

**C.M**

Ahmed Hassan Khamis  
Eduardo López Esteban

**2º ASIR**



CONSEJERÍA DE EDUCACIÓN  
E INVESTIGACIÓN

**Comunidad de Madrid**

## ÍNDICE

|  |    |
|--|----|
| 1. INTRODUCCIÓN.....                             | 3  |
| 2. DESCRIPCIÓN.....                              | 4  |
| 3. JUSTIFICACIÓN.....                            | 5  |
| 4. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS..... | 6  |
| 5. CALENDARIO.....                               | 7  |
| 6. APARTADOS DEL PROYECTO.....                   | 8  |
| HERRAMIENTAS.....                                | 13 |
| ELK.....   | 13 |
| MISP.....  | 22 |
| CORTEZA.....                                     | 37 |
| JUEGO PHP-Mysql.....                             | 41 |
| 7. CÓDIGO.....                                   | 47 |
| 8. CONCLUSIÓN.....                               | 56 |
| 9. BIBLIOGRAFÍA.....                             | 57 |

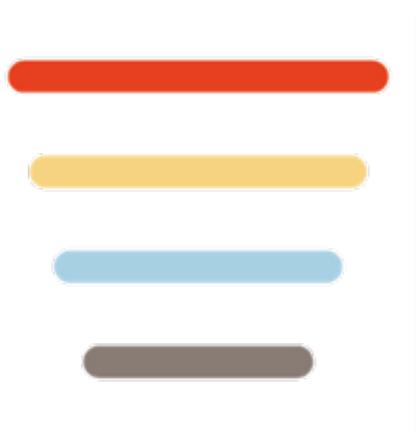
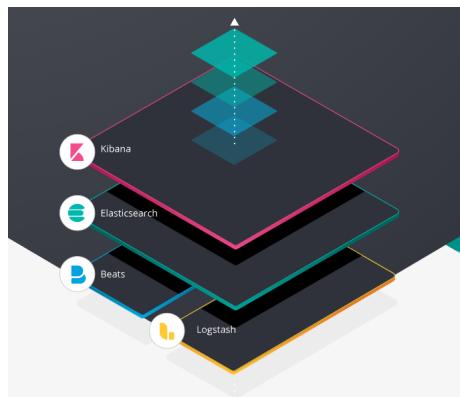
## 1. INTRODUCCIÓN

La informática es un conocimiento básico en la sociedad actual, y esta siempre está en continuo desarrollo, por lo que nuevas herramientas y programas son desarrollados y lanzados al mercado, con el objetivo de satisfacer las necesidades de las empresas o de personas. Por ello, hemos elaborado nuestro proyecto en torno a poder enseñar un poco el tipo de herramientas que se utilizan hoy en día y su funcionamiento.

Para poder enseñar estas herramientas nos hemos apoyado de un programa creado por nosotros con una interfaz gráfica que permite el poder navegar entre estas herramientas con la mayor comodidad y rapidez que hemos podido conseguir.

Esta idea ha surgido, como ya hemos mencionado anteriormente, a partir de que hemos notado, que hoy en día hay muchas herramientas, programas y demás de gran utilidad que facilitan en gran parte las diferentes “zonas” de la informática, ya sean las bases de datos, la ciberseguridad, redes y demás. Por lo que centrar nuestro proyecto en indagar en algunas de estas herramientas nos ha parecido muy buena idea para también darlas a conocer.

Además hemos querido implementar un “juego” de PHP para abarcar también el tema de la programación y que el usuario tenga en el programa una opción entretenida con la que aprender.

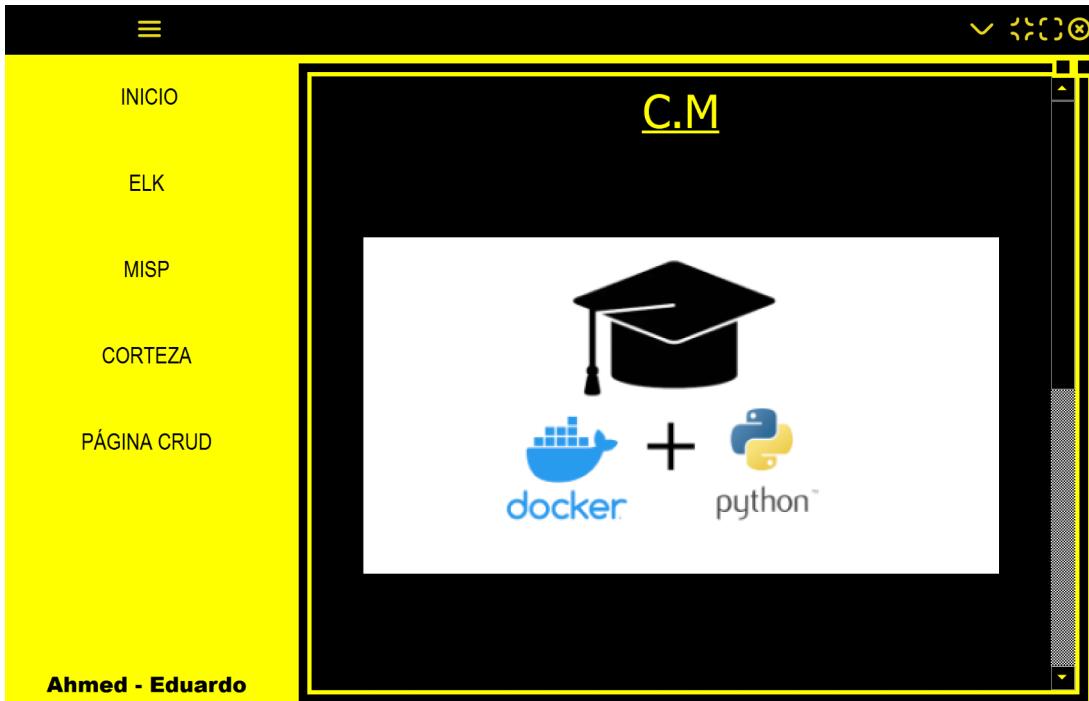


## 2. DESCRIPCIÓN

La descripción del proyecto es la siguiente:

Hemos querido llamar al proyecto Continens Melius ya que en latín, porque tiene un significado que hace relación a la mejora general que hacen los contenedores a la informática y por ese hecho los hemos implementado a nuestro programa.

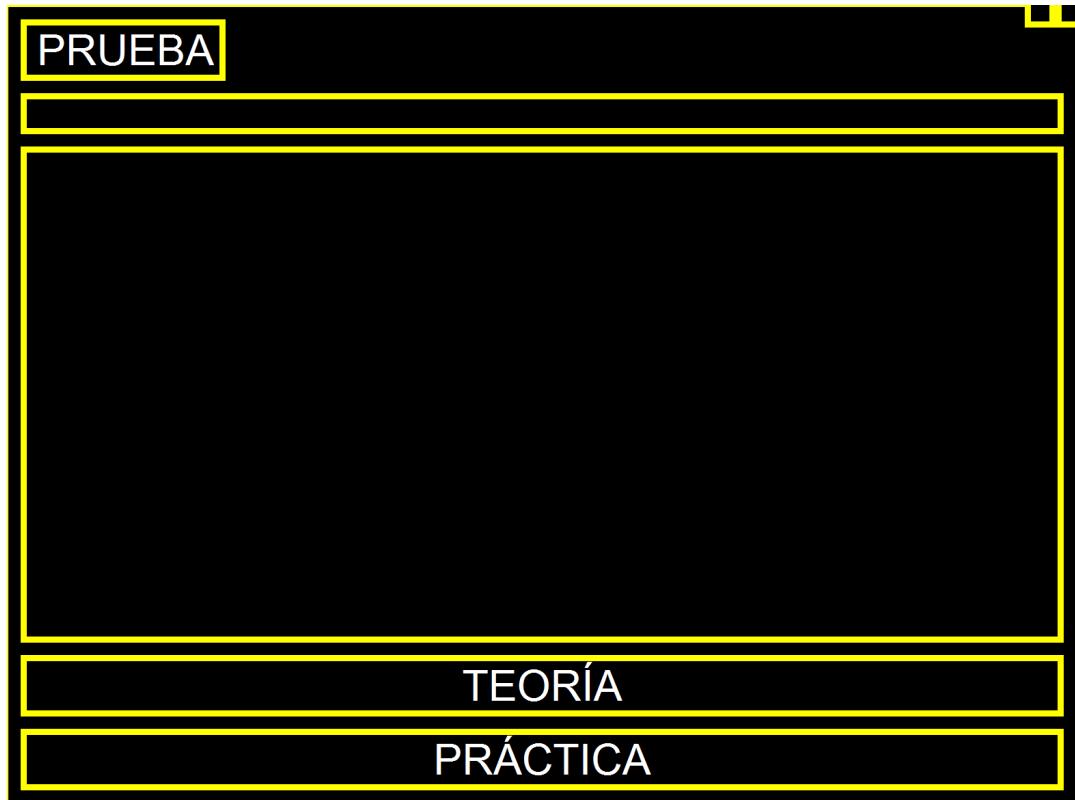
El proyecto tendría como base hacer dicho programa en forma de ejecutable, construido por nosotros desde 0 con la ayuda de PyQt5, que nos ha resultado una herramienta muy cómoda en la que hemos podido elaborar nuestro programa, aprendiendo como funcionaba esta. A partir de este programa, al iniciarla se abriría al usuario, un menú con acceso a las diferentes herramientas que hemos querido implementar en nuestro proyecto.



Al querer acceder a estas herramientas, en cada una se abriría una página en la que se daría una breve explicación de cada herramienta y sus respectivos apartados de *TEORÍA* y *PRÁCTICA*.

Al pulsar en el apartado *TEORÍA* se abriría al usuario un PDF realizado por nosotros con la documentación necesaria para poder realizar instalaciones pruebas y demás con esa herramienta.

Al pulsar en el apartado *PRÁCTICA* se iniciaría el docker correspondiente a la herramienta, en el que se encontrarían los medios necesario para poder hacer uso de dicha herramienta y comprobar su funcionamiento, y hacer pruebas si el usuario quiere, guiado siempre de la parte de *TEORÍA* en el que se encuentra el PDF de la herramienta.



### 3. JUSTIFICACIÓN

Como ya hemos tratado antes, este proyecto está orientado a la idea de que en el grado de ASIR no se puede dar todas las cosas que se pueden ver en relación a las asignaturas y a los medios relacionados con ellas, debido a la falta de tiempo, y que con el paso del tiempo es mayor el número de herramientas o innovaciones que van habiendo respecto a cada campo de la informática.

Por lo que con este proyecto tratamos de ver ciertas herramientas, que con los conocimientos adquiridos en ASIR, se puedan ver en profundidad y se sepan entender, y que incluso el usuario tenga la oportunidad de montar la propia herramienta. También consideramos que son herramientas útiles para empresas y para su administración por lo que vemos de utilidad el indagar en ellas.

## **4. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS**

-Objetivo general: nuestro objetivo general es implementar nuestro programa a pleno funcionamiento, siendo así que el usuario pueda desplazarse por el programa con total libertad y comodidad, y así que sea más claro y preciso el aprendizaje de cada herramienta y que los dockers funcionen perfectamente para que el usuario pueda realizar la práctica y comprobaciones de las herramientas.

-Objetivos específicos: los objetivos específicos que tenemos, son los que tienen que ver con la funcionalidad de cada parte de nuestro proyecto. Los más importantes serían, que nuestro programa de PyQt5 funcione correctamente y el entorno gráfico sea cómodo para el usuario, el realizar correctamente los dockers para cada herramienta y posteriormente implementarlos con éxito en nuestro programa para ya completar el funcionamiento, y el realizar la documentación adecuada a cada herramienta para que el usuario esté bien informado de estas.

Otro objetivo que nos gustaría completar es el poder adecuar el programa tanto al Linux como a Windows.

## 5. CALENDARIO

### 1. 21-27 Marzo

Realización de la portada, índice, introducción, descripción del proyecto, justificación del proyecto, objetivo general y objetivos específicos, actividades y tareas - métodos y técnicas y el calendario de actividades / cronograma individualizado.

### 2. 28-03 Marzo/Abril

Realizar la reproducción del script y del entorno gráfico de Python

### 3. 04-10 Abril

Avanzar con la producción el script y del entorno gráfico de Python, y las diferentes ventanas del este

### 4. 11-17 Abril

Hacer pruebas del programa y cambiar lo pertinente tanto en el script o en el entorno gráfico

### 5. 18-24 Abril

Realizar la documentación de la teoría e investigar como conectarlo al programa.

### 6. 25-01 Abril/Mayo

Realizar las imágenes de los dockers de cada asignatura

### 7. 02-08 Mayo

Probar las imágenes de los dockers para comprobar su funcionamiento, e ir probando el funcionamiento en Linux.

### 8. 09-15 Mayo

Sincronizar y comprobar funcionamiento entre el programa de PyQt5 y los dockers de cada herramienta, en Windows y en Linux .

### 9. 16-22 Mayo

Pulir errores y verificar el proyecto total en Windows y Linux.

### 10. 23-29 Mayo

Preparar la documentación del proyecto

## 6. APARTADOS DEL PROYECTO

Al iniciar nuestro proyecto, el objetivo inicial que teníamos era el instalar Python y el PyQt5 con sus respectivas herramientas.

Al haber probado la aplicación tanto en Ubuntu como en Windows los medios de instalación son diferentes, así que pondremos los pasos a seguir en cada uno:

### WINDOWS

```
pip install PyQt5
pip install PyQt5-tools
```

Para instalar Python te puedes ir a la Microsoft Store y buscar “Python” te saldrá la última versión de Python.

Con esto se obtendrán Python y las herramientas de PyQt5, pero también hay que instalar el Qt Designer que es la aplicación en la que se elabora todo el programa. Este nos lo hemos instalado desde un enlace de internet ya que por comandos en Windows tuvimos bastantes problemas.

