FERRAMENTAS PARA ENFRENTAMENTO À DESINFORMAÇÃO

EQUIPE DE DEMOCRACIA E TECNOLOGIA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

PEGABOT

por Diego Cerqueira

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

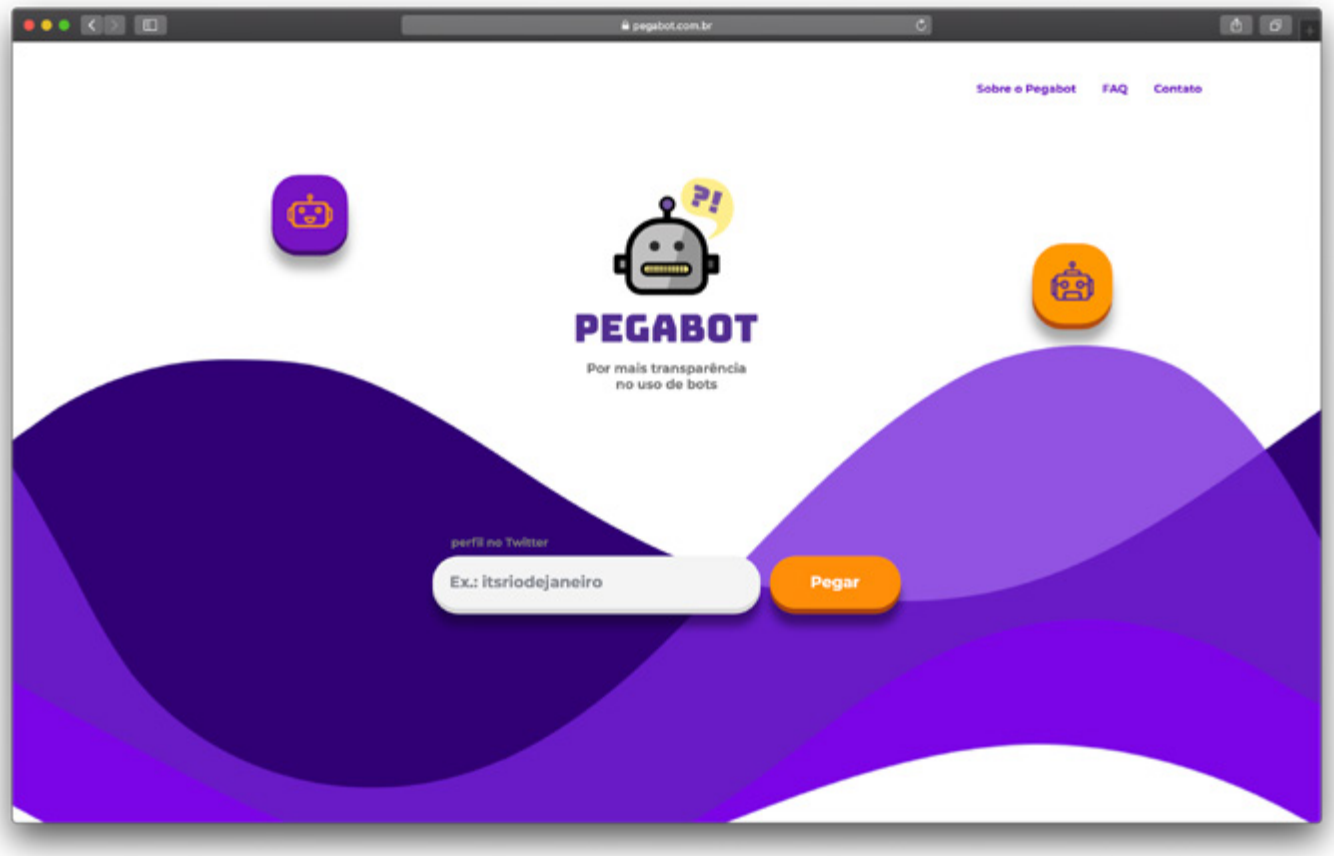
NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA PEGABOT. APROVEITE!

1. O QUE É:

Pegabot é uma de ferramenta gratuita desenvolvida pelo Instituto de Tecnologia e Sociedade (ITS Rio) em parceria com o Instituto de Tecnologia & Equidade (IT&E), para conscientização sobre o fenômeno de bots nas redes sociais. Ele atua como um instrumento de Educação Midiática sobre fenômenos de disseminação de desinformação por meio de automação no Twitter.

O Pegabot permite a identificação de contas com probabilidade de serem bots na plataforma. Para isso, basta o usuário da ferramenta pesquisar os arrobas (conhecidos como Handle) de usuários do Twitter para obter o resultado percentual do quão bot aquele perfil é considerado. Desta forma, a cada usuário pesquisado, o Pegabot realiza uma análise probabilística em relação ao comportamento do usuário na rede social. Para montar sua análise, o Pegabot leva em consideração diferentes critérios, que vão desde o sentimento expresso pelos Tweets postados, a frequência de postagens do perfil analisado e os intervalos de tempo entre as postagens.

A ferramenta foi construída em código aberto, e qualquer pessoa interessada pode verificar os códigos fontes. O Pegabot encoraja e busca constante melhorias por meio de colaborações feitas por comunidades de desenvolvedores e demais pesquisadores da área.



2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES:

Na atual versão do Pegabot, é possível realizar a análise de qualquer perfil do Twitter, individualmente, para verificar o percentual probabilístico da conta ser um robô. Ainda não há possibilidade de realizar análises de diversos perfis simultaneamente.

3. COMO ACESSAR

A ferramenta está disponível através do site www.pegabot.com.br, e não há necessidade de instalação ou de baixar qualquer software adicional para utilização. Toda a navegação pela interface da ferramenta foi pensada para possibilitar, ainda, uma experiência tanto pelo desktop quanto em aparelhos mobile, ou seja, pelo celular.

4. COMO UTILIZAR

Para realizar análises, acesse o site da ferramenta (www.pegabot.com.br). Observe na tela inicial dois elementos importantes:

1. Barra de pesquisa: barra onde você poderá inserir o perfil (ou arroba) do usuário a ser analisado pela ferramenta.

2. Botão “pegar”: botão para iniciar a análise do perfil.

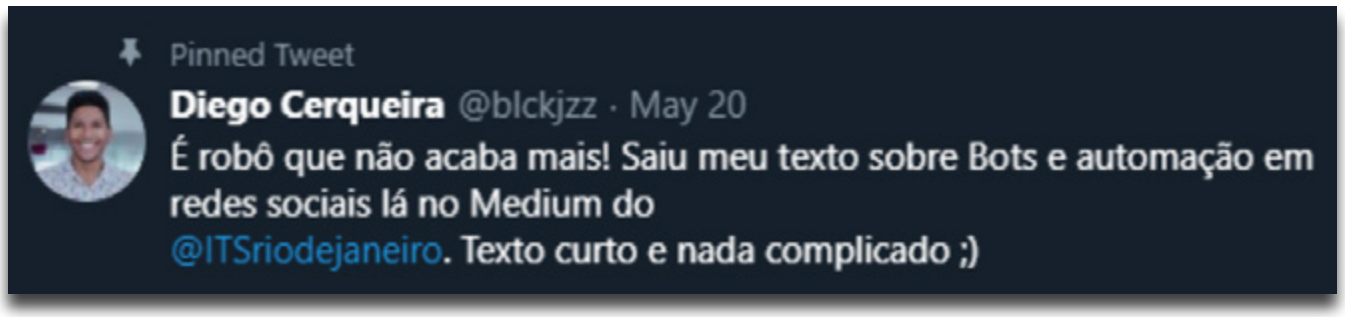
4.1. PARA OBTER O USUÁRIO

Para analisar um perfil no Pegabot você primeiro precisa conhecer o handle ou arroba (@), que pode ser obtida no perfil do usuário, dado que essa informação é pública.

Identificar o perfil do usuário é bem fácil, basta separar tudo que vem depois da barra no endereço do Twitter. Veja o exemplo abaixo.

LINK DO PERFIL	NOME DE USUÁRIO
https://twitter.com/blckjzz	blckjzz

Outra forma fácil de conseguir o nome do usuário, sem precisar realizar visitas ao perfil é copiando o arroba que aparece abaixo do nome identificado. O perfil abaixo é nomeado Diego Cerqueira, logo em seguida, podemos ver sua arroba @blckjzz, use o atalho do teclado para copiar e siga para o passo seguinte de análise.



4.2. REALIZANDO UMA ANÁLISE

Em posse do nome do usuário a ser analisado, já na página inicial, clique dentro da caixa destacada na imagem abaixo, em seguida, clique no botão pegar. O perfil analisado pode conter o arroba literal ou não.

A ferramenta não irá funcionar ou apresentará erros caso você insira usuários de outras redes sociais ou até mesmo o link completo do perfil para o Twitter. Para o perfil que vamos analisar, seriam aceitas duas formas @blckjzz ou blckjzz.

Ao clicar no botão análise, na tela seguinte será apresentado o resultado da análise feita pelo Pegabot, como pode ser visto na imagem abaixo.

O perfil @blckjzz apresenta uma probabilidade de 28% de comportamento de bot. Em análises, esse número representa uma baixa probabilidade do perfil ser controlado por algum tipo de automação.

ATENÇÃO! A ANÁLISE PODE FALHAR SE:

1. O perfil consultado não existir;
2. O perfil consultado foi suspenso;
3. O perfil consultado possui seus tweets privados;
4. O endereço para o perfil está incorreto.

BOT SENTINEL

por Thayane Guimarães

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA BOT SENTINEL. BOA LEITURA!

1. O QUE É:

O Bot Sentinel é uma plataforma apartidária e gratuita desenvolvida para classificar e rastrear contas não autênticas e trolls tóxicos. A plataforma utiliza aprendizado de máquina e inteligência artificial para classificar as contas do Twitter e, em seguida, adiciona as contas a um banco de dados disponível ao público que qualquer um pode navegar. Assim como o Pegabot e o Botometer, o Bot Sentinel indica a probabilidade de um perfil no twitter ser um bot ou Troll, a partir de critérios pré-estabelecidos.

A ferramenta Bot Sentinel foi treinada utilizando o modelo de aprendizado de máquina a partir de milhares de contas e milhões de tweets que possibilitam a classificação das contas do Twitter. O sistema pode classificar corretamente as contas com uma precisão de 95%. Ao contrário de outras ferramentas de aprendizado de máquina projetadas para detectar “bots”, o Bot Sentinel foca sua deteção em comportamentos e atividades específicas consideradas inadequadas pelas regras do Twitter. São analisados centenas de tweets para classificar com precisão cada conta do Twitter e fornecer um relatório de fácil compreensão. Abaixo, explicaremos conceitos e categorias importantes para uma análise correta dos resultados da ferramenta Bot Sentinel.

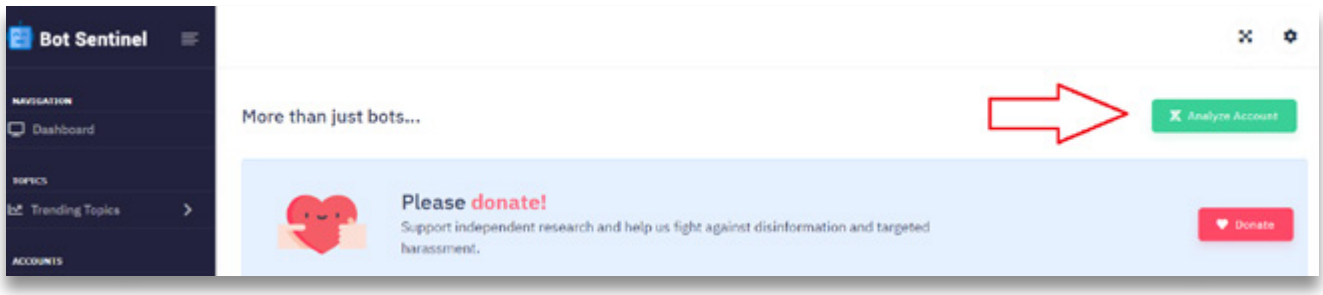
ALGUMAS DEFINIÇÕES IMPORTANTES PARA USO DO BOT SENTINEL:

Contas não autênticas: são indivíduos com intenções maliciosas que fingem ser algo que não são com a intenção política de enganar seus seguidores e público em geral, ou contas automatizadas (bots) desenvolvidas para se comportarem da maneira humana também com a intenção de manipular e distorcer o debate público. Atores ruins usam contas não autênticas para semear discórdia e causar caos nas plataformas de mídia social, e são frequentemente usadas para se envolver em assédio direcionado e trollagem tóxica.

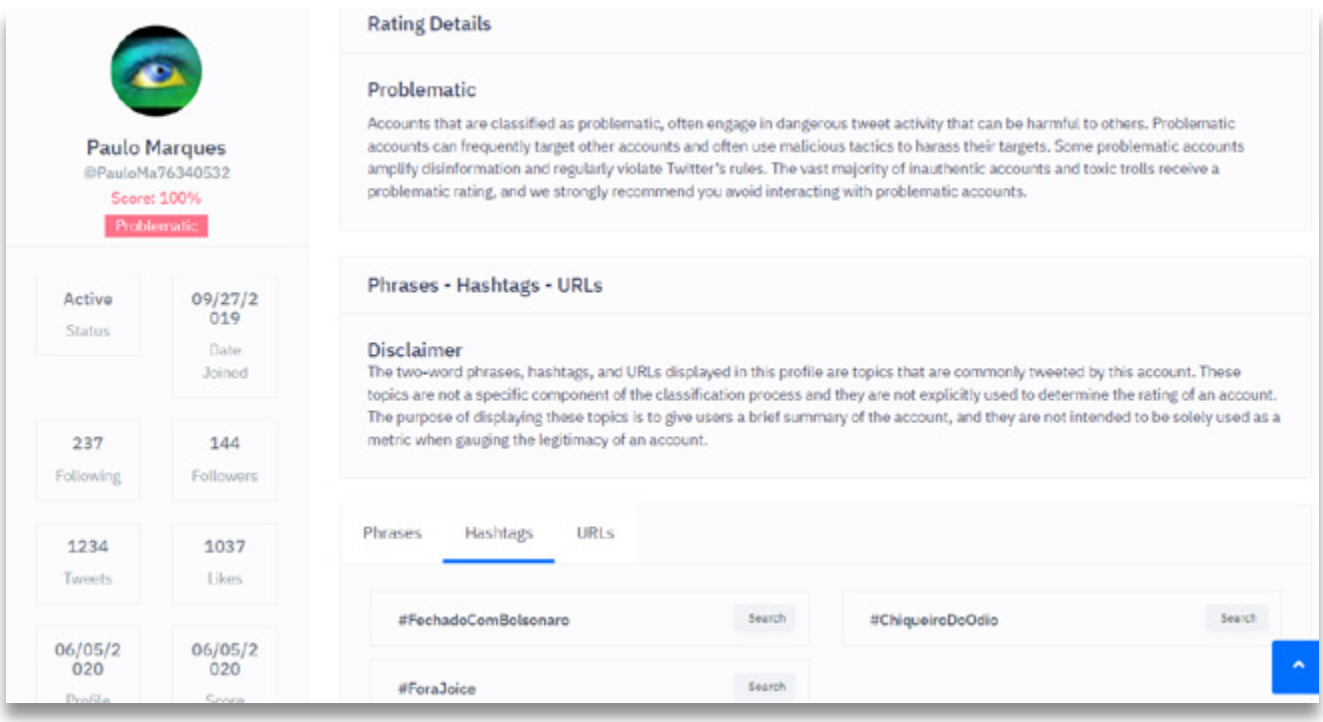
As contas são classificadas com base em um sistema de pontuação de 0% a 100%, quanto maior a pontuação, maior a probabilidade de a conta participar de atividades maliciosas. Também, várias centenas de tweets são analisados por conta e, quanto mais alguém se envolve em um comportamento que viola as regras do Twitter, maior é sua classificação no Bot Sentinel.

