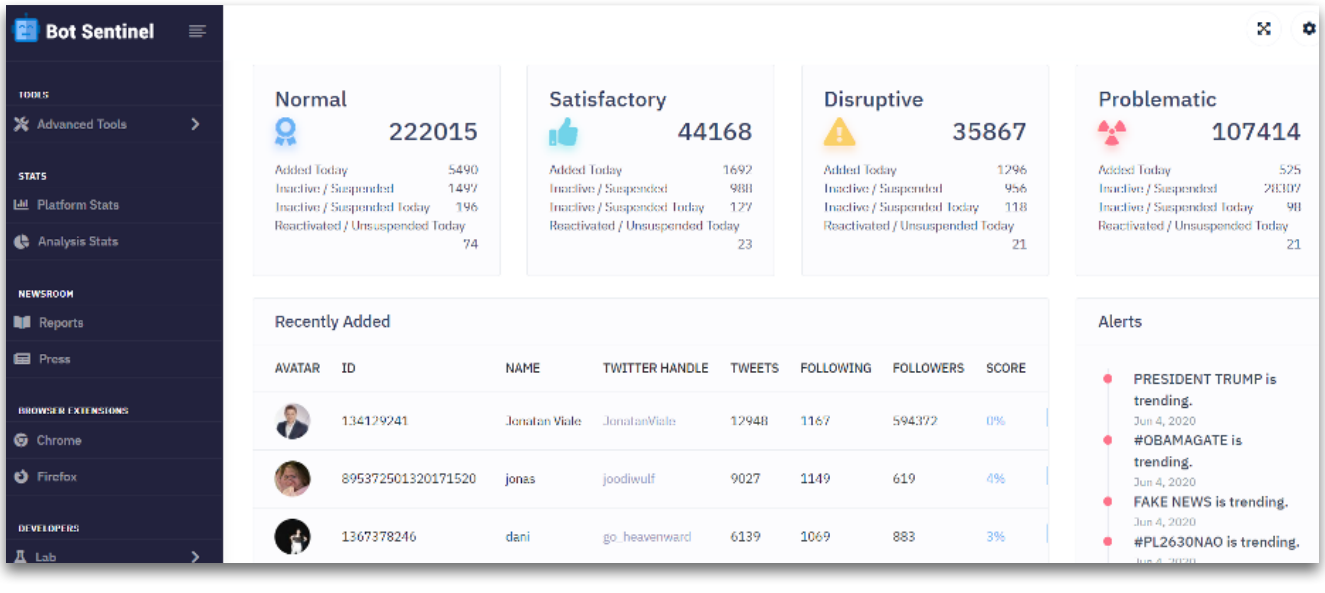
Pantalla inicial del Bot Sentinel con botón de “Analyze Account” para analizar perfiles de Twitter

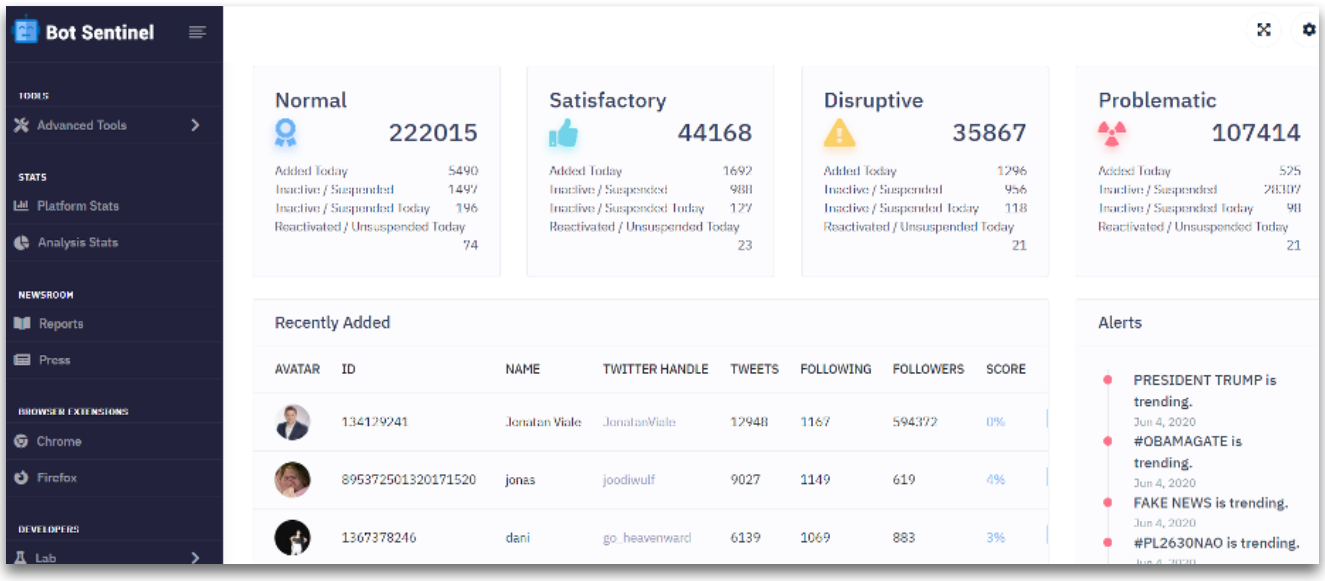


En el segundo momento, a partir de donaciones hechas por personas físicas de la sociedad civil que querían desarrollar el trabajo del Bot Sentinel, fue creada una interfaz frontend en beta con acceso permisionado, vía correo electrónico, de personas que donaron para la herramienta. Sus funcionalidades son:

A. DASHBOARD:

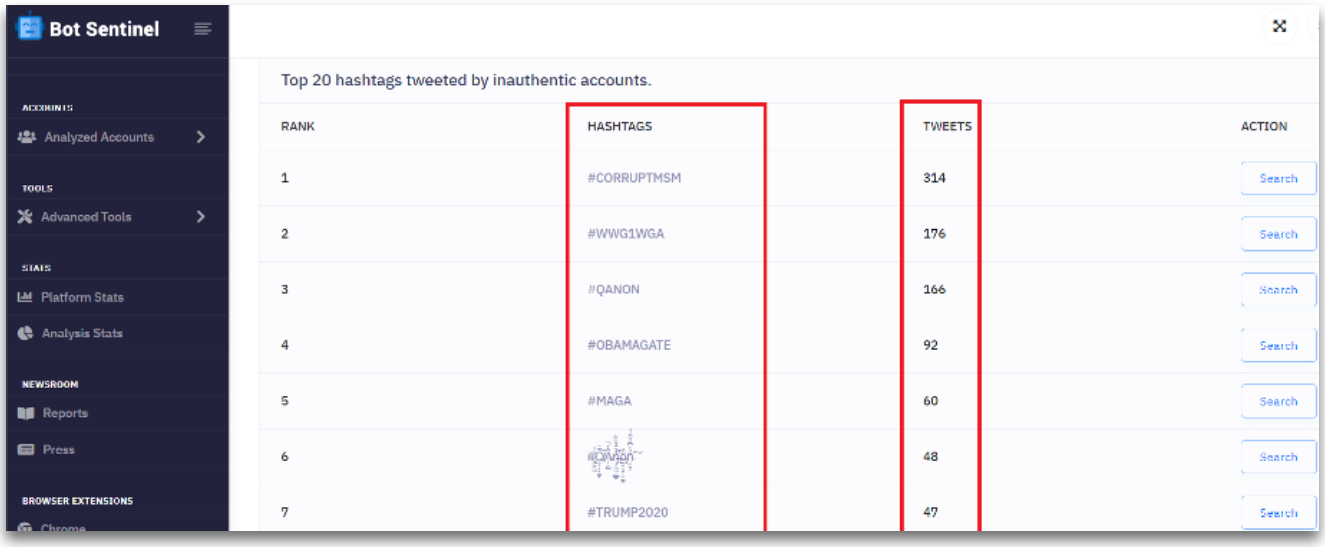
Panel con actualización automática de todos los perfiles que fueron analizados por la herramienta, segmentados por la categoría en que fueron asignados, con base en el “score” dado por la herramienta: normal, satisfactorio, disruptivo y problemático. Además, el dashboard inicial posee línea de tiempo con alertas de hashtags en el Trending Topics de Twitter que están sufriendo acción de impulso algoritmo





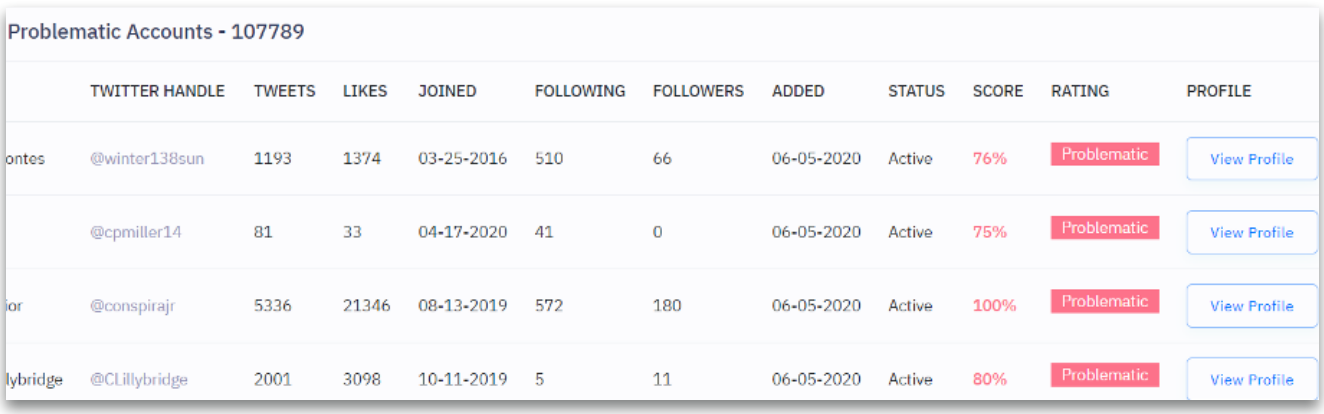
B. TRENDING TOPICS:

Monitoreo en tiempo real de trending topics que están siendo impulsados por acción algorítmica, son ellos: top hashtag, top two words phrases, top URLs y top mentions. Posibilita filtros para mes, día, año y hora, pero no para ubicación.



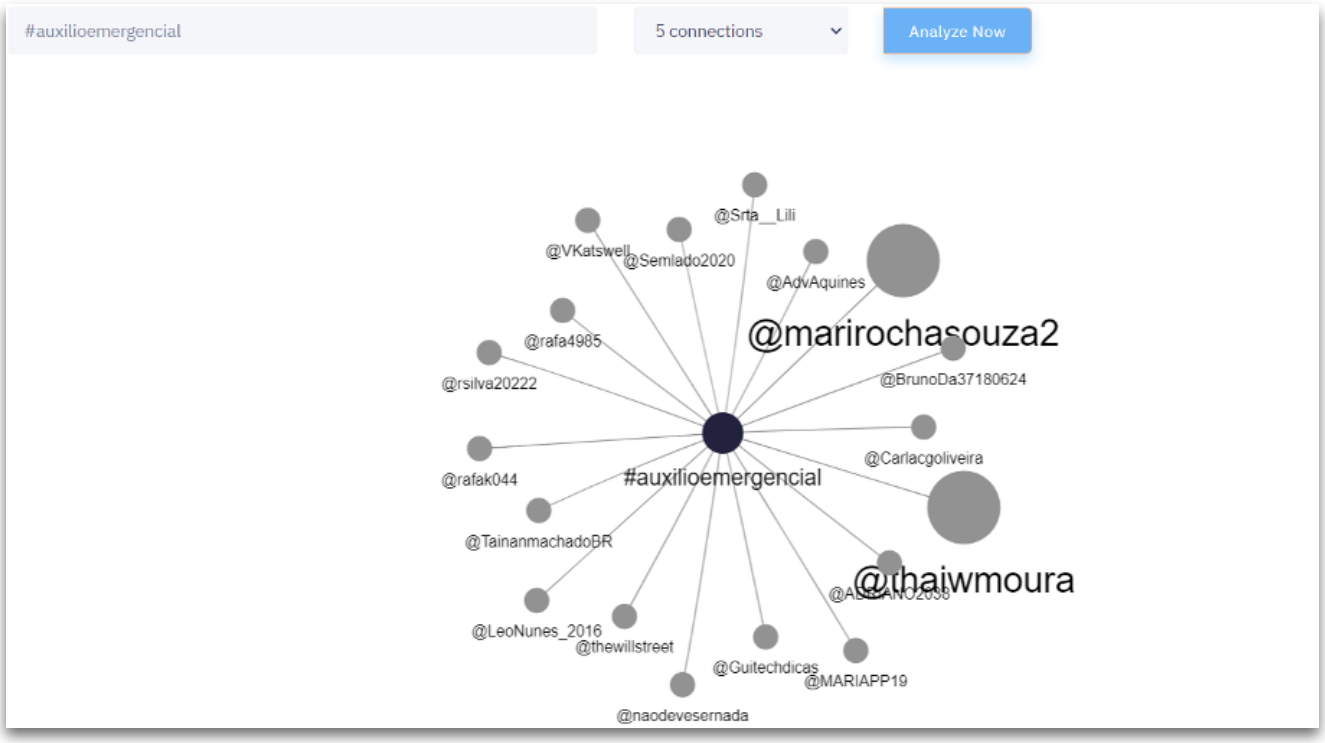
C. ANALYZED ACCOUNTS:

Banco de datos con almacenamiento automático de todas las cuentas que fueron analizadas por el detector y resultaron en 75% o más de probabilidad de ser un bot/trollbot. Inicialmente, almacena todas las cuentas, pero después de un tiempo exclui las que tienen un porcentaje inferior a 75%. Disponibiliza score cuentas y detalle de todos los perfiles, incluyendo número de seguidores, número de tuits de la cuenta, fecha en la que el perfil fue creado, hashtags, frases y URLs que más fueron tuiteadas por cada cuenta analizada y status (activa o inactiva). Además, en este menú es posible tener acceso al monitoreo constante de las cuentas que son desactivadas por Twitter.



D. ADVANCED TOOLS:

Análisis en lotes a partir del enlace de un tuit que verifica automáticamente todos los perfiles que interactuaron con una determinada publicación. En esta pestaña, también es posible crear un grafo de distribución de red con perfiles que tuitearon una hashtag o marcaron un handle, no obstante, sin filtro/critério de alcance o relevancia de cuentas.



3. CÓMO UTILIZAR

PASO 1:

Accede al sitio http://botsentinel.com/

PASO 2:

Haz clic en el botón “Analyze Account” en el rincón superior derecho e inserta un handle (perfil) de una cuenta de Twitter para recibir como resultado el porcentaje de probabilidad de que esta cuenta sea un bot o troll.

PASO 3:

Recurre el menú lateral para tener acceso a las demás funcionalidades de la herramienta.

PARA SABER CÓMO SACARLE MÁXIMO PROVECHO DE CADA UNA DE LAS FUNCIONALIDADES DEL BOT SENTINEL, VE AL WORKSHOP II (ENLACE), SOBRE HERRAMIENTAS PARA DETECCIÓN DE AUTOMATIZACIÓN Y DESINFORMACIÓN.