Mucha gente quiere usar Qt Designer sin tener que descargar gigabytes de otro software. Estos son pequeños instaladores independientes de Qt Designer para Windows y Mac:

[Windows \(31 MB\)](#)

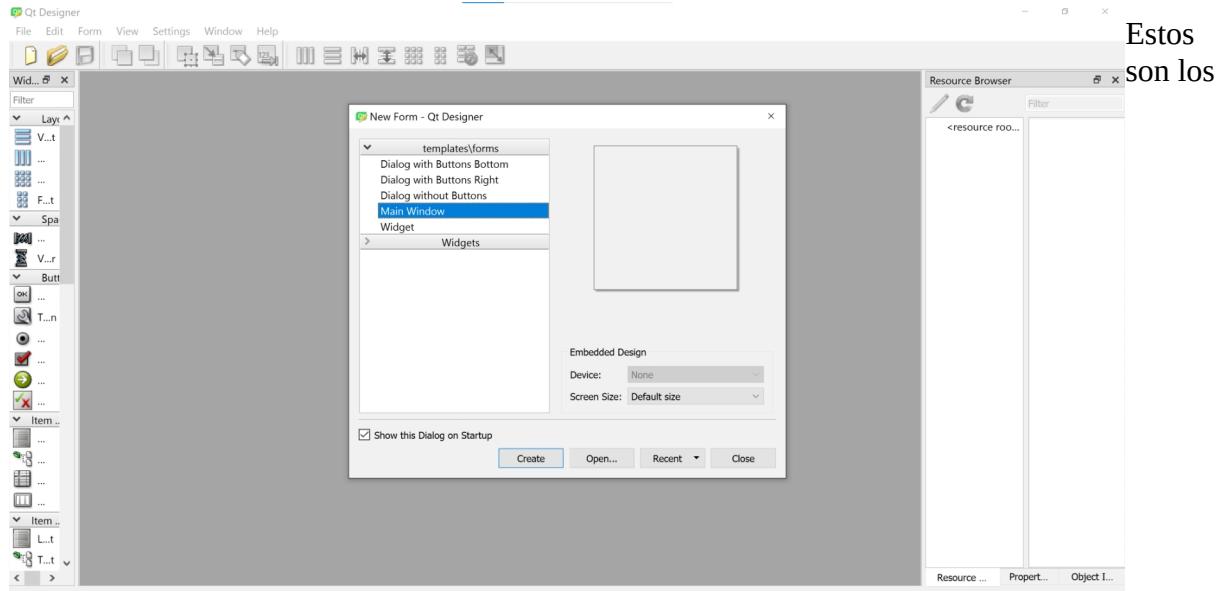
[Mac \(40 MB\)](#)

### UBUNTU

```
sudo apt-get install python3-pyqt5
sudo apt-get install PyQt5-dev-tools
sudo apt-get install qttools5-dev-tools
```

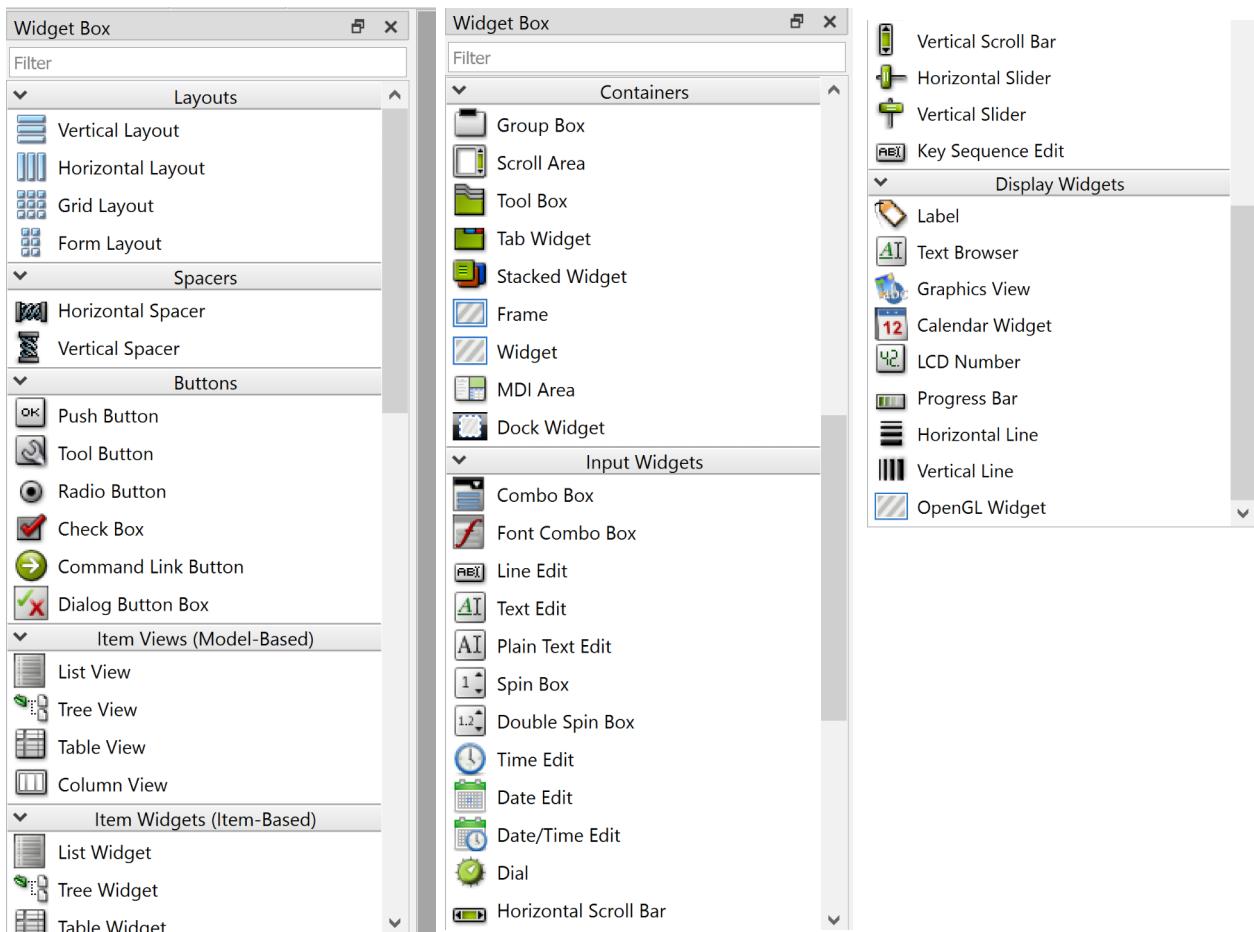
Para iniciar el QtDesigner ponemos por la línea de comandos: *designer*

Una vez instalado al ejecutarlo nos abre esta ventana en la que ya podemos empezar a hacer la aplicación



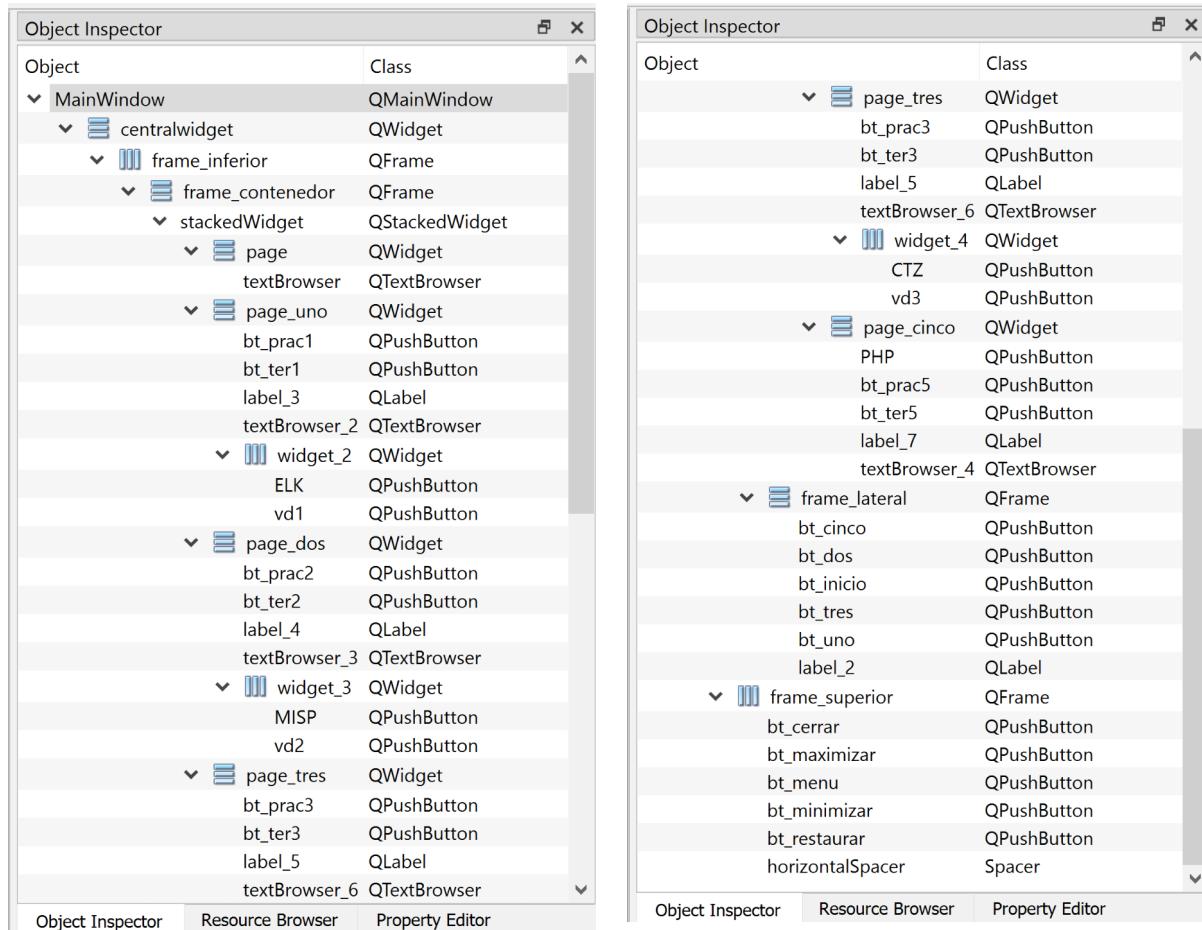
Estos  
son los

elementos con los que nos permite trabajar el QtDesigner, pero nosotros solo hemos elegido unos pocos, con los que hemos formado nuestra aplicación



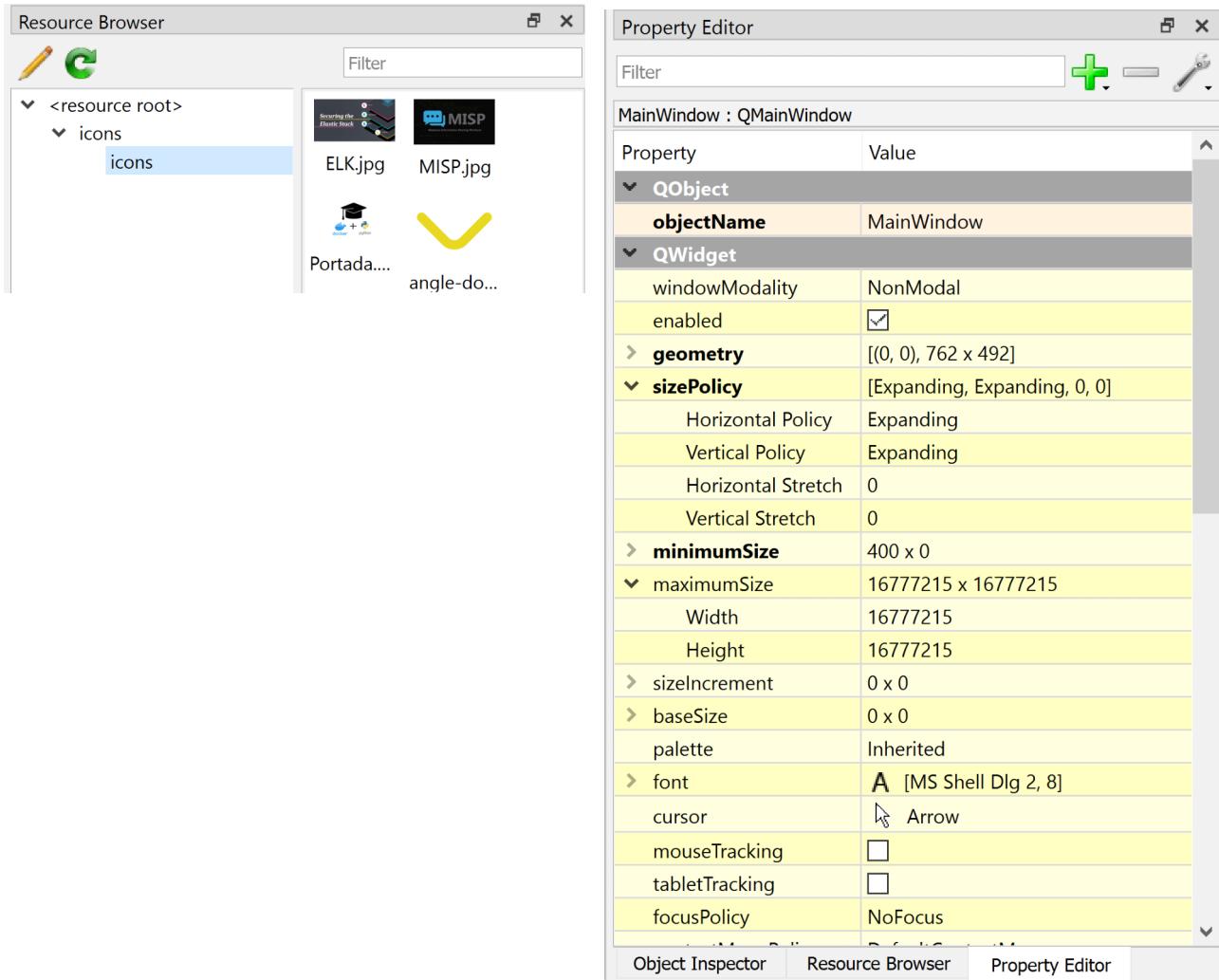
Una vez que nos hemos informado de como utilizar la aplicación, de como dar los primeros pasos y con qué elementos darlos, quisimos hacer un programa completo, y para este, se necesitarían funciones, como para cerrar, minimizar o maximizar la pantalla, o poner una función a los botones que hemos puesto.

Lo hemos querido hacer visual y cómodo para el usuario, y que tenga varias herramientas en las que pueda elegir.



Como se puede apreciar en la imagen, hay 3 ventanas con las que se puede interactuar.

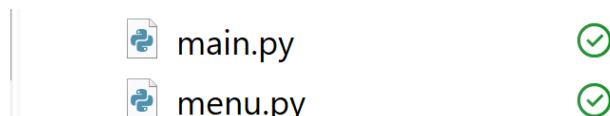
- Object inspector: es para ver los medios de la aplicación que hemos puesto en nuestro programa, y poder ver rápidamente sus nombre y el tipo de medio que es
- Resource Browser: es donde vamos a ubicar nuestras imágenes que queramos poner en el programa, pudiendo editar desde esta las imágenes de la carpeta que queramos introducir.
- Property Editor: como su nombre indica es el editor de propiedades de cada objeto que hemos utilizado de nuestro programa. Dependiendo del medio, hay más o menos cantidad de propiedades.



También hay que tener en cuenta que, una vez realizado la interfaz gráfica de nuestro programa necesitamos pasar todo el contenido gráfico de nuestra aplicación a código python. Para hacerlo hemos utilizado el comando:

```
python -m PyQt5.uic.pyuic youruifile -o yourpyfile -x
```

Una vez esté el archivo creado, necesitarás crear un archivo, con el que tu menú o entorno gráfico pueda tener funciones y demás funciones que cada uno haya querido implementar.