2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES:

Análise de perfis do Twitter: Inicialmente, a ferramenta Bot Sentinel era capaz, apenas, de analisar individualmente um perfil e dar como resultado um “score” sobre a probabilidade da conta ser um bot ou troll, com base no comportamento da conta. Esta funcionalidade ainda é central na ferramenta, já que é a partir dela que todas as outras foram derivadas.



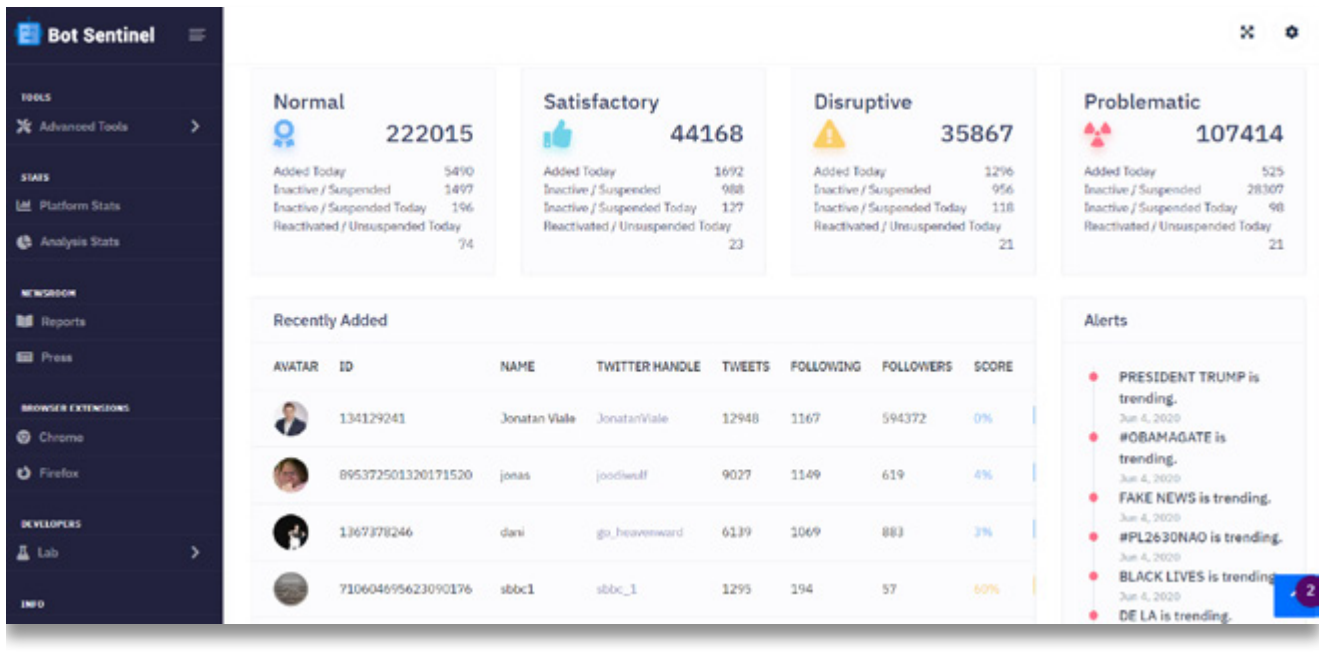
Tela inicial do Bot Sentinel com botão de “Analyze Account” para analisar perfis do



Em segundo momento, a partir de doações feitas por pessoas físicas da sociedade civil que queriam desenvolver o trabalho do Bot Sentinel, foi criada uma interface frontend em beta com acesso permissionado via e-mail de pessoas que doaram para a ferramenta. Suas funcionalidades são:

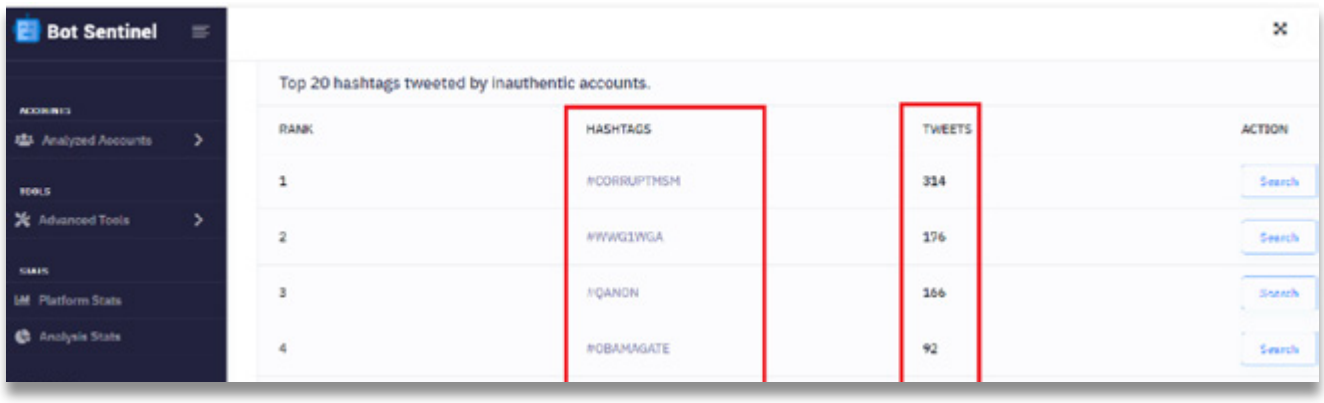
A. DASHBOARD:

Painel com atualização automática de todos os perfis que foram analisados pela ferramenta, segmentados pela categoria em que foram alocados, com base no “score” dado pela ferramenta: normal, satisfatório, disruptivo e problemático. Além disso, dashboard inicial possui linha do tempo com alertas de hashtags no Trending Topics do Twitter que estão sofrendo ação de impulsionamento algoritmo.



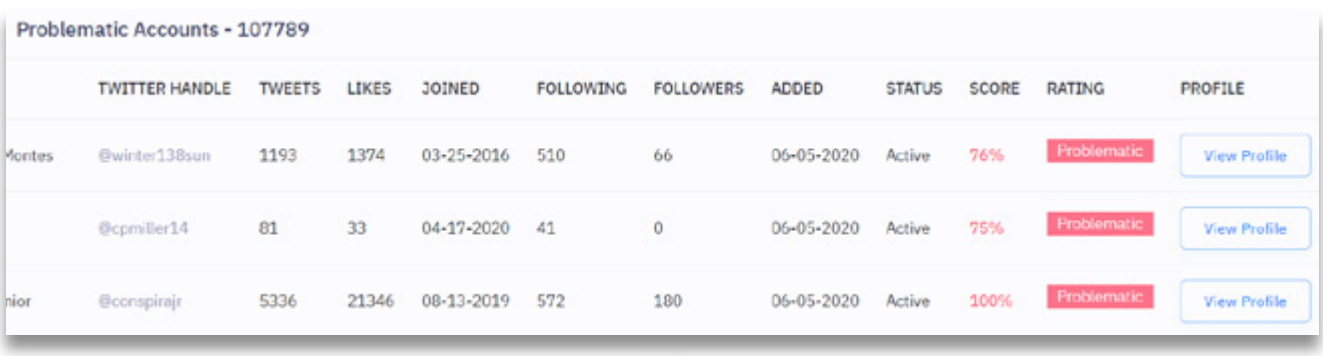
B. TRENDING TOPICS:

Monitoramento em tempo real de trending topics que estão sendo impulsionados por ação algorítmica, são eles: top hashtags, top two words phrases, top URLs e top mentions. Possibilita filtros para mês, dia, ano e hora, mas não para localidade.



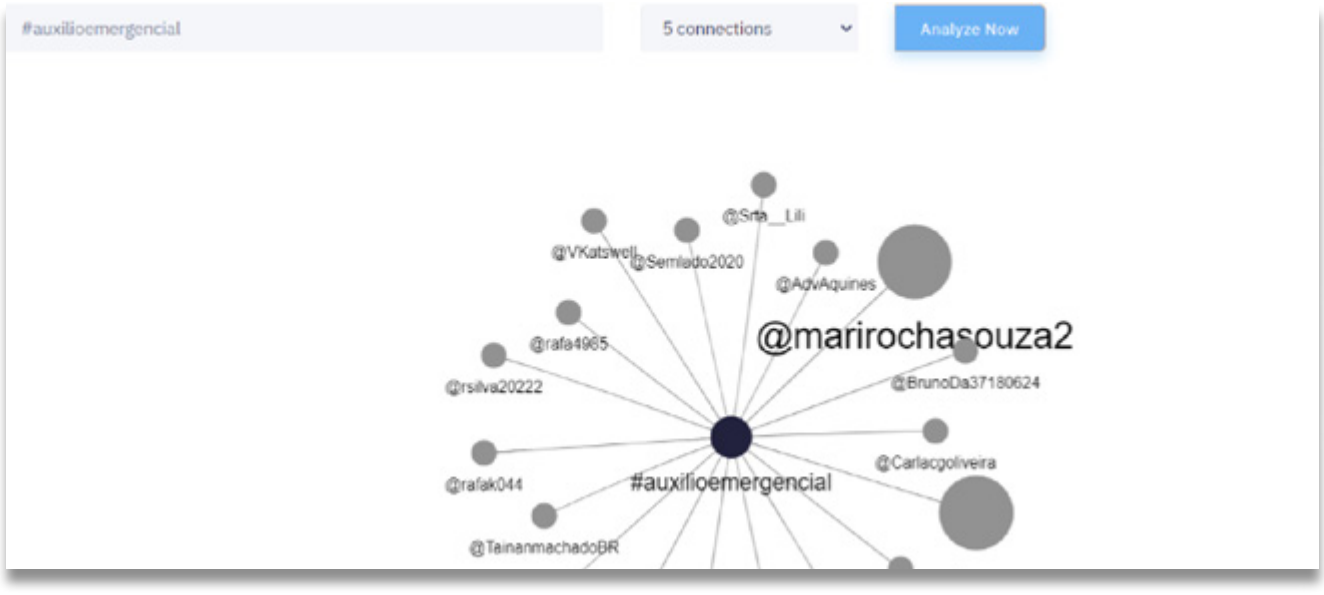
C. ANALYZED ACCOUNTS:

Banco de dados com armazenamento automático de todas as contas que foram analisadas pelo detector e resultaram em 75% ou mais de probabilidade de ser bot/trollbot. Inicialmente, armazena todas as contas, mas depois de um tempo exclui as com porcentagem inferior a 75%. Disponibiliza score contas e detalhamento de todos os perfis, incluindo número de seguidores, número de tweets da conta, data em que o perfil foi criado, hashtags, frases e URLs que mais foram twittadas por cada conta analisada e status (ativa ou inativa). Além disso, neste menu é possível ter acesso ao monitoramento constantemente das contas que são desativadas pelo Twitter.



D. ADVANCED TOOLS:

Análise em lotes a partir do link de um tweet que verifica automaticamente todas os perfis que interagiram com uma determinada postagem. Nesta aba, também é possível criar um grapho de distribuição de rede com perfis que twittaram uma hashtag ou marcaram um handle, sem, no entanto, filtro/critério de alcance ou relevância das contas.



4. COMO UTILIZAR:

PASSO 1:

Acesse o site http://botsentinel.com/

PASSO 2:

Clique no botão “Analyze Account” no canto superior direito e insira um handle (perfil) de uma conta do Twitter para receber como resultado o percentual de probabilidade desta conta ser um bot ou troll.

PASSO 3:

Percorra o menu lateral para ter acesso às demais funcionalidades da ferramenta.

PARA SABER COMO TIRAR O MÁXIMO PROVEITO DE CADA UMA DAS FUNCIONALIDADES DO BOT SENTINEL, ASSISTA AO WORKSHOP III, SOBRE FERRAMENTAS PARA DETECÇÃO DE AUTOMAÇÃO E DESINFORMAÇÃO.

BOTSLAYER

por Thayane Guimarães

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA BOTSLAYER. APROVEITE!

1. O QUE É

2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES

3. COMO INSTALAR

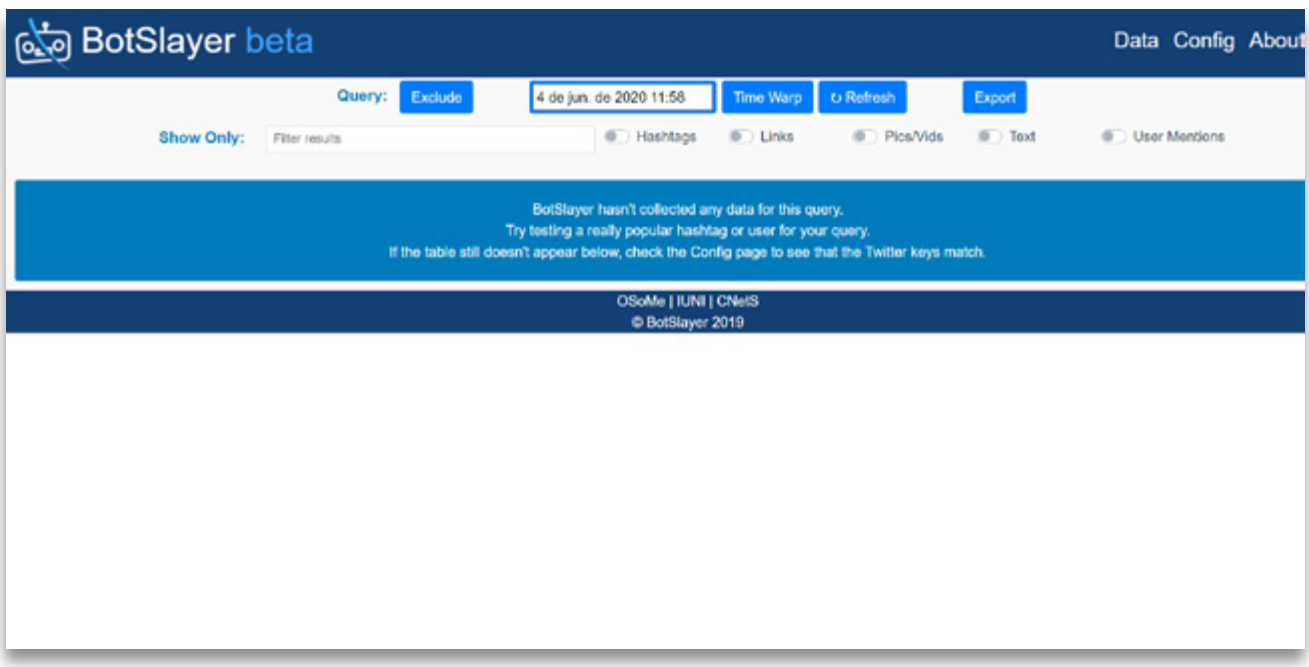
4. COMO UTILIZAR

1. O QUE É:

BotSlayer é uma ferramenta gratuita e desenvolvida pelo Observatório de Mídias Sociais da Universidade de Indiana (EUA) para investigar ações de ataques coordenados no Twitter, a partir do rastreamento e detecção de possíveis manipulações de informações no Twitter. O programa usa um algoritmo de detecção de anomalias e cria um índice para sinalizar hashtags, links, contas e mídias com alta probabilidade de terem sido impulsionadas na rede social de forma coordenada, com a ajuda de bots.

O BotSlayer possui integrações com o Botometer e o Hoaxy, outras ferramentas desenvolvidas previamente pelo mesmo Observatório de Indiana. O primeiro checa a atividade uma conta no Twitter e dá uma nota baseada na probabilidade do usuário em questão ser um robô, enquanto o Hoaxy permite visualizar como os fluxos de informação se espalham em redes de usuários.

O programa pode ser instalado tanto localmente, na máquina de cada usuário, como na nuvem. Porém, como seu objetivo maior é realizar análises em tempo real e 8 horas é o tempo mínimo de funcionamento para o melhor aproveitamento de suas métricas, é recomendável a instalação do software em um servidor. Um painel acessível pelo navegador permite que os usuários explorem os tweets e contas associados a campanhas suspeitas, visualizem sua propagação com o Hoaxy e pesquisem conteúdos relacionados na web.