BOTSLAYER

por Thayane Guimarães

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

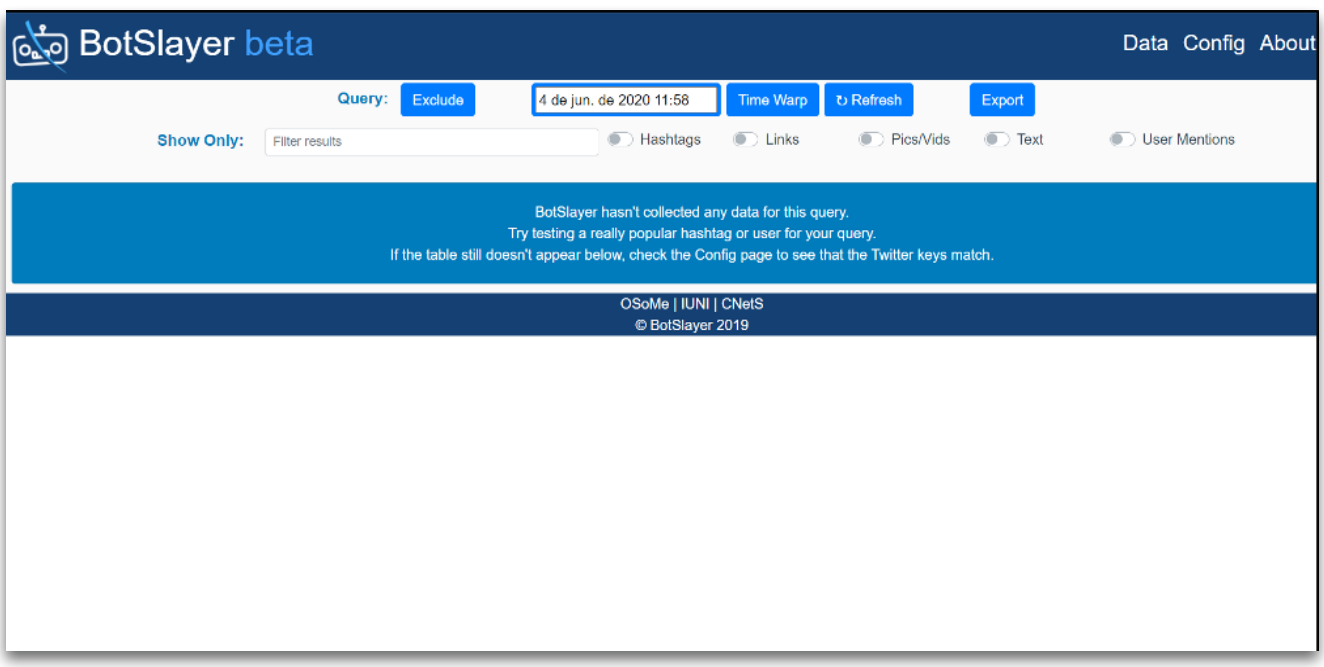
EN ESTE TUTORIAL CONOCERÁS LA HERRAMIENTA BOTSLAYER. ¡APROVÉCHALO!

1. LO QUÉ ES

BotSlayer es una herramienta gratuita y desarrollada por el Observatorio de Medias Sociales de la Universidad de Indiana (EUA) para pesquisar acciones de ataques coordinados en Twitter a partir del rastreamiento y detección de posibles manipulaciones de informaciones. El programa utiliza un algoritmo de detección de anomalías y crea un índice para señalar hashtags, enlaces, cuentas y medias con alta probabilidad de que hayan sido impulsadas en la red social de forma coordinada, con ayuda de bots.

El BotSlayer posee integraciones con el Botometer y el Hoaxy, otras herramientas desarrolladas previamente por el mismo Observatorio de Indiana. El primero chequea la actividad en una cuenta en Twitter y atribuye una nota basada en la probabilidad de que el usuario sea un robot, mientras el Hoaxy permite visualizar como los flujos de información se propagan en redes de usuarios.

El programa puede ser instalado tanto localmente, en la máquina de cada usuario, cuanto en una nube. Pero, como su objetivo mayor es realizar análisis en tiempo real, y 8 ocho horas es el tiempo mínimo de funcionamiento para el mejor aprovechamiento de sus métricas, se recomienda la instalación de un software en un servidor. Un panel accesible por el navegador permite que los usuarios exploren los tuits y cuentas asociados a campañas sospechosas, visualicen su propagación con el Hoaxy y busquen contenidos relacionados en la web.



2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES

La pesquisa empieza a partir de la definición de términos de búsquedas iniciales, que serán colectadas de forma contínua a partir del momento de la configuración inicial. Sin embargo, el sistema no almacena mensajes de manera retrospectiva y la API de Twitter no regresa más que 1% del volumen total de mensajes en la plataforma en un determinado período.

Esto exige cuidado en el momento de elegir los términos de búsqueda: caso sean suficientemente específicos, probablemente conseguirás colectar todos los los mensajes relativos al tema. En el caso de que sean muy genéricos, es posible que ni todos sean colectados a causa de la limitación de la API de Twitter.

Tras los mensajes colectados, el BotSlayer identifica las entidades involucradas en cada una de ellas. Las entidades pueden ser hashtags, enlaces, imágenes o videos, usuarios de Twitter y frases textuales. El funcionamiento de la última versión en portugués no está perfecto, pues el sistema elimina automáticamente palabras y expresiones comunes (“stopwords”) solo en inglés, de modo que muchas frases textuales identificadas por el BotSlayer son palabras comunes de nuestro vocabulario.

Después de extraer las entidades, el BotSlayer las exhibe en un panel con las métricas abajo para cada una de ellas;

A. TWEETS:

El número de tuits y retuits que corresponden a la consulta inicial y contienen esa entidad en las últimas cuatro horas;

B. ACCOUNTS:

El número de cuentas distintas que subieron mensajes que corresponden a la consulta en las últimas cuatro horas;

C. TRENDINESS:

Alteración relativa en el número de tuits que corresponden a la consulta y contienen esa entidad en las últimas cuatro horas, en comparación con las cuatro horas anteriores;

D. BOTNESS:

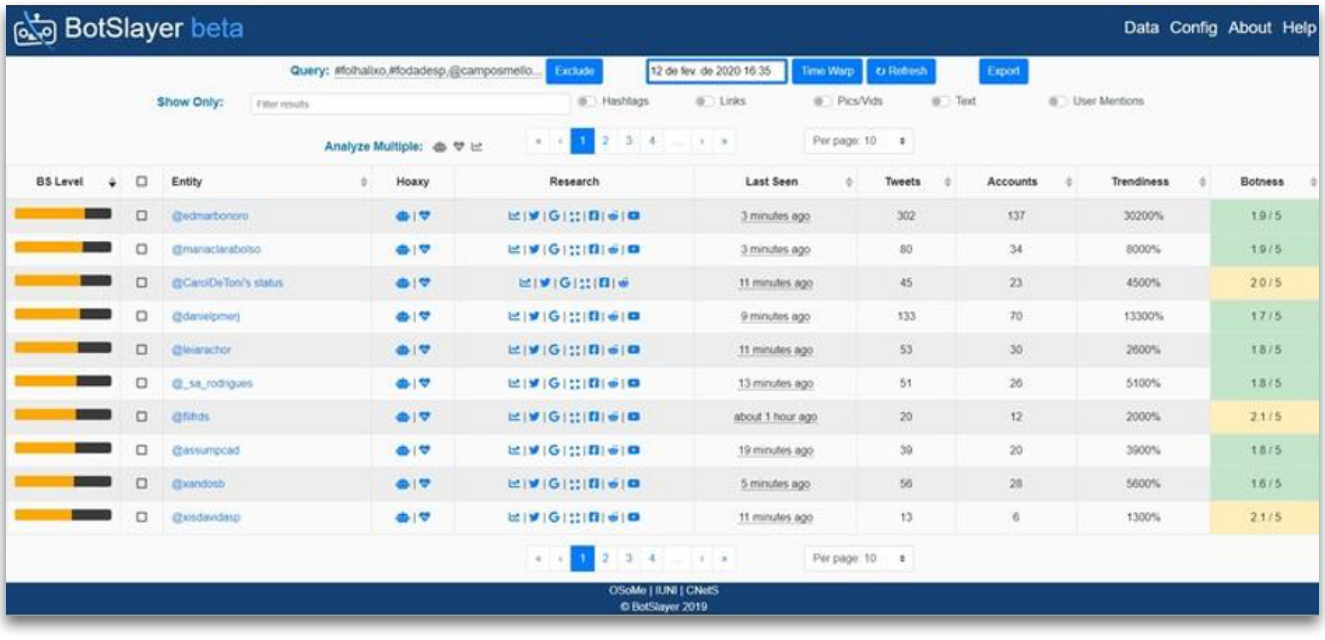
media del índice que mide la probabilidad de que un determinado usuario sea un bot entre los tuits que contienen esa entidad en las últimas cuatro horas;

E. BS LEVEL:

Este índice, mencionado en el comienzo del texto, considera los números anteriores para llegar a una nota entre 0 e 1. Cuanto mayor el índice, mayor es la probabilidad de que esa “entidad” tenga la participación de robots en su programación en línea. Su determinación ocurre de forma relativa, considerando cada conjunto de datos en lugar de una escala absoluta. Por lo tanto, la comparación del “BS Level” entre datasets diferentes no es recomendable. Según sus desarrolladores, la definición de un BS level alto debe ser hecha caso a caso.

ATENCIÓN: Es importante resaltar que el hecho de que el BotSlayer no colecta mensajes de manera retrospectiva. O sea, es necesario dejar el programa ejecutando por lo menos 8 horas sin interrupciones para llevar en cuenta el índice de Trendiness, por ejemplo.

Todos estos datos pueden ser exportados para el formato CSV directamente del panel web del programa.



3. PASOS PARA LA INSTALACIÓN:

Primeiro, para usar el BotSlayer es necesario rellenar este formulario. También debes estar conectado a una cuenta Google para verificar tu identidad y estar de acuerdo con el EULA (End User License Agreement). Recibirás los detalles necesarios para seguir las instrucciones de instalación abajo en el texto. Apunta la “Secret string”, el “URL” y la “Password” que serán generados tras rellenar el formulario: los necesitarás para hacer la descarga. Observa las diferentes instrucciones de instalación:

3.1. PARA USUARIOS DOCKER:

El BotSlayer puede ser instalado en cualquier ordenador por medio de una imagen preconstruida en el Docker. Para instalarlo en tu maquina, sigue las instrucciones en el sitio web del Docker.

Después de solicitar el software y concordar con los términos de uso, deberás recibir un URL vinculado a una imagen del Docker y una contraseña. Descarga el archivo de imagen. Necesitarás insertar un nombre de usuario (botslayer) y la contraseña suministrada.

También puedes utilizar el siguiente comando para descargar la imagen del Docker directo del terminal (sustituye *url2image* por el URL que recibiste):

wget --user = botslayer --ask-password url2image

A continuación, ejecuta en el terminal los siguientes comandos para cargar la imagen descargada y ejecuta el contenedor del Docker. Sustituye el nombre del archivo por el nombre del archivo descargado.

gunzip filename.gz

docker load < filename

docker volume create pgdata

docker volume create rpdata

docker run -dit -p 5000:5000 -p 9001:9001 -v rpdata:/root/bev -v pgdata:/var/lib/postgresql/data bev

El último comando mapea puertas que ofrecen funcionalidades diferentes. Las interfaces están disponibles en el “localhost” o en la dirección de IP de tu servidor. El panel del BotSlayer está en la puerta 5000. La interfaz con los log se expone en la puerta 9001, transmitiendo archivos desde dentro del contenedor sobre el funcionamiento del sistema.

Para un acceso más fácil al panel en la puerta HTTP patrón (80), puedes configurar un proxy reverso de la puerta 500 a la puerta 80 o (2) utilizar el sudo para forzar la puerta 5000 del mapa hasta la puerta 80 al ejecutar el docker recipiente.

Si el ordenador reinicia por cualquier razón, necesitarás reiniciar el contenedor BotSlayer en el Docker. Una solución alternativa es configurar algún gerenciador de procesos, como el *supervisord*.

Si quieres ver un ejemplo de código de configuración en un ambiente EC2 que incluye la instalación del Docker, la instalación del proxy reverso en el nginx y la configuración de la supervisión, consulta en esta página (en inglés) para obtener las etapas de instalación.

3.2. CON EL USO DE AMAZON WEB SERVICES

El BotSlayer utiliza el Amazon Web Services (AWS) por medio de una Amazon Machine Image (AMI) para optimizar el proceso de instalación para usuarios no técnicos.

ETAPA 1:

Accede a la AWS. Si no posees una cuenta, necesitarás crear una.

Haz el login en la consola. En el AWS Management Console (Consola de gerenciamento de la AWS), haz clic en “Servicios AWS”, después vas a ver el menú “Computación” y harás clic en “EC2”.

ETAPA 2:

Haz clic en el botón para iniciar una instancia de EC2. Haz clic en “Launch instance”.

ETAPA 3:

Tras solicitar el software y concordar con el EULA, deberás recibir instrucciones que incluyen una larga cadena secreta como “0e...f2”. Es el ítem “Secret String” que recibiste después de rellenar el formulario del BotSlayer.

Copia eso en la caja de búsqueda en la parte superior (aparece como ‘Search for AMI by entering a search term”). Haz clic en la pestaña “Community AMIs”.

Selecciona el resultado en AMIs de la comunidad. Si la búsqueda no obtiene ningún resultado, define tu región de servicio de la AWS como Ohio en el rincón superior derecho de la página y haz una nueva búsqueda.

ETAPA 4:

Selecciona la imagen correcta. Debe ser la imagen de un pingüino (el símbolo de Linux). Pulsa la tecla Select.

ETAPA 5:

En la nueva pantalla (Choose an Instance Type) puedes seleccionar el tipo de instancia marcado como “nivel gratuito calificado” (Free tier eligible).

Como alternativa, puedes seleccionar el “t2.xlarge”, recomendado por el Observatorio de Medias Sociales, pero no de manera gratuita; puede costar cerca de US$ 0,20/hora. Haz clic en “Configurar detalles de la instancia” (Next:Configure Instance Details) en el rincón inferior derecho para seguir. La Abraji utilizó la versión gratuita.

ETAPA 6:

Utiliza las configuraciones patrón en la página “Configurar detalles de la instancia (Configure Instance Details) y haz clic directo en “Añadir almacenamiento” (Next Add Storage) en la parte inferior derecha para seguir.

ETAPA 7:

Elige el tamaño de tu disco rígido. Puedes seleccionar hasta 30GB para el nivel gratuito. El Observatorio de Medias Sociales recomienda 100 GB o más para mantener los datos, además de varios días, dependiendo de la cantidad de informaciones que rastrees.

ETAPA 8:

Utiliza las configuraciones patrón en la página “Añadir tags” y haz clic directo en “Configurar grupo de seguridad” (Next: Configure Security Group) para seguir.

ETAPA 9:

Añade dos reglas para abrir las puertas exigidas por el BotSlayer.

Haz clic en Add Rule – elige “HTTP” en Type – “TCP” en Protocol – “80” en Port Range – “Custom” y “0.0.0.0/0, ::/0” en Source

Haz clic una vez más en Add Rule – elige “Custom TCP Rule” en Type – “TCP” en Protocol – “9001” en Port Range – “Custom” y “0.0.0.0/0, ::/0” en Source

Haz clic en “Revisar e iniciar” (Review and Launch) en el rincón inferior derecho para seguir.

ETAPA 10:

Revisa cuidadosamente la configuración de la máquina. Si encuentras algún error, podrás volver a corregirlo. Caso contrario, haz clic en “Iniciar” (Launch) en el rincón inferior derecho para seguir.