Y dentro del propio main.py (o el archivo donde se vaya a poner las funciones del entorno gráfico), habrá que importar las herramientas que queramos utilizar, y hacer referencia al archivo al que se le van a aplicar las funciones.

```
4  import sys
5  from menu_ui import *
6  from PyQt5 import QtCore
7  from PyQt5.QtCore import QPropertyAnimation
8  from PyQt5 import QtCore, QtGui, QtWidgets
9  import os
```

Nota: para que vuestro equipo de Windwos ejecute algunos comandos del programa se necesitará:

*Git-2.36.1-64-bit.exe*

Nota: para que vuestro equipo de Linux ejecute algunos comandos del programa se necesitará:

```
sudo apt update

sudo apt install apt-transport-https ca-certificates curl software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal
stable"

apt-cache policy docker-ce

sudo apt install docker-ce

sudo systemctl status docker

sudo usermod -aG docker ${USER}

su - ${USER}

id -nG

sudo usermod -aG docker username
```

## HERRAMIENTAS

### ELK

ELK es una fusión de tres proyectos llamados Elasticsearch, Logstash y Kibana. Elasticsearch está basado en JSON y consiste en ser un motor de búsqueda. Logstash consiste en un programa que recibe la información introducida de múltiples fuentes y la transforma. Kibana sirve como una herramienta para visualizar contenido.

Al ver esto el fusionar estos tres proyectos fue una gran idea y que con Elasticsearch se conseguía la búsqueda de los datos, con Logstash que esos datos se reciban y se envíen de forma que con Kibana se puedan visualizar de diversas maneras.

Esto hizo que ELK herramienta que tiene múltiples utilidades, las cuales vamos a desarrollar brevemente.

-Monitorizar sistemas y aplicaciones:

Principalmente se basa en implementar el Elastic Stack, para instalar un Elastic Agent en el host o equipo donde quieras visualizar la información. Para empezar tendrás que crear una implementación de Elastic Cloud. Una vez que esté hecha, dentro de Kibana, tendrás que agregar integraciones. Ahí en adelante puedes ver las diferentes opciones y elegir lo que más te guste o venga bien.

-Protección de los hosts con Elastic Security.

-Crear un motor de búsqueda personalizada con Elastic Enterprise Search.

-Implementar una plataforma propia con el fin de almacenar buscar y visualizar cualquier dato.

Para instalar java v-1.8

Tendremos que instalar una versión de java compatible

```
sudo apt-get install openjdk-8-jdk
```

Para instalar nginx:

```
sudo apt-get install nginx
```

Para descargar elasticsearch:

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch- 7.15.0-amd64.deb
```

Para descargar kibana:

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-7.15.0-amd64.deb
```

Para descargar logstash:

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-7.15.0-amd64.deb
```

Si queremos cambiar la versión de logstash, kibana o elasticsearch, solo tendremos que cambiar los números de versión dentro de wget.

**Para la version 7.15(logstasg):**

**wget https://artifacts.elastic.co/downloads/logstash/logstash-7.15.0-amd64.deb**

**Para la version 7.17(logstasg):**

**wget https://artifacts.elastic.co/downloads/logstash/logstash-7.17.0-amd64.deb**

**Para la version 8.1.1(logstasg):**

**wget https://artifacts.elastic.co/downloads/logstash/logstash-8.1.1-amd64.deb**

Una vez tengamos descargados los paquetes .deb tendremos que desempaquetar/installar los paquetes

Comando dpkg (instalar servicios) :

**sudo dpkg -i elasticsearch-7.15.0-amd64.deb**

**sudo dpkg -i kibana-7.15.0-amd64.deb**

**sudo dpkg -i logstash-7.15.0-amd64.deb**

## Comprobación de Servicios

Una vez los tengamos instalados, comprobaremos el funcionamiento:

### Elasticsearch

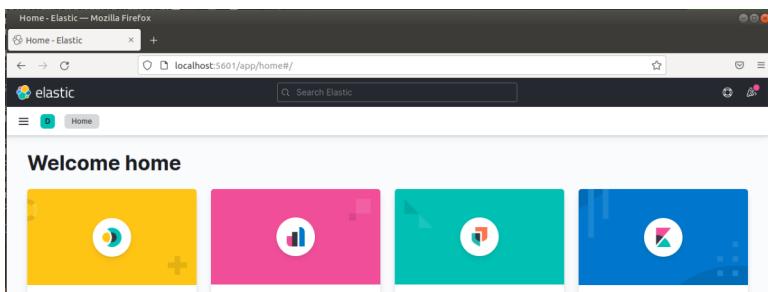
En un navegador se buscaría:

**localhost:9200**

### Kibana

En un navegador se buscaría:

**localhost:5601**

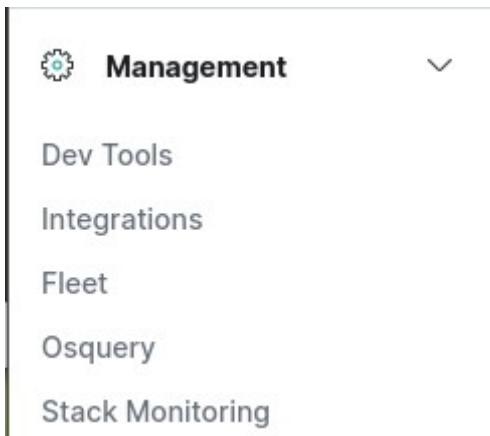


## Logstash

En una terminal se ejecutaría:

```
sudo /usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }'
```

Introducción de Datos  
Dentro de dev tools



Management

- Dev Tools
- Integrations
- Fleet
- Osquery
- Stack Monitoring

Tendremos que crear la plantilla de index para el csv.

```
POST /clientes/_doc
{
  "mappings": {
    "properties": {
      "usuario": { "type": "text" },
      "servicio": { "type": "text" },
      "permisos": { "type": "text" },
      "equipo": { "type": "text" }
    }
  }
}
```

La cual tendrá el que llamarse nombrefichero.csv

```
POST /clientes/_doc
{
  "mappings": { "properties": {
    "usuario": { "type": "text" },
    "servicio": { "type": "text" },
    "permisos": { "type": "text" },
    "equipo": { "type": "text" }
  }}
}
```

Una vez creada la plantilla para el csv crearemos el pipeline.conf para introducir los datos con logstashy que salga de la lectura del csv automáticamente cuando termine esto lo conseguiremos con los valores dentro input y file de: mode => read

```
exit_after_read => true
input {
  file {
    path => "ruta al fichero de csv"
    start_position => beginning
    since_db_path => "/dev/null"
    mode => read exit_after_read=>true
  }
}
filter {
  csv{
    columns => ["columnas creadas en la plantilla del index"]
    mutate
  }
  remove_field => ["columnas a eliminar"]
}
output {
  stdout { }
  elasticsearch {
    index => "nombre del index creado(clientes en este caso)"
  }
}sysctl -w vm.max_map_count=262144
```

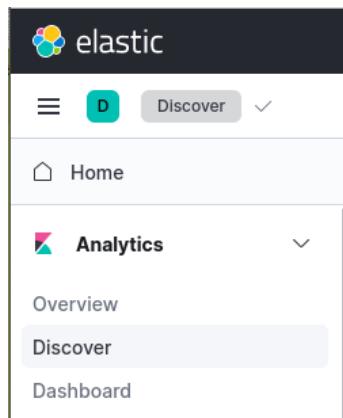
Estructura del fichero csv:

Dependiendo de las columnas puestas en nuestro index.

**valor,valor,valor,valor  
valor,valor,valor,valor**

....etc....

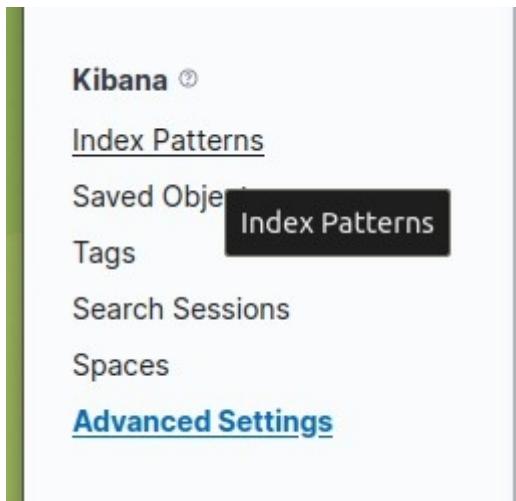
Nos iremos a discover.



Options ⇒ All discover options

The screenshot shows the Elastic Discover interface in a browser window. The URL is `localhost:5601/app/discover/?_g=(filters:!(),refreshInterval:(pause:1t,value:0),time:(from:now-15m,to:now))&_a=`. The interface includes a sidebar with 'Discover' selected, a search bar, and a main area displaying search results for the term 'clientes\*'. The results show 3 hits, including document mappings and user properties. A 'Get started' button is visible, along with a link to 'All Discover options'.

Magement ⇒ Kibana ⇒ Index Patterns



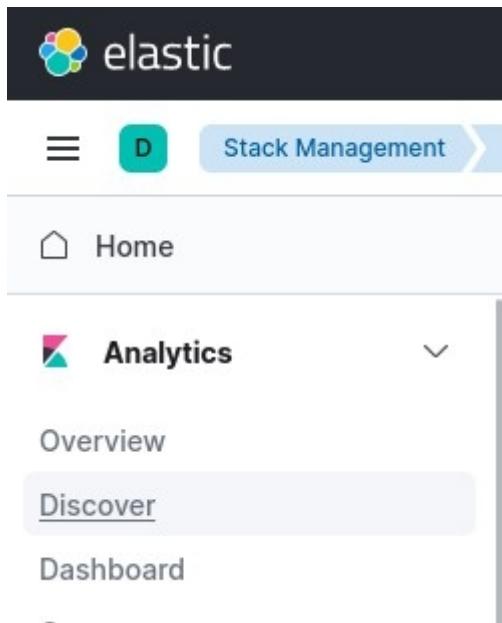
Create index pattern

The screenshot shows the 'Stack Management' section of the Elasticsearch interface. On the left, there's a sidebar with 'Management' and 'Ingest' sections. The main area is titled 'Index patterns' and contains the sub-instruction 'Create and manage the index patterns that help you retrieve your data from Elasticsearch.' To the right, there's a blue button labeled '+ Create index pattern'.

Y Crearemos el index pattern con el nombre que habíamos creado antes.

The screenshot shows the 'Create index pattern' dialog box. In the 'Name' field, the value 'cliente\*' is entered. A note below says: 'Use an asterisk (\*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.' Under 'Timestamp field', a dropdown menu says 'Select a timestamp field' and notes: 'No matching data stream, index, or index alias has a timestamp field.' There is a 'Show advanced settings' link. At the bottom, there are 'Close' and 'Create index pattern' buttons. To the right of the dialog, a green header bar says 'Your index pattern matches 1 source.' Below it, a table shows one row with the name 'clientes' and an 'Index' tab. A 'Rows per page: 10' dropdown is also visible.

Para ver el indice creado iremos a Analytics ⇒ Discover.



Y aquí seleccionar el indice que hemos creado.

A screenshot of the Elasticsearch Discover interface. The top bar has 'Search' and '+ Add filter'. The main search bar contains 'clientes\*' with a '3 hits' count. A dropdown menu titled 'Change index pattern' is open, showing 'clientes\*' selected. Other options like '\_id' and 'clientes\*' are also visible.

Para introducir los datos del csv ejecutaremos el siguiente comando:

```
sudo /usr/share/logstash/bin/logstash -f "ruta fichero pipeline.conf"
```

Y nos saldrán los datos introducidos por columnas.

| Document   |
|--|
| > mappings.properties.equipo.type: text mappings.properties.permisos.type: text mappings.properties.servicio.type: text<br>mappings.properties.usuario.type: text _id: 31govH8BuBRNG_KaxmRa _index: clientes _score: 1 _type: _doc |
| > equipo: equipo15 permiso: todos servicio: java usuario: ahmed _id: 99vhwH8Bwe16Zk6P3-r8 _index: clientes _score: 1<br>_type: _doc  |
| > equipo: equipo10 permiso: todos servicio: php usuario: samuel _id: -NvhwH8Bwe16Zk6P40qv _index: clientes _score: 1<br>_type: _doc  |

## MISP

MISP se basa en el intercambio de información sobre amenazas, como malware, ataques dirigidos y más.

Dentro de MISP hay comunidades cerradas, semiprivadas y abiertas, en las que hay diferentes tipos de información dependiendo de la que se haya transmitido en cada comunidad.

A partir de la información recibida, MISP trata de mejorar las contamedidas y acciones contra los ataques o malware que se comparten, para ayudar a combatirlos.

También va almacenando información sobre cada ataque y lo utiliza para generar reglas NIDS (Network Intrusion Detection System) para que posteriormente se importe a IDS.

El punto positivo de MISP es que ha conseguido una comunidad con numerosas empresas y organismos, lo que hace que haya cada vez más y más información lo que le hace uno de los mejoras.

Para realizar la instalación de MISP tendremos que bajarnos un script con la instalación de MISP en un servidor y meterlo en la carpeta tmp

```
wget -O /tmp/INSTALL.sh  
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

Una vez lo tengamos descargado, ejecutaremos el script

```
bash /tmp/INSTALL.sh
```

Nada mas ejecutarlo nos pedirá, que modo de instalación de MISP queremos realizar

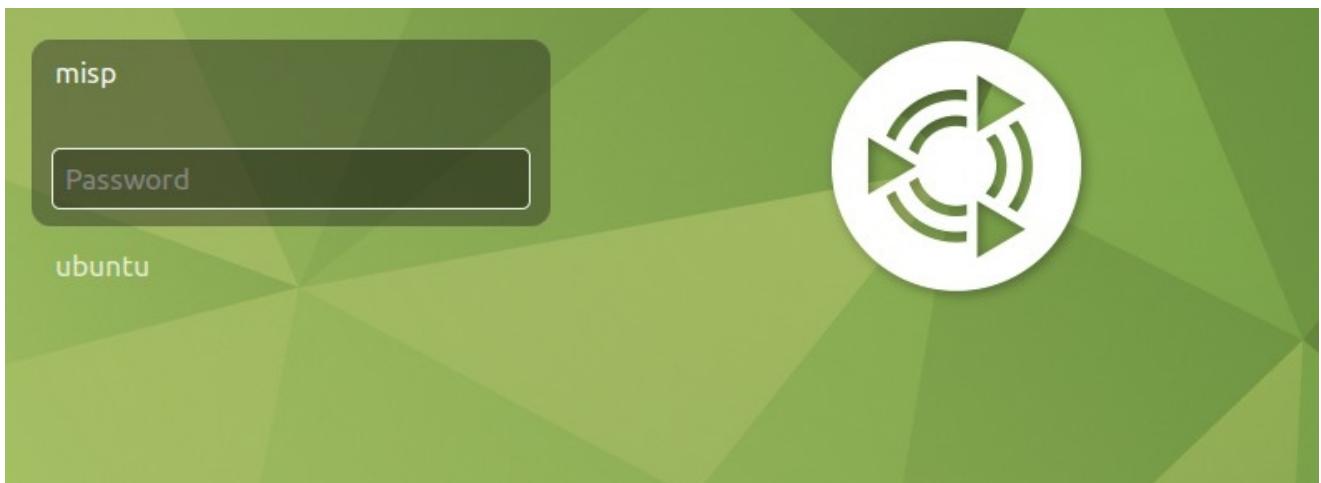
Con la opción -A nos realizara una instalación completa y desatendida.