2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES:

A investigação inicia a partir da definição de termos de buscas iniciais, que serão coletadas de forma contínua a partir do momento da configuração inicial. No entanto, o sistema não armazena mensagens retrospectivamente e a API do Twitter não retorna mais que 1% do volume total de mensagens na plataforma em um certo período.

Isto exige um cuidado na hora de escolher os termos de busca: se eles forem específicos o suficiente, você provavelmente conseguirá coletar todas as mensagens relativas àquele assunto. Já se forem demasiadamente genéricos, é possível que nem todos sejam coletados, por conta da limitação da API do Twitter.

Depois de coletadas as mensagens, o BotSlayer identifica as entidades envolvidas em cada uma delas. Entidades podem ser hashtags, links, imagens ou vídeos, usuários do Twitter e frases textuais. O funcionamento desta última em português ainda não é perfeito, pois o sistema remove automaticamente palavras e expressões comuns (“stopwords”) apenas em inglês, de modo que muitas frases textuais identificadas como entidades pelo BotSlayer são palavras comuns do nosso vocabulário.

Depois de extrair as entidades, o BotSlayer as exibe em um painel com as métricas abaixo para cada uma delas.:

A. TWEETS:

O número de tweets e retweets que correspondem à consulta inicial e contêm essa entidade nas últimas quatro horas;

B. ACCOUNTS:

O número de contas distintas que postaram mensagens que correspondem à consulta nas últimas quatro horas;

C. TRENDINESS:

Alteração relativa no número de tweets que correspondem à consulta e contêm essa entidade nas últimas quatro horas, em comparação com as quatro horas anteriores;

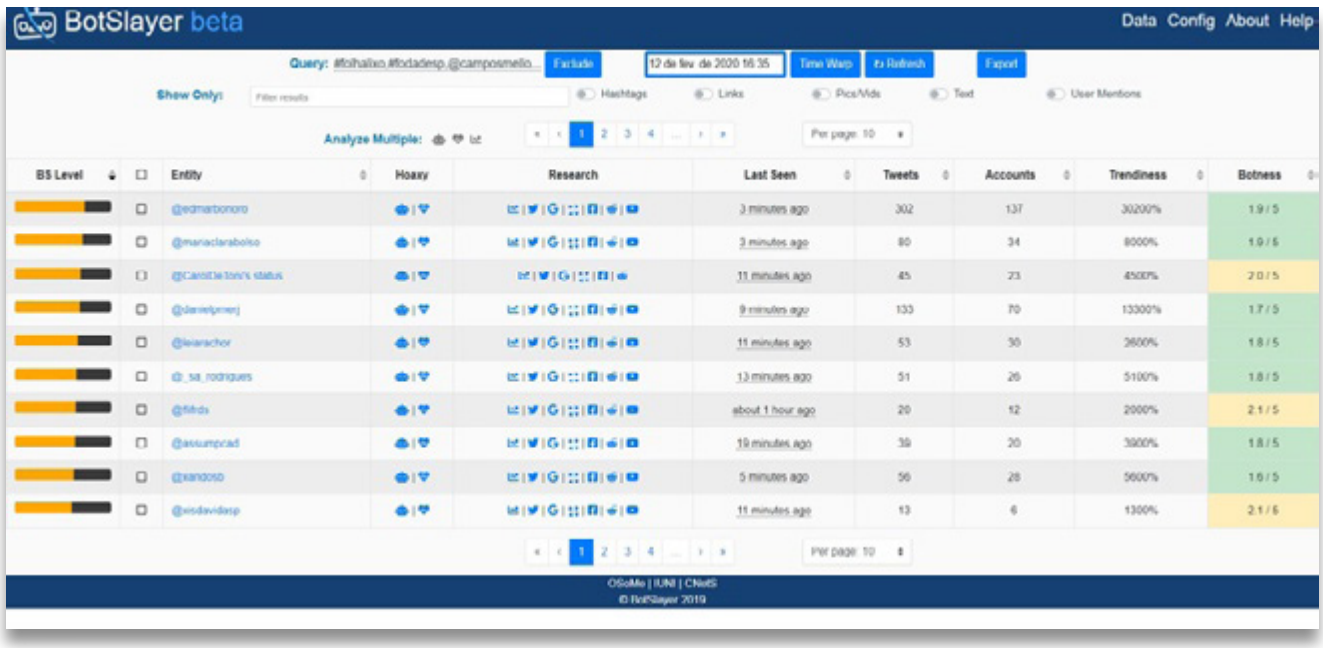
D. BOTNESS:

Média do índice que mede a probabilidade de dado usuário ser um bot, entre os tweets de que contêm essa entidade nas últimas quatro horas;

E. BS LEVEL:

Este índice, mencionado no início do texto, leva em consideração os números anteriores para chegar a uma nota entre 0 e 1. Quanto maior o índice, mais provável desta “entidade” ter a participação de robôs em sua propagação online. Ele é determinado de forma relativa, considerando cada conjunto de dados, e não através de uma escala absoluta. Por isso, a comparação do “BS Level” entre datasets diferentes não é recomendada. Segundo seus desenvolvedores, a definição do que é um BS Level alto deve ser feita caso a caso.

ATENÇÃO: Vale reforçar o fato de que o BotSlayer não coleta mensagens retrospectivamente. Ou seja, é preciso deixar o programa rodando por pelo menos 8h sem interrupções para levar em conta o índice de Trendiness, por exemplo. Todos estes dados podem ser exportados para o formato CSV diretamente do painel web do programa.



3. PASSOS PARA INSTALAÇÃO:

Primeiro, para usar o BotSlayer é preciso preencher este formulário. Você também deve estar conectado a uma conta do Google para verificar sua identidade e concordar com o EULA (End User License Agreement). Você receberá os detalhes necessários para seguir as instruções de instalação abaixo no texto. Anote a “Secret string”, a “URL”, e a “Password” que serão geradas após preencher o formulário: você precisará delas para fazer o download. Confira as diferentes instruções de instalação:

3.1. PARA USUÁRIOS DOCKER

O BotSlayer pode ser instalado em qualquer computador por meio de uma imagem pré-construída no Docker. Para instalá-lo na sua máquina, siga as instruções no site do Docker.

Depois de solicitar o software e concordar com os termos de uso, você deverá receber um URL vinculado a uma imagem do Docker e uma senha. Faça o download do arquivo de imagem. Você precisará inserir um nome de usuário (botslayer) e a senha fornecida.

Você também pode usar o seguinte comando para baixar a imagem do Docker diretamente do terminal (substitua *url2image* pelo URL que você recebeu):

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

Em seguida, execute no terminal os seguintes comandos para carregar a imagem baixada e execute o contêiner do Docker. Substitua o nome do arquivo pelo nome do arquivo baixado.

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

O último comando mapeia portas que fornecem funcionalidades diferentes. As interfaces estão disponíveis no “localhost” ou no endereço IP do seu servidor. O painel do BotSlayer está na porta 5000. A interface com os log é exposta na porta 9001, transmitindo arquivos de dentro do contêiner sobre o funcionamento do sistema.

Para um acesso mais fácil ao painel na porta HTTP padrão (80), você pode (1) configurar um proxy reverso da porta 5000 à porta 80 ou (2) usar o sudo para forçar a porta 5000 do mapa à porta 80 ao executar o docker recipiente.

Se o computador reiniciar por qualquer motivo, você precisará reiniciar o contêiner BotSlayer no Docker. Uma solução alternativa é configurar algum gerenciador de processos, como o supervisord.

Se você quiser ver um exemplo de código de configuração em ambiente EC2, que inclui a instalação do Docker, a instalação do proxy reverso no nginx e a configuração da supervisão, consulte esta página (em inglês) para obter as etapas da instalação.

3.2. COM O USO DO AMAZON WEB SERVICES

O BotSlayer usa o Amazon Web Services (AWS) por meio de uma Amazon Machine Image (AMI) para otimizar o processo de instalação para usuários não técnicos.

ETAPA 1:

Acesse à AWS. Se você não possui uma conta, precisará criar uma. Isso é gratuito, mas requer um cartão de crédito para cadastro. ATENÇÃO: Você pode selecionar o nível gratuito depois quando escolher seu plano, mas o cadastro deve cobrar US$ 1.

Faça o login no console. No AWS Management Console (Console de gerenciamento da AWS), clique em “Serviços AWS”, depois você irá ver o menu “Computação” e clique em “EC2”.

ETAPA 2:

Clique no botão para iniciar uma instância do EC2. Clique em “Launch instance”.

ETAPA 3:

Depois de solicitar o software e concordar com o EULA, você deverá receber instruções que incluem uma longa cadeia secreta como “0e ... f2”. É o item “Secret string” que você recebeu após preencher o formulário do BotSlayer.

Copie isso isso na caixa de pesquisa na parte superior (aparece como ‘Search for AMI by entering a search term”). Clique na guia “Community AMIs”.

Selecione o resultado em AMIs da comunidade. Se a pesquisa não retornar nada, defina sua região de serviço da AWS como Ohio no canto superior direito da página e pesquise novamente.

ETAPA 4:

Selecione a imagem correta. Deve ser a imagem de um pinguim (o símbolo do Linux). Pressione Select.

ETAPA 5:

Na nova tela (Choose an Instance Type) você pode selecionar o tipo de instância marcado como “nível gratuito qualificado” (Free tier eligible).

Como alternativa, você pode selecionar o “t2.xlarge”, recomendado pelo Observatório de Mídias Sociais, mas não gratuito; pode custar cerca de US$ 0,20/hora. Clique em “Configurar detalhes da instância” (Next:Configure Instance Details) no canto inferior direito para continuar. A Abraji usou a versão gratuita.

ETAPA 6:

Use as configurações padrão na página “Configurar detalhes da instância” (Configure Instance Details) e clique diretamente em “Adicionar armazenamento” (Next: Add Storage) na parte inferior direita para prosseguir.

ETAPA 7:

Escolha o tamanho do seu disco rígido. Você pode selecionar até 30 GB para o nível gratuito; o Observatório de Mídias Sociais recomenda 100 GB ou mais para manter os dados além de vários dias, dependendo da quantidade de informações que você rastrear. Clique em “Adicionar tags” (Next: Add Tags) no canto inferior direito para continuar.

ETAPA 8:

Use as configurações padrão na página “Adicionar tags” e clique diretamente em “Configurar grupo de segurança” (Next: Configure Security Group) para continuar.

ETAPA 9:

Adicione duas regras para abrir as portas exigidas pelo BotSlayer.

Clique em Add Rule – escolha “HTTP” em Type – “TCP” em Protocol – “80” em Port Range – “Custom” e “0.0.0.0/0, ::/0” em Source

Clique mais uma vez em Add Rule – escolha “Custom TCP Rule” em Type – “TCP” em Protocol – “9001” em Port Range – “Custom” e “0.0.0.0/0, ::/0” em Source

Clique em “Revisar e iniciar” (Review and Launch) no canto inferior direito para continuar.

ETAPA 10:

Revise cuidadosamente a configuração da máquina. Se você encontrar algum erro, poderá voltar para corrigi-lo. Caso contrário, clique em “Iniciar” (Launch) no canto inferior direito para continuar.

ETAPA 11:

Crie um novo par de chaves (Create a new key pair) e atribua um nome significativo, como “procura_bot_brasil” ou outro de sua preferência. Este par de chaves é necessário para acessar a máquina EC2. Faça o download do par de chaves (Download Key Pair) e mantenha-o em um ambiente seguro. Em seguida, inicie a instância (Launch Instances).

ETAPA 12:

Você terminou de configurar o BotSlayer, então clique no link da instância para ir para a página principal.

ETAPA 13:

Clique no link após a frase: “The following instance launches have been initiated:”.

Copie o nome do domínio ou o endereço IP e cole-o no seu navegador para acessar a interface web do BotSlayer. Em Instance State deve aparecer “running”.

Você pode encontrar o endereço em “IPv4 Public IP”. Algo como “18.XXX.XXX.XX”, sendo que no lugar dos Xs existirão números. Aguarde 5 minutos para que a máquina tenha tempo suficiente para iniciar o BotSlayer.

Marque o endereço IP como favorito, pois é assim que você acessará o painel do BotSlayer. Nota: se você reiniciar a instância do EC2, o endereço IP será alterado. Para atribuir um endereço IP estático, você pode usar um Endereço IP Elástico (não gratuito).

CONFIGURANDO O BOTSLAYER

Depois de instalar o BotSlayer e acessar o painel da Web, clique em “Config” no menu, digite a senha de sua escolha e forneça as chaves do aplicativo de desenvolvedor do Twitter e uma consulta permanente (veja abaixo mais detalhes em “Seu primeiro raspador”). Consulte a página de Ajuda (Help) para obter mais instruções, dicas sobre as chaves do Twitter e o formato da consulta.

ATENÇÃO: O painel é acessível via Web usando o endereço IP do servidor. Caso você esteja utilizando um servidor na nuvem, não compartilhe a URL com alguém de fora da sua organização ou pessoas em que você não confia. Eles podem fazer alterações no sistema ou acessar dados em violação dos termos de serviço do Twitter. Para evitar possíveis problemas de segurança e violação de termos, o BotSlayer bloqueia a indexação do mecanismo de pesquisa por padrão.

Coloque no browser o endereço do BotSlayer que você pegou no seu “IPv4 Public IP”. Clique em Config. É o momento que você escolhe uma senha para seu BotSlayer e depois clique em Change Password. E depois é preciso se logar com a senha que acabou de escolher.

INSERINDO CHAVES DA API DO TWITTER

Agora, chega o momento em que você precisa colocar suas identificações de desenvolvedor no Twitter para continuar. Para conseguir essas chaves você deve ir até o site desta rede social e se logar com seu usuário e senha no Twitter.

Clique no botão “Apps” e na próxima tela “Create an App”. Se for a primeira vez, você pode ter que preencher um questionário longo sobre os motivos do app e seus dados básicos.

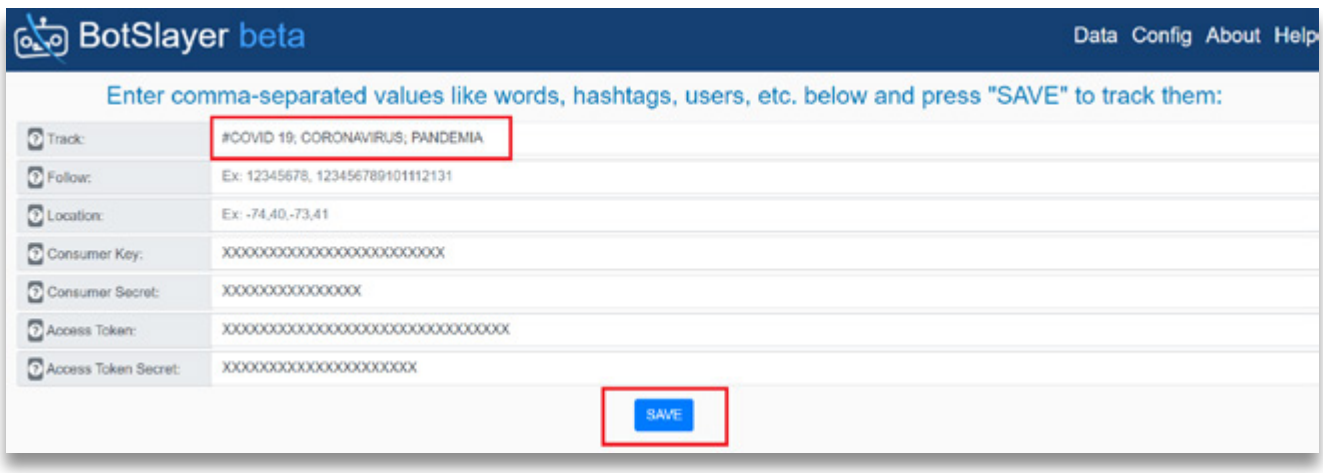
Após isso você precisa colocar em “App details” o “App name”, depois a descrição em “Application description”, o “Website URL” e “Callback URLs” do seu projeto (por exemplo, no nosso caso, http://www.abraji.org.br), e escrever “Diga-nos como este aplicativo será usado” (Tell us how this app will be used).O Twitter pode levar algum tempo para aprovar o App depois disso.