ETAPA 11:

Crea un nuevo par de claves (Create a new key pair) y atribuye un nombre significativo, como “busca_bot_brasil” u otro de tu preferencia. Este par de claves es necesario para accesar la máquina EC2. Descarga el par de claves (Download Key Pair) y mantenlo en un ambiente seguro. Luego inicia la instancia (Launch Instances).

ETAPA 12:

Terminaste de configurar el BotSlayer, ahora haz clic en el enlace de la instancia para ir a la pantalla principal.

ETAPA 13:

Haz clic en el enlace después de la frase: “The following instance launches have been initiated”.

Copia el nombre del dominio o dirección IP y pégalo en tu navegador para accesar la interfaz web de BotSlayer. En Instance State debe aparecer “running”.

Puedes encontrar la dirección en “IPv4 Public IP”. Algo como “18.XXX.XXX.XX”, pero en el lugar de los Xs existirán números. Espera 5 minutos para que la máquina tenga tiempo suficiente para iniciar el BotSlayer.

Marca la dirección IP como favorito, pues, de esa manera accederás al panel del BotSlayer. Observación: si reinicias la instancia de EC2, la dirección será alterada. Para atribuir una dirección IP estática puedes utilizar una Dirección IP Elástica (no gratuita).

CONFIGURANDO EL BOTSLAYER

Después de instalar el BotSlayer y acceder al panel Web, haz clic en “Config” en el menú, digita la contraseña de tu elección y suministra las claves de la aplicación de desarrollador de Twitter y una consulta permanente (ve abajo más detalles en “Tu primer raspador”). Consulta la página de Ayuda (Help) para obtener más instrucciones, dicas sobre las claves de Twitter y el formato de la consulta.

ATENCIÓN: El panel es accesible vía Web utilizando la dirección IP del servidor. Caso estés utilizando un servidor en la nube, no compartas un URL con alguien de fuera de tu organización o personas en las que no confies. Ellos pueden hacer alteraciones en el sistema o accesar datos de violación de los términos de servicio de Twitter. Para evitar posibles problemas de seguridad y violación de términos, el BotSlayer bloquea la indexación del mecanismo de búsqueda por patrón.

Pon en el browser la dirección del BotSlayer que tomaste en tu “IPv4 Public IP”. Haz clic en Config. Este es el momento en que eliges una contraseña para tu BotSlayer y después haz clic en Change Password. Luego es necesario hacer login con la contraseña que apenas elegiste.

INSERTANDO CLAVES DE LA API DE TWITTER

Ahora llega el momento en que necesitas poner tus identificaciones de desarrollador en el Twitter para seguir. Para conseguir estas claves, debes ir hasta el sitio web de la red social y hacer login con tu usuario y contraseña en Twitter.

Haz clic en el botón “Apps” y en la próxima pantalla “Create an App”. Si es la primera vez, quizás tengas que rellenar un cuestionario largo sobre los motivos de la app y tus datos básicos.

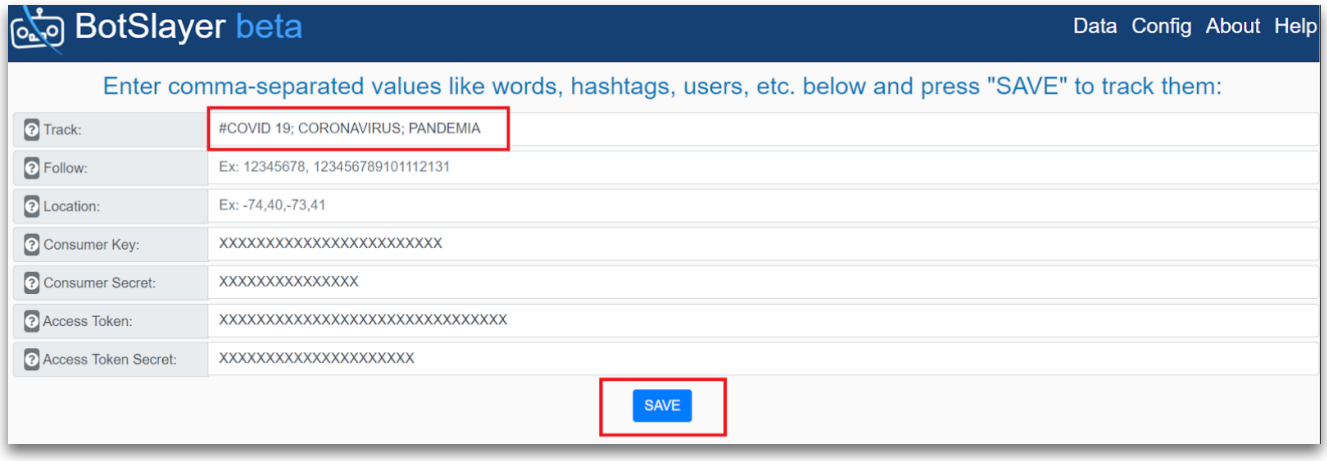
Enseguida necesitas poner en “App details” el “App name”, después la descripción en “Application description”, el “websiteURL” y “Callback URLs” de tu proyecto (por ejemplo, en nuestro caso, http://www.abraji.org.br) y escribir “Díganos cómo esta aplicación será utilizada” (Tell us how this app will be used). Twitter puede llevar algún tiempo para aprobar la App después de hacerlo.

Una vez creado, vete a la pestaña Key and tokens. Haz clic en los dos botones Regenerate. En la pantalla que abre, haz clic en Copy para Access token, pulsa Ctrl+C en el bloc de notas, después Copy para Access token secret y pulsa Ctrl+C en el bloc de notas. Copia también los valores de API Key. Guarda estas claves.

Da la vuelta a la pantalla de BotSlayer, copia en Consumer Key el contenido de API Key, después en Consumer Secret copia pI secret Key, después en Access Token copia el valor de Access token y, por fin, en Access Token Secret el valor de Access token secret. Haz clic en “Save”.

4. CÓMO UTILIZAR:

Ahora, en el campo “Track” puedes elegir lo que deseas buscar: palabras, nombres, hashtags, usuarios de Twitter y hasta ubicaciones.



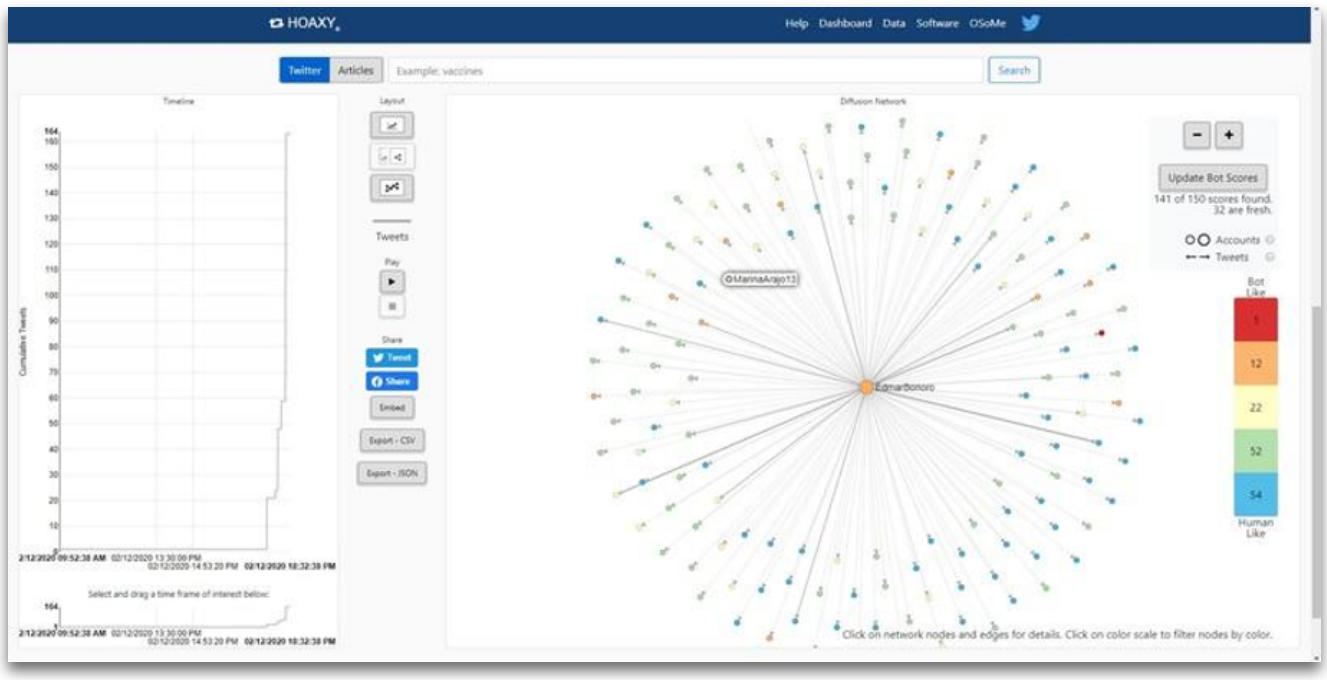
Haz clic en Save de nuevo para salvar los parámetros de búsqueda. También es posible elegir los ítems en Follow (delimitar usuarios específicos para seguir) y Location (locales de los tuits). Luego haz clic en Data y espera un rato.

El BotSlayer empezará a recolectar los mensajes de este momento. Después de algún tiempo, aprieta Refresh para ver los resultados y las métricas de la herramienta.

Además de chequear las métricas mencionadas arriba, también es posible alterar las fechas de búsqueda en “Time Warp” y filtrar la tabla solo por términos específicos. También pueden ser creadas visualizaciones de datos con otro proyecto del Observatorio de Medias Sociales, el Hoaxy. Por fin, en la pestaña “Research” es posible ver la timeline de los datos y los resultados de las búsquedas encontrados en Twitter, Google, 4chan, Facebook, Reddit y YouTube.

En el momento, no es posible obtener más informaciones sobre la cantidad total de mensajes colectadas o tener acceso a los contenidos descargados a través de la interfaz gráfica. Para ello, es necesario accesar el banco de datos que provee los datos para el BotSlayer. En un ambiente Docker es posible hacerlo a través del comando abajo:

sudo docker exec -it <id_docker> psql -U bev -h localhost -p 5432



PARA MÁS INFORMACIONES SOBRE LA ARQUITECTURA DE SOFTWARE DEL BOTSLAYER, CONSULTA ESTA PÁGINA EN GITHUB.

TWITONOMY

por Thayane Guimarães

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

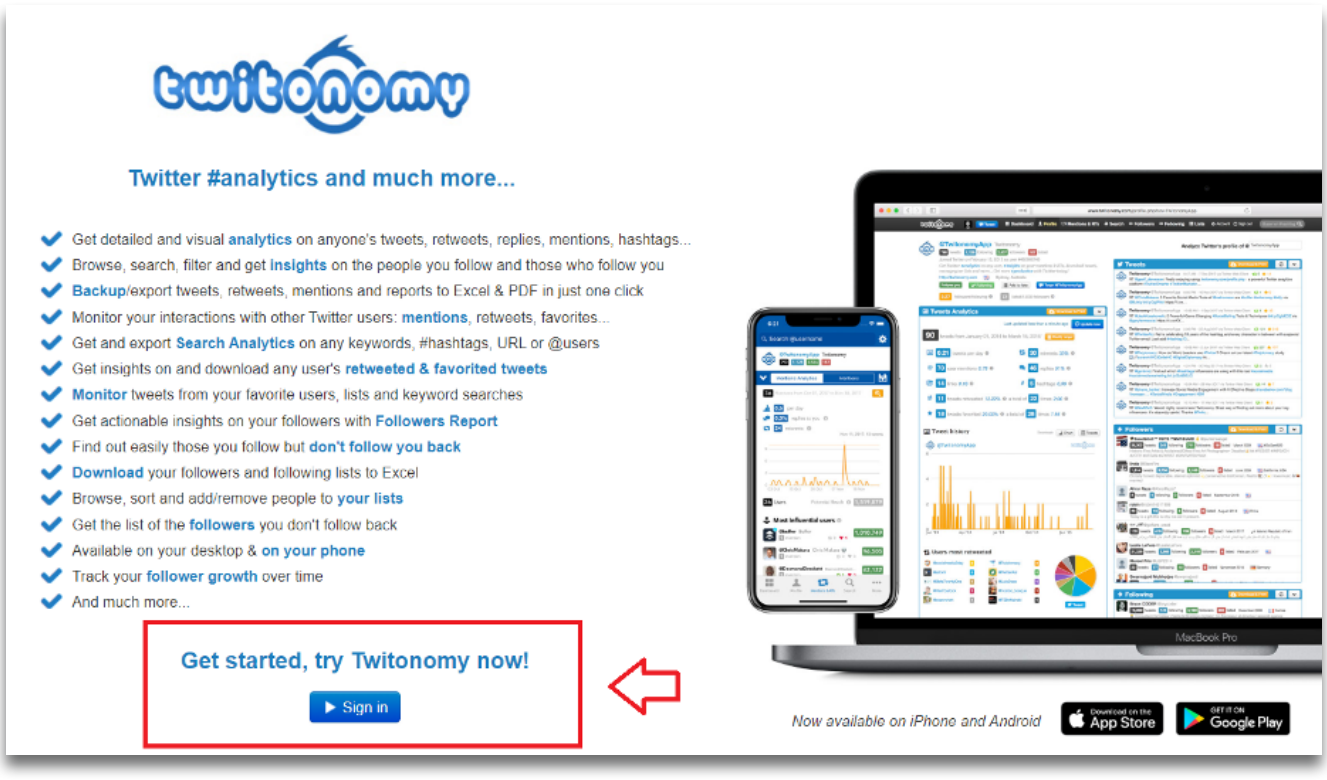
EN ESTE TUTORIAL CONOCERÁS LA HERRAMIENTA TWITONOMY. ¡BUENA LECTURA!

1. LO QUÉ ES
2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES
3. CÓMO UTILIZAR

1. LO QUÉ ES

Twitonomy es una poderosa herramienta que sirve para analizar datos de Twitter, producida por @MattFyot. El servicio es totalmente gratuito y permite realizar el monitoreo minucioso de las actividades que ocurren en Twitter, contribuyendo, de esa manera, para cualquier pesquisa política en la plataforma.

Permite, por ejemplo, monitorear en tiempo real hashtags, usuarios y crear listas con conjuntos de usuarios para la actualización constante de sus actividades, incluyendo aquellas realizadas en fechas retroactivas. En la versión premium, permite monitoreo basado en los perfiles más influyentes, perfiles más comprometidos y perfiles más activos, además de buscar por top hashtags más relacionadas al tema monitoreado. La versión premium posibilita hacer el descargue en csv o pdf de todas las infos. Observa abajo en detalles.