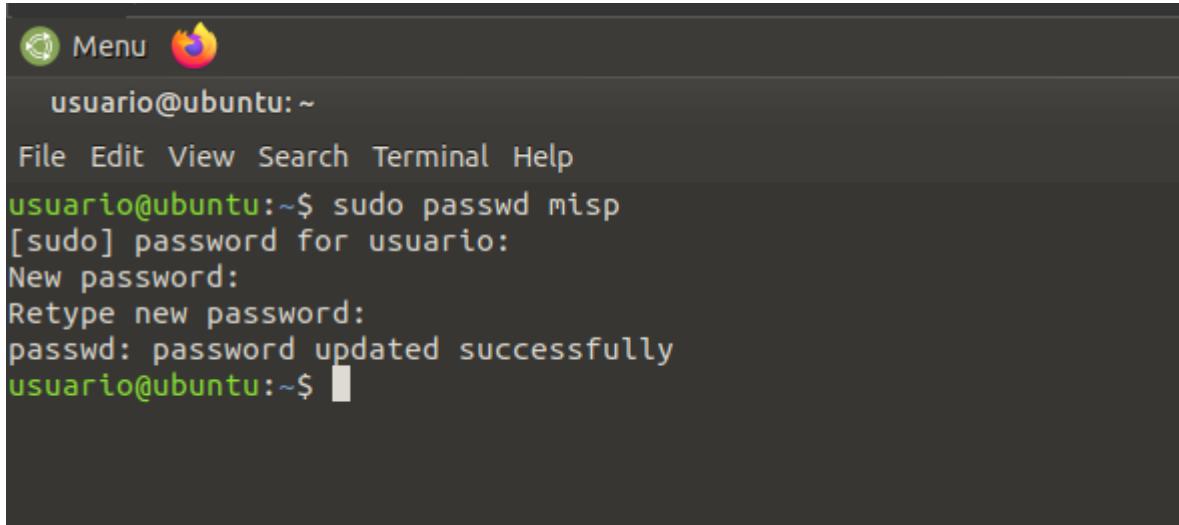
### bash /tmp/INSTALL.sh -A

Tardara un tiempo en instalar pero una vez instalado nos saldrá un resumen de todas las contraseñas generadas de los distintos servicios o cuentas.

```
usuario@ubuntu: ~/Downloads/MISP-2.4/INSTALL
File Edit View Search Terminal Help
#####
##### (88%)
#####
Admin (root) DB Password: 4656d556007c015724ee1c607e485f4f1d6b535747b9e97c5273dfa0304c17dd
User (misp) DB Password: b0bcdf338d28b4abea197d4795f1abe47a8b233804e78c3e72193f6cfdb9e8cd
Authkey: bwttZv33dWDDZZenpS2VH4157xQbeoeOyJee00cj
-----
MISP Installed, access here:
User: admin@admin.test
Password: admin
-----
The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
Contents:
Admin (root) DB Password: 4656d556007c015724ee1c607e485f4f1d6b535747b9e97c5273dfa0304c17dd
User (misp) DB Password: b0bcdf338d28b4abea197d4795f1abe47a8b233804e78c3e72193f6cfdb9e8cd
/home/misp/MISP-authkey.txt
Contents:
Authkey: bwttZv33dWDDZZenpS2VH4157xQbeoeOyJee00cj
-----
The LOCAL system credentials:
User: misp
Password: 0a9e78d264d946923cb1ddf2c9c56fc372e76de8d662508ce9ec44ea12b76705 # Or the password you used of your custom user
-----
GnuPG Passphrase is: 29e7ed5f89c635f2ae5b7a127441a9cae767b0bdf056328279308e8f5ced2d52
To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:
sudo nano /etc/postfix/main.cf
```

También tener en cuenta que se nos generará un usuario de sistema con uid (MISP) el cual su contraseña es bastante larga y seria recomendable cambiarla desde dicha cuenta o con sudo passwd MISP



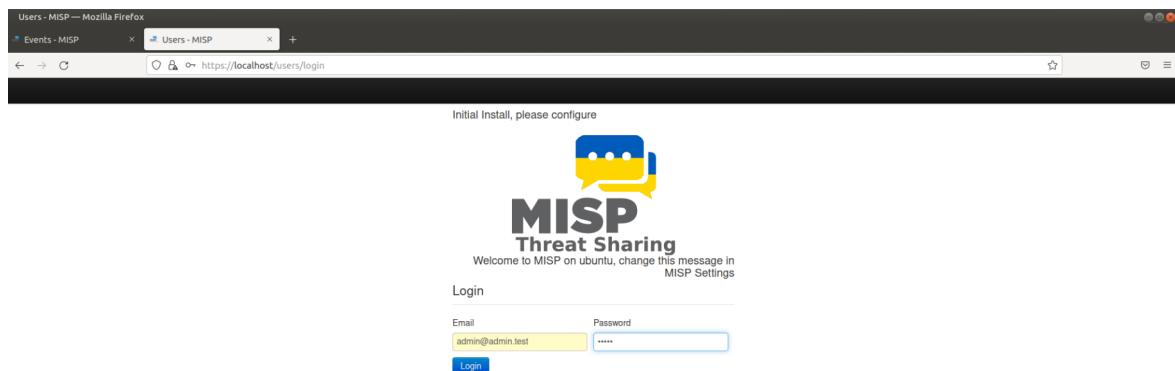


```

Menu 🔥
usuario@ubuntu: ~
File Edit View Search Terminal Help
usuario@ubuntu:~$ sudo passwd misp
[sudo] password for usuario:
New password:
Retype new password:
passwd: password updated successfully
usuario@ubuntu:~$ █

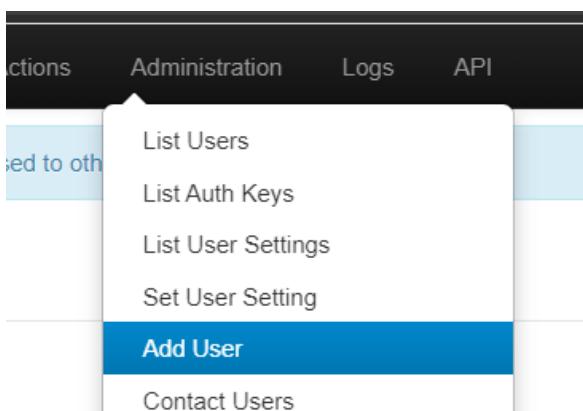
```

Para acceder a MISP una vez instalado, con ip/localhost en un navegador  
██████████ Credenciales: --- user: admin@admin.test password: admin



### Creacion de usuarios en MISP

Para crear un usuario en MISP sería Administration⇒ Add User



Donde podremos asignar a que tipo de organizacion, email, contraseña y rol va a tener dentro de MISP

## Admin Add User

Email

Set password

Password i

Confirm Password



Organisation

Role

NIDS SID

admin

admin  
Org Admin  
**User**  
Publisher  
Sync user  
Read Only

Para añadir un evento MISP:

Tendremos que ir a home ⇒ add event

- [List Events](#)
- [Add Event](#)
- [Import from...](#)
- [REST client](#)
- [List Attributes](#)
- [Search Attributes](#)
- [View Proposals](#)
- [Events with proposals](#)
- [View delegation requests](#)
- [Export](#)
- [Automation](#)

### Add Event

---

Date

Distribution i

Threat Level i

Analysis i

Event Info

Extends Event

Dentro de añadir un evento, especificando la distribución del evento, el nivel de amenaza, y el análisis de la amenaza.

The screenshot shows a user interface for managing network events. At the top, there is a toolbar with various icons and buttons: '+', 'Scope toggle', 'Deleted', 'Decay score', 'SightingDB', 'Context', 'Related Tags', 'Filtering tool'. Below the toolbar is a table header with columns: Date (sorted by Date), Org, Category, Type, Value, Tags, Galaxies, Comment, and Correlate. A red banner at the bottom of the table area states: "Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information)". Below the table are navigation buttons: '<< previous', 'next >>', and 'view all'.

## Discussion

Para añadir información de la amenaza, daremos a "Add attribute"

Dentro de El Atributo, añadiremos la categoría de la información y el tipo, \_\_El nuestro al ser IPs maliciosas)

El tipo de categoría sería network activity  
y el Tipo, ip-src

También podemos añadir, en que fecha se han divisado dicha amenaza.  
Y como vemos se añadirá.

| Date       | Org | Category         | Type   | Value           | Tags | Galaxies | Comment | Correlate                           | Related Events | Feed hits | IDS                                 | Distribution | Sightings   | Activity | Actions |
|------------|-----|------------------|--------|-----------------|------|----------|---------|-------------------------------------|----------------|-----------|-------------------------------------|--------------|-------------|----------|---------|
| 2022-03-29 |     | Network activity | ip-dst | 160.243.95.154  |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 192.204.128.198 |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 36.164.91.203   |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 141.184.52.126  |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 126.78.76.60    |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 65.175.128.132  |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 172.225.21.16   |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 0.230.240.118   |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 116.35.53.133   |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-dst | 79.59.39.81     |      |          |         | <input checked="" type="checkbox"/> |                |           | <input checked="" type="checkbox"/> | Inherit      | <br>(0 0 0) | *   *    |         |
| 2022-03-29 |     | Network activity | ip-src | 10.33.110.41    |      |          |         | <input checked="" type="checkbox"/> |                |           | <input type="checkbox"/>            | Inherit      | <br>(0 0 0) | *   *    |         |

## Instalación de pluggins:

Es interesante recalcar que podemos meter plugins a la plataforma lo cual nos permite hacer desde cosas específicas como relacionar eventos o sus atributos a otros como poder hacer que los eventos se retro-alimenten añadiendo cuando sea necesario nuevos atributos("amenazas"), y se conseguiría de la siguiente manera:

Primero nos dirigimos a ajustes de servidor y mantenimiento

Event #1 - MISP

https://localhost/events/view/1

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API MISP Admin Log

Warning: This event view is outdated. Please reload page to see latest changes.

**View Event**

prueba

**Event ID** 1  
**UUID** d708be5a-cc89-45f9-ba02-9c91c0f30889  
**Creator org** ORGNAME  
**Owner org** ORGNAME  
**Creator user** admin@admin.test  
**Protected Event (experimental)** Event is in unprotected mode. Switch to protected mode  
**Tags** +  
**Date** 2022-03-29

List Users  
List Auth Keys  
List User Settings  
Set User Setting  
Add User  
Contact Users  
User Registrations  
List Organisations  
Add Organisations  
List Roles  
Add Roles

Server Settings & Maintenance

Luego le damos a ajustes de pluggins

Diagnostics - MISP — Mozilla Firefox

https://localhost/servers/serverSettings/Plugin

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API MISP Admin Log out

Add User List Users Pending registrations User settings Set Setting Contact Users

**Server Settings & Maintenance**

Overview MISP settings (9) Encryption settings (4) Proxy settings (5) Security settings (5) **Plugin settings (363)** SimpleBackgroundJobs settings Diagnostics Manage file

| Level       | Setting                              | Value            | Description   |
|-------------|--------------------------------------|------------------|---|
| Critical    | Plugin.Enrichment_services_enable    | true             | Enable/disable the enrichment services  |
| Critical    | Plugin.Enrichment_hover_enable       | true             | Enable/disable the hover over information retrieved from the enrichment modules                       |
| Critical    | Plugin.Enrichment_hover_popover_only | false            | When enabled, users have to click on the magnifier icon to show the enrichment                        |
| Recommended | Plugin.Enrichment_timeout            | 300              | Set a timeout for the enrichment services   |
| Recommended | Plugin.Enrichment_hover_timeout      | 150              | Set a timeout for the hover services  |
| Recommended | Plugin.Enrichment_services_url       | http://127.0.0.1 | The url used to access the enrichment services. By default, it is accessible at http://127.0.0.1:6666 |

Después seleccionamos en la primera opción (enrichment) y nos saldrá una lista de las cuales podemos activar las que necesitemos y no sean de pago

Diagnostics - MISP — Mozilla Firefox

https://localhost/servers/serverSettings/Plugin

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API MISP Admin Log out

Add User List Users Pending registrations User settings Set Setting Contact Users

Add Organisation List Organisations

Add Role List Roles

Server Settings & Maintenance

Overview MISP settings (9) Encryption settings (4) Proxy settings (5) Security settings (5) **Plugin settings (363)** SimpleBackgroundJobs settings Diagnostics Manage file

**Enrichment**

| Level       | Setting                              | Value            | Description   |
|-------------|--------------------------------------|------------------|---|
| Critical    | Plugin.Enrichment_services_enable    | true             | Enable/disable the enrichment services  |
| Critical    | Plugin.Enrichment_hover_enable       | true             | Enable/disable the hover over information retrieved from the enrichment modules                       |
| Critical    | Plugin.Enrichment_hover_popover_only | false            | When enabled, users have to click on the magnifier icon to show the enrichment                        |
| Recommended | Plugin.Enrichment_timeout            | 300              | Set a timeout for the enrichment services   |
| Recommended | Plugin.Enrichment_hover_timeout      | 150              | Set a timeout for the hover services  |
| Recommended | Plugin.Enrichment_services_url       | http://127.0.0.1 | The url used to access the enrichment services. By default, it is accessible at http://127.0.0.1:6666 |

En este caso se activaran 2 pluggins los cuales serán:

The screenshot shows two configuration panels side-by-side.

**Panel 1 (dns module):**

- Section: Recommended Plugin.Enrichment\_dns\_enabled
- Setting: true (selected)
- Description: Enable or disable the dns module.

**Panel 2 (urlscan module):**

- Section: Recommended Plugin.Enrichment\_urlscan\_enabled
- Setting: true (selected)
- Description: Enable or disable the urlscan module.
- Section: Recommended Plugin.Enrichment\_urlscan\_restrict
- Setting: No organisation (selected)
- Description: Restrict the urlscan module to the given organisation.
- Text: Value not set.

Estos plugins nos permitirán por ejemplo en el caso de un evento, añadir un nombre de dominio como atributo y que su ip se añada automáticamente o en el caso del segundo plugin que cuando lo utilicemos nos avisaría de todas las url relacionadas con dicho atributo. Así en selección del usuario se podría abarcar un amplio abanico de posibilidades.

