



## OriON

---

OriON is a virtual machine based on Linux Ubuntu 22.10.

This '.ovf' has integrated different tools for research of information collection in open sources (OSINT) on people.



## Browsers

---

It has **3 different browsers (Chrome, Firefox and Tor)** with their respective bookmarks and web extensions.

Browser bookmarks are categorized:

- Email
- Domains
- Geolocation
- Google
- Identity
- IP
- Mozilla Firefox
- Media
- Browsers
  - o General
  - o Dark Web
- Social networks
  - o Twitter
  - o Instagram
  - o Facebook
  - o YouTube
  - o Other

- Phones
- Tor Project
- Users

## Tools

---

It has **application tools** for the researcher:

- Audacity
- Evince
- Google Earth
- HTTrack
- KeePassxc
- Maltego
- Notepad++
- Terminator
- VLC
- Xmind
- Others.



Finally, it has a variety of tools installed, which can be run directly from the command line.

In fact, to facilitate the use of these tools, the virtual machine has a **script**, called '**OriON**' in the path '**/home/orion/Escritorio/Herramientas**', to facilitate its execution.

## Execution of the script:

---

```
cd /Escritorio/Herramientas
```

```
sudo ./OriON
```

```
orion@orion:~$ cd Escritorio/Herramientas/
orion@orion:~/Escritorio/Herramientas$ sudo ./OriON
```

The **tools** are:

- **Alias\_generator**: generates nicknames based on known target information.
- **Checkfy**: guess possible emails based on a list of nicknames.
- **CloudFail**: finds IPs hidden behind the CloudFlare network.
- **Dmitry**: collects information from public sources of domains and IP addresses.
- **DNSRecon**: discover information about hosts and networks through DNS queries.
- **Domainfy**: finds domains that resolve using a word or nickname.
- **Elasticsearch**: search engine and data analysis.
- **EO-Ripper**: makes OSINT to an email or an email list.
- **Exiftool**: extracts metadata from images, files, or documents.
- **Instaloader**: allows downloads of any Instagram data.
- **Kibana**: data visualization.
- **Mailfy**: find out more about emails.
- **Maltego**: data analysis.
- **MediaInfo**: extracts metadata from media files: audio or video.
- **Phonefy**: retrieves mobile phone information.
- **ProtOSINT**: investigates ProtonMail accounts and IP addresses linked to ProtonVPN.
- **SE Toolkit**: social engineering.
- **Searchfy**: finds profiles linked to a full name.
- **Sherlock**: Searches social media accounts by username.
- **SpiderFoot**: collects and analyses data.
- **TheHarvester**: collects various information through a domain.
- **Tinfoleak**: Twitter public information analysis.
- **Usufy**: identifies social media profiles using a nickname.
- **WebScape**: collects emails and phone numbers from websites.



```
OSINT

[*] Autor : CL4rk-S
[*] Version : 1.0
[*] Última actualización : 2022/04/04

=====
Menú principal
=====

(1) Herramientas
  (1) Checkfy: sugiere posibles correos electrónicos basados en una lista de apodos.
  (2) EO-Ripper: hace OSINT a un email o a una lista de emails.
  (3) Mailfy: encuentra más información sobre los correos electrónicos.
  (4) ProtOSINT: investiga cuentas de ProtonMail y direcciones IP vinculadas a ProtonVPN.
  (5) SpiderFoot: recopila y analiza datos.
  (6) Tinfoleak: Análisis de información pública de Twitter.
  (7) WebScape: recoge correos y números de teléfono de páginas web.

(2) Dominios
  (1) CloudFail: encuentra IP ocultas detrás de la red CloudFlare.
  (2) Dmitry: recopila información de fuentes públicas de dominios y direcciones IP.
  (3) Domainfy: encuentra dominios que se resuelven usando una palabra o apodo.
  (4) Searchfy: encuentra perfiles vinculados a un nombre completo.
  (5) SpiderFoot: recopila y analiza datos.
  (6) TheHarvester: recopila diversa información a través de un dominio.
  (7) Tinfoleak: Análisis de información pública de Twitter.

(3) Búsqueda
  (1) Alias_generator: genera apodos basados en información conocida sobre el objetivo.
  (2) Searchfy: encuentra perfiles vinculados a un nombre completo.
  (3) Sherlock: busca nombres en gran cantidad de redes sociales por nombre de usuario.
  (4) Tinfoleak: Análisis de información pública de Twitter.

(4) IP
  (1) CloudFail: encuentra IP ocultas detrás de la red CloudFlare.
  (2) Dmitry: recopila información de fuentes públicas de dominios y direcciones IP.
  (3) ProtOSINT: investiga cuentas de ProtonMail y direcciones IP vinculadas a ProtonVPN.
  (4) SpiderFoot: recopila y analiza datos.
  (5) Tinfoleak: Análisis de información pública de Twitter.

(5) Multimedia
  (1) Exiftool: extrae metadatos de imágenes, archivos o documentos.
  (2) MediaInfo: extrae metadatos de archivos multimedia: audio o video.
  (3) Tinfoleak: Análisis de información pública de Twitter.

(6) Redes Sociales
  (1) Instaloader: permite descargas de cualquier dato de Instagram.
  (2) SpiderFoot: recopila y analiza datos.
  (3) Tinfoleak: Análisis de información pública de Twitter.

(7) Telefonos
  (1) Phonefy: recupera información sobre teléfonos móviles.
  (2) Tinfoleak: Análisis de información pública de Twitter.
  (3) WebScape: recoge correos y números de teléfono de páginas web.

(8) Usuarios
  (1) Alias_generator: genera apodos basados en información conocida sobre el objetivo.
  (2) Searchfy: recopila y analiza datos.
  (3) Sherlock: busca nombres en gran cantidad de redes sociales por nombre de usuario.
  (4) Tinfoleak: Análisis de información pública de Twitter.
  (5) Usufy: identifica perfiles de redes sociales usando un apodo.

(9) Otros
  (1) Elasticsearch: motor de búsqueda y análisis de datos.
  (2) Kibana: visualización de datos.
  (3) Maltego: análisis de datos.
  (4) SE Toolkit: ingeniería social.

(10) Otros
  (1) Tinfoleak: Análisis de información pública de Twitter.

=====
Elija su opción [0-9]:
```