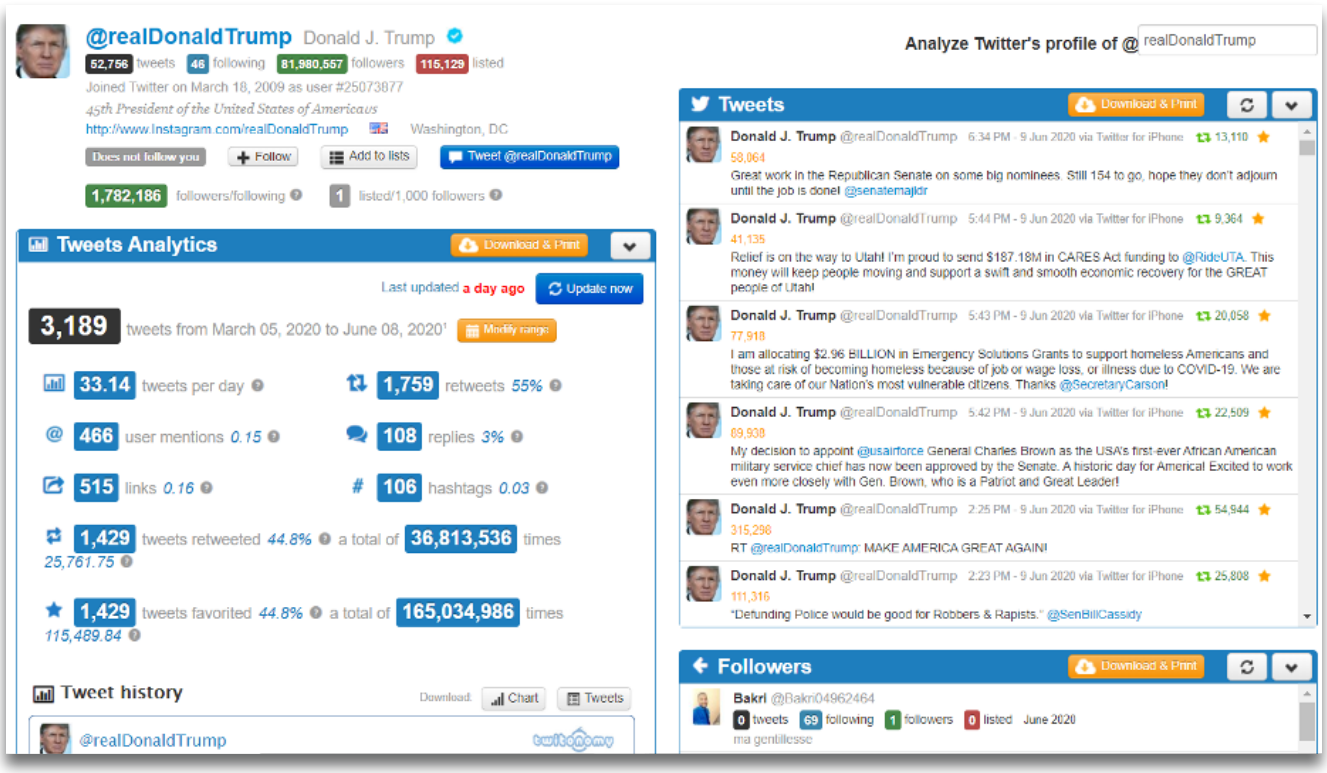


2. CUÁLES SON LAS FUNCIONALIDADES EXISTENTES

La herramienta Twitonomy está enfocada en la metrificación de un perfil en Twitter con funcionalidades que van desde la identificación de seguidores con mayor capacidad de influenciar otras personas, hasta las métricas minuciosas sobre quiénes son los perfiles más comprometidos con su contenido y cuáles han sido los tuits de su cuenta que tuvieron más repercusión en la red. Sin embargo, la plataforma todavía posee diversas capacidades que auxilian el monitoreo de las actividades del Twitter y, de esta manera, contribuyen con el análisis de los datos y la construcción de las estrategias de enfrentamiento a la desinformación. Observa bajo alguna de ellas:

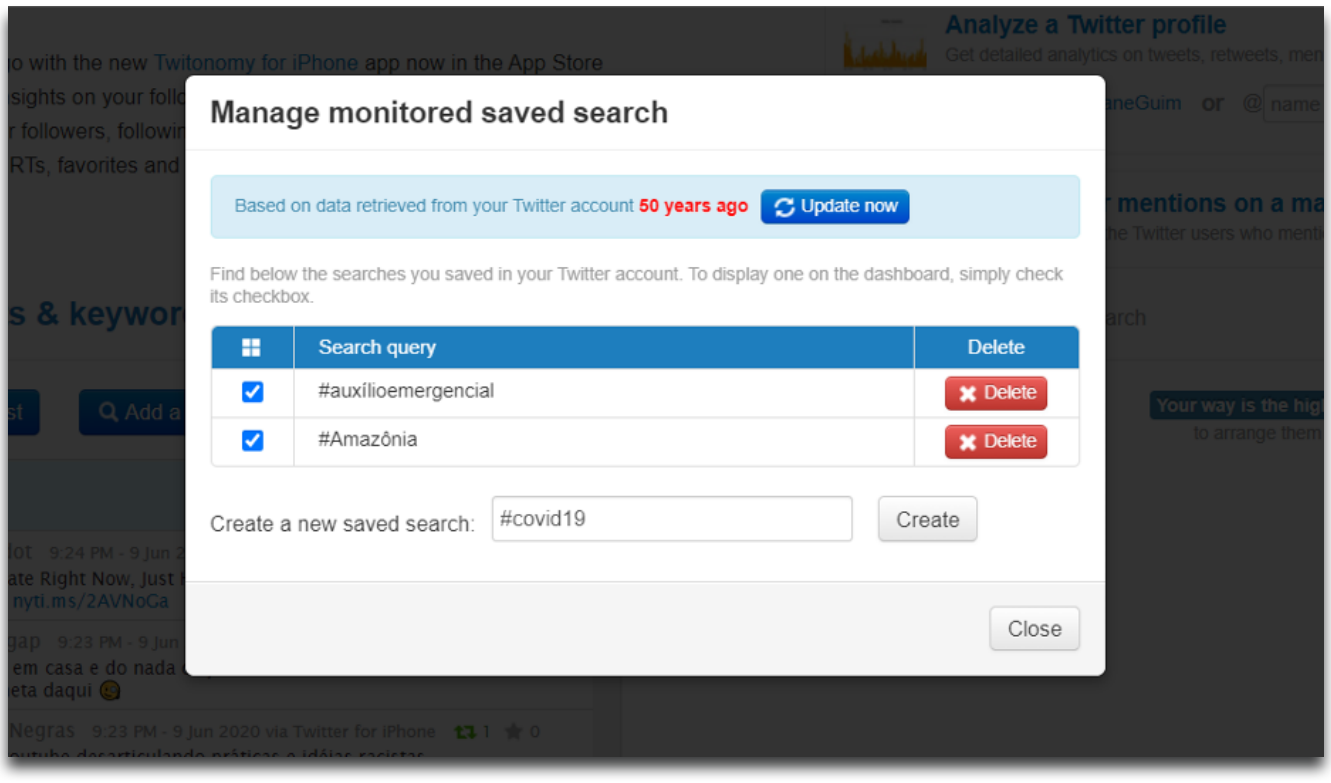
A. ANALYZE TWITTER'S PROFILE:

Posibilita el monitoreo de una cuenta específica de Twitter, incluyendo publicaciones que tuvieron mayor alcance y relevancia, lista de seguidores, perfiles que sigue, hashtags más utilizadas e informaciones como qué días de la semana y horas del día ocurren las actividades del perfil analizado.



B. MONITOR USERS, LISTS AND KEYWORDS:

Permite elegir usuarios, listas o cualquier palabra clave (termos, hashtags, etc) para monitorear. El twitonomy, por lo tanto, actualiza automáticamente los cuadros de monitoreo conforme tus intereses y aún permite hacer el descargue de todos los datos en archivo .csv.



C. LISTS

Permite, por ejemplo, crear una lista con todos los usuarios que tuitearon una determinada hashtag y exportar en archivo .csv, sin que sea necesario acceder a la API de Twitter y utilizar códigos para raspado de datos para realizar la tarea.

D. SEARCH:

Posibilita datos diversos sobre actividades en Twitter relacionados a un termo de búsqueda específico, incluyendo qué cuentas están hablando sobre el tema, qué perfiles son más influyentes, qué tuits tuvieron mayor repercusión, en qué días y horarios el termo estaba en alta, cuáles son las principales hashtags relacionadas a su termo y en qué países el termo tuvo mayor repercusión. Esa funcionalidad, sin embargo, solo está disponible en la versión premium de la herramienta.

E. MENCIONES Y ALCANCE POTENCIAL:

Posibilita no solo identificar la cantidad de menciones en tu perfil, sino también la frecuencia de menciones diarias, número total de usuarios que mencionaron la página que se analiza, retuits de las menciones y alcance potencial de los tuits, con base en el número de seguidores de cada usuario.

3. CÓMO UTILIZAR:

El Twitonomy no necesita instalación, por lo tanto, para empezar a utilizar la herramienta, basta con seguir los pasos adelante:

PASO 1:

Haz el login en una cuenta de Twitter, sea tu cuenta personal o de tu organización.

PASO 2:

Accede al sitio www.twitonomy.com

PASO 3:

Haz clic en el botón “Sign In”.

TINEYE

por Redson Fernando

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

EN ESTE TUTORIAL, CONOCERÁS LA HERRAMIENTA TINEYE. ¡APROVÉCHALO!

1. LO QUÉ ES

El TinEye es un mecanismo de búsqueda reversa de imágenes desarrollado por la empresa Idée, Inc., domiciliada en Toronto, Canadá. La búsqueda reversa es especialmente interesante para los que ya poseen una imagen en manos y quieren encontrar otras imágenes relacionadas, o también a los que pretenden descubrir el origen de una imagen para obtener más informaciones sobre ella, por ejemplo. El TinEye crea una impresión digital única y compacta de la imagen buscada utilizando el aprendizaje de máquina e inteligencia artificial y la compara con todas las otras imágenes indexadas en la plataforma para encontrar correspondencias.

2. CÚALES SON LAS FUNCIONALIDADES

A. MECANISMO DE BÚSQUEDA:

El TinEye realiza la búsqueda de copias exactas y alteradas de las imágenes buscadas en la plataforma, incluyendo las que fueron cortadas, las con colores modificadas, redimensionadas o rotativas, por ejemplo. De esa manera, la herramienta posee diversas aplicaciones, como descubrir si la imagen está siendo utilizada por terceros, si existen versiones modificadas y donde están. Además, descubre el origen de las imágenes para obtener más informaciones o para encontrar versiones de alta resolución. Es importante resaltar que el TinEye normalmente no reconoce el contenido de las imágenes. O sea, no se puede utilizarlo para encontrar imágenes diferentes con las mismas personas u objetos, por ejemplo. Además, es importante destacar que tu búsqueda en el TinEye nunca se salva o indexa sin que lo permitas. Ese proceso es realizado a partir de la propia API de la plataforma, que busca y agrega automáticamente las imágenes en el motor de búsqueda.

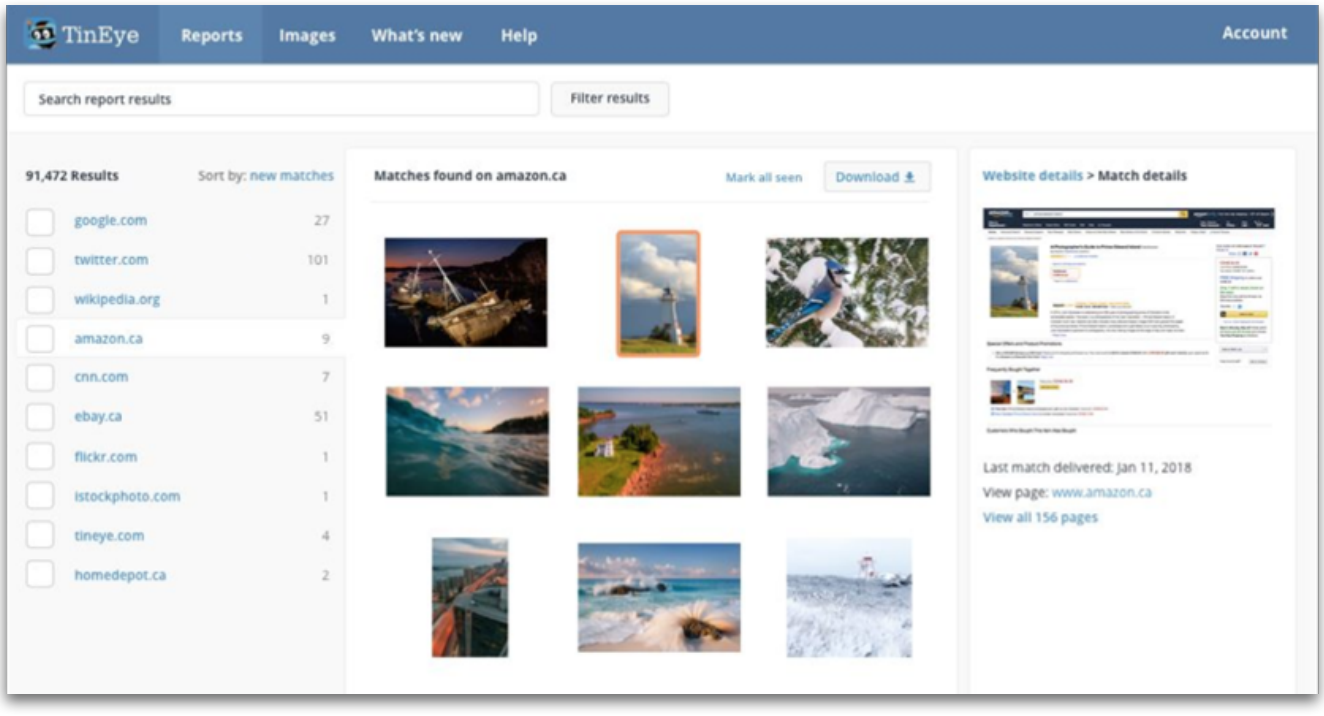
El TinEye es gratuito para el uso por medio de su interfaz de la Web y permite que el usuario realice hasta 100 búsquedas al día, con un máximo de 300 búsquedas por semana. También ofrece una versión para el uso comercial poseyendo paquetes prepagados, además de incluir una interfaz para facilitar la búsqueda manual y el acceso a la API para búsquedas automatizadas más avanzadas.

B. EXTENSIÓN PARA NAVEGADORES:

El TinEye también posee una extensión para los navegadores Google Chrome, Opera y Firefox que permite la búsqueda de cualquier imagen a partir de sus propios sitios de origen, sin que sea necesario descargar la imagen o copiar la URL para después enviarla en la plataforma. La funcionalidad queda disponible al hacer clic con el botón derecho del ratón sobre la imagen deseada.

C. TINEYE ALERTS:

Esa funcionalidad permite que cargues todas las imágenes que deseas rastrear y diariamente la plataforma rastreará la web buscando correspondencias y advirtiéndote en el momento en que sean indexadas por la API. Además de suministrar informes que indican exactamente donde tus imágenes aparecen. La funcionalidad TinEye Alerts es pagada y funciona por medio de paquetes prepagados. Es posible solicitar una demostración del servicio.



3. CÓMO ACCEDER

VERSIÓN WEB:

El TinEye es una herramienta que no necesita cualquier tipo de descarga o instalación. Basta con accesar la dirección https://tineye.com/ por medio de tu navegador web. Caso no poseas la versión comercial, haz el login en https://tineye.com/service_select.