Un ejemplo de esto seria:

The screenshot shows the MISP event details page with the following elements:

- Header: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, MISp, Admin, Log out.
- Event navigation: « previous, next », view all.
- Event toolbar: +, Scope toggle, Deleted, Decay score, SightingDB, Context, Related Tags, Filtering tool, Date ↑, Org, Category, Type, Value, Tags, Galaxies, Comment, Correlate, Related Events, Feed hits, IDS, Distributi.
- Message bar: Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful even.
- Event navigation: « previous, next », view all.
- Section: Discussion
- Buttons: Quote, Event, Thread, Link, Code.

Añadiría ahora el dns de google.com

## Add Attribute

The dialog has the following fields:

- Category**: Network activity
- Type**: domain
- Distribution**: Inherit event

### Value

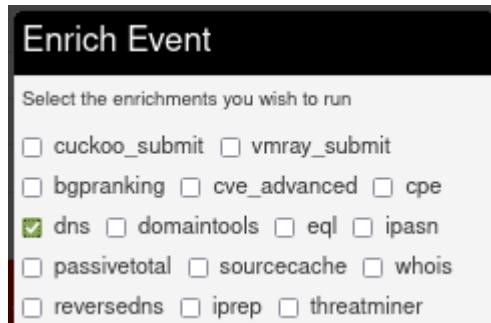
google.com

Una vez añadido se mostraría solo en dns iríamos a la parte de arriba del evento y clicaríamos a la izquierda en enrich event.

The screenshot shows the MISP web interface with two main windows. The top window is titled "Event #1 - MISP" and displays a list of attributes for a network activity event. The bottom window is also titled "Event #1 - MISP" and shows the detailed view of the same event, specifically the "prueba" entry. The left sidebar of the bottom window lists various actions: View Event (selected), View Correlation Graph, View Event History, Edit Event, Delete Event, Add Attribute, Add Object, Add Attachment, Add Event Report, Populate from..., Enrich Event (selected), Merge attributes from..., Publish Event, and Publish (no email). The event details in the bottom window include:

|                                |  |
|--------------------------------|--|
| Event ID                       | 1  |
| UUID                           | d708be5a-cc89-45f9-ba02-9c91c0f30889   |
| Creator org                    | ORGNAME  |
| Owner org                      | ORGNAME  |
| Creator user                   | admin@admin.test   |
| Protected Event (experimental) | <input checked="" type="checkbox"/> Event is in unprotected mode.<br><input type="checkbox"/> Switch to protected mode |
| Tags                           |  |
| Date                           | 2022-03-29   |
| Threat Level                   | High   |
| Analysis                       | Initial  |
| Distribution                   | This community only  |

Entonces saltaría una ventana la cual nos muestra todos los pluggins instalados en este caso hay mas de los necesarios pero solo daremos click a dns:



Después de darle y aceptar refrescamos la pagina y se puede apreciar la aparición de otro atributo el cual es una ip y pertenece al dominio agregado anteriormente

Una vez tengamos un lista de ips podremos guardar el evento y publicarlo.

Publish Event

- [Publish \(no email\)](#)
- [Contact Reporter](#)
- [Download as...](#)

---

[List Events](#)

[Add Event](#)

Y si nos vamos a la home, tendremos nuestro evento publicado.

## Events

« previous next »

| Published                           | Creator org | Owner org | ID  | Clusters | Tags                                     | #Attr. | #Corr. | Creator user     | Date       | Last modified at ↑  | Info           |
|-------------------------------------|-------------|-----------|-----|----------|--|--------|--------|------------------|------------|---------------------|----------------|
| <input checked="" type="checkbox"/> | ORGNAME     | ORGNAME   | ▼ 1 |          | osint:source-type="block-or-filter-list" | 11     |        | admin@admin.test | 2022-03-29 | 2022-03-29 03:06:53 | IPs maliciosas |

## Exportar / Importar eventos:

Para exportar eventos lo recomendable es descargar el evento que queremos exportar en este caso uno de prueba que contiene 4 atributos simples

Events - MISP

← → ↻ https://localhost/events/index/searchorg:1

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

★ MISP Admin Log out

List Events

Add Event

Import from...

REST client

List Attributes

Search Attributes

View Proposals

Events with proposals

View delegation requests

Events

« previous next »

| Published                           | Creator org | Owner org | ID  | Clusters | Tags | #Attr. | #Corr. | Creator user     | Date       | Last modified at ↑  | Info   | Distribution | Actions |
|-------------------------------------|-------------|-----------|-----|----------|------|--------|--------|------------------|------------|---------------------|--------|--------------|---------|
| <input checked="" type="checkbox"/> | ORGNAME     | ORGNAME   | ✖ 1 |          |      | 2      |        | admin@admin.test | 2022-03-29 | 2022-03-30 01:27:07 | prueba | Community    |         |

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

Al entrar al evento podemos apreciar un menu a la izquierda el cual tiene la opcion de descargar el evento ("download as " )

**Event #1 - MISP — Mozilla Firefox**

Event #1 - MISP +

https://localhost/events/view/1

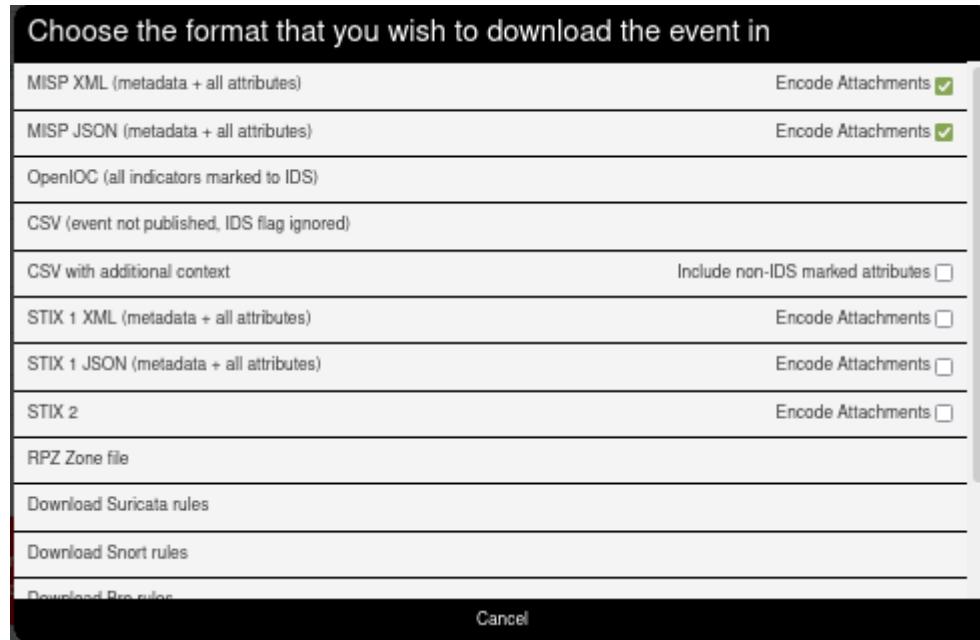
Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

**View Event**

**prueba**

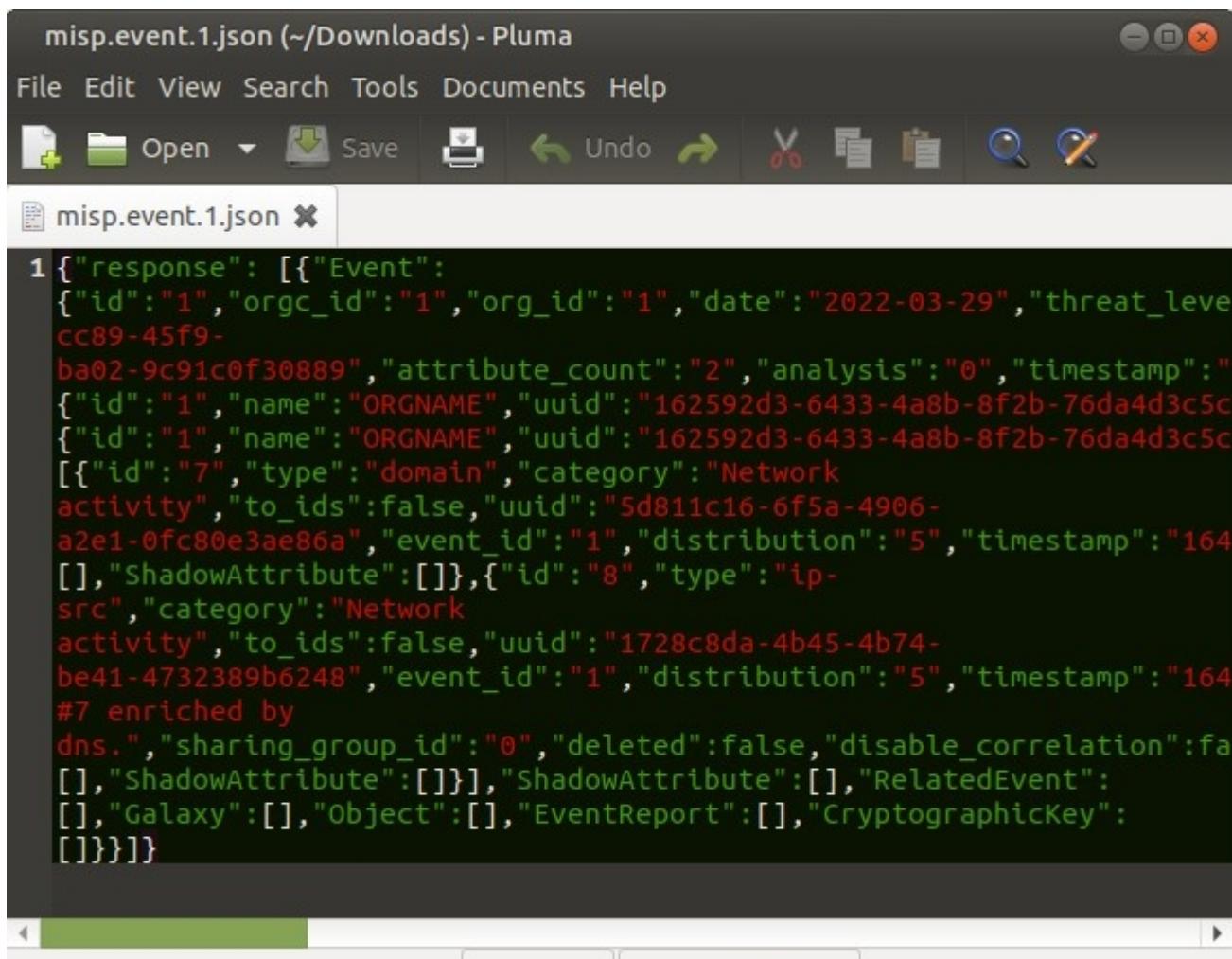
|                                |   |
|--------------------------------|---|
| Event ID                       | 1   |
| UUID                           | d708be5a-cc89-45f9-ba02-9c91c0f30889  |
| Creator org                    | ORGNAME   |
| Owner org                      | ORGNAME   |
| Creator user                   | admin@admin.test  |
| Protected Event (experimental) | <input checked="" type="checkbox"/> Event is in unprotected mode.<br><input type="checkbox"/> Switch to protected mode  |
| Tags                           | <input type="button"/> <input type="button"/>   |
| Date                           | 2022-03-29  |
| Threat Level                   | <input checked="" type="checkbox"/> High  |
| Analysis                       | Initial   |
| Distribution                   | This community only <input type="checkbox"/> <input type="checkbox"/>   |
| Warnings                       | <p><b>Contextualisation:</b><br/>Your event has neither tags nor galaxy clusters attached - generally adding context to an event allows for quicker decision making and more accurate filtering, it is highly recommended that you label your events to the best of your ability.</p> |
| Info                           | prueba  |
| Published                      | No  |
| #Attributes                    | 2 (0 Objects)   |

Si pulsamos en él, nos mostrara varias opciones:



La que nos interesaría para poder pasar eventos desde un modo practico seria en formato JSON. Aunque también se puede usar otros formatos como csv que se podrían implementar con otros servicios o plataformas como ELK que veremos mas adelante.....

Una vez seleccionada la opción se descargaría con el formato seleccionado por ejemplo en el caso de JSON`.

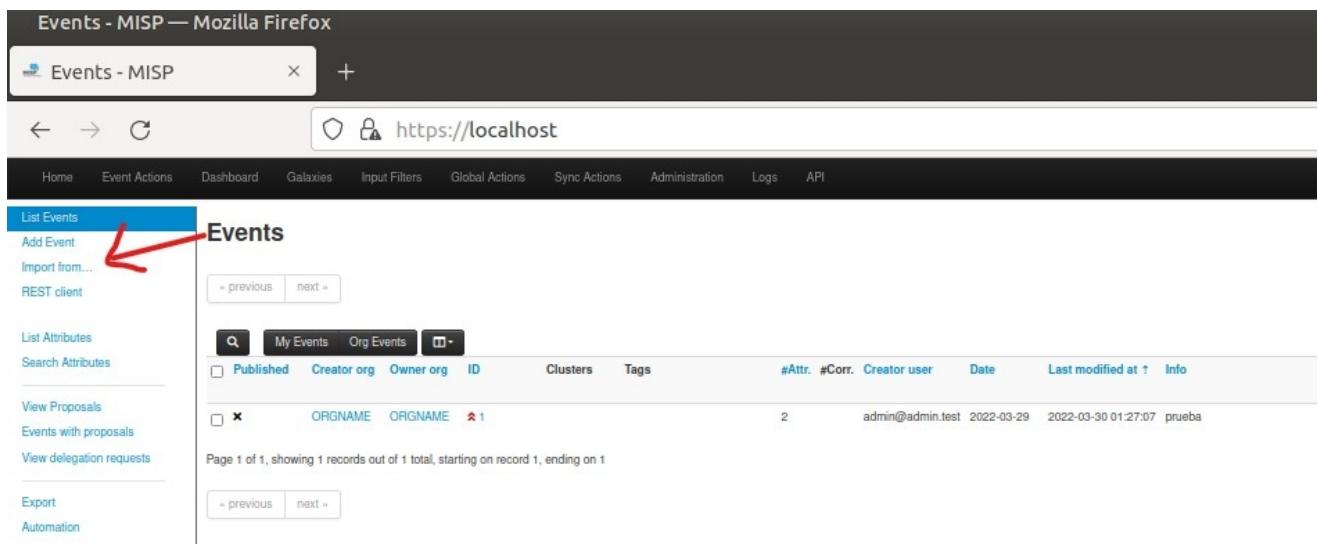


```

misp.event.1.json (~/Downloads) - Pluma
File Edit View Search Tools Documents Help
File Open Save Print Undo Redo Cut Copy Paste Find Replace
misp.event.1.json ✎
1 {"response": [{"Event": {"id": "1", "orgc_id": "1", "org_id": "1", "date": "2022-03-29", "threat_level": "Info", "modified": "2022-03-30 01:27:07", "published": true, "deleted": false, "disable_correlation": false, "sharing_group_id": "0", "attribute_count": "2", "analysis": "0", "timestamp": "2022-03-29T00:00:00Z", "event_id": "1", "distribution": "5", "timestamp": "1643029600000", "to_ids": false, "uuid": "ba02-9c91c0f30889", "category": "Network", "activity": "dns", "Object": [{"id": "7", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "8", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}], "ShadowAttribute": [{"id": "7", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "8", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}], "RelatedEvent": [{"id": "1", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "2", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}], "Galaxy": [{"id": "1", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "2", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}], "EventReport": [{"id": "1", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "2", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}], "CryptographicKey": [{"id": "1", "type": "domain", "value": "ORNGNAME", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "162592d3-6433-4a8b-8f2b-76da4d3c5c", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}, {"id": "2", "type": "ip-src", "value": "1728c8da-4b45-4b74-be41-4732389b6248", "category": "Network", "activity": "dns", "to_ids": false, "uuid": "1728c8da-4b45-4b74-be41-4732389b6248", "event_id": "1", "distribution": "5", "timestamp": "1643029600000}]}]}

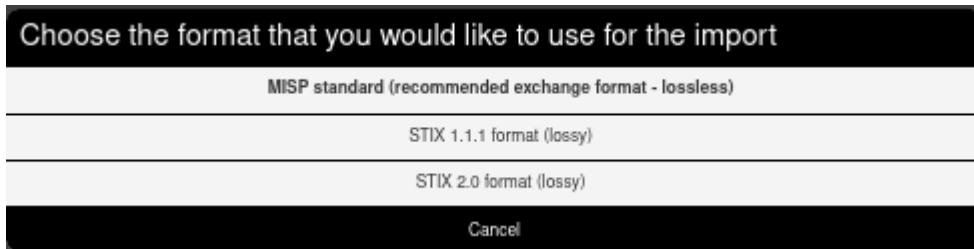
```