## DOWNLOAD

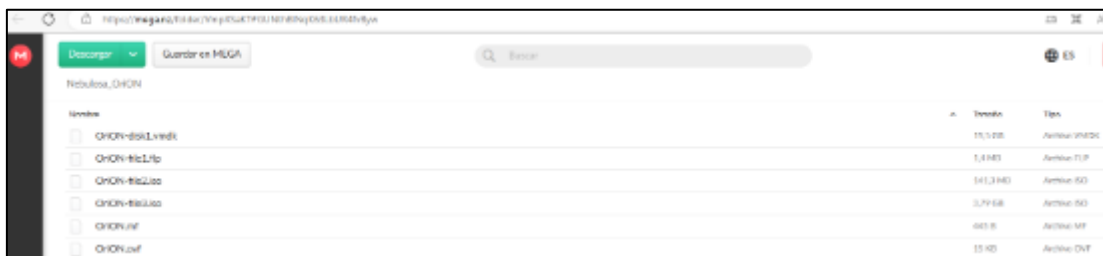
**Important:** As a good OSINT researcher, you need to use a VPN. None are offered specifically in the distribution because that is usually the choice of the analyst. Anyway, here are 5 different options:

- **ExpressVPN:** is one of the most popular on the market, has an official application for Linux and has a lot of advanced configuration options for more technical users.
- **NordVPN:** has a solid reputation for privacy and security, it also has an official Linux app and has a dual VPN option that adds an extra layer of security.
- **ProtonVPN:** is based on privacy and security and has a limited free plan for those who want to try the service.
- **CyberGhost:** It has a lot of configuration options, including a privacy mode to further protect your online identity.
- **Mullvad:** focuses on maintaining user privacy to the fullest, including the option to pay with cryptocurrencies.

**Now:** To start using it, just download it:

<https://mega.nz/folder/VmpXSaKT#GUNthBINqK63LbUR4fvByw>

- **User:** orion
- **Password:** orion



## DEMO

The following link provides a video demonstration of the distribution:  
<https://youtu.be/rTYlaGtA2tE>



I hope you can enjoy it as much as I have enjoyed doing it.