The background is a dark, atmospheric scene. On the left, a computer monitor sits on a desk, its screen glowing with a vibrant purple and blue brain scan. To the right, a large, muscular figure with a beard and a tattooed shoulder sits in a contemplative pose, resting their chin on their hand. A single, intense blue eye is visible on the right side of the frame, looking directly at the viewer. The overall mood is mysterious and tech-oriented.

ODYSSEUS OS

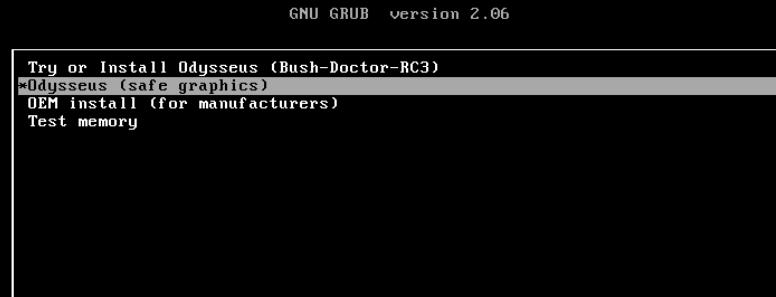
-
- Odysseus OS é uma distribuição Linux baseada no Xubuntu 22.04, utilizando o ambiente de desktop XFCE4. Focada em OSINT (Open Source Intelligence), oferece uma coleção de ferramentas especializadas para coleta e análise de dados de fontes abertas. Com uma interface leve e intuitiva, a Odysseus é ideal para analistas que buscam eficiência em suas investigações.



Desenvolvido por Franklin Soares dos Santos
Engenheiro de Software
Perito em Computação Forense



-  **Processador:** É necessário ter um processador dual-core de 2 GHz ou melhor.
-  **Memória RAM:** O mínimo recomendado é de 4 GB de RAM para uma instalação física.
-  **Espaço em disco:** É preciso ter 25 GB de espaço livre em disco para a instalação do Odysseus



Updates and other software

What apps would you like to install to start with?

Normal installation

Web browser, utilities, office software, games, and media players.

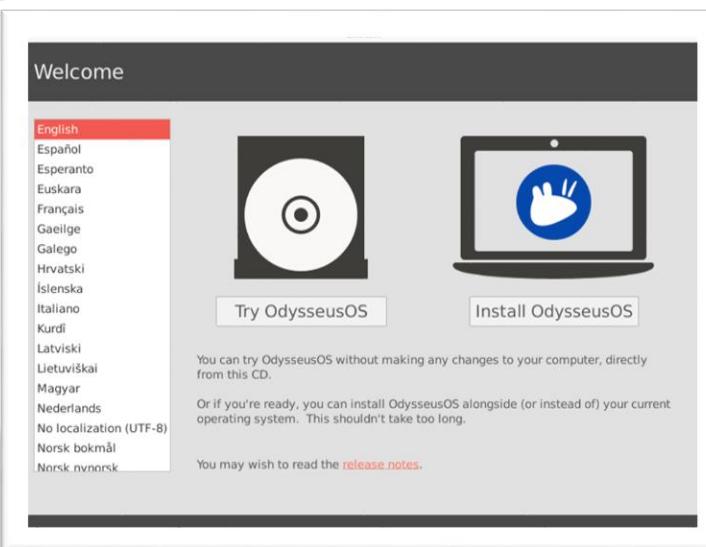
Minimal installation

Web browser and basic utilities.

Other options

Download updates while installing OdysseusOS

This saves time during the install.



- "Odysseus OS" foi projetado para fornecer uma gama de ferramentas "Open source" que permitem aos usuários realizar análises complexas e desenvolver estratégias eficazes em suas investigações. A distribuição incorpora softwares que facilitam a coleta, análise e interpretação de dados, permitindo que os usuários se destaquem em um ambiente de informações em constante mudança. (*Não marcar a opção de UPDATE*)

Installation type

This computer currently has Ubuntu 24.04.1 LTS on it. What would you like to do?

- Erase Ubuntu 24.04.1 LTS and reinstall

Warning: This will delete all your Ubuntu 24.04.1 LTS programs, documents, photos, music, and any other files.

- Install OdysseusOS 1.0 alongside Ubuntu 24.04.1 LTS

Documents, music, and other personal files will be kept. You can choose which operating system you want each time the computer starts up.

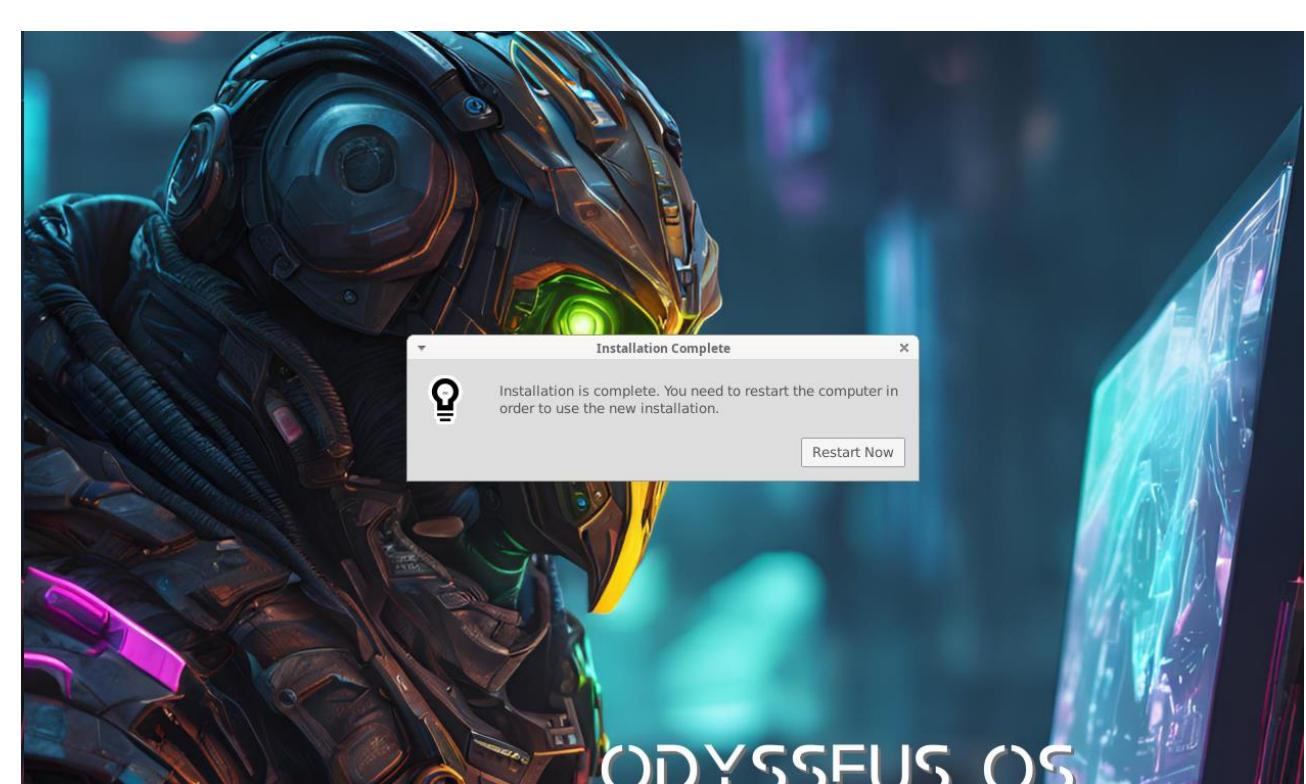
- Erase disk and install OdysseusOS

Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.

Advanced features... None selected

- Something else

You can create or resize partitions yourself, or choose multiple partitions for OdysseusOS.

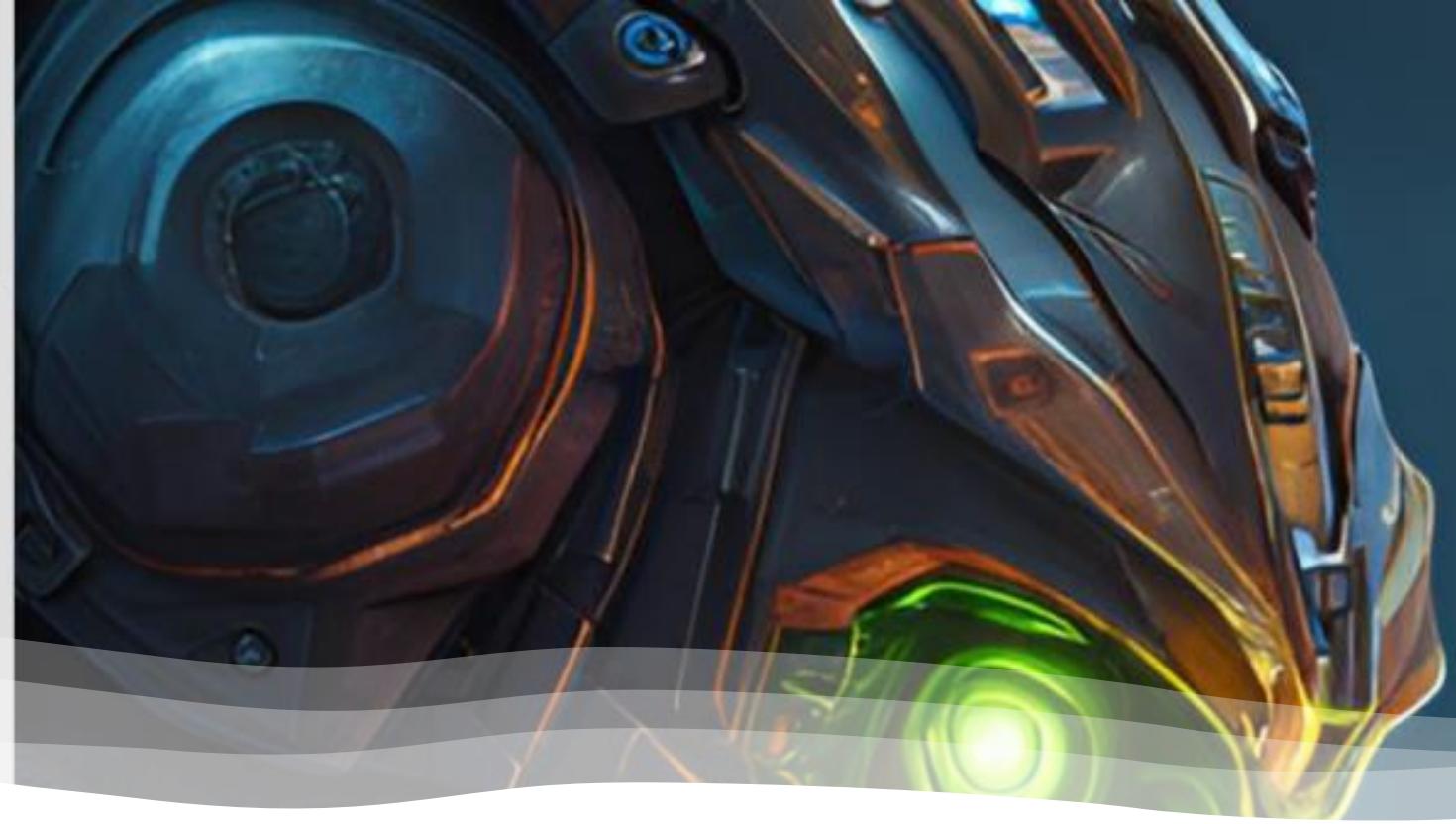
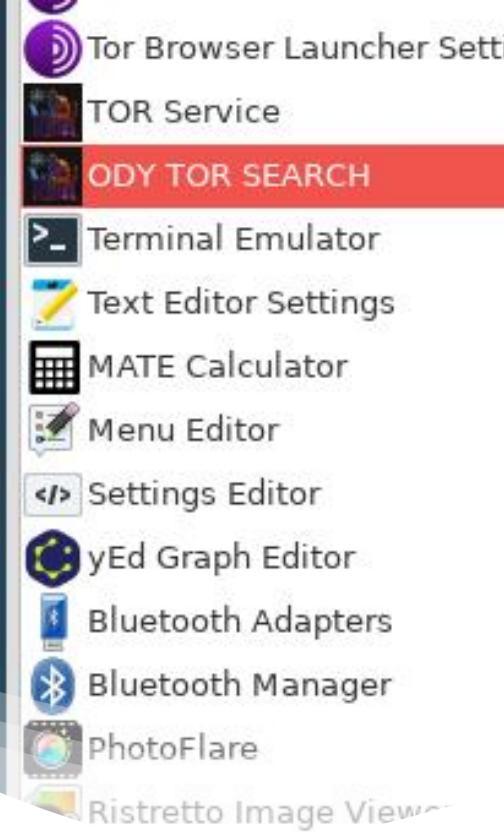


ODYSSEUS OS

ODYSSEUS OS

Navegação WEB





- Odysseus possibilita o uso da rede Tor com o Privoxy.
- O Privoxy atua como um proxy que melhora a privacidade e segurança ao navegar pela rede Tor, filtrando e modificando o tráfego da web.