Para importar eventos tenemos que tener en cuenta una cosa y es que los archivos/eventos a importar tienen que tener un formato xml o json. y se realizaria de la siguiente manera:  
Desde el home de MISP veremos la opción de import from("importar desde").



|                                     | Published | Creator org | Owner org | ID | Clusters | Tags | #Attr. | #Corr. | Creator user     | Date       | Last modified at    | Info   |
|-------------------------------------|-----------|-------------|-----------|----|----------|------|--------|--------|------------------|------------|---------------------|--------|
| <input checked="" type="checkbox"/> | x         | ORNGNAME    | ORNGNAME  | 1  |          |      | 2      |        | admin@admin.test | 2022-03-29 | 2022-03-30 01:27:07 | prueba |

Cuando le demos nos pedirá un formato.



En este caso vamos a probar a seleccionar el formato MISP que se basa en xml/json. Se puede ver que también se puede publicar a la hora de importar, una vez le damos a upload nos mostrará los eventos importados.

Luego al dar a home veremos que se han creado correctamente.

Implementar MISP a ELK

Para poder implementar MISP a ELK tendremos que descargarnos un evento en forma de CSV y aplicarlo con logstash.

Para ello, dentro de un evento tendremos que irnos a la parte de "download as"

| View Event                               |   |
|--|---|
| <a href="#">View Correlation Graph</a>   |   |
| <a href="#">View Event History</a>       |   |
| <hr/>                                    |   |
| <a href="#">Edit Event</a>               |   |
| <a href="#">Delete Event</a>             |   |
| <a href="#">Add Attribute</a>            |   |
| <a href="#">Add Object</a>               |   |
| <a href="#">Add Attachment</a>           |   |
| <a href="#">Add Event Report</a>         |   |
| <a href="#">Populate from...</a>         |   |
| <a href="#">Enrich Event</a>             |   |
| <a href="#">Merge attributes from...</a> |   |
| <hr/>                                    |   |
| <a href="#">Unpublish</a>                |   |
| <a href="#">Publish Sightings</a>        |   |
| <a href="#">Contact Reporter</a>         |   |
| <a href="#">Download as...</a>           |   |
| <hr/>                                    |   |
| IPs maliciosas                           |   |
| Event ID                                 | 1   |
| UUID                                     | 6a485d87-6cfa-4a39-b7d0-bad380cb6739                      |
| Creator org                              | ORGNAME   |
| Owner org                                | ORGNAME   |
| Creator user                             | admin@admin.test  |
| Protected Event<br>(experimental)        | Event is in unprotected mode.<br>Switch to protected mode |
| Tags                                     | osint:source-type="block-or-filter-list"                  |
| Date                                     | 2022-03-29  |
| Threat Level                             | Low   |
| Analysis                                 | Ongoing   |
| Distribution                             | This community only                                       |
| Info                                     | IPs maliciosas  |

## Eligiremos el csv

Choose the format that you wish to download the event in

|                                       |  |
|---------------------------------------|--|
| MISP XML (metadata + all attributes)  | Encode Attachments <input checked="" type="checkbox"/>     |
| MISP JSON (metadata + all attributes) | Encode Attachments <input checked="" type="checkbox"/>     |
| OpenIOC (all indicator)               | Export as CSV <input type="button"/>                       |
| CSV                                   | Include non-IDS marked attributes <input type="checkbox"/> |
| CSV with additional context           | Include non-IDS marked attributes <input type="checkbox"/> |

Como vemos se nos descarga en formato de CSV

```
misp.event.1.csv (~/Downloads) - Pluma
File Edit View Search Tools Documents Help



```
mispevent.1.csv
1 uuid,event_id,category,type,value,comment,to_ids,date,object_relation,attribute_tag,object_uuid,object_name,object_meta_category
2 "d9784f45-a3bd-478c-84d0-5c2fb4d17e3b","1","Network activity","ip-dst","100.243.95.154","",1,1648547824,"",,""
3 "41761c63-3929-4b45-9bab-5195e542e40a","1","Network activity","ip-dst","192.204.128.198","",1,1648547824,"",,""
4 "490aa668-4f15-4f15-8f69-ee5317374527","1","Network activity","ip-dst","36.164.91.203","",1,1648547824,"",,""
5 "5fe23439-b45f-4232-bf43-00c3b320bac0","1","Network activity","ip-dst","141.184.52.120","",1,1648547824,"",,""
6 "8637fc9e7-a7bc-49b7-89f7-0048cc088cc0","1","Network activity","ip-dst","126.78.76.60","",1,1648547824,"",,""
7 "d3592888-4839-4b0c-bf87-48de14eb5f3a","1","Network activity","ip-dst","65.175.128.132","",1,1648547824,"",,""
8 "a268ef77-3867-4b1c-a2ca-9a36f4520edd","1","Network activity","ip-dst","172.225.21.16","",1,1648547824,"",,""
9 "c08cc0df-913b-4910-f70a-7f0a77153f27","1","Network activity","ip-dst","0.230.240.118","",1,1648547824,"",,""
10 "763cf518-c945-4ae8-a0e2-0d70ccaf1100","1","Network activity","ip-dst","116.35.53.133","",1,1648547824,"",,""
11 "98472057-7bc3-4f60-b443-c2d034d6bdd0","1","Network activity","ip-dst","79.59.39.83","",1,1648547824,"",,""
12
```


```

Para implementarlo a ELK tendremos que tener una index mapeado creado

```
POST /ipsmaliciosas/_doc
{
  "mappings": { "properties": {
    "valor": { "type": "long" },
    "valor": { "type": "text" },
    "valor": { "type": "long" },
    "valor": { "type": "text" }
  }}
}
```

Y crearnos un pipeline para meter los datos de CSV

Y relizar un logstash

```
sudo /usr/share/logstash/bin/logstash -f '/home/usuario/Desktop/pipeline.conf'
```

```
input {
  file {
    path => "ruta al fichero de csv"
    start_position => beginning since db_path => "/dev/null" mode => read exit_after_read => true
  }
}

filter { csv {
  columns => ["columnas creadas en la plantilla del index"]
}
mutate {
  remove_field => ["columnas a eliminar"]
}
}

output { stdout { }
  elasticsearch {
    index => "nombre del index creado(ipsmaliciosas en este caso)"
  }
}
```

## Posibles usos de MISP:

Visto todo lo anterior MISP podría tener diferentes implementaciones gracias a su versatilidad y su adaptación al uso que le queremos dar. Existen usos como la implementación de eventos a un Firewall en el cual se irían añadiendo bloqueos a ips no deseadas de forma automática. por ejemplo, también existe la posibilidad de un dns automatizado con la implementación de un evento auto suficiente o se podría usar como una herramienta de aprendizaje donde los usuarios o equipo de seguridad se informen de nuevas amenazas, debilidades y fortalezas.

## CORTEZA

Corteza es una plataforma basada en el desarrollo con low code, que cuenta con tecnologías modernas.

Es una plataforma confiable y segura, que tiene muy en cuenta el mantenimiento de esta misma y su desarrollo, con el objetivo de que las organizaciones que cuenten con corteza, sepan de que siempre esta, va a estar controlada, segura, y con un desarrollo de mejoras continuo.

Además tiene muy bien explicada y desarrollada la documentación con el objetivo de que el usuario pueda utilizar la plataforma, y sea posible el crear y desarrollar en esta.

## Instalación Corteza

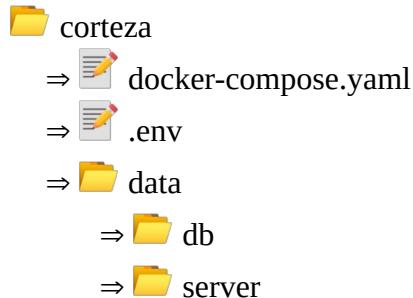
La instalación del entorno de corteza se realiza a través de docker-compose Por lo tanto para poder Realizarlo tendremos que instalarnos docker compose. Instalación de docker:

<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04-es>

## Instalación de docker-compose

Una vez tengamos instalador docker-compose, tendremos que crearnos la siguiente estrutura de directorios:

<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-20-04-es>



## Comandos:

```
mkdir corteza mkdir corteza/data  
mkdir corteza/data/db mkdir corteza/data/server  
touch corteza/docker-compose.yaml touch corteza/.env
```

Nos situaremos en la carpeta de corteza.

```
cd corteza
```

Tendremos que cambiar los permisos de las carpetas db y server para que no de problemas a la hora de instalar

```
sudo chown 1001:1001 data/db sudo chown 4242:4242 data/server
```

Dentro del fichero de docker-compose.yaml tendremos que poner el siguiente contenido. Cuidado con los espacios en blanco, es un fichero .yaml.

```
version: '3.5'  
  
services: server:  
image: cortezaproject/corteza:${VERSION} restart: always  
env_file: [ .env ] depends_on: [ db ] volumes:  
- "serverdata:/data"  
ports: [ "0.0.0.0:18080:80" ]  
  
db:  
# PostgreSQL Database
```

```
# See https://hub.docker.com/_/postgres for details image: postgres:13
restart: always
healthcheck: { test: ["CMD-SHELL", "pg_isready -U corteza"], interval: 10s, timeout: 5s,
retries: 5 }
volumes:
- dbdata:/var/lib/postgresql/data environment:
# Warning: these are values that are only used on 1st start
#       if you want to change it later, you need to do that # manually inside db container
POSTGRES_USER: corteza POSTGRES_PASSWORD: corteza

volumes:
  dbdata: serverdata:
```

Dentro del fichero de .env tendremos que poner el siguiente contenido en la linea de "DOMAIN" "NombreDeDominio:18080" pondremos el nombre de dominio con el que queremos acceder.

```
#####
## #####
# docker-compose supports environment variable interpolation/substitution in compose
configuration file
# (more info: https://docs.docker.com/compose/environment-variables)
#####
## #####
# General settings DOMAIN=dominio.educa.madrid:18080 VERSION=2021.9.7
#####
## #####
# Database connection DB_DSN=postgres://corteza:corteza@db:5432/corteza?
sslmode=disable
#####
## #####
# Server settings
# Running all-in-one and serving web applications directly from server container
HTTP_WEBAPP_ENABLED=true
# Disabled, we do not need detailed persistent logging of actions in local env
ACTIONLOG_ENABLED=false
#####
## #####
# SMTP (mail sending) settings

# Point this to your local or external SMTP server if you want to send emails. # In most cases,
Corteza can detect that SMTP is disabled and skips over sending emails without an error
#SMTP_HOST=smtp-server.example.tld:587

#SMTP_PASS=this-is-your-smtp-password #SMTP_FROM="Demo" <>
```

Y lanzaremos el docker

```
docker-compose up -d
```

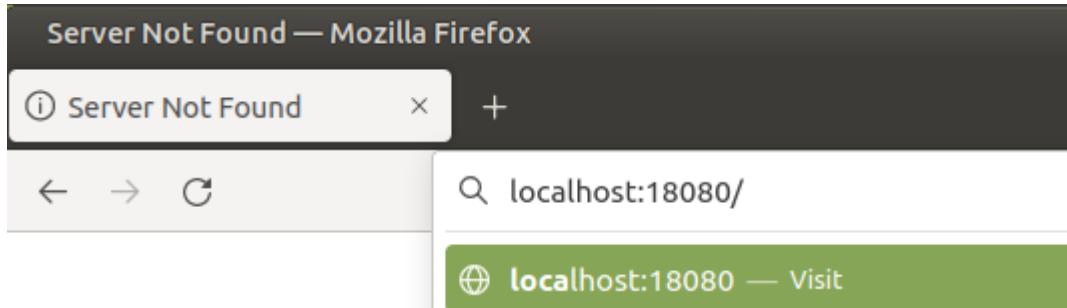
Para poder entrar tendremos que entrar el fichero hosts

```
sudo nano /etc/hosts  
ipmaquina dominio.educa.madrid
```

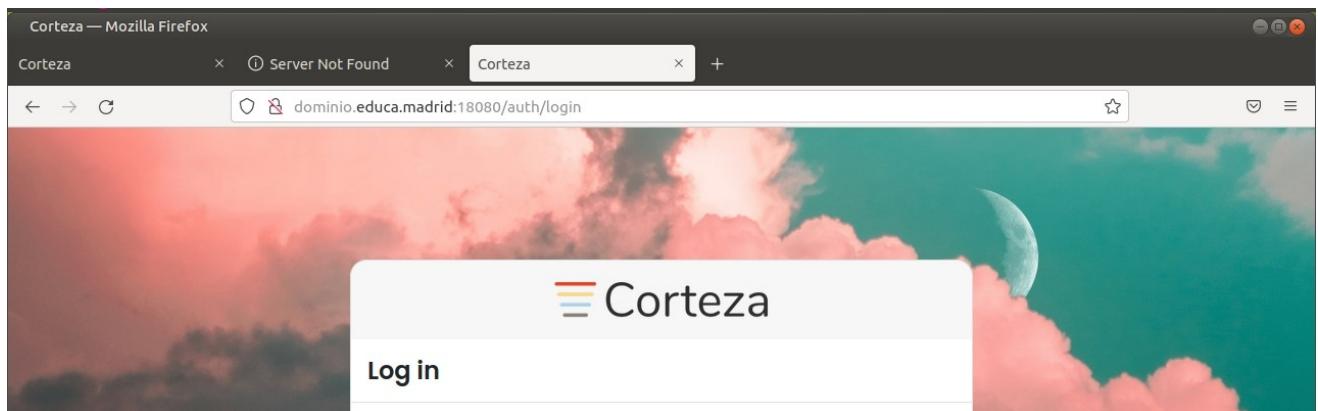
```
GNU nano 4.8                               /etc/hosts  
127.0.0.1      localhost  
127.0.1.1      ubuntu  
127.0.0.1      samuel.example.org  
10.227.53.211  dominio.educa.madrid
```

Entraremos mediante:

```
localhost:9000
```



Según entramos, se nos direccionalidad al dominio que pusimos anteriormente, y ya tendremos corteza instalado



## JUEGO PHP-Mysql

El usuario se encuentra en una empresa donde se gestionan usuarios que utilizan 4 servicios los cuales

son : correo, portal, aula virtual y Nube. Pero el usuario no tiene acceso a las cuentas de administrador ni básica para poder gestionar y trabajar en la empresa. Entonces el reto que se le propone al usuario es participar en 3 pruebas por las que podrá obtener las credenciales de los usuarios que le faltan y así poder tener el control. Aunque en estas 3 pruebas hay unas serie de reglas.