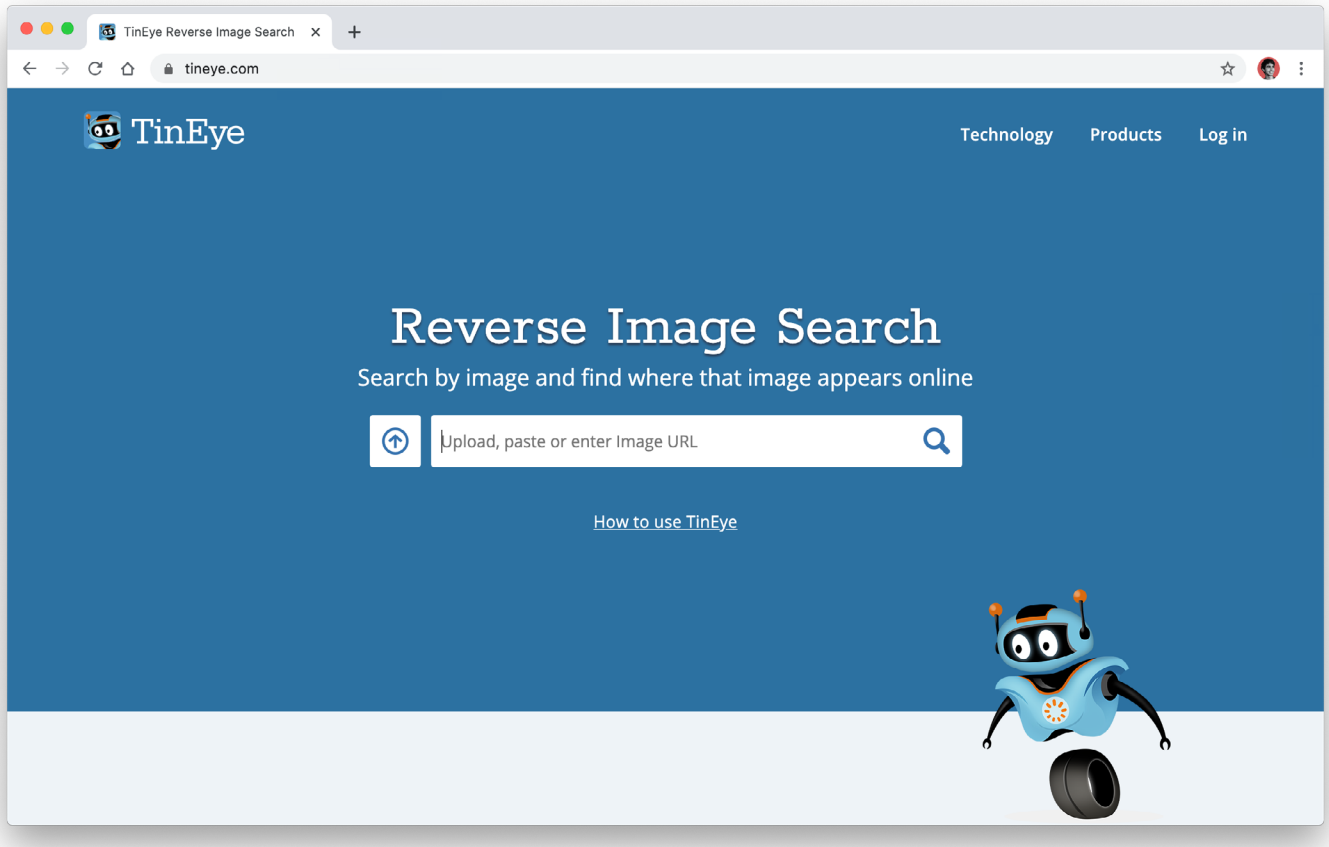
EXTENSIÓN:

Caso quieras, podrás utilizar la extensión gratuita para los navegadores Google Chrome y Mozilla Firefox accesando sus respectivas tiendas de extensión. Sin embargo, para utilizar en el navegador Opera será necesario primero instalar la herramienta "Install Chrome Extensions" y la propia extensión para el Chrome. De esa manera, podrás importarla del Chrome a tu navegador Opera.

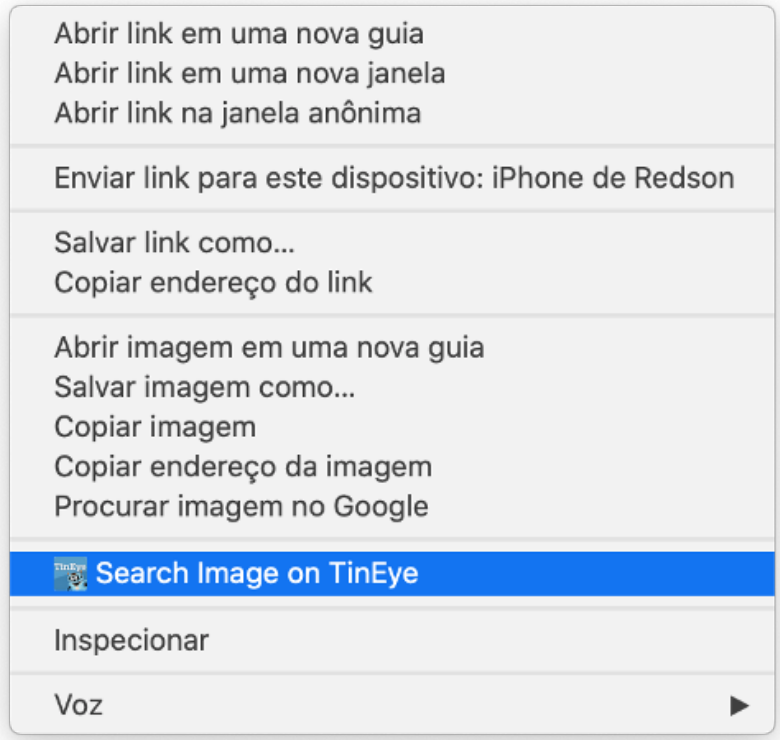
4. CÓMO UTILIZAR

PASO 1:

Tras accesar la dirección de la herramienta (https://tineye.com/), la primera etapa es realizar la búsqueda de la imagen. Puedes hacer upload de una imagen, copiarla o señalar hacia una imagen de la Web digitando o pegando una URL (sitio). También puedes utilizar el recurso "Arrastrar y Soltar". Eso permite que arrastres una imagen, pases el ratón sobre la pestaña en la cual el TinEye esté abierto y sueltes en la página para hacer la búsqueda.



Caso quieras utilizar la extensión, tras seguir las etapas de descargas descritas en “cómo acceder”, basta con hacer clic con el botón derecho del ratón y seleccionar la opción “Search Image on TinEye”. La búsqueda irá abrir por patrón en una nueva pestaña.

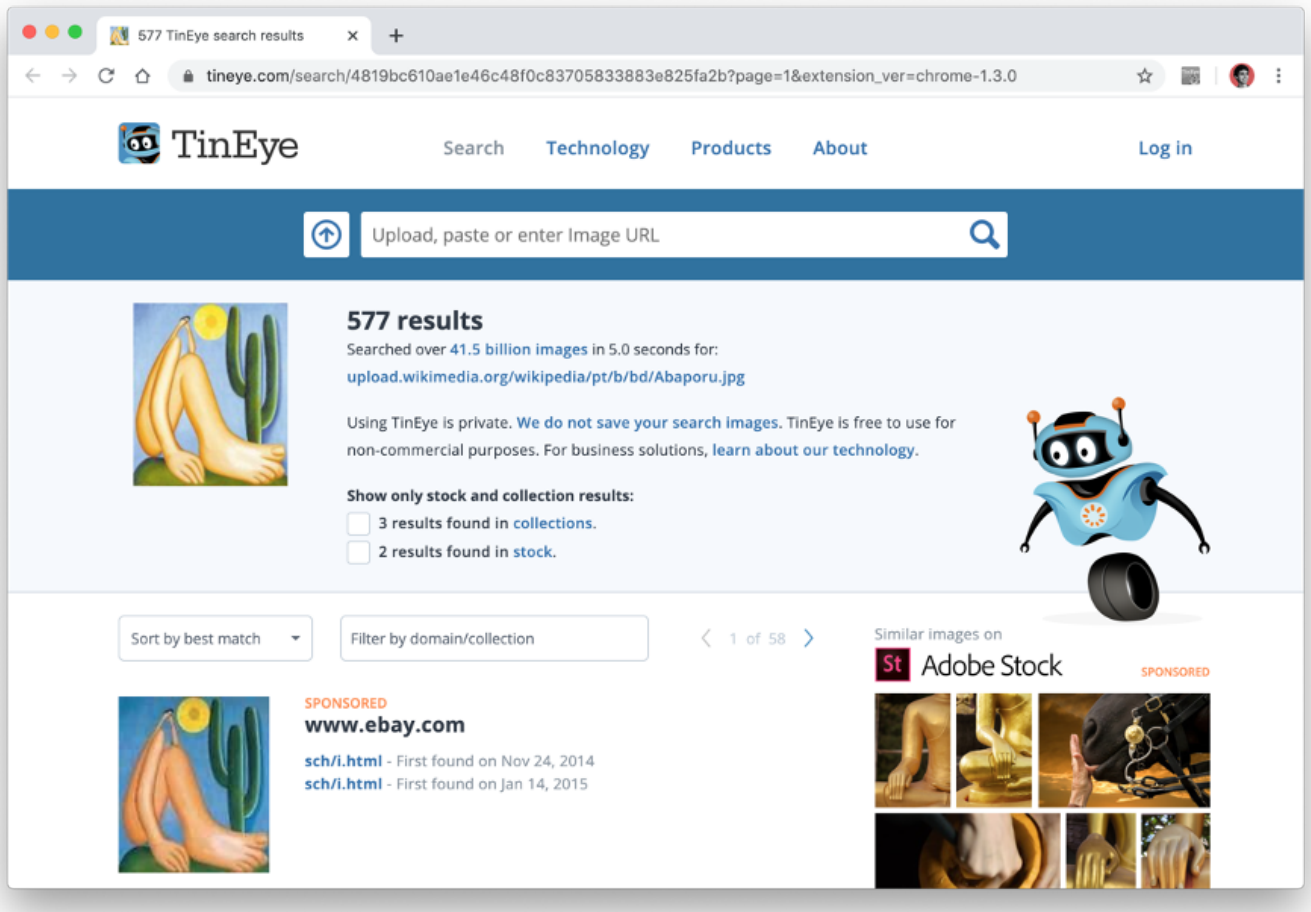


RECOMENDACIONES:

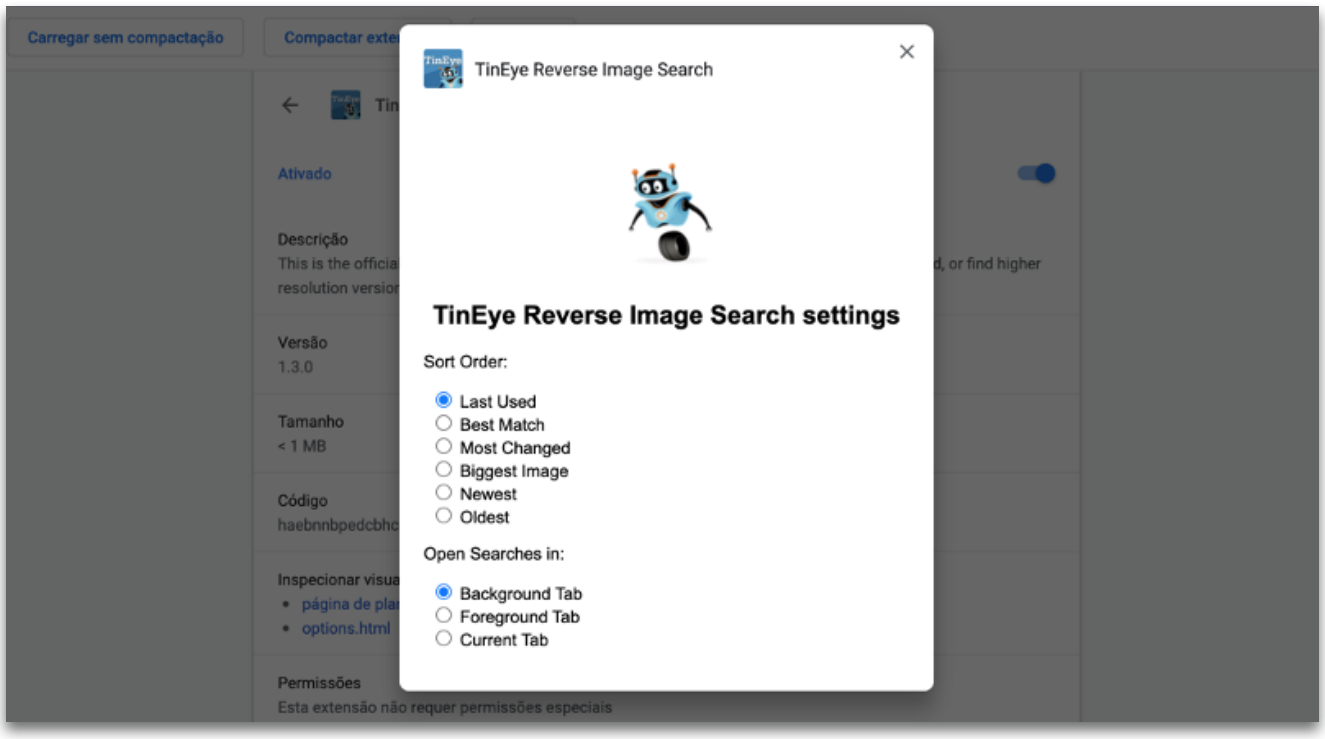
El TineEye exhibe resultados más exactos utilizando imágenes con por lo menos 300 pixels en cualquier dimensión y sin marcas de agua. Además, es importante resaltar también que el upload de imágenes posee algunas limitaciones, como por ejemplo un máximo de 20 megabytes por archivo y un mínimo de 100 pixels en cualquier dimensión de la imagen para realizar la búsqueda.

PASO 2:

Tras buscar la imagen, serás redirigido a la página de resultados. Por patrón, ellos son clasificados por “mejor correspondencia”. Sin embargo, también puedes clasificar por el tamaño de la imagen, fecha que la API del TinEye indexó la imagen en la herramienta o por la cantidad de alteraciones que sufrió. Es importante entender también que la fecha en que el TinEye rastreó una imagen no es necesariamente la fecha en la cual apareció por primera vez en alguna página web. Además, también es posible filtrar por domino o colección de imágenes stock haciendo clic en “Filter By...”.