<https://www.privoxy.org/>

ODYSSEUS OS



- 🌐 Privoxy é um proxy web não-caching que oferece filtros avançados para melhorar a privacidade, manipular cookies e modificar dados de páginas da web e cabeçalhos HTTP.
- 🔒 **Aumento da Privacidade** Ele permite que os usuários controlem o acesso e a forma como os dados são apresentados em suas navegações, contribuindo assim para uma experiência online mais segura.
- 💻 **Uso com Tor** O Privoxy pode ser usado em conjunto com a rede Tor para aumentar ainda mais a privacidade na internet, tornando-se uma ferramenta eficaz para usuários preocupados com segurança online.

```
analistaosint@analistaosint-VirtualBox:~$ systemctl status privoxy
● privoxy.service - Privacy enhancing HTTP Proxy
  Loaded: loaded (/lib/systemd/system/privoxy.service; enabled; vendor prese
  Active: active (running) since Tue 2024-11-19 12:16:19 -03; 16min ago
    Docs: man:privoxy(8)
          https://www.privoxy.org/user-manual/
    Main PID: 1052 (privoxy)
      Tasks: 1 (limit: 203991)
        Memory: 2.8M
          CPU: 20ms
        CGroup: /system.slice/privoxy.service
                  └─1052 /usr/sbin/privoxy --pidfile /run/privoxy.pid --user privoxy

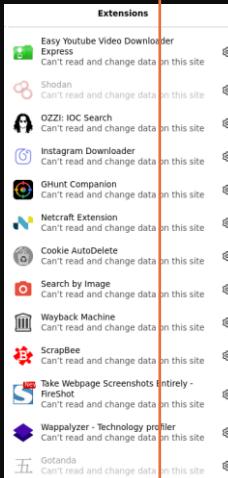
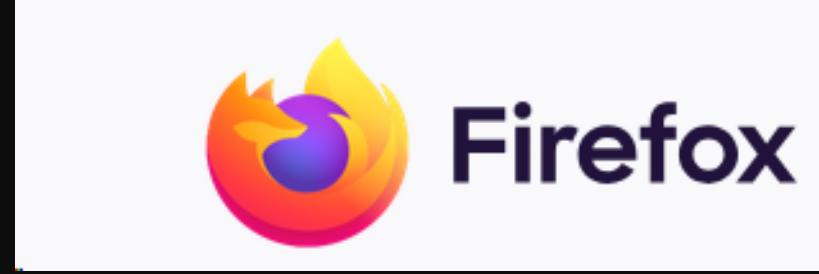
Nov 19 12:16:18 analistaosint-VirtualBox systemd[1]: Starting Privacy enhancing
Nov 19 12:16:19 analistaosint-VirtualBox systemd[1]: Started Privacy enhancing
```

```
analistaosint@analistaosint-VirtualBox:~$ systemctl status tor
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; enabled; vendor preset: en
  Active: active (exited) since Tue 2024-11-19 12:16:17 -03; 15min ago
    Main PID: 864 (code=exited, status=0/SUCCESS)
      CPU: 2ms

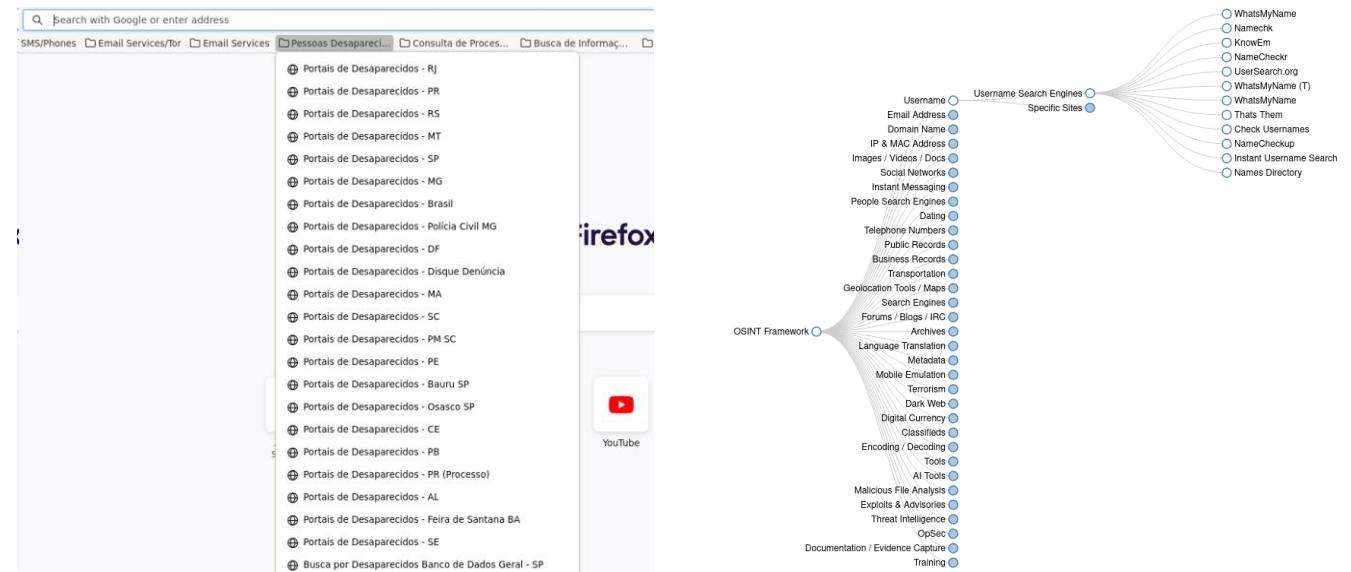
Nov 19 12:16:17 analistaosint-VirtualBox systemd[1]: Starting Anonymizing overl
Nov 19 12:16:17 analistaosint-VirtualBox systemd[1]: Finished Anonymizing overl
[lines 1-8/8 (END)]
```



- A distribuição Odysseus inclui uma versão do Firefox enriquecida com extensões voltadas para OSINT. Essas extensões podem incluir ferramentas para:
- **Análise de redes sociais:** Facilita a coleta de dados de plataformas sociais.
- **Verificação de informações:** Auxilia na validação de fatos e fontes.
- **Mapeamento geoespacial:** Permite a visualização de dados em mapas.
- **Captura de dados:** Ferramentas para extrair informações de páginas da web.



A distribuição
Odysseus vem com
inúmeros bookmarks
(favoritos) de
recursos e
ferramentas de OSINT



The screenshot shows the WhosMyName Web interface at <https://whosmyname.app>. The page features a search bar with placeholder text: "Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter". Below the search bar is a "Category Filters" button. The search results table has columns for SITE, USERNAME, and CATEGORY. The first result is for "Processo" with the site "https://www.poder360.com.br" and the category "Document". A note below the results says: "these results are document searches with the first username in the list used as the search term". To the right, there is a note about "Google Search": "these results are google searches with the first username in the list used as the search term".

Extensões do Firefox incluídas na distribuição:

| Nome | Descrição |
|--|---|
| Multi-Account Containers | Permite abrir abas que são completamente isoladas, não compartilhando cookies, dados de sessão ou outras informações. |
| FireShot: Full Web Page Screenshots | Captura e salva a parte visível, uma área selecionada ou a página inteira, incluindo partes que não estão visíveis. |
| uBlock Origin | Melhora a segurança do navegador bloqueando anúncios, rastreadores e sites de malware. |
| DownThemAll! | Permite baixar toda a mídia, como vídeos e imagens, de um site e salvá-los no computador. |
| ScrapBee | Permite salvar páginas da web inteiras para acesso offline e organizá-las para uma boa visão geral. |
| Search by Image | Realiza uma busca reversa de imagem em várias bases de dados (como Google, Bing, Yandex, TinEye, SauceNAO, IQDB) ao clicar com o botão direito na imagem. |
| User-Agent Switcher and Manager | Permite alterar sua string de user-agent para indicar que você está em um dispositivo diferente. |
| NoScript Security Suite | Permite que conteúdos web potencialmente maliciosos sejam executados apenas em sites confiáveis. |
| Privacy Badger | Bloqueia rastreadores invisíveis automaticamente. |
| Cookie AutoDelete | Permite controlar seus cookies, excluindo-os automaticamente após o fechamento das abas. |
| Shodan | Informa onde o site está hospedado (país, cidade), quem possui o IP e quais outros serviços/portas estão abertos. |
| Netcraft Extension | Fornece informações abrangentes sobre o site e proteção contra phishing e JavaScript malicioso ao navegar na web. |
| Wappalyzer | Ajuda a identificar tecnologias utilizadas em websites. |
| Wayback Machine | Permite voltar no tempo para ver como um site mudou ao longo da história da web. |



A distribuição Odysseus vem com o Firefox configurado por padrão para navegar na dark web. Isso inclui:

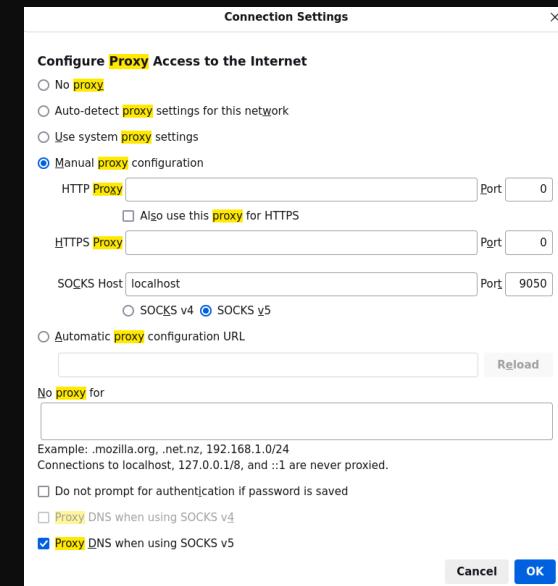
Configuração do Proxy: O Firefox é configurado para usar o Tor como proxy, permitindo acesso a sites .onion.

Privacidade Aumentada: Extensões como uBlock Origin e Privacy Badger estão ativadas para melhorar a segurança e privacidade durante a navegação.

Desativação de Scripts: A extensão NoScript está configurada para bloquear scripts não confiáveis, aumentando a segurança.

User-Agent Alterado: O User-Agent Switcher é usado para ocultar informações sobre o sistema operacional e navegador.

Bookmarks Específicos: Favoritos direcionados a recursos da dark web e ferramentas de OSINT.