Uma vez criado, vá até a aba Key and tokens. Clique nos dois botões Regenerate. Na tela que abre clique Copy para Access token, dê Ctrl+C no bloco de notas, depois Copy para Access token secret e dê Ctrl+C no bloco de notas. E também copie os valores de API key. Guarde estas chaves.

De volta à tela do BotSlayer, copie em Consumer Key o conteúdo de API key, depois em Consumer Secret copie API secret key, depois em Access Token copie o valor de Access token e, por fim, em Access Token Secret o valor de Access token secret. Clique em “Save”.

4. COMO UTILIZAR:

Agora, no campo “Track” você pode escolher o que deseja vasculhar: palavras, nomes, hashtags, usuários do Twitter e até localizações.



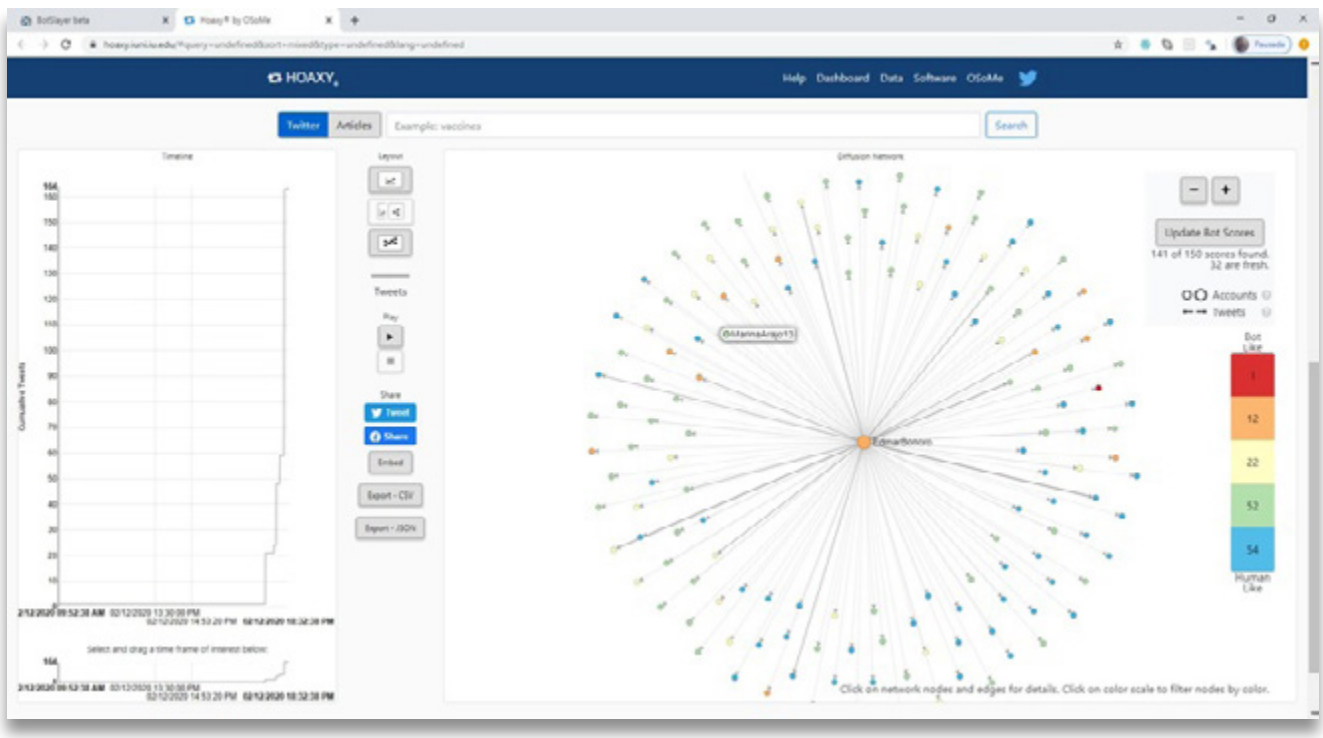
Clique em Save de novo para salvar os parâmetros de buscas. Também é possível escolher itens em Follow (delimitar usuários específicos para seguir) e Location (locais dos tweets). Depois clique em Data e aguarde um pouco.

O BotSlayer começará a coletar mensagens deste momento. Depois de algum tempo, aperte Refresh para ver os resultados e as métricas da ferramenta.

Além de conferir as métricas comentadas acima, também é possível alterar as datas de busca em “Time Warp” e filtrar a tabela apenas por termos específicos. Também podem ser criadas visualizações dos dados com outro projeto do Observatório de Mídias Sociais, o Hoaxy. Por fim, na aba “Research” é possível ver timeline dos dados e os resultados das buscas encontrados no Twitter, Google, 4chan, Facebook, Reddit e YouTube.

No momento, não é possível obter mais informações sobre a quantidade total de mensagens coletadas ou ter acesso aos conteúdos baixados através da interface gráfica. Para isso, é preciso acessar o banco de dados, que provê os dados para o BotSlayer. Em um ambiente Docker, isto pode ser feito através do comando abaixo:

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



PARA MAIS INFORMAÇÕES SOBRE A ARQUITETURA DE SOFTWARE DO BOTSLAYER, CONSULTE ESTA PÁGINA NO GITHUB.

TWITONOMY

por Thayane Guimarães

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA TWITONOMY. BOA LEITURA!

1. O QUE É

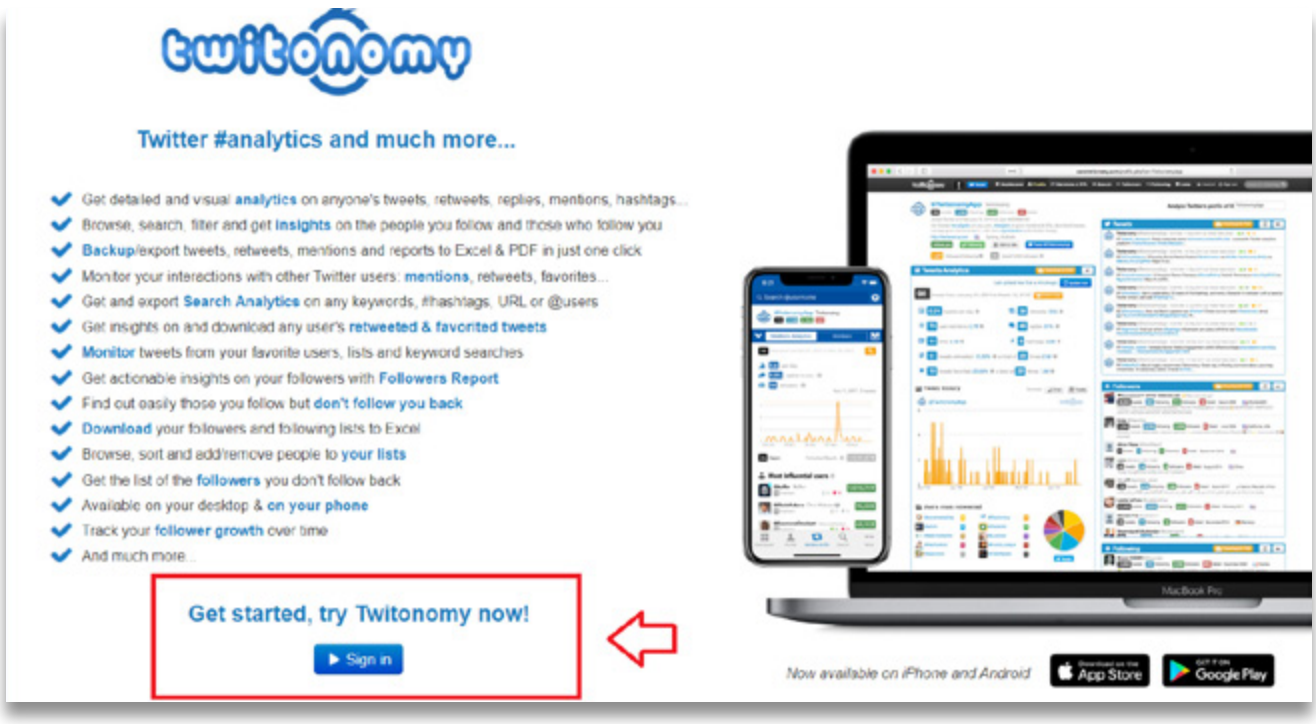
2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES

3. COMO UTILIZAR

1. O QUE É:

Twitonomy é uma poderosa ferramenta para analisar inúmeros dados do Twitter, produzida por @MattFyot. O serviço é totalmente gratuito e permite realizar o monitoramento minucioso das atividades que ocorrem no Twitter, contribuindo, assim, para qualquer investigação política na plataforma.

Ele permite, por exemplo, monitorar em tempo real hashtags, usuários e criar listas com conjuntos de usuários para atualização constante de suas atividades, incluindo aquelas realizadas em datas retroativas. Na versão premium, permite monitoramento com base nos perfis mais influentes, perfis mais engajados e perfis mais ativos, além de procurar por top hashtags mais relacionadas ao assunto monitorado. A versão premium possibilita fazer download em csv ou pdf de todas as infos. Veja abaixo, em detalhes.



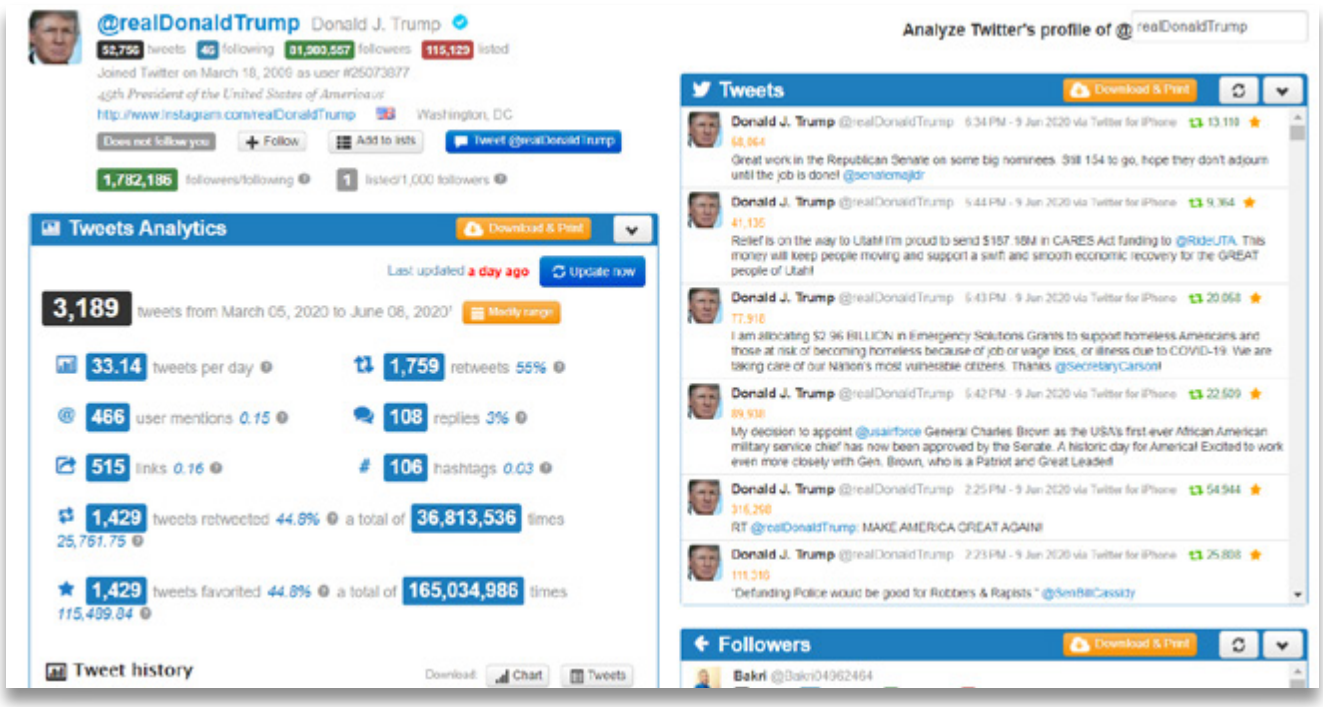
2. QUAIS SÃO AS FUNCIONALIDADES EXISTENTES:

A ferramenta Twitonomy é focada em metrificação de um perfil no Twitter, com funcionalidades que vão desde a identificação de seguidores com a maior capacidade de influenciar outras pessoas, até métricas minuciosas sobre quem são os perfis mais engajados com o seu conteúdo e quais tweets da sua conta que tiveram mais repercussão na rede. No entanto, a plataforma possui, ainda, diversas capacidades que auxiliam no monitoramento das atividades do Twitter e, desta forma, contribuem com análise de dados e construção de estratégias de enfrentamento à desinformação. Veja algumas delas:

A. ANALYZE TWITTER'S PROFILE:

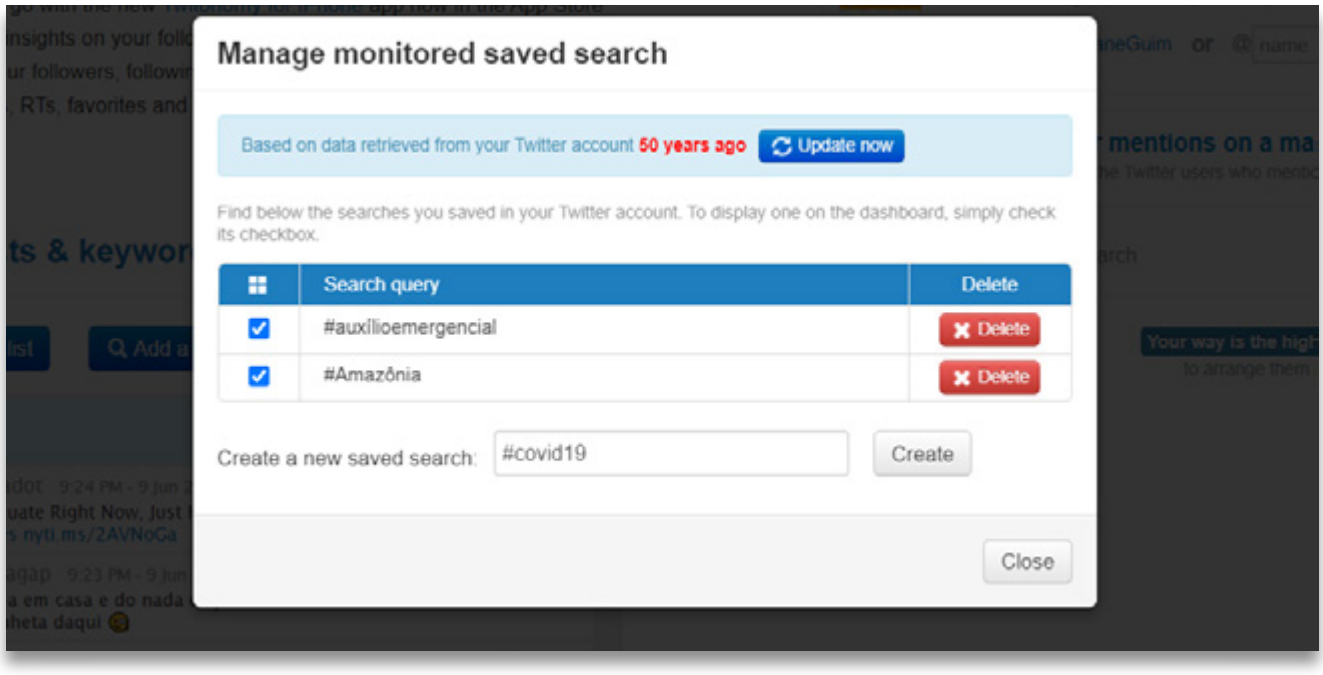
Possibilita o monitoramento de uma conta específica do Twitter, incluindo postagens que tiveram maior alcance e relevância, lista de seguidores, perfis que segue, hashtags

mais utilizadas e informações como em quais dias da semana e horas do dia acontecem as atividades do perfil analisado.