### Reglas:

- No se puede modificar, consultar, insertar o eliminar la tabla registros ya que si no se ha pasado el juego rompería la mecánica y su gracia(ademas de posible corrupción de dicha pagina).
- El juego se basa que al completar una prueba obtengas la contraseña de un usuario de distinto nivel.
- La base de datos se llama pagina\_crud y la tabla se llama registros en caso de no estar implementada se recomienda su ingesta mediante el archivo /php/data/migracion.sql.

### PRUEBAS

#### 1ª prueba

Disponiendo de una cuenta llamada “anónimo” con contraseña “1234” el usuario podrá acceder a la pagina php pero no dispondrá de ningún privilegio. Entonces para alcanzar el nivel “básico” tendrá que sacar el máximo de dinero de la tabla acertijos de la base de datos pagina\_crud.

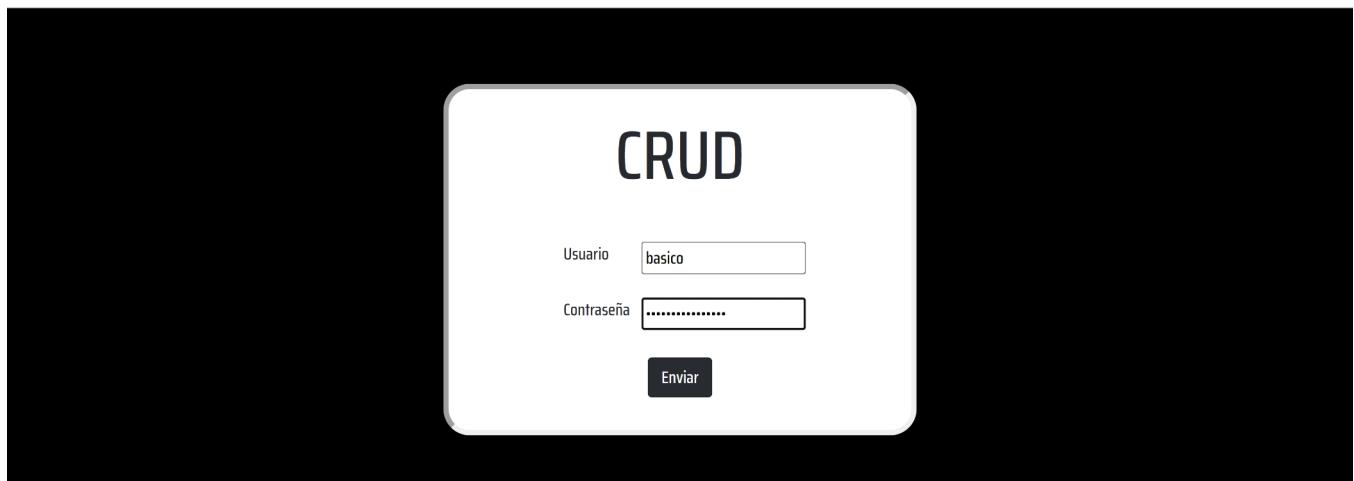
The screenshot shows a web application interface. At the top center is a modal window titled "CRUD" containing a login form with fields for "Usuario" (with value "anonimo") and "Contraseña" (with value "..."). Below the modal is a table titled "Lista de usuarios". The table has columns: #, Usuario, Servicio, Host, Permisos, Correo, Portal, A.virtual, Cloud, and Acciones. The data in the table is as follows:

| # | Usuario    | Servicio | Host    | Permisos | Correo | Portal | A.virtual | Cloud | Acciones |
|---|------------|----------|---------|----------|--------|--------|-----------|-------|----------|
| 1 | superadmin | *        | *       | →        | *      | *      | *         | *     | -        |
| 2 | admin      | gmail    | 1       | →        | admin  | nada   | nada      | nada  | -        |
| 3 | basico     | hotmail  | 2       | →        | basico | nada   | nada      | nada  | -        |
| 4 | anonimo    | unknown  | unknown | →        | nada   | nada   | nada      | nada  | -        |

At the bottom of the table are buttons for "Crear usuario" (Create user), "Buscar por usuario" (Search by user), and "Ver resultados" (View results). There are also red "Cerrar sesión" (Logout) and "Volver" (Back) buttons at the top right of the modal.

### Lista de usuarios

| # | Usuario    | Servicio | Host    | Permisos | Correo | Portal | A.virtual | Cloud | Acciones |
|---|------------|----------|---------|----------|--------|--------|-----------|-------|----------|
| 1 | superadmin | *        | *       | →        | *      | *      | *         | *     | -        |
| 2 | admin      | gmail    | 1       | →        | admin  | nada   | nada      | nada  | -        |
| 3 | basico     | hotmail  | 2       | →        | basico | nada   | nada      | nada  | -        |
| 4 | anonimo    | unknown  | unknown | →        | nada   | nada   | nada      | nada  | -        |



## Bienvenido basico

[Crear usuario](#) [Cerrar Sesión](#) [Perfil](#)

[Ver resultados](#)

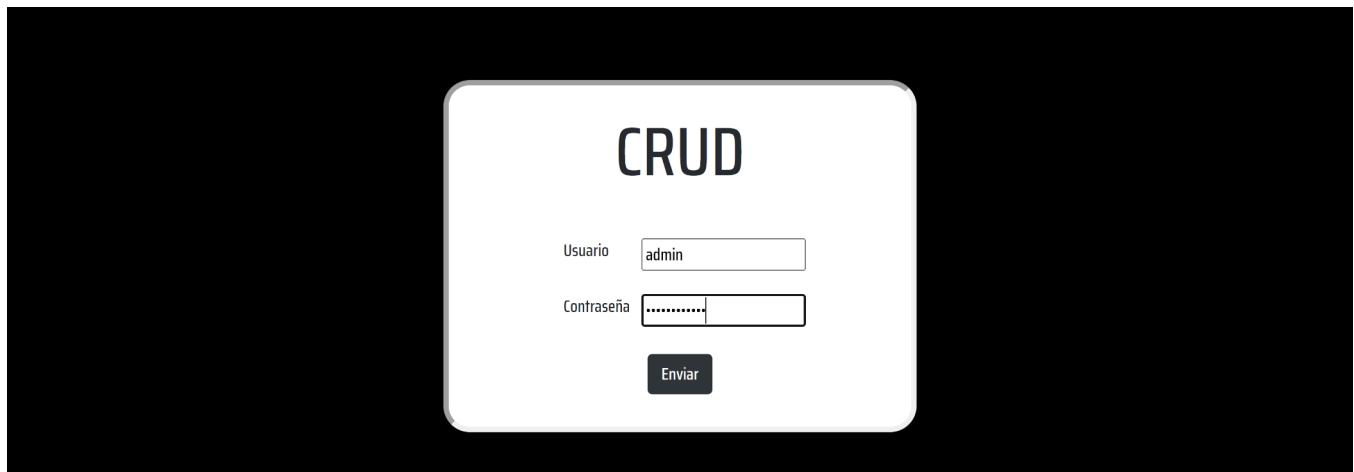
### Lista de usuarios

| # | Usuario    | Servicio | Host    | Permisos | Correo | Portal | A.virtual | Cloud | Acciones |
|---|------------|----------|---------|----------|--------|--------|-----------|-------|----------|
| 1 | superadmin | *        | *       | →        | *      | *      | *         | *     | -        |
| 2 | admin      | gmail    | 1       | →        | admin  | nada   | nada      | nada  | -        |
| 3 | basico     | hotmail  | 2       | →        | basico | nada   | nada      | nada  | -        |
| 4 | anonimo    | unknown  | unknown | →        | nada   | nada   | nada      | nada  | -        |

### 2ª prueba

Tras desbloquear la cuenta “básico” sabrá que no se puede hacer mucho con dicha cuenta, entonces

para obtener más poder en la página tendrás que buscar el host de Janessa en la tabla acertijos de la base de datos pagina\_crud, con el objetivo de obtener el usuario “admin”.



## Bienvenido admin

[Crear usuario](#)
[Cerrar Sesión](#)
[Perfil](#)

---

[Ver resultados](#)

### Listado de usuarios

| # | Usuario    | Servicio | Host    | Permisos | Correo | Portal | A.virtual | Cloud | Acciones   |
|---|------------|----------|---------|----------|--------|--------|-----------|-------|--|
| 1 | superadmin | *        | *       | →        | *      | *      | *         | *     | -  |
| 2 | admin      | gmail    | 1       | →        | admin  | nada   | nada      | nada  | -  |
| 3 | basico     | hotmail  | 2       | →        | basico | nada   | nada      | nada  | <span>trash</span> <a href="#">Borrar</a> <span>pencil</span> <a href="#">Editar</a> |
| 4 | anonimo    | unknown  | unknown | →        | nada   | nada   | nada      | nada  | -  |

## Editando el usuario basico hotmail

Usuario

basico

servicio

hotmail

Host

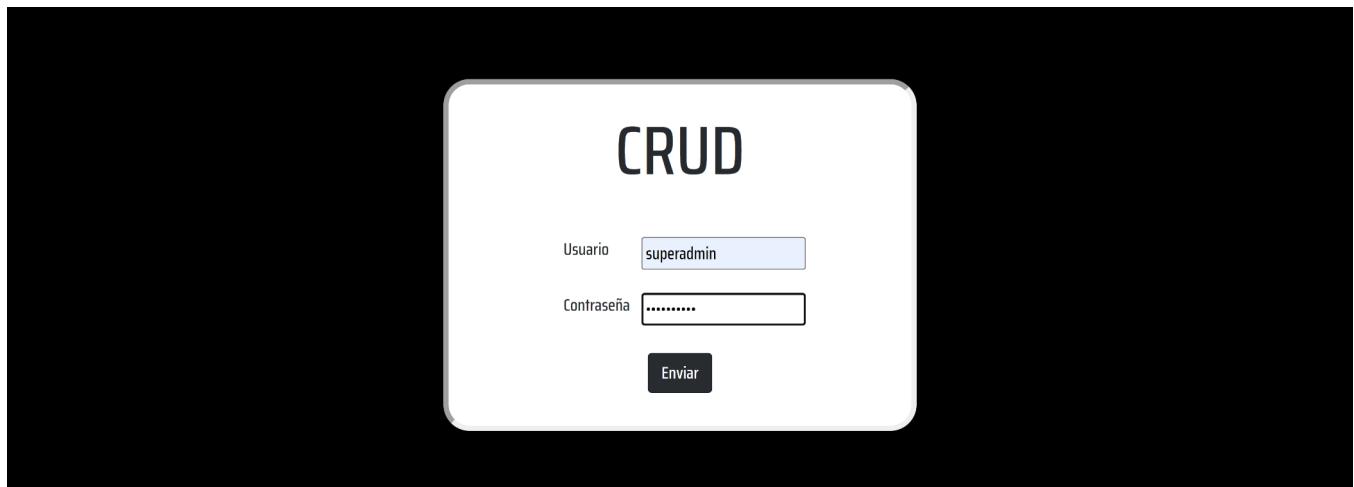
2

| Permisos     | Admin                 | Basico                           | Nada                             |
|--------------|-----------------------|----------------------------------|----------------------------------|
| correo       | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/>            |
| Portal       | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> |
| Aula virtual | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> |
| Cloud        | <input type="radio"/> | <input type="radio"/>            | <input checked="" type="radio"/> |

### 3ª prueba

Después de ver lo anterior seguramente el usuario aspirará a obtener el control total de la empresa/página, para que no solo puedas editar y crear solo a ciertos usuarios, si no para que tengas control total sobre todo. Para obtener dicho rango o privilegio, el usuario tendrá que obtener al usuario “superadministrador”, buscando una contraseña que empiece por la q y termine por la n cuyo id sea menor que 500.

Habiendo completado estas pruebas el usuario habrá obtenido el control total de la página con sus funcionalidades.