Arquivo Editar Ver Terminal Abas Ajuda

O endereço IP conectado à rede Tor é: 192.42.116.180

Informações de geolocalização do IP:

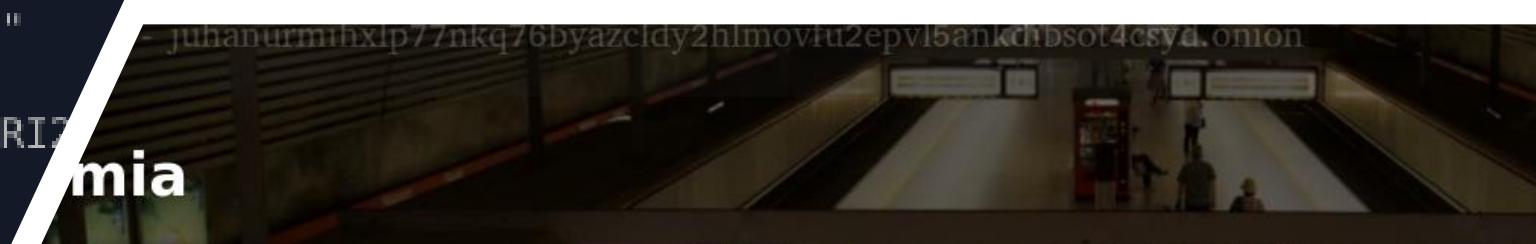
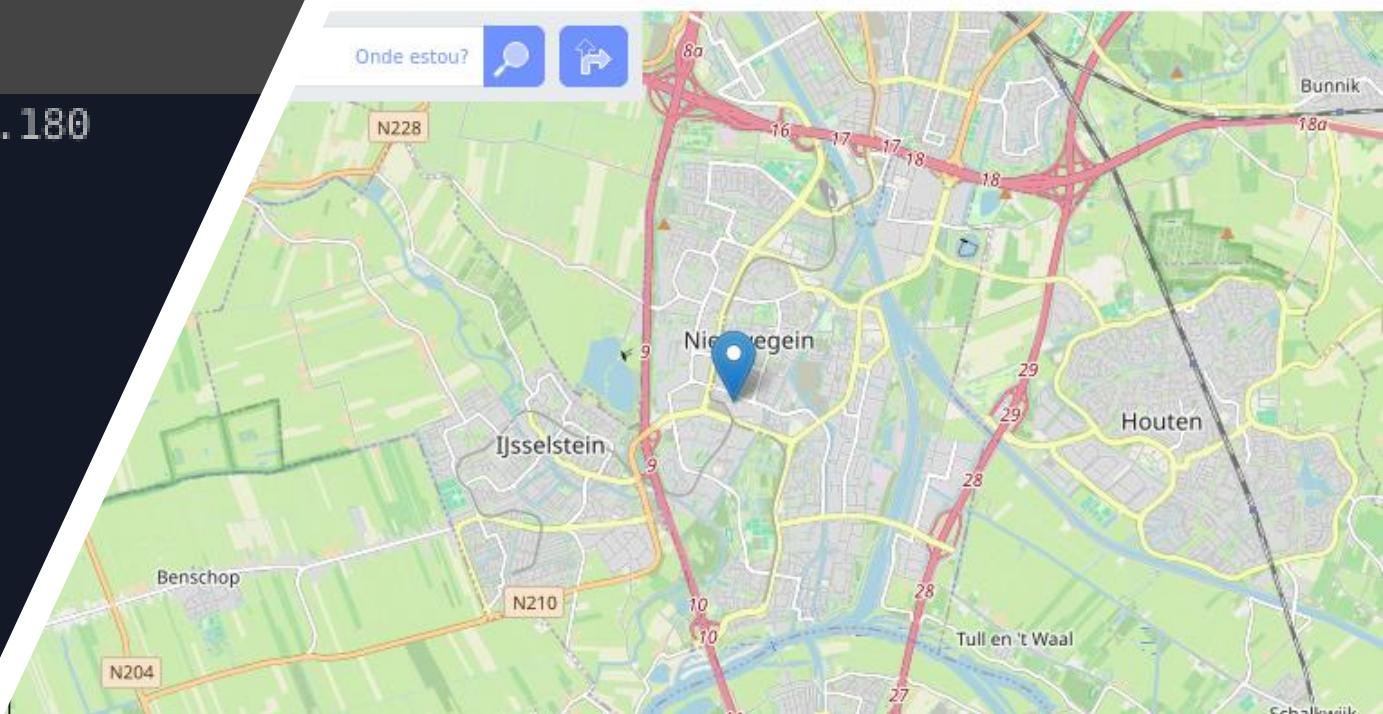
```
{
  "ip": "192.42.116.180",
  "hostname": "28.tor-exit.nothingtohide.nl",
  "city": "Nieuwegein",
  "region": "Utrecht",
  "country": "NL",
  "loc": "52.0292,5.0806",
  "org": "AS1101 SURF B.V.",
  "postal": "3431",
  "timezone": "Europe/Amsterdam",
  "readme": "https://ipinfo.io/missingauth"
}
```

odysseusos@odysseusos:~\$ libEGL warning: DRI2



·p Editar Mais Entrar Criar conta

Onde estou?

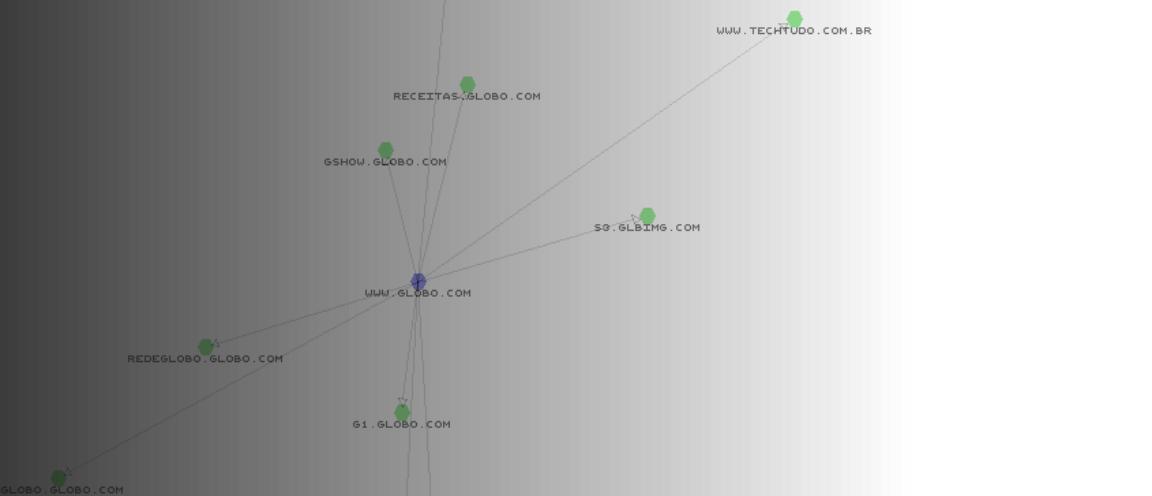


Ahmia searches hidden services on the Tor network. To access these hidden services, you need the [Tor browser bundle](#). Abuse material is not allowed on Ahmia. See our [service blacklist](#) and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see [indexing information](#), contribute to the source code.

[The Tor Project](#)

Onion service: juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion



- **Visão Geral do YaCy** YaCy é um software gratuito para criar seu próprio mecanismo de busca, permitindo que você se junte a uma comunidade de motores de busca ou crie seu próprio portal de busca.
- **Conceito de P2P** O YaCy é desenvolvido com base em redes peer-to-peer (P2P), promovendo a descentralização das buscas e o controle do usuário sobre seus dados.
- **Origem e Desenvolvimento** Criado por Michael Christen em 2003, o YaCy visa oferecer uma alternativa aos motores de busca centralizados, incentivando a participação coletiva na construção da Internet.



ODYSSEUS OS



- SpiderFoot é uma ferramenta de automação de OSINT (Open Source Intelligence) que permite a coleta e análise de informações sobre alvos (como domínios, endereços IP, e-mails, etc.). Aqui estão alguns dos principais recursos e funcionalidades do SpiderFoot:
 - **Coleta Automatizada de Dados:** Realiza varreduras em várias fontes de dados para coletar informações relevantes sobre o alvo.
 - **Módulos Diversificados:** Possui diversos módulos que permitem a busca em redes sociais, registros DNS, dados de geolocalização, informações de segurança, entre outros.
 - **Interface Web Intuitiva:** Oferece uma interface gráfica fácil de usar, permitindo que usuários realizem investigações sem necessidade de conhecimento técnico avançado.
 - **Relatórios Personalizados:** Gera relatórios detalhados com as informações coletadas, facilitando a análise e apresentação dos dados.
 - **Integração com Outras Ferramentas:** Pode ser integrado com outras ferramentas de segurança e análise, ampliando suas capacidades.

-
-  **O que é GHunt?** GHunt é uma ferramenta OSINT (Open Source Intelligence) projetada para extrair informações de contas do Google usando endereços de e-mail.
 - **GHunt Companion** É uma extensão para navegadores que facilita a configuração de cookies necessários para o uso do GHunt, otimizando a experiência do usuário.
 -  **Download e Desenvolvimento** GHunt está em constante evolução e está disponível para download, com foco em aplicações ofensivas relacionadas ao Google.
-



```
File Edit View Terminal Tabs Help
ghunt não encontrado, instalando com pipx...
  installed package ghunt 2.2.0, installed using Python 3.10.12
  These apps are now globally available
    - ghunt
done! ✨ * ✨

.d8888b. 888   888           888
d88P Y88b 888   888           888
888   888 888   888           888
888   88888888888 888   888 888888b. 888888
888   88888 888   888   888 888 "88b 888
888   888 888   888   888 888 888 888 888
Y88b d88P 888   888 Y88b 888 888 888 Y88b.
"Y8888P88 888   888 "Y88888 888 888 "Y888 v2
```

By: mxrch ([@mxrchreborn](#))
Support my work on GitHub Sponsors ! ❤

- Mr.Holmes é uma ferramenta de coleta de informações (OSINT) que tem como objetivo obter informações sobre domínios, nomes de usuário e números de telefone usando fontes públicas da Internet. Ela também utiliza ataques de dorks do Google para pesquisas específicas e proxies para anonimizar as solicitações. Além disso, a ferramenta possui uma API do WhoIS para obter mais informações sobre um domínio.

ODYSSEUS OS



```
MR.HOLMES
Now is the dramatic moment of fate, Watson,
when you hear a step upon the stair
which is walking into your life,
and you know not whether for good or ill.

A COMPLETE OSINT TOOL:          CODED BY LUCKSI
[+]VERSION:T_G_D-1_0_4           CURRENT-DATE: 12/09/2023
Instagram:lucks_022             DATE-FORMAT: EUROPE
Email:lukege287@gmail.com        CLI-LANGUAGE: ENGLISH
GitHub:lucksi
Twitter:@Lucks_i_22
LinkedIn:https://www.linkedin.com/in/Lucks_i

[INSERT AN OPTION :PRESS @ TO REFRESH THE QUOTE]
(1)SOCIAL-ACCOUNT-OSINT      (2)PHONE-NUMBER-OSINT      (11)ENCODING/DECODING
(3)DOMAIN/IP-OSINT           (4)CONFIGURATION         (12)PDF-GRAPH CONVERTER
(5)DATABASE(GUT)              (6)UPDATE               (13)FILE-TRANSFER
(7)PORT-SCANNER                (8)E-MAIL               (14)SESSION-OPTIONS
(9)DORKS-GENERATOR            (10)PEOPLE-OSINT        (15)EXIT

[#MR.HOLMES#]-->
```

ODYSSEUS OS



- O IVRE (Intelligence and Vulnerability Research Environment) é um framework de código aberto projetado para ajudar na coleta e análise de dados de inteligência e vulnerabilidades. Aqui estão alguns dos principais aspectos do IVRE:
 - **Coleta de Dados:** Permite a coleta de informações sobre redes e dispositivos, incluindo varreduras de portas e serviços.
 - **Análise de Vulnerabilidades:** Integra-se com ferramentas de análise para identificar vulnerabilidades conhecidas em sistemas e serviços.
 - **Interface Web:** Oferece uma interface gráfica que facilita a visualização e análise dos dados coletados.
 - **Relatórios e Dashboards:** Gera relatórios detalhados e dashboards interativos que ajudam na interpretação dos dados.
 - **Integração com Outras Ferramentas:** Pode ser integrado com outras ferramentas de segurança e análise, ampliando suas funcionalidades.
 - **Documentação e Comunidade:** Possui uma comunidade ativa e documentação abrangente, facilitando o aprendizado e a utilização da ferramenta.

A screenshot of the IVRE web interface. At the top, there is a navigation bar with a house icon and the text "IVRE". Below the navigation bar, there is a large search bar with the placeholder "Search docs". To the right of the search bar is a button labeled "latest ▾". In the center of the page is a large, dark rectangular area containing a white icon of a bottle inside a circle. The overall theme is dark blue and professional.

[Home](#) / Overview

Overview

- **Principais Funcionalidades**
 - Purpose
 - Status
 - Access



- **O que é o BBOT?** BBOT é uma ferramenta de OSINT (Open Source Intelligence) modular e recursiva escrita em Python, capaz de realizar todo o processo de levantamento de informações com um único comando.
- **Funcionalidades do BBOT** Através do BBOT, é possível realizar enumeração de subdomínios, varredura de portas, capturas de tela de sites e varreduras de vulnerabilidades.