B. MONITOR USERS, LISTS AND KEYWORDS:

Permite escolher usuários, listas ou qualquer palavra-chave (termos, hashtags etc) para monitorar. O twitonomy, então, atualiza automaticamente os quadros de monitoramento conforme seus interesses e permite, ainda, fazer o download em arquivo .csv de todos os dados.



C. LISTS:

Permite, por exemplo, criar uma lista com todos os usuários que twittaram uma dada hashtag e exportar em arquivo .csv, sem precisar acessar a API do Twitter e utilizar códigos para raspagem de dados para realizar a tarefa.

D. SEARCH:

Possibilita dados diversos sobre atividades no Twitter relacionados a um termo de busca específico, incluindo quais contas estão falando sobre aquele tema, quais perfis são mais influentes, quais tweets tiveram maior repercussão, em quais dias e horários o termo estava em alta, quais são as principais hashtags relacionadas ao seu termo e quais países o termo teve maior repercussão. Essa funcionalidade, no entanto, está disponível apenas na versão premium da ferramenta.

E. MENÇÕES E ALCANCE POTENCIAL:

Possibilita não apenas identificar a quantidade de menções ao seu perfil, mas também frequência de menções diárias, número total de usuários que mencionaram a página que está sendo analisada, retweets das menções e alcance potencial de tweets, com base no número de seguidores de cada usuário.

3. COMO UTILIZAR:

O Twitonomy não necessita de instalação, por isso, para começar a utilizar a ferramenta, basta seguir os passos adiante:

PASSO 1:

Faça o login em uma conta do Twitter, seja a sua pessoal ou o perfil da sua organização.

PASSO 2:

Acesse o site www.twitonomy.com

PASSO 3:

Clique no botão “Sign In”

PASSO 4:

Já dentro do Twitonomy, clique no botão “Sign in with Twitter” para que a plataforma tenha acesso aos dados do Twitter a partir da sua conta

PASSO 5:

Percorra o menu superior para conhecer e testar as funcionalidades da plataforma que foram apresentadas aqui neste tutorial.

TINEYE

por Redson Fernando

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA TINEYE. APROVEITE!

1. O QUE É:

O TinEye é um mecanismo de busca reversa de imagens desenvolvido pela empresa Idée, Inc., sediada em Toronto, no Canadá. A busca reversa é especialmente interessante para aqueles que já possuem uma imagem em mãos e querem encontrar outras imagens relacionadas ou então que pretendem descobrir a origem de uma imagem para obter mais informações sobre ela, por exemplo. O TinEye cria uma impressão digital única e compacta da imagem pesquisada utilizando aprendizado de máquina e inteligência artificial e compara ela com todas as outras imagens indexadas na plataforma para encontrar correspondências.

2. QUAIS SÃO AS FUNCIONALIDADES:

A. MECANISMO DE BUSCA:

O TinEye realiza a busca de cópias exatas e alteradas das imagens que você pesquisou na plataforma, incluindo aquelas que foram cortadas, com cores modificadas, redimensionadas ou rotacionadas, por exemplo. Assim, a ferramenta possui diversas aplicações, como descobrir se a imagem está sendo utilizada por terceiros, se existem versões modificadas dela e onde estão, além de descobrir a origem das imagens para obter mais informações ou para encontrar versões de alta resolução. É importante ressaltar que o TinEye normalmente não reconhece o conteúdo das imagens. Ou seja, ele não pode ser utilizado para encontrar imagens diferentes com as mesmas pessoas ou objetos, por exemplo. Além disso, é importante destacar que sua pesquisa no TinEye nunca é salva ou indexada sem a sua permissão. Esse processo é realizado a partir da própria API da plataforma, que pesquisa e adiciona automaticamente as imagens no motor de busca.

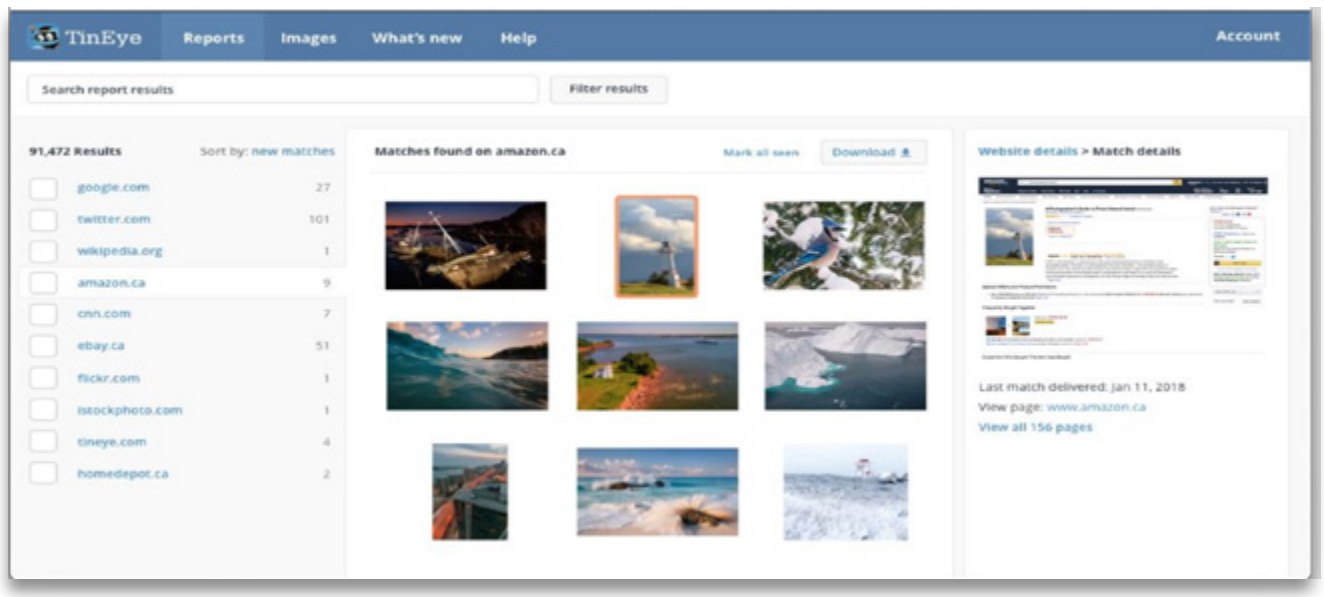
O TinEye é gratuito para uso por meio de sua interface da Web e permite que o usuário realize até 100 pesquisas por dia, com um máximo de 300 pesquisas por semana. Ele também oferece uma versão paga para uso comercial, possuindo pacotes pré-pagos que possibilitam mais pesquisas, além de incluírem uma interface para facilitar a pesquisa manual e o acesso à API para pesquisas automatizadas mais avançadas.

B. EXTENSÃO PARA NAVEGADORES:

O TinEye também possui uma extensão para os navegadores Google Chrome, Opera e Firefox que permite a busca de qualquer imagem a partir de seus próprios sites de origem, sem a necessidade de baixar a imagem ou copiar sua URL para depois enviar na plataforma. A funcionalidade fica disponível ao clicar com o botão direito do mouse em cima da imagem desejada.

C. TINEYE ALERTS:

Essa funcionalidade permite que você carregue todas as imagens que deseja rastrear e diariamente a plataforma irá rastrear a web buscando correspondências, avisando você quando elas forem indexadas pela API, além de também fornecer relatórios indicando exatamente onde suas imagens aparecem. A funcionalidade TinEye Alerts é paga e funciona por meio de pacotes pré-pagos. É possível solicitar uma demonstração do serviço.



3. COMO ACESSAR:

A. VERSÃO WEB:

O TinEye é uma ferramenta que não necessita qualquer tipo de download ou instalação. Basta acessar o endereço https://tineye.com/ pelo seu navegador web. Caso você possua a versão comercial, faça login em https://tineye.com/service_select.

B. EXTENSÃO:

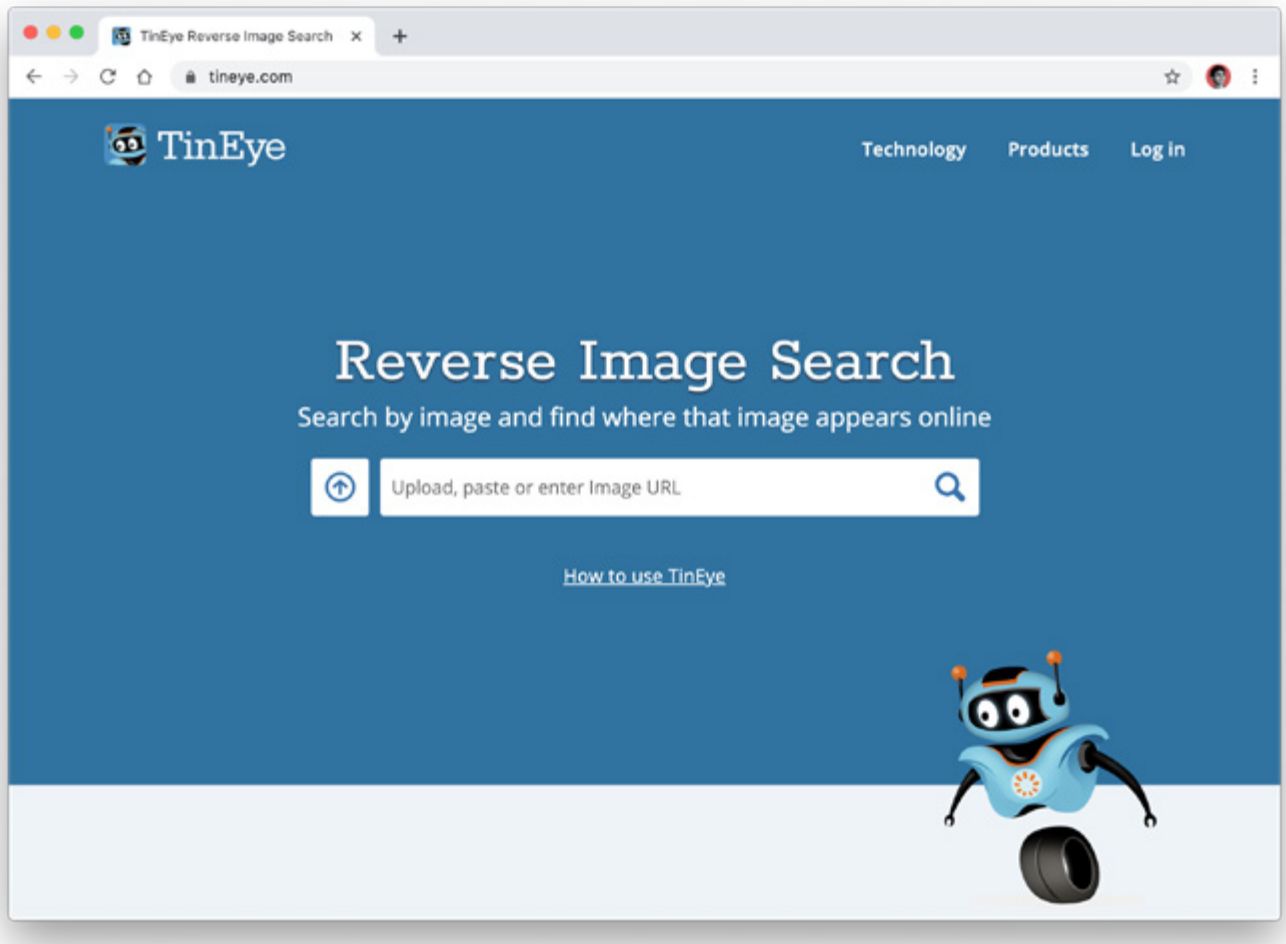
Caso queira, você poderá utilizar a extensão gratuita para os navegadores Google Chrome e Mozilla Firefox acessando suas respectivas lojas de extensão. Entretanto, para utilizar no navegador Opera, será necessário primeiro instalar a ferramenta "Install Chrome Extensions" e a própria extensão para o Chrome. Assim, você poderá importar ela do Chrome para seu navegador Opera.

4. COMO UTILIZAR:

PASSO 1:

Após acessar o endereço da ferramenta (https://tineye.com/), a primeira etapa é realizar a busca da sua imagem. Você pode fazer upload de uma imagem, colar uma imagem ou apontar para uma imagem da Web digitando ou colando uma URL (link). Você também pode usar o recurso "Arrastar e Soltar". Isso permite que você arraste uma imagem, passe o mouse sobre a guia na qual o TinEye está aberto e soltar na página para fazer a pesquisa.

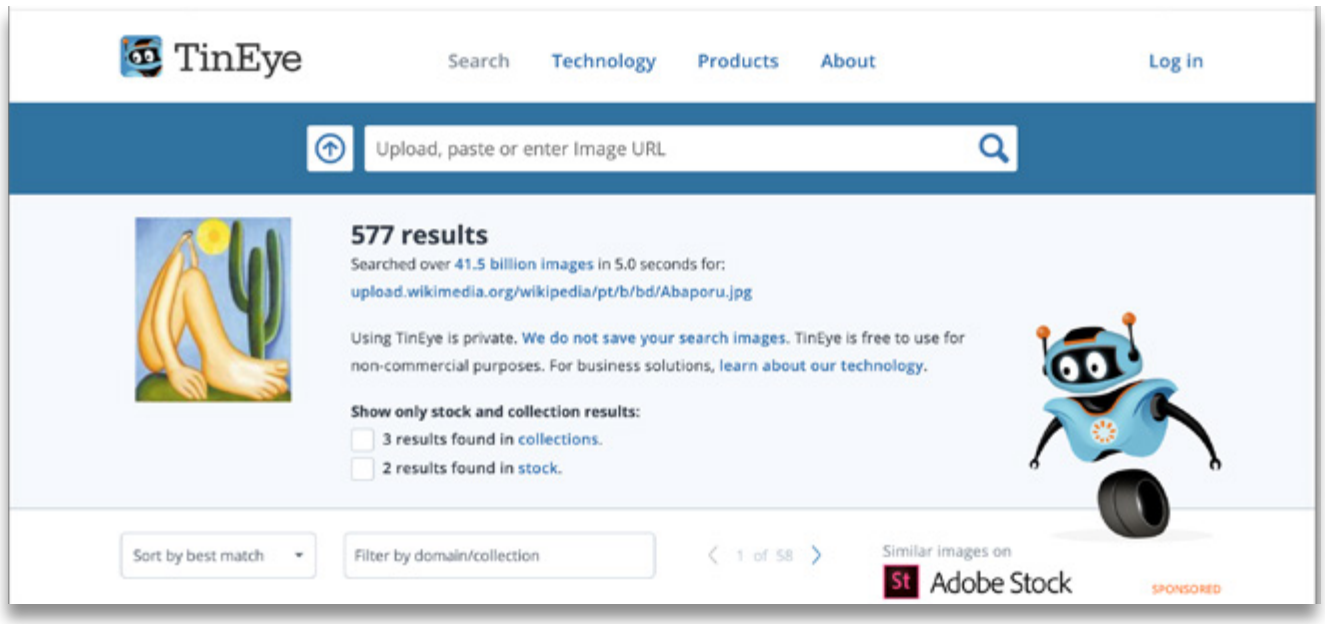
Caso você queira utilizar a extensão, após seguir as etapas de download descritas em "como acessar", basta clicar com o botão direito do mouse e selecionar a opção "Search Image on TinEye". A pesquisa irá abrir por padrão em uma nova guia.