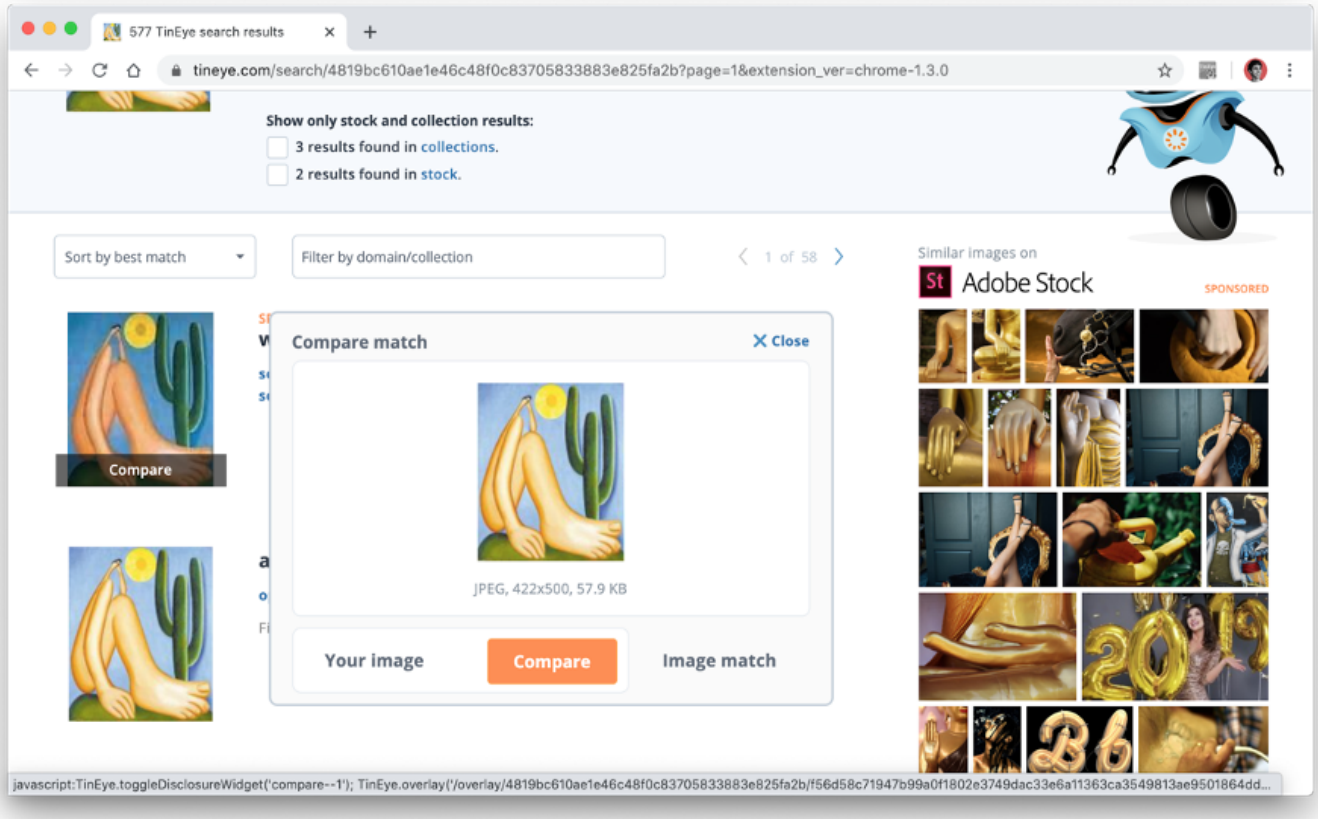


Las configuraciones de extensión del TinEye también suministran opciones para seleccionar el orden de clasificación, además de poder elegir si los resultados de las búsquedas deben ser abiertos en una nueva pestaña en segundo plano o en la pestaña actual. Para ello, haz clic con el botón derecho en el ícono de extensión, después haz clic en “opciones” y altera las propiedades deseadas.



PASO 3:

Después, es posible utilizar el recurso TinEye Compare, que permite alternar rápidamente entre la búsqueda y la imagen del resultado. De esa manera, es posible percibir mejor las diferencias entre las dos imágenes, sobre todo si fueron manipuladas de alguna forma. Para ello, selecciona la imagen en la lista y alterna entre las visualizaciones.



VIEWDNS

por Diego Cerqueira

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

EN ESTE TUTORIAL, CONOCERÁS LA HERRAMIENTA VIEWDNS. ¡APROVÉCHALO!

1. LO QUÉ ES

ViewDNS es una herramienta web que auxilia en el proceso de pesquisa de sitios y dominios de internet, principalmente en relación al DNS y otros detalles técnicos de cada dominio, que incluyen sus informaciones pero no se limitan al DNS .

El ViewDNS posee una diversidad de herramientas para explorar especificaciones técnicas. Por medio de una interfaz única y sencilla, serás capaz de obtener diversas informaciones para tu proceso de pesquisa sobre un dominio en internet.

Todas las informaciones obtenidas por el sitio son abiertas y están disponibles en internet, suministradas por los propios dueños de dominio al registrar sus nombres de dominio a través de intermediarios. El ViewDNS posee un banco de datos propios de esas informaciones y mantiene registros de dominios alrededor del mundo.

¡IMPORTANTE!

Servicio de Nombres de Dominio (DNS, en inglés) es uno de los alicerces de la web, una vez que es responsable por traducir las direcciones de IP (internet Protocol Address), un conjunto de cuatro dígitos asociado al servicio disponible en internet, ofreciendo la capacidad de traducir esas direcciones numéricas en formato textual, facilitando, de esa manera, la memorización.

2. CÚALES SON LAS FUNCIONALIDADES

Diversas funcionalidades del ViewDNS pueden y deben ser utilizadas en conjunto. Piensa en las herramientas presentadas en este tutorial como un kit de herramientas. La utilización de algunas de las que están disponibles en el sitio requiere algún conocimiento sobre Redes de Computadores y conceptos básicos sobre Protocolos de Internet y sus tecnologías. Sin embargo, las herramientas abajo pueden ser utilizadas sin ningún perjuicio.

A. BÚSQUEDA DE INFORMACIONES DE DOMINIO (DOMAIN / IP WHOIS):

Muestra informaciones sobre el contratante del dominio, si el dominio está registrado o no y sus informaciones de contacto.

B. BÚSQUEDA REVERSA WHOIS (REVERSE WHOIS LOOKUP):

“Quién es”, en su traducción literal, Whois es una herramienta para recuperar informaciones públicas sobre un nombre de dominio. A través de la búsqueda reversa (Reverse Lookup) con un nombre de dominio, por ejemplo itsrio.org, podrás buscar todos los dominios registrados por un individuo o empresa. Las búsquedas pueden ser realizadas a través de dos parámetros: por el nombre del individuo/empresa o por correo electrónico.

C. BÚSQUEDA DE DNS (DNS RECORD LOOKUP):

Podrás visualizar todas las configuraciones de registro (A, MX, CNAME) asociadas al dominio buscado. Para entender más sobre los tipos de registro accede: https://www.nerion.es/soporte/aprende-como-funcionan-los-registros-dns/

3. CÓMO ACCEDER

Para acceder a las herramientas disponibles por elViewDNS, digita o copia y pega en tu navegador de preferencia la dirección https://viewdns.info/

4. CÓMO UTILIZAR

Para utilizar la búsqueda de informaciones sobre un dominio es necesario tener a manos su nombre. Abajo un ejemplo de como identificar un nombre de dominio.

SITIO	DOMINIO
https://itsrio.org/pt/cursos/	itsrio.org
https://www1.folha.uol.com.br/poder/2020/06/assembleia-legislativa-do-rio-decide-abrir-processo-de--impeachment-contra-witzel.shtml	folha.uol.com.br

Encontrar el dominio es una tarea simple. Basta con observar en la dirección (sitio) lo que está después del **www** y lo que está antes de la primera barra (**/**). En la dirección del sitio ITS Rio podemos encontrar el dominio apenas excluyendo lo que está destacado en rojo:

Enlace completo: **www.**itsrio.org**/pt/cursos** | Dominio: itsrio.org

Para saber más sobre dominios y sus diversos niveles accede: https://miposicionamientoweb.es/que-es-un-dominio/

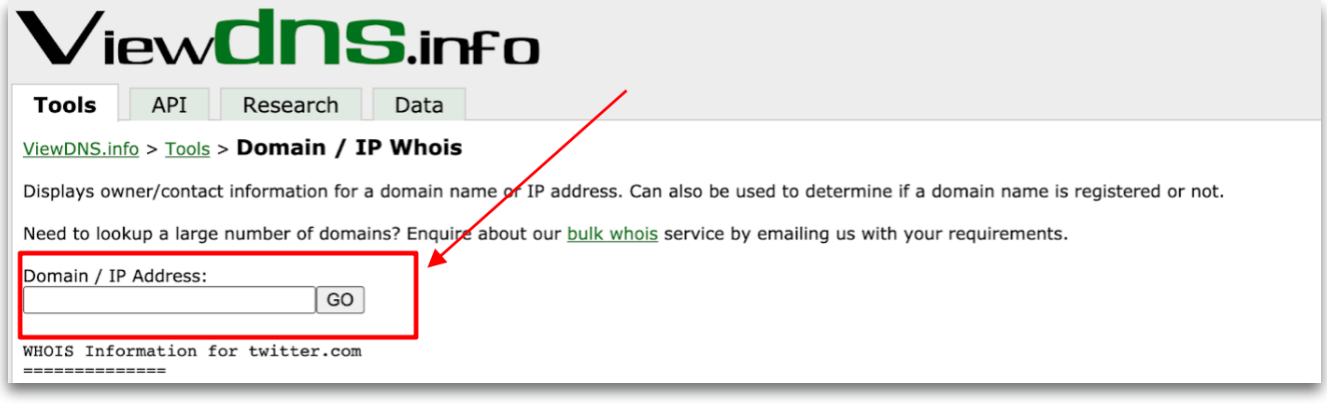
4.1 BÚSQUEDA DE INFORMACIONES DE DOMINIO (WHOIS)

PASO 1:

Accesa en el navegador: https://viewdns.info/whois/

PASO 2:

En la página, informa la dirección del dominio o dirección de IP que te gustaría buscar.



PASO 3:

Informa la dirección, haz clic en “GO”.

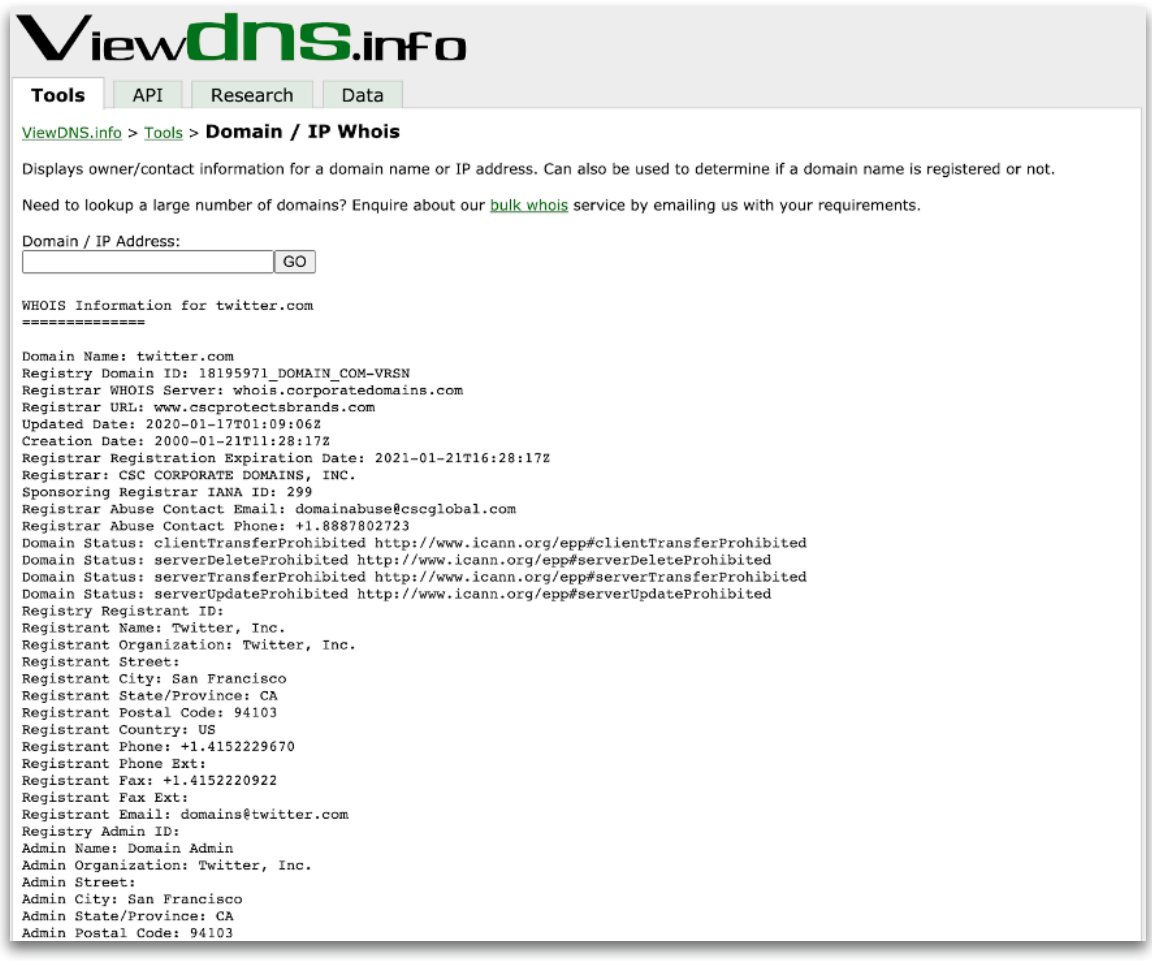
PASO 4:

Página de resultados: el dominio que utilizamos fue el de la red social Twitter, donde en el campo entramos con el valor: twitter.com. La imagen abajo muestra un ejemplo de los datos que pueden ser obtenidos.

IMPORTANTE:

a. Hay casos en que el propietario del dominio oculta informaciones;

b. Las informaciones disponibles pueden variar entre los dominios.



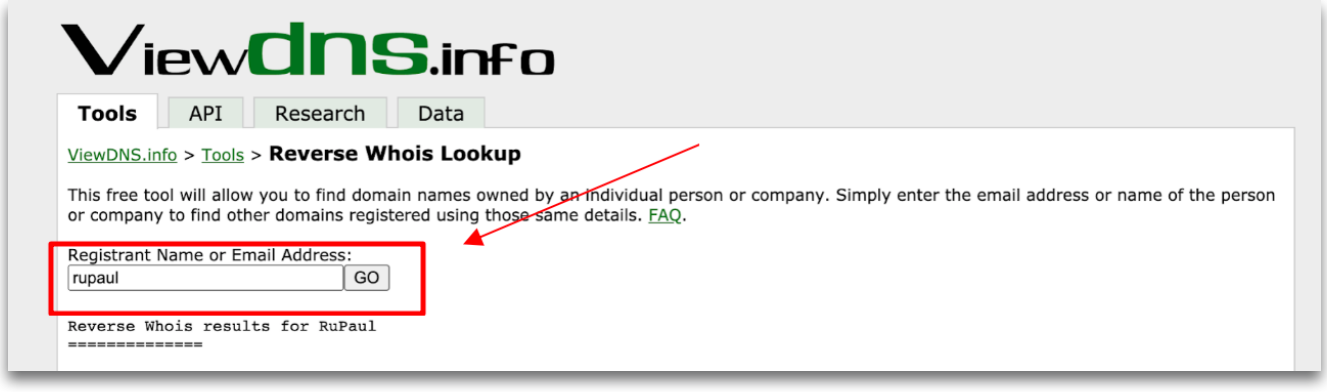
4.2 BÚSQUEDA REVERSA WHOIS (REVERSE WHOIS LOOKUP)

PASO 1:

Accesa en el navegador: https://viewdns.info/reversewhois/

PASO 2:

En la página, informa el nombre del propietario o dirección de correo electrónico que te gustaría buscar.



PASO 3:

Informa el término deseado, haz clic en “GO”.