## Bienvenido superadmin

[Crear usuario](#)
[Cerrar Sesión](#)
[Perfil](#)

[Ver resultados](#)

### Lista de usuarios

| #             | Usuario    | Servicio | Host    | Permisos | Correo | Portal | A.virtual | Cloud | Acciones       |
|---------------|------------|----------|---------|----------|--------|--------|-----------|-------|----------------|
| 1             | superadmin | *        | *       | →        | *      | *      | *         | *     | -              |
| 2             | admin      | gmail    | 1       | →        | admin  | nada   | nada      | nada  | Borrar  Editar |
| 3             | basico     | hotmail  | 2       | →        | basico | nada   | nada      | nada  | Borrar  Editar |
| 4             | anonimo    | unknown  | unknown | →        | nada   | nada   | nada      | nada  | Borrar  Editar |
| <b>correo</b> |            |          |         | ◎        |        | ○      |           |       | ○              |
| <b>Portal</b> |            |          |         | ◎        |        | ○      |           |       | ○              |

## 7. CÓDIGO

### MAIN.PY (Archivo de funciones del programa en WINDOWS)

```
import sys
from menu_ui import *
from PyQt5 import QtCore
from PyQt5.QtCore import QPropertyAnimation
from PyQt5 import QtCore, QtGui, QtWidgets
import os

class MiApp(QtWidgets.QMainWindow):
    def __init__(self):
        super().__init__()
        self.ui = Ui_MainWindow()
        self.ui.setupUi(self)

        #Eliminar barra y de titulo - opacidad
        self.setWindowFlag(QtCore.Qt.FramelessWindowHint)
        self.setWindowOpacity(1)

        #SizeGrip
        self.gripSize = 10
        self.grip = QtWidgets.QSizeGrip(self)
        self.grip.resize(self.gripSize, self.gripSize)

        #Mover ventana
        self.ui.frame_superior.mouseMoveEvent = self.mover_ventana

        #Acceder a las paginas
        self.ui.bt_inicio.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page))
        self.ui.bt_uno.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_uno))
        self.ui.bt_dos.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_dos))
        self.ui.bt_tres.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_tres))
        self.ui.bt_cinco.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_cinco))

        #Acceder a los pdfs
        self.ui.bt_ter1.clicked.connect(self.abrir1)
        self.ui.bt_ter2.clicked.connect(self.abrir2)
```

```
self.ui.bt_ter3.clicked.connect(self.abrir3)
self.ui.bt_ter5.clicked.connect(self.abrir4)

#Abrir los dockers
self.ui.bt_prac1.clicked.connect(self.dock_elk)
self.ui.bt_prac2.clicked.connect(self.dock_misp)
self.ui.bt_prac3.clicked.connect(self.dock_ctz)
self.ui.bt_prac5.clicked.connect(self.dock_php)

#Acceder a las paginas
self.ui.ELK.clicked.connect(self.ELK)
self.ui.MISP.clicked.connect(self.MISP)
self.ui.CTZ.clicked.connect(self.CTZ)
self.ui.PHP.clicked.connect(self.PHP)

#Acceder a los videos
self.ui.vd1.clicked.connect(self.vd1)
self.ui.vd2.clicked.connect(self.vd2)
self.ui.vd3.clicked.connect(self.vd3)

#Control barra de titulos
self.ui.bt_minimizar.clicked.connect(self.control_bt_minimizar)
self.ui.bt_restaurar.clicked.connect(self.control_bt_normal)
self.ui.bt_maximizar.clicked.connect(self.control_bt_maximizar)
self.ui.bt_cerrar.clicked.connect(lambda: self.close())

self.ui.bt_restaurar.hide()

#Menu lateral
self.ui.bt_menu.clicked.connect(self.mover_menu)

#Funciones para abrir paginas de google

def ELK(self):
    os.system("start chrome https://www.elastic.co/es/what-is/elk-stack")

def MISP(self):
    os.system("start chrome https://www.misp-project.org")

def CTZ(self):
    os.system("start chrome https://cortexaproject.org")

def PHP(self):
    os.system("start chrome https://www.php.net")

def vd1(self):
    os.system("start chrome https://www.youtube.com/watch?v=MhC3ZFY5dNI")
```

```

def vd2(self):
    os.system("start chrome https://www.youtube.com/watch?v=ICN4n8CNkNM")

def vd3(self):
    os.system("start chrome https://www.youtube.com/watch?v=S-CfD_FW3Co")

def abrir1(self):
    os.system("start chrome
https://github.com/ahmedhassank/documentacion")

def abrir2(self):
    os.system("start chrome
https://github.com/ahmedhassank/documentacion")

def abrir3(self):
    os.system("start chrome
https://github.com/ahmedhassank/documentacion")

def abrir4(self):
    os.system("start chrome
https://github.com/ahmedhassank/documentacion")

#Funciones para abrir los contenedores de las herramientas

def dock_elk(self):
    os.system("docker pull ahmedhassank/elk:latest")
    os.system("docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name
elk ahmedhassank/elk")
    os.system("docker start elk")
    os.system("start chrome http://localhost:5601")
    os.system("start chrome http://localhost:9200")

def dock_misp(self):
    os.system("git clone https://github.com/coolacid/docker-misp.git")
    os.system("start chrome https://localhost")
    os.chdir('docker-misp')
    os.system("docker-compose up")

def dock_ctz(self):
    os.system("git clone https://github.com/cortezaproject/corteza-all-in-
one.git")
    os.chdir('corteza-all-in-one')
    os.system("docker build -t corteza/all-in-one .")
    os.system("docker run -it --rm -p 90:80 -e
LOCAL_DEMO_API_PORT=90 -p 93:93 -e LOCAL_DEMO_SPA_PORT=93 -e
HOSTADDR=example.com -e

```

```

DB_DSN=corteza:change-me@tcp(example.com:3306)/corteza?
collation=utf8mb4_general_ci corteza/all-in-one")
    os.system("start chrome https://localhost")

def dock_php(self):
    os.system("docker pull ahmedhassank/php:latest")
    os.system("docker run -p 9000:9000 --name php
ahmedhassank/php:latest")
    os.system("docker start php")
    os.system("start chrome http://localhost:9000")
    os.system("docker exec --workdir /php php php -S 0.0.0.0:9000")

#Funciones para poder ajustar y modificar las caracteristicas del programa

def control_bt_minimizar(self):
    self.showMinimized()

def control_bt_normal(self):
    self.showNormal()
    self.ui.bt_restaurar.hide()
    self.ui.bt_maximizar.show()

def control_bt_maximizar(self):
    self.showMaximized()
    self.ui.bt_maximizar.hide()
    self.ui.bt_restaurar.show()

def mover_menu(self):
    if True:
        width = self.ui.frame_lateral.width()
        normal = 0
        if width==0:
            extender = 200
        else:
            extender = normal
        self.animacion = QPropertyAnimation(self.ui.frame_lateral,
b'minimumWidth')
            self.animacion.setDuration(300)
            self.animacion.setStartValue(width)
            self.animacion.setEndValue(extender)
            self.animacion.setEasingCurve(QtCore.QEasingCurve.InOutQuart)
            self.animacion.start()

def resizeEvent(self, event):
    rect = self.rect()
    self.grip.move(rect.right() - self.gripSize, rect.bottom() - self.gripSize)

def mousePressEvent(self, event):

```

```
self.clickPosition = event.globalPos()

def mover_ventana(self, event):
    if self.isMaximized() == False:
        if event.buttons() == QtCore.Qt.LeftButton:
            self.move(self.pos() + event.globalPos() - self.clickPosition)
            self.clickPosition = event.globalPos()
            event.accept()

    if event.globalPos().y() <=20:
        self.showMaximized()
    else:
        self.showNormal()

#Para iniciar el programa

if __name__ == "__main__":
    app = QtWidgets.QApplication(sys.argv)
    mi_app = MiApp()
    mi_app.show()
    sys.exit(app.exec_())
```

## MAIN.PY (Archivo de funciones del programa en LINUX)

```
import sys
from menu_u import *
from PyQt5 import QtCore
from PyQt5.QtCore import QPropertyAnimation
from PyQt5 import QtCore, QtGui, QtWidgets
import os

class MiApp(QtWidgets.QMainWindow):
    def __init__(self):
        super().__init__()
        self.ui = Ui_MainWindow()
        self.ui.setupUi(self)

        #Eliminar barra y de titulo - opacidad
        self.setWindowFlag(QtCore.Qt.FramelessWindowHint)
        self.setWindowOpacity(1)

        #SizeGrip
        self.gripSize = 10
        self.grip = QtWidgets.QSizeGrip(self)
        self.grip.resize(self.gripSize, self.gripSize)

        #Mover ventana
        self.ui.frame_superior.mouseMoveEvent = self.mover_ventana

        #Acceder a las paginas
        self.ui.bt_inicio.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page))
        self.ui.bt_uno.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_uno))
        self.ui.bt_dos.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_dos))
        self.ui.bt_tres.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_tres))
        self.ui.bt_cinco.clicked.connect(lambda:
self.ui.stackedWidget.setCurrentWidget(self.ui.page_cinco))

        #Acceder a los pdfs
        self.ui.bt_ter1.clicked.connect(self.abrir1)
        self.ui.bt_ter2.clicked.connect(self.abrir2)
        self.ui.bt_ter3.clicked.connect(self.abrir3)
        self.ui.bt_ter5.clicked.connect(self.abrir1)

        #Abrir los dockers
        self.ui.bt_prac1.clicked.connect(self.dock_elk)
        self.ui.bt_prac2.clicked.connect(self.dock_misp)
```

```
self.ui.bt_prac3.clicked.connect(self.dock_ctz)
self.ui.bt_prac5.clicked.connect(self.dock_php)

#Acceder a las paginas
self.ui.ELK.clicked.connect(self.ELK)
self.ui.MISP.clicked.connect(self.MISP)
self.ui.CTZ.clicked.connect(self.CTZ)
self.ui.PHP.clicked.connect(self.PHP)

#Acceder a los videos
self.ui.vd1.clicked.connect(self.vd1)
self.ui.vd2.clicked.connect(self.vd2)
self.ui.vd3.clicked.connect(self.vd3)

#Control barra de titulos
self.ui.bt_minimizar.clicked.connect(self.control_bt_minimizar)
self.ui.bt_restaurar.clicked.connect(self.control_bt_normal)
self.ui.bt_maximizar.clicked.connect(self.control_bt_maximizar)
self.ui.bt_cerrar.clicked.connect(lambda: self.close())

self.ui.bt_restaurar.hide()

#Menu lateral
self.ui.bt_menu.clicked.connect(self.mover_menu)

#Funciones para abrir paginas de google

def ELK(self):
    os.system("firefox https://www.elastic.co/es/what-is/elk-stack")

def MISP(self):
    os.system("firefox https://www.misp-project.org")

def CTZ(self):
    os.system("firefox https://cortezaproject.org")

def PHP(self):
    os.system("firefox https://www.php.net")

def vd1(self):
    os.system("firefox https://www.youtube.com/watch?v=MhC3ZFY5dNI")

def vd2(self):
    os.system("firefox https://www.youtube.com/watch?v=lCN4n8CNkNM")

def vd3(self):
    os.system("firefox https://www.youtube.com/watch?v=S-CfD_FW3Co")

def abrir1(self):
```

```
os.system("firefox https://github.com/ahmedhassank/documentacion")

def abrir2(self):
    os.system("firefox https://github.com/ahmedhassank/documentacion")

def abrir3(self):
    os.system("firefox https://github.com/ahmedhassank/documentacion")

def abrir4(self):
    os.system("firefox https://github.com/ahmedhassank/documentacion")

#Funciones para abrir los contenedores de las herramientas

def dock_elk(self):
    os.system("docker pull ahmedhassank/elk:latest")
    os.system("sysctl -w vm.max_map_count=262144")
    os.system("docker run -p 5601:5601 -p 9200:9200 -p 5044:5044 -it --name
elk ahmedhassank/elk")
    os.system("docker start elk")

def dock_misp(self):
    os.system("git clone https://github.com/coolacid/docker-misp.git")
    os.chdir('docker-misp')
    if os.name == "posix":
        os.system("sudo service apache2 stop && sudo service nginx stop")
    os.system("docker-compose up")

def dock_ctz(self):
    os.system("git clone https://github.com/ahmedhassank/corteza.git")
    os.chdir('corteza')
    os.system("./install.sh")
    os.system("docker-compose up -d")

def dock_php(self):
    os.system("docker pull ahmedhassank/php:latest")
    os.system("docker run -p 9000:9000 --name php
ahmedhassank/php:latest")
    os.system("docker start php")

#Funciones para poder ajustar y modificar las caracteristicas del programa
```

```

def control_bt_minimizar(self):
    self.showMinimized()

def control_bt_normal(self):
    self.showNormal()
    self.ui.bt_restaurar.hide()
    self.ui.bt_maximizar.show()

def control_bt_maximizar(self):
    self.showMaximized()
    self.ui.bt_maximizar.hide()
    self.ui.bt_restaurar.show()

def mover_menu(self):
    if True:
        width = self.ui.frame_lateral.width()
        normal = 0
        if width==0:
            extender = 200
        else:
            extender = normal
        self.animacion = QPropertyAnimation(self.ui.frame_lateral,
b'minimumWidth')
        self.animacion.setDuration(300)
        self.animacion.setStartValue(width)
        self.animacion.setEndValue(extender)
        self.animacion.setEasingCurve(QtCore.QEasingCurve.InOutQuart)
        self.animacion.start()

def resizeEvent(self, event):
    rect = self.rect()
    self.grip.move(rect.right() - self.gripSize, rect.bottom() - self.gripSize)

def mousePressEvent(self, event):
    self.clickPosition = event.globalPos()

def mover_ventana(self, event):
    if self.isMaximized() == False:
        if event.buttons() == QtCore.Qt.LeftButton:
            self.move(self.pos() + event.globalPos() - self.clickPosition)
            self.clickPosition = event.globalPos()
            event.accept()

        if event.globalPos().y() <=20:
            self.showMaximized()
        else:
            self.showNormal()

#Para iniciar el programa

```

```
if __name__ == "__main__":
    app = QtWidgets.QApplication(sys.argv)
    mi_app = MiApp()
    mi_app.show()
    sys.exit(app.exec_())
```

## JUEGO PHP (Al ser muchos archivos y líneas de código dejamos en enlace a Github)

**Repositorio:** [ENLACE](#)

## 8. CONCLUSIÓN

Las conclusiones que hemos podido sacar durante el tiempo en el que hemos realizado el proyecto, es que los programas y herramientas que hemos metido en nuestra aplicación tienen un uso bastante interesante, incluso para adaptarlo a alguna empresa que las quiera utilizar. También que el PyQt Designer es una herramienta bastante interesante para hacer entornos gráficos de Python y que sabiendo utilizarla en un nivel avanzado se puede llegar a hacer cosas bastantes preparadas y cómodas visualmente.

Respecto a nuestra parte más personal, este proyecto ha sido una manera de trabajar en equipo siguiendo horarios y fechas que nos hemos puesto, de esta manera, obligándonos a cumplir esos horarios y objetivos, de manera que nos ha permitido trabajar de una manera eficiente, siempre y claro respetando descansos. Ha sido también más complicado por el tema de estar haciendo las prácticas al mismo tiempo, ya que nos ocupaban la mayoría del tiempo.

## 9.BIBLIOGRAFÍA

<https://www.elastic.co/es/what-is/elk-stack>  
<https://www.MISP-project.org/>  
<https://cortezaproject.org/>  
<https://medium.com/@hektorprofe/primeros-pasos-en-pyqt-5-y-qt-designer-programas-gr%C3%A1ficos-con-python-6161fba46060>  
<https://build-system.fman.io/qt-designer-download>  
[https://www.youtube.com/watch?v=rC6uR9gR6w4&ab\\_channel=SpinnTV](https://www.youtube.com/watch?v=rC6uR9gR6w4&ab_channel=SpinnTV)  
<https://www.flaticon.es/uicons>  
<https://www.elastic.co/guide/index.html>  
<https://hub.docker.com/u/ahmedhassank>  
<https://hub.docker.com/r/cortezaproject/corteza-server>  
<https://github.com/coolacid/docker-misp.git>  
<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-20-04-es>  
<https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-on-ubuntu-20-04-es>