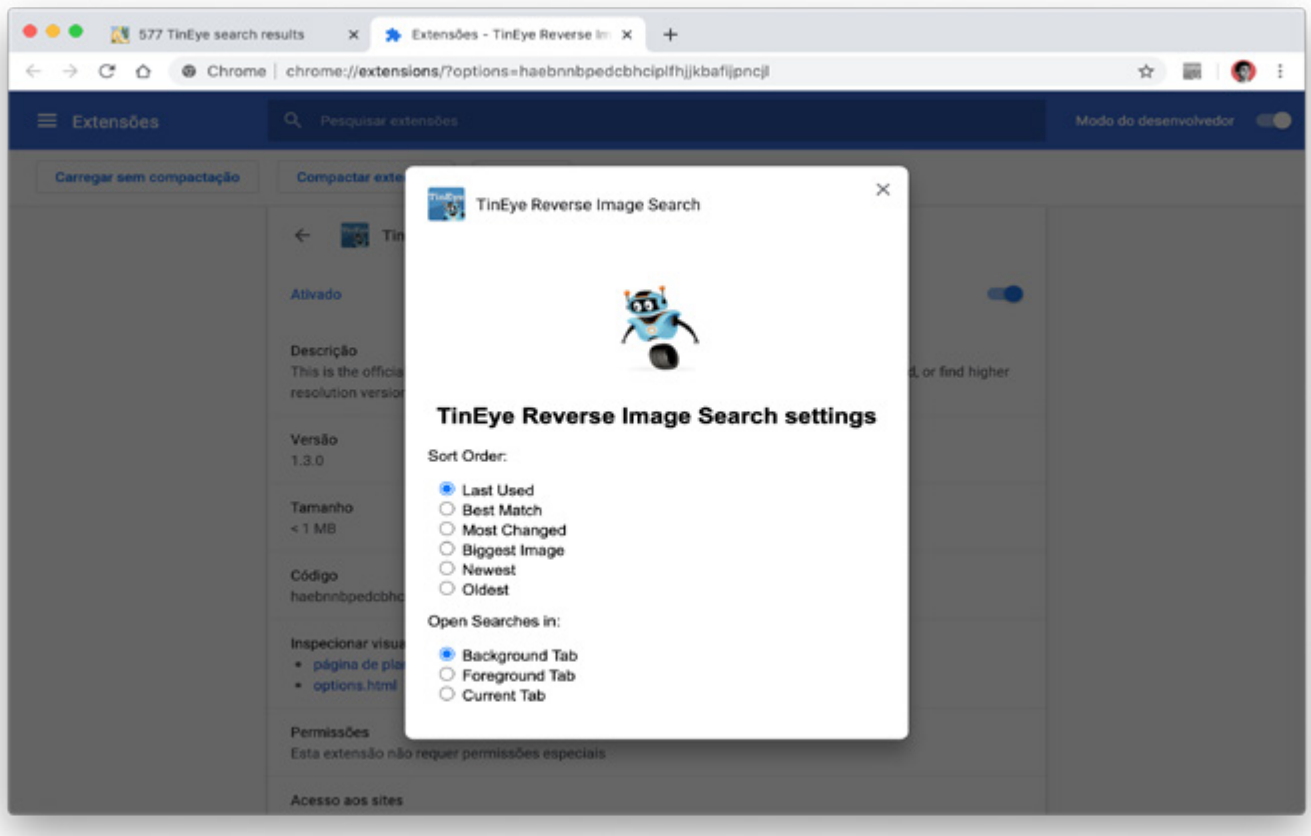
RECOMENDAÇÕES: O TineEye exibe resultados mais exatos utilizando imagens com pelo menos 300 pixels em qualquer dimensão e sem marcas d'água. Além disso, é válido ressaltar também que o upload de imagens possui algumas limitações, como, por exemplo, um máximo de 20 megabytes por arquivo e um mínimo de 100 pixels em qualquer dimensão da imagem para realizar a pesquisa.

PASSO 2:

Após buscar a imagem, você será redirecionado para a página de resultados. Por padrão, eles são classificados por "melhor correspondência". Entretanto, você também pode classificar pelo tamanho da imagem, pela data que a API do TinEye indexou a imagem na ferramenta ou pela quantidade de alterações que ela sofreu. Para isso, clique em "Short By..." e selecione a classificação desejada. É importante entender também que a data em que o TinEye rastreou uma imagem não é necessariamente a data na qual ela apareceu pela primeira vez em alguma pagina na web. Além disso, também é possível filtrar por domínio ou coleção de imagens stock, clicando em "Filter By...".

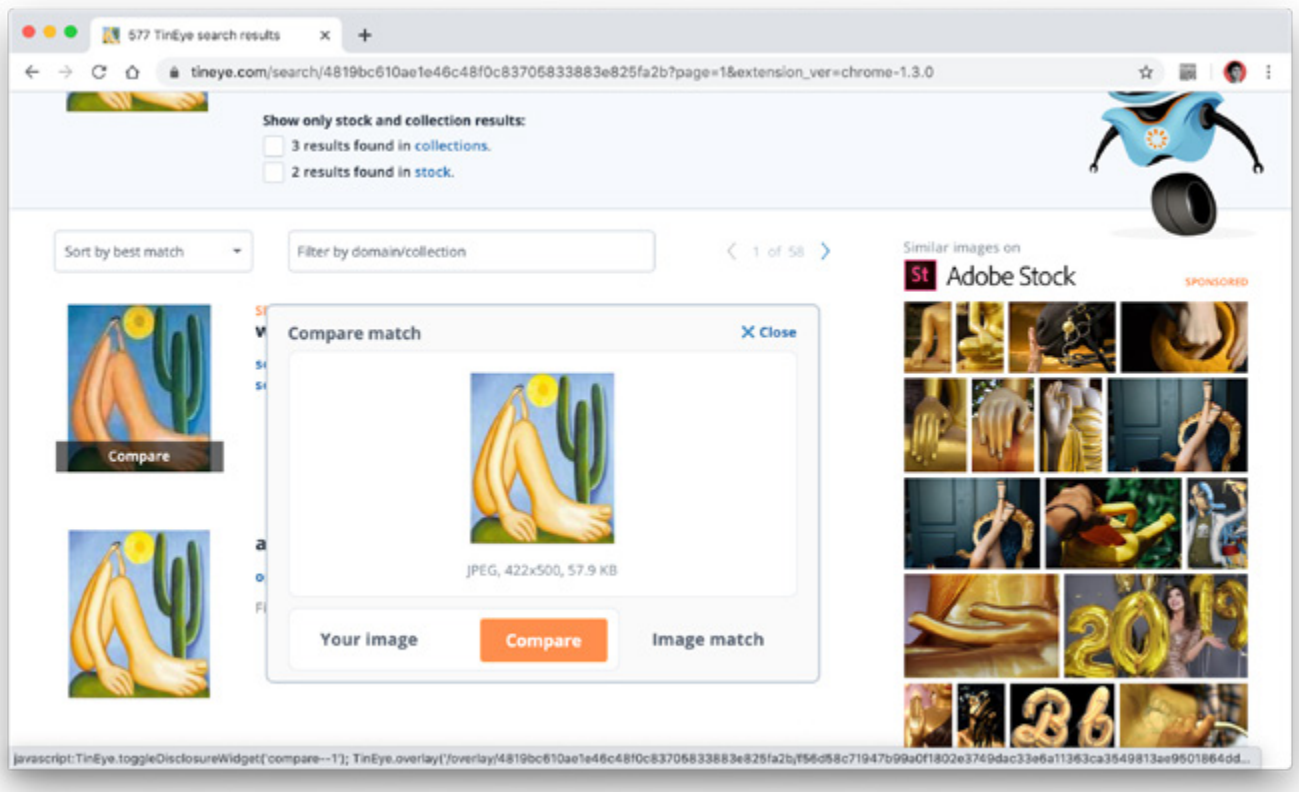


As configurações de extensão do TinEye também oferecem opções para selecionar a ordem de classificação, além de poder escolher se os resultados da pesquisa devem ser abertos em uma nova guia em segundo plano, em primeiro plano ou na guia atual. Para isso, clique com o botão direito no ícone da extensão, depois clique em ‘’opções” e altere as propriedades desejadas.



PASSO 3:

Depois, é possível utilizar o recurso TinEye Compare, que permite alternar rapidamente entre a pesquisa e a imagem do resultado. Assim, é possível perceber melhor as diferenças entre as duas imagens, principalmente se elas forem manipuladas de alguma forma. Para isso, selecione a imagem na lista e alterne entre as visualizações.



VIEWDNS

por Diego Cerqueira

EQUIPE DE DEMOCRACIA E TECNOLOGIA:

Debora Albu

Diego Cerqueira

Redson Fernando

Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA VIEWDNS. APROVEITE!

1. O QUE É:

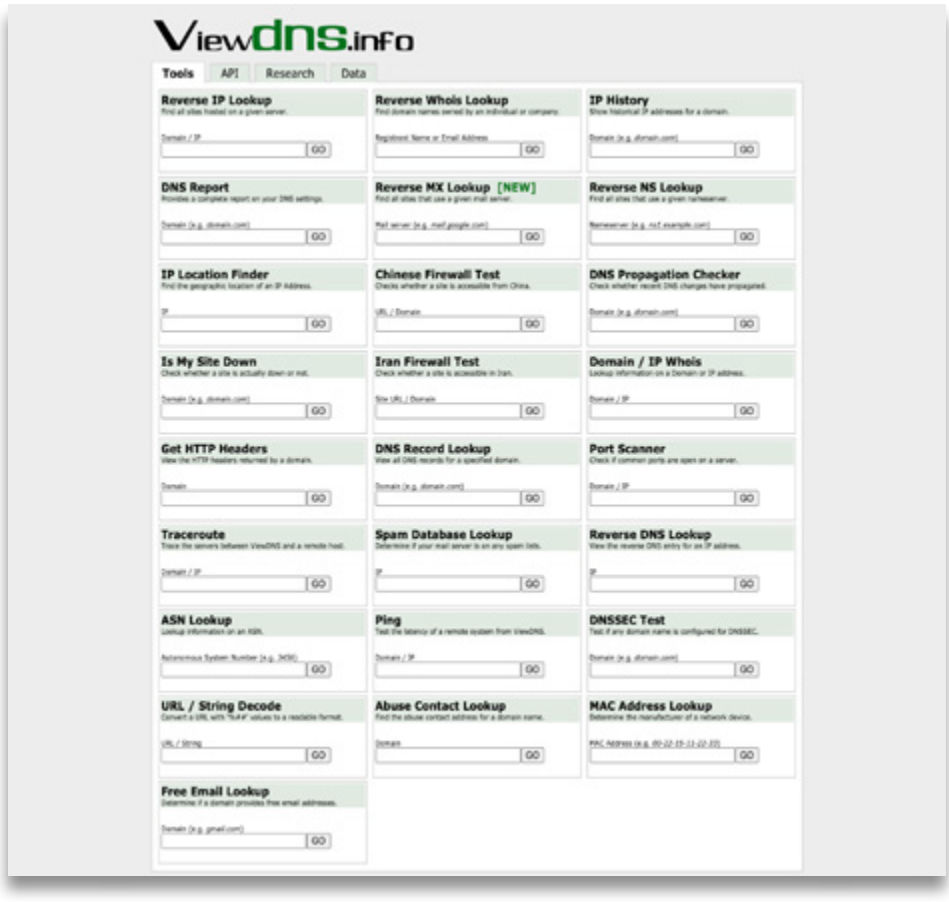
ViewDNS é uma ferramenta web que auxilia no processo de investigação de sites e domínios de internet, principalmente relacionadas ao DNS e outros detalhes técnicos de cada domínio, que incluem suas informações, mas não limitadas ao DNS.

O ViewDNS possui um diversas de ferramentas para explorar especificações técnicas. Por meio de uma interface única e simplificada, você será capaz de obter diversas informações para seu processo de investigação sobre sobre um domínio de internet.

Todas informações obtidas pelo site são abertas e disponíveis na internet, fornecidas pelos próprios donos de domínio ao registrar seus nomes de domínio através de intermediários. O ViewDNS possui um banco de dados próprio dessas informações e mantém registros de milhões de domínios ao redor do mundo.

Importante!

Serviço de Nomes de Domínio (DNS, em inglês) é um dos pilares da web, pois é responsável por traduzir endereços de IP (Internet Protocol Address), um conjunto de quatro dígitos associado a serviços disponível na internet, oferecendo a capacidade de traduzir esses endereços numéricos em formato textual, trazendo maior facilidade para memorização.



2. QUAIS SÃO AS FUNCIONALIDADES:

Diversas funcionalidades do ViewDNS podem e devem ser utilizadas em conjunto. Pense nas ferramentas apresentadas neste tutorial como um kit de ferramentas. A utilização de algumas delas disponíveis no site requer algum conhecimento sobre Redes de Computadores e conceitos básicos sobre Protocolos de Internet e suas tecnologias, porém as ferramentas apresentadas abaixo podem ser utilizadas sem nenhum prejuízo.

A. BUSCA DE INFORMAÇÕES DE DOMÍNIO (DOMAIN / IP WHOIS):

Mostra informações sobre o contratante do domínio, se o domínio está registrado ou não e suas informações de contato.

B. BUSCA REVERSA WHOIS (REVERSE WHOIS LOOKUP):

“Quem é”, em sua tradução literal, Whois é uma ferramenta para recuperar informações públicas sobre um nome de domínio. Através da busca reversa (Reverse Lookup) com um nome de domínio, exemplo itsrio.org, você poderá buscar todos os domínios registrados por um indivíduo ou empresa. As buscas podem ser realizadas através de dois parâmetros: Nome do indivíduo ou empresa ou por um e-mail.

C. BUSCA DE DNS (DNS RECORD LOOKUP):

Você poderá visualizar todas configurações de registro (A, MX, CNAME) associadas ao domínio pesquisado. Para entender mais sobre os tipos de registro acesse: www.nerion.es/soporte/aprende-como-funcionan-los-registros-dns/

D. HISTÓRICO DE IP (IP HISTORY):

Exibe uma lista de IP’s associados ao site/serviço buscado, revelando informações relevantes sobre a localização de onde esse serviço se encontra hospedado e informações sobre o dono do endereço de IP.

3. COMO ACESSAR:

Para acessar as ferramentas disponíveis pelo ViewDNS, digite ou cole em seu navegador de preferência o endereço https://viewdns.info/

4. COMO UTILIZAR:

Para utilizar a busca de informações sobre um domínio é preciso ter em mãos o nome do domínio. Abaixo um exemplo de como identificar um nome de domínio.

Site	Domínio
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 o domínio é uma tarefa simples. Basta observar no endereço (site) o que está depois do www e antes da primeira barra (/). No endereço do site do ITS Rio podemos encontrar o domínio apenas excluindo o que está destacado:

Link completo: www.itsrio.org/pt/cursos | Domínio: itsrio.org

Para saber mais sobre domínios e seus diversos níveis acesse: https://miposicionamientoweb.es/que-es-un-dominio/

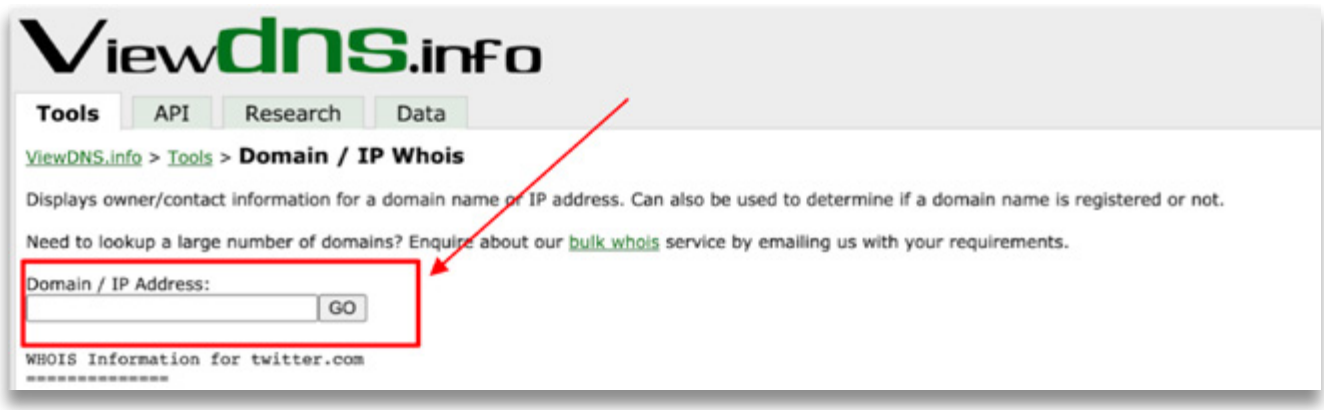
4.1 BUSCA DE INFORMAÇÕES DE DOMÍNIO (WHOIS)

PASSO 1:

Acesse no navegador: https://viewdns.info/whois/

PASSO 2

Na página, informe o endereço de domínio ou endereço de IP que gostaria de realizar a busca.