-  **O que é GoBuster?** GoBuster é uma ferramenta de força bruta utilizada para enumerar URI (diretórios e arquivos), subdomínios DNS e nomes de Virtual Host em sites. [source](#)
-  **Tutorial de GoBuster** O GoBuster é um recurso poderoso para explorar arquivos ocultos e diretórios remotos, sendo simples de instalar e executar, especialmente em distribuições como o Ubuntu. [source](#)

File Edit View Terminal Tabs Help

```
tlab, pyee, markdown-it-py, aiosignal, rich, playwright, aiohttp
```

```
    Running setup.py install for tqdm ... done
```

```
Successfully installed Pygments-2.17.2 aiohttp-3.9.3 aiosignal-1.3.1 as
ut-4.0.3 asyncio-3.4.3 attrs-23.2.0 certifi-2024.2.2 chardet-5.2.0 char
lizer-3.3.2 frozenlist-1.4.1 greenlet-3.0.3 idna-3.6 markdown-it-py-3.0
0.1.2 multidict-6.0.5 pillow-10.2.0 playwright-1.43.0 pyee-11.1.0 python
1.0.1 reportlab-4.1.0 requests-2.31.0 rich-13.7.1 tqdm-0.0.1 tqdm-4.67.
extensions-4.11.0 urllib3-2.2.0 yarl-1.9.4
```



ODYSSEUS OS



Made with ❤ by Lucas 'Plngulln0' Antoniaci

Either --username or --email is required

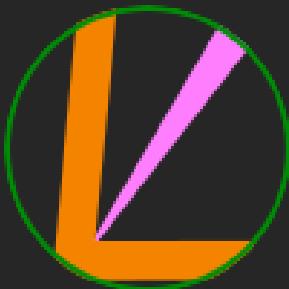
analistaosint@analistaosint-VirtualBox:~\$

-  **Blackbird OSINT** Blackbird é uma ferramenta de inteligência de fontes abertas (OSINT) que permite a pesquisa de contas de usuário por nome de usuário ou e-mail em diversas plataformas, facilitando a coleta de informações digitais.

-  **Busca em Redes Sociais** A ferramenta possibilita a busca em mais de 574 redes sociais, tornando-a uma opção robusta para investigações.



ODYSSEUS OS



Instaloader

```
Using cached requests-2.32.3-py3-none-any.whl (64 kB)
Collecting charset-normalizer<4,>=2
  Using cached charset_normalizer-3.4.0-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (144 kB)
Collecting urllib3<3,>=1.21.1
  Using cached urllib3-2.2.3-py3-none-any.whl (126 kB)
Collecting certifi>=2017.4.17
  Using cached certifi-2024.8.30-py3-none-any.whl (167 kB)
Collecting idna<4,>=2.5
  Using cached idna-3.10-py3-none-any.whl (70 kB)
Using legacy 'setup.py install' for instaloader, since package 'wheel' is not installed.
Installing collected packages: urllib3, idna, charset-normalizer, certifi, requests, instaloader
  Running setup.py install for instaloader ... done
Successfully installed certifi-2024.8.30 charset-normalizer-3.4.0 idna-3.10 instaloader-4.14 requests-2.32.3 urllib3-2.2.3
usage:
instaloader [--comments] [--geotags]
              [--stories] [--highlights] [--tagged] [--reels] [--igtv]
              [--login YOUR-USERNAME] [--fast-update]
              profile | "#hashtag" | %location_id | :stories | :feed | :saved
instaloader --help
```

- **Instaloader** O Instaloader é uma ferramenta de linha de comando gratuita que permite baixar fotos, vídeos e metadados do Instagram. Ele pode acessar perfis públicos e privados, hashtags, histórias e muito mais.

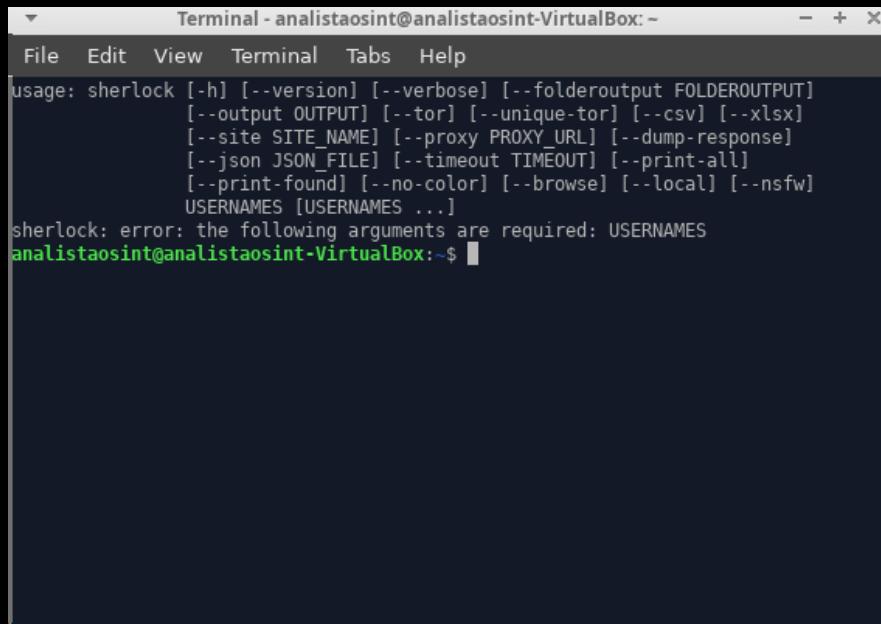
- **Biblioteca Python** O Instaloader é também uma biblioteca Python que oferece funcionalidades para baixar uma ampla variedade de conteúdos do Instagram de forma automatizada.

```
Terminal -  
File Edit View Terminal Tabs Help  
collecting charset-normalizer<4,>=2  
Using cached charset_normalizer-3.4.0-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whe (144 kB)  
Installing collected packages: urllib3, idna, charset-normalizer, certifi, requests  
Successfully installed certifi-2024.8.30 charset-normalizer-3.4.0 idna-3.10 requests-2.32.3 urllib3-2.2.3  
  
Protonmail API is ONLINE  
Protonmail VPN is ONLINE  
  
Let's take a look at your target:  
1 - Test the validity of one protonmail account  
2 - Try to find if your target have a protonmail account  
3 - Find if your IP is currently affiliate to ProtonVPN  
  
Choose a program: [
```

```
(root@kali:~/Desktop/ProtOSINT) root@kali:~/Desktop/ProtOSINT# python3 protosint.py  
Protosint  
  
Protonmail API is OFFLINE  
Protonmail VPN is ONLINE  
  
Let's take a look at your targets:  
1 - Test the validity of one protonmail account  
2 - Try to find if your target have a protonmail account  
3 - Find if your IP is currently affiliate to Protonmail  
  
Choose a program: [
```



- **ProtOSINT** ProtOSINT é um script em Python desenvolvido para ajudar na investigação de contas do ProtonMail e endereços IP do ProtonVPN.
- **Funcionalidade** O ProtOSINT pode ser utilizado para descobrir se um alvo precisa de uma conta do ProtonMail gerando múltiplos endereços dentro da ferramenta.
- **Acesso ao Código** O código-fonte do ProtOSINT está disponível no GitHub, permitindo que os usuários o modifiquem de acordo com suas necessidades.



```
Terminal - analistaosint@analistaosint-VirtualBox: ~
File Edit View Terminal Tabs Help
usage: sherlock [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]
                 [--output OUTPUT] [--tor] [--unique-tor] [--csv] [--xlsx]
                 [--site SITE_NAME] [--proxy PROXY_URL] [--dump-response]
                 [--json JSON_FILE] [--timeout TIMEOUT] [--print-all]
                 [--print-found] [--no-color] [--browse] [--local] [--nsfw]
                 USERNAMES [USERNAMES ...]
sherlock: error: the following arguments are required: USERNAMES
analistaosint@analistaosint-VirtualBox:~$
```



Sherlock

Hunt down social media
accounts by username across
400+ social networks

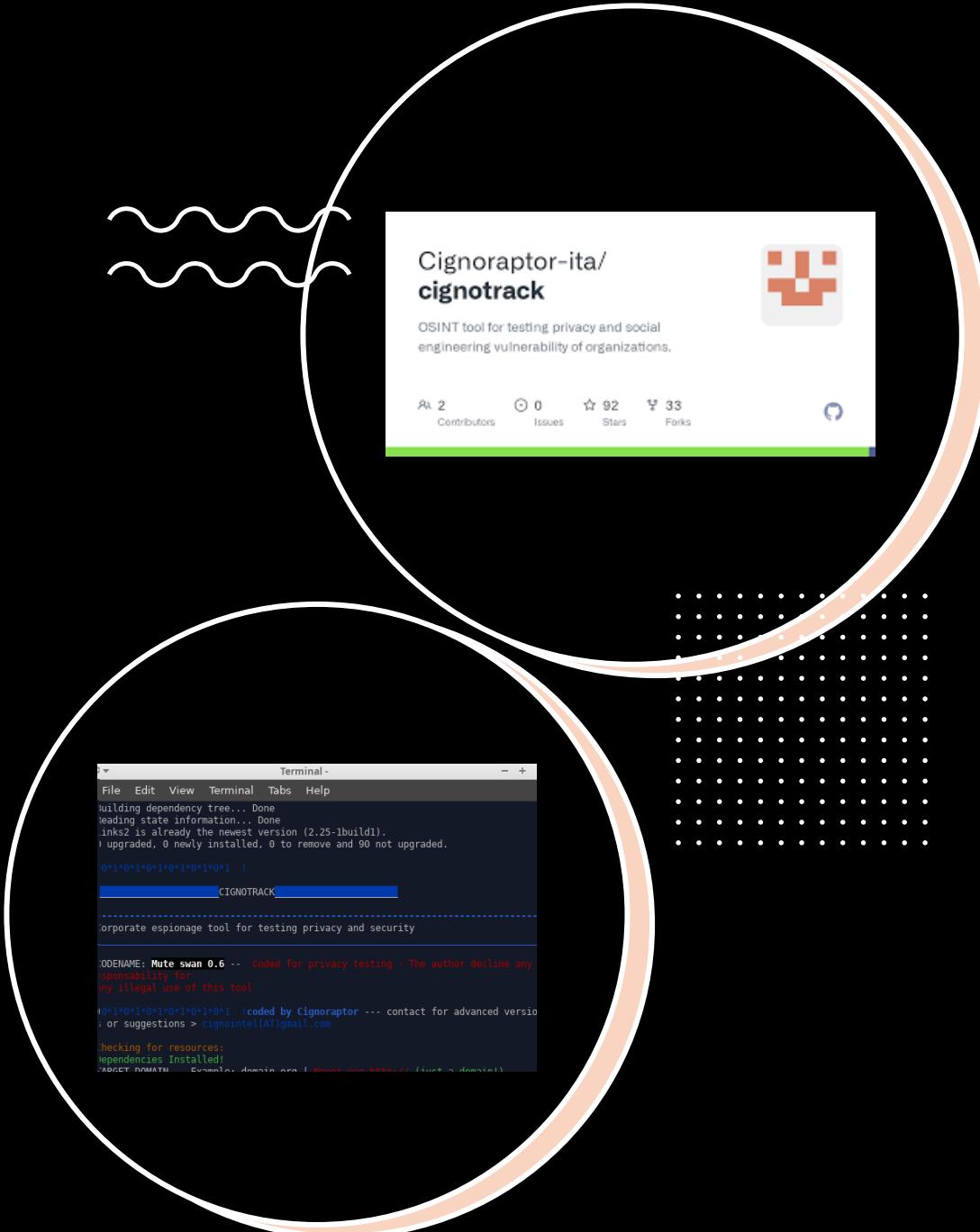


- 🔎 **O que é o Sherlock?** Sherlock é uma ferramenta de OSINT que permite a busca de contas em redes sociais a partir de um nome de usuário. É amplamente utilizada por investigadores digitais e profissionais de segurança para mapear a presença online de indivíduos. [source](#)

- 💡 **Funcionalidade da Ferramenta** Através do Sherlock, é possível confirmar em quais redes sociais um determinado usuário possui cadastro, facilitando investigações sobre identidade e reputação digital. [source](#)



ODYSSEUS OS



- **Ferramenta de OSINT** Cignotrack é uma ferramenta de espionagem corporativa para testar a privacidade e segurança através de OSINT e engenharia social.
- **Recursos do Cignotrack** A ferramenta possui funcionalidades como leitura de banco de dados whois, extração de metadados de documentos e coleta de e-mails e palavras de interesse

ODYSSEUS OS



- **💡 O que é CloudFail?** CloudFail é uma ferramenta de reconhecimento tático que visa reunir informações sobre alvos protegidos pelo Cloudflare, tentando descobrir endereços IP ocultos por meio de registros DNS mal configurados e bancos de dados antigos.
- **🔍 Uso da CloudFail** A ferramenta é usada por web scrapers para revelar endereços IP de servidores de origem, proporcionando uma nova oportunidade para extrair dados de sites que utilizam os serviços do Cloudflare.
- **📚 Estudo de Caso** O CloudFail também é abordado em estudos que discutem como contornar proxies reversos, demonstrando a eficácia das abordagens de bypass implementadas com esta ferramenta.