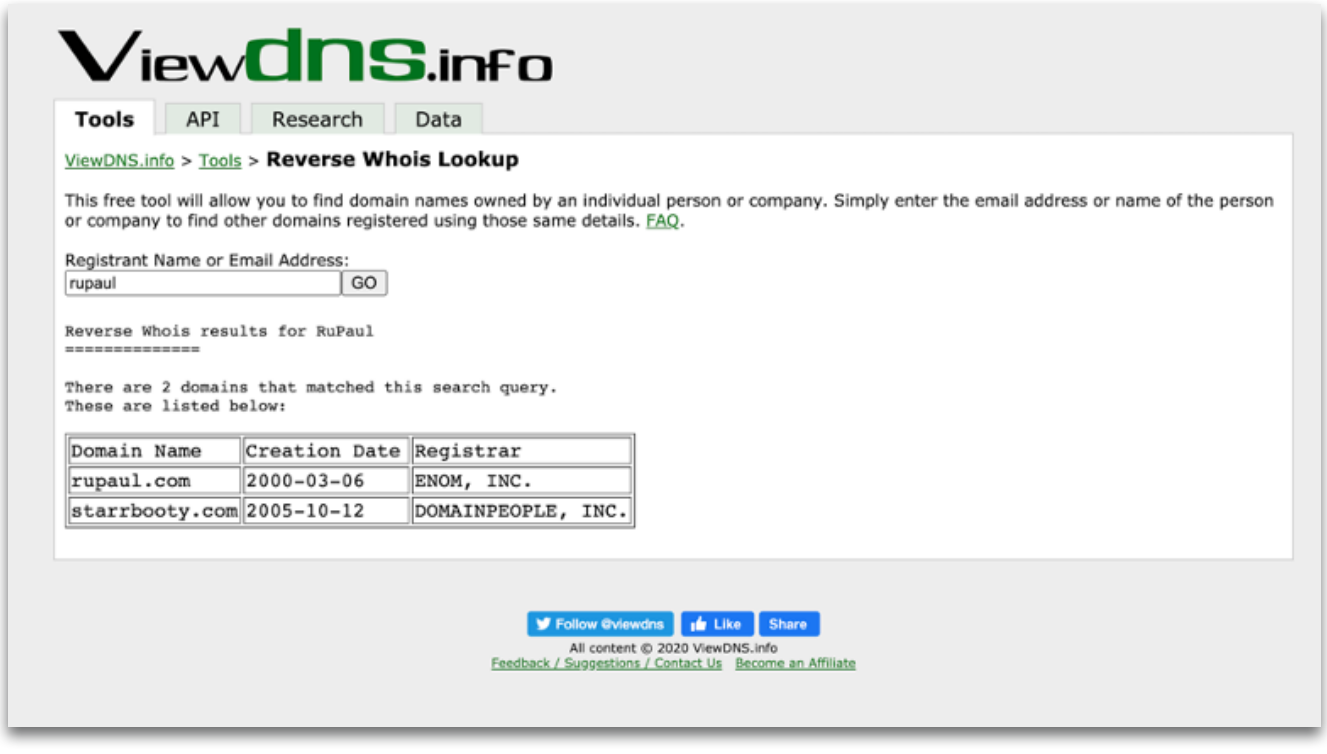
PASO 4:

Página de resultados: el dominio que utilizamos fue el de la red social Twitter, donde en el campo entramos con el valor: rupaul. La imagen abajo muestra un ejemplo de datos que pueden ser obtenidos.

IMPORTANTE:

a. Hay casos en que el propietario del dominio oculta informaciones;

b. Las informaciones disponibles pueden variar entre los dominios.



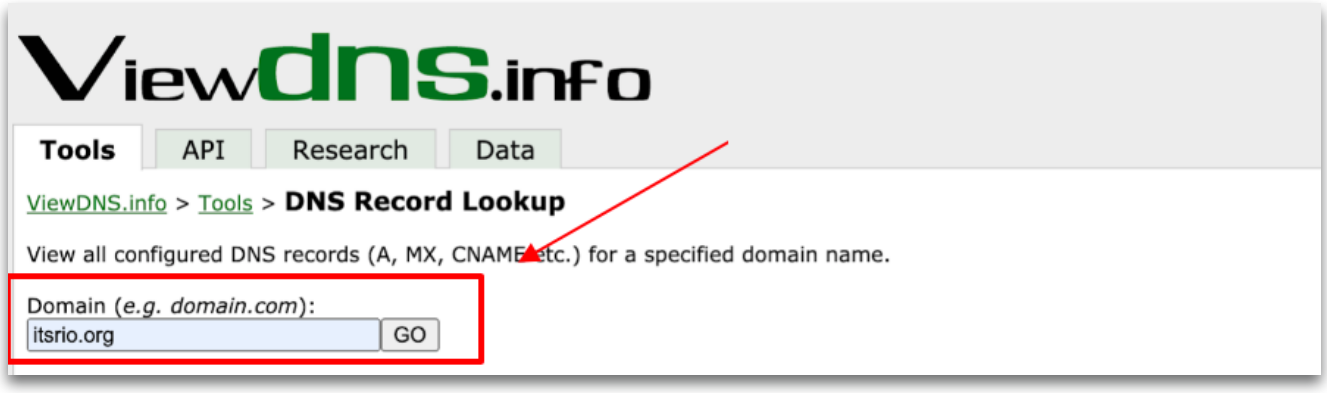
4.3 DNS RECORD LOOKUP

PASO 1:

Accesa en el navegador: https://viewdns.info/dnsrecord/

PASO 2:

En la página, informa la dirección de dominio que te gustaría buscar.



PASO 3:

Informa el término deseado, haz clic en ”GO”.

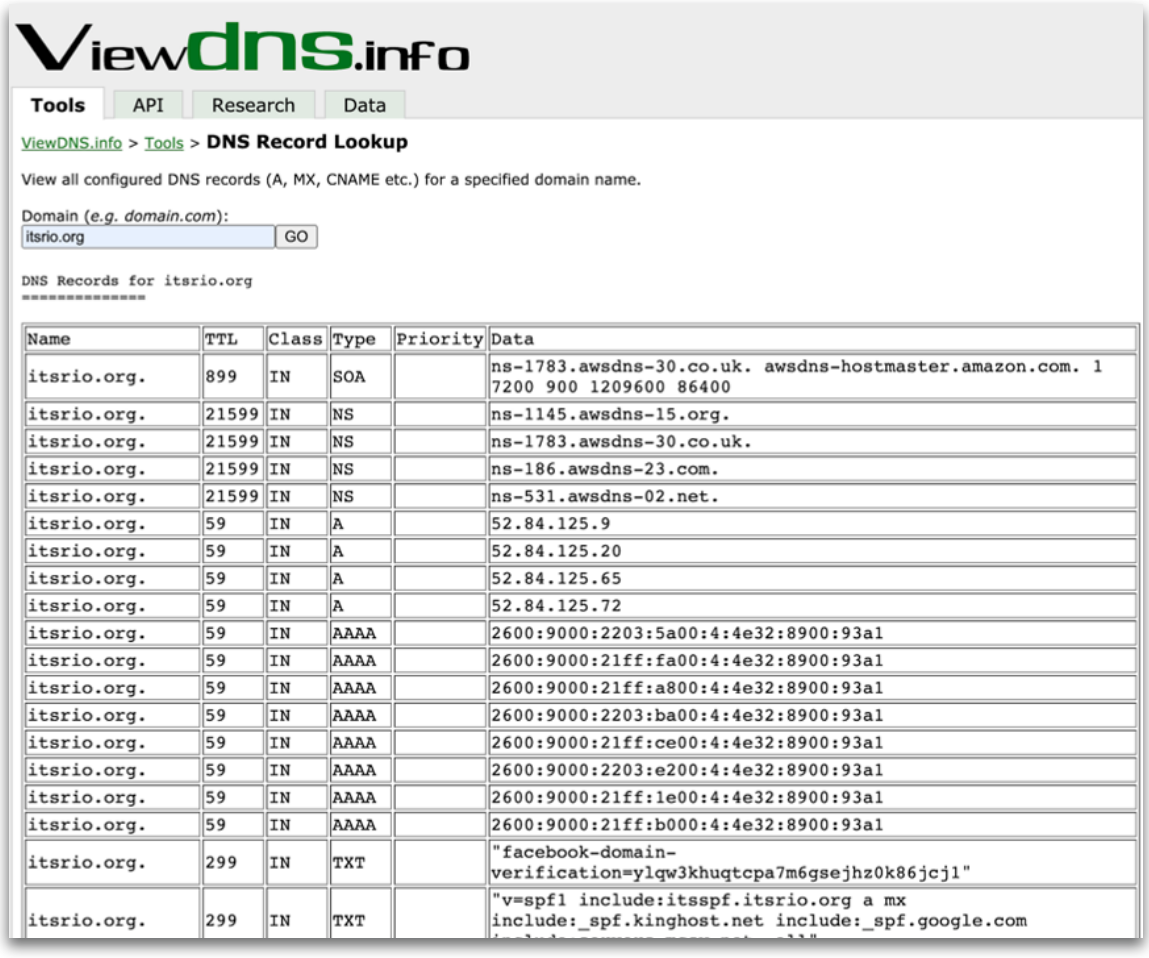
PASO 4:

Página de resultados: el dominio que utilizamos fue el de la red social Twitter, donde en el campo entramos con el valor: itsrio.org. La imagen abajo muestra un ejemplo de los datos que pueden ser obtenidos.

IMPORTANTE:

a. Hay casos en que el propietario del dominio oculta informaciones;

b. Las informaciones disponibles pueden variar entre los dominios.



Name	TTL	Class	Type	Priority	Data
itsrio.org.	899	IN	SOA		ns-1783.awsdns-30.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
itsrio.org.	21599	IN	NS		ns-1145.awsdns-15.org.
itsrio.org.	21599	IN	NS		ns-1783.awsdns-30.co.uk.
itsrio.org.	21599	IN	NS		ns-186.awsdns-23.com.
itsrio.org.	21599	IN	NS		ns-531.awsdns-02.net.
itsrio.org.	59	IN	A		52.84.125.9
itsrio.org.	59	IN	A		52.84.125.20
itsrio.org.	59	IN	A		52.84.125.65
itsrio.org.	59	IN	A		52.84.125.72
itsrio.org.	59	IN	AAAA		2600:9000:2203:5a00:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:21ff:fa00:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:21ff:a800:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:2203:ba00:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:21ff:ce00:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:2203:e200:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:21ff:1e00:4:4e32:8900:93a1
itsrio.org.	59	IN	AAAA		2600:9000:21ff:b000:4:4e32:8900:93a1
itsrio.org.	299	IN	TXT		"facebook-domain-verification=ylqw3khuqtcpa7m6gsejhz0k86jcj1"
itsrio.org.	299	IN	TXT		"v=spf1 include:itsspf.itsrio.org a mx include:_spf.kinghost.net include:_spf.google.com

4.4 IP HISTORY

PASO 1:

Accesa en el navegador: https://viewdns.info/iphistory/

PASO 2:

En la página, informa la **dirección de dominio** que te gustaría buscar.

PASO 3:

Informa el término deseado, haz clic en ”GO”.

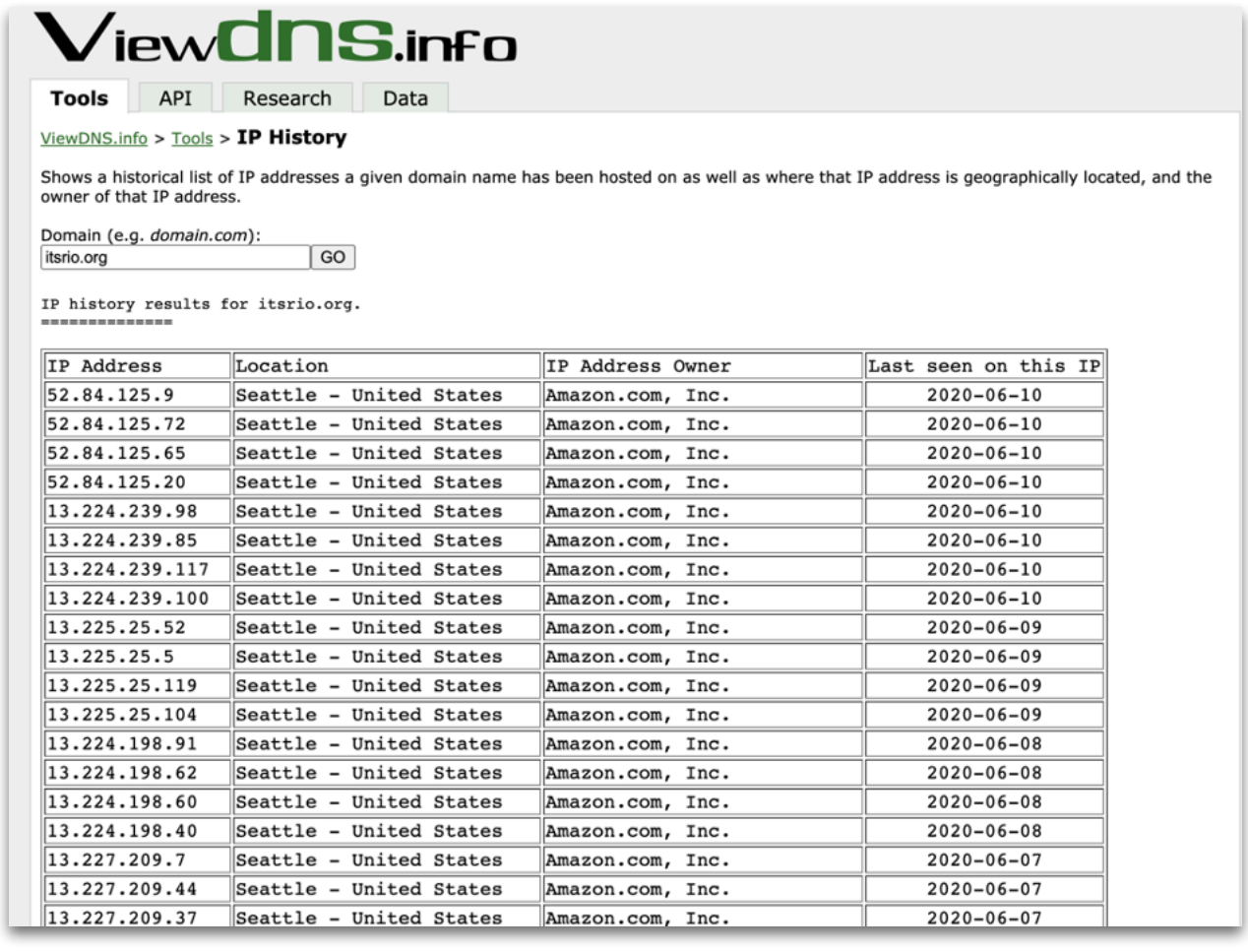
PASO 4:

Página de resultados: el dominio que utilizamos fue el de la red social Twitter, donde en el campo entramos con el valor: itsrio.org. La imagen abajo muestra un ejemplo de los datos que pueden ser obtenidos.

IMPORTANTE:

a. Hay casos en que el propietario del dominio oculta informaciones;

b. Las informaciones disponibles pueden variar entre los dominios.



IP Address	Location	IP Address Owner	Last seen on this IP
52.84.125.9	Seattle - United States	Amazon.com, Inc.	2020-06-10
52.84.125.72	Seattle - United States	Amazon.com, Inc.	2020-06-10
52.84.125.65	Seattle - United States	Amazon.com, Inc.	2020-06-10
52.84.125.20	Seattle - United States	Amazon.com, Inc.	2020-06-10
13.224.239.98	Seattle - United States	Amazon.com, Inc.	2020-06-10
13.224.239.85	Seattle - United States	Amazon.com, Inc.	2020-06-10
13.224.239.117	Seattle - United States	Amazon.com, Inc.	2020-06-10
13.224.239.100	Seattle - United States	Amazon.com, Inc.	2020-06-10
13.225.25.52	Seattle - United States	Amazon.com, Inc.	2020-06-09
13.225.25.5	Seattle - United States	Amazon.com, Inc.	2020-06-09
13.225.25.119	Seattle - United States	Amazon.com, Inc.	2020-06-09
13.225.25.104	Seattle - United States	Amazon.com, Inc.	2020-06-09
13.224.198.91	Seattle - United States	Amazon.com, Inc.	2020-06-08
13.224.198.62	Seattle - United States	Amazon.com, Inc.	2020-06-08
13.224.198.60	Seattle - United States	Amazon.com, Inc.	2020-06-08
13.224.198.40	Seattle - United States	Amazon.com, Inc.	2020-06-08
13.227.209.7	Seattle - United States	Amazon.com, Inc.	2020-06-07
13.227.209.44	Seattle - United States	Amazon.com, Inc.	2020-06-07
13.227.209.37	Seattle - United States	Amazon.com, Inc.	2020-06-07

GOOGLE ALERTS

por Redson Fernando

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

EN ESTE TUTORIAL, CONOCERÁS LA HERRAMIENTA GOOGLE ALERTS. ¡APROVÉCHALO!