PASSO 3

Informe o endereço, clique em “GO”

PASSO 4

Página de resultados: o domínio que utilizamos foi da rede social Twitter, onde no campo entramos com o valor: twitter.com. A imagem abaixo mostra um exemplo dos dados que podem ser obtidos.

IMPORTANTE:

a. Há casos em que o proprietário do domínio oculta informações;

b. As informações disponíveis podem variar entre domínios.

4.2 BUSCA REVERSA WHOIS (REVERSE WHOIS LOOKUP):

PASSO 1

Acesse no navegador: https://viewdns.info/reversewhois/

PASSO 2

Na página, informe o **nome do proprietário ou endereço de e-mail** que gostaria de realizar a busca.

PASSO 3

Informe o termo desejado, clique em “GO”.

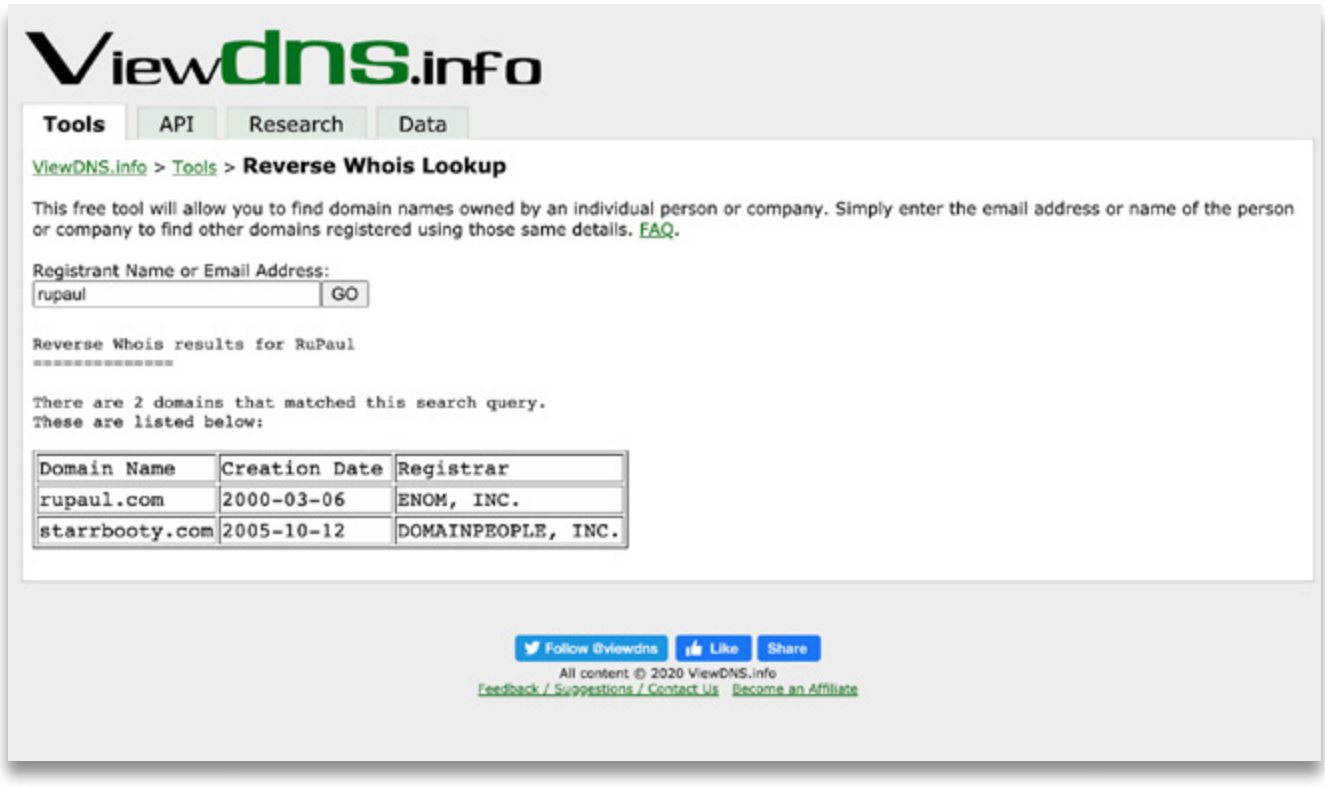
PASSO 4

Página de resultados: o domínio que utilizamos foi da rede social Twitter, onde no campo entramos com o valor: **rupaul**. A imagem abaixo mostra um exemplo dos dados que podem ser obtidos.

IMPORTANTE:

a. Há casos em que o proprietário do domínio oculta informações;

b. As informações disponíveis podem variar entre domínios.



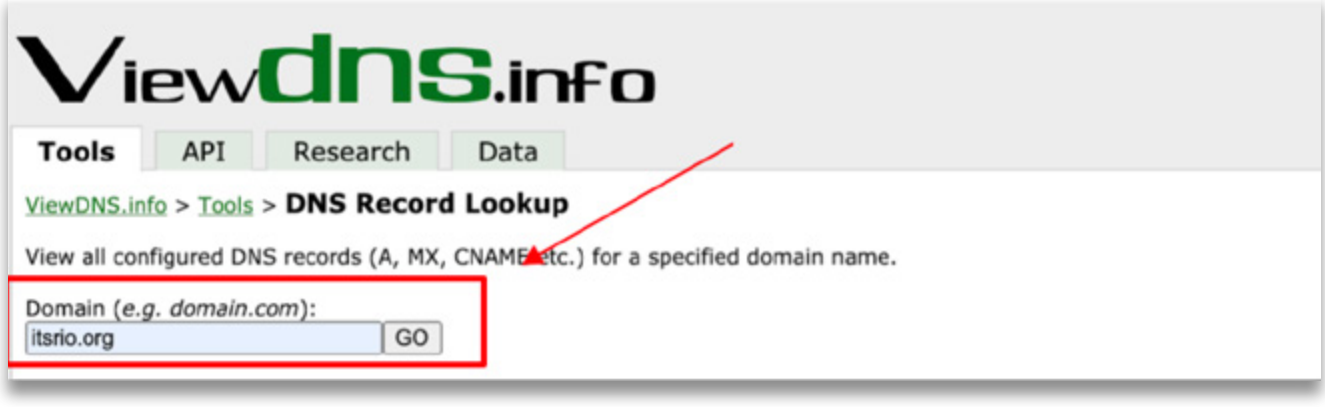
4.3 DNS RECORD LOOKUP:

PASSO 1:

Acesse no navegador: https://viewdns.info/dnsrecord/

PASSO 2:

Na página, informe o **endereço de domínio** que gostaria de realizar a busca



PASSO 3:

Informe o termo desejado, clique em “GO”

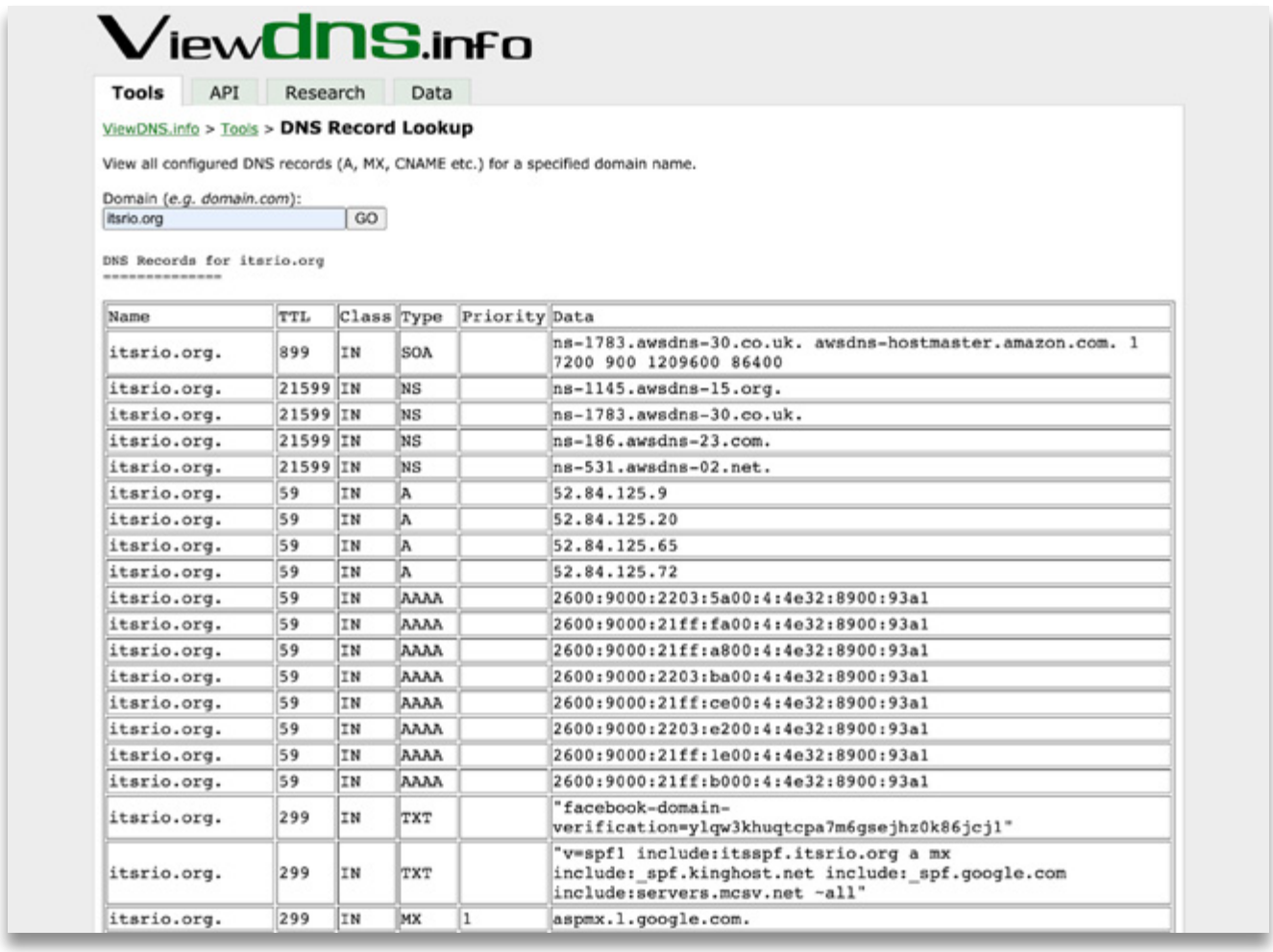
PASSO 4:

Página de resultados: o domínio que utilizamos foi da rede social Twitter, onde no campo entramos com o valor: **itsrio.org**. A imagem abaixo mostra um exemplo dos dados que podem ser obtidos.

IMPORTANTE:

Há casos em que o proprietário do domínio oculta informações;

As informações disponíveis podem variar entre domínios.



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 include:servers.mcsv.net -all"
itsrio.org.	299	IN	MX	1	aspmx.l.google.com.

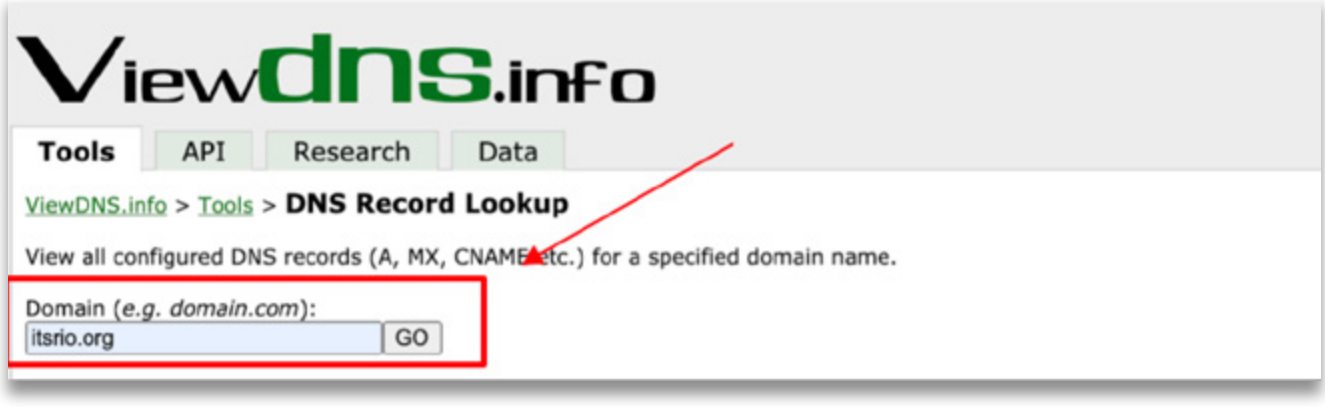
4.4 IP HISTORY:

PASSO 1:

Acesse no navegador: https://viewdns.info/iphistory/

PASSO 2:

Na página, informe o endereço de domínio que gostaria de realizar a busca.



PASSO 3:

Informe o termo desejado, clique em “GO”

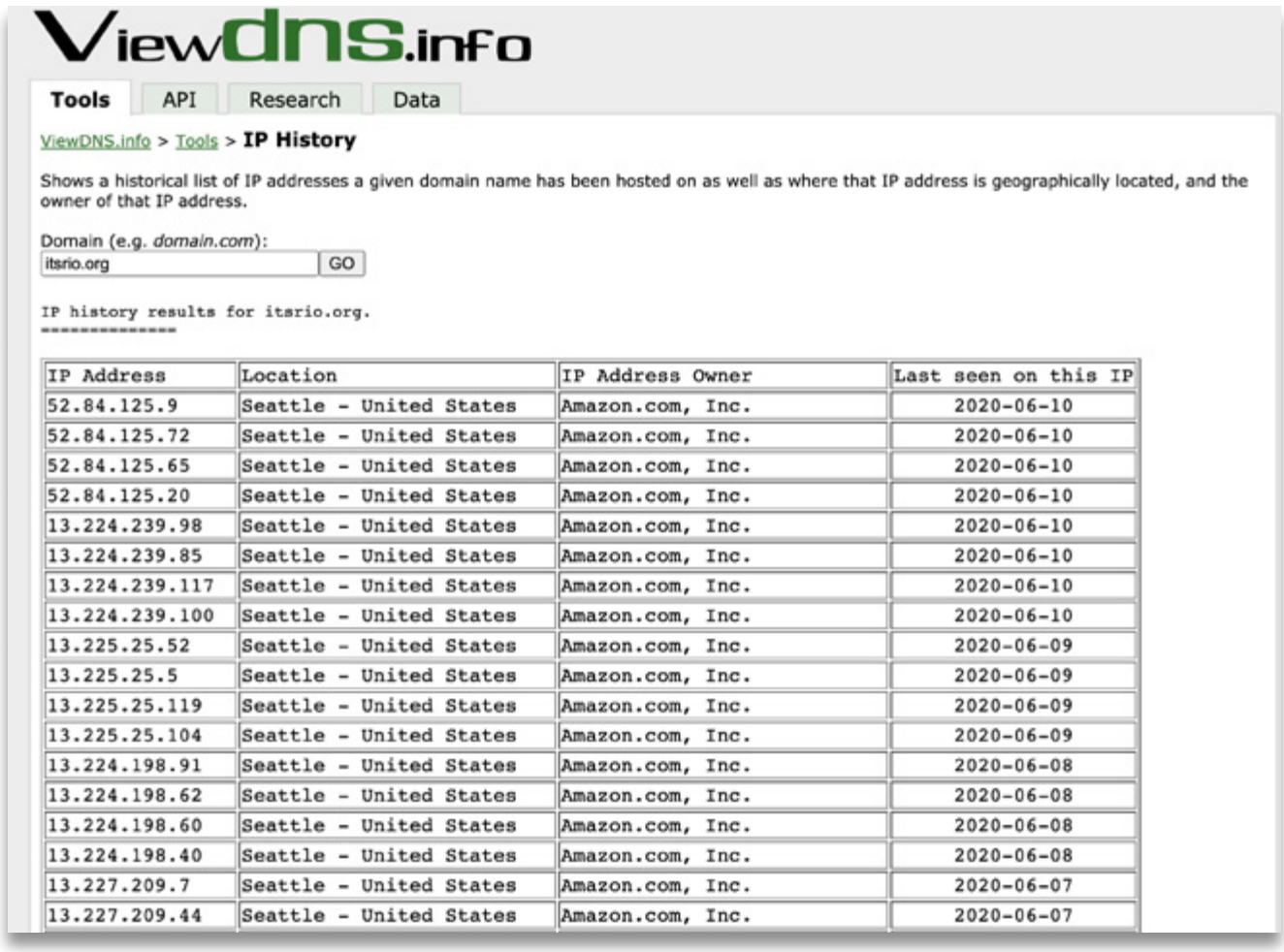
PASSO 4:

Página de resultados: o domínio que utilizamos foi da rede social Twitter, onde no campo entramos com o valor: itsrio.org. A imagem abaixo mostra um exemplo dos dados que podem ser obtidos.