File Edit View Terminal Tabs Help

```
successfully installed beautifulsoup4-4.6.0 bs4-0.0.1 certifi-2017.4.17 chardet-0.4 charset-normalizer-3.4.0 colorama-0.3.9 dnspython-1.15.0 idna-2.5 requests-3.2.3 urllib3-1.24.2 win_inet_pton-1.0.1
```



```
[04:44] Initializing CloudFail - the date is: 19/11/2024
usage: cloudfail.py [-h] [-t TARGET] [-T] [-u] [-s SUBDOMAINS]

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        target url of website
```

4CK3RT3CH/ CloudFail



0 Issues 4 Stars 4 Forks



ODYSSEUS OS



- **O que é o Cloudscraper?** Cloudscraper é um módulo Python que permite contornar a página anti-bot do Cloudflare, conhecido como 'Estou Sob Ataque', facilitando a raspagem de dados de sites protegidos. [source](#)
- **Como usar o Cloudscraper?** Para utilizar o Cloudscraper em Python, basta instalar a biblioteca e usar suas funções para acessar informações de sites que têm medidas de proteção da Cloudflare

File Edit View Terminal Tabs Help

```
linux2014_x86_64.whl (144 kB)
Collecting idna<4,>=2.5
  Using cached idna-3.10-py3-none-any.whl (70 kB)
Collecting certifi>=2017.4.17
  Using cached certifi-2024.8.30-py3-none-any.whl (167 kB)
Collecting soupsieve>1.2
  Using cached soupsieve-2.6-py3-none-any.whl (36 kB)
Installing collected packages: rfc3987, urllib3, termcolor, soupsieve, idna, charset-normalizer, certifi, requests, BeautifulSoup4
Successfully installed BeautifulSoup4-4.12.3 certifi-2024.8.30 charset-normalizer-3.4.0 idna-3.10 requests-2.32.3 rfc3987-1.3.8 soupsieve-2.6 termcolor-2.5.0 urllib3-2.2.3
usage: CloudScraper.py [-h] [-u URL] [-d DEPTH] [-l TARGETLIST] [-v]
                         [-p PROCESS] [--no-verify]

options:
  -h, --help            show this help message and exit
  -u URL               Target Scope
  -d DEPTH             Max Depth of links Default: 5
  -l TARGETLIST         Location of text file of Line Delimited targets
```



Cloud
Scraper

ODYSSEUS OS



- O dnsrecon é uma ferramenta de código aberto utilizada para realizar reconhecimento de DNS (Domain Name System) em redes de computadores. Ela foi projetada para ajudar os profissionais de segurança a identificar vulnerabilidades e obter informações sobre os registros DNS de um domínio.
- Com o dnsrecon, é possível realizar várias tarefas, como:
 - Enumeração de servidores DNS autoritativos e não autoritativos
 - Descoberta de subdomínios ocultos
 - Identificação de servidores DNS abertos à exploração
 - Análise de registros DNS, como MX, NS e SOA
 - Verificação de vulnerabilidades em servidores DNS

```
terminal - analistaosint@analistaosint-VirtualBox:~ - +  
File Edit View Terminal Tabs Help  
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY]  
[-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS]  
[--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV]  
[-j JSON] [--iw] [--disable_check_recursion]  
[--disable_check_bindversion] [-V] [-v] [-t TYPE]  
  
options:  
-h, --help show this help message and exit  
-d DOMAIN, --domain DOMAIN  
Target domain.  
-n NS_SERVER, --name_server NS_SERVER  
Domain server to use. If none is given, the SOA of the  
target will be used. Multiple servers can be specified using a comma separated  
list.  
-r RANGE, --range RANGE  
IP range for reverse lookup brute force in formats (1rst-last) or in (range/bitmask).  
-D DICTIONARY, --dictionary DICTIONARY  
Dictionary file of subdomain and hostnames to use for  
enumeration.
```



ODYSSEUS OS



- **XRay como Ferramenta OSINT** O XRay é uma ferramenta projetada para a coleta de dados OSINT (inteligência de fontes abertas) voltada para reconhecimento e mapeamento de redes, facilitando a automação de tarefas iniciais. [source](#)
- **Pesquisa Online com X-Ray** A plataforma X-Ray oferece uma interface amigável, permitindo que tanto especialistas quanto iniciantes em OSINT busquem informações pessoais agregando dados de mais de 33 provedores. [source](#)
- **Guia do Framework OSINT** O X-Ray também apresenta um guia avançado para o framework OSINT, abrangendo fontes, ferramentas e links úteis para auxiliar na busca de dados de forma eficiente. [source](#)

```
Terminal - analistaosint@analistaosint-VirtualBox: ~
File Edit View Terminal Tabs Help
go: downloading github.com/moul/http2curl v1.0.0
go: downloading github.com/google/go-querystring v1.1.0
go: downloading golang.org/x/text v0.3.7
go: downloading github.com/leodido/go-urn v1.2.1
go: downloading github.com/go-playground/universal-translator v0.18.0
go: downloading golang.org/x/crypto v0.0.0-20210711020723-a769d52b0f97
go: downloading github.com/go-playground/locales v0.14.0
\_\_v\_\_
 \ RAY v 1.0.0b
 / by Simone 'evilsocket' Margaritelli
/\_/\_\_
Invalid or empty domain specified.
Usage of /opt/applications/XRay/build/xray:
  -address string
        IP address to bind the web ui server to. (default "127.0.0.1")
  -consumers int
```

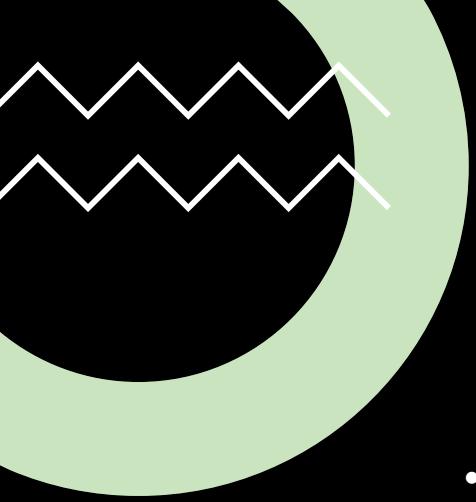
socket/xray

tool for recon, mapping and OSINT from public networks.



5 Issues 2k Stars 299 Forks



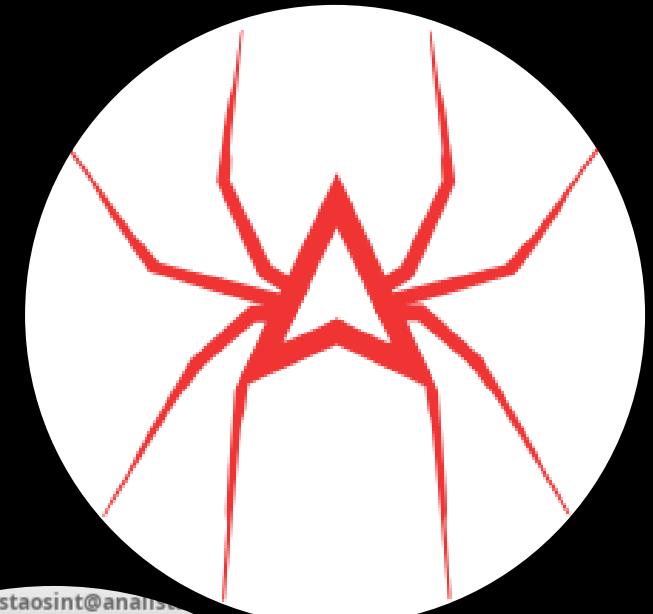


- **Photon como Ferramenta**

OSINT Photon é um crawleus de web projetado especificamente para inteligência de código aberto, permitindo uma análise profunda de websites. [source](#)

- **Análise Abrangente** O Photon pode escanear websites de forma abrangente, extraíndo dados valiosos durante o processo de coleta de informações. [source](#)

- **Personalização e Automação** Com uma interface simples e diversas opções de personalização, o Photon facilita a automação de tarefas OSINT. [source](#)



```
analistaosint@analistaosint:~/Desktop$ photon.py -h
usage: photon.py [-h] [-u ROOT] [-c COOK] [-r REGEX] [-e {csv,json}]
                 [-o OUTPUT] [-l LEVEL] [-t THREADS] [-d DELAY]
                 [-s SEEDS [SEEDS ...]] [-stdout STD]
                 [--user-agent USER_AGENT] [--exclude EXCLUDE]
                 [--timeout TIMEOUT] [-p PROXIES] [--clone] [--dns]
                 [--keys] [--update] [--only-urls] [--version]

optional arguments:
  -h, --help            show this help message and exit
  -u ROOT, --url ROOT  root url
  -c COOK, --cookie COOK
  -r REGEX, --regex REGEX
  -e {csv,json}, --export {csv,json}
  -o OUTPUT, --output OUTPUT
  -l LEVEL, --level LEVEL
  -t THREADS, --threads THREADS
  -d DELAY, --delay DELAY
  -s SEEDS [SEEDS ...], --seeds SEEDS ...
  -stdout STD, --stdout STD
  --user-agent USER_AGENT, --user-agent USER_AGENT
  --exclude EXCLUDE, --exclude EXCLUDE
  --timeout TIMEOUT, --timeout TIMEOUT
  -p PROXIES, --proxies PROXIES
  --clone, --clone
  --dns, --dns
  --keys, --keys
  --update, --update
  --only-urls, --only-urls
  --version, --version

  v1.3.2
```

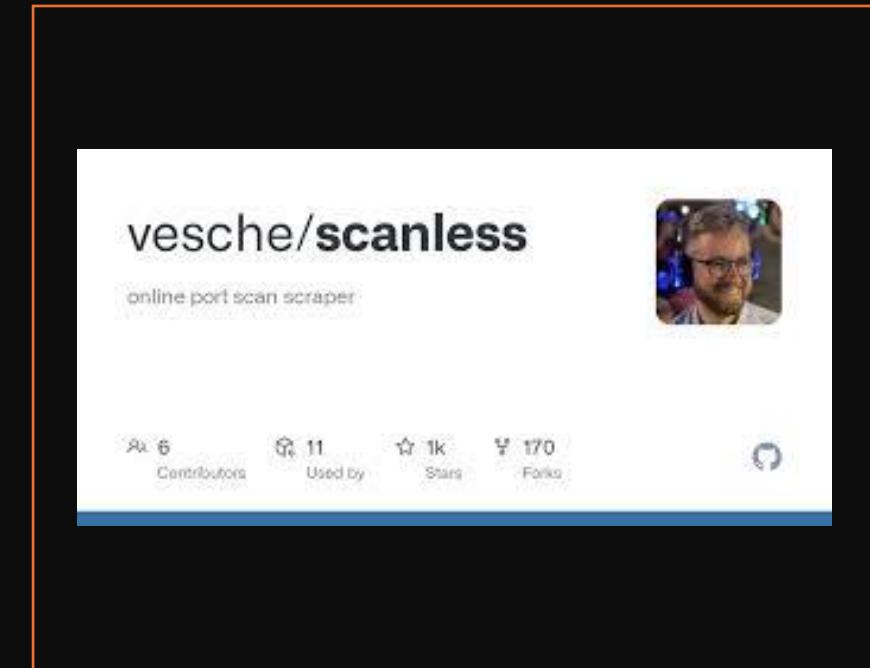


ODYSSEUS OS



- 🔎 **O que é Scanless?** Scanless é uma ferramenta automatizada desenvolvida na linguagem Python que permite realizar varreduras de portas em um host-alvo através de serviços online, garantindo anonimato na origem do escaneamento. [source](#)
- 🛡️ **Funcionalidade Principal** A principal função do Scanless é utilizar websites que realizam varreduras de portas em nome do usuário, ajudando em testes de penetração sem revelar o endereço IP do usuário. [source](#)