1. LO QUÉ ES

El Google Alerts es una herramienta gratuita creada para monitorear nuevos contenidos indexados por el motor de búsqueda que están relacionados a una palabra clave o termo definido por el usuario.

2. CÚALES SON LAS FUNCIONALIDADES

El Google Alerts permite detectar de manera sencilla y eficiente los contenidos descentralizados en la internet. Por ejemplo, cuando páginas de la web, noticias, artículos o publicaciones de blogs aparecen indexados en el Google conteniendo el termo definido en el alerta, el usuario es notificado por correo electrónico en el momento de la creación.

Además, el recurso es personalizable. Puedes elegir no solo los termos que deseas acompañar, sino también la periodicidad de los avisos, los tipos de contenidos, las fuentes, los idiomas y la ubicación de lo que ha sido publicado. De esa manera, puedes mantenerte informado en relación a los temas que consideras relevantes y consigues realizar el monitoreo de los temas.

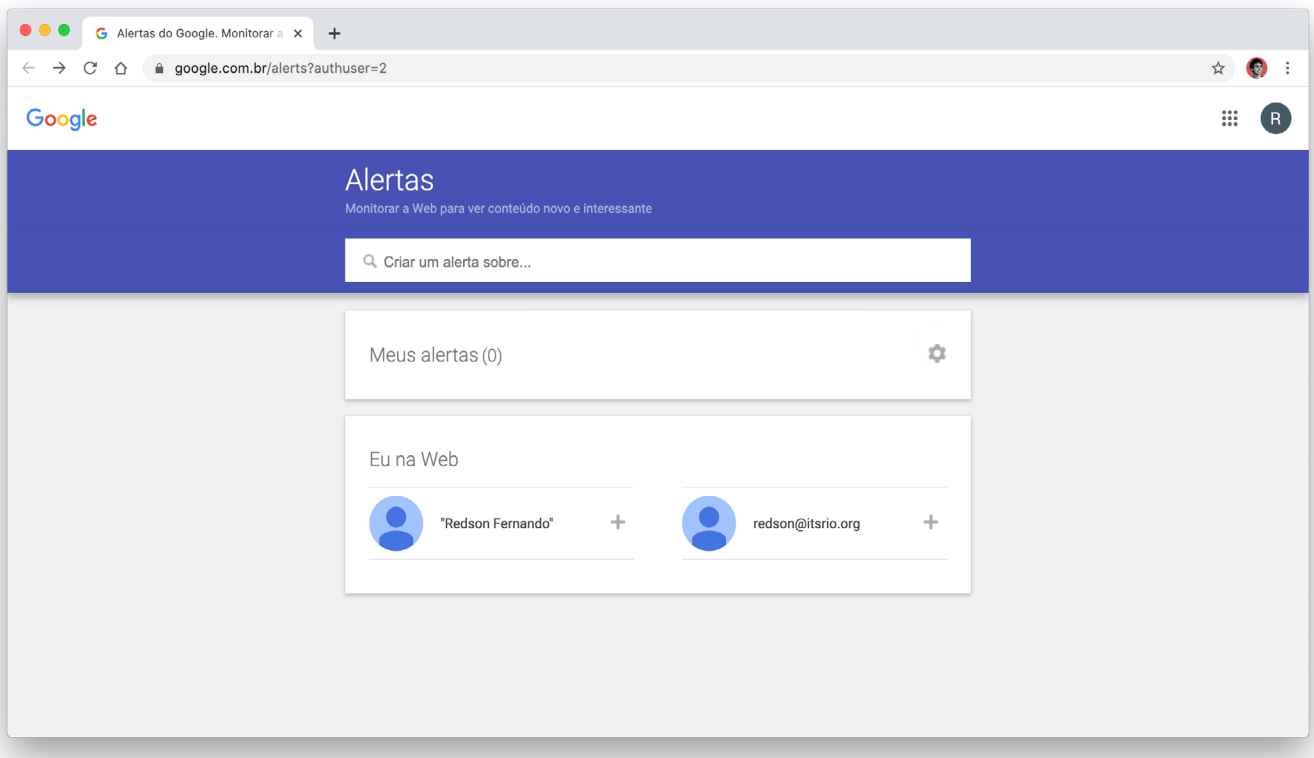
3. CÓMO ACCEDER

El Google Alerts es una herramienta que no necesita cualquier tipo de descarga o instalación. Basta con acceder a la dirección www.google.com/alerts a través de su navegador web.

4. CÓMO UTILIZAR

PASO 1:

Tras acceder a la dirección de la herramienta (www.google.com/alerts), la primera etapa es seleccionar cuales son los termos que deseas monitorear. Digita las palabras claves en la caja “Crear un alerta sobre...”. Consigues crear un alerta con su propio nombre o un correo electrónico cadastrado en el servicio por medio de la sección “Yo en la Web”. De esa manera, siempre que algún contenido en internet mencionarte a ti o a tu correo electrónico, el Google te enviará una notificación automáticamente.



PASO 2:

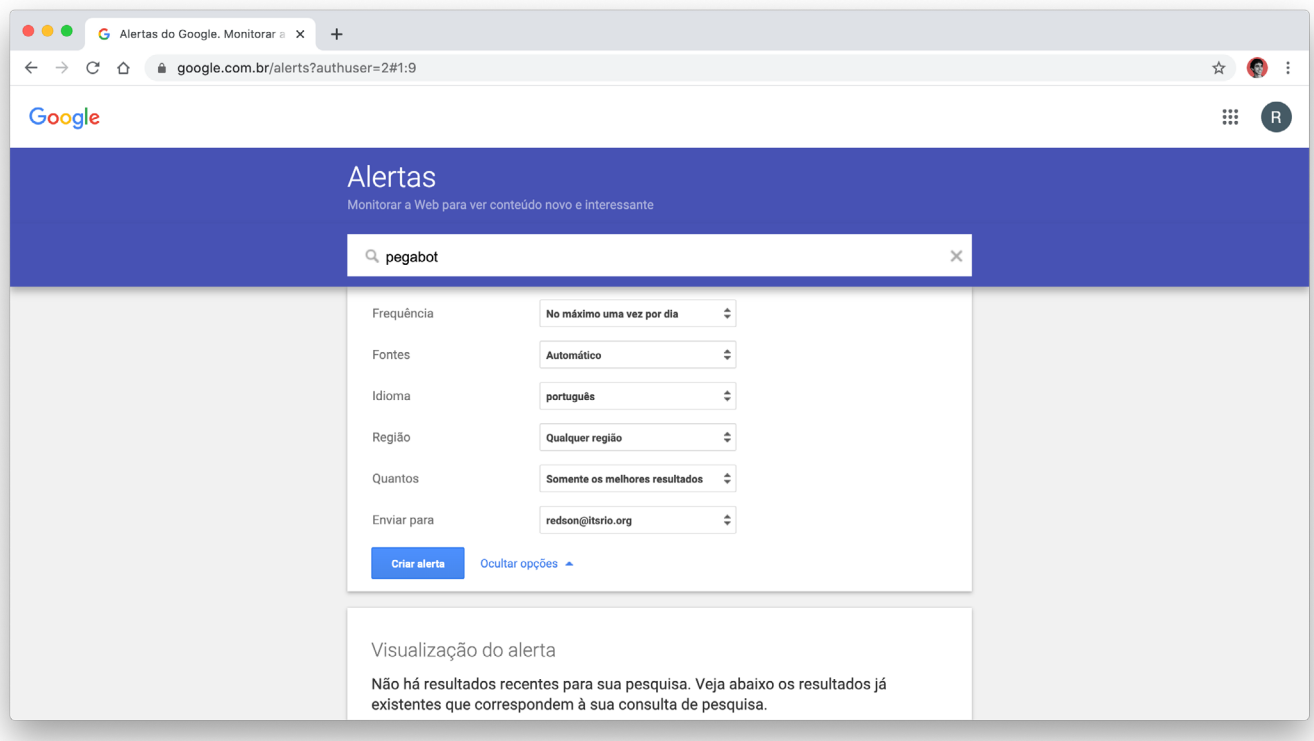
Después de seleccionar los termos, será necesario informar un correo electrónico para recibir los alertas. La herramienta utilizará automáticamente su correo electrónico Google en el caso de que esté logado en el servicio. Si quieres utilizar otro correo, es posible cambiarlo después.

PASO 3:

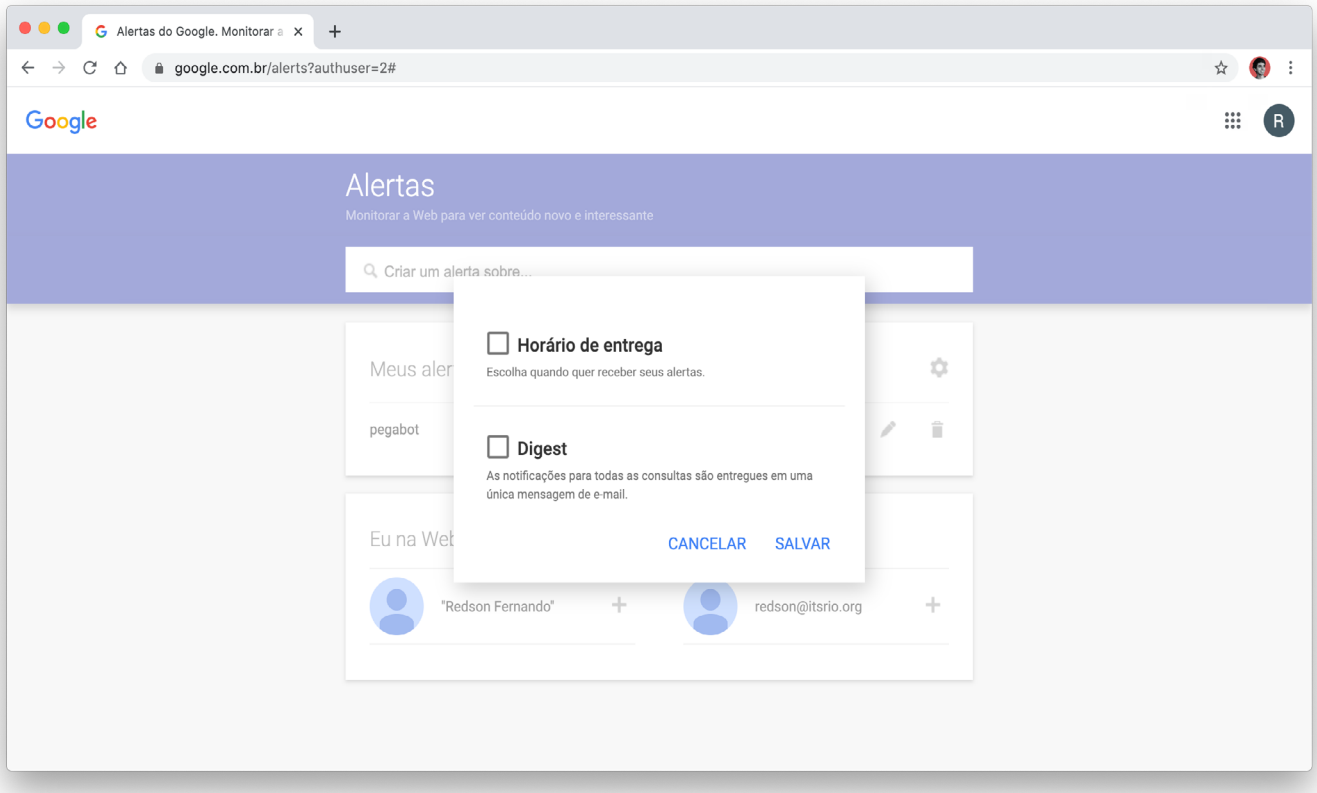
Para alterar las configuraciones del alerta, haz clic en “Mostrar opciones”. Puedes alterar la frecuencia con la que recibes notificaciones, los tipos de sitios exhibidos, su idioma, la región que deseas que las informaciones vengan, cuantos resultados quieres ver y el correo electrónico que recibirá los alertas.

PASO 4:

Después, basta con hacer clic en “Crear alerta” para recibir los correos siempre que el Google encuentre resultados de búsqueda correspondientes a las preferencias seleccionadas.



Caso quieras, es posible editar el alerta haciendo clic en el icono de lápiz y después en “Actualizar alerta”. También es posible excluir el alerta haciendo clic en el ícono de basurero en la página principal de la herramienta o haciendo clic en “Cancelar Inscripción” en el correo de notificación. En el icono de engranaje puedes elegir si recibirás los alertas siempre en un horario específico con la opción “Horario de entrega” o si deseas recibir todos los múltiples alertas creados en un mensaje único y con la frecuencia programada por medio de la opción “Digest.



LISTA DE REFERENCIAS

EQUIPO DE DEMOCRACIA Y TECNOLOGÍA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

AQUÍ ENCONTRARÁS UNA SERIE DE REFERENCIAS ACADÉMICAS, DOCUMENTOS DE INVESTIGACIÓN Y OTRAS HERRAMIENTAS QUE CUBREN LOS TEMAS DE AUTOMATIZACIÓN, DESINFORMACIÓN Y ANÁLISIS DE REDES. ¡EXPLORA AL MÁXIMO Y HAGA BUEN PROVECHO!

1. LIBROS

a. Handbook of Research on Deception, Fake News, and Misinformation Online

b. Lie Machines - How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives

c. The Reasoning Voter: Communication and Persuasion in Presidential Campaigns

d. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media

e. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics

2. INFORMES

a. Understanding Information Disorder

b. Lexicon of Lies: Terms for Problematic Information

c. Dealing with disinformation: Strategies for digital citizen empowerment

d. Supporting Information: Integrity and Civil Political Discourse

e. Computational Power: Automated Use of WhatsApp in the Elections

f. Industry responses to computational propaganda and social media manipulation

g. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation

h. Polarisation and the use of technology in political campaigns and communication

i. The spread of true and false news online

j. No Rest for the Sick: Coronavirus Disinformation from Chinese Users Targets Taiwan

k. Tweets That Chill: Analyzing Online Violence Against Women in Politics

3. ARTÍCULOS CIENTÍFICOS

a. What is an internet troll?

b. How to analyze Facebook data for misinformation trends and narratives

c. Misinformation Ecosystem

d. The Rise of Fake News and Social Media Manipulation in Latin American Politics

e. The Bots That Are Changing Politics

f. Become a bots hunter in 6 steps!

g. Misinformation on social media: Can technology save us?

4. TOOLKITS (CAJA DE HERRAMIENTAS)

a. Data Analytics for Social Media Monitoring: Guidance on Social Media Monitoring and Analysis - Techniques, Tools and Methodologies

b. RESIST: Counter-Disinformation Toolkit

c. Newsgathering and Monitoring on the Social Web

d. First Draft Basic Toolkit

e. Bellingcat's Online Investigation Toolkit

f. Introduction to Data Journalism

5. PROYECTOS

a. Chicas Poderosas

b. Media Monitoring Africa

c. Co-facts

d. The Social Observatory for Disinformation and Social Media (SOMA)

e. Newtral