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:

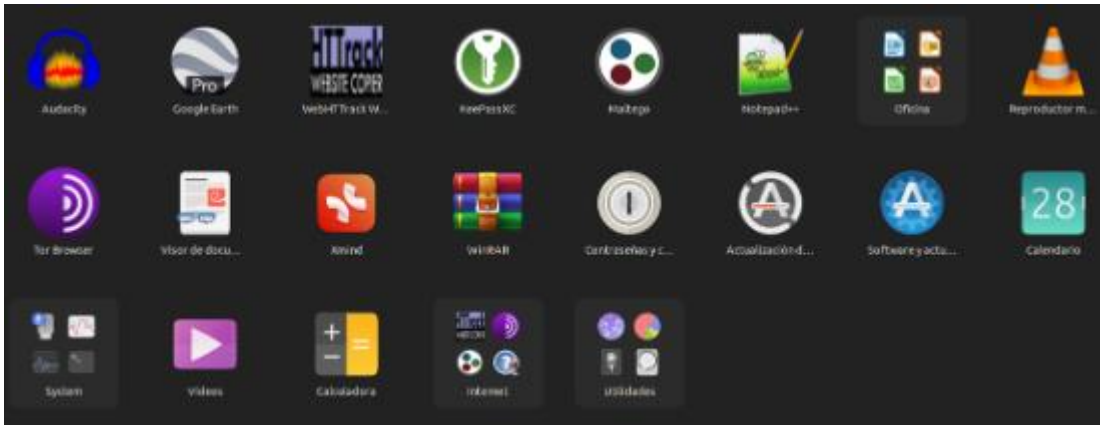
- Email
- Domains
- Geolocation
- Google
- Identity
- IP
- Mozilla Firefox
- Media
- Browsers
    - General
    - Dark Web
- Social networks
    - Twitter
    - Instagram
    - Facebook
    - YouTube
    - Other

- 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:

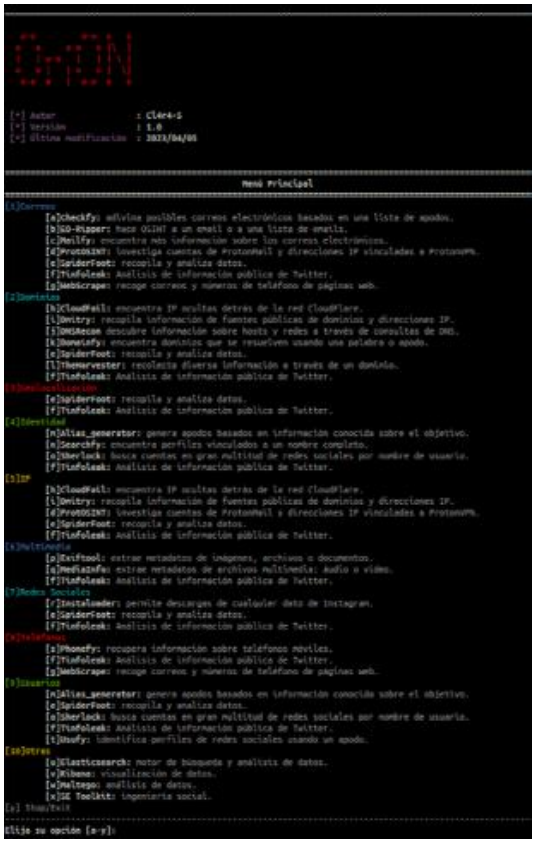
```
cd /Escritorio/Herramientas

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.
- **WebScrape**: collects emails and phone numbers from websites.



DOWNLOAD

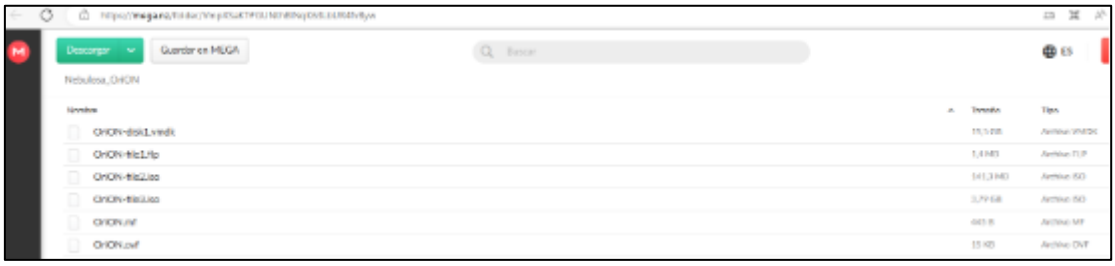
Important: As a good OSINT researcher, you need to use a VPN. None are offered specifically in the distribution because that is usually the choice of the analyst. Anyway, here are 5 different options:

- **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:

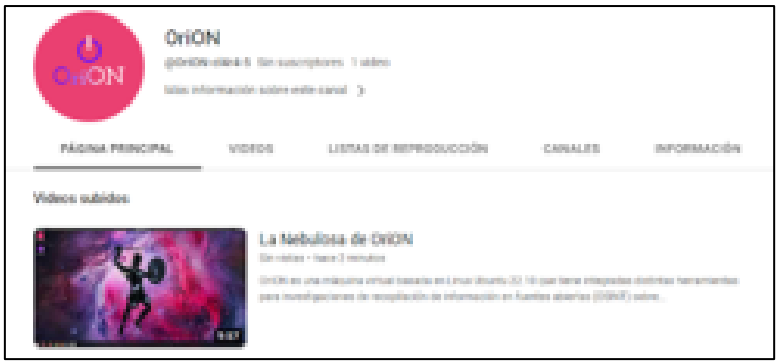
https://mega.nz/folder/VmpXSaKT#GUNthBlNqK63LbUR4fvByw

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



DEMO

The following link provides a video demonstration of the distribution: https://youtu.be/rTYIaGtA2tE



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