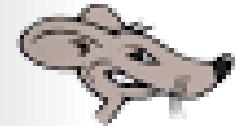
```
Terminal - analistaosint@analistaosint-VirtualBox:~  
File Edit View Terminal Tabs Help  
Using legacy 'setup.py install' for scanless, since package 'wheel' is not installed.  
Installing collected packages: urllib3, soupsieve, idna, colorama, charset-normalizer, certifi, requests, crayons, beautifulsoup4, scanless  
  Running setup.py install for scanless ... done  
Successfully installed beautifulsoup4-4.12.3 certifi-2024.8.30 charset-normalizer-3.4.0 colorama-0.4.6 crayons-0.4.0 idna-3.10 requests-2.32.3 scanless-2.2.1 soupsieve-2.6 urllib3-2.2.3  
usage: scanless [-h] [-v] [-t TARGET] [-s SCANNER] [-r] [-l] [-a] [-d]  
  
scanless, an online port scan scraper.  
  
options:  
-h, --help            show this help message and exit  
-v, --version         display the current version  
-t TARGET, --target TARGET  
                      ip or domain to scan  
-s SCANNER, --scanner SCANNER  
                      scanner to use (default: yougetsignal)  
-r, --random          use a random scanner  
-l, --list             list scanners  
-a, --all              use all the scanners  
-d, --debug            debug mode (cli mode off & show network errors)  
analistaosint@analistaosint-VirtualBox:~$
```



ODYSSEUS OS



lanrat/certgraph



An open source intelligence tool to crawl the graph
of certificate Alternate Names

- 🔎 **Definição do CertGraph** CertGraph é uma ferramenta de inteligência de código aberto que rastreia certificados SSL, criando um grafo dirigido onde cada domínio é um nó e os nomes alternativos do certificado para aquele domínio são as conexões. [source](#)
- 📊 **Visualização de Dados** O CertGraph permite visualizar a distribuição de nomes alternativos dos certificados, ajudando na análise de como diferentes domínios estão conectados através de seus certificados SSL. [source](#)

```
Terminal - analistaosint@analistaosint-VirtualBox: ~
File Edit View Terminal Tabs Help
Running setup.py install for censys ... done
Successfully installed OTXv2-1.5.12 censys-0.0.5 certifi-2024.8.30 charset-normalizer-3.4.0 click-8.1.7 colorama-0.4.6 dnspython-1.14.0 dshield-0.1 ez_setup-0.9.1 future-1.0.0 geoip2-2.4.0 idna-3.10 maxminddb-2.6.2 netaddr-1.3.0 passivetotal-0.30 python-dateutil-2.9.0.post0 pytz-2024.2 requests-2.32.3 shodan-1.5.5 simplejson-3.19.3 six-1.16.0 threatcrowd-0.4 urllib3-2.2.3 virustotal_api-1.1.2
usage: hostintel.py [-h] [-a] [-d] [-v] [-p] [-s] [-c] [-t] [-o] [-i] [-r]
                    ConfigurationFile InputFile
A modular application to look up host intelligence information. Outputs CSV to
stdout.
positional arguments:
ConfigurationFile      Configuration file
InputFile              Input file, one host per line (IP, domain, or FQDN
host name)
optional arguments:
-h, --help              show this help message and exit
-a, --all               Perform All Lookups.
-d, --dns               DNS Lookup.
-v, --virustotal        VirusTotal Lookup.
```

ODYSSEUS OS



- **O que é o WhatWeb?** O WhatWeb é um scanner web de última geração que identifica tecnologias de sites, respondendo à pergunta 'O que é esse site?'. [source](#)
- **Identificação de Tecnologias** Ele reconhece sistemas de gerenciamento de conteúdo (CMS), plataformas de blog, e muito mais, coletando informações detalhadas sobre o site. [source](#)
- **Segurança e Vulnerabilidades** O WhatWeb pode ser usado para identificar vulnerabilidades em sites, ajudando na análise de segurança.



```
h3ll0h4ll1: ~$ whatweb
WhatWeb - Next generation web scanner version 0.5.0.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles)
Homepage: https://www.morningstarsecurity.com/research/whatweb
```

```
Terminal - analistaosint@analistaosint-VirtualBox: ~
File Edit View Terminal Tabs Help
Usage: whatweb [options] <URLs>
<TARGETS> Enter URLs, hostnames, IP addresses, filenames or
          IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
          format.
          Read targets from a file.
--input-file=FILE, -i IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
          Read targets from a file.
--aggression, -a=LEVEL Set the aggression level. Default: 1.
          Makes one HTTP request per target and also
          follows redirects.
          1. Stealthy
          3. Aggressive
          If a level 1 plugin is matched, additional
          requests will be made.
--list-plugins, -l List all plugins.
--info-plugins, -I=[SEARCH] List all plugins with detailed information.
          Optionally search with a keyword.
--verbose, -v Verbose output includes plugin descriptions.
Note: This is the short usage help. For the complete usage help use -h or --help
analistaosint@analistaosint-VirtualBox: ~
```



- **💡 O que é o Metagoofil?** O Metagoofil é uma ferramenta de coleta de informações projetada para extrair metadados de arquivos públicos como PDF, DOC, XLS, PPT, entre outros. [source](#)
- **🔍 Funcionalidades** Ele permite buscar no Google por tipos específicos de arquivos hospedados publicamente em websites e pode baixar esses arquivos. [source](#)
- **🔒 Importância para a análise de documentos** A ferramenta desempenha um papel crucial na análise de documentos disponíveis na internet, facilitando a obtenção de informações relevantes de forma automatizada.

```
File Edit View Search Terminal Help
root@kali:~# mkdir arquivos
root@kali:~# cd arquivos/
root@kali:/arquivos# metagoofil -d microsoft.com -t docx,pdf -l 500 -n 20 ~> msf
root@kali:/arquivos# ./metagoofil.py -d microsoft.com -t docx,pdf -l 500 -n 20 ~> msf
[+] Metagoofil Ver 2.2
[+] Christian Martorella
[+] Edge-Security.com
[+] cmartorella_at_edge-security.com
[+] Starting online search...
[-] Starting online search...
[-] Searching for docx files, with a limit of 500
    Searching 100 results...
    Searching 300 results...
    Searching 500 results...
certifi, requests, beautifulsoup4, google
Successfully installed beautifulsoup4-4.12.3 certifi-2024.8.30 charset-normalizer-3.4.0 google-3.0.0 idna-3.10 requests-2.32.3 soupsieve-2.6 urllib3-2.2.3
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f [SAVE_FILE]] [-i URL_TIMEOUT] [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] -t FILE_TYPES [-u [USER_AGENT]] [-w]
Metagoofil v1.2.0 - Search Google and download specific file types.

options:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small Google may block your IP, too big and your search may take a while. Default: 30.0
  -f [SAVE_FILE]         Save the html links to a file.
                        no -f = Do not save links
                        -f = Save links to html_links_<TIMESTAMP>.txt
                        -f SAVE_FILE = Save links to SAVE_FILE
  -i URL_TIMEOUT        Number of seconds to wait before timeout for unreachable/stale pages. Default: 15
  -l SEARCH_MAX          Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
  -o SAVE_DIRECTORY      Directory to save the downloaded files.
  -r NUMBER_OF_THREADS  Number of threads to use for concurrent downloads. Default: 10
  -t FILE_TYPES          File types to search for. Default: docx,pdf
  -u [USER_AGENT]        User agent to use for the requests. Default: 'Metagoofil/2.2 (+https://github.com/ChristianMartorella/Metagoofil)'
```

The image shows a desktop interface for the Odysseus OS. On the left, there's a search bar with a magnifying glass icon and a list of application icons with their names: Browse Mirrored Websites, Firefox Web Browser, Google Chrome, Google Earth, HexChat, JDDownloader, Links 2, Parabolic, Remmina, Thunderbird Mail, Tor Browser, Tor Browser Launcher Settings, Transmission, and WebHTTrack Website Copier. Below this is a user profile icon labeled "analistaosint". A sidebar on the right lists categories like Busca, Busca de, Development, DNS, Framework, Games, Graphics, Internet, Multimedia, Navega, Network, and Of. Two "Add Download" dialogs are overlaid on the screen. Both dialogs have "File Type" set to MP4 (Video), "Quality" set to Best, and "Audio Language" set to Default. The first dialog has "Subtitles" and "Advanced Options" expanded. It shows a save folder of "/home/analistaosint/Downloads" and a file name "TESTE A VELOCIDADE DE SUA LE". The second dialog also has "Subtitles" and "Advanced Options" expanded, with a "Name" field containing "TESTE A VELOCIDADE DE SUA LE". Both dialogs have a "Download" button at the bottom.

analistaosint

- Na distribuição Odysseus, existem várias ferramentas específicas que podem ser utilizadas para extrair vídeos e informações de fontes na web, úteis no contexto de OSINT.



- **SpeechNote** é uma ferramenta de IA projetada para reconhecimento de áudio e degravação de fala. Aqui estão alguns dos principais recursos e funcionalidades dessa ferramenta:
- **Reconhecimento de Fala:** Converte áudio em texto com alta precisão, suportando vários idiomas.
- **Interface Intuitiva:** Oferece uma interface fácil de usar, permitindo que os usuários gravem ou façam upload de arquivos de áudio para degravação.
- **Edição de Texto:** Após a conversão, os usuários podem editar o texto gerado diretamente na plataforma.
- **Exportação de Arquivos:** Permite exportar o texto em diferentes formatos, como .txt ou .docx, facilitando o compartilhamento e a utilização do conteúdo.

Speech Note

Type to search

Português / pt

Português (Coqui MMS) / pt

Português brasileiro (Piper Edresson Low Male) / pt

Português brasileiro (Piper Faber Medium Male) / pt

Português (Piper Tugão Medium Male) / pt

Português brasileiro (RHVoice Letícia) / pt

Português (ESpeak Robot) / pt

Português brasileiro (ESpeak Robot) / pt

Close

Speech Note

Action in the settings.