IMPORTANTE:

a. Há casos em que o proprietário do domínio oculta informações;

b. As informações disponíveis podem variar entre domínios.



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

GOOGLE ALERTS

por Redson Fernando

EQUIPE DE DEMOCRACIA E TECNOLOGIA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

NESTE TUTORIAL, VOCÊ CONHECERÁ A FERRAMENTA GOOGLE ALERTS. APROVEITE!

1. O QUE É

O Google Alerts é uma ferramenta gratuita criada pelo Google para monitorar novos conteúdos indexados pelo motor de busca que estão relacionados a uma palavra-chave ou termo definido pelo usuário.

2. QUAIS SÃO AS FUNCIONALIDADES

O Google Alerts permite detectar e agrupar de forma simples e eficiente os conteúdos descentralizados na internet. Por exemplo, quando páginas da web, notícias, artigos ou posts de blog aparecem indexados no Google contendo o termo definido no alerta, o usuário é notificado pelo e-mail indicado no momento da criação.

Além disso, o recurso é personalizável. Você pode escolher não apenas os termos que deseja acompanhar, mas também a periodicidade dos avisos, os tipos de conteúdo, as fontes, os idiomas e a localização do que foi publicado. Dessa forma, você se mantém informado em relação aos assuntos que considera relevantes e consegue realizar o monitoramento de temas.

3. COMO ACESSAR

O Google Alerts é uma ferramenta que não necessita qualquer tipo de download ou instalação. Basta acessar o endereço www.google.com/alerts pelo seu navegador web.

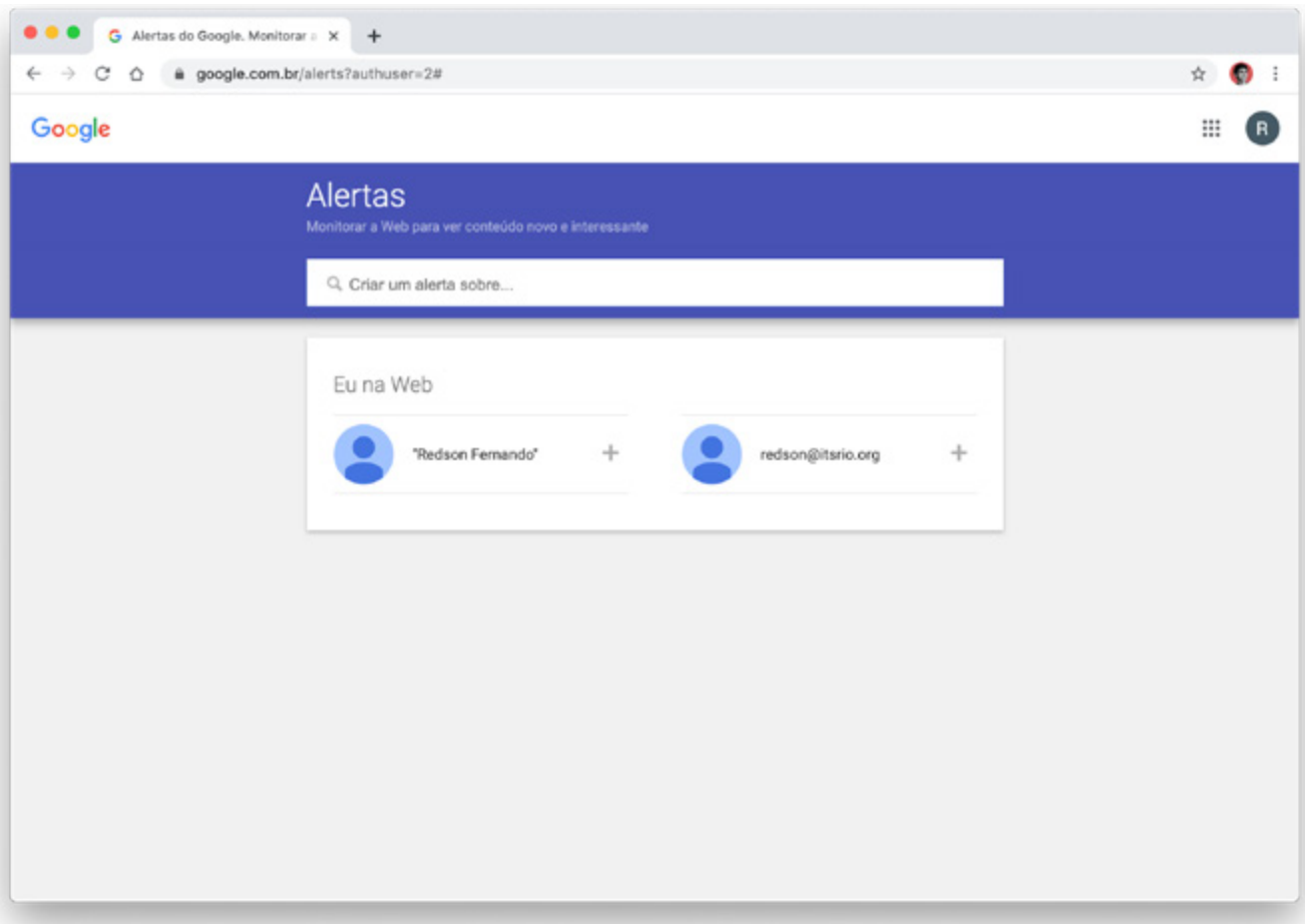
4. COMO UTILIZAR

PASSO 1:

Após acessar o endereço da ferramenta (www.google.com/alerts), a primeira etapa é selecionar quais são os termos que você deseja monitorar. Digite as palavras-chave na caixa “Criar um alerta sobre...”. Você consegue criar um alerta com seu próprio nome ou o e-mail cadastrado no serviço por meio da seção “Eu na Web”. Assim, sempre que algum conteúdo na internet citar você ou seu endereço de e-mail, o Google Alerts enviará uma notificação automaticamente.

PASSO 2:

Depois de selecionar os termos, será preciso informar um e-mail para receber os alertas. A ferramenta utilizará automaticamente seu e-mail Google caso você já esteja logado no serviço. Se quiser utilizar outro e-mail, é possível modificar depois.

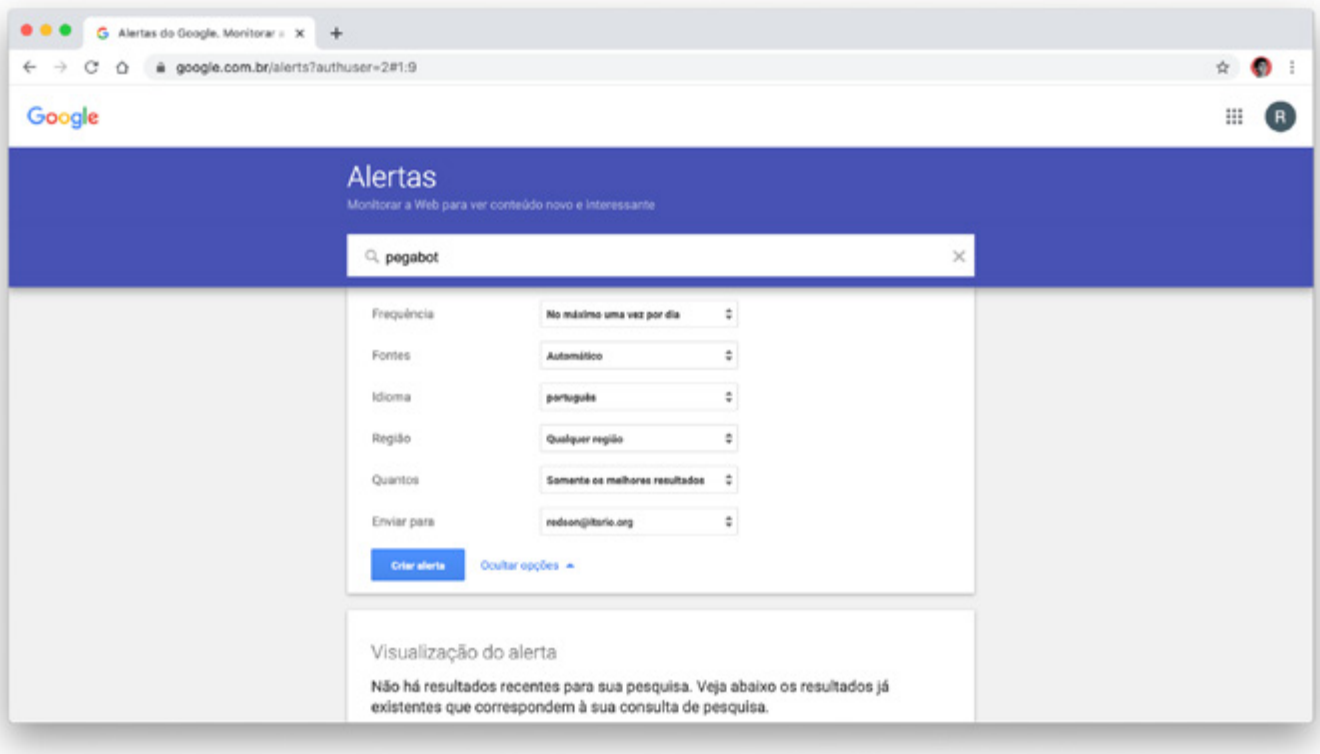


PASSO 3:

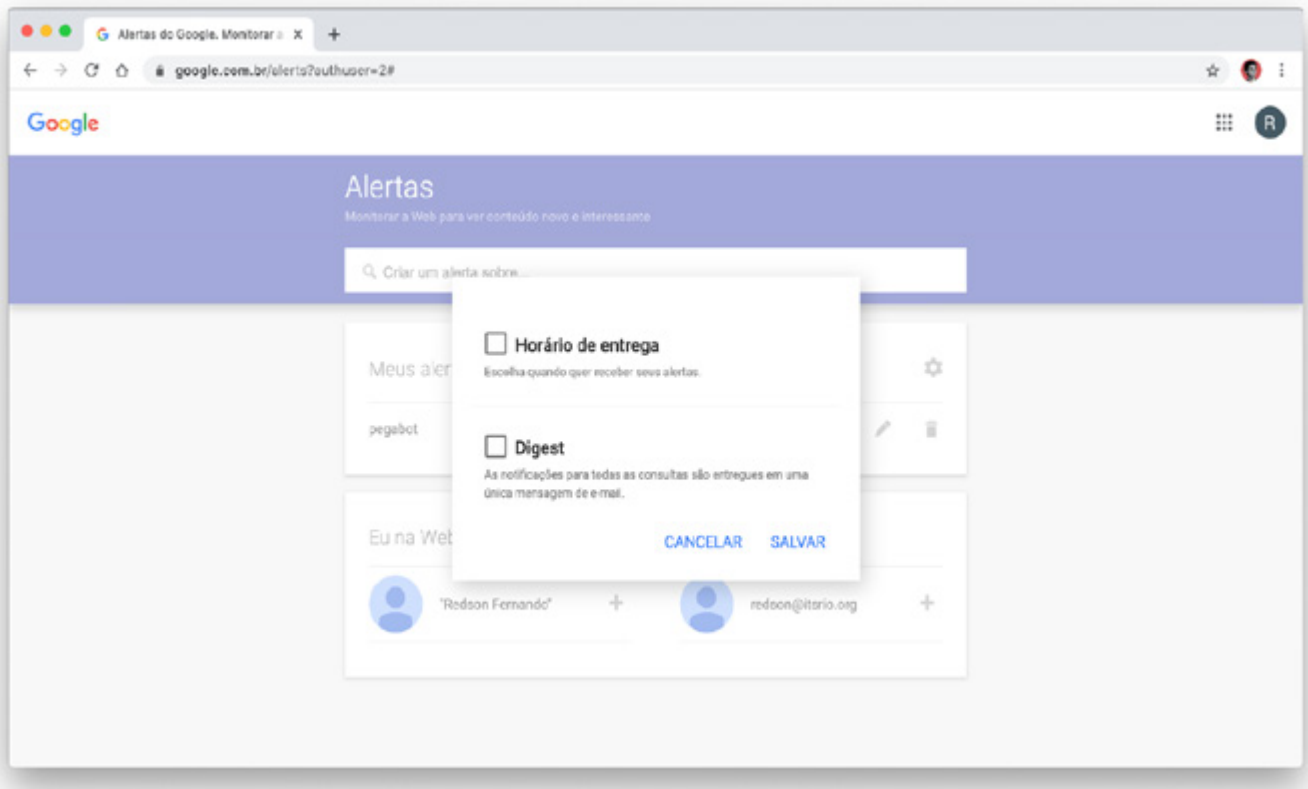
Para alterar as configurações do alerta, clique em “Mostrar opções”. Você pode alterar a frequência com que você recebe notificações, os tipos de sites exibidos, seu idioma, a região que você deseja que as informações venham, quantos resultados quer ver e o e-mail que irá receber os alertas.

PASSO 4:

Depois, basta clicar em “Criar alerta” para receber os e-mails sempre que o Google encontrar resultados de pesquisa correspondentes às preferências selecionadas.



Caso você queira, é possível editar o alerta clicando no ícone de lápis e depois em “Atualizar alerta”. Também é possível excluir o alerta clicando no ícone de lata de lixo na página principal da ferramenta ou clicando em “Cancelar inscrição” no e-mail da notificação. No ícone de engrenagem, você pode escolher se receberá os alertas sempre em um horário específico com a opção “Horário de entrega” ou se deseja receber todos os múltiplos alertas criados em uma mensagem única e com frequência programada por meio da opção “Digest”.



LISTA DE REFERÊNCIAS

EQUIPE DE DEMOCRACIA E TECNOLOGIA:
Debora Albu
Diego Cerqueira
Redson Fernando
Thayane Guimarães

AQUI VOCÊ ENCONTRARÁ UMA SÉRIE DE REFERÊNCIAS ACADÊMICAS, DOCUMENTOS DE PESQUISA E OUTRAS FERRAMENTAS QUE COBREM OS TÓPICOS DE AUTOMAÇÃO, DESINFORMAÇÃO E ANÁLISE DE REDE. EXPLORE AO MÁXIMO E FAÇA BOM USO!

1. LIVROS

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. RELATÓRIOS

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. ARTIGOS 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 (CONJUNTO DE FERRAMENTAS)

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

c. RESIST: Counter-Disinformation Toolkit

d. Newsgathering and Monitoring on the Social Web

e. First Draft Basic Toolkit

f. Bellingcat's Online Investigation Toolkit

g. Introduction to Data Journalism

5. PROJETOS

a. Chicas Poderosas

b. Media Monitoring Africa

c. Co-facts

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

e. Newtral