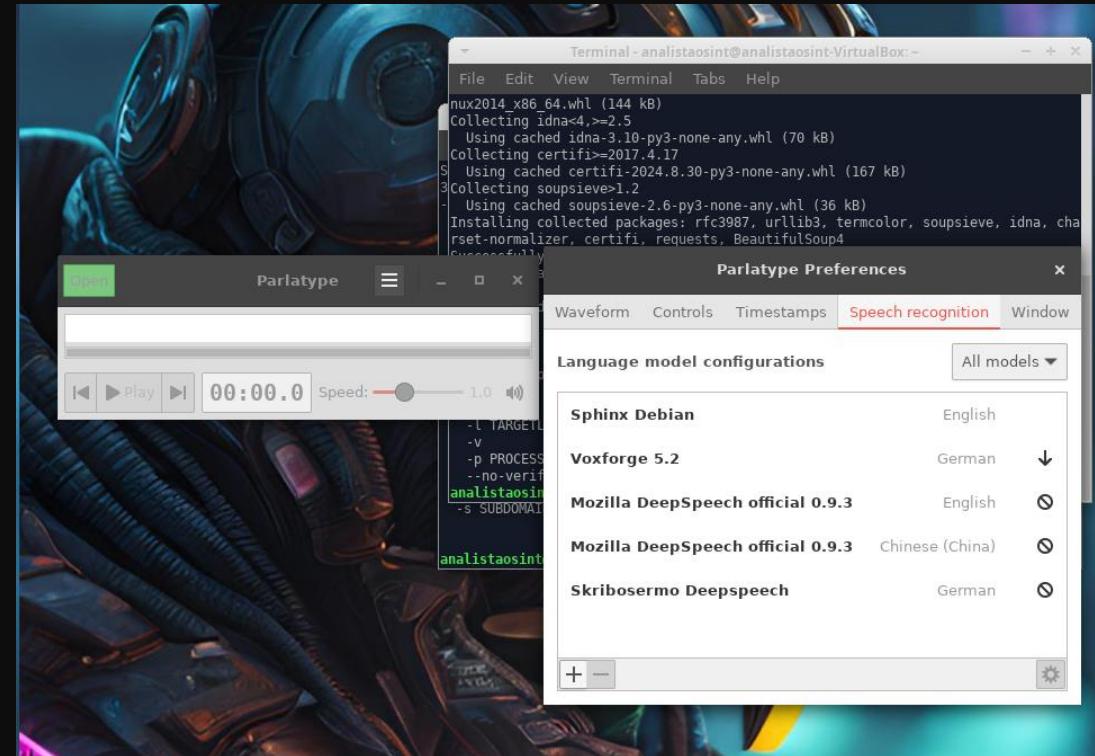
No Text to Speech model

Speech Note

Português (Coqui MMS) / pt

ODYSSEUS OS

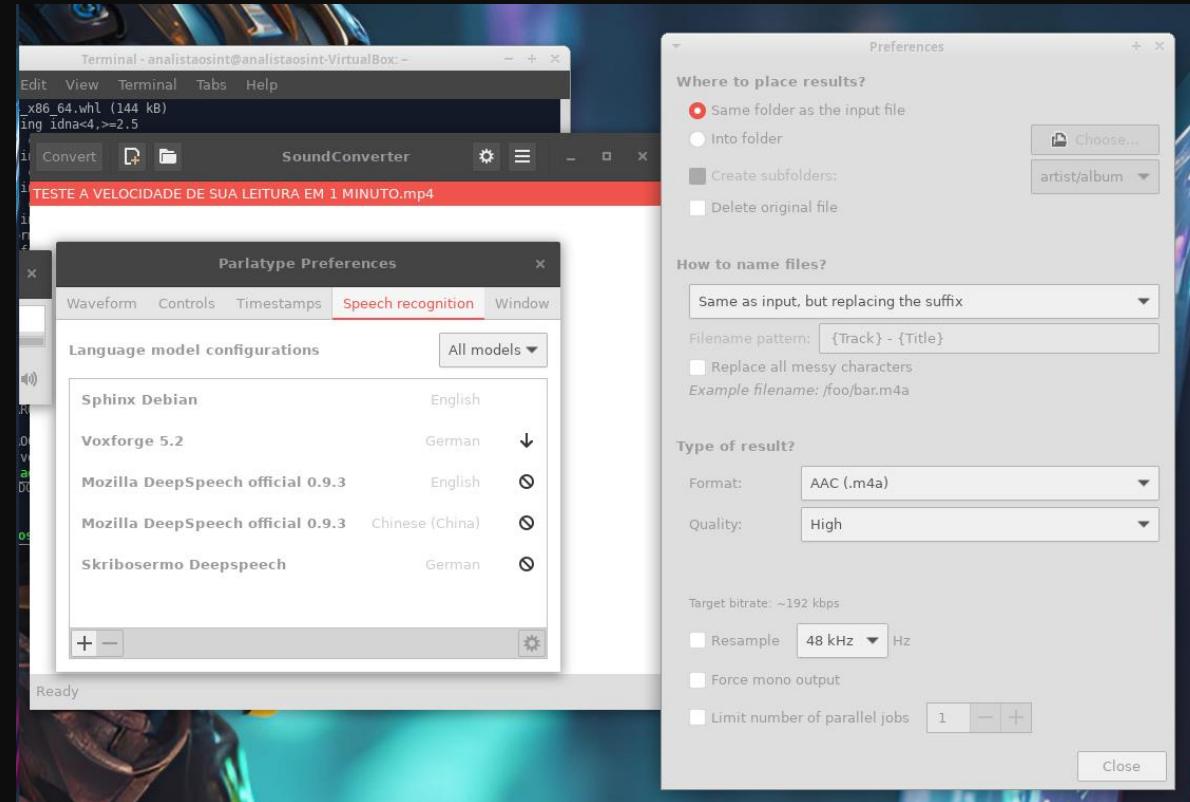
- **Parlatype** é uma ferramenta de código aberto projetada para facilitar a transcrição de áudio. Aqui estão alguns dos principais recursos e funcionalidades do Parlatype:
 - **Transcrição de Áudio:** Permite a reprodução de arquivos de áudio enquanto o usuário digita a transcrição, facilitando o processo.
 - **Interface de Usuário Simples:** Oferece uma interface intuitiva, tornando a transcrição mais eficiente e menos cansativa.
 - **Controles de Reprodução:** Possui controles de reprodução, como pausar, retroceder e avançar rapidamente, que ajudam a sincronizar a digitação com o áudio.



ODYSSEUS OS



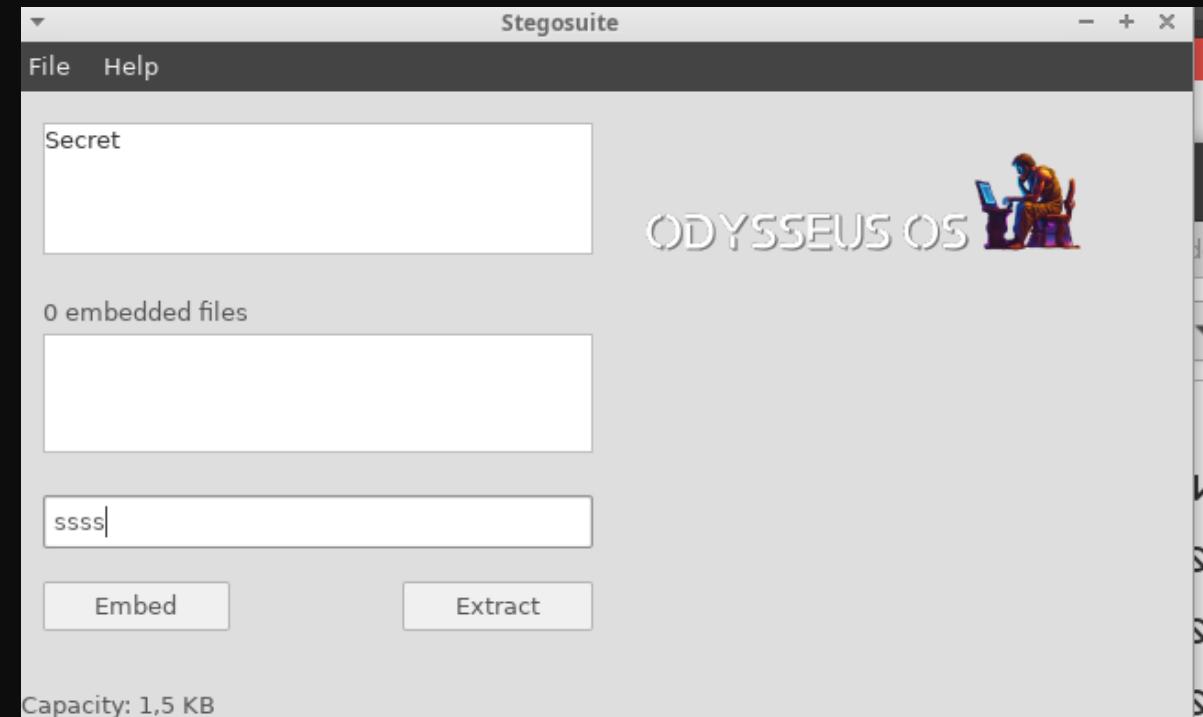
- A distribuição Odysseus inclui várias ferramentas que podem ser utilizadas para conversão de áudio e vídeo. Aqui estão algumas delas:
- **FFmpeg**: Uma ferramenta poderosa e versátil para conversão de áudio e vídeo. Permite a conversão entre diferentes formatos, extração de áudio de vídeos e muito mais.
- **Audacity**: Embora seja principalmente um editor de áudio, o Audacity permite a importação de arquivos de vídeo para extrair a trilha sonora e exportá-la em diferentes formatos.
- Essas ferramentas disponíveis na distribuição Odysseus são úteis para quem precisa realizar tarefas de conversão de áudio e vídeo em investigações de OSINT ou para outras finalidades.



ODYSSEUS OS



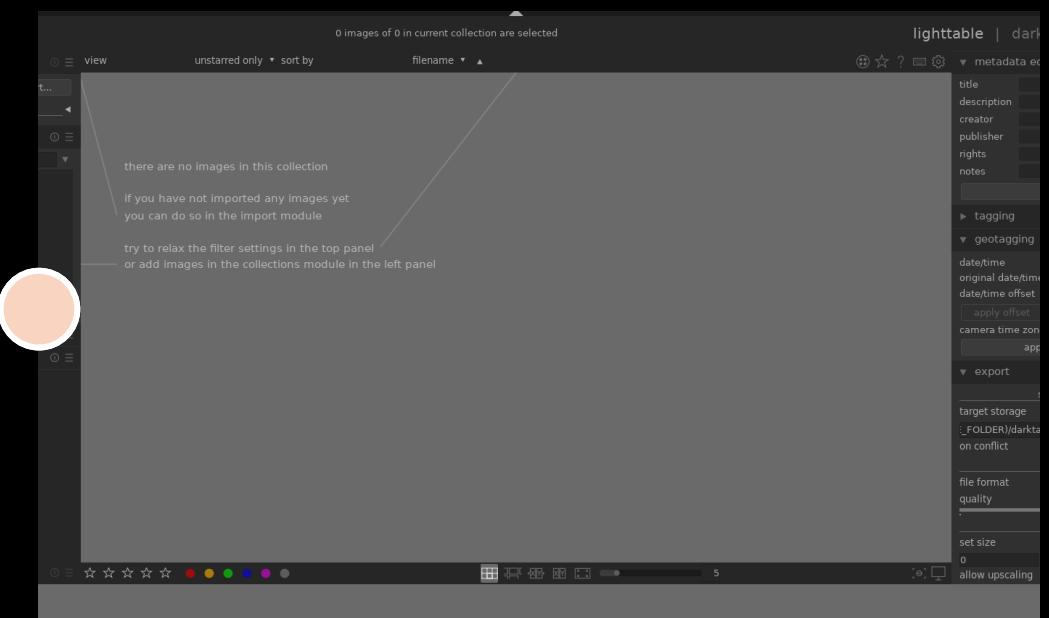
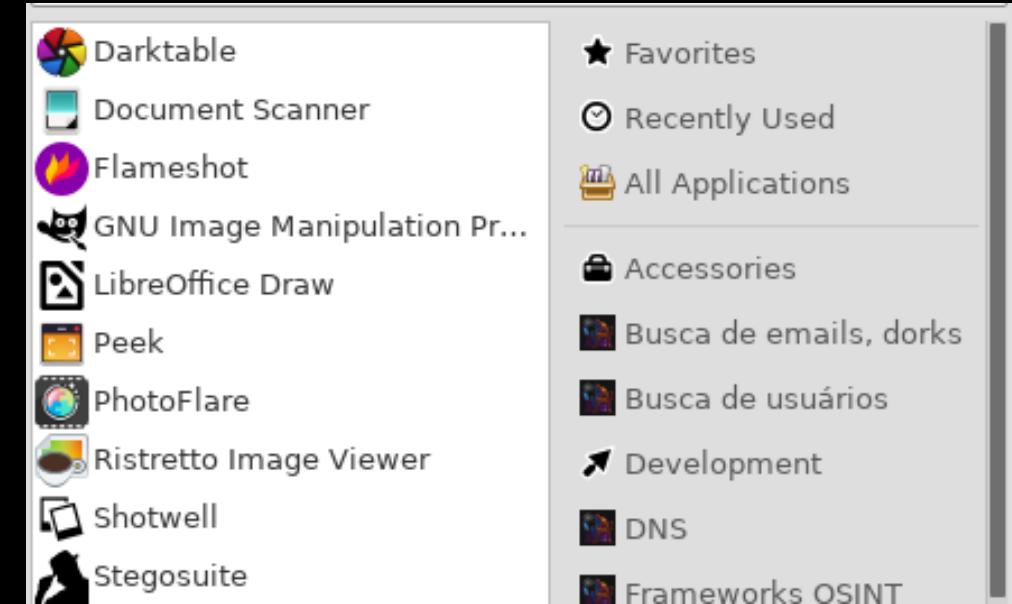
- **SteganoSuite** é uma ferramenta de código aberto projetada para a esteganografia, que é a prática de ocultar informações dentro de arquivos de mídia, como imagens e áudios. Aqui estão algumas das principais características e funcionalidades do SteganoSuite:
 - **Características do SteganoSuite**
 - **Ocultação de Dados:**
 - Permite ocultar mensagens ou arquivos dentro de imagens e sons sem que isso seja perceptível.
 - **Extração de Dados:**
 - Possibilita a extração de dados ocultos de arquivos de mídia.
 - **Suporte a Vários Formatos:**
 - Suporta diversos formatos de imagem (como BMP, PNG, JPG) e áudio (como WAV).



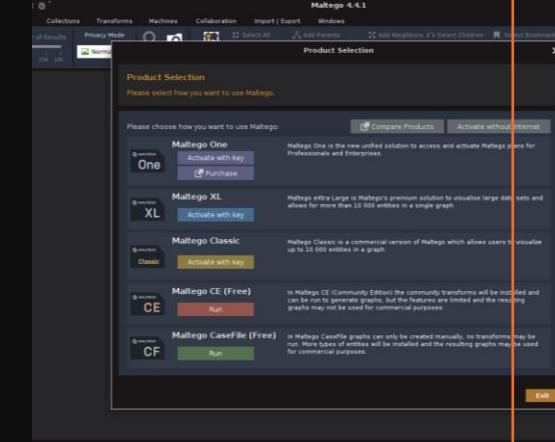
ODYSSEUS OS



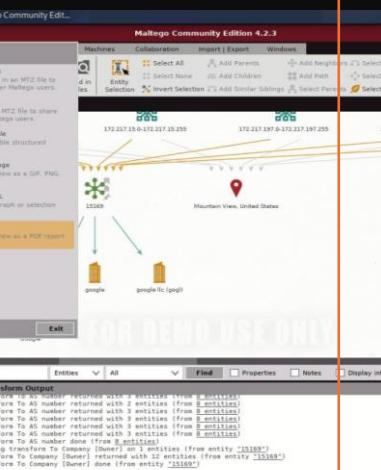
- Na distribuição Odysseus, você pode encontrar algumas dessas ferramentas pré-instaladas ou disponíveis para instalação. Aqui estão algumas que geralmente vêm na distro:
- **Ferramentas de Edição de Imagens**
- **GIMP**: Geralmente incluído nas distribuições, é uma ferramenta poderosa para edição de imagens.
- **Ferramentas de Gravação e Captura de Tela**
- **Peek**: Pode estar disponível para captura de tela e gravação de vídeo.
- **Flameshot**: Normalmente incluído, é uma ferramenta prática para captura de tela com anotações.

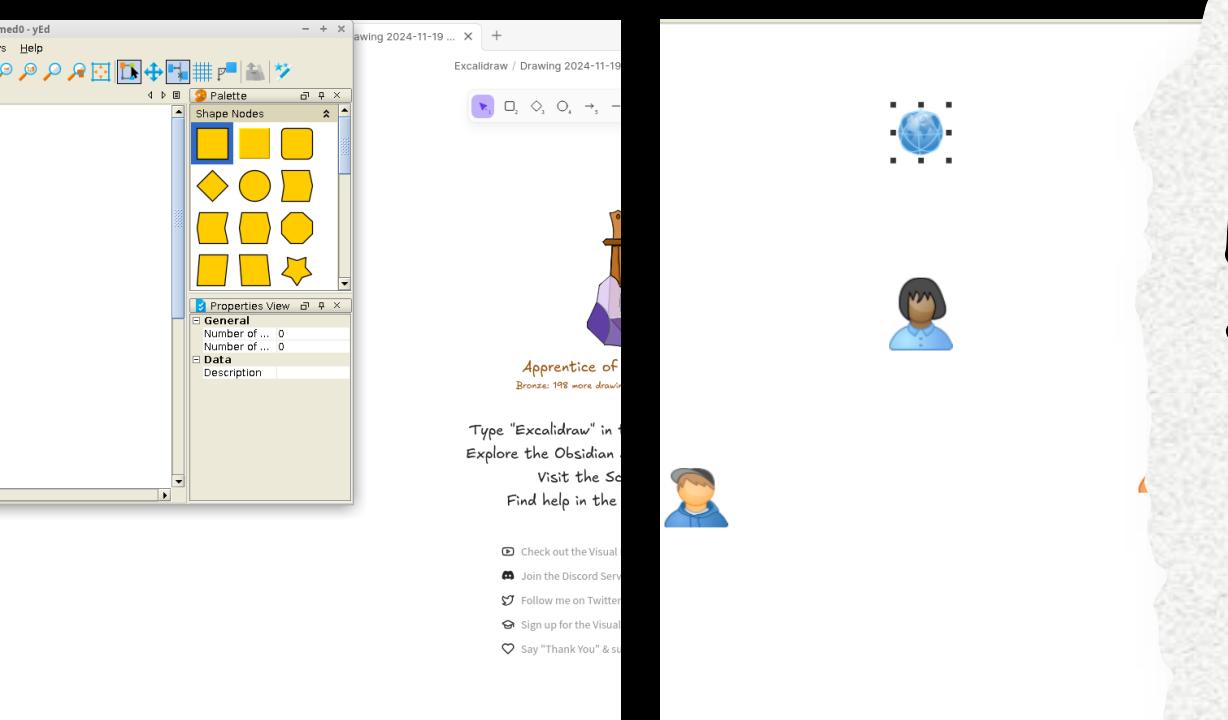
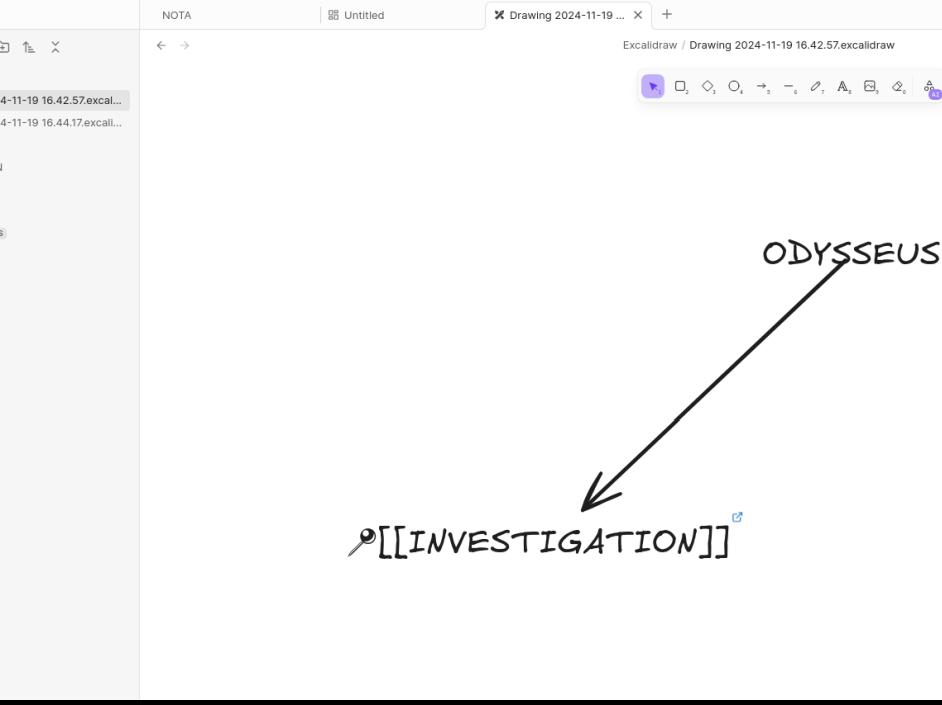


ODYSSEUS OS



- 🔎 **Maltego** é uma plataforma de investigação que acelera investigações cibernéticas complexas, permitindo a mineração e mapeamento de dados de forma eficiente.
- 📊 **Análise Gráfica** Esta ferramenta fornece uma análise detalhada de links e coleta de informações em tempo real, facilitando a visualização de relações entre dados. [source](#)

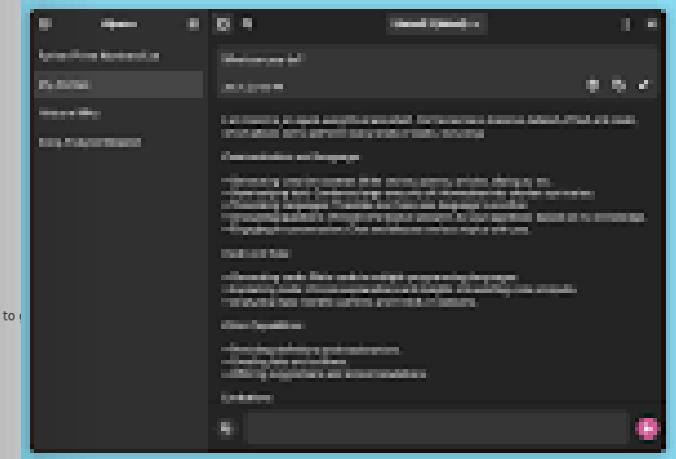
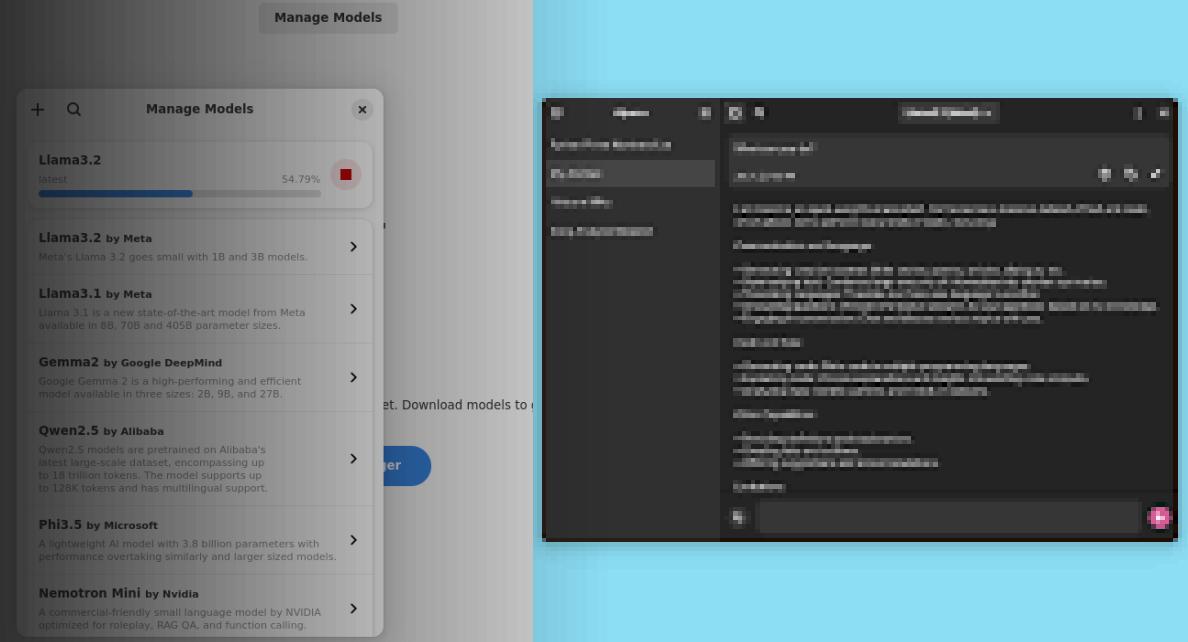




Obsidian e yEd

- Ambas as ferramentas são poderosas para organizar informações e visualizar dados de maneira eficaz. O Obsidian é ótimo para anotações e gerenciamento de conhecimento, enquanto o yEd é ideal para diagramas e visualizações.

-  **Instalação do Alpaca** Alpaca é um cliente Ollama que permite interagir com modelos de IA localmente, oferecendo uma forma simples e intuitiva para usuários iniciantes. [source](#)
-  **Funcionalidades** Com o Alpaca, você pode gerenciar e conversar com múltiplos modelos, além de puxar e deletar modelos conforme sua necessidade.



Alpaca

It looks like you don't have any models downloaded yet. Download models to get started

[Open Model Manager](#)


Socialize

Learn

Develop
Editor's Choice**Vivaldi**

A Powerful. Personal.
Private. web browser

Marble

Virtual Globe

Noson

The essential to control
music from your SONOS...

GNU Image Manipula...

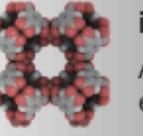
GNU Image Manipulation
Program

cantor

KDE Frontend to
Mathematical Software

**Eye of GNOME**

Eye of GNOME Image
Viewer

**iraspa**

A molecular visualizer/
editor

**datagrip**

DataGrip

**opentofu**

OpenTofu is a declarative
language for infrastructure

**Sublime Text**

Meet a new code editor
from the makers of Atom.

**FreeCAD**

An open source parametric
3D CAD system

**VLC**

The ultimate media
player

ODYSSEUS OS



- Odysseus pré-configurado com várias ferramentas úteis para tarefas de segurança e investigação, incluindo suporte para **Snap**, **apt-get** e **Flatpak**. Isso facilita a instalação de programas open source diretamente.

Ferramentas Pré-Configuradas

- **Snap**: Permite a instalação de aplicativos de forma simples.
- **apt-get**: Usado para gerenciar pacotes Debian.
- **Flatpak**: Suporta a instalação de aplicativos em sandbox.

New & Updated

Odysseus é frequentemente retratado como o "homem pensante" na literatura, especialmente na "Odisseia" de Homero. Ele é conhecido por sua astúcia e inteligência, utilizando seu intelecto para superar desafios e enganar adversários, como o famoso episódio do Cavalo de Tróia. Sua habilidade de pensar estrategicamente e resolver problemas complexos faz dele uma figura emblemática da astúcia e da sabedoria.

